

# 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 :

$$\mathbf{G}_p(n) = \{x \in (\mathbb{Z}/n\mathbb{Z})^* / x^p = 1\}.$$

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  $\mathbf{G}_p(n)$  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 :

$$\text{Card}(\mathbf{G}_p(n)) = p^t$$

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].

Rochdi Omami, Mohamed Omami and Raouf Ouni are doctoral students at the Faculty of Science of Tunis : University El Manar, Tunis 2092

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

Let us consider an integer  $n \geq 3$  and  $p$  a prime odd number, let  $n = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  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:

$$\alpha_p(m.n) = \alpha_p(m) + \alpha_p(n) - \alpha_p(\text{GCD}(m, n)).$$

In the following, we consider an integer  $n \geq 3$  whose the factorization is  $n = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ , 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  $x^p \equiv 1[n] \implies x^p \equiv 1[p_i]$  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:*

$$\text{GCD}(x - 1, 1 + x + x^2 + \dots + x^{p-1}) \in \{1, p\}$$

*Proof :*

One can easily verify that we have:

$$(x - 1)(x^{p-2} + 2x^{p-3} + 3x^{p-4} + \dots + (p - 2)x + (p - 1)) - (1 + x + x^2 + \dots + x^{p-1}) = p. \blacksquare$$

*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  $x^p \equiv 1[n] \implies x^p \equiv 1[p_i^{\alpha_i}]$  then  $p_i^{\alpha_i}$  divides  $x^p - 1 = (x - 1)(1 + x + x^2 + \dots + x^{p-1})$ , or  $p$  does not divide  $p_i - 1$  and thus  $p_i$  divides  $x - 1$  also we know that the  $GCD(x - 1, 1 + x + x^2 + \dots + x^{p-1}) \in \{1, p\}$  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  $x^p - 1 = (x - 1)(1 + x + x^2 + \dots + x^{p-1})$  and consequently  $p$  divides  $x - 1$  or  $1 + x + x^2 + \dots + x^{p-1}$  and seeing the relation given in the proof of *Lemma 2.1* we conclude that  $p$  divides both at the same time, and thus

$$PGCD(x - 1, 1 + x + x^2 + \dots + x^{p-1}) = p.$$

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 :

$$x^p \equiv 1 [p^3] \implies x \equiv 1 [p^2]$$

*Proof :*

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

*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  $x^p \equiv 1 [p^\alpha]$  ( $\alpha \geq 3$ ) and so in particular  $x^p \equiv 1 [p^3]$ , from the precedent lemma we conclude that  $x \equiv 1 [p^2]$ .

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

•  $n = 7^3 * 29 = 9947$ , we have  $344^7 \equiv 1 [n]$  and  $344 \equiv 1 [7^3]$ .  $2402^7 \equiv 1 [n]$  and  $2402 \equiv 1 [7^4]$ .

•  $n = 7^2 * 29 * 43 * 71 = 4338313$ , we have  $350547^7 \equiv 1 [n]$  and  $350547 \equiv 1 [7^4]$ .

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  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  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  $\{1, 2, \dots, m\}$  such that  $n = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(d)}^{\alpha_{\sigma(d)}} p_{\sigma(d+1)}^{\alpha_{\sigma(d+1)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$  and  $p$  divides only  $p_{\sigma(1)}^{\alpha_{\sigma(1)}}, p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots$  and  $p_{\sigma(d)}^{\alpha_{\sigma(d)}}$ , then  $p_{\sigma(d+1)}^{\alpha_{\sigma(d+1)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$  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  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  with  $p_i \neq p$  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  $p_2^{\alpha_2} \dots p_m^{\alpha_m}$  divides  $x - 1$ , then  $x$  is a solution of one of the following systems :

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

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

$$\begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K \\ 1 + x + x^2 + \dots + x^{p-1} = p_1^{\alpha_1} K' \end{cases} \quad (\star)$$

$$\begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K \\ 1 + x + x^2 + \dots + x^{p-1} = p_1 K' \end{cases} \quad (\star\star)$$

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  $(\star\star)$ , then  $x^p \equiv 1 [p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m}]$

that is to say  $x^p = 1 + p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1$  and therefore

$$\begin{aligned} x^{p p_1^{\alpha_1 - 1}} &= (1 + p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1)^{p_1^{\alpha_1 - 1}} \\ &= 1 + \sum_{i=1}^{p_1^{\alpha_1 - 1} - 1} C_{p_1^{\alpha_1 - 1}}^i (p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1)^i + \\ &\quad (p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1)^{p_1^{\alpha_1 - 1}} \end{aligned}$$

It is easily verified that all  $C_{p_1^{\alpha_1 - 1}}^i$  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

$$\begin{aligned} x^{p_1^{\alpha_1 - 1}} &= (1 + p_2^{\alpha_2} \dots p_m^{\alpha_m} K)^{p_1^{\alpha_1 - 1}} \\ &= 1 + \sum_{i=1}^{p_1^{\alpha_1 - 1} - 1} C_{p_1^{\alpha_1 - 1}}^i (p_2^{\alpha_2} \dots p_m^{\alpha_m} K)^i + \\ &\quad (p_2^{\alpha_2} \dots p_m^{\alpha_m} K)^{p_1^{\alpha_1 - 1}} \end{aligned}$$

and as the  $C_{p_1^{\alpha_1 - 1}}^i$  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 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  $(\star\star)$  such as  $x^{p_1^{\alpha_1 - 1}} = y^{p_1^{\alpha_1 - 1}} [n]$  and thus  $x^{p_1^{\alpha_1 - 1}} = y^{p_1^{\alpha_1 - 1}} [p_1]$ , hence  $x \equiv y [p_1]$ , on the other hand it is clear that  $x \equiv y [p_2^{\alpha_2} \dots p_m^{\alpha_m}]$  and consequently  $x \equiv y [p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m}]$ . 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  $(\star\star)$  have the same number of solutions modulo  $n$  and  $n/p_1^{\alpha_1 - 1}$  respectively. ■

**Lemma 2.4:** The following system

$$\begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K \\ 1 + x + x^2 + \dots + x^{p-1} = p_1 K' \end{cases} \quad (\star\star)$$

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

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

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

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

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

$$\begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K_2 \\ x - \gamma_2 = p_1 K'_2 \end{cases} \quad \begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K_3 \\ x - \gamma_3 = p_1 K'_3 \end{cases} \\ \dots \quad \begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K_p \\ x - \gamma_p = p_1 K'_p \end{cases}$$

It is clear that each of these systems has only one solution modulo  $p_1 p_2^{\alpha_2} \dots p_m^{\alpha_m}$ . Also the solutions of these systems are 2 by 2 distinct. Indeed if we denote  $x_i$  the solution of the following system

$$\begin{cases} x - 1 = p_2^{\alpha_2} \dots p_m^{\alpha_m} K_i \\ x - \gamma_i = p_1 K'_i \end{cases}$$

then  $x_i \equiv \gamma_i [p_1]$ . 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

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  $1 + X + X^2 + \dots + X^{p-1}$  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  $1 + X + X^2 + \dots + X^6$  in the field  $\mathbb{Z}/29\mathbb{Z}[X]$ , by using Berlekamp's algorithm, we obtain :

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

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  $K = -10$ .

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

$$\mathbf{G}_7(n) = \{1006441, 1006441^2, \dots, 1006441^7\}$$

that is to say

$$\mathbf{G}_7(n) = \{1006441, 8684356, 6860611, 4797001, 5450251, 9979951, 1\}$$

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  $\mathbf{G}_p(n)$ .

```

Gene_p := proc(n, p) local LB, LD, P, gen, i, LFact;
LD := []; LB := [];
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
if (LFact[i][1] - 1 mod p = 0) then
LD := [op(LD), LFact[i]];
end;
end;
P := convert(Berlekamp(x^p - 1, x) mod LD[1][1], list);
if (P[1] - x + 1 mod LD[1][1] <> 0) then
LB := Bezout(LD[1][1], n/(LD[1][1]^LD[1][2]), P[1] - x + 1);
gen := ((LD[1][1] * LB[1] - (P[1] - x) mod n) &^
(LD[1][1]^(LD[1][2] - 1))) mod n;
else
LB := Bezout(LD[1][1], n/(LD[1][1]^LD[1][2]), P[2] - x + 1);
gen := (LD[1][1] * LB[1] - (P[2] - x) mod n) &^
(LD[1][1]^(LD[1][2] - 1))) mod n;
end;
eval(gen);
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  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  and  $p$  a prime odd number such that  $p_i \neq p$  for all  $i$ . For a fixed permutation we can write  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m}$  with  $p$  divides  $p_i - 1$  for all  $i \in \{1, \dots, d\}$ . We have seen that if  $x$  is a  $p$ -th root of unity modulo  $n$ , then  $p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m}$  divides  $x - 1$ . Thus  $p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m}$  don't have a significant role in our study, for the rest we set  $p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m} = A$ .

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

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK.$$

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 :

$$\begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK & (*) \\ 1 + x + x^2 + \dots + x^{p-1} = p_i^{\alpha_i} K' \end{cases}$$

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

$$\begin{aligned} x - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK \text{ and} \\ y - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK' \end{aligned}$$

and therefore

$$\begin{aligned} x.y &= 1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} A(K \\ &+ K' + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AKK') \end{aligned}$$

Note that  $x.y$  is a  $p$ -th root of unity and therefore at this stage we have two case. If  $p_i$  divides  $(K + K' + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AKK')$ , then  $p_i^{\alpha_i}$  divides  $x.y - 1$  and we obtain  $x.y = 1$ . If  $p_i$  does not divide  $(K + K' + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AKK')$ , 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

$$x.y - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_j^{\alpha_j} \dots p_d^{\alpha_d} AK$$

with  $K$  is an integer which is not divisible by  $p_i$  and  $p_j$ .

*Proof :*

We have

$$\begin{aligned} x - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_1 \text{ and} \\ y - 1 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_j^{\alpha_j} \dots p_d^{\alpha_d} AK_2 \end{aligned}$$

and therefore

$$x.y = 1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_j^{\alpha_j} \dots p_d^{\alpha_d} A(p_i^{\alpha_i} K_1 + p_i^{\alpha_i} K_2)$$

and as  $p_i$  does not divide  $K_1$  also  $p_j$  does not divide  $K_2$ , then  $(p_i^{\alpha_j} K_1 + p_i^{\alpha_i} K_2)$  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  $p_i, i \in \{1, \dots, d\}$  does not divide  $x - 1$ , that is to say  $x - 1 = AK$ , with  $K$  an integer not divisible by any  $p_i, i \in \{1, \dots, d\}$ .

**Remark :**

The existence of final  $p$ -th roots of unity modulo  $n$  is ensured by the preceding proposition, in fact if for all  $i \in \{1, \dots, d\}$  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  $p_i, i \in \{1, \dots, d\}$ , 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  $p_1, p_2, \dots$  are  $p_t$  and thus

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} AK$$

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

$$x_i = 1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_i$$

with  $K_i$  not divisible by  $p_i$ , and thus

$$\prod_{i=1}^t x_i = \prod_{i=1}^t (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_i)$$

$$= 1 + p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} A \sum_{i=1}^t p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} K_i + K'n$$

but  $\sum_{i=1}^t p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} K_i$  is not divisible by any of the

$p_i, i \in \{1, \dots, t\}$  therefore  $y = \prod_{i=1}^t x_i$  is a  $p$ -th root of unity satisfies  $y = 1 + p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM$  with  $M$  an integer which is not divisible by  $p_i, i \in \{1, \dots, t\}$ . So

$$x.y = 1 + A(p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM + p_1^{\alpha_1} \dots p_t^{\alpha_t} AK)$$

It is clear that  $(p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM + p_1^{\alpha_1} \dots p_t^{\alpha_t} AK)$  is not divisible by any of the  $p_i, i \in \{1, \dots, d\}$ , and hence the result. ■

**Theorem 2.3:** Let  $x$  be a final  $p$ -th root of unity modulo  $n$ , then it exists  $d$  integers  $K_1, K_2, \dots, K_d$  such as:

$$x = 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i$$

and

$$(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n] \quad \forall 1 \leq i \leq d.$$

**Proof :**

Since  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d}$  and  $p_d^{\alpha_d}$  are coprime then it exists two integers  $\tilde{K}'_d$  and  $\tilde{K}_d$  such as

$$1 = p_d^{\alpha_d} \tilde{K}'_d + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} \tilde{K}_d \quad (*)$$

and therefore

$$x - 1 = p_d^{\alpha_d} AK'_d + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_d$$

with  $K'_d = ((x - 1)/A)\tilde{K}'_d$  and  $K_d = ((x - 1)/A)\tilde{K}_d$ . We have :

$$\begin{aligned} (x - p_d^{\alpha_d} AK'_d)^p &= (x - (x - 1)p_d^{\alpha_d} \tilde{K}'_d)^p \\ &= (a(1 - p_d^{\alpha_d} \tilde{K}'_d) + p_d^{\alpha_d} \tilde{K}'_d)^p \\ &= (xp_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} \tilde{K}_d + p_d^{\alpha_d} \tilde{K}'_d)^p \\ &= (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} \tilde{K}_d)^p + (p_d^{\alpha_d} \tilde{K}'_d)^p \quad [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d}] \\ &= 1 [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d}] \quad \text{from } (*) \end{aligned}$$

On the other hand

$$\begin{aligned} x - (x - 1)p_d^{\alpha_d} \tilde{K}'_d &= 1 + (x - 1)(1 - p_d^{\alpha_d} \tilde{K}'_d) \\ &= 1 [A] \end{aligned}$$

Thus  $(x - (x - 1)p_d^{\alpha_d} \tilde{K}'_d)^p = 1[n]$  and consequently  $(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_d)^p = 1[n]$ .

Suppose that it exists some integers  $K_t, K_2, \dots, K_d$  and  $K'_t$  such as :

$$x = 1 + \sum_{i=t}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i + p_t^{\alpha_t} \dots p_d^{\alpha_d} AK'_t$$

and

$$(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n] \quad \forall t \leq i \leq d$$

Let  $\tilde{K}'_{t-1}$  and  $\tilde{K}_{t-1}$  be two integers such as

$$1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1} + p_{t-1}^{\alpha_{t-1}} \tilde{K}'_{t-1} \quad (**)$$

and therefore

$$\begin{aligned} p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK'_t &= p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK'_t \tilde{K}'_{t-1} + \\ & p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK'_t \tilde{K}'_{t-1}. \end{aligned}$$

We have

$$\begin{aligned} & (p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1 - p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_t' \tilde{K}_{t-1}')^p \\ &= ((p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1)(1 - p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1}') + \\ & \quad p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1}')^p \\ &= ((p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1)p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1} + \\ & \quad p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1}')^p \\ &= (p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1)^p (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1})^p + \\ & \quad (p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1}')^p [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}}] \end{aligned}$$

however

$$\begin{aligned} & (p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1)^p \\ &= (x - \sum_{i=t}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p \\ &= x^p [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} A] \\ &= 1 [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} A] \end{aligned}$$

and consequently

$$\begin{aligned} & (p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1 - p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_t' \tilde{K}_{t-1}')^p \\ &= (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1})^p + \\ & \quad (p_{t-1}^{\alpha_{t-1}} \tilde{K}_{t-1}')^p [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}}] \\ &= 1 [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}}] \quad \text{from } (***) \end{aligned}$$

also it is clear that

$$(p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1 - p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_t' \tilde{K}_{t-1}')^p = 1 [p_d^{\alpha_d} \dots p_t^{\alpha_t} A]$$

and so

$$(p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_t' + 1 - p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_t' \tilde{K}_{t-1}')^p = 1 [n]$$

That means

$$(1 + p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_t' \tilde{K}_{t-1}')^p = 1 [n].$$

We set  $K_{t-1} = K_t' \tilde{K}_{t-1}$  and  $K_{t-1}' = K_t' \tilde{K}_{t-1}'$ , we obtain so

$$\begin{aligned} x &= 1 + \sum_{i=t}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i + \\ & \quad p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_{t-1} + p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_{t-1}' \\ &= 1 + \sum_{i=t-1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i + \\ & \quad p_{t-1}^{\alpha_{t-1}} \dots p_d^{\alpha_d} AK_{t-1}' \end{aligned}$$

with

$$(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n] \quad \forall t-1 \leq i \leq d$$

Thus by induction, we obtain

$$\begin{aligned} x &= 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i + p_1^{\alpha_1} \dots p_d^{\alpha_d} AK_1' \\ &= 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i \quad [n] \end{aligned}$$

with  $(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n], \forall 1 \leq i \leq d. \blacksquare$

*Corollary 2.2:* Any final  $p$ -th root of unity modulo  $n$  is a product of  $d$  initial  $p$ -th roots associated respectively to  $p_1, p_2, \dots$  and  $p_d$ .

*Proof:*

From the precedent theorem, it exists some integers  $K_1, K_2, \dots, K_d$  such as:

$$x = 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i$$

and

$$(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n] \quad \forall 1 \leq i \leq d$$

If we set  $x_i = 1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i$ , 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

$$\begin{aligned} \prod_{i=1}^d x_i &= \prod_{i=1}^d (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i) \\ &= 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i [n] = x. \blacksquare \end{aligned}$$

*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  $x_1, x_2, \dots$  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  $y_1, y_2, \dots$  and  $y_d$  initial  $p$ -th roots of unity modulo  $n$  associated respectively

to  $p_1, p_2, \dots$  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  $p_i. \blacksquare$

*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

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

with  $x_i$  an initial  $p$ -th root of unity modulo  $n$  associated to  $p_i$ .

**Theorem 2.4:** The map

$$\varphi : \mathbf{G}_p^{p_1}(n) \times \mathbf{G}_p^{p_2}(n) \dots \times \mathbf{G}_p^{p_d}(n) \longrightarrow \mathbf{G}_p(n)$$

$$(x_1, x_2, \dots, x_d) \longmapsto x_1 \cdot x_2 \cdot \dots \cdot x_d$$

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  $\varphi(x_1, x_2, \dots, x_d) = 1 \iff x_1 \cdot x_2 \cdot \dots \cdot x_d = 1$ , assume that there exists an integer  $i$  such that  $x_i \neq 1$ , then we can easily verify that  $x_1 \cdot x_2 \cdot \dots \cdot x_d - 1$  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  $Card(\mathbf{G}_p(n)) = p^d$ , 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:**

$$Card(\mathbf{G}_p(n)) = p^{\alpha_p(n)}.$$

*Remark :*

From the previous theorem we have

$$\mathbf{G}_p(n) = \left\{ \prod_{(i_1, i_2, \dots, i_d) \in I^d} x_1^{i_1} x_2^{i_2} \dots x_d^{i_d} \text{ , with } I = \{1, 2, \dots, p\} \right\}$$

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 := 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
LD := [op(LD), LFact[i]];
end :
end :
for 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);
GEN := [op(GEN), ((LD[i][1] * LB[1] - (P[1] - x) mod n) &^ (LD[i][1]^(LD[i][2] - 1)) mod n)];
else
LB := Bezout(LD[i][1], n/(LD[i][1]^LD[i][2]), P[2] - x + 1);
GEN := [op(GEN), (LD[i][1]*LB[1] - (P[2] - x) mod n) &^ (LD[i][1]^(LD[i][2] - 1)) mod n];
end :
end :
if (GEN = [ ]) then
```

$GEN := [1];$

$end :$

$eval(GEN);$

$end :$

### 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  $n = p p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  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  $(x - 1)(1 + x + \dots + x^{p-1})$  and from the lemma 2.1 we obtain  $p$  divides  $x - 1$  and  $1 + x + \dots + x^{p-1}$ .

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  $n = p p_1^{\alpha_1} \dots p_d^{\alpha_d} \dots p_m^{\alpha_m}$  with  $p$  divides  $p_i - 1$  for all  $i \in \{1, \dots, d\}$  and does not divide  $p_i - 1$  for every  $i \in \{d + 1, \dots, m\}$ . Assume for the following  $p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m} = A$ . We define in the same manner the initial  $p$ -th roots of unity modulo  $n$  by replacing  $A$  with  $pA$ . The initial  $p$ -th roots of unity modulo  $n$  associated to  $p_i, i \in \{1, \dots, d\}$  are the solutions of the system :

$$\begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} pAK \\ 1 + x + x^2 + \dots + x^{p-1} = p_i^{\alpha_i} K' \end{cases}$$

We show in the same manner that this system has exactly  $p - 1$  roots modulo  $n$ . Thus for all  $i \in \{1, \dots, d\}$  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  $pA$  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  $K_1, K_2, \dots, K_d$  such that :

$$x = 1 + \sum_{i=1}^d p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} pAK_i$$

and

$$(1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} pAK_i)^p = 1 [n] \quad \forall 1 \leq i \leq d.$$

Indeed to prove this result we can just proceed as above and replacing  $A$  by  $pA$ .

We deduce that any final  $p$ -th root of unity modulo  $n$  is the product of  $d$  initial  $p$ -th roots associated respectively to  $p_1, p_2, \dots$  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

$$\mathbf{G}_p(n) = \langle x_1, x_2, \dots, x_d \rangle.$$

Also we have the following results :

*Theorem 2.6:* The map

$$\begin{aligned} \varphi : \mathbf{G}_p^{p_1}(n) \times \mathbf{G}_p^{p_2}(n) \dots \times \mathbf{G}_p^{p_d}(n) &\longrightarrow \mathbf{G}_p(n) \\ (x_1, x_2, \dots, x_d) &\longmapsto x_1 x_2 \dots x_d \end{aligned}$$

is an isomorphism of groups.

*Corollary 2.6:*

$$\text{Card}(\mathbf{G}_p(n)) = p^{\alpha_p(n)}.$$

*Remark :*

From the previous theorem we can easily show that

$$\mathbf{G}_p(n) = \left\{ \prod_{(i_1, i_2, \dots, i_d) \in I^d} x_1^{i_1} x_2^{i_2} \dots x_d^{i_d}, \text{ with } I = \{1, 2, \dots, p\} \right\}$$

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  $n = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  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  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  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

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

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

*Proposition 2.5:* Let  $n = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  with  $\alpha \geq 2$  and  $p$  does not divide  $p_i - 1$  for all  $i$ , then

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

*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  $n = p^\alpha p_1^{\alpha_1} \dots p_d^{\alpha_d} \dots p_m^{\alpha_m}$  with  $p$  divides  $p_i - 1$  for all  $i \in \{1, \dots, d\}$  and does not divide  $p_i - 1$  for all  $i \in \{d+1, \dots, m\}$  and assume for the rest of this paper  $p_{d+1}^{\alpha_{d+1}} \dots p_m^{\alpha_m} = A$ .

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

It is clear that there are  $p$   $p$ -th roots of unity of class zero which are  $\{1 + kn/p; \quad 0 \leq k \leq p-1\}$  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 is said initial root if every  $p_i, i \in \{1, \dots, d\}$  divides  $x - 1$  except for only one  $p_i$ . We said that this root is associated to  $p_i$ . And we write :

$$x - 1 = p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK.$$

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 :

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

and we conclude with the following lemmas. ■

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

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

$$\begin{cases} x - 1 = p^{\alpha-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK \\ 1 + x + x^2 + \dots + x^{p-1} = p_1 K' \end{cases} \quad (\star\star)$$

*Proof :*

It is clear that any solution of  $(\star)$  is a solution of  $(\star\star)$ . Reciprocally let  $x$  be a solution of  $(\star\star)$ , then  $x^p \equiv 1 [p^\alpha p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} A]$  that is to say  $x^p = 1 + p^\alpha p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_1$  and therefore

$$\begin{aligned} x^{pp_1^{\alpha_1-1}} &= (1 + p^\alpha p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_1)^{p_1^{\alpha_1-1}} \\ &= 1 + \sum_{i=1}^{p_1^{\alpha_1-1}-1} \mathbf{C}_{p_1^{\alpha_1-1}}^i (p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_1)^i \\ &\quad + (p^\alpha p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_1)^{p_1^{\alpha_1-1}} \end{aligned}$$



It is easily verified that all  $C_{p_1^{\alpha_1-1}}^i$  are divisible by  $p_1^{\alpha_1-1}$  and  $p_1^{\alpha_1-1} \geq \alpha_1$ , then  $x^{p_1^{\alpha_1-1}} \equiv 1 [n]$ . On the other hand

$$\begin{aligned} x^{p_1^{\alpha_1-1}} &= (1 + p^{\alpha_1-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK)^{p_1^{\alpha_1-1}} \\ &= 1 + \sum_{i=1}^{p_1^{\alpha_1-1}-1} C_{p_1^{\alpha_1-1}}^i (p^{\alpha_1-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK)^i \\ &\quad + (p^{\alpha_1-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK)^{p_1^{\alpha_1-1}} \end{aligned}$$

And as  $C_{p_1^{\alpha_1-1}}^i$  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  $(\star\star)$  such that  $x^{p_1^{\alpha_1-1}} = y^{p_1^{\alpha_1-1}} [n]$  thus  $x^{p_1^{\alpha_1-1}} = y^{p_1^{\alpha_1-1}} [p_1]$ . Hence  $x \equiv y [p_1]$ , on the other hand it is clear that  $x \equiv y [p_2^{\alpha_2} \dots p_d^{\alpha_d} A]$  therefore  $x \equiv y [p_1 p_2^{\alpha_2} \dots p_d^{\alpha_d} A]$ . We conclude then that the systems  $(\star)$  and  $(\star\star)$  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  $n/p_1^{\alpha_1-1}$ .

$$\begin{cases} x - 1 = p^{\alpha_1-1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K \\ 1 + x + x^2 + \dots + x^{p-1} = p_1 K' \end{cases} \quad (\star\star)$$

*Proof :*

We know that

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

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

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

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

$$\begin{cases} x - 1 = p^{\alpha_1-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_2 \\ x - \gamma_2 = p_1 K'_2 \\ \vdots \\ x - 1 = p^{\alpha_1-1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK_p \\ x - \gamma_p = p_1 K'_p \end{cases}$$

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  $G_p^0(n)$  is a subgroup of  $G_p(n)$  denoted  $G_p^{p_i}(n)$  and we have  $Card(G_p^{p_i}(n)) = p^2$ .

*Proof :*

Let  $x$  and  $y$  be two elements of  $G_p^{p_i}(n)$ , there are three cases

to distinguish :

- If  $x$  and  $y$  are in  $G_p^0(n)$ , then in this case  $xy$  belongs  $G_p^0(n)$  since the latter is a group and hence  $xy$  is in  $G_p^{p_i}(n)$ .
- If  $x$  and  $y$  are respectively in  $G_p^{p_i}(n) \setminus G_p^0(n)$  and  $G_p^0(n)$ ,

then we have  $x - 1 = p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK$  and  $y - 1 = p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK'$  with  $K$  an integer not divisible by  $p_i$  thus

$$xy = 1 + p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} A(K + p_i^{\alpha_i} K')$$

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

- If  $x$  and  $y$  are in  $G_p^{p_i}(n) \setminus G_p^0(n)$ , then :

$x - 1 = p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK$  and  $y - 1 = p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK'$  with  $K$  and  $K'$  are two integers not divided by  $p_i$  therefore

$$\begin{aligned} xy &= 1 + p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} A(K + K') \\ &\quad + p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AKK' \end{aligned}$$

If the term  $K + K' + p^{\alpha_1-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AKK'$  is divided by  $p_i$  then  $xy$  belongs to  $G_p^0(n) \subset G_p^{p_i}(n)$ , otherwise  $xy$  is a  $p$ -th root associated to  $p_i$  and consequently  $xy$  is in  $G_p^{p_i}(n)$ .

Thus  $G_p^{p_i}(n)$  is stable for the product and as the inverse of the element  $x$  is  $x^{p-1}$ , then  $G_p^{p_i}(n)$  is stable by the inverse operation which proves that  $G_p^{p_i}(n)$  is a subgroup of  $G_p(n)$ . Finally, we can see that  $G_p^0(n)$  does not contain an initial  $p$ -th root associated to  $p_i$  which allows us to conclude that  $Card(G_p^{p_i}(n)) = (p^2 - p) + p = p^2$ . ■

*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 :

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

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

Let denote by  $G_p^+(n)$  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  $G_p^+(n)$  is a cyclic subgroup of  $G_p(n)$  of cardinality  $p$  and we have the following result :

*Proposition 2.8:* The map

$$\begin{aligned} \varphi : G_p^+(n) \times G_p^0(n) &\longrightarrow G_p^{p_i}(n) \\ (x, y) &\longmapsto xy \end{aligned}$$

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  $\mathbf{G}_p^{+1}(n)$  and  $\mathbf{G}_p^0(n)$  respectively such that  $x.y = 1$ , we have :

$$x - 1 = p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK \text{ and } y - 1 = p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK', \text{ therefore}$$

$$xy = 1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} A(K + p_i^{\alpha_i} K').$$

As  $x.y = 1$ , then the term  $K + p_i^{\alpha_i} K'$  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  $p_i, i \in \{1, \dots, d\}$  does not divide  $x - 1$ , which means  $x - 1 = p^{\alpha-1} AK$ , with  $K$  an integer not divisible by  $p_i, i \in \{1, \dots, d\}$ .

*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 :

$$\begin{aligned} x = yz &\iff x = (1 + p^\alpha AK)(1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK') \\ &\iff x - 1 = p^\alpha AK + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK' \\ &\iff \frac{x - 1}{p^{\alpha-1} A} = pK + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} K' \end{aligned}$$

This equation has solutions  $K$  and  $K'$ , also  $(1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK')^p = 1$ , therefore  $(1 + p^\alpha AK)^p = 1$  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  $(1 + p^\alpha AK)$  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  $1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_d^{\alpha_d} AK'$  are the same modulo  $n$ . ■

*Remark :*

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

*Proof :*

Let  $x$  be a final  $p$ -th root of the first class, we know that there

exist  $K_1, K_2, \dots$  and  $K_d$  such that

$$x = 1 + \sum_{i=1}^d p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i$$

and

$$(1 + p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i)^p = 1 [n] \quad \forall 1 \leq i \leq d.$$

If we set  $x_i = 1 + p^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_d^{\alpha_d} AK_i$ , then  $x_i$  is 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  $p_i, i \in \{1, \dots, d\}$ , 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  $p_1, p_2, \dots$  and  $p_t$ . Thus

$$x - 1 = p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} AK$$

with  $K$  an integer not divisible by  $p_i, i \in \{t+1, \dots, d\}$ . For all  $i \in \{1, \dots, t\}$ , let  $x_i$  be an initial  $p$ -th associated to  $p_i$  therefore

$$x_i = 1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_i$$

with  $K_i$  not divided by  $p_i$ , whereof

$$\prod_{i=1}^t x_i = \prod_{i=1}^t (1 + p^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AK_i)$$

$$= 1 + p^{\alpha-1} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} A \sum_{i=1}^t p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} K_i + K' n$$

but  $\sum_{i=1}^t p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_t^{\alpha_t} K_i$  is divisible by none of the  $p_i, i \in \{1, \dots, t\}$ . Consequently  $y = \prod_{i=1}^t x_i$  is a root which verify

$$y = 1 + p^{\alpha-1} p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM \text{ with } M \text{ an integer that not divided by } p_i, i \in \{1, \dots, t\}. \text{ Thereby}$$

$$x.y = 1 + p^{\alpha-1} A(p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM + p_1^{\alpha_1} \dots p_t^{\alpha_t} AK)$$

It is clear that  $(p_{t+1}^{\alpha_{t+1}} \dots p_d^{\alpha_d} AM + p_1^{\alpha_1} \dots p_t^{\alpha_t} AK)$  is divisible by none of the  $p_i, i \in \{1, \dots, d\}$ , 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  $p_1, p_2, \dots$  and  $p_d$ , hence the result. Now let us assume that  $x$  is not a final  $p$ -th root so there exists  $x_1, x_2, \dots$  and  $x_t$  initial  $p$ -th roots such that  $x_1 x_2 \dots x_t$  is a final conjugate of  $x$ , then  $x x_1 x_2 \dots x_t$  is a final  $p$ -th root, and we have :

$$x x_1 x_2 \dots x_t = y_1 y_2 \dots y_d y_0$$

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  $x_i = x_i^+ z_i$ , with  $x_i^+ \in \mathbf{G}_p^{p_1}(n)$  and  $z_i \in \mathbf{G}_p^0(n)$ . So

$$x = y_1 y_2 \dots y_d (x_1^+ x_2^+ \dots x_t^+)^{-1} (z_1 z_2 \dots z_t)^{-1} y_0$$

and as  $\mathbf{G}_p^{p_1}(n)$  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  $\mathbf{G}_p^{p_1}(n)$  are cyclic groups, then

$$\mathbf{G}_p(n) = \langle x_1, x_2, \dots, x_d, x_0 \rangle$$

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 :

**Theorem 2.9:** The map

$$\varphi : \mathbf{G}_p^{p_1}(n) \times \mathbf{G}_p^{p_2}(n) \dots \times \mathbf{G}_p^{p_m}(n) \times \mathbf{G}_p^0(n) \longrightarrow \mathbf{G}_p(n)$$

$$(x_1, x_2, \dots, x_m, y) \longmapsto x_1 x_2 \dots x_m y$$

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:**

$$\text{Card}(\mathbf{G}_p(n)) = p^{\alpha_p(n)+1}.$$

*Remark :*

From the previous theorem we have

$$\mathbf{G}_p(n) = \left\{ \prod_{(i_1, i_2, \dots, i_d, i) \in I^{d+1}} x_1^{i_1} x_2^{i_2} \dots x_d^{i_d} x_0^i \right\}$$

with  $I = \{1, 2, \dots, p\}$ ,  $x_i$  is one generator of the cyclic group  $\mathbf{G}_p^{p_i}(n)$  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  $\mathbf{G}_p(n)$ . 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;
LD := []; LB := []; GEN := [];
GEN := [op(GEN), 1 + n/p];
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
if (LFact[i][1] - 1 mod p = 0) then
LD := [op(LD), LFact[i]];
end;
end;
for 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);
GEN := [op(GEN), ((LD[i][1] * LB[1] - (P[1] - x) mod n) &^ (LD[i][1]^LD[i][2] - 1)) mod n];
else
LB := Bezout(LD[i][1], n/(LD[i][1]^LD[i][2]), P[2] - x + 1);
GEN := [op(GEN), (LD[i][1] * LB[1] - (P[2] - x) mod n) &^ (LD[i][1]^LD[i][2] - 1)) mod n];
end;
end;
if (GEN = []) 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 :

- $\text{Card}(\mathbf{G}_p(n)) = p^{\alpha_p(n)}$
- $\text{Card}(\mathbf{G}_p(pn)) = p^{\alpha_p(n)}$
- $\text{Card}(\mathbf{G}_p(p^\alpha n)) = p^{\alpha_p(n)+1}$  with  $\alpha \geq 2$

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

```
Gene_p := proc(n,p) local LB, LD, i, LFact, GEN, P;
LD := []; LB := []; GEN := [];
if (n mod p^2 = 0) then
GEN := [op(GEN), 1 + n/p];
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
if (LFact[i][1] - 1 mod p = 0) then
```

```

LD := [op(LD), LFact[i]];
end :
end :
for 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);
GEN := [op(GEN), ((LD[i][1] * LB[1] - (P[1] - x) mod n) &^(LD[i][1]^(LD[i][2] - 1)) mod n)];
else
LB := Bezout(LD[i][1], n/(LD[i][1]^LD[i][2]), P[2] - x + 1);
GEN := [op(GEN), (LD[i][1] * LB[1] - (P[2] - x) mod n) &^(LD[i][1]^(LD[i][2] - 1)) mod n)];
end :
end :
else
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
if (LFact[i][1] - 1 mod p = 0) then
LD := [op(LD), LFact[i]];
end :
end :
for 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);
GEN := [op(GEN), ((LD[i][1] * LB[1] - (P[1] - x) mod n) &^(LD[i][1]^(LD[i][2] - 1)) mod n)];
else
LB := Bezout(LD[i][1], n/(LD[i][1]^LD[i][2]), P[2] - x + 1);
GEN := [op(GEN), (LD[i][1] * LB[1] - (P[2] - x) mod n) &^(LD[i][1]^(LD[i][2] - 1)) mod n)];
end :
end :
end :
if (GEN = [ ]) then
GEN := [1];
end;
eval(GEN);
end :

```

#### 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.
- [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, 36:587-592, 1981.
- [10] Frank Garvan. *The Maple Book*. Chapman and Hall/CRC, Boca Raton, FL 2002