مجلة جامعة الزاوية للعلوم الطبيعية
University of Zawia Journal of Natural Sciences *(UZJNS)*
https://journals.zu.edu.ly/index.php/UZJNS ISSN: 3078-4999
UZJNS

A Topological Space Defined on Finite Rings Modulo Composite Number

Hamza A Daoub[a]*

[a]*Department of Mathematics, Faculty of Sciences, University of Zawia, Zawia, Libya*
**Corresponding author:*
E-mail address: h.daoub@zu.edu.ly

Received 01 Dec 2024 | Accepted 09 Feb 2025 | Available online 15 Mar 2025 | DOI: 10.26629/uzjns.2025.01

A B S T R A C T

For a composite number $\boldsymbol{n}$, we explore a topological space on the ring of integers modulo $\boldsymbol{n}$, we use basis sets formed by solutions to quadratic residue equations, where elements are units modulo $\boldsymbol{n}$. This definition allows us to investigate the algebraic relationships among solutions, focusing on properties like clopen sets, closure, and interior operations. Additionally, we examine the continuity of mappings between the group of units in $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ and quadratic residues, alongside the quotient topology induced on this group of units. A comparison of the separation properties of these topological spaces is also presented.

Keywords: *Topological space, Quadratic residues, Finite rings, Quotient topology, Quotient topology, Modular arithmetic, Group of units.*

فضاء تبولوجي معرف على حلقات منتهية بمقياس عدد مركب

[a]حمزة داعوب

**قسم الرياضيات، كلية العلوم، جامعة الزاوية، الزاوية، ليبيا.*

الملخص

نستكشف فضاء طوبولوجي على حلقة الأعداد الصحيحة بمقياس عدد مركب $\boldsymbol{n}$، باستخدام مجموعات أساس مكونة من حلول معادلات البواقي التربيعية حيث تكون العناصر عبارة عن وحدات بمقياس $\boldsymbol{n}$. يسمح لنا هذا النهج بالتحقيق في العلاقات الجبرية بين الحلول، مع التركيز على خصائص مثل المجموعات المغلقة والمفتوحة، والغلاقة، والعمليات الداخلية. بالإضافة إلى ذلك، نفحص استمرارية الدوال بين زمرة الوحدات في $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ والبواقي التربيعية، إلى جانب طوبولوجيا القسمة على هذه المجموعة من الوحدات. يتم أيضًا تقديم مقارنة لخصائص الفصل لهذه المساحات الطوبولوجية، مع تسليط الضوء على التمييز في توافقها مع بديهيات الفصل الكلاسيكية.

الكلمات المفتاحية: *فضاء تبولوجي، بواقي تربيعية، مجموعات مغلقة ومفتوحة، تبولوجيا القسمة، مسلمات الفصل، الحساب المعياري.*

1. Introduction

The study of topologies on modular arithmetic structures, such as the ring of integers modulo n, has gained significant attention due to its applications in algebra, number theory, and computer science. Researchers have explored various topologies on $\mathbb{Z}_n$, revealing connections between algebraic structures and computational frameworks. Notably, the Zariski topology, introduced by Oscar Zariski, defines closed sets as the zeros of polynomial functions, offering a bridge between algebraic structures and geometric intuition [1]. Saeid Jafari, Sang-Eon Han, and Jeong Min Kang have examined alternative topologies for $\mathbb{Z}_n$, extending classical structures to quasi-discrete and Khalimsky-type topologies [2]. These innovations have provided new perspectives in digital geometry, fixed-point analysis, and homotopy theory, enriching our understanding of the interplay between topology and modular arithmetic. Quadratic residues play a central role in number theory, particularly in modular arithmetic and the distribution of prime numbers. These residues offer deep insights into the solvability of quadratic equations in modular systems, linking number theory with algebraic structures. When the modulus is composite, the complexity of these systems increases due to the intricate structure of $\mathbb{Z}_n$, making it an ideal candidate for exploring both algebraic and topological properties [3, 4].

In this context, our study focuses on the group of units in $\mathbb{Z}_n$, the set of elements coprime to n. This group is crucial in applications such as cryptography and coding theory, where understanding modular structures is essential [5]. Quadratic residues are significant in exploring multiplicative structures in modular arithmetic, influencing both theoretical and practical aspects of these fields [6].

We propose a new topological space defined on $U_n \subset \mathbb{Z}_n$, using solution sets of quadratic residue equations of the form $x^2 \equiv a \ (mod\ n)$, where a is a quadratic residue modulo n. The topology τ_n is defined using a basis derived from these solution sets, enabling a comprehensive exploration of the algebraic relationships among solutions. Through this definition, we provide new insights into the intersection of algebra and topology within modular arithmetic. We also analyze the fundamental properties of τ_n, including clopen sets, closure, and interior operations, to reveal the underlying algebraic structure. Additionally, we investigate continuous mappings from the group of units in $\mathbb{Z}_n$ to the group of quadratic residues, employing a quotient topology to explore separation properties. This approach highlights the distinct topological behaviors in these spaces, enhancing our understanding of modular arithmetic through a topological perspective [7, 8].

2. Preliminaries

In this section, we introduce key theorems and concepts in number theory, including polynomial congruences, and important results from modular arithmetic [9, 10, 11, 12, 13, 14]. These foundational ideas will help frame the subsequent discussions and applications related to quadratic residues and their behavior in modular arithmetic.

Definition 2.1 *If m is a positive integer, the Euler's totient function, denoted $\phi(m)$, represents the number of positive integers up to m that are relatively prime to m.*

Quadratic residues are essential in determining whether a quadratic equation has a solution for a given modulus, and their properties are closely linked to the distribution of prime numbers and modular structures.

Definition 2.2 *We say that an integer a is a quadratic residue of m if $(a, m) = 1$ and the congruence $x^2 \equiv a \ (mod\ m)$ has a solution. If the congruence $x^2 \equiv a \ (mod\ m)$ has no solution, then a is called a quadratic nonresidue of m.*

This distinction is essential, as knowing if a number is a quadratic residue reveals potential solutions to the corresponding quadratic congruence.

To explore the implications of quadratic residues, we first consider their distribution among the integers.

Theorem 2.1 *If p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p and $(p-1)/2$ quadratic nonresidues of p among the integers $1, 2, \dots, p-1$.*

Next, we explore the structure of quadratic residues in various modular systems, which can differ significantly based on the modulus used.

Lemma 2.1 *The number of quadratic residues in $\mathbb{Z}_{2^k}$ is 2^{k-3}.*

This result emphasizes how the structure of quadratic residues changes when considering powers of 2, contrasting with the behavior observed with odd primes.

Lemma 2.2 *The number of quadratic residues in $\mathbb{Z}_{p^k}$ where p is an odd prime is $\frac{p^k - p^{k-1}}{2}$.*

The general problem of solving quadratic congruences modulo a composite number can often be reduced to solving congruences modulo its prime power factors.

Theorem 2.2 *Let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Then the number a is a quadratic residue $mod\ n$ iff a is a square modulo each prime power divisor $p_i^{e_i}$ of n.*

To decide whether a number a is a square modulo n, it suffices to decide if a is a square modulo the prime power divisors of n. To do that we must consider separately the case where the prime is odd.

Theorem 2.3 *Let p be an odd prime, and $(a, p) = 1$. Then there is a solution of $x^2 \equiv a \ (mod\ p^e)$, $e > 1$, if and only if there is a solution of $x^2 \equiv a \ (mod\ p)$.*

To further explore the nature of solutions to quadratic congruences, we can turn to the characteristics of such solutions specifically in the case of odd primes.

Theorem 2.4 *Let p be an odd prime and a an integer not divisible by p. Then, the congruence $x^2 \equiv a \ (mod\ p)$ has either no solutions or exactly two incongruent solutions modulo p.*

In contrast, the case where the modulus is a power of 2 is a bit different.

Theorem 2.5 *Suppose a is odd. Then:*

a) For $k = 1$, there is exactly one solution.

b) For $k = 2$, there are exactly two solutions.

c) For $k = 3$, if $a \equiv 1 \pmod 8$, there are four solutions; otherwise, there are none.

This characterization of solutions helps to understand how quadratic congruences behave under different moduli, especially when factoring integers. For example, Fermat's factorization method uses integer representations as differences of squares, providing an efficient way to factor numbers. This principle can be extended to other factoring techniques.

Proposition 2.1 (Basic Factorization Principle) *Let n be a positive integer and let x and y be integers with $x^2 \equiv y^2 \pmod n$ but $x \equiv \pm y \pmod n$. Then $gcd(x - y, n)$ is a nontrivial factor of n (that is, the gcd is not 1 or n).*

This factorization principle offers key insights into the structure of quadratic congruence solutions, which are crucial in number theory. In quadratic residue graphs [15], vertices represent quadratic roots, with edges connecting those whose squares are congruent modulo n. Each graph component corresponds to a quadratic residue, providing a visual representation of the factorization methods and revealing relationships between residues in modular arithmetic.

In general topology, concepts like open, closed, and clopen sets, as well as closure and interior operations, are fundamental to understanding topological spaces [16, 17, 18]. For any topological space (X, τ), open sets belong to the topology τ, closed sets are their complements, and clopen sets are those that are both open and closed. In the context of $\mathbb{Z}_n$, these principles guide the study of solution sets of quadratic residues, which form a basis for the topology τ_n defined in this paper. Analyzing clopen sets, closure, and interior within τ_n provides insight into the algebraic structures underlying modular arithmetic.

3. Results

In previous research, particularly in [19], the topological space defined on the group of integers modulo a prime number p has been studied, establishing key properties and behaviors. Drawing from this foundational work, we now concentrate on the more complex case of composite numbers n. In this section, we present our findings on the topological space τ_n defined on U_n, exploring the unique characteristics and algebraic relationships that arise when n is composite.

To investigate the properties of the defined topological space τ_n, it is essential to consider the various cases arising from the factorization of n. Specifically, the structure of n as a product of prime powers can significantly influence the characteristics of τ_n. Each case whether n is a prime, a power of a prime, or a product of distinct primes presents unique topological features and implications.

***Case* 1:** *$n = 2^k$, where k is a positive integer greater than or equal to 1.*

In this case, we explore the structure of the topological space (U_{2^k}, τ_{2^k}). A key feature of this space involves the solutions of the quadratic congruence $x^2 \equiv a \pmod{2^k}$, which for $k \geq 4$, always has exactly four solutions $\{x, 2^k - x, y, 2^k - y\}$. The cardinality of the set of quadratic residues, which is fundamental in defining the space, is expressed as 2^{k-3}.

The quadratic residues in this setting generate a graph structure, where each residue is connected to four elements, leading to a graph represented by $2^{k-3}K_4$. This graph captures essential information about the basis $\mathcal{B}$ and offers insight into the properties of the quadratic residue class system within the topological space (U_{2^k}, τ_{2^k}).

Proposition 3.1 *Let (U_n, τ_n) be a topological space, then:*

1. *If $n = 2$, then τ_n is trivial.*
2. *If $n = 2^2$, then τ_n is trivial.*
3. *If $n = 2^3$, then τ_n trivial.*
4. *If $n = 2^k$, where $k \geq 4$ is any positive integer, then τ_n has a basis $\{\{x_i, n - x_i, y_i, n - y_i\}\}_{i=1}^{2^{k-3}}$.*

Proof: (1) Based on the definition of the basis, the topological space (U_n, τ_n) is trivial.

In assertions (2) and (3) the only open sets are $\{1,3\} \in \tau_{2^2}$, and $\{1,3,5,7\} \in \tau_{2^3}$, which are U_4, and U_8 respectively. Therefore, τ_4 and τ_8 are trivial.

(4) Suppose that $n = 2^k$, with a positive integer $k \geq 4$, and $\mathcal{B}$ is the basis of the topological space (U_n, τ_n). Since for any quadratic residue $a \in U_n$, there are four solutions of the quadratic congruence $x^2 \equiv a \pmod n$. Therefore, every element $B_i \in \mathcal{B}$ consists of four unit elements $\{x_i, n - x_i, y_i, n - y_i\}$. Given that $\#(U_n) \geq 8$ and divisible by four, it follows from Lemma 2.1, that $\mathcal{B}$ consists of all open sets $\{\{x_i, n - x_i, y_i, n - y_i\}\}_{i=1}^{2^{k-3}}$. ■

Proposition 3.2 *Let k be any positive integer, and let (U_{2^k}, τ_{2^k}) be a topological space. For any $V \in \tau_{2^k}$ then the set V is a clopen.*

Before proceeding with the proof, note that for $k \leq$

3, the topology τ_{2^k} is trivial, making the proof straightforward. Therefore, in the ***case 1***, we focus on $k \geq 4$. By definition, the basis elements of the topology τ_{2^k} are of the form $B_i = \{x_i, 2^k - x_i, y_i, 2^k - y_i\}$, where $i = 1, 2, \dots, 2^{k-3}$, and these are open sets. If $V \subseteq U_{2^k}$ is any set that can be expressed as a union of basis elements, it means that V is an open set.

We call the solutions of the congruence equation $x^2 \equiv a \pmod n$, apart from a given root x_j, the *co-solutions* of x_j, which together form a basis element.

Proof:

To prove that V is closed, we must show that its complement $U_{2^k} - V$ is open. Suppose $x_i \in U_{2^k} - V$. Then its additive inverse $2^k - x_i$ and all co-solutions do not belong to V. If this were not the case, V would not be open. Thus, we can find a basis element $B_i = \{x_i, 2^k - x_i, y_i, 2^k - y_i\}$ contains x_i and its all co-solutions such that $B_i \subset U_{2^k} - V$. Therefore, for every point $x_i \in U_{2^k} - V$, we can find a basis element B_i contained in $U_{2^k} - V$, meaning that $U_{2^k} - V$ is open. Consequently, V is closed. ■

Proposition 3.3 *Let A be a subset of U_{2^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r < \phi(2^k)$.*

1. *If there exists an index j, where $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$, then $A^\circ = \bigcup_{i \neq j} B_i$, where $B_i \subset A$.*
2. *If for all $1 \leq j \leq r$, we have $x_j \in A$ and $2^k - x_j \notin A$, then $A^\circ = \phi$.*

Proof: **(1)** By definition, the interior A° of a set A is defined as the largest open set entirely contained within A. Thus, A° includes all points $x \in A$ for which there exists an open set $V \in \tau_{2^k}$ such that $x \in V \subseteq A$.

In the topology τ_{2^k}, each basis element has the form $B_i = \{x_i, 2^k - x_i, y_i, 2^k - y_i\}$, where $x_i, 2^k - x_i, y_i, 2^k - y_i \in U_{2^k}$ for each i. If there exists an element $x_j \in A$ but $2^k - x_j \notin A$, then the smallest open set B_j containing x_j cannot be entirely contained within A due to the absence of $2^k - x_j$. This implies that x_j and its co-solutions cannot be interior points of A. Consequently, for any $x_i \in A$ that is an interior point of A, we have $x_i \in B_i \subset A$. Therefore, the interior of A is given by $A^\circ = \bigcup_{i \neq j} B_i$.

(2) Suppose that $x_j \in A$ and $2^k - x_j \notin A$ for all $1 \leq j \leq r$. Then, the basis element B_j is open set containing x_j, and cannot be entirely contained in A, which implies that x_j is not an interior point of A for all j. Thus, $A^\circ = \phi$. ■

Remark 3.1 *In the Proposition 3.3:*

(1) *if for every j, with $1 \leq j \leq r$, both $x_j \in A$ and $2^k - x_j \in A$, and $\#(A) \nmid \phi(2^k)$, then some of the co-solutions $\{y_j, 2^k - y_j\} \subset B_j$ are missing for some j. Thus, the basis element, which represents this solution cannot be contained in A. Consequently, the interior of A is $A - (\bigcup_j B_j)$, for some j.*

(2) *If $\#(A) \leq 3$, then at least one co-solution is missing from A. This implies that there is no open set containing any point from A that can be entirely included within A. Consequently, $A^\circ = \emptyset$..*

Example 3.1 In the ring $\mathbb{Z}_{16}$, the group of units $U_{16} = \{1,3,5,7,9,11,13,15\}$, Let $A = \{1,3,5,11,13,15\}$. The basis elements in τ_{16} are $B_1 = \{3,5,11,13\}$, $B_2 = \{1,7,9,15\}$, and $\tau_{16} = \{\phi, U_{16}, \{3,5,11,13\}, \{1,7,9,15\}\}$. We observe that B_2 is the only open set containing $\{1, 15\}$, which is not included in A. Hence, $A^\circ = B_1$.

Proposition 3.4 *Let A be any subset of U_{2^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r < \phi(2^k)$. Then:*

1. *If there exists an index j, with $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$, then A' is:*

$$A' = A^\circ \cup \begin{cases} \bigcup_j (B_j - \{x_j\}) & y_j, 2^k - y_j \notin A \\ \bigcup_j B_j & y_j \text{ or } 2^k - y_j \in A \end{cases}$$

2. *If for every j, with $1 \leq j \leq r$, both $x_j \in A$ and $2^k - x_j \in A$, then*

$$A' = \bigcup_{j=1}^{r} B_j .$$

Clarifying before the proof, $\bigcup_j B_j$ denotes the union of basis elements that include x_j for specific indices j meeting the given condition.

***Proof*: (1)** Suppose that there exists an index j, with $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$. The smallest open set B_j contains x_j, $2^k - x_j$, and the co-solutions $\{y_j, 2^k - y_j\}$.

We examine the accumulation points by considering the intersections of A with various open sets excluding certain elements:

$$A \cap (B_j - \{x_j\}) = \begin{cases} \phi & y_j, 2^k - y_j \notin A \\ y_j & y_j \in A \\ 2^k - y_j & 2^k - y_j \in A \\ D_j & \{y_j, 2^k - y_j\} \subset A \end{cases}$$

$$A \cap \left(B_j - \{2^k - x_j\}\right) = \begin{cases} x_j & y_j, 2^k - y_j \notin A \\ \{x_j, y_j\} & y_j \in A \\ \{x_j, 2^k - y_j\} & 2^k - y_j \in A \\ \{x_j, y_j, 2^k - y_j\} & \{y_j, 2^k - y_j\} \subset A \end{cases}$$

$$A \cap \left(B_j - \{y_j\}\right) = \begin{cases} x_j & y_j, 2^k - y_j \notin A \\ x_j & y_j \in A \\ \{x_j, 2^k - y_j\} & 2^k - y_j \in A \\ \{x_j, 2^k - y_j\} & \{y_j, 2^k - y_j\} \subset A \end{cases}$$

$$A \cap \left(B_j - \{2^k - y_j\}\right) = \begin{cases} x_j & y_j, 2^k - y_j \notin A \\ \{x_j, y_j\} & y_j \in A \\ x_j & 2^k - y_j \in A \\ \{x_j, y_j\} & D_j \subset A \end{cases}$$

In all cases, $2^k - x_j$ is an accumulation point of A. If neither y_j nor $2^k - y_j$ is in A, then x_j can not be an accumulation point of A. However, if one element of the pair $\{y_j, 2^k - y_j\}$ is in A, then $x_j, y_j, 2^k - x_j$, and $2^k - y_j$ are all accumulation points of A. Furthermore, every $x_i \in B_i \subset A$ is an accumulation point A', because, $A \cap (B_i - \{x_i\}) \neq \phi$. Therefore, the set of accumulation points A' is:

$$A' = A^{\circ} \cup \begin{cases} \bigcup_j \left(B_j - \{x_j\}\right) & y_j, 2^k - y_j \notin A \\ \bigcup_j B_j & y_j \text{ or } 2^k - y_j \in A \end{cases}$$

(2) Suppose that for all j, with $1 \leq j \leq r$, we have that $x_j \in A$ and $2^k - x_j \in A$. We determine the accumulation points by examining the intersections of A with open sets excluding certain elements:

1. $A \cap \left(B_j - \{x_j\}\right) \neq \phi$,
2. $A \cap \left(B_j - \{2^k - x_j\}\right) \neq \phi$,
3. $A \cap \left(B_j - \{y_j\}\right) \neq \phi$,
4. $A \cap \left(B_j - \{2^k - y_j\}\right) \neq \phi$.

Since all of these intersections are nonempty, every basis element B_j contributes points to the accumulation set. Since every $x_i \in B_i \subset A$ is an accumulation point A'. Thus, the set of accumulation points A' is:

$$A' = \bigcup_{j=1}^{r} B_j \ . \blacksquare$$

Proposition 3.5 *Let A be any subset of U_{2^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r < \phi(2^k)$. If there exists an index j, with $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$, then $\bar{A} = A \cup \left(\bigcup_j B_j\right)$*

Proof: By definition, the closure $\bar{A}$ of a set A is the smallest closed set that contains A. Suppose there exists an index j such that $1 \leq j \leq r$, with $x_j \in A$ but $2^k - x_j \notin A$. This indicates that A is not closed, as the complement of A is not open. To ensure A is closed, we must extend it by including the basis elements that contain x_j and its co-solutions, specifically the set $\bigcup_j B_j$ for some j. Consequently, the closure can be expressed as

$$\bar{A} = A \cup \left(\bigcup_j B_j\right)$$

Thus, the proof is established. ■

Proposition 3.6 *Let A be any subset of U_{2^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r < \phi(2^k)$. Then:*

1. *If there exists an index j, with $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$, then $b(A) = \bigcup_j B_j$.*
2. *If A is open, then $b(A) = \emptyset$.*

Proof: **(1)** Suppose there exists an index j, with $1 \leq j \leq r$, such that $x_j \in A$ but $2^k - x_j \notin A$. The basis element $B_j = \{x_j, 2^k - x_j, y_j, 2^k - y_j\}$ is the smallest open set containing x_j. By definition, the boundary of a set A consists of all points x_j in the space U_{2^k} such that every open set containing x_j intersects both A and its complement $U_{2^k} - A$. We examine the intersections for boundary points as follows:

$$A \cap B_j = \begin{cases} x_j & y_j, 2^k - y_j \notin A \\ \{x_j, y_j\} & y_j \in A \\ \{x_j, 2^k - y_j\} & 2^k - y_j \in A \\ \{x_j, y_j, 2^k - y_j\} & D_j \subset A \end{cases}$$

$$\left(U_{2^k} - A\right) \cap B_j = \begin{cases} 2^k - x_j & y_j, 2^k - y_j \notin A \\ \{2^k - x_j, y_j\} & y_j \in A \\ \{2^k - x_j, 2^k - y_j\} & 2^k - y_j \in A \\ \{2^k - x_j, y_j, 2^k - y_j\} & D_j \subset A \end{cases}$$

In both cases, the intersection between A and B_j, as well as the intersection between $U_{2^k} - A$ and B_j, is a non-empty set. Therefore, each B_j contributes points to the boundary of A. Thus, the set of boundary points is:

$$b(A) = \bigcup_j B_j \text{ for some } j.$$

(2) Now, consider that A is open. In this case, the basis element B_j is entirely contained within A. Thus, we have that $A \cap B_j = B_j$ and $\left(U_{2^k} - A\right) \cap B_j = \phi$. As a result, no points in B_j lie on the boundary of A, because no open set containing x_j intersects both A and its complement. Therefore, the

boundary of A is empty. ■

Case 2: *$n = p^k$ where p is an odd prime and $k \geq 2$ is a positive integer.*

In this case, we explore the structure of the topological space (U_{p^k}, τ_{p^k}). A key aspect of this space is related to the solutions of the quadratic congruence $x^2 \equiv a \ (mod\ p^k)$, which always has exactly two solutions. The cardinal number of the set of quadratic residues, which plays a fundamental role in defining the space, is given by $\frac{p^{k-1}(p-1)}{2}$.

We define the topological space (U_{p^k}, τ_{p^k}) using a basis $\mathcal{B}$, consisting of sets of the form $\{x^2 \equiv a \ (mod\ p^k), a \in U_{p^k}\} = \{x, p^k - x\}$, where $x \in U_{p^k}$. The quadratic residues in this setting form a graph structure, where each residue is connected to two elements, leading to a graph represented by $\frac{p^{k-1}(p-1)}{2} K_2$.

Proposition 3.7 *Let (U_{p^k}, τ_{p^k}) be a topological space, if $V \in \tau_{p^k}$ then V is a clopen set.*

Proof: In the topological space (U_{p^k}, τ_{p^k}), every basis element $B_i = \{ x_i, p^k - x_i \}$ is an open set. Let $V \in \tau_{p^k}$, then V is a union of basis elements, which is an open set. To prove that V is closed, we will demonstrate that its complement $U_{p^k} - V$, is open.

Consider any element $x_i \in U_{p^k} - V$. Since $x_i \notin V$, its pair $p^k - x_i$ also does not belong to V. For each $x_i \in U_{p^k} - V$, we can construct a basis element $\{ x_i, p^k - x_i \}$, which is contained in $U_{p^k} - V$. Consequently, $U_{p^k} - V$ can be expressed as a union of basis elements. Confirming that $U_{p^k} - V$ is open. Therefore, V is closed. ■

Proposition 3.8 *Let A be any subset of U_{p^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r \leq \phi(n)$, then:*

1. *If $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \leq j \leq r$, then $A^\circ = A - (\cup_j \{x_j\})$.*
2. *If $x_j \in A$ and $p^k - x_j \in A$ for all $1 \leq j \leq r$, then $A^\circ = A$.*
3. *If $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \leq j \leq r$, then $A^\circ = \phi$.*

Proof: **(1)** Assume that $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \leq j \leq r$. In this topology, each basis element B_j contains exactly two-unit elements $\{x_j, p^k - x_j\}$. If x_j belongs to the interior A°, then the open set B_j must be entirely contained in A, implying that both x_j and $p^k - x_j$ are in A. However, since $p^k - x_j \notin A$, the set $\{x_j, p^k - x_j\}$ cannot be fully contained in A, contradicting the condition for $x_j \in A^\circ$. Therefore, we conclude that $A^\circ = A - (\cup_j \{x_j\})$.

(2) Assume that for each $1 \leq j \leq r$, both $x_j \in A$ and $p^k - x_j \in A$. This implies that for every element $x_j \in A$, there exists a unique complement $p^k - x_j$, and the elements of A can be grouped into pairs of the form $B_j = \{x_j, p^k - x_j\}$.

By the definition of the basis in this topology, each B_j contains exactly two elements and forms an open set entirely contained within A. Thus, every $x_j \in A$ is an interior point of A. Since this condition holds for all $x_j \in A$, it follows that the interior of A is equal to A. ■

Proposition 3.9 *Let A be any subset of U_{p^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \leq r < \phi(p^k)$. Then:*

1. *If $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \leq j \leq r$, then $A' = A^\circ \cup (\cup_j \{p^k - x_j\})$.*
2. *If $x_j \in A$ and $p^k - x_j \in A$ for all $1 \leq j \leq r$, then $A' = A$.*
3. *If $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \leq j \leq r$, then $A' = \cup_{j=1}^{r} \{p^k - x_j\}$.*

Proof: **(1)** Assume that $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \leq j \leq r$. In the topology (U_{p^k}, τ_{p^k}), the set $B_j = \{x_j, p^k - x_j\}$ is the smallest open set containing x_j. Since $p^k - x_j \notin A$, then $A \cap (B_j - \{p^k - x_j\}) = \{x_j\} \neq \phi$. It follows that $p^k - x_j$ is an accumulation point of A. While x_j is not an accumulation point of A, because of $A \cap (B_j - \{x_j\}) = \phi$. Moreover, all points in A° are accumulation points of A. Hence, $A' = A^\circ \cup (\cup_j \{p^k - x_j\})$.

(2) Assume $x_j \in A$ and $p^k - x_j \in A$ for all $1 \leq j \leq r$, This implies that $B_j \subset A$ for all $1 \leq j \leq r$, which by definition, means that A is an open set.

Since A is open, any accumulation point y can not be in $U_{p^k} - A$, because for any open set $V \subset U_{p^k}$ containing y, we have $A \cap (V - \{y\}) = \emptyset$.

Therefore, for each x_i in A, the open set B_i satisfies $A \cap (B_i - \{x_i\}) \neq \emptyset$. This shows that every point in A can be an accumulation point. Consequently, the set of accumulation points $A' = A$.

(3) Assume $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \leq j \leq r$. In this case, x_j cannot be an accumulation point of A because, for each open set B_j containing x_j, we have $A \cap (B_j - \{x_j\}) = \emptyset$.

On the other hand, $p^k - x_j$ is an accumulation point of A, since $A \cap (B_j - \{x_j\}) = \{x_j\} \neq \emptyset$. Thus, the

set of accumulation point $A' = \bigcup_{j=1}^{r}\{p^k - x_j\}$ ■

Proposition 3.10 *Let A be any subset of U_{p^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(p^k)$ then:*

1. *If $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \le j \le r$, then $\bar{A} = A \cup \left(\bigcup_j \{p^k - x_j\}\right)$.*
2. *If $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \le j \le r$, then $\bar{A} = A \cup \left(\bigcup_{j=1}^{r}\{p^k - x_j\}\right)$.*
3. *If $x_j \in A$ and $p^k - x_j \in A$ for all $1 \le j \le r$, then $\bar{A} = A$*

Proof: **(1)** Given $A = \{x_1, x_2, \dots, x_k\}$, assume that $x_j \in A$, and $p^k - x_j \notin A$ for some $1 \le j \le r$. By Proposition 3.9, the set of accumulation points of A is given by $A' = A^{\circ} \cup \left(\bigcup_j \{p^k - x_j\}\right)$. The closure of A is the union of A and its accumulation points A'. Therefore, we have:

$$\bar{A} = A \cup A' = A \cup \left(\bigcup_j \{p^k - x_j\}\right).$$

(2) Suppose that $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \le j \le r$. By Proposition 3.9, we have

$$\bar{A} = A \cup \left(\bigcup_{j=1}^{r} \{p^k - x_j\}\right).$$

(3) Given that each $1 \le j \le r$, both x_j and its complement $p^k - x_j$ are included in A, it follows that the set $B_j = \{x_j, p^k - x_j\} \subseteq A$, for each j. Thus A can be expressed as the union of these basis elements, which form an open set. By Proposition 3.7 we conclude that A is also closed. Therefore, the closure of A, is equal to A, i.e., $\bar{A} = A$. ■

Proposition 3.11 *Let A be any subset of U_{p^k} such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(p^k)$ then:*

1. *If $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \le j \le r$, then $b(A) = \bigcup_j B_j$.*
2. *If $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \le j \le r$, then $b(A) = \bigcup_{j=1}^{r} B_j$*
3. *If $x_j \in A$ and $p^k - x_j \in A$ for all $1 \le j \le r$, then $b(A) = \emptyset$.*

Proof: **(1)** Suppose that $x_j \in A$ and $p^k - x_j \notin A$ for some $1 \le j \le r$. The smallest open set containing x_j is B_j, which satisfies the following:

x_j is a boundary point of A, because $A \cap B_j = \{x_j\} \neq \phi$ and $\left(U_{p^k} - A\right) \cap B_j = \{p^k - x_j\} \neq \phi$.

Similarly, $p^k - x_j$ is a boundary point of A. Consequently, the boundary of A is given by $b(A) = \bigcup_j B_j$.

(2) Suppose that $x_j \in A$ and $p^k - x_j \notin A$ for all $1 \le j \le r$. In this case, x_j and $p^k - x_j$ are boundary points of A for all j. Because $A \cap B_j = \{x_j\} \neq \phi$ and $\left(U_{p^k} - A\right) \cap B_j = \{p^k - x_j\} \neq \phi$. Thus,

$$b(A) = \bigcup_{j=1}^{r} B_j$$

(3) Now, suppose $x_j \in A$ and $p^k - x_j \in A$ for all $1 \le j \le r$. This implies that A is open, meaning all points in A are interior points. For any open set B_j containing x_j, it follows that $A \cap \mathrm{B_j} = \{x_j, p^k - x_j\} \neq \phi$ and $\left(U_{p^k} - A\right) \cap \mathrm{V} = \phi$. Therefore, no points of A can be boundary points, and we conclude that $b(A) = \emptyset$. ■

Case 3: *$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd prime numbers.*

In this case, we explore the structure of the topological space (U_n, τ_n), where $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, with p being an odd prime and r being a positive integer. The topological space (U_n, τ_n) is defined using a basis $\mathcal{B}$, which consists of sets of the form $\{x^2 \equiv a \pmod n \mid a \in U_n\}$, where $x \in U_n$, and each set B_i contains 2^{r-1} pairs of solutions.

A key aspect of this space is related to the solutions of the quadratic congruence $x^2 \equiv a \pmod n$, which always has exactly 2^r solutions. The cardinality of the set of quadratic residues is given by $\frac{\phi(n)}{2^r}$.

In this context, the quadratic residues form a graph structure, where each residue is connected to 2^r elements, resulting in a graph represented by $\frac{\phi(n)}{2^r} K_{2^r}$. This graph provides crucial insight into the basis $\mathcal{B}$ and helps elucidate the properties of the quadratic residue class system within the topological space (U_n, τ_n).

Proposition 3.12 *Let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct odd primes, and (U_n, τ_n) be a topological space, if $V \in \tau_n$ then V is a clopen set.*

Proof: In the topological space (U_n, τ_n), every basis element $\{x_1, n - x_1, x_2, n - x_2, \dots, x_{2^{r-1}}, n - x_{2^{r-1}}\}$ is an open set. Let $V \in \tau_n$ be any open set. To show that V is closed, we will prove that its complement $U_n - V$, is open.

Consider any element $y_i \in U_n - V$. Since $y_i \notin V$, its co-solutions also do not belong to V. For each $y_i \in U_n - V$, we can find a basis element B_i containing y_i and its co-solutions (elements correspond to solutions of the quadratic congruence $x^2 \equiv y_i^2 \pmod n$). It satisfies $V \cap B_i = \phi$, since no

element from B_i is in V. Consequently, for every $y_i \in U_n - V$ there exists a basis element B_i contained within $U_n - V$, confirming that $U_n - V$ is open. Therefore, V is closed. ■

Proposition 3.13 *Let A be any subset of U_n such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(n)$. If $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$, then $A^\circ = \bigcup_{i \ne j} B_i$, where $B_i \subset A$.*

Proof: Assume $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$. Since each basis element in τ_n contains x_j has the form $B_j = \{x_1, n - x_1, x_2, n - x_2, \dots, x_{2^{r-1}}, n - x_{2^{r-1}}\}$. For x_j to belong to the interior A°, the open set B_j that containing x_j must be entirely contained in A, meaning both x_j and $n - x_j$ must lie within A. However, since we are given that $n - x_j \notin A$, it follows that B_j cannot be fully contained in A, which means x_j is not an interior point of A. Therefore, for a point $x_i \in A$, to be an interior point of A, then all its co-solutions lie in A. This implies that $x_i \in B_i \subset A$. We conclude that $A^\circ = \bigcup_{i \ne j} B_i$. ■

Remark 3.2 *In Proposition 3.13*:

(1) *If $x_j \in A$ and $n - x_j \notin A$ for all $1 \le j \le r$, then $A^\circ = \emptyset$. Because the basis element B_j can not be contained in A.*

(2) *If $x_j \in A$ and $n - x_j \in A$ for all $1 \le j \le r$, and $2^{r-1} \nmid \#(A)$ then $A^\circ = \bigcup_i B_i$, for each $x_i \in B_i \subseteq A$.*

Proposition 3.14 *Let A be any subset of U_n such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(n)$. If $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$, then*

$$A' = A^\circ \cup \begin{cases} \bigcup_j (B_j - \{x_j\}) & A \cap B_j = \{x_j\} \\ \bigcup_j B_j & \#(A \cap B_j) > 1 \end{cases}$$

Proof: Assume $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$. In the topology (U_n, τ_n), the basis element $B_j = \{x_1, n - x_1, x_2, n - x_2, \dots, x_{2^{r-1}}, n - x_{2^{r-1}}\}$ is the smallest open set containing x_j. Since $A \cap (B_j - \{n - x_j\}) = \{x_j\} \ne \phi$, it follows that $n - x_j$ must be an accumulation point of A. If none of the co-solutions of x_j are in A then x_j cannot be an accumulation point of A, because $A \cap (B_j - \{x_j\}) = \phi$. As usual, each $x_i \in A^\circ$ is an accumulation point of A. Thus, we have $A' = A^\circ \cup (\bigcup_j (B_j - \{x_j\}))$.
On the other hand, if some co-solutions of x_j are in A, then x_j can be an accumulation point of A because $A \cap (B_j - \{x_j\}) \ne \phi$. In this case, we have $A' = A^\circ \cup (\bigcup_j B_j)$. ■

Proposition 3.15 *Let A be any subset of U_n such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(n)$. If $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$, then $b(A) = \bigcup_j B_j$.*

Proof: Suppose that $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$. The smallest open set containing x_j is B_j. Within this open set, consider any element $y \in B_j$, We observe the following:

- $A \cap B_j \ne \phi$, because of $x_i \in A \cap B_j$.
- Similarly, $(U_n - A) \cap B_j \ne \phi$, because, $n - x_j \in (U_n - A) \cap B_j$.

These observations imply that B_j contains points from both A and $U_n - A$. As a result, every $y \in B_j$ satisfies the condition of being a boundary point of A. Since this holds for all such basis elements, the boundary of A is given by $b(A) = \bigcup_j B_j$. ■

Proposition 3.16 *Let A be any subset of U_n such that $A = \{x_1, x_2, \dots, x_r\}$, where $1 \le r < \phi(n)$. If $x_j \in A$ and $n - x_j \notin A$ for some $1 \le j \le r$, then $\bar{A} = A \cup (\bigcup_j B_j)$.*

Proof: Given $A = \{x_1, x_2, \dots, x_k\}$, assume that $x_j \in A$, and $n - x_j \notin A$ for some $1 \le j \le r$. Consider the open set B_j containing x_j.

- If $A \cap B_j = \{x_j\}$, then by Proposition 3.14, the set of accumulation points of A is given by $A' = A^\circ \cup (\bigcup_j (B_j - \{x_j\}))$.
- Otherwise, if the intersection $A \cap B_j$ contains more elements, then the set of accumulation points becomes $A' = A^\circ \cup (\bigcup_j B_j)$.

The closure of A is the union of A and its accumulation points A'. Since $x_j \in A$, it follows that:

$$\bar{A} = A \cup (\bigcup_j B_j). \blacksquare$$

Case 4: *$n = 2^k p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct odd primes and k is any positive integer.*

In this case, we examine the structure of the topological space (U_n, τ_n), defined for $n = 2^k p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, with p_i being distinct odd primes, and k and r are positive integers. The topology (U_n, τ_n) utilizes a basis $\mathcal{B}$, consisting of sets of the form $\{x^2 \equiv a \pmod n \mid a \in U_n\}$, where $x \in U_n$.

The cardinality of each base element B is influenced by the positive integer k as follows:

- If $k = 0$, or 1, then $\#(B) = 2^r$.

- If $k = 2$, then $\#(B) = 2^{r+1}$.
- If $k \geq 3$, then $\#(B) = 2^{r+2}$.

A fundamental aspect of this topological space is the solutions to the quadratic congruence $x^2 \equiv a \pmod{n}$, with number of solutions depending on the value of k. Consequently, the cardinality of the set of quadratic residues varies accordingly.
In this context, the quadratic residues form a graph structure that provides valuable insights into the organization of the basis $\mathcal{B}$ and reveals key properties of the quadratic residue classes within the topological space.

To analyze the properties of the topological space (U_n, τ_n), it is essential to consider how the variation in the integer k influences the results. Specifically, for $k = 0$ or $k = 1$, the outcomes are consistent with those observed in cases where $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. When $k = 2$, the number of solutions increases by two, while the propositions can be proven similarly. For $k \geq 3$, the number of solutions increases by an additional two solutions, where the propositions and proofs remain applicable in the same manner.

For any composite number n, the topological space (U_n, τ_n) defined by the basis $\mathcal{B}$ satisfies the following:

1. *The topological space (U_n, τ_n) is not T_0 space.*

To show that, consider the points x_j and $n - x_j$ in U_n. The only open set that contains both points is $B_j = \{x_1, n - x_1, x_2, n - x_2, \dots, x_j, n - x_j, \dots, x_r, n - x_r\}$ for some positive integer r, where $x_i^2 \equiv x_j^2 \pmod{n}$ for all $x_i, x_j \in B_j$. Therefore, there are no open sets that can contain one of these points while excluding the other. Thus, we conclude that τ_n is not T_0.

2. *The topological space (U_n, τ_n) is disconnected space.*

To determine that, consider the open sets:

$$V = B_1 = \{x_1, n - x_1, x_2, n - x_2, \dots, x_r, n - x_r\}$$

$$W = \bigcup_{i \neq 1} B_i$$

Since x_i is distinct for each $1 \leq i \leq \#(U_n)$ then V and W are disjoint; that is $V \cap W = \emptyset$. Therefore, τ_n is disconnected.

3. *The topological space (U_n, τ_n) is a compact space.*

To show that (U_n, τ_n) is a compact space, we verify that every open cover of U_n has a finite subcover. Since U_n is a finite set by definition, any open cover of U_n must also consist of a finite collection of basis elements that fully cover U_n. Therefore, it is always possible to select a finite subcollection of these open sets to cover U_n, confirming that (U_n, τ_n) is indeed compact.

4. *The topological space (U_n, τ_n) is a Lindelöf space.*

Since (U_n, τ_n) is finite, every open cover trivially has a countable subcover, confirming that (U_n, τ_n) is indeed Lindelöf.

5. *The topological space (U_n, τ_n) is a regular space.*

To show that (U_n, τ_n) is a regular space, consider any closed set $F = B_j \subseteq U_n$, where B_j is open and closed (clopen) and disjoint from all other basis elements. Let $x \in V = U_n - F = \bigcup_{i \neq j} B_i$.
Since B_i is clopen and $x \in V$, we can construct disjoint open sets U and V such that $F \subseteq B_j = U$ and $x \in V$. This guarantees that for any closed set and a point outside it, we can find disjoint open neighborhoods, confirming that (U_n, τ_n) is a regular space.
To further explore the topological space (U_n, τ_n), we define a related space based on the set of quadratic residues modulo n. By assigning this set with a discrete topology, we gain a finer understanding of the structure of quadratic residues within (U_n, τ_n).

Definition 3.2 *Let $Q_n = \{q_1, q_2, \dots, q_s\}$ be the set of all quadratic residues in U_n, and $P(Q_n)$ be the power set of Q_n, then $\tau_Q = P(Q_n)$ defines a topology on Q_n.*

The topology τ_Q is a discrete topology on the group of quadratic residues modulo a composite n. In this topology, every subset of Q_n is an open set. This discrete structure offers a highly detailed perspective, enabling precise analysis of each element within the group. While both τ_Q and τ_n are topologies associated with the composite number n and involve modular arithmetic, they differ in significant ways. They are defined on distinct sets, have different bases, and generate unique classes of open sets.
Each basis element $B_i \in \mathcal{B}$ in τ_n corresponds to a quadratic residue $a \in Q_n$. This relationship allows us to define a function between the topological spaces (U_n, τ_n) and (Q_n, τ_Q) as follows:

$$f(x) = x^2, \quad x \in U_n .$$

The function f maps roots of the quadratic

polynomial $x^2 \equiv a \ (mod\ n)$ to the quadratic residue $a \in Q_n$, which implies that each basis element B_i in τ_n is mapped to a corresponding quadratic residue a in Q_n.

Example 3.2 Let $n = 30$ then $U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$, $Q_{30} = \{1,19\}$ and

$$\tau_Q = \{\emptyset, Q_{30}, \{1\}, \{19\}\}$$

We have only two element bases

$$B_1 = \{1,11,19,29\}, B_2 = \{7,13,17,23\}$$

so

$$\tau_{30} = \{\emptyset, U_{30}, \{1,11,19,29\}, \{7,13,17,23\}\},$$

and $f: (U_{30}, \tau_{30}) \rightarrow (Q_{30}, \tau_Q)$ will be as

$f(1) = 1, f(7) = 19, f(11) = 1, f(13) = 19,$
$f(17) = 19, f(19) = 1, f(23) = 19, f(29) = 1.$

Therefore, we have $B_1 \mapsto \{1\}$, $B_2 \mapsto \{19\}$, which correspond to the basis of the topology τ_p and τ_Q respectively.

The function $f: U_n \rightarrow Q_n$, establishes a topological connection between these spaces. As shown in **Example 2.2**, this mapping preserves key structural properties, effectively connecting the topologies of U_n and Q_n. We now analyze the continuity of f and explore its impact on the topological structures of both U_n and Q_n, starting with the following proposition.

Proposition 3.17 *The function* $f: (U_n, \tau_n) \rightarrow (Q_n, \tau_Q)$ *is continuous.*

Proof: Define $f: U_n \rightarrow Q_n$ by $f(x) = x^2$ for $x \in U_n$, where Q_n consists of all quadratic residues modulo n. To establish continuity, we show that the preimage of every open set in $Q_n$is an open set in U_n. Since τ_Q is a discrete topology, every subset of Q_n is clopen. Let $V = f(U) \subseteq Q_n$ be an open set in Q_n for some $U \subset U_n$. The set $U = \{x \in U_n: x^2 \in V\}$ contains all elements in U_n whose squares are in V. For each $a \in V$, the set $\{x \in U_n: x^2 \equiv a\ mod(n)\}$ corresponds to a basis element $B \in \mathcal{B}$. Thus, $U = f^{-1}(V)$ can be expressed as a union of these basis elements, which are open in U_n. Therefore, f is continuous. ■

Since f is continuous and every open set in both topological spaces (U_n, τ_n) and (Q_n, τ_Q) is also closed, we arrive at the following.

Corollary 3.1 *The function* $f: (U_n, \tau_n) \rightarrow (Q_n, \tau_Q)$ *is open.*

Corollary 3.2 *The function* $f: (U_n, \tau_n) \rightarrow (Q_n, \tau_Q)$ *is closed.*

Remark 3.3 *For any composite number* n*, the topological space* (Q_n, τ_Q) *is* T_0, T_1*,* T_2*,* T_3*, and* T_4 *space.*

In examining the topological spaces on the group of units modulo a composite number n, we observe that (U_n, τ_n) lacks certain separation properties, as it is neither T_0, T_1, nor T_2 (Hausdorff). In contrast, (Q_n, τ_Q), defined on the group of quadratic residues modulo n, satisfies all three separation properties.

This distinction is critical for the function $f: (U_n, \tau_n) \rightarrow (Q_n, \tau_Q)$, which is continuous, open, and closed. While f ensures that the preimage of open sets in Q_n remains open in U_n, the open and closed nature of f allows it to preserve separation properties in the range even if they are absent in the domain. This interplay emphasizes how f can maintain a stronger topological structure in its range, independent of the limitations in U_n.

To define a quotient topology on U_n, we start by establishing an equivalence relation on U_n, allowing us to partition U_n into equivalence classes that will form the basis for this topology.

Define an equivalence relation $\sim$ on U_n by setting $x \sim y$ if and only if x and y belong to the same basis element B, which occurs if $x^2 \equiv y^2 \ (mod\ n)$. This relation groups elements in U_n that share equivalent squares. The equivalence class of an element x under this relation, denoted by $[x]$, is defined as $[x] = \{y \in U_n: x^2 \equiv y^2 \ (mod\ n)\}$.

We then define the quotient topology on the set $U_n / \sim$ by introducing the quotient map $q: U_n \rightarrow U_n / \sim$, which maps each element $x \in U_n$ to its equivalence class $[x]$. The quotient topology on $U_n / \sim$ is the finest topology making q continuous, meaning that a subset $V \subseteq U_n / \sim$ is open in τ_q if and only if $q^{-1}(V)$ is open in U_n under the original topology τ_n.

Since U_n is clopen in its original topology, each equivalence class retains this property in the quotient topology. Thus, the quotient topology on U_n provides a structure where open sets are determined by the preimages of open sets in U_n, allowing us to study U_n while preserving the relationships between elements within their equivalence classes.

Remark 3.4 *The quotient topology on* $U_n / \sim$*, defined by the equivalence relation* $x \sim y \Leftrightarrow (x^2 \equiv y^2 \ (mod\ n))$*, is naturally isomorphic to the discrete topology on* Q_n*. Thus,* Q_n *is the quotient space of* U_n *under this relation, inheriting a discrete topology from the quotient structure. The map* $f(x) = x^2$ *acts as a quotient map, and this discrete topology on* Q_n *reflects its nature as the quotient space* $U_n / \sim$*.*

4. Conclusion

In this work, we explore a topological space defined on the group of units modulo a composite number n using solutions to quadratic residue equations. The defined topology using sets formed by these solutions provides a detailed exploration of the algebraic relationships among solutions. Some properties were examined, such as clopen sets, closure, interior, limit points, and the behavior of continuous functions. Some results highlight differences in the separation axioms of these spaces through the analysis of the quadratic residues and quotient topologies.

References

[1] Zariski, Oscar. *The Topology of the Spectrum of an Algebraic Field*. Transactions of the American Mathematical Society, vol. 44, no. 2, 1938, pp. 138–161.

[2] Han, Sang-Eon, Saeid Jafari, and Jeong Min Kang. *Topologies on $\mathbb{Z}_n$ that Are Not Homeomorphic to the n-Dimensional Khalimsky Topological Space*. Mathematics 7.11 (2019): 1072.

[3] Ireland, Kenneth, and Michael Rosen. *A Classical Introduction to Modern Number Theory*. 2nd ed., Springer-Verlag, 1990.

[4] Cohen, Henri, S. Axler, and K. A. Ribet. *Number theory: Volume I: Tools and diophantine equations*. Vol. 560. Springer New York, 2007.

[5] Stinson, Douglas R. *Cryptography: Theory and Practice*. 3rd ed., Chapman & Hall/CRC, 2006.

[6] M. R. S., and M. J. *Quadratic Residues and Their Applications in Cryptography*. Journal of Number Theory, vol. 210, 2020, pp. 123-135.

[7] Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[8] Rosen, Kenneth H.. *Elementary number theory and its applications*. United Kingdom, Addison-Wesley, 2000.

[9] Childs, Lindsay N. *A concrete introduction to higher algebra*. New York: Springer, 2009.

[10] Kraft, James, and Lawrence Washington. *An introduction to number theory with cryptography*. Chapman and Hall/CRC, 2018.

[11] Gallian, Joseph A. *Contemporary Abstract Algebra*. Cengage Learning, 2016.

[12] Hardy, G. H., and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford UP, 2008.

[13] Lang, Serge. *Algebra*. Springer, 2002.

[14] Silverman, Joseph H. *A Friendly Introduction to Number Theory*. Pearson, 2013.

[15] Rezaei, M., et al. *Quadratic residues graphs*. International Journal of Pure and Applied Mathematics 113.3 (2017): 465-470.

[16] Munkres, James R. *Topology*. 2nd ed., Pearson, 2018.

[17] Willard, Stephen. *General Topology*. Dover Publications, 2012.

[18] Engelking, Ryszard. *General Topology*. Revised and expanded edition, Heldermann Verlag, 2020.

[19] Daoub, Hamza, Osama Shafah, and Fathi Brebish. *A topological space defined on the group of units modulo p. unpublished*, (2024).