ON THE STRUCTURE OF THE GENERALIZED GROUP OF UNITS

TERRAR KADRI AND MOHAMMAD EL-HINDI

ABSTRACT. Let \( R \) be a finite commutative ring with identity and \( U(R) \) be its group of units. In 2005, El-Kassar and Chehade presented a ring structure for \( U(R) \) and as a consequence they generalized this group of units to the generalized group of units \( U_k(R) \) defined iteratively as the group of the units of \( U^{k-1}(R) \), with \( U^1(R) = U(R) \). In this paper, we examine the structure of this group, when \( R = \mathbb{Z}_{n} \). We find a decomposition of \( U_k(\mathbb{Z}_{n}) \) as a direct product of cyclic groups for the general case of any \( k \), and we study when these groups are boolean and trivial. We also show that this decomposition structure is directly related to the Pratt Tree primes.

1. INTRODUCTION

Let \( R \) be a finite commutative ring with identity and let \( U(R) \) denote its group of units. The fundamental theorem of finite abelian groups states that any finite abelian group is isomorphic to a product of cyclic groups. That is,

\[
U(R) \approx \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_i}.
\]

(1.1)

The problem of determining the structure of the group of units of any commutative ring \( R \) is an open problem and has received lots of attention. However, the problem is solved for certain classes for example the ring of integers modulo \( n \), \( \mathbb{Z}_n \), see [3], and the factor ring of Gaussian integer modulo \( \beta \), \( \mathbb{Z}[i]/\langle \beta \rangle \), see Cross [4]. Also Smith and Gallian in [7], solved the problem of decomposing the group of units of the finite ring \( F[x]/\langle h(x) \rangle \), where \( F \) is a finite field and \( h(x) \) is polynomial in \( F[x] \).

In 2006, a generalization for the group of units of any finite commutative ring \( R \) with identity, was introduced by El-Kassar and Chehade [1]. They proved that the group of units of a commutative ring \( R \); \( U(R) \); supports a ring structure and this has made it possible to define the second group of units of \( R \) as, \( U^2(R) = U(U(R)) \). Extending this definition to the \( k \)-th level, the \( k \)-th group of units is defined as, \( U^k(R) = U(U^{k-1}(R)) \). On the other hand the decomposition in [1] can be generalized so that \( U^k(R) \approx U^{k-1}(\mathbb{Z}_{n_1}) \times U^{k-1}(\mathbb{Z}_{n_2}) \times \cdots \times U^{k-1}(\mathbb{Z}_{n_i}) \). For example, if we consider \( R = \mathbb{Z}[i]/\langle p^n \rangle \), the factor ring of Gaussian integer modulo \( p^n \), where \( p \) is an odd prime in \( \mathbb{Z} \) of the form \( \equiv 3 \text{(mod 4)} \). Cross [2] determined the structure of the group of units of \( \mathbb{Z}[i]/\langle p^n \rangle \) as \( U(\mathbb{Z}[i]/\langle p^n \rangle) \approx \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1} \). Thus structure of \( U^k(\mathbb{Z}[i]/\langle p^n \rangle) \) can be examined through the isomorphism \( U^k(\mathbb{Z}[i]/\langle p^n \rangle) \approx U^{k-1}(\mathbb{Z}_{p^{n-1}}) \times U^{k-1}(\mathbb{Z}_{p^{n-1}}) \times U^{k-1}(\mathbb{Z}_{p^2-1}) \). Arising from all finite commutative rings \( R \) with identity, the structure of \( U^k(R) \) is obtained through the structure the generalized group of units of \( \mathbb{Z}_n \).

Key words and phrases. Commutative rings; Finite rings; Group of units; Cyclic groups; Generalized group of units; Pratt Tree.
Moreover, let $R$ be any finite ring with $|R| > 1$. Since $0 \notin U(R)$, we have $|U(R)| < |R|$ and hence $|U^k(R)| < |U^{k+1}(R)|$. Thus, $U^k(R)$ must eventually become a boolean ring and $U^{k+1}(R)$ is the trivial group. This mean the iterative structures of $U^k(R)$ will reach the trivial group. These problems were considered by some authors and arose a problem of determining all finite commutative rings $R$ such that $U^k(R)$ is boolean or trivial group. Also some considered the problem when $U^i(R)$ is a cyclic group for some rings $R$ and values of $i$. El-Kassar and Chehade [1] solved both problems completely for $R = \mathbb{Z}_n$ and $k = 2$. Later, Kadri and El-Kassar in [2], considered the problem for the case when $R = \mathbb{Z}_n$ and $k = 3$ and also provided a complete solution for these two problems.

In this paper, we examine the structure of the generalized group of units of $\mathbb{Z}_n$. The structure is discussed by considering the two possible factors of $n$ which are $2^a$ and $p_1^{\alpha_1} \cdots p_i^{\alpha_i}$, where $p_i$ is an odd prime integer. Thus, we find a decomposition of $U^k(\mathbb{Z}_n)$ as a direct product of cyclic groups for the general case of any $k$. Also we examine the problem of having $U^k(\mathbb{Z}_n)$, a boolean ring and those that are trivial. We solve the problem completely when $n = 2^a$, while the case when $n = p^\alpha$, $p$ is an odd integer, is examined and some necessary conditions are given. Also we give some properties of having $U^k(\mathbb{Z}_n)$ a boolean or a trivial group. Eventually, we show that this decomposition structure is directly related to the Pratt Tree primes, illustrated in an example showing this relation.

2. SOME PRELIMINARIES

Let $R$ be the ring of integers modulo $n$, $\mathbb{Z}_n$. The decomposition of the group of units of $\mathbb{Z}_n$, $U(\mathbb{Z}_n)$ can be found in [3] stated in the following Lemma.

**Lemma 1.** The group of units of $\mathbb{Z}_n$ when $n$ is a prime power integer is given by

1. $U(\mathbb{Z}_2) \cong \{0\}$,
2. $U(\mathbb{Z}_{2^a}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}$ when $a \geq 2$,
3. $U(\mathbb{Z}_{p^\alpha}) \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\alpha-1}}$ when $\alpha \geq 1$.

Thus the above isomorphism gives the structure of any group of units $U(\mathbb{Z}_n)$. If $n = 2^a p_1^{\alpha_1} \cdots p_i^{\alpha_i}$ be the decomposition of $n$ into product of distinct prime powers. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{2^a} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\alpha_i}}$$

and

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{2^a}) \times U(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times U(\mathbb{Z}_{p_i^{\alpha_i}}).$$

Moreover, we can conclude from this decomposition that $U(\mathbb{Z}_n)$ is a trivial group if and only if $n = 1$ or $2$. $U(\mathbb{Z}_n)$ is boolean ring for $a = 2$ or $3$ and when $U(\mathbb{Z}_{p_i^{\alpha_i}}) \cong \mathbb{Z}_{p_i-1} \times \mathbb{Z}_{p_i^{\alpha_i-1}} \cong \mathbb{Z}_2$ then $\alpha_i = 1$ and $p_i = 3$. Then $U(\mathbb{Z}_n)$ is a boolean, when $n = 2^2, 2^3, 2^2 \times 3$ or $2^3 \times 3$.

Kadri and El-Kassar in [1], introduced a generalization of the group of units as the $k^{th}$ group of units of commutative ring with identity $R$ denoted as $U^k(R)$. The definition is based on the following theorem.

**Theorem 1.** If a group $(G, \ast)$ is isomorphic to the additive group $(R, +)$ of the ring $(R, +, .)$, then there is an operation $\oplus$ on $G$ such that $(G, \ast, \oplus)$ is a ring isomorphic to $(R, +, \cdot)$.
Theorem 4. Following theorem.

Continuing in the same manner, we obtain that \( U \) is the second group of units of \( R \), which is defined to be the generalized group of units of the commutative ring \( R \) with identity. Eventually, \( U^k(R) \) shall be a commutative ring with identity.

The launching of this group opened several problems from studying the structure of this group and determining all rings \( R \) with a given characteristic of \( U^k(R) \). In particular, El-Kassar and Chihade [1] studied the decomposition of \( U^k(R) \) in the following theorem.

Theorem 2. Let \( k \geq 0 \). If \( R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_r \), then

\[
U^k(R) \cong U^k(R_1) \times U^k(R_2) \times \cdots \times U^k(R_r)
\]

and

\[
U^k(R) \cong U^k(R_1) \oplus U^k(R_2) \oplus \cdots \oplus U^k(R_r)
\]

Note that the first is a group isomorphism and the second is a ring isomorphism. So that at any step of this paper this isomorphism can represent a group or a ring isomorphism. Also the zero group of units of \( R \), \( U^0(R) \), is the ring \( R \) itself.

One of the most important classes is the ring of integers modulo \( n \), \( \mathbb{Z}_n \). So if \( n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_i^{\alpha_i} \) be the decomposition of \( n \) into product of distinct prime powers. Then

\[
U^k(\mathbb{Z}_n) \cong U^k \left( \mathbb{Z}_{p_1^{\alpha_1}} \right) \times U^k \left( \mathbb{Z}_{p_2^{\alpha_2}} \right) \times \cdots \times U^k \left( \mathbb{Z}_{p_i^{\alpha_i}} \right).
\]

An application showing how these iterated groups are determined. Let \( R = \mathbb{Z}_{338} \). We have \( \mathbb{Z}_{338} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{132} \). Then the first group of units is \( U(\mathbb{Z}_{338}) \), which is isomorphic to \( \mathbb{Z}_{12} \times \mathbb{Z}_{13} \). Now, \( U(\mathbb{Z}_{338}) \) is a ring isomorphic to \( \mathbb{Z}_{12} \oplus \mathbb{Z}_{13} \). However, the group of units of \( U(\mathbb{Z}_{338}) \), \( U^2(\mathbb{Z}_{338}) \), is the second group of units of \( \mathbb{Z}_{338} \). \( U^2(\mathbb{Z}_{338}) \) is isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12} \), which is a ring isomorphic to \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \).

Continuing in the same manner, we obtain that \( U^3(\mathbb{Z}_{338}) \) is the third group of units of \( \mathbb{Z}_{338} \) isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). Also \( U^4(\mathbb{Z}_{338}) \) is the 4th group of units isomorphic to the trivial ring \( \mathbb{Z}_1 = \{0\} \).

Also, for any ring \( R \) with \( |R| > 1 \). Since \( 0 \notin U(R) \), we have \( |U(R)| < |R| \) and hence \( |U^k(R)| < |U^{k-1}(R)| \). Thus, \( U^k(R) \) must eventually become a boolean ring and \( U^{k+1}(R) \) is the trivial ring. In the above example \( U^3(\mathbb{Z}_{338}) \) is a boolean ring and \( U^4(\mathbb{Z}_{338}) \) is the trivial ring.

El-Kassar and Chihade in [1] solved the problem of determining all rings \( R \), such that \( U^k(R) \) is trivial completely when \( R = \mathbb{Z}_n \) and \( k = 2 \) summarized in the following theorem.

Theorem 3. \( U^2(\mathbb{Z}_n) \) is trivial if and only if \( n \) divisor of 24.

Also Kadri and El-Kassar in [2], solved the problem for \( U^3(\mathbb{Z}_n) \) given in the following theorem

Theorem 4. \( U^3(\mathbb{Z}_n) \) is trivial if and only if \( n \) divisor of 131040.

Moreover, they established a structure of \( U^3(\mathbb{Z}_n) \) as

\[
U^3(\mathbb{Z}_{2^a}) \cong \begin{cases} 
\{0\} & \text{if } a < 6 \\
\mathbb{Z}_2 \times \mathbb{Z}_{2^{a-6}} & \text{if } a \geq 6
\end{cases}
\]
and when \( p \) is an odd prime. Then
\[
U^3(Z_p^n) \approx \begin{cases} 
U^2(Z_{p-1}) & \text{if } \alpha = 1 \\
U^2(Z_{p-1}) \times U(Z_{p-1}) & \text{if } \alpha = 2 \\
U^2(Z_{p-1}) \times U(Z_{p-1}) \times Z_{p^n-3} & \text{if } \alpha \geq 3 
\end{cases}
\]

3. The Decomposition of \( K^{th} \) Group of Units of \( Z_n \)

In this section we determine the structure of the \( k^{th} \) group of units of \( Z_n \). First we consider the case when \( n = 2^\alpha \) and then the case when \( n = p^\alpha \), where \( p \) is an odd prime.

**Lemma 2.** \( U^k(Z_2) \approx \{0\} \) for all \( k \geq 1 \) and \( U^k(Z_4) \approx \{0\} \) for all \( k \geq 2 \).

**Proof.** Let \( k = 1 \). We have from Lemma \( \text{[1]} \) \( U(Z_2) \approx \{0\} \). Now, let \( k > 1 \). We obtain \( U^{k-1}(U(Z_2)) \approx U^{k-1}(\{0\}) \) which gives that \( U^k(Z_2) \approx \{0\} \). Therefore, \( U^k(Z_2) \approx \{0\} \) for all \( k \geq 1 \). Now, by Lemma \( \text{[1]} \) \( U(Z_4) \approx Z_2 \), and thus \( U^{k-1}(U(Z_4)) \approx U^{k-1}(Z_2) \). However, from the previous result \( U^{k-1}(Z_2) \approx \{0\} \) for \( k - 1 \geq 1, k \geq 2 \). Therefore, \( U^k(Z_4) \approx \{0\} \) for all \( k \geq 2 \). \( \square \)

**Lemma 3.** Let \( \alpha > 2t \geq 0 \) and \( k > t \geq 0 \). Then \( U^k(Z_{2^n}) \approx U^{k-t}(Z_{2^{n-t}}) \).

**Proof.** Suppose that \( \alpha > 2 \) and \( k > 1 \). By Lemma \( \text{[1]} \) we have \( U(Z_{2^n}) \approx Z_2 \times Z_{2^{n-2}} \), then \( U^{k-1}(U(Z_{2^n})) \approx U^{k-1}(Z_2 \times Z_{2^{n-2}}) \). However, \( U^{k-1}(Z_2 \times Z_{2^{n-2}}) \approx U^{k-1}(Z_2) \times U^{k-1}(Z_{2^{n-2}}) \), and by Lemma \( \text{[2]} \) \( U^{k-1}(Z_2) \approx \{0\} \). Therefore, \( U^k(Z_{2^n}) \approx U^{k-1}(Z_{2^{n-2}}) \).

Applying the above relation \( t \) times, we obtain the result. \( \square \)

**Lemma 4.** \( U^k(Z_{2^n}) \approx U^{k+t}(Z_{2^{n+t}}) \) for all nonzero natural numbers \( k \) and \( \alpha \), where \( t \geq 0 \).

**Proof.** Suppose that \( k > 0 \) and \( \alpha > 0 \). Then by Lemma \( \text{[1]} \) \( U(Z_{2^{n+2}}) \approx Z_2 \times Z_{2^{n}} \) and \( U^{k+1}(Z_{2^{n+2}}) \approx U^k(Z_2) \times U^k(Z_{2^n}) \). But by Lemma \( \text{[2]} \) \( U^k(Z_2) \approx \{0\} \). Hence, \( U^{k+1}(Z_{2^{n+2}}) \approx U^k(Z_{2^n}) \).

Applying the above relation \( t \) times, we obtain the result. \( \square \)

In the following theorem we give the decomposition of \( U^k(Z_{2^n}) \) into a direct product of \( Z_n \)’s.

**Theorem 5.** Let \( k > 0 \) and \( \alpha > 0 \). Then the decomposition of \( U^k(Z_{2^n}) \) is given by

\[
\begin{align*}
(1) & \quad U^k(Z_{2^n}) \approx Z_2 \times Z_{2^n-2k} \quad \text{if } \alpha > 2k, \\
(2) & \quad U^k(Z_{2^n}) \approx Z_2 \quad \text{if } \alpha = 2k, \\
(3) & \quad U^k(Z_{2^n}) \approx \{0\} \quad \text{if } \alpha < 2k.
\end{align*}
\]

Note that for \( \alpha = 2k + 1 \), \( U^k(Z_{2^{2k+1}}) \approx Z_2 \times Z_2 \) which is a boolean ring. Also (3) can be written as: \( U^k(Z_{2^n}) \approx \{0\} \) if and only \( 2^\alpha \) is a divisor of \( 2^{2k-1} \).

**Proof.** Let \( k > 0 \) and \( \alpha > 0 \).

(1) Suppose \( \alpha > 2k \) and \( t = k - 1 \). Then \( \alpha - 2(k - 1) = \alpha - 2t > 2 \) and \( k > t \).

Now, from Lemma \( \text{[3]} \) we have \( U^k(Z_{2^n}) \approx U^{k-t}(Z_{2^{n-2t}}) \). Hence,
\[
U^k(Z_{2^n}) \approx U^k(Z_{2^{n-2(2k-1)}}) = U(Z_{2^{2k-1}}) \quad \text{(3.1)}
\]
and by Lemma \( \text{[1]} \) \( U(Z_{2^{2k-1}}) \approx Z_2 \times Z_{2^n-2k} \). Therefore, \( U^k(Z_{2^n}) \approx Z_2 \times Z_{2^n-2k} \).
(2) Suppose that $\alpha = 2k$ and $t = k - 1$. Since $k > t$ and $\alpha - 2t = \alpha - 2k + 2 = 2 > 0$, we have from Lemma 3 the same formula of (64). But $U(Z_{2^{k+2}}) = U(Z_4) \approx Z_2$. Therefore, $U^k(Z_{2^t}) \approx Z_2$.

(3) Suppose $\alpha < 2k$. In the case $\alpha$ is odd, set $t = \frac{\alpha - 1}{2}$. Since $\alpha - 2t = \alpha - 2 \left( \frac{\alpha - 1}{2} \right) = 1 > 0$ and $k - t = k - \frac{\alpha - 1}{2} = \frac{2k - \alpha + 1}{2} > 0$, Lemma 3 gives that $U^k(Z_{2^t}) \approx U^{k-t}(Z_{2^t})$ and $U^{k-t}(Z_{2^t})$ is the trivial group. Now, the case when $\alpha$ is even, set $t = \frac{\alpha}{2}$. Since $\alpha - 2t = \alpha - 2 \left( \frac{\alpha}{2} \right) = 2 > 0$ and $k - t = k - \frac{\alpha}{2} = \frac{2k - \alpha + 2}{2} > 1$. From Lemma 4 $U^k(Z_{2^t}) \approx U^{k-t}(Z_{2^t})$ which is also the trivial group by Lemma 2. Therefore, $U^k(Z_{2^t}) \approx \{0\}$ if $\alpha < 2k$.

Next, we study the decomposition of $k^{th}$ group of units of the ring $Z_{p^\alpha}$, when $p$ is an odd prime.

**Lemma 5.** Let $p$ be an odd prime and let $k \geq 1$. Then $U^k(Z_p) \approx U^{k-1}(Z_{p-1})$.

**Proof.** The proof is a direct consequence that $U(Z_p) \approx Z_{p-1}$.

**Theorem 6.** Let $p$ be an odd prime and let $0 \leq t < \alpha$ and $1 \leq t < k$. Then

$$U^k(Z_{p^\alpha}) \approx U^k(Z_p) \times U^{k-1}(Z_p) \times \cdots \times U^{k+t-1}(Z_p) \times U^{k-t}(Z_{p^{-t}}).$$

**Proof.** Suppose $t = 0$, then $1 < \alpha$ and $1 \leq k$. We have from Lemma 1 $U(Z_{p^\alpha}) \approx Z_{p-1} \times Z_{p-1}$ and so $U^k(Z_{p^\alpha}) \approx U^{k-1}(Z_{p-1}) \times U^{k-1}(Z_{p-1})$. But by Lemma 5 $U^{k-1}(Z_{p-1}) \approx U^k(Z_p)$. Hence,

$$U^k(Z_{p^\alpha}) \approx U^k(Z_p) \times U^{k-1}(Z_{p^\alpha-1})$$

(3.2)

Now, Suppose $t = 2, 2 < \alpha$ and $2 \leq k$. Then the isomorphism in (3.2) can be written as

$$U^{k-1}(Z_{p^\alpha-1}) \approx U^{k-1}(Z_p) \times U^{k-2}(Z_{p^\alpha-2}).$$

by replacing $k$ and $\alpha$ by $k - 1$ and $\alpha - 1$ respectively. Hence,

$$U^k(Z_{p^\alpha}) \approx U^k(Z_p) \times U^{k-1}(Z_p) \times U^{k-2}(Z_{p^\alpha-2}).$$

Continuing in the same manner. When $t < \alpha$ and $t \leq k$, we conclude that,

$$U^{k-(t-1)}(Z_{p^\alpha-t-1}) \approx U^{k-(t-1)}(Z_p) \times U^{k-t}(Z_{p^\alpha-1}).$$

Therefore,

$$U^k(Z_{p^\alpha}) \approx U^k(Z_p) \times U^{k-1}(Z_p) \times U^{k-t}(Z_{p^\alpha-1}).$$

\[\square\]

**Example 1.** Applying the above theorem we obtain the following. Let $p = 47$, $k = 8$, $\alpha = 6$ and $t = 5$. Then

$$U^8(Z_{47^8}) \approx U^8(Z_{47}) \times U^7(Z_{47}) \times \cdots \times U^4(Z_{47}) \times U^3(Z_{47}).$$

But $U(Z_{47}) \approx Z_{46} \approx Z_2 \times Z_{23}$, which implies that $U^2(Z_{47}) \approx U(Z_{23}) \approx Z_{22} \approx Z_2 \times Z_2 \times \cdots$, and so $U^3(Z_{47}) \approx U(Z_{11}) \approx Z_{10} \approx Z_2 \times Z_5$, $U^4(Z_{47}) \approx U(Z_5) \approx Z_4$, and $U^5(Z_{47}) \approx U(Z_4) \approx Z_2$ and hence, $U^6(Z_{47}) \approx U^7(Z_{47}) \approx U^8(Z_{47}) \approx \{0\}$. Therefore,

$$U^8(Z_{47^8}) = U^5(Z_{47}) \times U^4(Z_{47}) \times U^3(Z_{47}) \approx Z_2 \times Z_4 \times Z_2 \times Z_5.$$

**Theorem 7.** Let $p$ be an odd prime and let $\alpha > 0$ and $k > 0$. Then

(1) $U^k(Z_{p^\alpha}) \approx U^k(Z_p) \times U^{k-1}(Z_p) \times \cdots \times U^{k-\alpha+1}(Z_p)$, when $\alpha < k$. 

\[\square\]
(2) $U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^2(\mathbb{Z}_p) \times U(\mathbb{Z}_p)$, when $\alpha = k$,
(3) $U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U(\mathbb{Z}_p) \times \mathbb{Z}_{p^{n-k}}$, when $\alpha > k$.

Proof. Let $p$ be an odd prime and let $\alpha > 0$ and $k > 0$.

(1) Let $\alpha \leq k$ and $t = \alpha - 1$. Then $t < \alpha$ and $t < k$ and by Theorem 6

$$U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-t+1}(\mathbb{Z}_p) \times U^{k-t}(\mathbb{Z}_{p^{n-t}}).$$

Thus,

$$U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+2}(\mathbb{Z}_p) \times U^{k-\alpha+1}(\mathbb{Z}_p).$$

(2) The proof is obtained by replacing $\alpha = k$ in the isomorphism (3.3).

(3) Let $\alpha > k$ and $t = k - 1$. Then $t < \alpha$ and $t < k$. From Theorem 6

$$U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-t+1}(\mathbb{Z}_p) \times U^{k-t}(\mathbb{Z}_{p^{n-t}})$$

$$\approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-(k-1)+1}(\mathbb{Z}_p) \times U^{k-(k-1)}(\mathbb{Z}_{p^{n-(k-1)}})$$

$$\approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^2(\mathbb{Z}_p) \times U(\mathbb{Z}_{p^{n-k+1}}).$$

Now, since $\alpha - k + 1 > 0$, Lemma 11 gives that $U(\mathbb{Z}_{p^{n-k+1}}) \approx \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{n-k}}$. Therefore,

$$U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^2(\mathbb{Z}_p) \times \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{n-k}}.$$  



The above theorem gives the decomposition of $U^k(\mathbb{Z}_{p^n})$ into a direct product of $U^i(\mathbb{Z}_p)$ and $\mathbb{Z}_{p^j}$. So by finding the decomposition of $U^i(\mathbb{Z}_p)$, for a given odd prime $p$, the decomposition $U^k(\mathbb{Z}_{p^n})$ is established.

Next, we give some application of decompositions of $U^k(\mathbb{Z}_{p^n})$ in the case $p = 3$.

Corollary 1. Let $n = 3^a$. Then the decomposition of the $k$th group of units of $\mathbb{Z}_n$ is given by

$$U^k(\mathbb{Z}_{3^n}) \approx \begin{cases} 
\mathbb{Z}_2 \times \mathbb{Z}_{3^a-k} & \text{if } \alpha > k \\
\mathbb{Z}_2 & \text{if } \alpha = k \\
\{0\} & \text{if } \alpha < k
\end{cases}$$

Proof. We have $U^i(\mathbb{Z}_3) = U^{i-1}(U(\mathbb{Z}_3)) \approx U^{i-1}(\mathbb{Z}_2)$. But $U^{i-1}(\mathbb{Z}_2) = \mathbb{Z}_2$ if $i = 1$ and $U^{i-1}(\mathbb{Z}_2) \approx \{0\}$ for $i > 1$. Hence,

$$U^i(\mathbb{Z}_3) \approx \begin{cases} 
\mathbb{Z}_2 & \text{if } i = 1 \\
\{0\} & \text{if } i > 1
\end{cases}$$

By applying Theorem 11 for $p = 3$, we obtain that when $\alpha < k$, 

$$U^k(\mathbb{Z}_{3^n}) \approx U^k(\mathbb{Z}_3) \times U^{k-1}(\mathbb{Z}_3) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_3).$$

But $k - j + 1 > 1$ for $j = 1, 2, \cdots, \alpha$, and so $U^k(\mathbb{Z}_3) \approx U^{k-1}(\mathbb{Z}_3) \approx \cdots \approx U^{k-\alpha+1}(\mathbb{Z}_3) \approx \{0\}$. Therefore, $U^k(\mathbb{Z}_{3^n}) \approx \{0\}$.

Now, if $\alpha = k$,

$$U^k(\mathbb{Z}_{3^k}) \approx U^k(\mathbb{Z}_3) \times U^{k-1}(\mathbb{Z}_3) \times \cdots \times U^2(\mathbb{Z}_3) \times U(\mathbb{Z}_3).$$

But $U^k(\mathbb{Z}_3) \approx U^{k-1}(\mathbb{Z}_3) \approx U^2(\mathbb{Z}_3) \approx \{0\}$. Hence, $U^k(\mathbb{Z}_{3^k}) \approx U(\mathbb{Z}_3) \approx \mathbb{Z}_2$.

If $\alpha > k$, then 

$$U^k(\mathbb{Z}_{3^n}) \approx U^k(\mathbb{Z}_3) \times U^{k-1}(\mathbb{Z}_3) \times \cdots \times U^2(\mathbb{Z}_3) \times U(\mathbb{Z}_3) \times \mathbb{Z}_{3^{n-k}} 
\approx \mathbb{Z}_2 \times \mathbb{Z}_{3^{n-k}}.$$
The following corollary is a direct conclusion done by combining Theorem 7 and Lemma 5.

**Corollary 2.** Let $p$ be an odd prime and let $\alpha > 0$ and $k > 0$. Then

1. $U^k(\mathbb{Z}_{p^n}) \cong U^{k-1}(\mathbb{Z}_{p-1}) \times U^{k-2}(\mathbb{Z}_{p-1}) \times \cdots \times U^{k-\alpha}(\mathbb{Z}_{p-1})$, when $\alpha < k$,
2. $U^k(\mathbb{Z}_p^k) \cong U^{k-1}(\mathbb{Z}_{p-1}) \times U^{k-2}(\mathbb{Z}_{p-2}) \times \cdots \times U(\mathbb{Z}_{p-1}) \times \mathbb{Z}_{p-1}$, when $\alpha = k$,
3. $U^k(\mathbb{Z}_{p^n}) \cong U^{k-1}(\mathbb{Z}_{p-1}) \times U^{k-2}(\mathbb{Z}_{p-1}) \times \cdots \times \mathbb{Z}_{p^n-k(p-1)}$, when $\alpha > k$.

The next corollaries refer to Corollary 2 in determining the structure of $U^k(\mathbb{Z}_{p^n})$ by knowing the structure of $U^i(\mathbb{Z}_{p-1})$ where $i < k$. We apply this on $U^k(\mathbb{Z}_{5^n})$ and $U^k(\mathbb{Z}_{7^n})$.

**Corollary 3.** Let $n = 5^\alpha$. Then the decomposition of the $k^{th}$ group of units of $\mathbb{Z}_n$ is given

$$U^k(\mathbb{Z}_{5^n}) \cong \begin{cases} Z_2 \times Z_4 \times Z_{5^n-k} & \text{if } \alpha > k, \\ Z_2 \times Z_4 & \text{if } \alpha = k, \\ Z_2 & \text{if } \alpha = k - 1, \\ \{0\} & \text{if } \alpha < k - 1 \end{cases}$$

**Proof.** Using Theorem 5 and setting $\alpha = 2$ the case $\alpha > 2k$ is rejected, so we are left with

$$U^k(\mathbb{Z}_4) \cong \begin{cases} Z_2 & \text{if } k = 1, \\ \{0\} & \text{if } k > 1 \end{cases}$$

$$U^{k-i}(\mathbb{Z}_4) \cong \begin{cases} Z_2 & \text{if } i = k - 1, \\ \{0\} & \text{if } i < k - 1, \ i = 1, 2, \ldots, k - 1 \end{cases}$$

By applying Corollary 2 we get

$$U^k(\mathbb{Z}_{5^n}) \cong \begin{cases} U^{k-1}(\mathbb{Z}_4) \times U^{k-2}(\mathbb{Z}_4) \times \cdots \times U^{k-\alpha}(\mathbb{Z}_4) & \text{if } \alpha < k, \\ U^{k-1}(\mathbb{Z}_4) \times U^{k-2}(\mathbb{Z}_4) \times \cdots \times U(\mathbb{Z}_4) \times Z_4 & \text{if } \alpha = k, \\ U^{k-1}(\mathbb{Z}_4) \times U^{k-2}(\mathbb{Z}_4) \times \cdots \times U(\mathbb{Z}_4) \times Z_4 \times Z_{5^n-k} & \text{if } \alpha > k \end{cases}$$

for $\alpha < k$, if $\alpha = k - 1$ $U^{k-\alpha}(\mathbb{Z}_4) \approx Z_2$ and $U^{k-i}(\mathbb{Z}_4) \approx \{0\}$ for $i < k - 1$, thus $U^k(\mathbb{Z}_{5^n}) \approx Z_2$. And if $\alpha < k - 1$, we have $U^{k-i}(\mathbb{Z}_4) \approx \{0\}$ for $i = 1, 2, \ldots, \alpha$. Thus $U^k(\mathbb{Z}_{5^n}) \approx Z_2$.

For the second case $\alpha = k$, all the summands are trivial except $U(\mathbb{Z}_4) \approx Z_2$. Then $U^k(\mathbb{Z}_{5^n}) \approx Z_2 \times Z_4$. Consequently to the case $\alpha = k$, we can conclude directly the case $\alpha > k$, that is $U^k(\mathbb{Z}_{5^n}) \approx Z_2 \times Z_4 \times Z_{5^n-k}$.

**Corollary 4.** Let $n = 7^\alpha$. Then the decomposition of the $k^{th}$ group of units of $\mathbb{Z}_n$ is given

$$U^k(\mathbb{Z}_{7^n}) \cong \begin{cases} Z_2 \times Z_6 \times Z_{7^n-k} & \text{if } \alpha > k, \\ Z_2 \times Z_6 & \text{if } \alpha = k, \\ Z_2 & \text{if } \alpha = k - 1, \\ \{0\} & \text{if } \alpha < k - 1 \end{cases}$$

**Proof.** From Corollary 2 we relate the decomposition of $U^k(\mathbb{Z}_{p^n})$ to $U^i(\mathbb{Z}_{p-1})$ for $i < k$ then for $p = 7$ we need to find $U^i(\mathbb{Z}_6)$ for $i < k$. We have $U^i(\mathbb{Z}_6) \approx U^i(\mathbb{Z}_2) \times U^i(\mathbb{Z}_4)$. However from Theorem 5 $U^i(\mathbb{Z}_2) \approx \{0\}$ and from Corollary 1

$$U^i(\mathbb{Z}_4) \approx \begin{cases} Z_2 & \text{if } i = 1, \\ \{0\} & \text{if } i > 1 \end{cases}$$
then
\[ U^i(\mathbb{Z}_6) \approx \begin{cases} \mathbb{Z}_2 & \text{if } i = 1 \\ \{0\} & \text{if } i > 1 \end{cases} \]

By applying Corollary 2, we get for \( \alpha > k \),
\[ U^k(\mathbb{Z}_{7^\alpha}) \approx U^{k-1}(\mathbb{Z}_6) \times U^{k-2}(\mathbb{Z}_6) \times \cdots \times U(\mathbb{Z}_6) \times \mathbb{Z}_6 \times \mathbb{Z}_{7^\alpha-k} \]
\[ \approx \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{7^\alpha-k} \]

for \( \alpha = k \),
\[ U^k(\mathbb{Z}_{7^\alpha}) \approx U^{k-1}(\mathbb{Z}_6) \times U^{k-2}(\mathbb{Z}_6) \times \cdots \times U(\mathbb{Z}_6) \times \mathbb{Z}_6 \]
\[ \approx \mathbb{Z}_2 \times \mathbb{Z}_6 \]

for \( \alpha < k \), if \( \alpha = k - 1 \)
\[ U^k(\mathbb{Z}_{7^\alpha}) \approx U^{k-1}(\mathbb{Z}_6) \times U^{k-2}(\mathbb{Z}_6) \times \cdots \times U(\mathbb{Z}_6) \]
\[ \approx \mathbb{Z}_2 \]

and if \( \alpha = k - 2 \)
\[ U^k(\mathbb{Z}_{7^\alpha}) \approx U^{k-1}(\mathbb{Z}_6) \times U^{k-2}(\mathbb{Z}_6) \times \cdots \times U(\mathbb{Z}_6) \]
\[ \approx \{0\} \cdot \mathbb{Z}_2 \]

and thus \( U^k(\mathbb{Z}_{7^\alpha}) \approx \{0\} \) for \( \alpha < k - 2 \). Therefore, we obtain the required. \( \square \)

We end this section by noting that for higher prime integers the decomposition is more complicated. But we noticed that the decomposition of \( U^k(\mathbb{Z}_{3^\alpha}) \) and \( U^k(\mathbb{Z}_{5^\alpha}) \) were obtained knowing the decomposition of \( U^k(\mathbb{Z}_2) \). Also the decomposition of \( U^k(\mathbb{Z}_{7^\alpha}) \) is obtained from the decomposition of \( U^k(\mathbb{Z}_2) \) and \( U^k(\mathbb{Z}_3) \) and so on. We may conclude that each decomposition of \( U^k(\mathbb{Z}_{p^\alpha}) \) has a Tree of decompositions of \( U^k(\mathbb{Z}_{p^i}) \) for a given sequence of primes \( p_i \). This problem is discussed in Section 5.

4. Boolean and Trivial \( U^k(\mathbb{Z}_n) \)

The previous section opened the importance in examining the rings that have \( k^{th} \) group of units, \( U^k(\mathbb{Z}_n) \), a boolean and those that are trivial. In this section, we study these two problems. First, we consider the case \( n = 2^\alpha \), then when \( n = p^\alpha \), where \( p \) is a odd prime. We solve the problem completely when \( n = 2^\alpha \), while the case when \( n = p^\alpha \) is examined and some necessary conditions are given. We end this section by concluding some properties of having \( U^k(\mathbb{Z}_n) \) a boolean or a trivial group.

In the following theorem our two major problems are solved in the case \( n = 2^\alpha \) and \( n = 3^\alpha \).

**Theorem 8.** Let \( \alpha \geq 1 \) and \( k \geq 1 \). Then
(1) \( U^k(\mathbb{Z}_{2^\alpha}) \) is a boolean ring if and only if \( \alpha = 2k \) or \( \alpha = 2k + 1 \) and is trivial if and only if \( \alpha < 2k \).
(2) \( U^k(\mathbb{Z}_{3^\alpha}) \) is boolean ring if and only if \( \alpha = k \) and is trivial if and only if \( \alpha < k \).

**Proof.** The proof is a direct consequence from Theorem 5 and Corollary 1. \( \square \)
Next, we consider the case when \( p \) is an odd prime integer and since in Theorem 8 the special case \( p = 3 \) is solved so we may consider the cases when \( p \) is an odd prime integer different than 3.

**Lemma 6.** Let \( p \) be an odd prime different from 3. If \( U^k(\mathbb{Z}_{p^n}) \) is boolean ring, then \( \alpha < k \).

*Proof.* Let \( p \) be an odd prime different from 3 and suppose that \( U^k(\mathbb{Z}_{p^n}) \) is a boolean ring. Assume for contradiction that \( \alpha \geq k \). If \( \alpha = k \), then by Theorem 7, we have

\[
U^k(\mathbb{Z}_{p^k}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^2(\mathbb{Z}_p) \times U(\mathbb{Z}_p).
\]

Hence, \( U^k(\mathbb{Z}_{p^k}) \) is boolean if and only if \( U(\mathbb{Z}_p) \) is a boolean ring implies that \( p = 3 \) a contradiction.

Now, suppose that \( \alpha > k \). By Theorem 7 we have

\[
U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U(\mathbb{Z}_p) \times \mathbb{Z}_{p^n-k}.
\]

Hence, \( \mathbb{Z}_{p^n-k} \) is boolean or trivial, a contradiction. Therefore, \( \alpha < k \). \( \square \)

**Lemma 7.** Let \( p \) be an odd prime. If \( U^k(\mathbb{Z}_{p^n}) \) is trivial, then \( \alpha < k \).

*Proof.* Let \( p \) be an odd prime and suppose that \( U^k(\mathbb{Z}_{p^n}) \) is trivial. Suppose that \( \alpha = k \), then by Theorem 7, we have

\[
U^k(\mathbb{Z}_{p^k}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^2(\mathbb{Z}_p) \times U(\mathbb{Z}_p).
\]

Hence, \( U(\mathbb{Z}_p) \) is trivial, since \( U^k(\mathbb{Z}_{p^k}) \) is trivial if and only if

\[
U^k(\mathbb{Z}_p) \approx U^{k-1}(\mathbb{Z}_p) \approx \cdots \approx U(\mathbb{Z}_p) \approx \{0\}.
\]

But \( U(\mathbb{Z}_p) \) is trivial implies that \( p = 1, 2 \), a contradiction. Therefore \( \alpha \neq k \).

Now, suppose that \( \alpha > k \). By Theorem 7 we have

\[
U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U(\mathbb{Z}_p) \times \mathbb{Z}_{p^n-k}.
\]

But \( U^k(\mathbb{Z}_{p^n}) \) is trivial if and only if

\[
U^{k-1}(\mathbb{Z}_{p^n-k}) \approx U^{k-2}(\mathbb{Z}_{p^n-k}) \approx \cdots \approx U(\mathbb{Z}_p) \approx \mathbb{Z}_{p^n-k} \approx \{0\};
\]

a contradiction, as \( \mathbb{Z}_{p^n-k} \) is never trivial. Therefore, \( \alpha < k \). \( \square \)

From the previous two Lemmas we conclude one of necessary condition to have \( U^k(\mathbb{Z}_{p^n}) \) a boolean ring or a trivial one which is \( \alpha < k \). Next, we find the sufficient condition to obtain these rings.

**Theorem 9.** Let \( p \) be an odd prime different from 3. Then \( U^k(\mathbb{Z}_{p^n}) \) is boolean ring if and only if \( \alpha < k \) and \( U^{k-\alpha+1}(\mathbb{Z}_p) \) is a boolean ring. Moreover,

\[
U^k(\mathbb{Z}_{p^n}) \approx U^{k-\alpha+1}(\mathbb{Z}_p).
\]

*Proof.* Let \( p \) be an odd prime different from 3 and let \( U^k(\mathbb{Z}_{p^n}) \) be a boolean ring. Then from Lemma 6 we obtain that \( \alpha < k \). Also by Theorem 7

\[
U^k(\mathbb{Z}_{p^n}) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_p).
\]

Then, \( U^{k-\alpha+1}(\mathbb{Z}_p) \) is a boolean ring also

\[
U^{k-\alpha+2}(\mathbb{Z}_p) \approx U^{k-\alpha+3}(\mathbb{Z}_p) \approx \cdots \approx U^{k-\alpha+\alpha}(\mathbb{Z}_p) \approx \{0\}.
\]

Therefore, \( U^k(\mathbb{Z}_{p^n}) \approx U^{k-\alpha+1}(\mathbb{Z}_p) \).
Conversely, let \( \alpha < k \) and \( U^{k-\alpha+1}(\mathbb{Z}_p) \) is a boolean ring. Then
\[
U^s(U^{k-\alpha+1}(\mathbb{Z}_p)) \approx \{0\}, \quad \text{when } s = 1, 2, \ldots, \alpha - 1.
\]
That is,
\[
U^{k+1}(\mathbb{Z}_p) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\}.
\]
Therefore, \( U^k(\mathbb{Z}_p) \approx U^{k-\alpha+1}(\mathbb{Z}_p) \), which is a boolean ring. \( \square \)

**Theorem 10.** Let \( p \) be an odd prime. Then \( U^k(\mathbb{Z}_p) \) is trivial if and only if \( \alpha < k \) and \( U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\} \).

**Proof.** Let \( p \) be an odd prime and suppose that \( U^k(\mathbb{Z}_p) \) is trivial. Then from Lemma 6, we obtain that \( \alpha < k \). Also by Theorem 7,
\[
U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\}.
\]
Therefore, \( U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\} \).

Conversely, let \( \alpha < k \) and \( U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\} \). Then \( U^s(U^{k-\alpha+1}(\mathbb{Z}_p)) \approx \{0\} \), when \( s = 0, 1, 2 \ldots, \alpha - 1 \). That is,
\[
U^{k+1}(\mathbb{Z}_p) \approx U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_p) \approx \{0\}.
\]
Therefore, \( U^k(\mathbb{Z}_p) \approx \{0\} \). \( \square \)

Next, we take an example to check if a given ring \( U^k(\mathbb{Z}_p) \) is a boolean ring or trivial. Let us suppose \( U^k(\mathbb{Z}_p) \) is a boolean ring. Then with the necessary condition that \( \alpha < k \) else it is not a boolean neither a trivial group. Along the check the nature of \( U^{k-\alpha+1}(\mathbb{Z}_p) = U^{9-1+1}(\mathbb{Z}_{23}) = U^4(\mathbb{Z}_{23}) \). We have
\begin{itemize}
  \item (1) \( U(\mathbb{Z}_{23}) \approx \mathbb{Z}_{22} \approx \mathbb{Z}_2 \times \mathbb{Z}_{11} \),
  \item (2) \( U^2(\mathbb{Z}_{23}) \approx U(\mathbb{Z}_{11}) \approx \mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_5 \),
  \item (3) \( U^3(\mathbb{Z}_{23}) \approx U(\mathbb{Z}_5) \approx \mathbb{Z}_4 \) and
  \item (4) \( U^4(\mathbb{Z}_{23}) \approx U(\mathbb{Z}_4) \approx \mathbb{Z}_2 \).
\end{itemize}

Therefore, \( U^3(\mathbb{Z}_{23}) \) is a boolean ring with \( U^3(\mathbb{Z}_{23}) \approx U^4(\mathbb{Z}_{23}) \approx \mathbb{Z}_2 \).

**Theorem 11.** Let \( p \) be an odd prime and let \( k > 0, \alpha > 0 \) and \( t > 0 \). Then \( U^k(\mathbb{Z}_p) \) is a boolean ring if and only if \( U^{k+t}(\mathbb{Z}_{p^{\alpha+t}}) \) is boolean ring. Moreover, \( U^k(\mathbb{Z}_p) \approx U^{k+t}(\mathbb{Z}_{p^{\alpha+t}}) \).

**Proof.** Let \( p \) be an odd prime and \( U^k(\mathbb{Z}_p) \) is a boolean ring. Suppose \( p \neq 3 \), from Lemma 5 \( \alpha < k \), then \( \alpha + 1 < k + 1 \). However, Theorem 6 gives
\[
U^{k+1}(\mathbb{Z}_{p^\alpha+t}) \approx U^{k+1}(\mathbb{Z}_p) \times U^k(\mathbb{Z}_p) \times \cdots \times U^{k+1-\alpha+1}(\mathbb{Z}_p) \\
\approx U^{k+1}(\mathbb{Z}_p) \times U^k(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_p) \\
\approx U^{k+1}(\mathbb{Z}_p) \times U^k(\mathbb{Z}_p) \\
\approx \{0\}.
\]

Also, from Corollary 2 we have \( U^k(\mathbb{Z}_p) \approx U^{k-\alpha+1}(\mathbb{Z}_p) \) and are boolean rings. Then \( U^\alpha(U^{k-\alpha+1}(\mathbb{Z}_p)) = U^{k+1}(\mathbb{Z}_p) \approx \{0\} \). Therefore, \( U^{k+1}(\mathbb{Z}_{p^{\alpha+t}}) \approx U^k(\mathbb{Z}_p) \).

Applying this isomorphism \( t \) times, we obtain that \( U^{k+t}(\mathbb{Z}_{p^{\alpha+t}}) \approx U^k(\mathbb{Z}_p) \).

Conversely, let \( U^{k+t}(\mathbb{Z}_{p^{\alpha+t}}) \) be a boolean ring. Then by Theorem 6
\[
U^{k+t}(\mathbb{Z}_{p^{\alpha+t}}) \approx U^{(k+t)-(\alpha+t)+1}(\mathbb{Z}_p) \\
= U^{k-\alpha+1}(\mathbb{Z}_p)
\]
and are boolean rings. We may conclude that $U^r(U^{k-\alpha+1}(\mathbb{Z}_p)) \cong \{0\}$ for $r = 1, 2, \ldots, \alpha$. Thus we have
\[
U^k(\mathbb{Z}_{p^\alpha}) \cong U^k(\mathbb{Z}_p) \times \cdots \times U^{k-\alpha+1}(\mathbb{Z}_p) \\
\cong U^{k-\alpha+1}(\mathbb{Z}_p)
\]
On the other hand, when $p = 3$, Corollary 5. can be written as $U^k(\mathbb{Z}_{3^k}) \cong U^{k+t}(\mathbb{Z}_{3^{k+t}}) \cong \mathbb{Z}_2$. □

The following corollary is a direct consequence of Theorem 11.

**Corollary 5.** Let $p$ be an odd prime and let $t > 0$, $k > 0$ and $\alpha > 0$. Then

1. $U^k(\mathbb{Z}_{p^\alpha})$ is not a boolean ring if and only if $U^{k+t}(\mathbb{Z}_{p^\alpha+1})$ is not a boolean ring.

2. $U^k(\mathbb{Z}_{p^\alpha})$ is a trivial ring if and only if $U^{k+t}(\mathbb{Z}_{p^\alpha+1})$ is a trivial ring.

3. $U^k(\mathbb{Z}_{p^\alpha})$ is nontrivial ring if and only if $U^{k+t}(\mathbb{Z}_{p^\alpha+1})$ is nontrivial ring.

**Lemma 8.** Let $p$ be a prime and let $0 \leq t \leq \alpha$. If $U^k(\mathbb{Z}_{p^\alpha}) \cong \{0\}$, then $U^k(\mathbb{Z}_{p^\alpha}) \cong \{0\}$.

**Proof.** Let $p$ be a prime and let $0 \leq t \leq \alpha$. Suppose $U^k(\mathbb{Z}_{p^\alpha}) \cong \{0\}$. By Theorem 10 we obtain that $\alpha < k$. Now, since $0 \leq t \leq \alpha$, $0 \leq t < k$ and by Theorem 7 we have

\[
U^k(\mathbb{Z}_{p^\alpha}) \cong U^k(\mathbb{Z}_p) \times U^{k-1}(\mathbb{Z}_p) \times \cdots \times U^{k-t+1}(\mathbb{Z}_p).
\]

Since $U^k(\mathbb{Z}_{p^\alpha}) \cong \{0\}$, Theorem 11 gives that $U^{k-\alpha+1}(\mathbb{Z}_p) \cong \{0\}$. However, $U^{s}(U^{k-\alpha+1}(\mathbb{Z}_p)) \cong \{0\}$, where $s = 0, 1, 2 \cdots, t - 1$. That is,

\[
U^k(\mathbb{Z}_p) \cong U^{k-1}(\mathbb{Z}_p) \cong \cdots \cong U^{k-t+1}(\mathbb{Z}_p) \cong \{0\}.
\]

Therefore, $U^k(\mathbb{Z}_{p^\alpha}) \cong \{0\}$.

Now, let $p = 2$. From Theorem 5. $U^k(\mathbb{Z}_{2^\alpha}) \cong \{0\}$ if and only if $\alpha < 2k$. But $0 \leq t \leq \alpha < 2k$. Therefore, $U^k(\mathbb{Z}_{2^\alpha}) \cong \{0\}$. □

**Theorem 12.** Let $U^k(\mathbb{Z}_n) \cong \{0\}$. Then for all divisors $m$ of $n$, $U^k(\mathbb{Z}_m) \cong \{0\}$.

**Proof.** Let $n = 2^{\alpha_1}p_1^{\alpha_1'}\cdots p_r^{\alpha_r'}$ be the decomposition of $n$ into product of distinct prime powers and let $U^k(\mathbb{Z}_n) \cong \{0\}$. Suppose that $m$ be a divisor of $n$. Then $m = 2^{\alpha'_1}p_1^{\alpha'_1}\cdots p_r^{\alpha'_r}$, where $0 \leq \alpha'_1 \leq \alpha_1$ and $0 \leq \alpha'_r \leq \alpha_r$. We have

\[
U^k(\mathbb{Z}_n) \cong U^k(\mathbb{Z}_{2^{\alpha'}}) \times U^k\left(\mathbb{Z}_{p_1^{\alpha'_1}}\right) \times \cdots \times U^k\left(\mathbb{Z}_{p_r^{\alpha'_r}}\right).
\]

Hence, $U^k(\mathbb{Z}_{2^{\alpha'}}), U\left(\mathbb{Z}_{p_1^{\alpha'_1}}\right), \cdots$ and $U^k\left(\mathbb{Z}_{p_r^{\alpha'_r}}\right)$ are trivial. By the Lemma 8 we obtain that $U^k(\mathbb{Z}_{2^{\alpha'}}), U\left(\mathbb{Z}_{p_1^{\alpha'_1}}\right), \cdots$ and $U^k\left(\mathbb{Z}_{p_r^{\alpha'_r}}\right)$ are trivial. Therefore,

\[
U^k(\mathbb{Z}_{2^{\alpha'}}) \times U^k\left(\mathbb{Z}_{p_1^{\alpha'_1}}\right) \times \cdots \times U^k\left(\mathbb{Z}_{p_r^{\alpha'_r}}\right) \cong \{0\},
\]

and $U^k(\mathbb{Z}_m)$ is trivial. □

**Theorem 13.** Let $U^k(\mathbb{Z}_n)$ be a boolean ring. Then for all divisors $m$ of $n$, $U^k(\mathbb{Z}_m) \cong \{0\}$ or $U^k(\mathbb{Z}_m)$ is a boolean ring.

**Proof.** Let $U^k(\mathbb{Z}_n)$ be a boolean ring. Then $U^{k+1}(\mathbb{Z}_n) \cong \{0\}$. From Theorem 12 we have for all divisors $m$ of $n$, $U^{k+1}(\mathbb{Z}_m) \cong \{0\}$. The later leads to two possibilities either $U^k(\mathbb{Z}_m) \cong \{0\}$ or $U^k(\mathbb{Z}_m)$ is a boolean ring. □
5. Pratt’s Tree and Decomposition of $U^k(Z_n)$

V. Pratt in [8] showed that short proofs of primality do exist, that is, PRIMES is in NP where he introduced what so called Pratt certificate and Pratt tree. The authors in [8] discussed in details the dimensions of Pratt’s tree introduced in his paper. In this section, we refer Pratt’s tree to the complete structure of $U^k(Z_n)$. The steps to find the decomposition $U^k(Z_n)$ are similar to the step in determining the Pratt tree with same structure and dimension, see Fig.

V. Pratt in [7] showed that short proofs of primality do exist, that is, PRIMES is in NP where he introduced what so called Pratt certificate and Pratt tree. The authors in [8] discussed in details the dimensions of Pratt’s tree introduced in his paper. In this section, we refer Pratt’s tree to the complete structure of $U^k(Z_n)$. The steps to find the decomposition $U^k(Z_n)$ are similar to the step in determining the Pratt tree with same structure and dimension, see Fig.

of prime divisors of $n$, where all primes given in Pratt tree are used to reach the decomposition of $U^k(Z_n)$.

The primes in Pratt tree are the Prime chains $p_1 < p_2 < \cdots < p_k$ such that for which $p_j+1 \equiv 1 \pmod{p_j}$ in other words, $p_j|p_{j+1} - 1$ for each $j$, see [8]. By charting this process, we find what is called a Lucas-Pratt tree [9]. On the other hand, we have

If $p_j = 2$ the decomposition is solved in Theorem [5] While when $p_j$ is an odd prime, it is clear from Corollary [8] that to find the decomposition of $U^k(Z_{p_j})$, we need to find decomposition of $U^i(Z_{p_j-1})$, $i = 1, 2, \ldots, k - 1$. which is also determined from the prime factors of $p_j - 1$ which shall be the Primes in the Pratt tree.

To illustrate the relation, we set $p_j = 269$ and our aim is to determine the decomposition of $U^k(Z_{269^n})$, and relate it to Pratt Tree.

The Pratt Tree is obtained by the following steps:

Step 1: $p_j - 1 = 268 = 2^2 \times 67$. First level in Pratt Tree is (2, 67),
Step 2: $67 - 1 = 66 = 2 \times 3 \times 11$ and Second Level in Pratt Tree is (2, 3, 11),
Step 3: $3 - 1 = 2$ also $11 - 1 = 2 \times 5$ and thus Third Level in Pratt Tree is (2, 2, 5),
Step 4: $5 - 1 = 2^2$ which give the Last level in the the Pratt Tree (2).

Next, we show the steps in determining the decomposition of $U^k(Z_{269^n})$. Starting from Corollary [2] which shows that the decomposition of $U^k(Z_{269^n})$ is determined from $U^i(Z_{p_j-1})$, $i = 1, 2, \ldots, k - 1$. Thus

$$U^i(Z_{p_j-1}) = U^i(Z_{268}) \approx U^i(Z_{67}) \times U^i(Z_{2})\times U^i(Z_{3})\times U^i(Z_{11}),$$

$i = 1, 2, \ldots, k - 1$. Thus we get in this decomposition the First Level of Pratt Tree (2, 67). Now, the decomposition of $U^i(Z_{2})$ can be determined from Theorem [5] thus next we need to determine the decomposition of $U^i(Z_{67})$.

Having $67 - 1 = 66 = 2 \times 3 \times 11$ thus we get

$$U^i(Z_{67}) \approx U^{i-1}(Z_{66}) \approx U^{i-1}(Z_{2})\times U^{i-1}(Z_{3})\times U^{i-1}(Z_{11}),$$

we get in this decomposition the Second Level of Pratt Tree (2, 3, 11). Next, we need the decomposition of $U^{i-1}(Z_{3})$ and $U^{i-1}(Z_{11})$. In the same manner, we get

$$U^{i-1}(Z_{3}) \approx U^{i-2}(Z_{2})$$

and

$$U^{i-1}(Z_{11}) \approx U^{i-2}(Z_{2}) \times U^{i-2}(Z_{5}).$$

This is Third Level in Pratt Tree (2) and (2, 5).

Finally with the last decomposition of

$$U^{i-2}(Z_{5}) \approx U^{i-3}(Z_{2})$$

giving Last Level of Pratt Tree that is (2).
As a consequence that all the decompositions will reach eventually to \( U^k(\mathbb{Z}_{269}) \) which is solved in Theorem 5. Thus the decomposition of \( U^k(\mathbb{Z}_n) \) can be obtained.

![Figure 1](image)

(A) Decomposition of \( U^k(\mathbb{Z}_{269}) \)  
(B) Pratt Tree of 269

**Figure 1.** Equivalence between the decomposition \( U^k(\mathbb{Z}_{269}) \) and Pratt Tree.

**REFERENCES**

[1] El-Kassar, A. N., & Chehade, H. Y. (2006). Generalized Group of Units. Mathematica Balkanica, New Series, 20, 275-286.
[2] Kadri, T, & El-Kassar, A. N. (2016). The third group of units of the ring \( \mathbb{Z}_n \), *JP Journal of Algebra, Number Theory & Applications*, 38(4) 385–413.
[3] Gallian, J. A. (2010). Contemporary Abstract Algebra: Student Solutions Manual. Brooks/Cole, Cengage Learning.
[4] Ligh, S., & Garcia, P. G. (1985). A generalization of Euler’s \( \phi \)-function, II. Math. Japon., 30, 519-522.
[5] Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). An introduction to the theory of numbers. John Wiley & Sons.
[6] Smith, J. L., & Gallian, J. A. (1985). Factoring finite factor rings. Mathematics Magazine, 58(2), 93–95.
[7] Pratt, V. R. (1975). Every prime has a succinct certificate. SIAM Journal on Computing, 4(3), 214-220.
[8] Ford, K., Konyagin, S. V., & Luca, F. (2010). Prime chains and Pratt trees. Geometric and Functional Analysis, 20(5), 1231-1258.
[9] Bayless, J. (2008). The Lucas-Pratt primality tree. Mathematics of computation, 77(261), 495-502.

**Therrar Kadri**  
Department of Pedagog, Lebanese University.  
*Email address: therrar.kadri@ul.edu.lb*

**Mohammad Elhindi**  
Department of Mathematics and Computer Science, Faculty of Science, Beirut Arab University, Beirut, Lebanon  
*Email address: mohammadyhind198@gmail.com*