# Group of p -th roots of unity modulo n 

Rochdi Omami, Mohamed Omami and Raouf Ouni


#### Abstract

Let $n \geq 3$ be an integer and $p$ be a prime odd number.


 Let us consider $\mathbf{G}_{p}(n)$ the subgroup of $(\mathbb{Z} / n \mathbb{Z})^{*}$ defined by :$$
\mathbf{G}_{p}(n)=\left\{x \in(\mathbb{Z} / n \mathbb{Z})^{*} / x^{p}=1\right\}
$$

In this paper, we give an algorithm that computes a generating set of this subgroup.

Keywords-Group, p-th roots, modulo, unity.

## I. Introduction

LET $n \geq 3$ be an integer, recall that $(\mathbb{Z} / n \mathbb{Z})^{*}$ denotes the group of units of the ring $(\mathbb{Z} / n \mathbb{Z})$. For more details on the structure of $(\mathbb{Z} / n \mathbb{Z})^{*}$ see [2], [3] and [4].
The group $(\mathbb{Z} / n \mathbb{Z})^{*}$ has several applications, the most important is cryptography, that is RSA cryptosystem (see [7]). The security of the RSA cryptosystem is based on the problem of factoring large integers and the task of finding $e$-th roots modulo a composite number $n$ whose factors are not known.

Let $p$ be a prime odd number, we notice by $\mathbf{G}_{p}(n)$ the part of $(\mathbb{Z} / n \mathbb{Z})^{*}$ formed by the elements $x$ that verify $x^{p}=1$. We can easily prove that $\mathbf{G}_{p}(n)$ is a subgroup of $(\mathbb{Z} / n \mathbb{Z})^{*}$ which contains exactly the unity and the elements of order $p$.
Remember also that these elements of order $p$ in $(\mathbb{Z} / n \mathbb{Z})^{*}$ exist if and only if $p$ divides $\lambda(n)$, with $\lambda$ is the Carmichael lambda function, otherwise $\mathbf{G}_{p}(n)$ is not reduced to $\{1\}$ if and only if $p$ divides $\lambda(n)$.
The elements of $\mathbf{G}_{p}(n)$ other than 1 have the order $p$ and so the order of $\mathbf{G}_{p}(n)$ is of the form $p^{t}$ with $t$ an integer. Then we obtain the following result:

## Proposition :

Let $n \geq 3$ be an integer and $p$ be a prime number, then there exists an integer $t$ such as :

$$
\operatorname{Card}\left(\mathbf{G}_{p}(n)\right)=p^{t}
$$

with $t=0$ if and only if $p$ does not divide $\lambda(n)$.
Our work consists to determine explicitly the integer $t$ described in the preceding proposition and by giving at the same time with an effective manner the decomposition of $\mathbf{G}_{p}(n)$ in product of cyclic groups and give a generating family of this group. Finally, we give the algorithm written in Maple. The case $p=2$ is treated in [1] and in this article, our approach is the same as it. For more details about the algorithmic number theory see [5] and [6], and for introduction to Maple see [10].

## II. P-TH ROOTS OF UNITY MODULO N

Let us consider an integer $n \geq 3$ and $p$ a prime odd number, let $n=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ the decomposition of $n$ in prime factors.
We know that the p-th roots of unity modulo $n$, which are nontrivial, exist if and only if $p$ divides $\lambda(n)$, that is to say $\alpha \geq 2$ or there exists $i$ such as $p$ divides $p_{i}-1$.
Thus, in our study, we will distinguish these following cases $\alpha=0, \alpha=1$ and $\alpha \geq 2$, but before that we are going to give some results which will be useful thereafter.

Definition 2.1: Let $n \geq 3$ be an integer and $p$ be a prime number, we denote $\alpha_{p}(n)$ the number of prime factors $q$ of $n$ such that $p$ divides $q-1$.

## Remark :

- $\alpha_{2}(n)$ is the number of prime odd factors of $n$.
- The function $\alpha_{p}$ is additive, that is to say if $n$ and $m$ are coprime numbers, then

$$
\alpha_{p}(m . n)=\alpha_{p}(m)+\alpha_{p}(n)
$$

and generally, for all the numbers not equal to $0, n$ and $m$ we have:

$$
\alpha_{p}(m . n)=\alpha_{p}(m)+\alpha_{p}(n)-\alpha_{p}(G C D(m, n))
$$

In the following, we consider an integer $n \geq 3$ whose the factorization is $n=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$, with $p$ a prime odd number dividing $\lambda(n)$.

Proposition 2.1: Let $x$ be a $p$-th root of unity modulo $n$. If $p$ does not divide $p_{i}-1$, then $p_{i}$ divides $x-1$.

## Proof:

We have $x^{p} \equiv 1[n] \Longrightarrow x^{p} \equiv 1\left[p_{i}\right]$ and thus the order of $x$ in $\left(\mathbb{Z} / p_{i} \mathbb{Z}\right)^{*}$ is 1 or $p$, but the order of $x$ in $\left(\mathbb{Z} / p_{i} \mathbb{Z}\right)^{*}$ divides $p_{i}-1$ and thus it cannot be $p$. Therefore $x \equiv 1\left[p_{i}\right]$ and then we obtain the result.

Now, we will ameliorate the precedent result with the following lemma:

Lemma 2.1:

$$
G C D\left(x-1,1+x+x^{2}+\ldots+x^{p-1}\right) \in\{1, p\}
$$

Proof:
One can easily verify that we have:

$$
\begin{array}{r}
(x-1)\left(x^{p-2}+2 x^{p-3}+3 x^{p-4}+\ldots+(p-2) x+(p-1)\right)- \\
\left(1+x+x^{2}+\ldots+x^{p-1}\right)=p
\end{array}
$$

# International Journal of Engineering, Mathematical and Physical Sciences <br> ISSN: 2517-9934 <br> Vol:4, No:7, 2010 

Corollary 2.1: Let $x$ be a $p$-th root of unity modulo $n$. If $p$ does not divide $p_{i}-1$ and $p \neq p_{i}$, then $p_{i}^{\alpha_{i}}$ divides $x-1$.

Proof:
We have $x^{p} \equiv 1[n] \Longrightarrow x^{p} \equiv 1\left[p_{i}^{\alpha_{i}}\right]$ then $p_{i}^{\alpha_{i}}$ divides $x^{p}-1=(x-1)\left(1+x+x^{2}+\ldots+x^{p-1}\right)$, or $p$ does not divide $p_{i}-1$ and thus $p_{i}$ divides $x-1$ also we know that the $G C D\left(x-1,1+x+x^{2}+\ldots+x^{p-1}\right) \in\{1, p\}$ and $p \neq p_{i}$, then $p_{i}^{\alpha_{i}}$ divides $x-1$.

If $p$ divides $n$, that is to say $\alpha \geq 1$, and $x$ is a $p$-th root of unity modulo $n$, then $p$ divides $x^{p}-1=(x-1)\left(1+x+x^{2}+\ldots+x^{p-1}\right)$ and consequently $p$ divides $x-1$ or $1+x+x^{2}+\ldots+x^{p-1}$ and seeing the relation given in the proof of Lemma 2.1 we conclude that $p$ divides both at the same time, and thus

$$
P G C D\left(x-1,1+x+x^{2}+\ldots+x^{p-1}\right)=p .
$$

We are interested now in the case of $\alpha \geq 2$, we saw in [1] for $p=2$ that $2^{\alpha-1}$ divides $x-1$ or $x+1$, we are going to see that this result is not true for an odd prime $p$ and more precisely we have the following result:

Proposition 2.2: Let $x$ be a $p$-th root of unity modulo $n$ $(\alpha \geq 2)$, then $p^{\alpha-1}$ divides $x-1$.

The case $\alpha=2$ is trivial, for $\alpha \geq 3$, one needs the following lemma:

Lemma 2.2: Let $p$ be a prime odd number and $x$ be an integer, then we have :

$$
x^{p} \equiv 1\left[p^{3}\right] \Longrightarrow x \equiv 1\left[p^{2}\right]
$$

Proof:
It is clear that $x^{p} \equiv 1\left[p^{3}\right] \Longrightarrow x \equiv 1[p]$, so $x=1+k p$ $\left(k \in \mathbb{N}\right.$ ) and consequently $x^{p} \equiv 1+p^{2} k\left[p^{3}\right]$ (this writing is possible because $p \geq 3$ ) moreover $p^{3}$ divides $p^{2} k$, then $p$ divides $k$ and finally we obtain: $x \equiv 1\left[p^{2}\right]$.

Remark : Notice that the precedent lemma is not true for $p=2$, for instance $3^{2} \equiv 1[8]$ and $3 \not \equiv 1[4]$.

## Proof of Proposition 2.2:

We have $x^{p} \equiv 1\left[p^{\alpha}\right](\alpha \geq 3)$ and so in particulary $x^{p} \equiv 1\left[p^{3}\right]$, from the precedent lemma we conclude that $x \equiv 1\left[p^{2}\right]$.
We have $p^{\alpha}$ divides $x^{p}-1=(x-1)\left(1+x+x^{2}+\ldots+x^{p-1}\right)$ and as $P G C D\left(x-1,1+x+x^{2}+\ldots+x^{p-1}\right)=p$ besides $p^{2}$ divides $x-1$, so $p^{\alpha-1}$ divides $x-1$.

## Remark :

The precedent proposition shows that $p^{\alpha-1}$ divides $x-1$, but this does not mean that the p -adic valuation of $x-1$ is $\alpha-1$ and this is proved by the following examples.

## An application example :

- $n=7^{3} * 29=9947$, we have $344^{7} \equiv 1[n]$ and $344 \equiv 1\left[7^{3}\right] .2402^{7} \equiv 1[n]$ and $2402 \equiv 1\left[7^{4}\right]$.
- $n=7^{2} * 29 * 43 * 71=4338313$, we have $350547^{7} \equiv 1[n]$ and $350547 \equiv 1\left[7^{4}\right]$.

Let us return to our principal aim, which is the study of the group $\mathbf{G}_{p}(n)$, we begin by the case $\alpha=0$.

## Case 1: $\alpha=0$

Let $n$ be an integer whose decomposition into prime factors is $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $p_{i} \neq p$ for all $i$. Let $x$ be a $p$-th root of unity modulo $n$, we have shown in the above results that if $p$ does not divide $p_{i}-1$, then $p_{i}^{\alpha_{i}}$ divides $x-1$. The condition $p$ divides $\lambda(n)$ implies that it exists at least an integer $i$ such that $p$ divides $p_{i}-1$, let $\sigma$ be a permutation of the set $\{1,2, . ., m\}$ such that $n=p_{\sigma_{\sigma(1)}}^{\alpha_{\sigma(1)}} p_{\sigma_{\alpha(2)}}^{\alpha_{\alpha_{\sigma(2)}}^{\alpha_{(2)}}} \ldots p_{\sigma(d)}^{\alpha_{\sigma(d)}} p_{\sigma_{\sigma(d+1)}}^{\alpha_{\alpha(d+1)}} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$ and $p$ divides only $p_{\sigma(1)}^{\alpha_{\sigma(1)}}, p_{\sigma(2)}^{\alpha_{\sigma}(2)} \ldots$ and $p_{\sigma(d)}^{\alpha_{\sigma(d)}}$, then $p_{\sigma(d+1)}^{\alpha_{\sigma(d+1)}} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$ divides $x-1$.
We start our study by the following theorem:
Theorem 2.1: Let $n$ be an integer whose decomposition in prime factors is $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $p_{i} \neq p$ for all $i$ and $p$ divides only $p_{1}-1$, then $\mathbf{G}_{p}(n)$ is a cyclic subgroup of $(\mathbb{Z} / n \mathbb{Z})^{*}$ of order $p$.

## Proof :

Let $x$ be a $p$-th root of unity modulo $n$, we have $p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ divides $x-1$, then $x$ is a solution of one of the following systems :

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1}^{\alpha_{1}} K^{\prime}
\end{array}\right. \\
& \left\{\begin{array}{c}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=K^{\prime}
\end{array}\right.
\end{aligned}
$$

Clearly, 1 is the unique solution of the second system. Now, we will show that the first system have exactly $p-1$ solutions, which follows immediately from the two following lemmas.

Lemma 2.3: The systems

$$
\begin{align*}
& \left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1}^{\alpha_{1}} K^{\prime}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1} K^{\prime}
\end{array}\right. \tag{**}
\end{align*}
$$

have the same number of solutions respectively modulo $n$ and $n / p_{1}^{\alpha_{1}-1}$.

Proof :
It is clear that any solution of $(\star)$ is a solution of $(\star \star)$. Reciprocally let $x$ be a solution of ( $(\star)$, then $x^{p} \equiv 1\left[p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}\right]$
that is to say $x^{p}=1+p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}$ and therefore

$$
\begin{aligned}
x^{p p_{1}^{\alpha_{1}-1}}= & \left(1+p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}\right)^{p_{1}^{\alpha_{1}-1}} \\
= & 1+\sum_{i=1}^{p_{1}^{\alpha_{1}-1}-1} \mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}\left(p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}\right)^{i}+ \\
& \left(p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}\right)^{p_{1}^{\alpha_{1}-1}}
\end{aligned}
$$

It is easily verified that all $\mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}$ are divisible by $p_{1}^{\alpha_{1}-1}$ and $p_{1}^{\alpha_{1}-1} \geq \alpha_{1}$, then $x^{p p_{1}^{\alpha_{1}-1}} \equiv 1[n]$. From the other hand

$$
\begin{aligned}
x^{p_{1}^{\alpha_{1}-1}}= & \left(1+p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K\right)^{p_{1}^{\alpha_{1}-1}} \\
= & 1+\sum_{i=1}^{p_{1}^{\alpha_{1}-1}-1} \mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}\left(p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K\right)^{i}+ \\
& \left(p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K\right)^{p_{1}^{\alpha_{1}-1}}
\end{aligned}
$$

and as the $\mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}$ are divisible by $p_{1}$ and $K$ is not divisible by $p_{1}$, then $x^{p_{1}^{\alpha_{1}-1}}{ }_{\alpha_{1}}$ is divisible by all the $p_{i}$ except $p_{1}$ and consequently $x^{p_{1}^{\alpha_{1}-1}}$ is a solution of $(\star)$.
Let $x$ and $y$ be two solutions of ( $* *$ ) such as $x^{p_{1}^{\alpha_{1}-1}}=y^{p_{1}^{\alpha_{1}-1}}[n]$ and thus $x^{p_{1}^{\alpha_{1}-1}}=y^{p_{1}^{\alpha_{1}-1}}\left[p_{1}\right]$, hence $x \equiv y\left[p_{1}\right]$, on the other hand it is clear that $x \equiv y\left[p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}\right]$ and consequently $x \equiv y\left[p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}\right]$.
We therefore conclude that the number of solutions of $(\star)$ is greater than or equal to that of $(\star \star)$. Thus the systems $(\star)$ and ( $* *$ ) have the same number of solutions modulo $n$ and $n / p_{1}^{\alpha_{1}-1}$ respectively.

Lemma 2.4: The following system

$$
\left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1} K^{\prime}
\end{array}\right.
$$

has $p-1$ solutions modulo $n / p_{1}^{\alpha_{1}-1}$.

## Proof:

We know that $\mathbb{Z} / p_{1} \mathbb{Z}$ is the field of decomposition of the polynomial $X^{p_{1}}-X$, and more precisely we have :

$$
X^{p_{1}}-X=\prod_{i=0}^{p_{1}-1}(X-i)
$$

and therefore

$$
X^{p_{1}-1}-1=\prod_{i=1}^{p_{1}-1}(X-i)
$$

and as $p$ divides $p_{1}-1$ then the polynomial $X^{p}-1$ divides $X^{p_{1}-1}-1$ and therefore the polynomial $X^{p}-1$ is also a product of factors of degree 1 , that is to say

$$
X^{p}-1=\prod_{i=1}^{p}\left(X-\gamma_{i}\right)
$$

and as 1 is a root of $X^{p}-1$ then we take $\gamma_{1}=1$ and finally we obtain

$$
1+X+X^{2}+\ldots X^{p-1}=\prod_{i=2}^{p}\left(X-\gamma_{i}\right)
$$

and consequently the system $(\star \star)$ is equivalent to the following systems:

$$
\begin{aligned}
\left\{\begin{aligned}
x-1= & p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{2} \\
x-\gamma_{2}= & p_{1} K_{2}^{\prime}
\end{aligned}\right. & \left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{3} \\
x-\gamma_{3}=p_{1} K_{3}^{\prime}
\end{array}\right. \\
& \ldots\left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{p} \\
x-\gamma_{p}=p_{1} K_{p}^{\prime}
\end{array}\right.
\end{aligned}
$$

It is clear that each of these systems has only one solution modulo $p_{1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$. Also the solutions of these systems are 2 by 2 distinct. Indeed if we denote $x_{i}$ the solution of the following system

$$
\left\{\begin{array}{l}
x-1=p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{i} \\
x-\gamma_{i}=p_{1} K_{i}^{\prime}
\end{array}\right.
$$

then $x_{i} \equiv \gamma_{i}\left[p_{1}\right]$. Since the $\gamma_{i}$ are distinct modulo $p_{1}$, then the $x_{i}$ are also distinct. We conclude that ( $\star \star$ ) have $p-1$ solutions modulo $n / p_{1}^{\alpha_{1}-1}$.

## Remark:

The proof of the previous theorem gives an algorithm for calculating the solutions of $(\star)$, and this is done in two steps : Step 1
$\overline{\text { We resolve }}(\star \star)$, the most difficult point in this step is to determinate the $\gamma_{i}$. We must give the factorization of the polynomial $1+X+X^{2}+\ldots+X^{p-1}$ in the field $\mathbb{Z} / p_{1} \mathbb{Z}[X]$ and for this we can use Berlekamp's algorithm [8] or Cantor-Zassenhaus algorithm [9]. Then we decompose ( $\star \star$ ) in small systems that are resolved easily with Euclidian's algorithm.

## Step 2

To find the solutions of $(\star)$, it is sufficient to see that they are also solutions of $(\star \star)$ set to the power $p_{1}^{\alpha_{1}-1}$ modulo $n$.

Note also that the set of solutions of ( $\star$ ) forms with 1 a cyclic group of order $p$, then any solution of $(\star)$ generates this group. Thus in practice it is sufficient to determine a solution of $(\star)$ to find the others.

A sample calculation :
We want to determine the elements of order 7 modulo $n$ with $n=10609215=29^{4} * 5 * 3$. The first step consists to give the factorization of $1+X+X^{2}+\ldots+X^{6}$ in the field $\mathbb{Z} / 29 \mathbb{Z}[X]$, by using Berlekamp's algorithm, we obtain :

$$
\begin{aligned}
& 1+X+X^{2}+\ldots+X^{6} \\
= & (X+4)(X+5)(X+6)(X+9)(X+13)(X+22) .
\end{aligned}
$$

Let's consider the following system

$$
\left\{\begin{array}{l}
x-1=15 K \\
x+4=29 K^{\prime}
\end{array}\right.
$$

which gives $29 K^{\prime}-15 K=5$, and by the euclidian algorithm we obtain $K^{\prime}=-5$ and $K=-10$.

Therefore $x=-149=286$ modulo $435=29 * 5 * 3$. Thereby $286^{29^{3}} \bmod n=1006441$ is an element of order 7 modulo $n$ and consequently the elements of $\mathbf{G}_{7}(n)$ are

$$
\mathbf{G}_{7}(n)=\left\{1006441,1006441^{2}, \ldots, 1006441^{7}\right\}
$$

that is to say

$$
\begin{aligned}
& \mathbf{G}_{7}(n)=\{1006441,8684356,6860611,4797001, \\
& 5450251,9979951,1\}
\end{aligned}
$$

Now, we give an algorithm in MAPLE which allows us for any fixed integer $n$ and a prime odd number $p$, as described in the last theorem, to give a generator of the cyclic group $\mathbf{G}_{p}(n)$.

Gene_p $:=\operatorname{proc}(n, p) \quad$ local LB, LD,$P$, gen,, LFact; $L D:=[] ; L B:=[] ;$
LFact $:=$ ifactors $(n)[2]$;
for $i$ from 1 to nops(LFact) do
if $($ LFact $[i][1]-1 \bmod p=0)$ then
$L D:=[$ op $(L D), L F a c t[i]] ;$
end:
end:
$P:=\operatorname{convert}(\operatorname{Berlekamp}(\widehat{x p}-1, x) \bmod L D[1][1]$, list); if $(P[1]-x+1 \bmod L D[1][1]<>0)$ then
$L B:=\operatorname{Bezout}\left(L D[1][1], n /\left(L D[1][1]^{\wedge} L D[1][2]\right), P[1]-\right.$ $x+1$ );
gen $:=((L D[1][1] * L B[1]-(P[1]-x) \bmod n)) \&^{\wedge}$
$\left(L D[1][1]^{\wedge}(L D[1][2]-1)\right) \bmod n$;
else
$L B:=\operatorname{Bezout}\left(L D[1][1], n /\left(L D[1][1]^{\wedge} L D[1][2]\right), P[2]-\right.$ $x+1$ );
gen $:=(L D[1][1] * L B[1]-(P[2]-x) \bmod n) \not \&^{\wedge}$
$\left(L D[1][1]^{\wedge}(L D[1][2]-1)\right) \bmod n$;
end :
eval(gen);
end :
end :
Algorithm 2.1

## Remark :

The Berlekamp's procedure used in this algorithm is predefined in MAPLE.

In the remainder of this paragraph, considering an integer $n$ whose decomposition in prime factors is $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ and $p$ a prime odd number such that $p_{i} \neq p$ for all $i$. For a fixed permutation we can write $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} p_{d+1}^{\alpha_{d+1}} \ldots p_{m}^{\alpha_{m}}$ with $p$ divides $p_{i}-1$ for all $i \in\{1, . ., d\}$. We have seen that if $x$ is a $p$-th root of unity modulo $n$, then $p_{d+1}^{\alpha_{d+1}} \ldots p_{m}^{\alpha_{m}}$ divides $x-1$. Thus $p_{d+1}^{\alpha_{d+1}} \ldots p_{m}^{\alpha_{m}}$ don't have a significant role in our study, for the rest we set $p_{d+1}^{\alpha_{d+1}} \ldots p_{m}^{\alpha_{m}}=A$.

Definition 2.2: Let $x$ a $p$-th root of unity modulo $n$, we say that $x$ is initial if all the $p_{i}, i \in\{1, . ., d\}$ divides $x-1$ except for only one $p_{i}$. We say that this $p$-th root is associated to $p_{i}$, and we write :

$$
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K . . . .}{ }
$$

with $K$ is an integer not divisible par $p_{i}$.
We denote by $\mathbf{G}_{p}^{p_{i}}(n)$ the set formed by the unity and the initial $p$-th roots of unity associated to $p_{i}$, and we have the following theorem :

Theorem 2.2: $\mathbf{G}_{p}^{p_{i}}(n)$ is a cyclic subgroup of $\mathbf{G}_{p}(n)$ with cardinality $p$.

Proof:
The initial $p$-th roots of unity associated to $p_{i}$ are the solutions of the system :

$$
\left\{\begin{array}{l}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K \\
1+x+x^{2}+. .+x^{p-1}=p_{i}^{\alpha_{i}} K^{\prime}
\end{array}\right.
$$

We saw in the foregoing that this system have $p-1$ solutions modulo $n$ and then $\operatorname{Card}\left(\mathbf{G}_{p}^{p_{i}}(n)\right)=p$. Let's prove now that $\mathbf{G}_{p}^{p_{i}}(n)$ is a subgroup. Let $x$ and $y$ be two solutions of $(\star)$, we have

$$
\begin{aligned}
& y-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}
\end{aligned}
$$

and therefore

$$
\begin{aligned}
x . y & =1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A(K \\
& \left.+K^{\prime}+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K K^{\prime}\right)
\end{aligned}
$$

Note that $x . y$ is a $p$-th root of unity and therefore at this stage we have two case. If $p_{i}$ divides $\left(K+K^{\prime}+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K K^{\prime}\right)$, then $p_{i}^{\alpha_{i}}$ divides $x . y-1$ and we obtain $x . y=1$. If $p_{i}$ does not divide $\left(K+K^{\prime}+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K K^{\prime}\right)$, then $x . y$ is an initial to $p$-th root of unity associated to $p_{i}$. It is clear that if $x$ is a $p$-th root of unity, then its inverse $x^{-1}=x^{p-1}$ is an element of $\mathbf{G}_{p}^{p_{i}}(n)$. Whereof $\mathbf{G}_{p}^{p_{i}}(n)$ is a cyclic subgroup of $\mathbf{G}_{p}(n)$ because its cardinality is a prime number $p$.

Proposition 2.3: Let $x$ and $y$ be two initial $p$-th roots of unity associated to $p_{i}$ and $p_{j}$ with $i \neq j$, then $x . y$ is a $p$-th root of unity satisfying

$$
x . y-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee_{i}^{\alpha_{i}}} \ldots \stackrel{\vee p_{j}^{\alpha_{j}}}{V_{i}} . p_{d}^{\alpha_{d}} A K
$$

with $K$ is an integer which is not divisible by $p_{i}$ and $p_{j}$.
Proof:
We have

$$
\begin{gathered}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{d}^{\alpha_{d}} A K_{1} \text { and } \\
y-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{j}^{\alpha_{j}} \ldots p_{d}^{\alpha_{d}} A K_{2}
\end{gathered}
$$

and therefore
$x . y=1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}}}{\ldots} \stackrel{\vee p_{j}^{\alpha_{j}}}{ } \ldots p_{d}^{\alpha_{d}} A\left(p_{i}^{\alpha_{j}} K_{1}+p_{i}^{\alpha_{i}} K_{2}\right)$

ISSN: 2517-9934
Vol:4, No:7, 2010
and as $p_{i}$ does not divide $K_{1}$ also $p_{j}$ does not divide $K_{2}$, then $\left(p_{i}^{\alpha_{j}} K_{1}+p_{i}^{\alpha_{i}} K_{2}\right)$ is not divisible by both $p_{i}$ and $p_{j}$.

Definition 2.3: Let $x$ be a $p$-th root of unity modulo $n$, we say that it is final if all the $p_{i}, i \in\{1, . ., d\}$ does not divide $x-1$, that is to say $x-1=A K$, with $K$ an integer not divisible by any $p_{i}, i \in\{1, . ., d\}$.

## Remark :

The existence of final $p$-th roots of unity modulo $n$ is ensured by the preceding proposition, in fact if for all $i \in\{1, . ., d\}$ we take $x_{i}$ an initial $p$-th root of unity associated to $p_{i}$, then $\prod_{i=1}^{d} x_{i}$ is a final $p$-th root of unity modulo $n$.

Definition 2.4: Let $x$ and $y$ be two $p$-th roots of unity modulo $n$, we say that $y$ is a final conjugate of $x$ if $x . y-1$ is not divisible by any of the $p_{i}, i \in\{1, . ., d\}$, that is to say $x . y$ is a final $p$-th root of unity modulo $n$.

Proposition 2.4: Any $p$-th root of unity modulo $n$ have a final conjugate.

## Proof :

If $x=1$ or $x$ is a final $p$-th root of unity modulo $n$, then we have the result. When $d=1$, then a final $p$-th root of unity modulo $n$ is also an initial $p$-th root of unity associated to $p_{1}$ and thus all the $p$-th roots of unity distinct from 1 are final.
Now, we suppose that $d \geq 2$ and $x-1$ is divisible by a nonempty subset of $p_{i}$ of cardinality $t<d$ and we can assume that, for a fixed permutation, this $p_{i}$ are $p_{1}, p_{2}, \ldots$ are $p_{t}$ and thus

$$
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t}^{\alpha_{t}} A K
$$

with $K$ is an integer which is not divisible by any of the $p_{i}$, $i \in\{t+1, . ., d\}$. For all $i \in\{1, . ., t\}$ let $x_{i}$ be an initial $p$-th root of unity associated to $p_{i}$ and therefore
with $K_{i}$ not divisible by $p_{i}$, and thus

$$
\begin{aligned}
& \prod_{i=1}^{t} x_{i}=\prod_{i=1}^{t}\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right) \\
& =1+p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A \sum_{i=1}^{t} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots v_{i}^{\vee_{i}} \ldots p_{t}^{\alpha_{t}} K_{i}+K^{\prime} n
\end{aligned}
$$

but $\sum_{i=1}^{t} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{t}^{\alpha_{t}} K_{i}$ is not divisible by any of the $p_{i}, i \in\{1, . ., t\}$ therefore $y=\prod_{i=1}^{t} x_{i}$ is a $p$-th root of unity satisfies $y=1+p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M$ with $M$ an integer which is not divisible by $p_{i}, i \in\{1, \ldots, t\}$. So

$$
x . y=1+A\left(p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M+p_{1}^{\alpha_{1}} \ldots p_{t}^{\alpha_{t}} A K\right)
$$

It is clear that $\left(p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M+p_{1}^{\alpha_{1}} \ldots p_{t}^{\alpha_{t}} A K\right)$ is not divisible by any of the $p_{i}, i \in\{1, . ., d\}$, and hence the result.

Theorem 2.3: Let $x$ be a final $p$-th root of unity modulo $n$, then it exists $d$ integers $K_{1}, K_{2}, \ldots, K_{d}$ such as:

$$
x=1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee} \ldots p_{d}^{\alpha_{d}} A K_{i}
$$

and

$$
\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\ldots} p_{d}^{\alpha_{d}} A K_{i}\right)^{p}=1[n] \quad \forall 1 \leq i \leq d
$$

Proof:
Since $p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots{\underset{\sim}{p}}_{d}^{\alpha_{d}}$ and $p_{d}^{\alpha_{d}}$ are coprime then it exists two integers $\widetilde{K}_{d}^{\prime}$ and $\widetilde{K}_{d}$ such as

$$
1=p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} \widetilde{K}_{d}(\star)
$$

and therefore

$$
x-1=p_{d}^{\alpha_{d}} A K_{d}^{\prime}+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p_{d}^{\alpha_{d}} A K_{d}}{ }
$$

with $K_{d}^{\prime}=((x-1) / A) \widetilde{K}_{d}^{\prime}$ and $K_{d}=((x-1) / A) \widetilde{K}_{d}$.
We have :

$$
\begin{aligned}
\left(x-p_{d}^{\alpha_{d}} A K_{d}^{\prime}\right)^{p}= & \left(x-(x-1) p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)^{p} \\
= & \left(a\left(1-p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)+p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)^{p} \\
= & \left(x p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} \widetilde{K}_{d}+p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)^{p} \\
= & \left(p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} \widetilde{K}_{d}\right)^{p}+\left(p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)^{p} \quad\left[p_{1}^{\alpha_{1}}\right. \\
& \left.p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}}\right] \\
= & 1\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}}\right] \quad \text { from }(\star)
\end{aligned}
$$

On the other hand

$$
\begin{aligned}
x-(x-1) p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime} & =1+(x-1)\left(1-p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right) \\
& =1[A]
\end{aligned}
$$

Thus $\left(x-(x-1) p_{d}^{\alpha_{d}} \widetilde{K}_{d}^{\prime}\right)^{p}=1[n]$ and consequently $(1+$ $\left.p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{d}\right)^{p}=1[n]$.
Suppose that it exists some integers $K_{t}, K_{2}, \ldots, K_{d}$ and $K_{t}^{\prime}$ such as :

$$
x=1+\sum_{i=t}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{d}^{\alpha_{d}} A K_{i}+p_{t}^{\alpha_{t}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}
$$

and

Let $\widetilde{K}_{t-1}$ and $\widetilde{K}_{t-1}^{\prime}$ be two integers such as

$$
1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{\alpha_{t-1}}} \widetilde{K}_{t-1}+p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}(\star \star)
$$

and therefore

$$
\begin{gathered}
p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}=p_{1}^{\alpha_{1}} \ldots p_{t-1}^{\vee_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}+ \\
p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}
\end{gathered}
$$

We have

$$
\begin{aligned}
& \left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1-p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}\right)^{p} \\
= & \left(\left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1\right)\left(1-p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}\right)+\right. \\
& \left.p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}\right)^{p} \\
= & \left(\left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1\right) p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}+\right. \\
& \left.p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}\right)^{p} \\
= & \left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1\right)^{p}\left(p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}\right)^{p}+ \\
& \left(p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}\right)^{p}\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}}\right]
\end{aligned}
$$

however

$$
\begin{aligned}
& \left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1\right)^{p} \\
= & \left(x-\sum_{i=t}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right)^{p} \\
= & x^{p}\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}} A\right] \\
= & 1\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}} A\right]
\end{aligned}
$$

and consequently

$$
\begin{aligned}
& \left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1-p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}\right)^{p} \\
= & \left(p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}\right)^{p}+ \\
& \left(p_{t-1}^{\alpha_{t-1}} \widetilde{K}_{t-1}^{\prime}\right)^{p}\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}}\right] \\
= & 1\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t-1}^{\alpha_{t-1}}\right] \text { from }(\star \star)
\end{aligned}
$$

also it is clear that

$$
\begin{aligned}
& \left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1-p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}\right)^{p}= \\
& 1\left[p_{d}^{\alpha_{d}} \ldots p_{t}^{\alpha_{t}} A\right]
\end{aligned}
$$

and so
$\left(p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime}+1-p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}\right)^{p}=1[n]$
That means

$$
\left(1+p_{1}^{\alpha_{1}} \ldots p_{t-1}^{\vee_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t}^{\prime} \widetilde{K}_{t-1}\right)^{p}=1[n] .
$$

We set $K_{t-1}=K_{t}^{\prime} \widetilde{K}_{t-1}$ and $K_{t-1}^{\prime}=K_{t}^{\prime} \widetilde{K}_{t-1}^{\prime}$, we obtain so

$$
\begin{aligned}
x= & 1+\sum_{i=t}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee} \ldots p_{d}^{\alpha_{d}} A K_{i}+ \\
& p_{1}^{\alpha_{1}} \ldots p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t-1}+p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t-1}^{\prime} \\
= & 1+\sum_{i=t-1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}+ \\
& p_{t-1}^{\alpha_{t-1}} \ldots p_{d}^{\alpha_{d}} A K_{t-1}^{\prime}
\end{aligned}
$$

with

Thus by induction, we obtain

$$
\begin{aligned}
x & =1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{d}^{\alpha_{d}} A K_{i}+p_{1}^{\alpha_{1}} \ldots p_{d}^{\alpha_{d}} A K_{1}^{\prime} \\
& =1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots v_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i} \quad[n]
\end{aligned}
$$

with $\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right)^{p}=1[n], \forall 1 \leq i \leq d$
Corollary 2.2: Any final $p$-th root of unity modulo $n$ is a product of $d$ initial $p$-th roots associated respectively to $p_{1}, p_{2} \ldots$ and $p_{d}$.

## Proof :

From the precedent theorem, it exists some integers $K_{1}, K_{2}, \ldots, K_{d}$ such as:

$$
x=1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}
$$

and

$$
\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{\alpha_{i}}}^{\left.\ldots p_{d}^{\alpha_{d}} A K_{i}\right)^{p}=1[n] \quad \forall 1 \leq i \leq d . d .}\right.
$$

If we set $x_{i}=1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}$, then $x_{i}$ is a $p$-th root of unity modulo $n$ also from the construction of $K_{i}$ in the preceding proof, $K_{i}$ is not divisible by $p_{i}$. Thus $x_{i}$ is an initial $p$-th root associated to $p_{i}$. On the other hand we have

$$
\begin{aligned}
\prod_{i=1}^{d} x_{i} & =\prod_{i=1}^{d}\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right) \\
& =1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}[n]=x
\end{aligned}
$$

Corollary 2.3: Every $p$-th root of unity modulo $n$ is a product of initial $p$-th roots.

## Proof :

Let $x$ be a $p$-th root of unity modulo $n$, if this root is final, then the result is immediate, otherwise there is $x_{1}, x_{2}, \ldots$ and $x_{t}$ such as $x . \prod_{i=1}^{t} x_{i}$ is final $p$-th root of unity modulo $n$ and from the precedent corollary there exists $y_{1}, y_{2}, \ldots$ and $y_{d}$ initial $p$-th roots of unity modulo $n$ associated respectively to $p_{1}, p_{2} \ldots$ and $p_{d}$ such as $x . \prod_{i=1}^{t} x_{i}=\prod_{i=1}^{d} y_{i}$ and thus $x=\prod_{i=1}^{t} x_{i}^{-1} \cdot \prod_{i=1}^{d} y_{i}$ and as the set of initial $p$-th roots of unity modulo $n$ associated to $p_{i}$ form with 1 a group, then $x$ can be written like following $x=\prod_{i=1}^{d} z_{i}$ with $z_{i}$ is either 1 or an initial $p$-th root associated to $p_{i}$

Corollary 2.4: $\mathbf{G}_{p}(n)$ is generated by the initial $p-$ th roots of unity modulo $n$.

## Remark :

As for each $p_{i}$ the set of initial $p$-th roots of unity modulo $n$ associated to $p_{i}$ form with 1 a cyclic group then

$$
\mathbf{G}_{p}(n)=<x_{1}, x_{2}, \ldots, x_{d}>
$$

with $x_{i}$ an initial $p$-th root of unity modulo $n$ associated to $p_{i}$.

Theorem 2.4: The map

$$
\begin{aligned}
\varphi: \mathbf{G}_{p}^{p_{1}}(n) \times \mathbf{G}_{p}^{p_{2}}(n) \ldots \times \mathbf{G}_{p}^{p_{d}}(n) & \longrightarrow \\
\left(x_{1}, x_{2}, \ldots, x_{d}\right) & \longmapsto
\end{aligned} \mathbf{G}_{p}(n) \cdot x_{2}, \ldots x_{d} .
$$

is an isomorphism of groups.

## Proof :

We have shown that $\varphi$ is a surjective morphism of groups, remains to prove that it is injective.
We have $\varphi\left(x_{1}, x_{2}, \ldots, x_{d}\right)=1 \Longleftrightarrow x_{1} \cdot x_{2}, \ldots x_{d}=1$, assume that there exists an integer $i$ such that $x_{i} \neq 1$, then we can easily verify that $x_{1} \cdot x_{2}, \ldots x_{d}-1$ is also not divisible by $p_{i}$ but this is absurd, thus $x_{i}=1$ for all $i$ and hence $\varphi$ is injective

From the previous theorem it is clear that $\operatorname{Card}\left(\mathbf{G}_{p}(n)\right)=p^{d}$, where $d$ is a number of distinct prime factors $q$ of $n$ such that $p$ divides $q-1$, that is to say $d=\alpha_{p}(n)$ and we obtain the following result :

Corollary 2.5:

$$
\operatorname{Card}\left(\mathbf{G}_{p}(n)\right)=p^{\alpha_{p}(n)} .
$$

Remark :
From the previous theorem we have
$\mathbf{G}_{p}(n)=\left\{\prod_{\left(i_{1}, i_{2}, ., i_{d}\right) \in I^{d}} x_{1}^{i_{1}} x_{2}^{i_{2}} \ldots x_{d}^{i_{d}} \quad\right.$, with $\left.I=\{1,2, . ., p\}\right\}$
with $x_{i}$ is a generator of the cyclic group $\mathbf{G}_{p}^{p_{i}}(n)$.
We give now an algorithm written in Maple that allows us from an integer $n$ and an odd prime $p$, as described in this foregoing, to give a generating set of $\mathbf{G}_{p}(n)$.

Gene_p $:=\operatorname{proc}(n, p) \quad$ local LB,LD,, LFact, GEN, P; $L D:=[] ; L B:=[] ; G E N:=[] ;$
LFact $:=$ ifactors $(n)[2]$;
for $i$ from 1 to nops(LFact) do
if $($ LFact $[i][1]-1 \bmod p=0)$ then
$L D:=[o p(L D)$, LFact $[i]] ;$
end :
end :
for $i$ from 1 to nops $(L D)$ do
$P:=\operatorname{convert}($ Berlekamp $(\widehat{x p}-1, x) \bmod L D[i][1]$, list $)$; if $(P[1]-x+1 \bmod L D[i][1]<>0)$ then
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1)^{\wedge} L D[i][2]\right), P[1]-x+\right.$ 1);
$G E N:=\quad[o p(G E N),((L D[i][1] * L B[1]-(P[1]-$
x) $\left.\bmod n)) \&^{\wedge}\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
else
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1]^{\wedge} L D[i][2]\right), P[2]-x+\right.$ 1);
$G E N:=[o p(G E N),(L D[i][1] * L B[1]-(P[2]-x) \bmod n) \& \wedge$ $\left.\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
end :
end :
if $(G E N=[])$ then
$G E N:=[1] ;$
end :
$\operatorname{eval}(G E N)$;
end :
Algorithm 2.2
A sample application :
Let $n=53 * 79 * 131 * 17 * 19$ and $p=13$, to find a generating set of the group formed by the $p$-th roots of unity modulo $n$, it suffices to use the previous algorithm with the command line Gene $\_p(n, 13)$. The displayed result is [50140906, 174921943, 71677254], which represents the list of generators of this group.

## Remark :

In the case when this algorithm return [1], then this means that $G_{p}(n)=\{1\}$.

## Case 2: $\alpha=1$

Let $n$ be an integer whose decomposition into prime factors is $n=p p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $p_{i} \neq p$ for all $i$ and let $x$ be a $p$-th root of unity modulo $n$, the above results show that if $p$ does not divide $p_{i}-1$ then $p_{i}^{\alpha_{i}}$ divides $x-1$, on the other hand we have $x^{p}=1[n]$ implies that $p$ divides $(x-1)(1+$ $x+. .+x^{p-1}$ ) and from the lemma 2.1 we obtain $p$ divides $x-1$ and $1+x+. .+x^{p-1}$.
Also provided $p$ divides $\lambda(n)$ implies that there exists at least one integer $i$ such that $p$ divides $p_{i}-1$. For a fixed permutation we can write $n=p p_{1}^{\alpha_{1}} \ldots p_{d}^{\alpha_{d}} \ldots p_{m}^{\alpha_{m}}$ with $p$ divides $p_{i}-1$ for all $i \in\{1, . ., d\}$ and does not divide $p_{i}-1$ for every $i \in$ $\{d+1, . ., m\}$. Assume for the following $p_{d+1}^{\alpha_{d+1}} \ldots p_{m}^{\alpha_{m}}=A$. We define in the same manner the initial $p$-th roots of unity modulo $n$ by replacing $A$ with $p A$. The initial $p$-th roots of unity modulo $n$ associated to $p_{i}, i \in\{1, . ., d\}$ are the solutions of the system :

$$
\left\{\begin{array}{l}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}}}{ } \ldots p_{d}^{\alpha_{d}} p A K \\
1+x+x^{2}+. .+x^{p-1}=p_{i}^{\alpha_{i}} K^{\prime}
\end{array}\right.
$$

We show in the same manner that this system has exactly $p-1$ roots modulo $n$. Thus for all $i \in\{1, \ldots, d\}$ there are $p-1$ initial $p$-th roots associated to $p_{i}$. We also show that the initial $p$-th roots of unity modulo $n$ associated to $p_{i}$ form with 1 a cyclic subgroup of $\mathbf{G}_{p}(n)$ of cardinality $p$ and it is denoted as $\mathbf{G}_{p}^{p_{i}}(n)$.
We define in the same way a final $p$-th root of unity and its conjugate by replacing $A$ by $p A$ and we obtain the following theorem :

Theorem 2.5: Let $x$ be a final $p$-th root of unity modulo $n$, then there exists integers $K_{1}, K_{2}, \ldots, K_{d}$ such that :

$$
x=1+\sum_{i=1}^{d} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{d}^{\alpha_{d}} p A K_{i}
$$

# International Journal of Engineering, Mathematical and Physical Sciences <br> ISSN: 2517-9934 <br> Vol:4, No:7, 2010 

and

$$
\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} p A K_{i}\right)^{p}=1[n] \quad \forall 1 \leq i \leq d
$$

Indeed to prove this result we can just proceed as above and replacing $A$ by $p A$.
We deduce that any final $p$-th root of unity modulo $n$ is the product of $d$ initial $p$-th roots associated respectively to $p_{1}, p_{2}, \ldots$ and $p_{d}$. Hence every $p$-th root of unity is the product of initial $p$-th roots, and we can show that $\mathbf{G}_{p}(n)$ is generated by the initial $p$-th roots of unity and more precisely if we denote $x_{i}$ an initial $p$-th root of unity associated to $p_{i}$, then

$$
\mathbf{G}_{p}(n)=<x_{1}, x_{2}, \ldots, x_{d}>.
$$

Also we have the following results :
Theorem 2.6: The map

$$
\begin{aligned}
\varphi: \mathbf{G}_{p}^{p_{1}}(n) \times \mathbf{G}_{p}^{p_{2}}(n) \ldots \times \mathbf{G}_{p}^{p_{d}}(n) & \longrightarrow \mathbf{G}_{p}(n) \\
\left(x_{1}, x_{2}, \ldots, x_{d}\right) & \longmapsto x_{1} \cdot x_{2}, \ldots x_{d}
\end{aligned}
$$

is an isomorphism of groups.
Corollary 2.6:

$$
\operatorname{Card}\left(\mathbf{G}_{p}(n)\right)=p^{\alpha_{p}(n)} .
$$

Remark :
From the previous theorem we can easily show that
$\mathbf{G}_{p}(n)=\left\{\prod_{\left(i_{1}, i_{2}, ., i_{d}\right) \in I^{d}} x_{1}^{i_{1}} x_{2}^{i_{2}} \ldots x_{d}^{i_{d}} \quad\right.$, with $\left.I=\{1,2, . ., p\}\right\}$
with $x_{i}$ is a generator of the cyclic group $\mathbf{G}_{p}^{p_{i}}(n)$.
Finally, note that Algorithm 2.2 remains valid in this case.

Case 3: $\alpha \geq 2$
Let $n$ be an integer whose decomposition into prime factors is $n=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $p_{i} \neq p$ for all $i$ and $\alpha \geq 2$. The fact that $\alpha \geq 2$ ensures that $\mathbf{G}_{p}(n)$ is not reduced to $\{1\}$. Suppose that for every $i, p$ does not divide $p_{i}-1$ and let $x$ be a $p$-th root of unity modulo $n$, then $p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ divides $x-1$ and by Proposition 2.2 it follows that $p^{\alpha-1}$ divides $x-1$. So $x$ is a solution of the system

$$
\left\{\begin{array}{l}
x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+. .+x^{p-1}=K^{\prime}
\end{array}\right.
$$

But this system has $p$ solutions modulo $n$ which are $1,1+n / p, 1+2 n / p, .$. and $1+(p-1) n / p$. Then we obtain the following result:

Proposition 2.5: Let $n=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $\alpha \geq 2$ and $p$ does not divide $p_{i}-1$ for all $i$, then

$$
\mathbf{G}_{p}(n)=\{1+k n / p ; \quad 0 \leq k \leq p-1\}
$$

Remark:
It is clear that $\mathbf{G}_{p}(n)$ is a cyclic group of order $p$.

We will now exclude this case from our study, that is, there exists at least $i$ such that $p$ divides $p_{i}-1$. For a fixed permutation we can write $n=p^{\alpha} p_{1}^{\alpha_{1}} \ldots p_{d}^{\alpha_{d}} \ldots p_{m}^{\alpha_{m}}$ with $p$ divides $p_{i}-1$ for all $i \in\{1, . ., d\}$ and does not divide $p_{i}-1$ for all $i \in\{d+1, . ., m\}$ and assume for the rest of this paper $p_{d+1}^{\alpha_{d+1}} \cdots p_{m}^{\alpha_{m}}=A$.

Definition 2.5: Let $x$ be a $p$-th root of unity modulo $n, x$ is said of class zero if $x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K$ with $K$ an integer.

It is clear that there are $p p$-th roots of unity of class zero which are $\{1+k n / p ; \quad 0 \leq k \leq p-1\}$ and one can easily verify that they form a cyclic group of order $p$ denoted $\mathbf{G}_{p}^{0}(n)$.

Definition 2.6: Let $x$ be a $p$-th root of unity modulo $n$, it said initial root if every $p_{i}, i \in\{1, \ldots, d\}$ divides $x-1$ except for only one $p_{i}$. We said that this root is associated to $p_{i}$. And we write :

$$
x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}}}{\ldots p_{d}^{\alpha_{d}} A K . . .}
$$

with $K$ an integer that is not divided by $p_{i}$.
Theorem 2.7: There exists $p^{2}-p$ initial $p$-th roots of unity associated to $p_{i}$ for all $1 \leq i \leq d$.

Proof:
We may assume $i=1$, the initial $p$-th roots associated to $p_{1}$ are the solutions of the system :

$$
\left\{\begin{array}{l}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K \\
1+x+x^{2}+. .+x^{p-1}=p_{1}^{\alpha_{1}} K^{\prime}
\end{array}\right.
$$

and we conclude with the following lemmas.
Lemma 2.5: The following systems have the same number of solutions respectively modulo $n$ and $n / p_{1}^{\alpha_{1}-1}$.

$$
\begin{align*}
& \left\{\begin{array}{l}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1}^{\alpha_{1}} K^{\prime}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1} K^{\prime}
\end{array}\right.
\end{align*}
$$

Proof :
It is clear that any solution of $(\star)$ is a solution of $(* *)$. Reciprocally let $x$ be a solution of ( $(*)$, then $x^{p} \equiv 1\left[p^{\alpha} p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A\right]$ that is to say $x^{p}=1+$ $p^{\alpha} p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{1}$ and therefore

$$
\begin{aligned}
x^{p p_{1}^{\alpha_{1}-1}} & =\left(1+p^{\alpha} p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{1}\right)^{p_{1}^{\alpha_{1}-1}} \\
& =1+\sum_{i=1}^{p_{1}^{\alpha_{1}-1}-1} \mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}\left(p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{1}\right)^{i} \\
& +\left(p^{\alpha} p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{1}\right)^{p_{1}^{\alpha_{1}-1}}
\end{aligned}
$$

It is easily verified that all $\mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}$ are divisible by $p_{1}^{\alpha_{1}-1}$ and $p_{1}^{\alpha_{1}-1} \geq \alpha_{1}$, then $x^{p p_{1}^{\alpha_{1}-1}} \equiv 1[n]$. On the other hand

$$
\begin{aligned}
x^{p_{1}^{\alpha_{1}-1}} & =\left(1+p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K\right)^{p_{1}^{\alpha_{1}-1}} \\
& =1+\sum_{i=1}^{p_{1}^{\alpha_{1}-1}-1} \mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}\left(p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K\right)^{i} \\
& +\left(p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K\right)^{p_{1}^{\alpha_{1}-1}}
\end{aligned}
$$

And as $\mathbf{C}_{p_{1}^{\alpha_{1}-1}}^{i}$ are divisible by $p_{1}$ and $K$ is not divisible by $p_{1}$, then $x^{p_{1}^{\alpha_{1}-1}}-1$ is divisible by all $p_{i}$ except $p_{1}$. Consequently $x^{p_{1}^{\alpha_{1}-1}}$ is a solution of ( $\star$ ).
Let $x$ and $y$ be two solutions of ( $* *$ ) such that $x^{p_{1}^{\alpha_{1}-1}}=y^{p_{1}^{\alpha_{1}-1}}[n]$ thus $x^{p_{1}^{\alpha_{1}-1}}=y^{p_{1}^{\alpha_{1}-1}}\left[p_{1}\right]$. Hence $x \equiv y\left[p_{1}\right]$, on the other hand it is clear that $x \equiv y\left[p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A\right]$ therefore $x \equiv y\left[p_{1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A\right]$. We conclude then that the systems $(\star)$ and ( $* \star$ ) have the same number of solutions respectively modulo $n$ and $n / p_{1}^{\alpha_{1}-1}$.

Lemma 2.6: The following system have $p^{2}-p$ solutions modulo $n / p_{1}^{\alpha_{1}-1}$.

$$
\left\{\begin{array}{l}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K \\
1+x+x^{2}+\ldots+x^{p-1}=p_{1} K^{\prime}
\end{array}\right.
$$

Proof:
We know that

$$
X^{p}-1=\prod_{i=1}^{p}\left(X-\gamma_{i}\right)
$$

and as 1 is a root of $X^{p}-1$ then we take $\gamma_{1}=1$. Finally, we obtain

$$
1+X+X^{2}+\ldots X^{p-1}=\prod_{i=2}^{p}\left(X-\gamma_{i}\right)
$$

and consequently $(\star \star)$ is equivalent to the following systems :

$$
\begin{aligned}
& \left\{\begin{array}{c}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{2} \\
x-\gamma_{2}=p_{1} K_{2}^{\prime} \\
\vdots
\end{array}\right. \\
& \left\{\begin{array}{c}
x-1=p^{\alpha-1} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K_{p} \\
x-\gamma_{p}=p_{1} K_{p}^{\prime}
\end{array}\right.
\end{aligned}
$$

It is clear that for each one of these systems have $p$ solutions modulo $n / p_{1}^{\alpha_{1}-1}$. Since, the solutions of these systems are distinct, we conclude that $(\star \star)$ have $p(p-1)$ solutions modulo $n / p_{1}^{\alpha_{1}-1}$.

Proposition 2.6: The set formed by the initial $p$-th roots of unity modulo $n$ associated to $p_{i}$ and by the elements of $\mathbf{G}_{p}^{0}(n)$ is a subgroup of $\mathbf{G}_{p}(n)$ denoted $\mathbf{G}_{p}^{p_{i}}(n)$ and we have $\operatorname{Card}\left(\mathbf{G}_{p}^{p_{i}}(n)\right)=p^{2}$.

Proof :
Let $x$ and $y$ be two elements of $\mathbf{G}_{p}^{p_{i}}(n)$, there are three cases
to distinguish :

- If $x$ and $y$ are in $\mathbf{G}_{p}^{0}(n)$, then in this case $x y$ belongs $\mathbf{G}_{p}^{0}(n)$ since the latter is a group and hence $x y$ is in $\mathbf{G}_{p}^{p_{i}}(n)$.
- If $x$ and $y$ are respectively in $\mathbf{G}_{p}^{p_{i}}(n) \backslash \mathbf{G}_{p}^{0}(n)$ and $\mathbf{G}_{p}^{0}(n)$, then we have $x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K$ and $y-$ $1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}$ with $K$ an integer not divisible by $p_{i}$ thus

$$
x y=1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}}}{\ldots p_{d}^{\alpha_{d}} A\left(K+p_{i}^{\alpha_{i}} K^{\prime}\right) ~}
$$

The term $K+p_{i}^{\alpha_{i}} K^{\prime}$ is not divided by $p_{i}$ and therefore $x y$ is a $p$-th root of unity associated to $p_{i}$. Hence $x y$ is in $\mathbf{G}_{p}^{p_{i}}(n)$. - If $x$ and $y$ are in $\mathbf{G}_{p}^{p_{i}}(n) \backslash \underset{V_{p}}{\mathbf{G}}(n)$, then :
$x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K$ and $y-1=$ $p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}$ with $K$ and $K^{\prime}$ are two integers not divided by $p_{i}$ therefore

$$
\begin{aligned}
x y & =1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee} \ldots p_{d}^{\alpha_{i}} A\left(K+K^{\prime}\right. \\
& \left.+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K K^{\prime}\right)
\end{aligned}
$$

If the term $K+K^{\prime}+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K K^{\prime}$ is divided by $p_{i}$ then $x y$ belongs to $\mathbf{G}_{p}^{0}(n) \subset \mathbf{G}_{p}^{p_{i}}(n)$, otherwise $x y$ is a $p$-th root associated to $p_{i}$ and consequently $x y$ is in $\mathbf{G}_{p}^{p_{i}}(n)$.
Thus $\mathbf{G}_{p}^{p_{i}}(n)$ is stable for the product and as the inverse of the element $x$ is $x^{p-1}$, then $\mathbf{G}_{p}^{p_{i}}(n)$ is stable by the inverse operation which proves that $\mathbf{G}_{p}^{p_{i}}(n)$ is a subgroup of $\mathbf{G}_{p}(n)$. Finally, we can see that $\mathbf{G}_{p}^{0}(n)$ does not contain an initial $p$-th root associated to $p_{i}$ which allows us to conclude that $\operatorname{Card}\left(\mathbf{G}_{p}^{p_{i}}(n)\right)=\left(p^{2}-p\right)+p=p^{2}$.

Definition 2.7: Let $x$ be a $p$-th root, we said that $x$ is of the first class if $p^{\alpha}$ divides $x-1$, otherwise it said to be of the second class.

Proposition 2.7: There are $p-1$ initial $p$-th roots of unity associated to $p_{i}$ which are of the first class.

## Proof :

The initial $p$-th roots associated to $p_{i}$ which are of first class are solutions of the system :

$$
\left\{\begin{array}{l}
x-1=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K \\
x+1=p_{i}^{\alpha_{i}} K^{\prime}
\end{array}\right.
$$

And from the previous we know that this system has $p-1$ solutions modulo $n$.
Let denote by $\mathbf{G}_{p}^{+}{ }^{p_{i}}(n)$ the set formed by 1 and the initial $p$-th roots of unity associated to $p_{i}$ that are of the first class and we can easily verify that $\mathbf{G}_{p}^{+}{ }_{p}^{p_{i}}(n)$ is a cyclic subgroup of $\mathbf{G}_{p}(n)$ of cardinality $p$ and we have the following result :

Proposition 2.8: The map

$$
\begin{aligned}
\varphi: \mathbf{G}_{p}^{p_{i}}(n) \times \mathbf{G}_{p}^{0}(n) & \longrightarrow \mathbf{G}_{p}^{p_{i}}(n) \\
(x, y) & \longmapsto x . y
\end{aligned}
$$

# International Journal of Engineering, Mathematical and Physical Sciences 

ISSN: 2517-9934
Vol:4, No:7, 2010
is an isomorphism of groups.

Proof:
It is clear that $\varphi$ is surjective morphism of groups. For the injectivity, let us consider two elements $x$ and $y$ of $\mathbf{G}_{p}^{+}(n)$ and $\mathbf{G}_{p}^{0}(n)$ respectively such that $x . y=1$, we have :
$x-1=p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{\vee} p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K$ and $y-1=$ $p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}$, therefore

$$
x y=1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee \alpha_{i}} \ldots p_{d}^{\alpha_{d}} A\left(K+p_{i}^{\alpha_{i}} K^{\prime}\right)
$$

As $x . y=1$, then the term $K+p_{i}^{\alpha_{i}} K^{\prime}$ is divided by $p_{i}^{\alpha_{i}}$ therefore $p_{i}^{\alpha_{i}}$ divides $K$, hence $x=y=1$

Definition 2.8: Let $x$ be a $p$-th root of unity modulo $n$, we said $x$ is final if all the $p_{i}, i \in\{1, \ldots, d\}$ does not divide $x-1$, which means $x-1=p^{\alpha-1} A K$, with $K$ an integer not divisible by $p_{i}, i \in\{1, . ., d\}$.

Proposition 2.9: Any final $p$-th root of unity modulo $n$ can be written in a single manner as product of a final $p$-th root of the first class by a class zero's $p$-th root.

## Proof:

Let $x$ be a final $p$-th root of unity modulo $n$ and let's consider an integer $y$ of the form $y=1+p^{\alpha} A K$ and $z$ a class zero's $p$-th root. We have :

$$
\begin{aligned}
x=y z & \Longleftrightarrow x=\left(1+p^{\alpha} A K\right)\left(1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}\right) \\
& \Longleftrightarrow x-1=p^{\alpha} A K+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime} \\
& \Longleftrightarrow \frac{x-1}{p^{\alpha-1} A}=p K+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} K^{\prime}
\end{aligned}
$$

This equation has solutions $K$ and $K^{\prime}$, also $\left(1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}\right)^{p}=1, \quad$ therefore $\left(1+p^{\alpha} A K\right)^{p}=1$ and as $x-1$ is divisible by none of the $p_{i}$ which implies that $K$ is divisible by none of the $p_{i}$, this proves that $\left(1+p^{\alpha} A K\right)$ is a final $p$-th root of the first class. Also it is clear that if we take $K$ and $K^{\prime}$ as other solutions, then $1+p^{\alpha} A K$ and $1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{d}^{\alpha_{d}} A K^{\prime}$ are the same modulo $n$.

## Remark :

If for all $i \in\{1, . ., d\}$ we take $x_{i}$ an initial $p$-th root of the first class associated to $p_{i}$, then $\prod_{i=1}^{d} x_{i}$ is a final root of the first class. The following theorem shows that any final root of the first class is a product of this form.

Theorem 2.8: Any final $p$-th root of the first class is product of $d$ initial $p$-th roots of the first class associated respectively to $p_{1}, p_{2}, .$. and $p_{d}$.

Proof:
Let $x$ be a final $p$-th root of the first class, we know that there
exist $K_{1}, K_{2}, .$. and $K_{d}$ such that

$$
x=1+\sum_{i=1}^{d} p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee} \ldots p_{d}^{\alpha_{d}} A K_{i}
$$

and

$$
\left(1+p^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\left.\vee p_{i}^{\alpha_{i}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right)^{p}=1[n] \quad \forall 1 \leq i \leq d . . . ~}{\text {. }}\right.
$$

 an initial $p$-th root of the first class associated to $p_{i}$ and we can easily verify that $x=\prod_{i=1}^{d} x_{i}$.

Definition 2.9: Let $x$ and $y$ be two $p$-th roots of unity modulo $n$, we say $y$ is a final conjugate root of $x$ if $x . y-1$ is divisible by none of the $p_{i}, i \in\{1, \ldots, d\}$, that means $x . y$ is a final $p$-th root modulo $n$.

Proposition 2.10: Any $p$-th root of unity modulo $n$ have a final conjugate.

## Proof :

Let $x$ be a $p$-th root of unity modulo $n$, if $x \in \mathbf{G}_{p}^{0}(n)$ or $x$ is a final $p$-th root then we have the expected result. When $d=1$, a final $p$-th root is an initial $p$-th root associated to $p_{1}$ and therefore any root that not belongs to $\mathbf{G}_{p}^{0}(n)$ are finals. Assume that $d \geq 2$ and $x-1$ is divisible by a nonempty subfamily of $p_{i}$ of cardinality $t<d$ and for a permutation, we can assume them $p_{1}, p_{2}, \ldots$ and $p_{t}$. Thus

$$
x-1=p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{t}^{\alpha_{t}} A K
$$

with $K$ an integer not divisible by $p_{i}, i \in\{t+1, . ., d\}$. For all $i \in\{1, . ., t\}$, let $x_{i}$ be an initial $p$-th associated to $p_{i}$ therefore
with $K_{i}$ not divided by $p_{i}$, whereof
$\prod_{i=1}^{t} x_{i}=\prod_{i=1}^{t}\left(1+p^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee p_{i}} \ldots p_{t}^{\alpha_{t}} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A K_{i}\right)$
$=1+p^{\alpha-1} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A \sum_{i=1}^{t} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{v}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{t}^{\alpha_{t}} K_{i}+K^{\prime} n$

$i \in\{1, \ldots, t\}$. Consequently $y=\prod_{i=1}^{t} x_{i}$ is a root which verify $y=1+p^{\alpha-1} p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M$ with $M$ an integer that not divided by $p_{i}, i \in\{1, . ., t\}$. Thereby

$$
x . y=1+p^{\alpha-1} A\left(p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M+p_{1}^{\alpha_{1}} \ldots p_{t}^{\alpha_{t}} A K\right)
$$

It is clear that $\left(p_{t+1}^{\alpha_{t+1}} \ldots p_{d}^{\alpha_{d}} A M+p_{1}^{\alpha_{1}} \ldots p_{t}^{\alpha_{t}} A K\right)$ is divisible by none of the $p_{i}, i \in\{1, . ., d\}$, hence the result.

Corollary 2.7: Every $p$-th root of unity is a product of a first class initial $p$-th roots by a class zero's $p$-th root.

## Proof:

Let $x$ be a $p$-th root modulo $n$, if $x$ is final then we can write it as a product of a final $p$-th root of unity of the first class by a class zero's $p$-th root and from the previous results this final $p$-th root of the first class is product of $d$ initial $p$-th roots of the first class associated respectively to $p_{1}, p_{2}, .$. and $p_{d}$, hence the result. Now let us assume that $x$ is not a final $p$-th root so there exists $x_{1}, x_{2}, .$. and $x_{t}$ initial $p$-th roots such that $x_{1} x_{2} \ldots x_{t}$ is a final conjugate of $x$, then $x x_{1} x_{2} \ldots x_{t}$ is a final $p$-th root, and we have :

$$
x x_{1} x_{2} . . x_{t}=y_{1} y_{2} . . y_{d} y_{0}
$$

with $y_{i}$ is an initial $p$-th root of the first class associated to $p_{i}$ and $y_{0}$ is a class zero's $p$-th root.
From Proposition 2.8 any initial $p$-th root associated to $p_{i}$ can be written uniquely as a product of an initial first class $p$-th root associated to $p_{i}$ by class zero's $p$-th root. Thereby $x_{i}=\stackrel{+}{x_{i}} z_{i}$, with $\stackrel{+}{x_{i} \in \mathbf{G}_{p}^{p_{1}}}(n)$ and $z_{i} \in \mathbf{G}_{p}^{0}(n)$. So

$$
x=y_{1} y_{2} . . y_{d}\left(\dot{x}_{1} \dot{x}_{2}^{+} \ldots \stackrel{+}{x_{t}}\right)^{-1}\left(z_{1} z_{2} \ldots z_{t}\right)^{-1} y_{0}
$$

and as $\stackrel{+}{\mathbf{G}_{p}^{p_{1}}}(n)$ and $\mathbf{G}_{p}^{0}(n)$ are groups, then we obtain the result.

## Remark:

The previous result shows that $\mathbf{G}_{p}(n)$ is generated by the initial $p$-th roots of the first class and the class zero's $p$-th roots and as $\mathbf{G}_{p}^{0}(n)$ and $\mathbf{G}_{p}^{+}(n)$ are cyclic groups, then

$$
\mathbf{G}_{p}(n)=<x_{1}, x_{2}, \ldots, x_{d}, x_{0}>
$$

with $x_{i}$ is an initial $p$-th root of the first class associated to $p_{i}$ and $x_{0}$ is a $p$-th root of the class zero distinct from 1. More generally, we have the following result :

We now give an algorithm in MAPLE that allows us to find a generating set of $\mathbf{G}_{p}(n)$. For the computing of $x_{0}$ it suffices to take $x_{0}=1+n / p$ and for the others $x_{i}$, we proceed as above.

Gene_p:=proc $(n, p)$ local LB,LD, $i$, LFact, GEN, P; $L D:=[] ; L B:=[] ; G E N:=[] ;$
$G E N:=[o p(G E N), 1+n / p] ;$
LFact $:=$ ifactors( $n$ )[2];
for $i$ from 1 to nops(LFact) do
if $($ LFact $[i][1]-1 \bmod p=0)$ then
$L D:=[o p(L D), L F a c t[i]] ;$
end:
end:
for $i$ from 1 to nops $(L D)$ do
$P:=\operatorname{convert}(\operatorname{Berlekamp}(\widehat{x p}-1, x) \bmod L D[i][1]$, list); if $(P[1]-x+1$ mod $L D[i][1]<>0)$ then
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1]^{\wedge} L D[i][2]\right), P[1]-x+\right.$ 1);
$G E N:=\quad[o p(G E N),((L D[i][1] * L B[1]-(P[1]-$ x) $\left.\bmod n)) \&^{\wedge}(L D[i][1] \wedge(L D[i][2]-1)) \bmod n\right]$; else
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1]^{\wedge} L D[i][2]\right), P[2]-x+\right.$ 1);
$G E N \quad:=[o p(G E N),(L D[i][1] * L B[1]-(P[2]-$ x) $\left.\bmod n) \mathcal{\&}^{\wedge}\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
end :
end:
if $(G E N=[])$ then
GEN := [1];
end;
eval(GEN);
end :
Algorithm 2.3

## III. Conclusion

For the cardinality of $\mathbf{G}_{p}(n)$, we can summarize it in the following theorem :

Theorem 3.1: Let $n \geq 3$ be an integer and $p$ be a prime odd number which does not divide $n$, then :

- $\operatorname{Card}\left(\mathbf{G}_{p}(n)\right)=p^{\alpha_{p}(n)}$
- $\operatorname{Card}\left(\mathbf{G}_{p}(p n)\right)=p^{\alpha_{p}(n)}$
- $\operatorname{Card}\left(\mathbf{G}_{p}\left(p^{\alpha} n\right)\right)=p^{\alpha_{p}(n)+1}$ with $\alpha \geq 2$

We will now give an algorithm which help us to find, from a fixed integer $n$, a generating set of $\mathbf{G}_{p}(n)$.

Gene_p $:=\operatorname{proc}(n, p) \quad$ local LB, LD $, i, L F a c t, G E N, P ;$
$L D:=[] ; L B:=[] ; G E N:=[] ;$
if $\left(n \bmod p^{\wedge} 2=0\right)$ then
$G E N:=[o p(G E N), 1+n / p] ;$
LFact :=ifactors(n)[2];
for $i$ from 1 to nops(LFact) do
if $($ LFact $[i][1]-1 \bmod p=0)$ then

# International Journal of Engineering, Mathematical and Physical Sciences 

ISSN: 2517-9934
Vol:4, No:7, 2010
$L D:=[o p(L D), L F a c t[i]] ;$
end :
end :
for $i$ from 1 to nops $(L D)$ do
$P:=\operatorname{convert}($ Berlekamp $(\widehat{x} p-1, x) \bmod L D[i][1]$, list $)$;
if $(P[1]-x+1 \bmod L D[i][1]<>0)$ then
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1)^{\wedge} L D[i][2]\right), P[1]-x+\right.$ 1);
$G E N:=\quad[o p(G E N),((L D[i][1] * L B[1]-(P[1]-$ x) $\left.\bmod n)) \&^{\wedge}(L D[i][1] \wedge(L D[i][2]-1)) \bmod n\right]$;
else
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1]^{\wedge} L D[i][2]\right), P[2]-x+\right.$ 1);
$G E N:=[o p(G E N),(L D[i][1] * L B[1]-(P[2]-$ x) $\left.\bmod n) \not \& \wedge\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
end:
end:
else
LFact $:=$ ifactors( $n$ )[2];
for i from 1 to nops(LFact) do
if $($ LFact $[i][1]-1 \bmod p=0)$ then
$L D:=[o p(L D), L F a c t[i]] ;$
end :
end:
for $i$ from 1 to nops $(L D)$ do
$P:=\operatorname{convert}($ Berlekamp $(\widehat{x p}-1, x) \bmod L D[i][1]$, list); if $(P[1]-x+1$ mod $L D[i][1]<>0)$ then
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1)^{\wedge} L D[i][2]\right), P[1]-x+\right.$ 1);
$G E N:=\quad[o p(G E N),((L D[i][1] * L B[1]-(P[1]-$ x) $\left.\bmod n)) \&^{\wedge}\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
else
$L B:=\operatorname{Bezout}\left(L D[i][1], n /\left(L D[i][1]^{\wedge} L D[i][2]\right), P[2]-x+\right.$ 1);
$G E N \quad:=[o p(G E N),(L D[i][1] * L B[1]-(P[2]-$ x) $\left.\bmod n) \&^{\wedge}\left(L D[i][1]^{\wedge}(L D[i][2]-1)\right) \bmod n\right]$;
end:
end:
end:
if $(G E N=[])$ then
GEN := [1];
end;
eval(GEN);
end :

[^0] -
[6] V. Shoup, A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005.
[7] David M. Bressoud, Factorization and Primality Testing. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1989.
[8] Elwyn R. Berlekamp. Factoring Polynomials Over Finite Fields. Bell Systems Technical Journal, 46:1853-1859, 1967.
[9] David G. Cantor and Hans Zassenhaus. A New Algorithm for Factoring Polynomials Over Finite Fields. Mathematics of Computation, 36:587592, 1981.
[10] Frank Garvan. The Maple Book. Chapman and Hall/CRC, Boca Raton, FL 2002


[^0]:    Algorithm 2.4

    ## References

    [1] R. Omami, M. Omami and R. Ouni, Group of Square Roots of Unity Modulo n. International Journal of Computational and Mathematical Sciences, 2009
    [2] J-P. Serre, A Course in Arithmetic. Graduate Texts in Mathematics, Springer, 1996
    [3] S. Lang, Undergraduate Algebra, 2nd ed. UTM. Springer Verlag, 1990
    [4] Hardy, G. H, Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work, 3rd ed. New York: Chelsea, 1999. G. H.
    [5] H. Cohen, A course in computational algebraic number theory. Springer-Verlag, 1993.

