Libyan Journal of Science & Technology 15:2 (2025) 243-246

Faculty of Science - University of Benghazi

Libyan Journal of Science & Technology

journal home page: www.sc.uob.edu.ly/pages/page/77

A Topological Space Defined On The Group Of Unites Modulo p.

Hamza A. Daoub[a], **Osama A. Shafah**[b], **Fathi A. Bribesh**[a*]

[a] *Department of Mathematics, Faculty of Science, University of Zawia, Zawia, Libya.*

[b] *Department of Mathematical Sciences, Libyan Academy for Postgraduate Studies, Tripoli, Libya*

Highlights

- **A novel non-discrete topology τ_p is defined on the unit group U_p using conjugate pairs $\{\alpha, p-\alpha\}$ as basic open sets, where every open set is also closed (clopen).**
- **The function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$ mapping x to x^2 is continuous, open, and closed, establishing a strong topological link between the unit group and quadratic residues.**
- **The quotient space $U_p/\sim$, under the equivalence $x \sim y \Leftrightarrow x^2 \equiv y^2 (\text{mod } p)$, is homeomorphic to the discrete space of quadratic residues (Q_p, τ_Q).**
- **The topology τ_p is disconnected and fails the T_0 separation axiom, whereas the discrete topology on Q_p satisfies stronger separation properties such as T_4.**
- **Key topological operators (interior, closure, boundary, limit points) are explicitly characterized for arbitrary subsets of U_p, revealing how structure depends on conjugate-pair symmetry**

ARTICLE INFO

Article history:

Received 29 September 2025
Revised 15 October 2025
Accepted 22 October 2025

Keywords:

Unit Groups, Quadratic Residues, Quotient Topology, Quadratic Congruence, Topological Groups

**Address of correspondence:*

E-mail address: f.bribesh@zu.edu.ly

F. A. Bribesh

ABSTRACT

This paper introduces a finite topological space τ_p on the group of units modulo a prime p, defined by its basis of conjugate residue pairs $\{\alpha, p-\alpha\}$ for all units $\alpha \in U_p$. We investigate the fundamental topological concepts such as point-set topology, separation axioms, and characterise the structure and behaviour of this topology. Additionally, we examine a function f from τ_p to the topology of quadratic residues τ_Q, mapping each unit to its square modulo p. We analyse the continuity, openness of f, and explore its implications for separation properties. Furthermore, we define a quotient topology on U_p based on the equivalence relation $x \sim y$ if and only if $x^2 \equiv y^2 \ mod \ p$, showing that the resulting quotient space is homeomorphic to (Q_p, τ_Q).

1. Introduction

Quadratic residues are an important part of number theory that used in areas like algebraic number theory and cryptography (Shapiro, 2008). Meanwhile, topological approaches have become common in studying algebraic structures, especially in fields like algebraic geometry and commutative algebra (Atiyah and Macdonald, 2018; Zariski and Samuel, 2013). By applying topological tools, we can gain a richer perspective on the behaviour of these algebraic structures.

Let U_p denote the group of units in the ring of integers modulo a prime number p. An element $a \in U_p$ is called a quadratic residue modulo p if there exists $x \in U_p$ such that $x^2 \equiv a\ (mod\ p)$. The set of all such residues, denoted by Q_p, forms a subgroup of U_p under multiplication, with each element having a multiplicative inverse in the group (Gallian, 2021). We define a topology τ_p on the group U_p, where the basis consists of the sets of conjugate residue pairs $B_\alpha = \{\alpha, p-\alpha\}$ for all $\alpha \in U_p$.

Unlike the standard discrete topology on finite sets, our definition gives a non-discrete topology τ_p that reflects the symmetry of conjugate pairs $\{\alpha, p-\alpha\}$ in U_p. While the Zariski topology (Zariski and Samuel, 2013) focuses on polynomial structures in rings, and prior work has examined profinite topologies on unit groups, τ_p is the first dedicated topology for U_p based on algebraic symmetry. However, τ_p satisfies that every open set is also closed (clopen), setting it apart from standard topologies like the discrete or metric ones (Dummit and Foote, 2004; Munkres, 2014; Artin, 2014; Willard, 2012).

The nature of such a basis in this topology leads to several novel characteristics. Singleton sets are not open, and the set topology like closure and interior, depends on these symmetric relationships. Such a topology offers a new perspective for analysing finite algebraic structures, which has potential implications in number theory (Daoub, 2025) and cryptographic applications (Lang, 2002; Alali *et al.*, 2023).

Additionally, we define a function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$, where $f(x) = x^2\ \ (mod\ p)$, with τ_Q representing the discrete topology on Q_p. It is found that this function is continuous, open, and closed, which can establish a strong topological connection between the unit group and the set of quadratic residues.

 ISSN: Online 2663-1407, Print 2663-1393; National Library of Libya, Legal number: 390/2018

To further explore, we construct a quotient topology on U_p induced by the equivalence relation $x \sim y$ if and only if $x^2 \equiv y^2 (mod\ p)$. This provides partitions of each unit with its inverse in a manner that reflects the structure of the basis. We show that the resulting quotient space $U_p/\sim$ is homeomorphic to (Q_p, τ_Q), bridging concepts in modular arithmetic and topology (Rudin, 1976).

2. Results

Our findings are organised into three main parts, each exploring distinct topological structures derived from the group of units modulo a prime p. First, we investigate the topology τ_p defined on U_p, where the space basis consists of all the sets of conjugate residue pairs $\{\alpha, p-\alpha\}$. This topology exhibits striking properties, such as the clopen property, and its separation and connectivity characteristics. Second, we examine the discrete topology on the set of quadratic residues Q_p investigating the interplay between these spaces via a function that maps all units into their quadratic residues, revealing both similarities and fundamental differences. Third, we introduce a quotient topology on U_p, induced by the equivalence relation $x \sim y$ if and only if $x^2 \equiv y^2 (mod\ p)$. The resulting quotient space $U_p/\sim$ consists of equivalence classes of the form $\{x, p-x\}$ and is shown to be homeomorphic to Q_p with the discrete topology.

2.1 Topology on The Group of Units

This section explores the topology (U_p, τ_p) defined by a basis consists of all sets of conjugate residue pairs $\{\alpha, p-\alpha\}$. This space is trivial if $p = 2$, or $p = 3$. We show that every open set is closed and derive more key properties of point-set topology such as interior, closure, and limit points, to explain the properties of separation and connectivity within the defined topological space.

Proposition 1. Let (U_p, τ_p) be a topological space, if $U \in \tau_p$ then U is a clopen set.

Proof: By the definition of the topology τ_p, every basis element $\{\alpha, p-\alpha\}$ is an open set. If $U \in \tau_p$, it can be expressed as a union of basis elements. Thus, U is open.

To show that U is closed, we prove that U^c is open, where $U^c = U_p - U$. If $x \in U^c$, then $x \notin U$, it follows that the element $p-x$ is not in U whenever x is a unit (i.e., $x \in U_p$). Thus, for each $x \in U^c$, we can construct a basis element $\{x, p-x\}$ that is contained in U^c. Therefore, U^c is a union of basis elements. Thus, U is closed.

Proposition 2. Let A be any subset of U_p such that $A = \{x\}$ then:

1. $A^\circ = \emptyset$.
2. $\bar{A} = \{x, p-x\}$
3. $b(A) = \{x, p-x\}$
4. $A' = \{p-x\}$

Proof: **(1)** Let $A = \{x\}$, since A contains only the single element x, any open set O that contains x must also include the element $p-x$. Hence, O cannot be contained in A, as O would include at least one element that is not in A. Thus, $A^\circ = \emptyset$.

(2) The smallest open set containing A is the basis element B_x. Since B_x includes both x and $p-x$, Proposition 1 implies that B_x is closed. Thus, $\bar{A} = \{x, p-x\}$

(3) By definition,

$b(A) = \bar{A} \cap \overline{U_p - A}$, where $U_p - A$ is the complement of A.

From (2), we know that $\bar{A} = \{x, p-x\}$, and $U_p - A = U_p - \{x\}$. Next, we determine $\overline{U_p - A}$. The point $p-x$ is not an interior point of $U_p - \{x\}$, because the smallest open set B_x is not contained in $U_p - \{x\}$. Consequently, U_p is a smallest open(closed) set containing $U_p - \{x\}$. Thus,

$$\overline{U_p - A} = U_p.$$

Now, we compute

$b(A) = \bar{A} \cap \overline{U_p - A} = \{x, p-x\} \cap U_p = \{x, p-x\}$.

(4) In the topology τ_p, the basis element containing x contains exactly the two points x and $p-x$. Let V be any open set containing $p-x$, then $\{x, p-x\} \subset V$ intersects A at the point x. Therefore, $p-x$ is a limit point of A.

Proposition 3. Let A be any subset of U_p such that $A = \{x_1, x_2, \dots, x_k\}$, where $1 \le k < p-1$ then:

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

Proof: **(1)** Suppose that $x_j \in A$ and $p - x_j \notin A$ for some $1 \le j \le k$, the set B_{x_j} is the smallest open set containing x_j and $p - x_j$. B_{x_j} is not contained in A, which means that x_j is not an interior point of A. For $i \ne j$, the points $x_i \in B_{x_i} \subset A$. Consequently, $A^\circ = \bigcup_{i \ne j} B_{x_i} = A - (\bigcup_j \{x_j\})$.

(2) Suppose that $x_j \in A$ and $p - x_j \notin A$ for all $1 \le j \le k$. In this case, there is no basis element B_{x_j}contains x_j and contained within A. Thus $A^\circ = \phi$.

(3) Suppose that $x_j \in A$ and $p - x_j \in A$ for all $1 \le j \le k$. Then, for each element $x_j \in A$, there exists a basis element $B_{x_j} \subset A$, which implies x_j is an interior point of A for all j. Hence, $A^\circ = A$.

Proposition 4. Let A be any subset of U_p such that $A = \{x_1, x_2, \dots, x_k\}$, where $1 \le k < p-1$ then:

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

***Proof*:** **(1)** Since $\bar{A} = \cap \{F \mid F \text{ is a closed set}, A \subset F\}$, and for a given $A = \{x_1, x_2, \dots, x_k\}$, we know that $x_j \in A$, and $p - x_j \notin A$. From Proposition 1, we have shown that the closure of a single-point set $\{x_j\}$ is $\{x_j, p - x_j\}$. Since $p - x_j$ is not in A but is in $\bar{A}$, this implies $A \cup \{p - x_j\} \subset \bar{A}$. Consequently, $\bar{A} = A \cup (\bigcup_j \{p - x_j\})$.

(2) Let $x_j \in A$ and $p - x_j \notin A$ for all $1 \le j \le k$, then from (1), we conclude $\bar{A} = A \cup (\bigcup_{j=1}^k \{p - x_j\})$.

(3) Given that each x_j and $p - x_j$ are included in A. it follows that:

$\overline{\{x_j\}} = \{x_j, p - x_j\} \subseteq A$.

Since this holds for all j, we conclude

$\bar{A} = \bigcup_{x_j \in A} \{x_j, p - x_j\} = A$.

Proposition 5. Let A be any subset of U_p such that $A = \{x_1, x_2, \dots, x_k\}$, where $1 \le k < p-1$ then:

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

***Proof*:** **(1)** From Proposition **4,** $\overline{U_p - A} = (U_p - A) \cup (\bigcup_j \{x_j\})$, for some j. Thus, $b(A) = \bar{A} \cap \overline{U_p - A} = (A \cup (\bigcup_j \{p - x_j\})) \cap ((U_p - A) \cup (\bigcup_j \{x_j\})) = (\bigcup_j \{p - x_j\}) \cup (\bigcup_j \{x_j\}) = \bigcup_j B_{x_j}$.

(2) Similar to (1), $\overline{U_p - A} = (U_p - A) \cup (\cup_{j=1}^{k}\{x_j\})$. Thus, $b(A) = \bar{A} \cap \overline{U_p - A} = \left(A \cup (\cup_{j=1}^{k}\{p - x_j\})\right) \cap \left((U_p - A) \cup (\cup_{j=1}^{k}\{x_j\})\right) = (\cup_{j=1}^{k}\{p - x_j\}) \cup (\cup_{j=1}^{k}\{x_j\}) = \cup_{j=1}^{k} B_{x_j}$.

(3) From Proposition **4**, since $\bar{A} = A$, and $\overline{U_p - A} = U_p - A$. Then $b(A) = A \cap U_p - A = \emptyset$.

Proposition 6. Let A be any subset of U_p such that $A = \{x_1, x_2, \dots, x_k\}$, where $1 \le k < p - 1$ then:

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

Proof: **(1)** Suppose that $x_j \in A$ and $p - x_j \notin A$ for some $1 \le j \le k$. Since the set B_{x_j} is the smallest open set containing x_j and $p - x_j$, then $A \cap \left(B_{x_j} - \{x_j\}\right) = \phi$ and $A \cap \left(B_{x_j} - \{p - x_j\}\right) \neq \phi$, which means that x_j is not a limit point of A. However, $p - x_j$ is a limit point of A. For $i \neq j$, the points $x_i \in B_{x_i} \subset A$. Consequently, $A \cap (B_{x_i} - \{x_i\}) \neq \phi$ and $A \cap (B_{x_i} - \{p - x_i\}) \neq \phi$. Thus, x_i and $p - x_i$ are the limit points of A. Hence, $A' = A^{\circ} \cup (\cup_j\{p - x_j\})$.

(2) Suppose that $x_j \in A$ and $p - x_j \notin A$ for all $1 \le j \le k$. Since the set $B_{x_j} = \{x_j, p - x_j\}$ satisfies $A \cap \left(B_{x_j} - \{x_j\}\right) = \phi$ and $A \cap \left(B_{x_j} - \{p - x_j\}\right) \neq \phi$ for all j, then $p - x_j$ is a limit point of A. Thus, $A' = \cup_{j=1}^{k}\{p - x_j\}$.

(3) Suppose that $x_j \in A$ and $p - x_j \in A$ for all $1 \le j \le k$. Then from proposition 4, $\bar{A} = A$. Therefore, $A' = A^{\circ} = A$.

Remarks:

1. The topological space (U_p, τ_p) is not T_0 space.

Since x_j and $p - x_j$ are two distinct points in U_p, and by the definition of τ_p there are no open sets that contain one of these points and exclude the other. Thus, τ_p is not a T_0 space.

2. The topological space $(U_p, \tau_p), p > 3$ is disconnected.

Consider the open sets:

$$V = \{x_1, p - x_1\}$$
$$W = U_p - V$$

Then V and W are two open sets that satisfy $V \cup W = U_p$, and $V \cap W = \emptyset$. Therefore, τ_p is disconnected.

3. The topological space (U_p, τ_p) is a compact and Lindelöf space, as it is finite
4. The topological space (U_p, τ_p) is a regular space.

Let $F \subseteq U_p$ be a closed set, $x \notin F$ and let $U = \{x, p - x\}$, then $V = U_p - U$ is an open set containing F, $x \notin V$, and $U \cap F = \emptyset$. Then the regularity of τ_p follows.

2.2 Quadratic Residues Topology

This section examines the discrete topology (Q_p, τ_Q) on quadratic residues modulo p, unlike the conjugate-pair structure of τ_p. Moreover, τ_Q treats each residue as an isolated point, enabling sharper separation properties. We analyse the function $f: U_p \to Q_p$, which maps each unit to its square, showing their continuity and openness.

Definition 1. *Let $Q_p = \{q_1, q_2, \dots, q_{\frac{p-1}{2}}\}$ be the set of all quadratic residues in U_p, and $P(Q_p)$ be the power set of Q_p, then $\tau_Q = P(Q_p)$ defines a topology on Q_p.*

This topology is a discrete topology of the group of quadratic residues modulo a prime p, it is an interesting topic in algebraic number theory. This group comprises the set of residue classes that are quadratic residues modulo a prime p. This group plays a significant role in various number-theoretic applications, including quadratic reciprocity and cryptography.

The discrete topology on Q_p is a particular type of topology, where the set of a singleton quadratic residue modulo p, $\{a\}$ is open. This topology provides a fine-grained level of detail, allowing for precise analysis of the individual elements in the group.

The discrete topology τ_Q and the topology τ_p are related but distinct topologies defined on different sets. Both topologies are defined on sets related to the prime number p and modulo arithmetic; they have different basis and generate different classes of open sets.

Since every subset $B_\alpha = \{\alpha, p - \alpha\} \in \mathfrak{B}$ corresponds to a quadratic residue $a \in Q_p$. We define a function between two topological spaces (U_p, τ_p) and (Q_p, τ_Q) as follows:

$$f(x) = \{x^2 : x \in U_p\}$$

The function f maps the roots of the quadratic polynomial $x^2 \equiv a \ (mod\ p)$ to the quadratic residue $a \in Q_p$, maps B_a to a quadratic residue.

Example 1. Let $p = 7$ then $Q_7 = \{1,2,4\}$ and

$$\tau_{Q_7} = \{\emptyset, Q_7, \{1\}, \{2\}, \{4\}, \{1,2\}, \{1,4\}, \{2,4\}\}$$

and

$$\mathfrak{B} = \{B_1 = \{1,6\}, B_2 = \{2,5\}, B_3 = \{3,4\}\},$$

so

$$\tau_7 = \{\emptyset, U_7, \{1,6\}, \{2,5\}, \{3,4\}, \{1,2,5,6\}, \{1,3,4,6\}, \{2,3,4,5\}\},$$

and $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$ will be as

$$f(1) = 1,\ f(2) = 4,\ f(3) = 2, f(4) = 2,\ f(5) = 4, f(6) = 1.$$

Therefore, $\{1,6\} \mapsto \{1\}$, $\{2,5\} \mapsto \{4\}$, $\{3,4\} \mapsto \{2\}$, which corresponds to the basis of the topology τ_p and τ_Q, respectively. From the definition of Q_p, it is clear that $U_p \mapsto Q_p$.

The function $f: U_p \to Q_p$, highlights the interesting topological connection between these spaces. **Example 1** illustrated this mapping and its structure.

Next, we examine the continuity of f and its effect on the topologies of both U_p and Q_p, starting with the following proposition.

Proposition 7. The function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$ is continuous.

Proof: Consider $f: U_p \to Q_p$ is defined by $f(x) = x^2$, where $x \in U_p$, and let $V \subseteq Q_p$ be an open set in Q_p. Then $f^{-1}(\{a\})$ for any $a \in Q_p$ is the set of elements $x \in U_p$ such that $x^2 \equiv a\ (mod\ p)$. This set is either $\{\alpha, p - \alpha\}$ or ϕ, which is a basis element of the topology on U_p. Therefore, $f^{-1}(V) = \{x \in U_p : x^2 \in V\}$ can be expressed as a union of basis elements $\{\alpha, p - \alpha\}$ of U_p.

Proposition 8. The function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$ is open.

Proof: Since any open set in U_p is a union of basis elements $\beta_a = \{\alpha, p - \alpha\}$, and $f(\beta_a) = \{a\}$, where $a = \alpha^2\ (mod\ p)$. The image of an open set $O \subseteq U_p$ under f is a subset of Q_p. Since Q_p has the discrete topology. Thus, f is open.

Corollary 1. The function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$ is closed.

Corollary 2. The topological space (Q_p, τ_Q) is a T_4 space.

In the context of the topological spaces defined on the group of units modulo a prime p, we observe that (U_p, τ_p) exhibits certain limitations regarding separation properties. Specifically, this topology is not a T_0 space. In contrast, the topology (Q_p, τ_Q) on the group of quadratic residues modulo p has stronger separation properties, being T_4. This distinction is crucial when examining the function $f: (U_p, \tau_p) \to (Q_p, \tau_Q)$, which is not only continuous but also open and closed. The function f is continuous because the preimage of any open set in Q_p is open in U_p. Moreover, f is both open and closed it maps basis elements $\{\alpha, p-\alpha\}$ in U_p to singletons $\{a\}$ in Q_p, preserving topological structure. While (Q_p, τ_Q) fails separation axioms (e.g., non-T_0), the discrete topology on (Q_p, τ_Q) satisfies stronger properties like T_4 . This contrast shows how f bridges the two spaces: despite the weak topology of U_p, the image under f inherits the strong separation properties of Q_p. Such behaviour underscores how functions can transfer structure between topologies, even when their domains exhibit limitations.

2.3 Quotient Topology on U_p

To define a quotient topology on U_p, we first need to establish a suitable equivalence relation on U_p. This relation will allow for partition U_p into equivalence classes, which form a basis for the quotient topology.

To define an Equivalence Relation, let U_p be the group of units modulo p. We can define an equivalence relation $\sim$ on U_p as follows:

For any $x, y \in U_p$, say $x \sim y$ if and only if x and y belong to B_α, i. e.,

$$x \sim y \Leftrightarrow (x^2 \equiv y^2 \ (mod\ p)).$$

This relation associates each element with its additive inverse in the group of units.

The set of equivalence classes under this relation is denoted by $U_p / \sim$. Each equivalence class has the form $[x] = \{x, p-x\}$.

We define the quotient topology τ_q on the set $U_p / \sim$ as follows:

Consider the quotient map $q: U_p \to U_p / \sim$ that sends each element $x \in U_p$ to its equivalence class $[x]$. The quotient topology defined on $U_p / \sim$ is the finest topology that makes the quotient map q is continuous. Since U_p is clopen in (U_p, τ_p), the equivalence classes also retain this property under the quotient topology.

The quotient topology on U_p is defined through the equivalence relation $x \sim y \Leftrightarrow x^2 \equiv y^2 \, (mod\ p)$, which partitions U_p into classes $[x] = \{x, p-x\}$. In this topology, a set is open if its preimage under the quotient map $q: U_p \to U_p/\sim$ is open in τ_p. Remarkably, this construction yields a space isomorphic to Q_p with its discrete topology, the following Remark, effectively shows transforming the conjugate-pair structure of U_p into the separated, point-like structure of quadratic residues. This quotient preserves the fundamental relationships between elements while simplifying the topological analysis.

Remarks: The quotient space $U_p / \sim$, where $x \sim y \Leftrightarrow (x^2 \equiv y^2 (mod\ p))$ is homomorphic to the discrete topology Q_p. To show that $\tilde{f}: U_p / \sim \to \mathrm{Q_p}$ defined by $\tilde{f}([x]) = x^2 \ (mod\ p)$, it is indeed well defined. Since for any $x, y \in [x]$ we have $x^2 \equiv y^2 \ (mod\ p)$ by definition of $\sim$, which implies $\tilde{f}([x]) = \tilde{f}([y])$.

By the definition of $\tilde{f}$, for any y in Q_p there is $[x]$ in the quotient topology $U_p / \sim$ such that $\tilde{f}([x]) = y$, i.e., $\tilde{f}$ is bijective. $\tilde{f}$ is continues as the quotient topology on $U_p / \sim$ is the finest topology making $q: U_p \to U_p / \sim$ continuous.

In the discrete topology on Q_p, every subset is open. Thus, $\tilde{f}$ trivially maps open sets to open sets. Therefor, $\tilde{f}$ is a homeomorphism.

3. Conclusion

This paper establishes a novel topological framework on the group of units modulo a prime p, revealing how algebraic symmetries specifically conjugate pairs induce a non-discrete, clopen topology τ_p. By constructing a continuous, open, and closed map from (U_p, τ_p) to the discrete space of quadratic residues (Q_p, τ_Q), the work demonstrates a direct topological correspondence between these algebraic sets. Furthermore, the quotient of U_p by square equivalence is shown to be homeomorphic to Q_p, effectively translating modular arithmetic structure into a discrete topological model. These findings provide a meaningful synthesis of algebraic and topological methods, with potential applications in number theory and cryptography.

References

Alali, A.S., Ali, S., Hassan, N., Mahnashi, A.M., Shang, Y. and Assiry, A. (2023) 'Algebraic structure graphs over the commutative ring Z m: exploring topological indices and entropies using M-polynomials', Mathematics, 11(18), p. 3833.

Artin, M. (2014) Algebra. United Kingdom: Pearson Education Limited.

Atiyah, M.F. and Macdonald, I.G. (2018) Introduction to commutative algebra. CRC Press.

Daoub, H. A. (2025) A Topological Space Defined on Finite Rings Modulo Composite Numbers. University of Zawia, Journal of Natural Sciences, 2(1), pp. 1–11.

Dummit, D.S., Foote, R. M. (2004) Abstract algebra: Volume III. Hoboken: Wiley.

Gallian, J. (2021) Contemporary abstract algebra. Chapman and Hall/CRC.

Lang, S., (2002) Algebra. 3rd edn. Springer Verlag.

Munkres, J. (2014) Topology. 2nd edn. United Kingdom: Pearson Education Limited.

Rudin, W. (1976) Principles of Mathematical Analysis. McGraw-Hill.

Shapiro, H.N. (2008) Introduction to the Theory of Numbers. Courier Corporation.

Willard, S. (2012) General topology. Courier Corporation.

Zariski, O. and Samuel, P. (2013) Commutative algebra: Volume II. Springer Science & Business Media.