A Topological Proof That There Are Infinitely Many Prime Numbers

Hajime

September 21, 2024

1 Introduction

There are many proofs demonstrating that there are infinitely many prime numbers, most of which involve assuming there are only finitely many primes and then deriving a contradiction. In this document, we will focus on one such proof—a topological proof that is both simple and elegant.

This proof requires us to carefully examine several key steps. The general approach is as follows: we first define a basis for a topology τ on $\mathbb{Z}$ and explore the properties of open sets within this topology. We then apply the fundamental theorem of arithmetic and, by assuming there are finitely many prime numbers, arrive at a contradiction.

2 Proof

Consider a following form of subsets of $\mathbb{Z}$.

$$\text{Given } a, b \in \mathbb{Z}, \text{ with } a \neq 0, \text{ let } S(a, b) := \{ax + b : x \in \mathbb{Z}\}.$$

Before delving into the actual proof, it's imperative to review some basic concepts in topology. We start by recalling the key definitions.

Definition 1. *A topology on a set X is a collection $\mathcal{T}$ of subsets of X having the following properties:*

1. *$\emptyset$ and X are in $\mathcal{T}$.*
2. *The union of the elements of any subcollection of $\mathcal{T}$ is in $\mathcal{T}$.*
3. *The intersection of the elements of any finite subcollection of $\mathcal{T}$ is in $\mathcal{T}$.*

A set X for which a topology $\mathcal{T}$ has been specified is called a topological space.

Definition 2. *If X is a set, a* basis *for a topology on X is a collection $\mathcal{B}$ of subsets of X (called* basis elements*) such that:*

1. *For each $x \in X$, there is at least one basis element B containing x.*
2. *If x belongs to the intersection of two basis elements B_1 and B_2, then there is a basis element B_3 containing x such that $B_3 \subseteq B_1 \cap B_2$.*

Definition 3. *Let U be a subset of X. Then $U \in \tau$ is called an* open set *if for each $x \in U$, there is a basis element B of $\mathcal{B}$ such that $x \in B \subseteq U$.*

Definition 4. *Let C be a subset of X. Then C is called a* closed set *if its complement $X - C$ is open in X.*

Note that the sets that are simultaneously open and closed are called **clopen sets**.

Theorem 1. *A collection $\{S(a, b) : a, b \in \mathbb{Z}$ and $a \neq 0\}$ is a basis for a topology τ on $\mathbb{Z}$.*

Proof. To prove that the collection $\{S(a, b) : a, b \in \mathbb{Z}$ and $a \neq 0\}$ is a basis for a topology τ on $\mathbb{Z}$, we need to verify two conditions:

1. For each $x \in \mathbb{Z}$, there exists a basis element $S(a, b)$ containing x.

Let $x \in \mathbb{Z}$. Consider the set $S(1, x) = \{1 \cdot k + x : k \in \mathbb{Z}\} = \{x + k : k \in \mathbb{Z}\}$. Clearly, $x \in S(1, x)$, so the first condition is satisfied.

2. If $x \in S(a_1, b_1) \cap S(a_2, b_2)$, then there exists a basis element $S(a_3, b_3)$ such that $x \in S(a_3, b_3) \subseteq S(a_1, b_1) \cap S(a_2, b_2)$.

Suppose $x \in S(a_1, b_1) \cap S(a_2, b_2)$. Let y be a least common multiple of a_1 and a_2. Then consider a basic neighbourhood of x, $S(x, y)$. Clearly, we have $x \in S(y, x) \subseteq S(a_1, b_1) \cap S(a_2, b_2)$

Thus, a collection $\{S(a, b) : a, b \in \mathbb{Z}$ and $a \neq 0\}$ is a basis for a topology τ on $\mathbb{Z}$.

□

Next, we will show every nonempty open set in the topology τ is infinite. Note that $\mathbb{Z}$ is countably infinite. There is a bijection between $\mathbb{Z}$ and $\mathbb{N}$, hence $\mathbb{Z}$ is countable. There is also a bijection between $\mathbb{Z}$ and each $S(a, b)$, so it follows that $|\mathbb{Z}| = |S(a, b)|$. Thus, each basic open set $S(a, b)$ is countably infinite.

Theorem 2. *Every nonempty open set in the topology τ is infinite.*

Proof. Consider any open set $U \in \tau$. By definition 3, there is a basic open set $S(a, b)$ such that $x \in S(a, b) \subseteq U$. Since $|\mathbb{Z}| = |S(a, b)|$ and $S(a, b)$ is countably infinite, U is also infinite.

□

Another interesting property of this basis for the topology τ on $\mathbb{Z}$ is that every basis element is also closed, making it clopen. Therefore, the collection $\{S(a,b) : a,b \in \mathbb{Z} \text{ and } a \neq 0\}$ is a basis consisting of clopen sets. This is essentially what the following theorem states.

Theorem 3. *for each $a, b \in Z$, with $a \neq 0$, $\mathbb{Z} \setminus S(a,b)$ is open.*

Proof. By definition 3, we can infer that any open set U in $\mathbb{Z}$ is a union of some collection of basic open sets. That is,

$$U = \bigcup_{B \in \mathcal{B}_U} B,$$

where $\mathcal{B}_U$ denotes the collection of basis elements corresponding to the open set U. We aim to show that $\mathbb{Z} \setminus S(a,b)$ is a union of a collection of basic open sets. In fact, each $\mathbb{Z} \setminus S(a,b)$ corresponds to the following:

$$Z \setminus S(a,b) = \bigcup_{c \notin S(a,b)} S(a,c),$$

This shows that $Z \setminus S(a,b)$ is open and $S(a,b)$ is closed in $\mathbb{Z}$.

□

Corollary 1. *A collection $\{S(a,b) : a,b \in \mathbb{Z}$ and $a \neq 0\}$ is a basis consisting of clopen sets for a topology τ on $\mathbb{Z}$.*

Remark 1. *$\mathbb{Z}$ under this topology τ is a T_1 space. We call **zero-dimensional** any T_1 topological space with a basis consisting of clopen sets. Thus, a topological space $\mathbb{Z}$ with a base $\{S(a,b) : a,b \in \mathbb{Z}$ and $a \neq 0\}$ is zero-dimensional.*

There is a fundamental theorem from which we draw a contradiction proof to show there are infinitely many prime numbers. The theorem is called **Fundamental Theorem of Arithmetic**.

Theorem 4. *(Fundamental Theorem of Arithmetic)*
Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.

There is an immediate consequence that follows from the fundamental theorem of arithmetic.

Theorem 5.

$$\bigcap_{p \ prime} \mathbb{Z} \setminus S(p,0) = \{-1, 1\}$$

Proof. By elementary set theory, we have,

$$\bigcap_{p \text{ prime}} \mathbb{Z} \setminus S(p,0) = \mathbb{Z} \setminus \bigcup_{p \text{ prime}} S(p,0) = \{-1, 1\}$$

Now choose an arbitrary integer greater than 1, call it n. Then it follows from the fundamental theorem that,

$n = \prod_{i \in I} p_i,$ where I is an index set and each p_i is a prime number.

Now take some p_j for some $j \in I$, and consider S(p_j, 0). Then since $\prod_{i \neq j} p_i$ is an integer, $n \in S(p_j, 0)$. Moreover, by taking a negative number of $\prod_{i \neq j} p_i$, we can see that $-n \in S(p_j, 0)$. Also, $0 \in S(p_j, 0)$.

Therefore, it follows that $\bigcap_{p \text{ prime}} \mathbb{Z} \setminus S(p, 0) = \{-1, 1\}$

□

Finally, using theorems above, we conclude that there are infinitely many prime numbers.

Theorem 6. *There are infinitely many prime numbers.*

Proof. Suppose to the contrary that there are only finitely many prime numbers. From theorem 3, we know that each $\mathbb{Z} \setminus S(p, 0)$ is open. Now from theorem 5, we also have the following:

$$\bigcap_{p \text{ prime}} \mathbb{Z} \setminus S(p, 0) = \{-1, 1\}$$

Since a finite intersection of open sets in τ is open by Definition 1, $\{-1, 1\}$ is open in $\mathbb{Z}$. Theorem 2 states that every nonempty open set in the topology τ is infinite, but $\{-1, 1\}$ is open and finite, contradiction.

Thus, there are infinitely many prime numbers.

□