

The following definitions and theorems are adapted from James R. Munkres' Topology (second edition)

Definition_{12.1}: A topology τ on a set X is a collection of subsets of X , called open sets, satisfying the following properties.
(Page 76)

- i) $\emptyset \in \tau$ and $X \in \tau$.
- ii) If $Y \subseteq \tau$, then $\bigcup_{t \in Y} t \in \tau$.
- iii) If $Y \subseteq \tau$ is finite, then $\bigcap_{t \in Y} t \in \tau$.

The ordered pair (X, τ) is called a topological space.

Definition_{13.1}: A basis \mathcal{B} for a topology τ on X is a collection of subsets of X satisfying the following properties.
(Page 78)

- i) If $x \in X$, then we can find $B \in \mathcal{B}$ such that $x \in B$.
- ii) If $x \in B_1 \cap B_2$ for some sets B_1 and B_2 in \mathcal{B} , then we can find a set $B_3 \in \mathcal{B}$ such that $x \in B_3$ and $B_3 \subseteq B_1 \cap B_2$.

Lemma_{13.1}: If \mathcal{B} is a basis for a topology τ on X , then $\tau = \{\bigcup_{b \in B} b : B \subseteq \mathcal{B}\}$.
(Page 80)

Definition_{17.1}: Let (X, τ) be a topological space. A set $S \subseteq X$ is closed if $S^c \in \tau$.
(Page 93)

Theorem_{17.1(3)}: The union of any finite number of closed sets in a topological space is closed.
(Page 94)

Theorem:

There are infinitely many prime numbers.

Proof(By Contradiction):**Part I – The evenly spaced integer topology.**

Suppose \mathcal{B} is the set of all arithmetic progressions $\mathbb{Z}(a, m) := \{a + nm : n \in \mathbb{Z}\}$ where $m \neq 0$. We must first show that \mathcal{B} is a basis for a topology τ on \mathbb{Z} . To do this, we must show that \mathcal{B} satisfies both criteria from definition_{13.1}.

i) If $k \in \mathbb{Z}$, then clearly $k \in \mathbb{Z}(0, k) \in \mathcal{B}$.

ii) If $k \in \mathbb{Z}(a, b) \cap \mathbb{Z}(c, d)$, then $k \in \mathbb{Z}(k, bd)$, since we have $k = k + bd(0)$.

Now suppose we have $j \in \mathbb{Z}(k, bd)$. Then $j = k + bdn$.

We can write k as $a + bm$ for some integer m , so $j = a + bm + bdn = a + b(m + dn)$, and therefore $j \in \mathbb{Z}(a, b)$. Likewise, we can write k as $c + dn$ for some integer n , so $j = c + dn + bdn = c + d(n + bn)$, and therefore $j \in \mathbb{Z}(c, d)$.

So we have $\mathbb{Z}(k, bd) \subseteq \mathbb{Z}(a, b) \cap \mathbb{Z}(c, d)$.

We have shown that \mathcal{B} is a basis for a topology on \mathbb{Z} , so lemma₁ gives us a topology τ on \mathbb{Z} whose elements are the unions of arithmetic progressions in \mathcal{B} . In other words, if B is any subset of \mathcal{B} , then $\bigcup_{b \in B} b$ is contained in τ .

Part II – Finite unions of arithmetic progressions of the form $\mathbb{Z}(0, p)$ are closed.

Now suppose p is prime and observe that $\bigcup_{k=1}^{p-1} \mathbb{Z}(k, p)$ is the set of all integers which are congruent to k modulo p for all values of k satisfying $0 < k < p$. Equivalently, this set can be described as the set of integers which are not divisible by p , which is precisely what $\mathbb{Z}(0, p)^c$ is. So $\mathbb{Z}(0, p)^c = \bigcup_{k=1}^{p-1} \mathbb{Z}(k, p)$. And since $\mathbb{Z}(0, p)^c$ can be written as a union of arithmetic progressions, i.e. open sets, it must be open by property (ii) of definition_{12.1}. Furthermore, since $\mathbb{Z}(0, p)^c$ is open, definition_{17.1} tells us that $(\mathbb{Z}(0, p)^c)^c = \mathbb{Z}(0, p)$ must be closed. It follows by theorem_{17.1(3)} that finite unions of arithmetic progressions of the form $\mathbb{Z}(0, p)$ are also closed.

Part III – If $\{p_1, p_2, \dots, p_r\}$ is the set of all primes, then $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$ can't be open.

Finally, suppose for contradiction that there are finitely many prime numbers p_1, p_2, \dots, p_r . Since we have shown that finite unions of arithmetic progressions of the form $\mathbb{Z}(0, p)$ are closed, we know that $\bigcup_{k=1}^r \mathbb{Z}(0, p_k)$ must be closed. And this tells us that the complement of this union must be open. But $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c = \{-1, 1\}$ is not an arithmetic progression nor the empty set. Therefore $\{-1, 1\}$ cannot be open. So we have a contradiction. Thus we can conclude that there are infinitely many prime numbers. ■

How we can conclude that $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c = \{-1, 1\}$?

Proof:

We will show that $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c = \{-1, 1\}$ by showing that

- i) $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$ contains everything in $\{-1, 1\}$, and
- ii) $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$ and nothing that isn't part of $\{-1, 1\}$.

i) Observe that if p is prime, then $\mathbb{Z}(0, p)$ contains neither -1 nor 1 , since neither of these is a multiple of p . Therefore $\{-1, 1\} \cap \bigcup_{k=1}^r \mathbb{Z}(0, p_k) = \emptyset$. So $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$ contains everything in $\{-1, 1\}$.

ii) Suppose k isn't part of $\{-1, 1\}$. i.e. $k \in \{-1, 1\}^c = \mathbb{Z} \setminus \{-1, 1\}$.

There are two cases to consider.

Case 1) $k = 0$.

Let p be prime. Then $k \in \mathbb{Z}(0, p)$ since $k = 0 \cdot p$. So $k \in \bigcup_{k=1}^r \mathbb{Z}(0, p_k)$, and therefore $k \notin (\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$.

Case 2) $k \geq 2$.

Then k has a prime divisor q by the fundamental theorem of arithmetic. And since we have assumed that $\{p_1, p_2, \dots, p_r\}$ contains all of the primes, we must have $q = p_i$ for some $1 \leq i \leq r$. Therefore $k \in \mathbb{Z}(0, q) = \mathbb{Z}(0, p_i)$. So $k \in \bigcup_{k=1}^r \mathbb{Z}(0, p_k)$ and thus $k \notin (\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c$.

It follows that $(\bigcup_{k=1}^r \mathbb{Z}(0, p_k))^c = \{-1, 1\}$, so we are done.

■