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 \( G_p(n) \) the subgroup of \( (\mathbb{Z}/n\mathbb{Z})^* \) defined by:

\[
G_p(n) = \{ x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x^p = 1 \}.
\]

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 \( G_p(n) \) the part of \((\mathbb{Z}/n\mathbb{Z})^*\) formed by the elements \( x \) that verify \( x^p = 1 \). We can easily prove that \( G_p(n) \) 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 \( G_p(n) \) is not reduced to \( \{1\} \) if and only if \( p \) divides \( \lambda(n) \).

The elements of \( G_p(n) \) other than 1 have the order \( p \) and so the order of \( G_p(n) \) 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 :

\[
\text{Card}(G_p(n)) = p^t
\]

with \( t = 0 \) if and only if \( p \) does not divide \( \lambda(n) \).

II. P-TH ROOTS OF UNITY MODULO N

Let us consider an integer \( n \geq 3 \) and \( p \) a prime odd number, let \( n = p^m_1 p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m} \) 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 :
• \( \alpha_p(n) \) 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:

\[
\alpha_p(m.n) = \alpha_p(m) + \alpha_p(n) - \alpha_p(GCD(m,n)).
\]

In the following, we consider an integer \( n \geq 3 \) whose the factorization is \( n = p^m_1 p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m} \), 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 \( x^p \equiv 1[n] \Longrightarrow x^p \equiv 1[p_i] \) and thus the order of \( x \) in \((\mathbb{Z}/p_i\mathbb{Z})^*\) is 1 or \( p \), but the order of \( x \) in \((\mathbb{Z}/p_i\mathbb{Z})^*\) divides \( p_i - 1 \) and thus it cannot be \( p \). Therefore \( x \equiv 1[p_i] \) and then we obtain the result.

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

Lemma 2.1:

\[
GCD(x - 1, 1 + x + x^2 + \ldots + x^{p-1}) \in \{1, p\}
\]

Proof :
One can easily verify that we have:

\[
(x - 1)(x^{p-2} + 2x^{p-3} + 3x^{p-4} + \ldots + (p - 2)x + (p - 1)) - (1 + x + x^2 + \ldots + x^{p-1}) = p.
\]
Corollary 2.1: Let \( x \) be a \( p \)-th root of unity modulo \( n \). If \( p \) does not divide \( p_1 - 1 \) and \( p \neq p_1 \), then \( p_1^{n_1} \) divides \( x - 1 \).

**Proof:** We have \( x^p \equiv 1 \mod{n} \) \( \Rightarrow \) \( x^p \equiv 1 \mod{\varphi(n)} \) then \( p_1^\alpha \) divides \( x^p - 1 = (x - 1)(1 + x + x^2 + \ldots + x^{p-1}) \), or \( p \) does not divide \( p_1 - 1 \) and thus \( p_1 \) divides \( x - 1 \). Also we know that the \( \text{PGCD}(x - 1, 1 + x + x^2 + \ldots + x^{p-1}) \in \{1, p\} \) and \( p \neq p_1 \), then \( p_1^{n_1} \) 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 \( x^p - 1 = (x - 1)(1 + x + x^2 + \ldots + x^{p-1}) \) 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 \( \text{PGCD}(x - 1, 1 + x + x^2 + \ldots + x^{p-1}) = p \).

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:

\[
x^p \equiv 1 \mod{p^3} \Rightarrow x \equiv 1 \mod{p^2}
\]

**Proof:** It is clear that \( x^p \equiv 1 \mod{p^3} \Rightarrow x \equiv 1 \mod{p} \), so \( x = 1 + kp \) \((k \in \mathbb{N})\) and consequently \( x^p \equiv 1 \mod{p^3} \). (This writing is possible because \( p \geq 3 \)) moreover \( p^2 \) divides \( p^k \), then \( p \) divides \( k \) and finally we obtain: \( x \equiv 1 \mod{p^3} \).

**Remark:** Notice that the precedent lemma is not true for \( p = 2 \), for instance \( 3^2 \equiv 1 \mod{8} \) and \( 3 \equiv 1 \mod{4} \).

**Proof of Proposition 2.2:**

We have \( x^p \equiv 1 \mod{p^\alpha} \) \((\alpha \geq 3)\) and so in particular \( x^p \equiv 1 \mod{p^3} \), from the precedent lemma we conclude that \( x \equiv 1 \mod{p^3} \).

We have \( p^\alpha \) divides \( x^p - 1 = (x - 1)(1 + x + x^2 + \ldots + x^{p-1}) \) and as \( \text{PGCD}(x - 1, 1 + x + x^2 + \ldots + x^{p-1}) = p \) 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:

- \( n = 7^3 \times 29 = 9947 \), we have \( 344^7 \equiv 1 \mod{n} \) and \( 344 \equiv 1 \mod{7^3} \). \( 2402^7 \equiv 1 \mod{n} \) and \( 2402 \equiv 1 \mod{7^4} \).

- \( n = 7^2 \times 29 \times 43 \times 71 = 4338313 \), we have \( 350547^7 \equiv 1 \mod{n} \) and \( 350547 \equiv 1 \mod{7^4} \).

Let us return to our principal aim, which is the study of the group \( G_p(n) \), 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 \( p_1 \neq p \) 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 \( p_1 - 1 \), then \( p_1^{n_1} \) 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 \( \{1, 2, \ldots, m\} \) such that \( n = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(d+1)}^{\alpha_{\sigma(d+1)}} p_{\sigma(d+2)}^{\alpha_{\sigma(d+2)}} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} \) and \( p \) divides only \( p_{\sigma(d+1)}^{\alpha_{\sigma(d+1)}} p_{\sigma(d+2)}^{\alpha_{\sigma(d+2)}} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} \) divides \( x - 1 \).

We start our study by the following theorem:

**Theorem 2.1:** Let \( n \) be an integer whose decomposition into prime factors is \( n = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_m^{\alpha_m} \) with \( p_1 \neq p \) for all \( i \) and \( p \) divides only \( p_1 - 1 \), then \( G_p(n) \) 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:

- \( x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} K \)
- \( 1 + x + x^2 + \ldots + x^{p-1} = p_1^{\alpha_1} K' \)
- \( x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} K \)
- \( 1 + x + x^2 + \ldots + x^{p-1} = K' \)

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

- \( x - 1 = p_2^{\alpha_2} \ldots p_m^{\alpha_m} K \)
- \( 1 + x + x^2 + \ldots + x^{p-1} = p_1^{\alpha_1} K' \)
- \( x - 1 = p_2^{\alpha_2} \ldots p_m^{\alpha_m} K \)
- \( 1 + x + x^2 + \ldots + x^{p-1} = p_1^{\alpha_1} K' \)

have the same number of solutions respectively modulo \( n \) and \( n/p_1^{\alpha_1} \).

**Proof:** It is clear that any solution of \( (\ast) \) is a solution of \( (\ast\ast) \). Reciprocally let \( x \) be a solution of \( (\ast\ast) \), then \( x^p \equiv 1 \mod{p_1 p_2^{\alpha_2} \ldots p_m^{\alpha_m}} \).
that is to say $x^p = 1 + p_1p_2^2 \ldots p_m^{\alpha_m}K_1$ and therefore

$$x^{p_1-1} = (1 + p_1p_2^2 \ldots p_m^{\alpha_m}K_1)^{p_1-1}$$

$$= 1 + \sum_{i=0}^{p_1-1} C_{p_1-1}^i (p_1p_2^2 \ldots p_m^{\alpha_m}K_1)^i + (p_1p_2^2 \ldots p_m^{\alpha_m}K_1)^{p_1-1}$$

It is easily verified that all $C_{p_1-1}^i$ are divisible by $p_1$ and $p_1-1 \geq \alpha_1$, thus $x^{p_1-1} = \equiv 1 \mod n$. From the other hand

$$x^{p_1-1} = (1 + p_2^2 \ldots p_m^{\alpha_m}K)^{p_1-1}$$

$$= 1 + \sum_{i=0}^{p_1-1} C_{p_1-1}^i (p_2^2 \ldots p_m^{\alpha_m}K)^i + (p_2^2 \ldots p_m^{\alpha_m}K)^{p_1-1}$$

and as the $C_{p_1-1}^i$ are divisible by $p_1$ and $K$ is not divisible by $p_1$, then $x^{p_1-1}$ is divisible by all $p_1$ except $p_1$ and consequently $x^{p_1-1}$ is a solution of $(\ast)$. Let $x$ and $y$ be two solutions of $(\ast \ast)$ such as $x^{p_1-1} = y^{p_1-1} \mod n$ and thus $x^{p_1-1} = y^{p_1-1} \mod [p_1]$, hence $x \equiv y \mod [p_1]$, on the other hand it is clear that $x \equiv y [p_2^2 \ldots p_m^{\alpha_m}]$ and consequently $x \equiv y [p_2^2 \ldots p_m^{\alpha_m}] \mod n[p_1]$. We therefore conclude that the number of solutions of $(\ast)$ is greater than or equal to that of $(\ast \ast)$. Thus the systems $(\ast)$ and $(\ast \ast)$ have the same number of solutions modulo $n$ and $n/p_1^{\alpha_1-1}$ respectively.

**Lemma 2.4:** The following system

$$\begin{cases}
x - 1 = p_2^2 \ldots p_m^{\alpha_m}K \\
1 + x + x^2 + \ldots + x^{p-1} = p_1K
\end{cases}$$

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, to that is to say

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

and as 1 is a root of $X^p - 1$ then we take $\gamma_1 = 1$ and finally we obtain

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

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

$$\begin{cases}
x - 1 = p_2^2 \ldots p_m^{\alpha_m}K_2 \\
x - \gamma_2 = p_1K_2' \\
x - \gamma_3 = p_1K_3' \\
\vdots \\
x - \gamma_p = p_1K_p'
\end{cases}$$

It is clear that each of these systems has only one solution modulo $p_1p_2^2 \ldots p_m^{\alpha_m}$. Also the solutions of these systems are 2 by 2 distinct. Indeed if we denote $x_i$ the solution of the following system

$$\begin{cases}
x - 1 = p_2^2 \ldots p_m^{\alpha_m}K_i \\
x - \gamma_i = p_1K_i'
\end{cases}$$

then $x_i \equiv \gamma_i \mod [p_1]$. Since the $\gamma_i$ are distinct modulo $p_1$, then the $x_i$ are also distinct. We conclude that $(\ast \ast)$ has $p - 1$ solutions modulo $n/p_1^{\alpha_1-1}$.

**Remark:**

The proof of the previous theorem gives an algorithm for calculating the solutions of $(\ast)$, and this is done in two steps:

**Step 1**

We resolve $(\ast \ast)$, the most difficult point in this step is to determine the $\gamma_i$. We must give the factorization of the polynomial $1 + X + X^2 + \ldots + X^{p-1}$ in the field $\mathbb{Z}/p_1\mathbb{Z}$ and for this we can use Berlekamp’s algorithm [8] or Cantor-Zassenhaus algorithm [9]. Then we decompose $(\ast \ast)$ in small systems that are resolved easily with Euclidean’s algorithm.

**Step 2**

To find the solutions of $(\ast)$, it is sufficient to see that they are also solutions of $(\ast \ast)$ set to the power $p_1^{\alpha_1-1}$ modulo $n$.

Note also that the set of solutions of $(\ast)$ forms with 1 a cyclic group of order $p_1$ then any solution of $(\ast)$ generates this group. Thus in practice it is sufficient to determine a solution of $(\ast)$ to find the others.

**A sample calculation:**

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

$$1 + X + X^2 + \ldots + X^{29} = (X + 4)(X + 5)(X + 6)(X + 9)(X + 13)(X + 22).$$

Let’s consider the following system

$$\begin{cases}
x - 1 = 15K \\
x + 4 = 29K'
\end{cases}$$

which gives $29K' - 15K = 5$, and by the euclidian algorithm we obtain $K' = -5$ and $K = -10$. 

---

*International Scholarly and Scientific Research & Innovation 4(7) 2010* 981

ISNI:0000000091950263
Therefore $x = -149 = 286$ modulo $435 = 29 \times 5 \times 3$. Thereby $286^{286} \mod n = 1006441$ is an element of order $7$ modulo $n$ and consequently the elements of $G_7(n)$ are

$$G_7(n) = \{1006441, 1006441^2, \ldots, 1006441^7\}$$

that is to say

$$G_7(n) = \{1006441, 10684356, 6860611, 4797001, 5450251, 9979951, 1\}$$

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 $G_p(n)$.

**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 $n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ and $p$ a prime odd number such that $p_i \neq p$ for all $i$. For a fixed permutation we can write $n = p_1^{d_1} p_2^{d_2} \cdots p_d^{d_d} p_{d+1} \cdots p_m^{d_m}$ with $p$ divides $p_i - 1$ for all $i \in \{1, \ldots, d\}$. We have seen that if $x$ is a $p$-th root of unity modulo $n$, then $p^{d_1+1} \cdots p^{d_m}$ divides $x - 1$. Thus $p^{d_1+1} \cdots p^{d_m}$ don’t have a significant role in our study, for the rest we write $p^{d_1+1} \cdots p^{d_m} = A$.

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

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} A K$$

with $K$ is an integer not divisible par $p_i$.

We denote by $G^0_p(n)$ 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**:

$G^0_p(n)$ is a cyclic subgroup of $G_p(n)$ with cardinality $p$.

**Proof (**)**: The initial $p$-th roots of unity associated to $p_i$ are the solutions of the system:

$$\begin{align*}
  x - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} A K \\
  1 + x + x^2 + \ldots + x^{p-1} &= p_i^{\alpha_i} K'
\end{align*}$$

We saw in the foregoing that this system have $p - 1$ solutions modulo $n$ and then $\text{Card}(G^0_p(n)) = p$. Let’s prove now that $G^0_p(n)$ is a subgroup. Let $x$ and $y$ be two solutions of (**), we have

$$\begin{align*}
  x - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} A K \\
  y - 1 &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_i^{\beta_i} \cdots p_d^{\beta_d} A' K'
\end{align*}$$

and therefore

$$\begin{align*}
  x.y &= 1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} A(K + K') + p_i^{\alpha_i} K K' \\
  x.y &= 1 + p_1^{\alpha_1} p_2^{\beta_2} \cdots p_i^{\beta_i} \cdots p_d^{\beta_d} A(K + K')
\end{align*}$$

Note that $x.y$ is $p$-th root of unity and therefore at this stage we have two cases. If $p$ divides $(K + K' + p_1^{\alpha_1} p_2^{\beta_2} \cdots p_i^{\beta_i} \cdots p_d^{\beta_d} A K')$, then $p_i$ divides $x.y - 1$ and we obtain $x.y = 1$. If $p$ does not divide $(K + K' + p_1^{\alpha_1} p_2^{\beta_2} \cdots p_i^{\beta_i} \cdots p_d^{\beta_d} A K')$, 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 $G^0_p(n)$. Whereof $G^0_p(n)$ is a cyclic subgroup of $G_p(n)$ because its cardinality is a prime number $p$. ■
and as \( p_i \) does not divide \( K_1 \) also \( p_i \) does not divide \( K_2 \), then \( (p_1^{\alpha_1} K_1 + p_2^{\alpha_2} K_2) \) 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 \( p_i, i \in \{1, \ldots, d\} \) does not divide \( x - 1 \), that is to say \( x - 1 = AK \), with \( K \) an integer not divisible by any \( p_i, i \in \{1, \ldots, d\} \).

**Remark :**
The existence of final \( p \)-th roots of unity modulo \( n \) is ensured by the preceding proposition, in fact if for all \( i \in \{1, \ldots, d\} \) we take \( x_i \) an initial \( p \)-th root of unity associated to \( p_i \), then
\[
\prod_{i=1}^{d} x_i \text{ is a final } p \text{-th root of unity modulo } n.
\]

**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 \( x \cdot y - 1 \) is not divisible by any of the \( p_i \), \( i \in \{1, \ldots, d\} \), 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, 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, \( p_i \) is \( p_1, p_2, \ldots, p_t \) and thus
\[
x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} AK
\]
with \( K \) is an integer which is not divisible by any of the \( p_i \), \( i \in \{1, \ldots, t\} \). For all \( i \in \{1, \ldots, t\} \) the \( p_i \)-th root of unity associated to \( p_i \) and therefore
\[
x_i = 1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} AK_i
\]
with \( K_i \) not divisible by \( p_i \), and thus
\[
\prod_{i=1}^{t} x_i = \prod_{i=1}^{t} (1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} AK_i) = 1 + \prod_{i=1}^{t} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} AK_i
\]
with \( K_i \) not divisible by \( p_i \), but
\[
\prod_{i=1}^{t} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} K_i
\]
is not divisible by any of the \( p_i \), \( i \in \{1, \ldots, t\} \) therefore \( y = \prod_{i=1}^{t} x_i \) is a \( p \)-th root of unity satisfies
\[
x.y = 1 + \prod_{i=1}^{t} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} AM
\]
and it is clear that \( (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_t^{\alpha_t} AK) \) is not divisible by any of the \( p_i \), \( i \in \{1, \ldots, d\} \), 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 that:
\[
x = 1 + \sum_{i=1}^{d} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} AK_i
\]
and
\[
(1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} AK_i) = 1 \quad [n] \quad \forall 1 \leq i \leq d.
\]

**Proof :**
Since \( p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d} \) and \( p_d^{\alpha_d} \) are coprime then it exists two integers \( K'_d \) and \( K_d \) such as
\[
1 = p_d^{\alpha_d} K'_d + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{d-1}^{\alpha_{d-1}} K_d \quad (*)
\]
and therefore
\[
x - 1 = p_d^{\alpha_d} AK'_d + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{d-1}^{\alpha_{d-1}} K_d
\]
with \( K'_d = ((x - 1)/A)K_d \) and \( K_d = ((x - 1)/A)K'_d \).
We have:
\[
(x - p_d^{\alpha_d} AK_d)' = (x - (x - 1)p_d^{\alpha_d} K_d)' = ((1 - p_d^{\alpha_d} K_d) + p_d^{\alpha_d} K_d)' = (\alpha(1 - p_d^{\alpha_d} K_d) + p_d^{\alpha_d} K_d)' = (xp_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{d-1}^{\alpha_{d-1}} K_d + p_d^{\alpha_d} K_d)' = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d})' [p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d}] = 1 \quad [p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d}] \quad \text{from (*)}
\]
On the other hand
\[
x - (x - 1)p_d^{\alpha_d} K_d' = 1 - (x - 1)(1 - p_d^{\alpha_d} K_d') = 1 \quad [A]
\]
Thus \( (x - (x - 1)p_d^{\alpha_d} K_d') = 1 \quad [n] \) and consequently \( (1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d} AK_d)' = 1 \quad [n] \).
Suppose that it exists some integers \( K_1, K_2, \ldots, K_d \) and \( K'_t \) such as:
\[
x = 1 + \sum_{i=1}^{d} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} AK_i + p_1^{\alpha_1} \cdots p_d^{\alpha_d} K'_t
\]
and
\[
(1 + p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} AK_i)' = 1 \quad [n] \quad \forall t \leq i \leq d.
\]
Let \( K_{t-1} \) and \( K'_{t-1} \) be two integers such as
\[
1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{t-1}^{\alpha_{t-1}} K_{t-1} + p_{t-1}^{\alpha_{t-1}} K'_{t-1} \quad (**)
\]
and therefore
\[
p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_d^{\alpha_d} AK_1 = p_1^{\alpha_1} \cdots p_{t-1}^{\alpha_{t-1}} p_d^{\alpha_d} AK_{t-1} + p_{t-1}^{\alpha_{t-1}} \cdots p_d^{\alpha_d} AK_1 K_{t-1}.
\]
We have
\[
(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1 - p_{t-1}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1})^p =
( (p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1)(1 - p_{t-1}^\alpha K_{t-1}) + p_{t-1}^\alpha K_{t-1}^p )
= ( (p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1)p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha \tilde{K}_{t-1} + p_{t-1}^\alpha \tilde{K}_{t-1}^p )
= ( p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1)(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha \tilde{K}_{t-1} + p_{t-1}^\alpha \tilde{K}_{t-1}^p )
= ( p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1)( p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha \tilde{K}_{t-1} + p_{t-1}^\alpha \tilde{K}_{t-1}^p )
\]

however
\[
(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1)^p =
( x - \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK'_{i} )^p
= x^p [ p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha A ]
= 1 [ p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha A ]
\]
and consequently
\[
(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1 - p_{t-1}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1})^p
= ( p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1 - p_{t-1}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1} )^p
= 1 [ p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha A ]
\]
also it is clear that
\[
(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1 - p_{t-1}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1})^p
= 1 [ p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha A ]
\]
and so
\[
(p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK'_{t} + 1 - p_{t-1}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1})^p = 1 [ n ]
\]
That means
\[
(1 + p_{t}^\alpha \ldots p_{d}^\alpha AK'_{t}K_{t-1})^p = 1 [ n ]
\]
We set $K_{i-1} = K'_{i-1}$ and $K'_{t-1} = K_{t-1}$, we obtain so
\[
x = 1 + \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i} + 
\]
with
\[
(1 + p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK_{i})^p = 1 [ n ] \quad \forall t - 1 \leq i \leq d
\]
Thus by induction, we obtain
\[
x = 1 + \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i} + p_{t}^\alpha \ldots p_{d}^\alpha AK'_{t-1} 
= 1 + \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i} + p_{t}^\alpha \ldots p_{d}^\alpha AK'_{t-1}
\]
with 
\[
(1 + p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK_{i})^p = 1 [ n ] \quad \forall t - 1 \leq i \leq d
\]

**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:
\[
x = 1 + \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i}
\]
and
\[
(1 + p_{t}^\alpha p_{t+1}^\alpha \ldots p_{d}^\alpha AK_{i})^p = 1 [ n ] \quad \forall t - 1 \leq i \leq d
\]
If we set $x_i = 1 + p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i}$, 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
\[
\prod_{i=t}^{d} x_i = \prod_{i=t}^{d} (1 + p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i})
\]
\[
= 1 + \sum_{i=t}^{d} p_{i}^\alpha p_{i+1}^\alpha \ldots p_{d}^\alpha AK_{i} [ n ] = x.
\]

**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
\[
x_i = x_1^{p_1} x_2^{p_2} \ldots x_{t-1}^{p_{t-1}} x_t^{p_t} \ldots x_d^{p_d}
\]
from the preceding 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 $x \prod_{i=1}^{t} x_i$ is final $p$-th root of unity modulo $n$ and thus $x = \prod_{i=1}^{t} x_i - 1 \prod_{i=1}^{d} y_i$ 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:** $G_p(n)$ 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
\[
G_p(n) = \langle x_1, x_2, \ldots, x_d \rangle
\]
with $x_i$ an initial $p$-th root of unity modulo $n$ associated to $p_i$. 

International Scholarly and Scientific Research & Innovation 4(7) 2010 984

ISNI:0000000091950263
Theorem 2.4: The map

$$\varphi : G_p^{\phi_1}(n) \times G_p^{\phi_2}(n) \times \cdots \times G_p^{\phi_d}(n) \rightarrow G_p(n)$$

$$(x_1, x_2, \ldots, x_d) \rightarrow x_1 x_2 \cdots x_d$$

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 $\varphi(x_1, x_2, \ldots, x_d) = 1 \iff x_1, x_2, \ldots, x_d = 1$.
Assume for the following that there exists an integer $i$ such that $x_i \neq 1$.
We can easily verify that $x_1, x_2, \ldots, x_d = 1$ is also not divisible.
By $p_i$ but this is absurd, thus $x_1 = 1$ for all $i$ and hence $\varphi$ is injective.

From the previous theorem it is clear that $Card(G_p(n)) = p^d$, where $d$ is a number of distinct
prime factors of $n$ such that $p_i$ divides $q - 1$, that is to say $d = \alpha_p(n)$ and we obtain the following result:

Corollary 2.5:

$$Card(G_p(n)) = p^{\alpha_p(n)}.$$ 

Remark:
From the previous theorem we have

$$G_p(n) = \{ \prod_{1 \leq i \leq d} x_i^{a_i} \mid a_i \in \{0, 1, \ldots, p_i - 1\}, \prod_{i=1}^{d} x_i \}$$

with $x_i$ is a generator of the cyclic group $G_p^{\phi_i}(n)$.

Example:
We give now an algorithm written in Maple that allows us
to give a generating set of the group formed by the $p$-th roots of unity
modulo $n$, where $d$ is the number of distinct prime factors of $n$ such that
$p_i$ divides $n - 1$ for all $i$ and hence $\varphi$ is injective.

We show in the same manner that this system has exactly
one integer $i$ such that $p_i$ divides $n - 1$. For a fixed permutation
we can write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ with $p_i \neq p_j$ for all $i$ and let $x$ be a
$p$-th root of unity modulo $n$, the above results show that if $p_i$ does not divide $p_j - 1$ then $p_i^{\alpha_i}$ divides $x - 1$, on the other hand we have $x^p = 1[n]$ implies that $p_i$ divides $(x - 1)(1 + x + \ldots + x^{p-1})$ and from the lemma 2.1 we obtain $p_i$ divides $x - 1$ and $1 + x + \ldots + x^{p-1}$.

Also provided $p_i$ divides $\lambda(n)$ implies that there exists at least
one integer $i$ such that $p_i$ divides $p_j - 1$. For a fixed permutation
we can write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ with $p_i$ divides $p_j - 1$ for all $i \in \{1, \ldots, d\}$ and does not divide $p_i - 1$ for every $i \in \{d + 1, \ldots, m\}$. Assume for the following $p_{d+1}^{\alpha_{d+1}} \cdots p_m^{\alpha_m} = A$.

We define in the same manner the initial $p$-th roots of unity
modulo $n$ by replacing $A$ with $A$. The initial $p$-th roots of unity
modulo $n$ associated to $p_i$, $i \in \{1, \ldots, d\}$ are the solutions of the system:

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} pAK$$

$$1 + x + x^2 + \ldots + x^{p_i-1} = p_i^{\alpha_i} K'$$

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 $G_p(n)$ of cardinality $p$ and it is
denoted as $G_p^{\phi_i}(n)$.

We define in the same way a final $p$-th root of unity and its
conjugate by replacing $A$ by $pA$ 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:

$$x = 1 + \sum_{i=1}^{d} p_i^{\alpha_i} p_2^{\alpha_2} \cdots p_i^{\alpha_i} \cdots p_d^{\alpha_d} pAK_i$$

Vol:4, No:7, 2010
Finally, note that the product of $d$\thinspace p\thinspace n$ We deduce that any final $A$\thinspace p\thinspace n$ is a cyclic group of order $p$. Hence every $p$\thinspace p\thinspace n$ is generated by the initial $p$\thinspace p\thinspace n$ of unity and more precisely if we denote $x_i$ an initial $p$\thinspace p\thinspace n$ of unity associated to $p_i$, then

$$G_p(n) = \langle x_1, x_2, \ldots, x_d \rangle.$$ 

Also we have the following results:

**Theorem 2.6:** The map $\varphi : G_p^n(n) \times G_p^2(n) \times \ldots \times G_p^d(n) \rightarrow G_p(n)$

$$(x_1, x_2, \ldots, x_d) \mapsto x_1 x_2 \ldots x_d$$

is an isomorphism of groups.

**Corollary 2.6:**

$$\text{Card}(G_p(n)) = p^{n_p(n)}.$$ 

**Remark:**

From the previous theorem we can easily show that $G_p(n) = \{ \prod_{i_1, \ldots, i_d=1}^{d} x_i^{i_1} x_2^{i_2} \ldots x_d^{i_d} \mid , i \in \{1, 2, \ldots, p\} \}$

with $x_i$ is a generator of the cyclic group $G_p^i(n)$.

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 $G_p(n)$ 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 $p^\alpha$ divides $x - 1$.

So $x$ is a solution of the system

$$\begin{cases}
x - 1 = p^{\alpha - 1} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m} K \\
1 + x + x^2 + \ldots + x^{p - 1} = K'
\end{cases}$$

But this system has $p$ solutions modulo $n$ which are $1, 1 + n/p, 1 + 2n/p, \ldots$ 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

$$G_p(n) = \{ 1 + kn/p \mid 0 \leq k \leq p - 1 \}$$

**Remark:**

It is clear that $G_p(n)$ 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 $i \in \{d + 1, \ldots, m\}$ and does not divide $p_i - 1$ for all $i \in \{1, \ldots, d\}$ and assume for the rest of this paper $p_{d+1}^{\alpha_{d+1}} \ldots p_m^{\alpha_m} = A$.

**Definition 2.5:** Let $x$ be a $p$-th root of unity modulo $n, x$ is said of class zero if $x - 1 = p^{\alpha - 1} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_d^{\alpha_d} AK$ with $K$ an integer.

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

**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:

$$x - 1 = p^{\alpha - 1} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_d^{\alpha_d} AK$$

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:

$$\begin{cases}
x - 1 = p^{\alpha - 1} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_d^{\alpha_d} AK \\
1 + x + x^2 + \ldots + x^{p - 1} = p^{\alpha_1} K'
\end{cases}$$

and we conclude with the following lemmas.

**Lemma 2.5:** The following systems have the same number of solutions respectively modulo $n$ and $n/p_1^{\alpha_1 - 1}$.

$$\begin{cases}
x - 1 = p^{\alpha_1 - 1} p_1^{\alpha_2} \ldots p_d^{\alpha_d} AK \\
1 + x + x^2 + \ldots + x^{p - 1} = p^{\alpha_1} K'
\end{cases}$$

**Proof:**

It is clear that any solution of $(\ast)$ is a solution of $(\ast\ast)$. Reciprocally let $x$ be a solution of $(\ast\ast)$, then $x^p = 1 [p^\alpha p_1 p_2 \ldots p_d A]$ that is to say $x^p = 1 + p^\alpha p_1 p_2 \ldots p_d AK_1$ and therefore

$$x^{p_1^{\alpha_1 - 1}} = (1 + p^\alpha p_1 p_2 \ldots p_d AK_1)^{p_1^{\alpha_1 - 1}}$$

$$= 1 + \sum_{i=1}^{p_1^{\alpha_1 - 1}} C_1^{p_1^{\alpha_1 - 1}} (p_1 p_2 \ldots p_d AK_1)^i$$

$$+ (p^\alpha p_1 p_2 \ldots p_d AK_1)^{p_1^{\alpha_1 - 1}}$$
It is easily verified that all $C_{i+1}^i$ are divisible by $p_i^{a_i}$ and $p_i^{a_i-1} \geq \alpha_i$, then $x^{p_i^{a_i-1}} \equiv 1[n]$. On the other hand

$$x^{p_i^{a_i-1}} = (1 + p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK)^{p_i^{a_i-1}}$$

$$= 1 + \sum_{i=1}^{p_i^{a_i-1}} C_{p_i^{a_i-1}}(p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK)^i$$

$$+ (p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK)^{p_i^{a_i-1}}$$

And as $C_{i+1}^i$ are divisible by $p_i$ and $K$ is not divisible by $p_i$, then $x^{p_i^{a_i-1}} - 1$ is divisible by all $p_i$ except $p_i$. Consequently $x^{p_i^{a_i-1}}$ is a solution of $(\ast)$. Let $x$ and $y$ be two solutions of $(\ast)$ such that $x^{p_i^{a_i-1}} = y^{p_i^{a_i-1}}[n]$, then $x^{p_i^{a_i-1}} - 1 = y^{p_i^{a_i-1}} - 1$. Hence $x \equiv y[p_i]$, on the other hand it is clear that $x \equiv y[p_i^{a_i-1}]$, therefore $x \equiv y[p_i^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}]$. We conclude then that the systems $(\ast)$ and $(\ast\ast)$ have the same number of solutions respectively modulo $n$ and $n/p_i^{a_i-1}$. 

**Lemma 2.6**: The following system have $p^2 - p$ solutions modulo $n/p_i^{a_i-1}$.

$$\begin{cases} x - 1 = p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}K \
1 + x + x^2 + \ldots + x^{p_i^{a_i-1}} = p_i K' \end{cases} \tag{\ast\ast}$$

**Proof**: We know that

$$X^p - 1 = \prod_{i=1}^{p_i} (X - \gamma_i)$$

and as 1 is a root of $X^p - 1$ then we take $\gamma_1 = 1$. Finally, we obtain

$$1 + x + x^2 + \ldots + x^{p_i^{a_i-1}} = \prod_{i=2}^{p_i} (X - \gamma_i)$$

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

$$\begin{cases} x - 1 = p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK_2 \\
x - \gamma_2 = p_i K'_2 \\
\vdots \\
x - 1 = p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK_p \\
x - \gamma_p = p_i K'_p \end{cases}$$

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

**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 $G^0_p(n)$ is a subgroup of $G_p(n)$ denoted $G^0_p(n)$ and we have $Card(G^0_p(n)) = p^2$.

**Proof**: Let $x$ and $y$ be two elements of $G^0_p(n)$, there are three cases to distinguish:

- If $x$ and $y$ are in $G^0_p(n)$, then in this case $xy$ belongs $G^0_p(n)$ since the latter is a group and hence $xy$ is in $G^0_p(n)$.
- If $x$ and $y$ are respectively in $G^0_p(n) \setminus G^0_p(n)$ and $G^0_p(n)$, then we have $x - 1 = p^{a_i-1}p_2^{a_2} \ldots p_i^{a_i} \ldots p_d^{a_d}AK$ and $y - 1 = p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK'$. Hence $xy$ is in $G^0_p(n)$.
- If $x$ and $y$ are in $G^0_p(n) \setminus G^0_p(n)$, then:

$$xy = 1 + p^{a_i-1}p_2^{a_2} \ldots p_i^{a_i} \ldots p_d^{a_d}A(K + p_i^{a_i}K')$$

The term $K + p_i^{a_i}K'$ is not divided by $p_i$ and therefore $xy$ is a $p$-th root of unity associated to $p_i$. Hence $xy$ is in $G^0_p(n)$.

- Finally, we can see that $G^0_p(n) \setminus G^0_p(n)$ is a subgroup of $G_p(n)$ associated to $p_i$ and consequently $xy$ is in $G^0_p(n)$.

**Definition 2.7**: Let $x$ be a $p$-th root, we said that $x$ is of the first class if $p^2$ 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:

$$\begin{cases} x - 1 = p^{a_i-1}p_2^{a_2} \ldots p_d^{a_d}AK \\
x + 1 = p_i^{a_i}K' \end{cases}$$

And from the previous we know that this system has $p - 1$ solutions modulo $n$.

Let denote by $G^\times_p(n)$ the set formed by 1 and the initial $p$-th roots of unity associated to $p_i$ that are of first class and we can easily verify that $G^\times_p(n)$ is a cyclic subgroup of $G_p(n)$ of cardinality $p$ and we have the following result:

**Proposition 2.8**: The map

$$\varphi : G^\times_p(n) \times G^0_p(n) \rightarrow G^0_p(n)$$

$$(x, y) \mapsto xy$$
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 $G^+_{n}(n)$ and $G^0(n)$ respectively such that $x \cdot y = 1$, we have:

$$x \cdot y = 1 = p^\alpha p_{\alpha_1}^\alpha p_{\alpha_2}^\alpha \ldots p_{\alpha_d}^\alpha AK \text{ and } y \cdot x = 1 = p^{-\alpha} p_{\alpha_1}^{-\alpha} p_{\alpha_2}^{-\alpha} \ldots p_{\alpha_d}^{-\alpha} AK',$$

therefore

$$xy = 1 = p^\alpha p_{\alpha_1}^\alpha p_{\alpha_2}^\alpha \ldots p_{\alpha_d}^\alpha A(K + p_{\alpha}^{\alpha} K').$$

As $x \cdot y = 1$, then the term $K + p_{\alpha}^{\alpha} K'$ is divided by $p_{\alpha}^{\alpha}$, therefore $p_{\alpha}^{\alpha}$ 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 $x - 1 = p^{-\alpha} AK$, with $K$ an integer not divisible by $p_i$, $i \in \{1, \ldots, d\}$.

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 $y = 1 + p^\alpha AK$ and $z$ a class zero’s $p$-th root. We have:

$$x \cdot y = x = 1 + p^\alpha AK$$

This equation has solutions $K$ and $K'$, also

$$(1 + p^\alpha AK)^p = 1, \text{ therefore } (1 + p^\alpha AK)^p = 1 \text{ as } x - 1 \text{ is divisible by none of the } p_i, \text{ which implies that } K \text{ is divisible by none of the } p_i,$$

this proves that $(1 + p^\alpha AK)$ is a final $p$-th root of the first class. Also it is clear that if we take $K$ and $K'$ as other solutions, then $1 + p^\alpha AK$ and $1 + p^{-\alpha} p_{\alpha_1}^{-\alpha} p_{\alpha_2}^{-\alpha} \ldots p_{\alpha_d}^{-\alpha} AK'$ are the same modulo $n$.

Remark:
If for all $i \in \{1, \ldots, d\}$ 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 $p_1, p_2, \ldots$ and $p_d$.

Proof:
Let $x$ be a final $p$-th root of the first class, we know that there exist $K_1, K_2, \ldots$ and $K_d$ such that

$$x = 1 + \sum_{i=1}^{d} p^\alpha p_{\alpha_1}^\alpha p_{\alpha_2}^\alpha \ldots p_{\alpha_d}^\alpha AK_i$$

and

$$\left(1 + p^\alpha p_{\alpha_1}^\alpha p_{\alpha_2}^\alpha \ldots p_{\alpha_d}^\alpha AK_i\right)^p = 1 \quad \forall 1 \leq i \leq d.$$
Proposition 2.8
The previous result shows that $\phi$ is an isomorphism of groups.

Generally, we have the following result:

and as $G_p^{\pm i}(n)$ and $G_p(\bar{p})(n)$ are groups, then we obtain the result.

Remark:
The previous result shows that $G_p(n)$ is generated by the initial $p$-th roots of the first class and the class zero’s $p$-th roots and as $G_p^{0}(n)$ and $G_p^{\pm}(n)$ are cyclic groups, then

$G_p(n) = \langle x_1, x_2, \ldots, x_d, x_0 \rangle$

with $x_1$ is an initial $p$-th root of the first class associated to $p_1$ and $y_0$ is a class zero’s $p$-th root.

From Proposition 2.8 any initial $p$-th root associated to $p_1$ can be written uniquely as a product of an initial first class $p$-th root associated to $p_1$ by class zero’s $p$-th root.

Theorem 2.9: The map

$\varphi: G_p^{+\pm}(n) \times G_p^{\pm}(n) \times G_p^0(n) \times G_p^{\bar{p}}(n) \rightarrow G_p(n)$

$(x_1, x_2, \ldots, x_m, y) \rightarrow x_1x_2\ldots x_m.y$

is an isomorphism of groups.

Proof:
It is clear that $\varphi$ is a surjective morphism of groups and we show that it is injective as in the analogous previous results.

Corollary 2.8:

Card($G_p(n)$) = $p^{\alpha_p(n)+1}$.

Remark:
From the previous theorem we have

$G_p(n) = \{ x_1^{i_1}x_2^{i_2}\ldots x_d^{i_d}x_0 \}$

with $I = \{1, 2, \ldots, p\}$, $x_i$ is one generator of the cyclic group $G_p^0(n)$ for $i \neq 0$ and $x_0$ is a $p$-th root of the first class different from 1.

We now give an algorithm in MAPLE that allows us to find a generating set of $G_p(n)$. 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; LD := [ ]; LB := [ ]; GEN := [ ];
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
if (LFact[i][1] − 1 mod p = 0) then
end;
end;
end:
end:
end:
end:

Algorithm 2.3

III. Conclusion

For the cardinality of $G_p(n)$, 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:

- Card($G_p(n)$) = $p^{\alpha_p(n)}$
- Card($G_p(pm)$) = $p^{\alpha_p(n)}$
- Card($G_p(p^{\alpha_m}n)$) = $p^{\alpha_p(n)+1}$ with $\alpha \geq 2$

We will now give an algorithm which help us to find, from a fixed integer $n$, a generating set of $G_p(n)$.

Gene_p := proc(n, p) local LB, LD, i, LFact, GEN, P; LD := [ ]; LB := [ ]; GEN := [ ];
if (n mod p^2 = 0) then
GEN := [ ]
end:
end:
end:
for i from 1 to nops(LFact) do
if (LFact[i][1] − 1 mod p = 0) then
end:
end:
LD := \{op(LD), LFact[i]\};
end:
end:
for \texttt{i} from 1 to nops(LD) do
P := convert(Berlekamp(x^p - 1, x) mod LD[i][1], list);
if (P[1] - x + 1 mod LD[i][1] <> 0) then
LB := Bezout(LD[i][1], n/(LD[i][1]^\*LD[i][2]), P[1] - x + 1);
else
LB := Bezout(LD[i][1], n/(LD[i][1]^\*LD[i][2]), P[2] - x + 1);
end:
end:
else
LB := Bezout(LD[i][1], n/(LD[i][1]^\*LD[i][2]), P[2] - x + 1);
end:
end:
end:
for \texttt{i} from 1 to nops(LFact) do
if \(LFact[i][1] - 1 \mod p = 0\) then
LD := \{op(LD), LFact[i]\};
end:
end:
end:
for \texttt{i} from 1 to nops(LP) do
P := convert(Berlekamp(x^p - 1, x) mod LD[i][1], list);
if (P[1] - x + 1 mod LD[i][1] <> 0) then
LB := Bezout(LD[i][1], n/(LD[i][1]^\*LD[i][2]), P[1] - x + 1);
else
LB := Bezout(LD[i][1], n/(LD[i][1]^\*LD[i][2]), P[2] - x + 1);
end:
end:
end:
end:
end:
end:
end:
end:
end:
end:
if (GEN = \[ \]) then
GEN := \[ \];
end;
eval(GEN);
end:

Algorithm 2.4

REFERENCES