

Group of Square Roots of Unity Modulo n

Rochdi Omami, Mohamed Omami and Raouf Ouni

Abstract—Let $n \geq 3$ be an integer and $\mathbf{G}_2(n)$ be the subgroup of square roots of 1 in $(\mathbb{Z}/n\mathbb{Z})^*$. In this paper, we give an algorithm that computes a generating set of this subgroup.

Keywords—Group, modulo, square roots, 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 $(\mathbb{Z}/n\mathbb{Z})$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ the primary decomposition of n , then

$$(\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1}^m (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

for more details on the structure of $(\mathbb{Z}/n\mathbb{Z})^*$ see [1] and [2]. The group $(\mathbb{Z}/n\mathbb{Z})^*$ has several applications, the most important is cryptography, that is RSA cryptosystem (see [5]). The security of the RSA cryptosystem is based on the problem of factoring large numbers and the task of finding e^{th} roots modulo a composite number n whose factors are not known.

In [8], D.Shanks gives a probabilistic algorithm that computes a square root of an integer modulo an odd prime p . There are other algorithms that compute a square root of an integer modulo an integer n (see [7]) and more generally in a finite fields (see [6]).

We denote by $\mathbf{G}_2(n)$ the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ which is formed by the integers x that satisfies $x^2 = 1$, such integers are called square roots of unity modulo n . More precisely $\mathbf{G}_2(n)$ contains the unity and elements of order 2.

Recall that elements of order 2 exists always in $(\mathbb{Z}/n\mathbb{Z})^*$ (-1 has for order 2), therefore $\mathbf{G}_2(n)$ is not a trivial group. Finally remark that all elements of $\mathbf{G}_2(n)$ except the unity has for order 2, so $\mathbf{G}_2(n)$ has an order a power of 2, so we obtain the following result :

Proposition

Let $n \geq 3$ be an integer, then there exists an integer $t \geq 1$ such that :

$$Ord(\mathbf{G}_2(n)) = 2^t.$$

In this article, we will give an algorithm that computes a generating set of $\mathbf{G}_2(n)$ and gives its decomposition into product of cyclic subgroups. Finally this algorithm will be written in MAPLE language.

II. SQUARE ROOTS OF UNITY MODULO N

Let $n \geq 3$ be an integer and $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ its primary decomposition. In this study, we shall distinguish the

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

cases $\alpha = 0$, $\alpha = 1$, $\alpha = 2$ and $\alpha \geq 3$.

Case 1 : $\alpha = 0$

Let $n \geq 3$ be an integer and $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ its primary decomposition. Let x be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $x^2 = 1$, that is n divides $x^2 - 1 = (x - 1)(x + 1)$. We have $(x + 1) - (x - 1) = 2$, therefore $GCD(x - 1, x + 1) \in \{1, 2\}$, so if p_i divides $x - 1$ then $p_i^{\alpha_i}$ divides $x - 1$.

If we note, for example, p_1, p_2, \dots, p_s the primes among the p_i which divide $x - 1$, then x is a solution of this system :

$$\begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} K \\ x + 1 = p_{s+1}^{\alpha_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_m^{\alpha_m} K' \end{cases}$$

It's clear that x is the unique solution of this system modulo n . Conversely, any system of the previous form gives a square root of unity modulo n .

Note that a two different systems of this form give two different solutions, indeed let the systems :

$$\begin{cases} x - 1 = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \\ y - 1 = p_{\rho(1)}^{\alpha_{\rho(1)}} p_{\rho(2)}^{\alpha_{\rho(2)}} \dots p_{\rho(r)}^{\alpha_{\rho(r)}} K'_1 \\ y + 1 = p_{\rho(r+1)}^{\alpha_{\rho(r+1)}} p_{\rho(r+2)}^{\alpha_{\rho(r+2)}} \dots p_{\rho(m)}^{\alpha_{\rho(m)}} K'_2 \end{cases}$$

where σ and ρ are two permutations of the set $\{1, 2, \dots, m\}$, if $x = y$, then the set of prime divisors of $x - 1$ among the p_i is the same of $y - 1$. Therefore the set of prime divisors of $x - 1$ among the p_i is $\{p_{\sigma(1)}, p_{\sigma(2)}, \dots, p_{\sigma(s)}\}$ because $p_{\sigma(s+1)}, p_{\sigma(s+2)}, \dots$ and $p_{\sigma(m)}$ does not divide K_1 , indeed :

$$p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 - p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 = 2.$$

Thus $GCD(K_1, p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}}) \in \{1, 2\}$, so $\{p_{\sigma(1)}, p_{\sigma(2)}, \dots, p_{\sigma(s)}\} = \{p_{\rho(1)}, p_{\rho(2)}, \dots, p_{\rho(r)}\}$, it follows that the two systems are identical.

We conclude that the number of square roots of unity modulo n is equal to the number of partitions of the set $\{1, 2, \dots, m\}$, that is 2^m . Note that the empty subset corresponds to -1 and if all p_i divide $x - 1$, then $x = 1$. So we have proved :

Proposition 2.1: Let $n \geq 3$ be an integer, then

$$Ord(\mathbf{G}_2(n)) = 2^{\omega(n)}$$

where $\omega(n)$ denote the number of distinct prime factors of n .

Now we study the structure of the group $\mathbf{G}_2(n)$. For simplicity throughout this section, we take $n \geq 3$ to be an odd integer

and $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ its primary decomposition. we start with this definition :

Definition 2.1: Let x be a square root of unity modulo n . x is said to be initial if all prime factors of n divide $x - 1$ except only one p_i , we said that x is associated with p_i . And we note :

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K$$

where K is an integer not divisible by p_i and the symbol $p_i^{\alpha_i}$ means that we remove the factor $p_i^{\alpha_i}$.

Note that for any $i \in \{1, 2, \dots, m\}$ there exist only one square root of unity associated with p_i which is the solution of this system:

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

We denote by $\mathbf{G}_2^{p_i}(n)$ the set that contains this solution and the unity, so $\mathbf{G}_2^{p_i}(n)$ is a cyclic subgroup of $\mathbf{G}_2(n)$ of order 2. We have the following theorem :

Theorem 2.1: The map

$$\begin{aligned} \varphi : \mathbf{G}_2^{p_1}(n) \times \mathbf{G}_2^{p_2}(n) \dots \times \mathbf{G}_2^{p_m}(n) &\longrightarrow \mathbf{G}_2(n) \\ (x_1, x_2, \dots, x_m) &\longmapsto x_1.x_2, \dots, x_m \end{aligned}$$

is an isomorphism of groups.

Proof :

It's clear that φ is a morphism of groups, we will show first that φ is injective.

We have $\varphi(x_1, x_2, \dots, x_m) = 1 \iff x_1.x_2, \dots, x_m = 1$. Suppose that there exists an integer i such that $x_i \neq 1$, therefore p_i does not divides $x_i - 1$. Also, for $j \neq i$, p_i divides $x_j - 1$. Then we have:

$$x_i = 1 + K_i \quad \text{and} \quad x_j = 1 + p_i.K_j$$

where p_i does not divides K_i , so

$$\begin{aligned} x_1.x_2, \dots, x_m &= (1 + p_i.K_1).(1 + K_i).(1 + p_i.K_m) \\ &= (1 + p_i.K')(1 + K_i) \\ &= 1 + (p_i.K' + p_i.K'K_i + K_i). \end{aligned}$$

Since p_i does not divides K_i , then p_i does not divides $x_1.x_2, \dots, x_m - 1$, that is absurd. Thus $x_i = 1$ for all $i \in \{1, 2, \dots, m\}$. Hence φ is injective.

Finally, we remark that:

$$Ord(\mathbf{G}_2^{p_1}(n) \times \mathbf{G}_2^{p_2}(n) \dots \times \mathbf{G}_2^{p_m}(n)) = Ord(\mathbf{G}_2(n)) = 2^m$$

so φ is bijective, therefore it's an isomorphism.■

Remark :

The fact that φ is injective is due to the choice of x_i , i.e. the initial square roots of the unity. The previous theorem shows that $\mathbf{G}_2(n)$ is exactly formed by the unity and finished

products without the repetition of the initial square roots of the unity. In other words, if x_i denote the initial square root of the unity associated with p_i , then :

$$\mathbf{G}_2(n) = \left\{ \prod_{i \in I} x_i \quad , \text{ avec } I \subset \{1, 2, \dots, m\} \right\}.$$

With the convention that the unity is the product over empty set.

Remark also that -1 is the product of all x_i , Indeed :

$$\begin{aligned} \prod_{i=1}^m x_i &= \prod_{i=1}^m (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i) \\ &= 1 + \sum_{i=1}^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i + Kn \end{aligned}$$

since $\sum_{i=1}^m p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i$ is not divisible by all p_i

because K_i is not divisible by p_i , we conclude that $\prod_{i=1}^m x_i - 1$

is not divisible by all p_i . It follows $\prod_{i=1}^m x_i = -1$. Finally, we have the following result :

Corollary 2.1: Let x_i be the initial square root of the unity associated with p_i , then :

$$\mathbf{G}_2(n) = \langle x_1, x_2, \dots, x_m \rangle .$$

Now, we give an algorithm written in *MAPLE* that computes the x_i , i.e. a generating set of $\mathbf{G}_2(n)$.

Let us give some explanations. Resuming the system :

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

This system gives the following equation :

$$p_i^{\alpha_i} K' - p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K = 2$$

and Bezout algorithm allows us to compute K and K' and all x_i .

```
Gene_2 := proc(n) local LB, i, LFact, GEN;
GEN := []; LB := [];
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
LB := Bezout(LFact[i][1]^LFact[i][2],
n/(LFact[i][1]^LFact[i][2]), 2);
GEN := [op(GEN), LB[1] *
LFact[i][1]^LFact[i][2] - 1 mod n];
end;
eval(GEN);
end;
```

Algorithm 1.1

An application example :

To find the generators of the group of square root of the unity modulo $11 \times 13 \times 17 \times 19$, we can use the previous algorithm with the command

$$Gene_2(11 * 13 * 17 * 19);$$

We have the following result [33593, 21319, 32605, 4863], that is the list of generators.

Remark :

The *Bezout* function which is used in the previous algorithm is not a *MAPLE* function, but it's a classical algorithm called **Extended Euclidean algorithm**.

Case 2 : $\alpha = 1$

Let $n \geq 3$ be an integer such that its primary decomposition is $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$. Let x be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $x^2 = 1$, that is n divides $x^2 - 1 = (x-1)(x+1)$. We have $(x+1) - (x-1) = 2$, therefore $GCD(x-1, x+1) \in \{1, 2\}$. So, if p_i divides $x-1$, then $p_i^{\alpha_i}$ divides $x-1$. Also 2 divides $(x-1)(x+1)$, thus 2 divides $(x-1)$ or $(x+1)$. Since $(x+1) - (x-1) = 2$, then 2 divides $(x-1)$ and $(x+1)$, so x is a solution of a system of this form :

$$\begin{cases} x - 1 = 2p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \end{cases}$$

where σ is a permutation of the set $\{1, 2, \dots, m\}$. It's clear that x is the only solution modulo n of this system and every system of this form gives a square root of the unity modulo n . We show in the same way as the previous case, that two different systems gives two distinct solutions. Therefore, the number of square roots of the unity modulo n is the number of partitions of the set $\{1, 2, \dots, m\}$, that is 2^m . Hence, we have the following result:

Proposition 2.2: Let $n \geq 3$ be an odd integer, then

$$Ord(\mathbf{G}_2(2n)) = 2^{\omega(n)}$$

where $\omega(n)$ denote the number of distinct prime factors of n .

For simplicity throughout this section we take $n \geq 3$ to be an integer and $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ its primary decomposition. We start the study of $\mathbf{G}_2(n)$ with this definition :

Definition 2.2: Let x be a square root of unity modulo n . x is said to be initial if all the prime factors of n divide $x-1$ except only one p_i , we said that x is associated with p_i . And we note :

$$x - 1 = 2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K$$

where K is an integer that does not divisible by p_i and the symbol $p_i^{\alpha_i}$ means that we remove the factor $p_i^{\alpha_i}$.

We remark that for each $i \in \{1, 2, \dots, m\}$, there exists only one square root of unity associated with p_i which is the solution of the following system :

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

We denote by $\mathbf{G}_2^{p_i}(n)$ the set that contains this solution and the unity, so $\mathbf{G}_2^{p_i}(n)$ is a cyclic subgroup of $\mathbf{G}_2(n)$ of order 2. We have the following theorem :

Theorem 2.2: The map

$$\begin{aligned} \varphi : \mathbf{G}_2^{p_1}(n) \times \mathbf{G}_2^{p_2}(n) \dots \times \mathbf{G}_2^{p_m}(n) &\longrightarrow \mathbf{G}_2(n) \\ (x_1, x_2, \dots, x_m) &\longmapsto x_1 \cdot x_2 \cdot \dots \cdot x_m \end{aligned}$$

is an isomorphism of groups.

Remark :

the previous theorem shows that

$$\mathbf{G}_2(n) = \left\{ \prod_{i \in I} x_i \quad , \text{ avec } I \subset \{1, 2, \dots, m\} \right\}$$

and we have also $\prod_{i=1}^m x_i = -1$.

Corollary 2.2: Let x_i be the initial square root of the unity associated with p_i , then

$$\mathbf{G}_2(n) = \langle x_1, x_2, \dots, x_m \rangle .$$

We finish this section with the fact that the algorithm 1.1 remains valid with integers of the form $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, just replacing $LFact := ifactors(n)[2];$ by $LFact := ifactors(n/2)[2];$, it follows the algorithm 1.2.

Case 3 : $\alpha = 2$

Let $n \geq 3$ be an integer such that its primary decomposition is $n = 4p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$. If all α_i are nuls, then $n = 4$. We know that $(\mathbb{Z}/4\mathbb{Z})^* = \{1, -1\} = \langle -1 \rangle$, therefore, we suppose that at least one of the α_i is not null.

Let x be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $x^2 = 1$, that is n divides $x^2 - 1 = (x-1)(x+1)$. We have $(x+1) - (x-1) = 2$, therefore 2 divides $(x-1)$ and $(x+1)$. But 2 is not an ordinary prime, indeed we have the following equivalence :

$$x \equiv 1[2] \iff x^2 \equiv 1[8].$$

It follows that 8 divide $x^2 - 1 = (x-1)(x+1)$. Since $GCD(x-1, x+1) = 2$, therefore 4 divides $(x-1)$ or $(x+1)$, so x is a solution of one of the following systems :

$$\begin{cases} x - 1 = 4p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \\ x - 1 = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K'_1 \\ x + 1 = 4p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K'_2 \end{cases}$$

where σ is a permutation of the set $\{1, 2, \dots, m\}$. It's clear that each one of these systems has a unique solution modulo n and each system of this form gives a square root of the unity modulo n . We shows also that a two different systems gives two distinct solutions. Therefore, the number of square roots of the unity modulo n is twice the number of partitions of the set $\{1, 2, \dots, m\}$, that is 2^m . Hence, we have the following result:

Proposition 2.3: Let $n \geq 3$ be an odd integer, then

$$Ord(\mathbf{G}_2(4n)) = 2^{\omega(n)+1}$$

where $\omega(n)$ denote the number of distinct prime factors of n .

For simplicity throughout this section we take $n \geq 3$ to be an integer and $n = 4p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ its primary decomposition with at least one of the α_i as being not null. Now we start studying of $\mathbf{G}_2(n)$. Consider the following systems :

$$\begin{cases} x - 1 = 4p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1 \\ x + 1 = K_2 \end{cases} \quad \begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K'_1 \\ x + 1 = 4K'_2 \end{cases}$$

It's clear that 1 is the only solution of the first system. The second system has only solution which is $x_0 = n/2 + 1$. This solution is called second trivial square root of the unity, we denote by $\mathbf{G}_2^0(n)$ the cyclic subgroup which is formed by 1 and x_0 .

Proposition 2.4: Let the systems :

$$\begin{cases} x - 1 = 4p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \end{cases} \quad \begin{cases} x - 1 = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K'_1 \\ x + 1 = 4p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K'_2 \end{cases}$$

if we note by x the solution of the first system and y that of the second. then $y = x_0x$ (and also $x = x_0y$).

Proof :

It's clear that x_0x is a square root of the unity. We have :

$$\begin{aligned} x_0x &= (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K'_1) \\ &\quad (1 + 4p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1) \\ &= 1 + p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} (4K_1 + \\ &\quad p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K'_1) + Kn \end{aligned}$$

Since K'_1 is not divisible by 4 and K_1 is not divisible by $p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots$ and $p_{\sigma(m)}^{\alpha_{\sigma(m)}}$, therefore $x_0x - 1$ is not divisible by 4, $p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots$ and $p_{\sigma(m)}^{\alpha_{\sigma(m)}}$. So x_0x is solution of the second system, i.e. $x_0x = y$. ■

Definition 2.3: Let x be a square root of the unity modulo n . We said that x is of the first category if 4 divides $x - 1$, else we said that x is of the second category.

Remark :

From the definition, we see that a square root of the unity of the first category is a solution of a system of the form :

$$\begin{cases} x - 1 = 4p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \end{cases}$$

also a square root of the unity of the second category is the product of a square root of the unity of the first category by x_0 .

Definition 2.4: Let x be a square root of unity modulo n . x is said to be initial if all prime factors of n divide $x - 1$ except only one p_i , we said that x is associated with p_i . And we note :

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K$$

where K is an integer not divisible by p_i .

Note that there exist two initial square roots of the unity associated with p_i , which are the solutions of the following systems :

$$\begin{cases} x - 1 = 4p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K \\ x + 1 = p_i^{\alpha_i} K' \end{cases} \quad \begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K \\ x + 1 = 4p_i^{\alpha_i} K' \end{cases}$$

We remark that the solution of the first system is of the first category and that of second is of the second category. If we note by x_i the solution of the first system and y_i that of second, then $y_i = x_i x_0$. So the set $\{1, x_0, x_i, y_i\}$ is a subgroup of $\mathbf{G}_2(n)$, which we denote by $\mathbf{G}_2^{p_i}(n)$.

The set formed by 1 and x_i (the initial square root of the unity of the first category associated with p_i) is a cyclic subgroup of order 2, which we denote by $\mathbf{G}_2^{+p_i}(n)$ and we have the following isomorphism :

$$\mathbf{G}_2^{p_i}(n) \simeq \mathbf{G}_2^{+p_i}(n) \times \mathbf{G}_2^0(n).$$

More generally, we have the following result :

Theorem 2.3: The map

$$\begin{aligned} \varphi : \mathbf{G}_2^{+p_1}(n) \times \dots \times \mathbf{G}_2^{+p_m}(n) \times \mathbf{G}_2^0(n) &\longrightarrow \mathbf{G}_2(n) \\ (x_1, \dots, x_m, y) &\longmapsto x_1 \cdot x_2 \cdot \dots \cdot x_m \cdot y \end{aligned}$$

is an isomorphism of groups.

Proof :

It's clear that φ is an morphism of groups. For showing that φ is an isomorphism, we should prove that φ is injective and

we conclude by cardinality.

We have $\varphi(x_1, x_2, \dots, x_m, y) = 1 \iff x_1 \cdot x_2 \cdot \dots \cdot x_m \cdot y = 1$, if we suppose that there exists an integer i such that $x_i \neq 1$, then p_i does not divides $x_i - 1$. Since if $j \neq i$ then p_i divides $x_j - 1$ and p_i divides y . Therefore $x_1 \cdot x_2 \cdot \dots \cdot x_m \cdot y - 1$ is not divisible by p_i , that is absurd. Thus $x_i = 1$ for all i . Finally we have $y = 1$, therefore φ is injective. ■

Remark :

From the previous theorem, we can see that :

$$\mathbf{G}_2(n) = \left\{ \prod_{i \in I} x_i \quad , \text{ avec } I \subset \{1, 2, \dots, m\} \right\} \times \{1, x_0\}$$

and we can also show that $x_0 \prod_{i=1}^m x_i = -1$.

Corollary 2.3: With the previous notations, we have :

$$\mathbf{G}_2(n) = \langle x_0, x_1, x_2, \dots, x_m \rangle .$$

Now we give an algorithm in *MAPLE* that computes the x_i .i.e. a generating set of $\mathbf{G}_2(n)$. x_0 is computed from the relation $x_0 = n/2 + 1$. The other x_i are computed in the same way as the previous case.

```
Gene_2 := proc(n) local LB, i, LFact, GEN;
GEN := [ ]; LB := [ ];
GEN := [op(GEN), n/2 + 1];
LFact := ifactors(n/4)[2];
for i from 1 to nops(LFact) do
LB := Bezout(LFact[i][1]~LFact[i][2],
n/(LFact[i][1]~LFact[i][2]), 2);
GEN := [op(GEN), LB[1] *
LFact[i][1]~LFact[i][2] - 1 mod n];
end do;
eval(GEN);
end do;
```

Algorithm 1.3

An application example :

To find the generators of the group of square root of the unity modulo $4 \times 11 \times 13 \times 17$, we can use the previous algorithm with the command

```
Gene_2(4 * 11 * 13 * 17);
```

We have the following result [4863, 4421, 6733, 3433], that is the list of generators. We note that the first value of the given list is the second trivial square root of the unity.

Case 4 : $\alpha \geq 3$

Let $n \geq 3$ be an integer such that its primary decomposition is $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ with $\alpha \geq 3$.

If all α_i are null, then $n = 2^\alpha$ with $\alpha \geq 3$. Recall that $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic and its cardinal is $n/2$. Let x be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $x^2 = 1$, that is 2^α divides $x^2 - 1 = (x - 1)(x + 1)$. We have $GCD(x - 1, x + 1) = 2$,

therefore $2^{\alpha-1}$ divides $(x - 1)$ or $(x + 1)$. So x is the solution of one of the following systems :

$$\begin{cases} x - 1 = 2^{\alpha-1} K_1 \\ x + 1 = K_2 \end{cases} ; \begin{cases} x - 1 = K'_1 \\ x + 1 = 2^{\alpha-1} K'_2 \end{cases}$$

The first system has two solutions which are 1 and $2^{\alpha-1} + 1$, the second system has two solutions which are -1 and $2^{\alpha-1} - 1$. It's clear that all of the previous solutions are square roots of the unity. We have the following result :

Proposition 2.5: Let $n = 2^\alpha$ with $\alpha \geq 3$, then

$$\mathbf{G}_2(n) = \{1, n/2 - 1, n/2 + 1, -1\}$$

Remark :

We remark that $(n/2 - 1)(n/2 + 1) = (2^{\alpha-1} - 1)(2^{\alpha-1} + 1) = -1$, therefore

$$\mathbf{G}_2(n) = \langle n/2 - 1, n/2 + 1 \rangle .$$

Now we suppose that $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ with $\alpha \geq 3$ and at least one of the α_i is not null. Let x be an element of $(\mathbb{Z}/n\mathbb{Z})^*$ such that $x^2 = 1$. Since $GCD(x - 1, x + 1) = 2$, then x is the solution of one of the following systems :

$$\begin{cases} x - 1 = 2^{\alpha-1} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \end{cases} ; \begin{cases} x - 1 = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K'_1 \\ x + 1 = 2^{\alpha-1} p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K'_2 \end{cases}$$

where σ is a permutation of the set $\{1, 2, \dots, m\}$. It's clear that each of these systems has two solutions modulo n and each system of this form gives a square root of the unity modulo n , because x is odd. We shows also that a two different systems give distinct solutions. Therefore, the number of square roots of the unity modulo n is four times the number of partitions of the set $\{1, 2, \dots, m\}$, that is 2^{m+2} . Hence, we have the following result:

Proposition 2.6: Let $n \geq 3$ be an odd integer, then

$$Ord(\mathbf{G}_2(2^\alpha n)) = 2^{\omega(n)+2} \quad \text{with } \alpha \geq 3.$$

For simplicity throughout this section we take $n \geq 3$ to be an integer and $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ ($\alpha \geq 3$) its primary decomposition with at least one of the α_i is not null. Now we begin to study $\mathbf{G}_2(n)$. Consider the following systems :

$$\begin{cases} x - 1 = 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1 \\ x + 1 = K_2 \end{cases} ; \begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K'_1 \\ x + 1 = 2^{\alpha-1} K'_2 \end{cases}$$

It's clear that the first system has two solutions modulo n and 1 is one of these solutions, we note by y_0 the other solution. Also the second system has two solutions modulo n , denoted

by y_1 and y_2 .

We have :

$$y_0 = 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} + 1 = n/2 + 1$$

and $y_2 = y_1 + 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, therefore $y_2 y_1 = 1 + 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} y_1$. Since y_1 is odd, then $y_2 y_1 = y_0$ and $y_2 = y_1 y_0$.

So, the set $\{1, y_0, y_1, y_2\}$ is a subgroup of $G_2(n)$, which is noted by $G_2^0(n)$. Finally remark that :

$$G_2^0(n) = \{1, y_0\} \times \{1, y_1\}.$$

Definition 2.5: Let x be a square root of the unity modulo n , We said that x is of the first category if 2^α divides $x - 1$, else we said that x is of the second category.

Remark :

Let $x \in G_2^0(n)$, then x is of the first category if and only if $x = 1$.

Definition 2.6: Let x be a square root of unity modulo n . x is said to be initial if all prime factors of n divide $x - 1$ except only one p_i , we said that x is associated with p_i . And we note :

$$x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K.$$

where K is an integer not divisible by p_i .

Note that the initial square roots of the unity associated with p_i are the solutions of the following systems :

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

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

Since each of these system has two solutions modulo n , therefore there exist 4 initial square roots of the unity associated with p_i .

Proposition 2.7: Let the system :

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

If we denote by x_1 and x_2 the solutions of this system, then $x_1 = y_0 \cdot x_2$.

Proof :

We have $x_1 = x_2 + 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, therefore $x_1 \cdot x_2 = 1 + 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} x_2$. Since x_2 is odd, then $x_1 \cdot x_2 = y_0$ it follows that $x_1 = x_2 \cdot y_0$. ■

Remark :

In the same way, we show that the product of the solutions of the following system:

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

is equal to y_0 .

Proposition 2.8: there exists an only initial square root of the unity associated with p_i and of the first category.

Proof :

Indeed, this square root of the unity is the only solution of the system

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

We denote by $G_2^{p_i}(n)$, the cyclic subgroup of order 2 which is formed by 1 and the initial square root of the unity associated with p_i and of the first category.

Proposition 2.9: Let us consider these systems :

$$\begin{cases} x - 1 = 2^{\alpha-1} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1 \\ x + 1 = p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2 \end{cases} \quad (1)$$

$$\begin{cases} x - 1 = p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1' \\ x + 1 = 2^{\alpha-1} p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_2' \end{cases} \quad (2)$$

where σ is a permutation of the set $\{1, 2, \dots, m\}$, then the product of each solution of (1) by y_1 or y_2 is a solution of (2).

Proof :

Let x be a solution of (1). suppose that x is of the first category, that is

$$x = 1 + 2^\alpha p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1.$$

Therefore

$$\begin{aligned} y_1 \cdot x &= (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K) \cdot (1 + 2^\alpha p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_1) \\ &= 1 + p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \dots p_{\sigma(s)}^{\alpha_{\sigma(s)}} (2^\alpha K_1 + p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K) + nK'' \end{aligned}$$

Since $2^{\alpha-1}$ does not divides K and $p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$ does not divide K_1 , then $2^{\alpha-1} p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}}$ does not divide $2^\alpha K_1 + p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\alpha_{\sigma(s+2)}} \dots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K$. Hence $y_1 \cdot x$ is a solution of (2).

If z is the other solution of (1), then $z = y_0 \cdot x$. Thus,

$$z \cdot y_1 = y_0 \cdot (x \cdot y_1).$$

Since $(x.y_1)$ is a solution of (2), therefore $z.y_1$ is also a solution of (2).

Finally, remark that reasoning is also valid to y_2 . ■

If we denote by $G_2^{p_i}(n)$ the set which is formed by the initial square roots of the unity associated with p_i and with the elements of $G_2^0(n)$, then we have the following result:

Corollary 2.4: $G_2^{p_i}(n)$ is a group and we have :

$$G_2^{p_i}(n) \simeq G_2^{+p_i}(n) \times G_2^0(n).$$

Proof :

The initial square roots of the unity associated with p_i are the solutions of the following systems :

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

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

We deduce that $Ord(G_2^{p_i}(n)) = 8$.

From the previous proposition, we know that the solutions of (2) are the product of the solutions of (1) by y_1 . If we note by x a solution of (1), then the solutions of (1) are x and $x.y_0$. So, the initial square roots of the unity associated with p_i are $\{x, x.y_0, x.y_1, x.y_0.y_1\}$, it follows :

$$G_2^{p_i}(n) = \{1, y_0, y_1, y_1.y_0, x, x.y_0, x.y_1, x.y_0.y_1\}.$$

And obviously, we have

$$G_2^{p_i}(n) \simeq G_2^{+p_i}(n) \times G_2^0(n). \blacksquare$$

More generally, we have the following result :

Theorem 2.4: The map

$$\begin{aligned} \varphi : G_2^{+p_1}(n) \times \dots \times G_2^{+p_m}(n) \times G_2^0(n) &\longrightarrow G_2(n) \\ (x_1, \dots, x_m, y) &\longmapsto x_1 \dots x_m y \end{aligned}$$

is an isomorphism of groups.

Proof :

In the same way as the previous theorem, we show that φ is an injective morphism of groups and we conclude by cardinality. ■

Remark :

The group $G_2^0(n)$ is not cyclic, but we have $G_2^0(n) = \{1, y_0\} \times \{1, y_1\}$, thus :

$$G_2(n) \simeq G_2^{+p_1}(n) \times G_2^{+p_2}(n) \dots \times G_2^{+p_m}(n) \times \{1, y_0\} \times \{1, y_1\}.$$

Finally we have the following result :

Corollary 2.5: As it is noted above, we have

$$G_2(n) = \langle y_0, y_1, x_1, x_2, \dots, x_m \rangle .$$

Now we give an algorithm in *MAPLE* that computes x_i, y_0 and y_1 , i.e. a generating set of $G_2(n)$.

The solution y_0 is computed by the formula $y_0 = n/2 + 1$ and y_1 is a solution of the system :

$$\begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K'_1 \\ x + 1 = 2^{\alpha-1} K'_2 \end{cases}$$

we will choose that satisfied this system

$$\begin{cases} x - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1 \\ x + 1 = 2^\alpha K_2 \end{cases} \quad (*)$$

Since (*) implies that $2^\alpha K_2 - (n/2^\alpha) K_1 = 2$, so we get K_2 and K_1 with the Bezout algorithm. Therefore $y_1 = 2^\alpha K_2 - 1 + n/2$.

The other x_i are computed in the same way as the previous case.

```
Gene_2 := proc(n) local a, LB, i, LFact, GEN;
GEN := []; LB := [];
a := ifactors(n)[2][1][2];
GEN := [op(GEN), n/2 + 1];
LB := Bezout(2^a, n/(2^a), 2);
GEN := [op(GEN), LB[1] * 2^a - 1 +
n/2 mod n];
LFact := ifactors(n/(2^a))[2];
for i from 1 to nops(LFact) do
LB := Bezout(LFact[i][1]^LFact[i][2],
n/(LFact[i][1]^LFact[i][2]), 2);
GEN := [op(GEN), LB[1] *
LFact[i][1]^LFact[i][2] - 1 mod n];
end;
eval(GEN);
end;
```

Algorithm 1.4

An application example :

To find the generators of the group of square root of the unity modulo $8 \times 11^2 \times 13$, we can use the previous algorithm with this command :

```
Gene_2(8 * 11^2 * 13);
```

We have the following result [4863, 4421, 6733, 3433], that is the list of generators. We note that the first value of the given list is y_0 , and the second is y_1 .

Remark :

The choice of y_1 allows us to have :

$$y_0.y_1 \prod_{i=1}^m x_i = -1.$$

Indeed, $y_0.y_1$ is the solution of (\star) . Therefore

$$\begin{aligned} y_0.y_1 \prod_{i=1}^m x_i &= (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1) \prod_{i=1}^m (1 + \\ & 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i) \\ &= (1 + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1)(1 + \\ & \sum_{i=1}^m 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i + Kn) \\ &= 1 + [p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_1 + \\ & \sum_{i=1}^m 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i] + Kn \end{aligned}$$

It's clear that the term between the brackets is not divisible by $2^{\alpha-1}, p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_m^{\alpha_m}$. So, $y_0.y_1 \prod_{i=1}^m x_i$ is a solution of this system

$$\begin{cases} x - 1 = K_1 \\ x + 1 = 2^{\alpha-1} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} K_2 \end{cases}$$

Since the solutions of this system are -1 and $(n/2 - 1)$. To conclude, just shows that 2^α divides $y_0.y_1 \prod_{i=1}^m x_i + 1$.

We have

$$y_0.y_1 \prod_{i=1}^m x_i + 1 = (y_0.y_1 + 1) \prod_{i=1}^m x_i - \left(\prod_{i=1}^m x_i - 1 \right)$$

so it's clear that $(y_0.y_1 + 1)$ is divisible by 2^α because $y_0.y_1$ is solution of (\star) , and $\prod_{i=1}^m x_i - 1 = \sum_{i=1}^m 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_m^{\alpha_m} K_i + Kn$, thus

$\prod_{i=1}^m x_i - 1$ is divisible by 2^α it follow that 2^α divides $y_0.y_1 \prod_{i=1}^m x_i + 1$. ■

Now we give an explicit formula for y_1 in special cases.

Proposition 2.10: Let n be an integer of the form $8b$, with b is an odd positive integer, then :

- $y_1 = n/4 + 1$ if $b \equiv 1[4]$.
- $y_1 = 3n/4 + 1$ if $b \equiv 3[4]$.

Proof :

• On the first hand, we have $(n/4 + 1)^2 = (2p + 1)^2 = 1 + 4p(p + 1)$, and since 2 divides $p + 1$, then n divides $4p(p + 1)$. Hence $(n/4 + 1)^2 = 1$.

On the other hand, $(n/4 + 1) - 1 = n/4$ is divisible by all the prime factors of n . Since $(n/4 + 1) + 1 = 2(p + 1)$ and $b \equiv 1[4]$, then $p + 1$ is divisible by 2 and not by 4 . Thus $(n/4 + 1) + 1$ is divisible by 4 and not by 8 , hence the result.

• We will show this point in the same way. ■

Proposition 2.11: Let n be an integer of the form $2^\alpha b$ with b is an odd positive integer and $\alpha \geq 3$. if $b \equiv 1[2^{\alpha-1}]$, the

solution of (\star) is :

$$y_2 = \frac{(2^{\alpha-1} - 1)n}{2^{\alpha-1}} + 1.$$

Therefore

$$y_1 = \frac{(2^{\alpha-2} - 1)n}{2^{\alpha-1}} + 1.$$

Proof :

We have

$$\begin{aligned} y_2^2 &= (2b(2^{\alpha-1} - 1) + 1)^2 \\ &= 1 + 4b^2(2^{\alpha-1} - 1)^2 + 4b(2^{\alpha-1} - 1) \\ &= 1 + 4b(2^\alpha b(2^{\alpha-2} - 1) + 2^{\alpha-1} + b - 1). \end{aligned}$$

Since $2^{\alpha-1}$ divides $b - 1$, then n divides $4b(2^\alpha b(2^{\alpha-2} - 1) + 2^{\alpha-1} + b - 1)$, therefore $y_2^2 = 1$.

It's clear that all the prime factors of n divide $y_2 - 1$. On the other hand, $y_2 + 1 = 2b(2^{\alpha-1} - 1) + 2 = 2^\alpha b - 2(b - 1)$, then 2^α divides $y_2 + 1$. So, y_2 is solution of (\star) .

We know that $y_1 = y_2 - n/2$, it follows the expression of y_1 . ■

III. CONCLUSION

For the cardinal of $G_2(n)$, we have the following theorem :

Theorem 3.1: Let $n \geq 3$ be an odd integer, then :

- $Ord(G_2(n)) = 2^{\omega(n)}$
- $Ord(G_2(2n)) = 2^{\omega(n)}$
- $Ord(G_2(4n)) = 2^{\omega(n)+1}$
- $Ord(G_2(2^\alpha n)) = 2^{\omega(n)+2}$ with $\alpha \geq 3$

where $\omega(n)$ is the number of distinct prime factors of n .

Now we give an algorithm that computes a generating set for $G_2(n)$, where n is an integer.

```

Gene_2 := proc(n) local a, LB, i, LFact, GEN;
GEN := []; LB := [];
if(n mod 2 = 1) then
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
LB := Bezout(LFact[i][1]^LFact[i][2],
n/(LFact[i][1]^LFact[i][2]), 2);
GEN := [op(GEN), LB[1] *
LFact[i][1]^LFact[i][2] - 1 mod n];
end;
eval(GEN);
else
a := ifactors(n)[2][1][2];
if a = 1 then
LFact := ifactors(n)[2];
for i from 1 to nops(LFact) do
LB := Bezout(LFact[i][1]^LFact[i][2],
n/(LFact[i][1]^LFact[i][2]), 2);
GEN := [op(GEN), LB[1] *
LFact[i][1]^LFact[i][2] - 1 mod n];
end;
eval(GEN);
elif a = 2 then
GEN := [op(GEN), n/2 + 1];

```



```

LFact := ifactors(n/4)[2];
for i from 1 to nops(LFact) do
  LB := Bezout(LFact[i][1]^LFact[i][2],
  n/(LFact[i][1]^LFact[i][2]), 2);
  GEN := [op(GEN), LB[1] *
  LFact[i][1]^LFact[i][2] - 1 mod n];
end :
eval(GEN);
else
  GEN := [op(GEN), n/2 + 1];
  LB := Bezout(2^a, n/(2^a), 2);
  GEN := [op(GEN), LB[1] * 2^a - 1
  + n/2 mod n];
  LFact := ifactors(n/(2^a))[2];
  for i from 1 to nops(LFact) do
    LB := Bezout(LFact[i][1]^LFact[i][2],
    n/(LFact[i][1]^LFact[i][2]), 2);
    GEN := [op(GEN), LB[1] *
    LFact[i][1]^LFact[i][2] - 1 mod n];
  end :
  eval(GEN);
end :
end :
end :

```

Algorithm 1.5

Complexity of the algorithm :

It's clear that the complexity of the **Algorithm 1.5** is the same as the **Algorithm 1.1**. Recall that the number of distinct prime factors of a number n is denoted $\omega(n)$. We know that $\omega(n) = O(\ln(\ln n))$ (see [9] and [10]), and the complexity of the **Extended Euclidean algorithm** is $O(\ln^2 n)$ (see [3] and [4]). Therefore the complexity of **Algorithm 1.1** without the factorization is $O(\ln(\ln n) \ln^2 n)$.

REFERENCES

- [1] J-P. Serre, *A Course in Arithmetic*. Graduate Texts in Mathematics, Springer, 1996
- [2] S. Lang, *Undergraduate Algebra*, 2nd ed. UTM. Springer Verlag, 1990
- [3] H. Cohen, *A course in computational algebraic number theory*. Springer-Verlag, 1993.
- [4] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2005.
- [5] David M. Bressoud, *Factorization and Primality Testing*. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1989.
- [6] E. Bach, *A note on square roots in finite fields*. IEEE Trans. Inform. Theory, 36(6):1494–1498, 1990. Eric
- [7] E. Bach and K. Huber, *Note on taking square-roots modulo N* . IEEE Transactions on Information Theory, 45(2):807809, 1999.
- [8] D. Shanks, *Five number-theoretic algorithms*. In Proc. Second Munitoba Conf. Numerical Math. 51-70, 1972.
- [9] Hardy, G. H, *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*, 3rd ed. New York: Chelsea, 1999. G. H.
- [10] Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed. Oxford University Press, 1960.