# 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 $1 \mathrm{in}(\mathbb{Z} / n \mathbb{Z})^{*}$. 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 $n=$ $p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ the primary decomposition of $n$, then

$$
(\mathbb{Z} / n \mathbb{Z})^{*}=\prod_{i=1}^{m}\left(\mathbb{Z} / p_{i}^{\alpha_{i}} \mathbb{Z}\right)^{*}
$$

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 $e^{t h}$ 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 :

$$
\operatorname{Ord}\left(\mathbf{G}_{2}(n)\right)=2^{t} .
$$

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 $n=2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ 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 $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ 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 $G C D(x-1, x+1) \in\{1,2\}$, so if $p_{i}$ divides $x-1$ then $p_{i}^{\alpha_{i}}$ divides $x-1$.
If we note, for example, $p_{1}, p_{2}, \ldots, p_{s}$ the primes among the $p_{i}$ which divide $x-1$, then $x$ is a solution of this system :

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

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 :

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right. \\
& \left\{\begin{array}{l}
y-1=p_{\rho(1)}^{\alpha_{\tau(1)}} p_{\rho(2)}^{\alpha_{\rho(2)}} \ldots p_{\rho(r)}^{\alpha_{\rho(r)}} K_{1}^{\prime} \\
y+1=p_{\rho(r+1)}^{\alpha_{\rho(r+1)}} p_{\rho(r+2)}^{\rho(r+2)} \ldots p_{\rho(m)}^{\alpha_{\rho(m)}} K_{2}^{\prime}
\end{array}\right.
\end{aligned}
$$

where $\sigma$ and $\rho$ are two permutations of the set $\{1,2, . ., m\}$, 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 $\left\{p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(s)}\right\}$ because $p_{\sigma(s+1)}, p_{\sigma(s+2)}, \ldots$ and $p_{\sigma(m)}$ does not divide $K_{1}$, indeed :
$p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}-p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}=2$.
Thus $G C D\left(K_{1}, p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}}\right) \in\{1,2\}$, so $\left\{p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(s)}\right\}=\left\{p_{\rho(1)}, p_{\rho(2)}, \ldots, p_{\rho(r)}\right\}$, 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 $\{1,2, . ., m\}$, 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

$$
\operatorname{Ord}\left(\mathbf{G}_{2}(n)\right)=2^{\omega(n)}
$$

where $\omega(n)$ denote the number of distinct prime factors of $n$.
Now we study the structure of the group $G_{2}(n)$. For simplicity throughout this section, we take $n \geq 3$ to be an odd integer
and $n=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ 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 :

$$
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{v_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K . ~}{\text {. }}
$$

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 $i \in\{1,2, . ., m\}$ there exist only one square root of unity associated with $p_{i}$ which is the solution of this system:

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

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

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

is an isomorphism of groups.

## Proof :

It's clear that $\varphi$ is a morphism of groups, we will show first that $\varphi$ is injective.
We have $\varphi\left(x_{1}, x_{2}, \ldots, x_{m}\right)=1 \Longleftrightarrow x_{1} \cdot x_{2}, \ldots x_{m}=1$. 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:

$$
x_{i}=1+K_{i} \quad \text { and } \quad x_{j}=1+p_{i} \cdot K_{j}
$$

where $p_{i}$ does not divides $K_{i}$, so

$$
\begin{aligned}
x_{1} \cdot x_{2}, \ldots x_{m} & =\left(1+p_{i} \cdot K_{1}\right) . .\left(1+K_{i}\right) . .\left(1+p_{i} \cdot K_{m}\right) \\
& =\left(1+p_{i} K^{\prime}\right)\left(1+K_{i}\right) \\
& =1+\left(p_{i} K^{\prime}+p_{i} K^{\prime} K_{i}+K_{i}\right) .
\end{aligned}
$$

Since $p_{i}$ does not divides $K_{i}$, then $p_{i}$ does not divides $x_{1} \cdot x_{2}, \ldots x_{m}-1$, that is absurd. Thus $x_{i}=1$ for all $i \in\{1,2, . ., m\}$. Hence $\varphi$ is injective.
Finally, we remark that:
$\operatorname{Ord}\left(\mathbf{G}_{2}^{p_{1}}(n) \times \mathbf{G}_{2}^{p_{2}}(n) \ldots \times \mathbf{G}_{2}^{p_{m}}(n)\right)=\operatorname{Ord}\left(\mathbf{G}_{2}(n)\right)=2^{m}$
so $\varphi$ is bijective, therefore it's an isomorphism.

## Remark :

The fact that $\varphi$ 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 :

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

With the convention that the unity is the product over empty set.
Remark also that -1 is the product of all $x_{i}$, Indeed :

$$
\begin{aligned}
\prod_{i=1}^{m} x_{i} & =\prod_{i=1}^{m}\left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\ldots} p_{m}^{\alpha_{m}} K_{i}\right) \\
& =1+\sum_{i=1}^{m} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{v_{i}^{\alpha_{i}}} \ldots p_{m}^{\alpha_{m}} K_{i}+K n
\end{aligned}
$$

since $\sum_{i=1}^{m} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K_{i}$ 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 :

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

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 :

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

This system gives the following equation :

$$
p_{i}^{\alpha_{i}} K^{\prime}-p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\vee \alpha_{i}} \ldots p_{m}^{\alpha_{m}} K=2
$$

and Bezout algorithm allows us to compute $K$ and $K^{\prime}$ and all $x_{i}$.

Gene_2 $:=\operatorname{proc}(n) \quad$ local LB,, LFFact, GEN;
GEN := [ ]; LB := [];
LFact := ifactors(n)[2];
for $i$ from 1 to nops(LFact) do
$L B:=\operatorname{Bezout}\left(\operatorname{LFact}[i][1]^{\wedge} \operatorname{LFact}[i][2]\right.$,
$n /($ LFact $[i][1] \sim$ LFact $[i][2]), 2)$;
$G E N:=[o p(G E N), L B[1] *$
LFact $[i][1]^{\wedge}$ LFact $\left.[i][2]-1 \bmod n\right]$;
end :
$\operatorname{eval}(G E N)$;
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

$$
\text { Gene_2(11 * } 13 * 17 * 19) \text {; }
$$

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 $n=2 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$. 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 $G C D(x-1, x+1) \in\{1,2\}$. 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 :

$$
\left\{\begin{array}{l}
x-1=2 p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right.
$$

where $\sigma$ is a permutation of the set $\{1,2, \ldots, m\}$. 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 $\{1,2, . ., m\}$, that is $2^{m}$. Hence, we have the following result:

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

$$
\operatorname{Ord}\left(\mathbf{G}_{2}(2 n)\right)=2^{\omega(n)}
$$

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 $n=2 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ 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 :

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

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 $i \in\{1,2, . ., m\}$, there exists only one square root of unity associated with $p_{i}$ which is the solution of the following system :

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

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

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

is an isomorphism of groups.

## Remark :

the previous theorem shows that

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

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

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

We finish this section with the fact that the algorithm 1.1 remains valid with integers of the form $n=2 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$, just replacing LFact $:=\quad$ 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 $n=4 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$. If all $\alpha_{i}$ are nuls, then $n=4$. We know that $(\mathbb{Z} / 4 \mathbb{Z})^{*}=\{1,-1\}=<-1>$, therefore, we suppose that at least one of the $\alpha_{i}$ 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 :

$$
x \equiv 1[2] \Longleftrightarrow x^{2} \equiv 1[8] .
$$

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

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=4 p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}^{\prime} \\
x+1=4 p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}^{\prime}}
\end{array}\right.
\end{aligned}
$$

where $\sigma$ is a permutation of the set $\{1,2, . ., m\}$. 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 $\{1,2, \ldots, m\}$, that is $2^{m}$. Hence, we have the following result:

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

$$
\operatorname{Ord}\left(\mathbf{G}_{2}(4 n)\right)=2^{\omega(n)+1}
$$

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 $n=4 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ its primary decomposition with at least one of the $\alpha_{i}$ as being not null. Now we start studying of $\mathbf{G}_{2}(n)$. Consider the following systems :

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=4 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1} \\
x+1=K_{2}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}^{\prime} \\
x+1=4 K_{2}^{\prime}
\end{array}\right.
\end{aligned}
$$

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 :

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=4 p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}^{\prime} \\
x+1=4 p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}^{\prime}
\end{array}\right.
\end{aligned}
$$

if we note by $x$ the solution of the first system and $y$ that of the second. then $y=x_{0} x$ (and also $x=x_{0} y$ ).

## Proof:

It's clear that $x_{0} x$ is a square root of the unity. We have :

$$
\begin{aligned}
x_{0} x= & \left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}^{\prime}\right) \\
& \left(1+4 p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}\right) \\
= & 1+p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}}\left(4 K_{1}+\right. \\
& \left.p_{\sigma(s+1)}^{\alpha_{\sigma(s) 1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{1}^{\prime}\right)+K n
\end{aligned}
$$

Since $K_{1}^{\prime}$ is not divisible by 4 and $K_{1}$ is not divisible by $p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}}, p_{\sigma(s+2)}^{\sigma(s+2)} \ldots$ and $p_{\sigma(m)}^{\alpha_{\sigma(m)},}$, therefore $x_{0} x-1$ is not divisible by $4, p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}}, p_{\sigma(s+2)}^{\sigma(s+2)} \cdots$ and $p_{\sigma(m)}^{\alpha_{\sigma(m)}}$. So $x_{0} x$ is solution of the second system,i.e. $x_{0} x=y$

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 :

$$
\left\{\begin{array}{l}
x-1=4 p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right.
$$

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 :

$$
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots{\stackrel{\vee}{p_{i}}}_{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K
$$

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 :

$$
\begin{aligned}
& \left\{\begin{array}{l}
x-1=4 p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{m}^{\alpha_{m}} K \\
x+1=p_{i}^{\alpha_{i}} K^{\prime}
\end{array}\right. \\
& \left\{\begin{array}{l}
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K \\
x+1=4 p_{i}^{\alpha_{i}} K^{\prime}
\end{array}\right.
\end{aligned}
$$

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 $\left\{1, x_{0}, x_{i}, y_{i}\right\}$ 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 $\mathbf{G}_{2}^{+}(n)$ and we have the following isomorphism :

$$
\mathbf{G}_{2}^{p_{i}}(n) \simeq{\stackrel{+}{p_{i}}}_{2}(n) \times \mathbf{G}_{2}^{0}(n)
$$

More generally, we have the following result :
Theorem 2.3: The map

$$
\begin{aligned}
{\stackrel{+}{\mathbf{p}_{1}}}_{p_{2}}(n) \times \ldots \times \mathbf{G}_{2}^{+}(n) \times \mathbf{G}_{2}^{0}(n) & \longrightarrow \mathbf{G}_{2}(n) \\
\left(x_{1}, \ldots, x_{m}, y\right) & \longmapsto x_{1} \cdot x_{2}, \ldots x_{m} . y
\end{aligned}
$$

is an isomorphism of groups.

## Proof:

It's clear that $\varphi$ is an morphism of groups. For showing that $\varphi$ is an isomorphism, we should prove that $\varphi$ is injective and
we conclude by cardinality.
We have $\varphi\left(x_{1}, x_{2}, \ldots, x_{m}, y\right)=1 \Longleftrightarrow x_{1} \cdot x_{2}, \ldots x_{m} \cdot y=1$, 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 $x_{1} \cdot x_{2}, \ldots x_{m} . y-1$ is not divisible by $p_{i}$, that is absurd. Thus $x_{i}=1$ for all $i$. Finally we have $y=1$, therefore $\varphi$ is injective.

## Remark :

From the previous theorem, we can see that :

$$
\mathbf{G}_{2}(n)=\left\{\prod_{i \in I} x_{i} \quad, \text { avec } I \subset\{1,2, . ., m\}\right\} \times\left\{1, x_{0}\right\}
$$

and we can also show that $x_{0} \prod_{i=1}^{m} x_{i}=-1$.
Corollary 2.3: With the previous notations, we have :

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

Now we give an algorithm in MAPLE that computes the $x_{i}$ 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]^}\mathrm{ LFact[i][2]), 2);
GEN := [op(GEN),LB[1]*
LFact[i][1]`LFact[i][2]-1 mod n];
end:
eval(GEN);
end:
```

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 $n=2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $\alpha \geq 3$.
If all $\alpha_{i}$ 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 $2^{\alpha}$ divides $x^{2}-1=(x-1)(x+1)$. We have $G C D(x-1, x+1)=2$,
therefore $2^{\alpha-1}$ divides $(x-1)$ or $(x+1)$. So $x$ is the solution of one of the following systems :

$$
\left\{\begin{array}{l}
x-1=2^{\alpha-1} K_{1} \\
x+1=K_{2}
\end{array} ;\left\{\begin{array}{l}
x-1=K_{1}^{\prime} \\
x+1=2^{\alpha-1} K_{2}^{\prime}
\end{array}\right.\right.
$$

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 $(n / 2-1)(n / 2+1)=\left(2^{\alpha-1}-1\right)\left(2^{\alpha-1}+1\right)=$ -1 , therefore

$$
\mathbf{G}_{2}(n)=<n / 2-1, n / 2+1>.
$$

Now we suppose that $n=2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$ with $\alpha \geq 3$ and at least one of the $\alpha_{i}$ is not null. Let $x$ be an element of $(\mathbb{Z} / n \mathbb{Z})^{*}$ such that $x^{2}=1$. Since $G C D(x-1, x+1)=2$, then $x$ is the solution of one of the following systems :

$$
\begin{gathered}
\left\{\begin{array}{c}
x-1=2^{\alpha-1} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}
\end{array}\right. \\
\left\{\begin{array}{l}
x-1=p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}^{\prime} \\
x+1=2^{\alpha-1} p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}^{\prime}
\end{array}\right.
\end{gathered}
$$

where $\sigma$ is a permutation of the set $\{1,2, . ., m\}$. 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 $\{1,2, . ., m\}$, that is $2^{m+2}$. Hence, we have the following result:

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

$$
\operatorname{Ord}\left(\mathbf{G}_{2}\left(2^{\alpha} n\right)\right)=2^{\omega(n)+2} \quad \text { with } \alpha \geq 3
$$

For simplicity throughout this section we take $n \geq 3$ to be an integer and $n=2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}(\alpha \geq 3)$ its primary decomposition with at least one of the $\alpha_{i}$ is not null. Now we begin to study $\mathbf{G}_{2}(n)$. Consider the following systems:

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

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:

$$
y_{0}=2^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}+1=n / 2+1
$$

and $y_{2}=y_{1}+2^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$, therefore $y_{2} y_{1}=1+$ $2^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} y_{1}$. Since $y_{1}$ is odd, then $y_{2} y_{1}=y_{0}$ and $y_{2}=y_{1} y_{0}$.
So, the set $\left\{1, y_{0}, y_{1}, y_{2}\right\}$ is a subgroup of $\mathbf{G}_{2}(n)$, which is noted by $\mathbf{G}_{2}^{0}(n)$. Finally remark that :

$$
\mathbf{G}_{2}^{0}(n)=\left\{1, y_{0}\right\} \times\left\{1, y_{1}\right\}
$$

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

Remark :
Let $x \in \mathbf{G}_{2}^{0}(n)$, 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:

$$
x-1=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee p_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K . . . . ~}{\text {. }}
$$

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 :

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

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 :

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

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 $x_{1}=x_{2}+2^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}}$, therefore $x_{1} \cdot x_{2}=1+2^{\alpha-1} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} x_{2}$. 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:

$$
\left\{\begin{aligned}
x-1 & =p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{\vee}{p_{i}^{\alpha_{i}}} \ldots p_{m}^{\alpha_{m}} K \\
x+1 & =2^{\alpha-1} p_{i}^{\alpha_{i}} K^{\prime}
\end{aligned}\right.
$$

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

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

We denote by ${\stackrel{+}{G_{2}}}_{p_{i}}(n)$, 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 :

$$
\begin{gather*}
\left\{\begin{array}{c}
x-1=2^{\alpha-1} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1} \\
x+1=p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}}
\end{array}\right.  \tag{1}\\
\left\{\begin{array}{l}
x-1=p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}^{\prime} \\
x+1=2^{\alpha-1} p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K_{2}^{\prime}
\end{array}\right. \tag{2}
\end{gather*}
$$

where $\sigma$ is a permutation of the set $\{1,2, . ., m\}$, 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

$$
x=1+2^{\alpha} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}
$$

Therefore

$$
\begin{aligned}
y_{1} \cdot x= & \left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K\right) \cdot(1+ \\
& \left.2^{\alpha_{0}} p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}} K_{1}\right) \\
= & 1+p_{\sigma(1)}^{\alpha_{\sigma(1)}} p_{\sigma(2)}^{\alpha_{\sigma(2)}} \ldots p_{\sigma(s)}^{\alpha_{\sigma(s)}}\left(2^{\alpha} K_{1}+\right. \\
& p_{\sigma(s+1)}^{\left.\alpha_{\sigma(s+1)} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K\right)+n K^{\prime \prime} .}
\end{aligned}
$$

 then $2^{\alpha-1}, p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}}, p_{\sigma(s+2)}^{\sigma(s+2)} \ldots$ et $p_{\sigma(m)}^{\alpha_{\sigma(m)}}$ does not divide $2^{\alpha} K_{1}+p_{\sigma(s+1)}^{\alpha_{\sigma(s+1)}^{\alpha(s+1)}} p_{\sigma(s+2)}^{\sigma(s+2)} \ldots p_{\sigma(m)}^{\alpha_{\sigma(m)}} K$. 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,

$$
z \cdot y_{1}=y_{0} \cdot\left(x \cdot y_{1}\right)
$$

Since $\left(x . y_{1}\right)$ 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 $\mathbf{G}_{2}^{p_{i}}(n)$ the set which is formed by the initial square roots of the unity associated with $p_{i}$ and with the elements of $\mathbf{G}_{2}^{0}(n)$, then we have the following result:

Corollary 2.4: $\mathbf{G}_{2}^{p_{i}}(n)$ is a group and we have :

$$
\mathbf{G}_{2}^{p_{i}}(n) \simeq \mathbf{G}_{2}^{p_{i}}(n) \times \mathbf{G}_{2}^{0}(n) .
$$

Proof:
The initial square roots of the unity associated with $p_{i}$ are the solutions of the following systems :

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

We deduce that $\operatorname{Ord}\left(\mathbf{G}_{2}^{p_{i}}(n)\right)=8$.
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 $\left\{x, x . y_{0}, x . y_{1}, x . y_{0} . y_{1}\right\}$, it follows :

$$
\mathbf{G}_{2}^{p_{i}}(n)=\left\{1, y_{0}, y_{1}, y_{1} \cdot y_{0}, x, x . y_{0}, x \cdot y_{1}, x . y_{0} \cdot y_{1}\right\} .
$$

And obviously, we have

$$
\mathbf{G}_{2}^{p_{i}}(n) \simeq \mathbf{G}_{2}^{p_{i}}(n) \times \mathbf{G}_{2}^{0}(n)
$$

More generally, we have the following result :
Theorem 2.4: The map

$$
\begin{aligned}
& \stackrel{+}{p_{1}}(n) \times \ldots \times{\stackrel{\mathbf{G}_{2}^{p_{2}}}{p_{m}}(n) \times \mathbf{G}_{2}^{0}(n)}^{\mathbf{G}_{2}}(n) \times \mathbf{G}_{2}(n) \\
&\left(x_{1}, \ldots, x_{m}, y\right) \longmapsto \\
& x_{1}, \ldots x_{m} \cdot y
\end{aligned}
$$

is an isomorphism of groups.

## Proof :

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

## Remark :

The group $\mathbf{G}_{2}^{0}(n)$ is not cyclic, but we have $\mathbf{G}_{2}^{0}(n)=\left\{1, y_{0}\right\} \times\left\{1, y_{1}\right\}$, thus :

Finally we have the following result :
Corollary 2.5: As it is noted above, we have

$$
\mathbf{G}_{2}(n)=<y_{0}, y_{1}, x_{1}, x_{2}, \ldots, x_{m}>.
$$

Now we give an algorithm in MAPLE that computes $x_{i}, y_{0}$ and $y_{1}$,i.e. a generating set of $\mathbf{G}_{2}(n)$.
The solution $y_{0}$ is computed by the formula $y_{0}=n / 2+1$ and $y_{1}$ is a solution of the system :

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

we will choose that satisfied this system

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

Since $(\star)$ implies that $2^{\alpha} K_{2}-\left(n / 2^{\alpha}\right) K_{1}=2$, 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 :

$$
y_{0} \cdot y_{1} \prod_{i=1}^{m} x_{i}=-1
$$

ISSN: 2517-9934
Vol:3, No:7, 2009

Indeed, $y_{0} . y_{1}$ is the solution of $(\star)$. Therefore

$$
\begin{aligned}
y_{0} \cdot y_{1} \prod_{i=1}^{m} x_{i}= & \left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}\right) \prod_{i=1}^{m}(1+ \\
& \left.2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K_{i}\right) \\
= & \left(1+p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}\right)(1+ \\
& \left.\sum_{i=1}^{m} 2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots \stackrel{p}{i}_{\alpha_{i}}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K_{i}+K n\right) \\
= & 1+\left[p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{m}^{\alpha_{m}} K_{1}+\right. \\
& \left.\sum_{i=1}^{m} 2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K_{i}\right]+\mathbf{K} n
\end{aligned}
$$

It's clear that the term between the brackets is not divisible by $2^{\alpha-1}, p_{1}^{\alpha_{1}}, p_{2}^{\alpha_{2}} \ldots, p_{m}^{\alpha_{m}}$. So, $y_{0} \cdot y_{1} \prod_{i=1}^{m} x_{i}$ is a solution of this system

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

Since the solutions of this system are -1 and $(n / 2-1)$. To conclude, just shows that $2^{\alpha}$ divides $y_{0} . y_{1} \prod_{i=1}^{m} x_{i}+1$.
We have

$$
y_{0} \cdot y_{1} \prod_{i=1}^{m} x_{i}+1=\left(y_{0} \cdot y_{1}+1\right) \prod_{i=1}^{m} x_{i}-\left(\prod_{i=1}^{m} x_{i}-1\right)
$$

so it's clear that $\left(y_{0} \cdot y_{1}+1\right)$ is divisible by $2^{\alpha}$ because $y_{0} \cdot y_{1}$ is solution of ( $\star$ ), and $\prod_{i=1}^{m} x_{i}-1=\sum_{i=1}^{m} 2^{\alpha} p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \ldots p_{i}^{\alpha_{i}} \ldots p_{m}^{\alpha_{m}} K_{i}+K n, \quad$ thus $\prod_{i=1}^{m} x_{i}-1$ is divisible by $2^{\alpha}$ it follow that $2^{\alpha}$ divides $y_{0} \cdot y_{1} \prod_{i=1}^{m} x_{i}+1$.
Now we give an explicit formula for $y_{1}$ in special cases.
Proposition 2.10: Let $n$ be an integer of the form $8 b$, with $b$ is an odd positive integer, then :

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


## Proof:

- On the first hand, we have $(n / 4+1)^{2}=(2 p+1)^{2}=$ $1+4 p(p+1)$, and since 2 divides $p+1$, then $n$ divides $4 p(p+1)$. 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 $b \equiv 1\left[2^{\alpha-1}\right]$, the
solution of $(\star)$ is :

$$
y_{2}=\frac{\left(2^{\alpha-1}-1\right) n}{2^{\alpha-1}}+1
$$

Therefore

$$
y_{1}=\frac{\left(2^{\alpha-2}-1\right) n}{2^{\alpha-1}}+1
$$

Proof:
We have

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

Since $2^{\alpha-1}$ divides $b-1$, then $n$ divides $4 b\left(2^{\alpha} b\left(2^{\alpha-2}-1\right)+\right.$ $2^{\alpha-1}+b-1$ ), therefore $y_{2}^{2}=1$.
It's clear that all the prime factors of $n$ divide $y_{2}-1$. On the other hand, $y_{2}+1=2 b\left(2^{\alpha-1}-1\right)+2=2^{\alpha} b-2(b-1)$, then $2^{\alpha}$ 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 $\mathbf{G}_{2}(n)$, we have the following theorem :
Theorem 3.1: Let $n \geq 3$ be an odd integer, then :

- $\operatorname{Ord}\left(\mathbf{G}_{2}(n)\right)=2^{\omega(n)}$
- $\operatorname{Ord}\left(\mathbf{G}_{2}(2 n)\right)=2^{\omega(n)}$
- $\operatorname{Ord}\left(\mathbf{G}_{2}(4 n)\right)=2^{\omega(n)+1}$
- $\operatorname{Ord}\left(\mathbf{G}_{2}\left(2^{\alpha} n\right)\right)=2^{\omega(n)+2}$ 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 $\mathbf{G}_{2}(n)$, where $n$ is an integer.

Gene_2 := proc(n) local a,LB, i,LFact,GEN;
$G E N:=[] ; L B:=[] ;$
$i f(n \bmod 2=1)$ then
LFact :=ifactors(n)[2];
for $i$ from 1 to nops(LFact) do
$L B:=\operatorname{Bezout}\left(\operatorname{LFact}[i][1]{ }^{\wedge}\right.$ LFact $[i][2]$,
$n /($ LFact $[i][1] \sim$ LFact $[i][2]), 2)$;
$G E N:=[o p(G E N), L B[1] *$
LFact $[i][1]^{\wedge}$ LFact $\left.[i][2]-1 \bmod n\right]$;
end :
$\operatorname{eval}(G E N)$;
else
$a:=$ ifactors $(n)[2][1][2] ;$
if $a=1$ then
LFact :=ifactors(n)[2];
for $i$ from 1 to nops(LFact) do
$L B:=\operatorname{Bezout}\left(\operatorname{LFact}[i][1]^{\wedge} \operatorname{LFact}[i][2]\right.$,
$n /($ LFact $[i][1] \sim$ LFact $[i][2]), 2)$;
$G E N:=[o p(G E N), L B[1] *$
LFact $\left.[i][1]^{\wedge} L F a c t[i][2]-1 \bmod n\right]$;
end:
$\operatorname{eval}(G E N)$;
elifa $=2$ then
$G E N:=[o p(G E N), n / 2+1] ;$

LFact :=ifactors(n/4)[2];
for $i$ from 1 to nops (LFact) do
$L B:=\operatorname{Bezout}\left(\operatorname{LFact}[i][1]^{\wedge} \operatorname{LFact}[i][2]\right.$,
$n /($ LFact $[i][1] \sim$ LFact $[i][2]), 2)$;
$G E N:=[o p(G E N), L B[1] *$
LFact $[i][1]^{\wedge}$ LFact $\left.[i][2]-1 \bmod n\right]$;
end:
$\operatorname{eval}(G E N)$;
else
$G E N:=[o p(G E N), n / 2+1] ;$
$L B:=\operatorname{Bezout}(2$ a $a, n /(2$ 2a), 2);
$G E N:=[o p(G E N), L B[1] * 2$ - $a-1$
$+n / 2 \bmod n]$;
LFact $:=$ ifactors $\left(n /\left(2^{\wedge} a\right)\right)[2]$;
for $i$ from 1 to nops(LFact) do
$L B:=\operatorname{Bezout}\left(\operatorname{LFact}[i][1]^{\wedge} \operatorname{LFact}[i][2]\right.$,
$n /($ LFact $[i][1] \sim$ LFact $[i][2]), 2)$;
$G E N:=[o p(G E N), L B[1] *$
LFact $[i][1]^{\wedge}$ LFact $\left.[i][2]-1 \bmod n\right] ;$
end:
$\operatorname{eval}(G E N)$;
end :
end:
end:
Algorithm 1.5

Complexity of the algorithm :
It's clear that the complexity of the Algorithm $\mathbf{1 . 5}$ 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 $O\left(n^{2} n\right)$ (see [3] and [4]). Therefore the complexity of Algorithm 1.1 without the factorization is $O\left(\ln (\ln n) \ln ^{2} n\right)$.

## 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.

