A Topological Proof of the Infinitude of Primes

Alex Provost

July 6, 2012

1 Introduction

2 Review of Elementary Topology

3 Proving Euclid's Theorem

Euclid's Theorem

Euclid, circa 300 BC:

Theorem

There are infinitely many prime numbers.

Proof.

Suppose that $p_1 = 2 < p_2 = 3 < \ldots < p_r$ are all of the primes. Let $P = p_1 p_2 \cdots p_r + 1$ and let p be a prime dividing P; then p can not be any of the p_i, otherwise p would divide the difference $P - p_1 p_2 \cdots p_r = 1$, which is impossible. So this prime p is still another prime. □

What Is Topology?

Topology formalizes notions of

- Nearness
- Continuity

by specifying that certain sets be "open" and "closed".

...but Euclid's theorem is a statement about prime numbers.

- Integers appear as discrete rather than continuous.
- So what does topology have to do with our statement?

What Does Topology Have to Do With Our Statement?

There are many ways of "topologizing" the integers.
However, consider the following subsets: for $a, b \in \mathbb{Z}$, $b \neq 0$,

$$N(a, b) = a + b\mathbb{Z} = \{a + bk \mid k \in \mathbb{Z}\}$$

These are the *arithmetical sequences*.

- These subsets of $\mathbb{Z}$ possess interesting properties.
- They will be used as building blocks for our topology.
- Under this topology, $\mathbb{Z}$ will be "forced" into having infinitely many prime numbers.

Basic Concepts: Topological Spaces

Definition

Let X be a set. A collection $\mathcal{T}$ of subsets of X is called a topology on X if it satisfies the following axioms:

(i) $\emptyset, X \in \mathcal{T}$

(ii) $\{U_i\}_{i \in I} \subseteq \mathcal{T} \implies \bigcup_{i \in I} U_i \in \mathcal{T}$

(iii) $U_1, \ldots, U_n \in \mathcal{T} \implies \bigcap_{i=1}^{n} U_i \in \mathcal{T}$

Definition

If $\mathcal{T}$ is a topology on X, $(X, \mathcal{T})$ is called a topological space, X is the set of points, and the elements of $\mathcal{T}$ are the open sets.

Basic Concepts: Neighborhoods, Closed Sets

Definition

A neighborhood of $x \in X$ is an open set containing x (some authors use the term "open neighborhood").

Definition

A set $U \subseteq X$ is closed if its complement $X \setminus U$ is open.

Remark

Closed sets possess properties "dual" to those of open sets:

- Finite unions of closed sets are closed.
- Arbitrary intersections of closed sets are closed.

Examples of Topological Spaces

Some examples of topological spaces:

- Any set X with topology $\mathcal{T} = \{\emptyset, X\}$ (the *trivial topology*)
- Any set X with topology $\mathcal{T} = \mathcal{P}(X)$ (the *discrete topology)*
- The set $\mathbb{R}$ with its familiar open and closed sets
- Any metric space with the topology induced by its metric
- The set $\{a, b, c\}$ can be given 29 different topologies!

Basic Concepts: Basis

Definition

A basis for a topology on X is a collection $\mathcal{B}$ of subsets of X satisfying:

(i) For all $x \in X$, there exists at least one basis element $B \in \mathcal{B}$ containing x.

(ii) If x belongs to the intersection of two basis elements $B_1, B_2 \in \mathcal{B}$, then there exists a basis element $B_3 \in \mathcal{B}$ containing x such that $B_3 \subseteq B_1 \cap B_2$.

Example

The collection of open sets of the form (a, b) forms a basis for a topology on $\mathbb{R}$.

Basic Concepts: Topology Generated by a Basis

Definition

Given a basis $\mathcal{B}$ for a topology on X, the topology $\mathcal{T}$ generated by $\mathcal{B}$ is described as follows:
$U \subseteq X$ is open iff for each $x \in U$, there exists a basis element $B \in \mathcal{B}$ such that B contains x and $B \subseteq U$.

There is a simple characterization of open sets using basis elements:

Proposition

If $\mathcal{B}$ is a basis for a topology $\mathcal{T}$ on X, then every open set in $\mathcal{T}$ is a union of elements of $\mathcal{B}$.

Topologizing the Integers

Recall the arithmetic sequences in $\mathbb{Z}$ that we defined earlier on:

$$N(a, b) = a + b\mathbb{Z} = \{a + bk \mid k \in \mathbb{Z}\} \quad (b \neq 0)$$

Take the collection $\mathcal{B}$ of all these subsets:

$$\mathcal{B} = \{N(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$$

Let's check that this is, in fact, a basis for a topology on $\mathbb{Z}$.

Checking That We Have a Basis

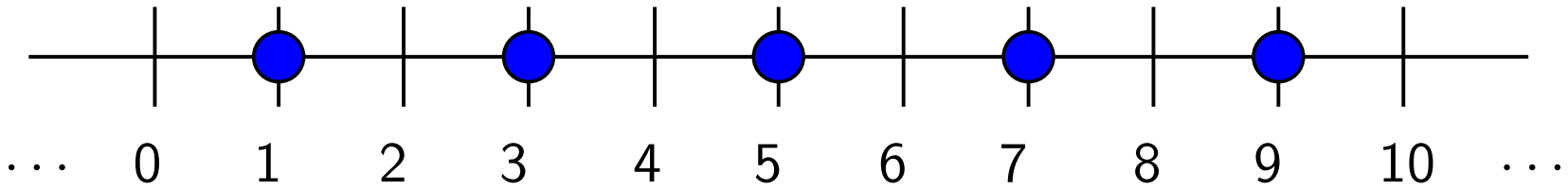
We need to verify two things:

(i) That $\mathcal{B}$ covers $\mathbb{Z}$. But $N(0,1) = \mathbb{Z}$ is a basis element that covers $\mathbb{Z}$, so we are done.

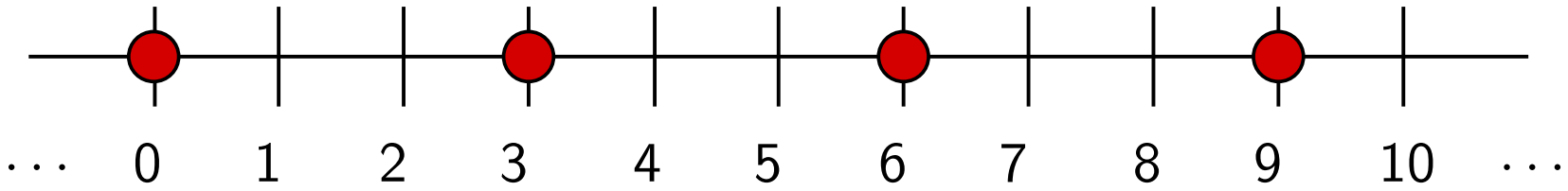
(ii) That given basis elements $N(a_1, b_1)$ and $N(a_2, b_2)$, and x in their intersection, there exists a basis element $B \in \mathcal{B}$ such that $x \in B \subseteq N(a_1, b_1) \cap N(a_2, b_2)$.

But taking $b = \text{lcm}(b_1, b_2)$, one has that $B = N(x, b) = N(a_1, b_1) \cap N(a_2, b_2)$ and this is sufficient.

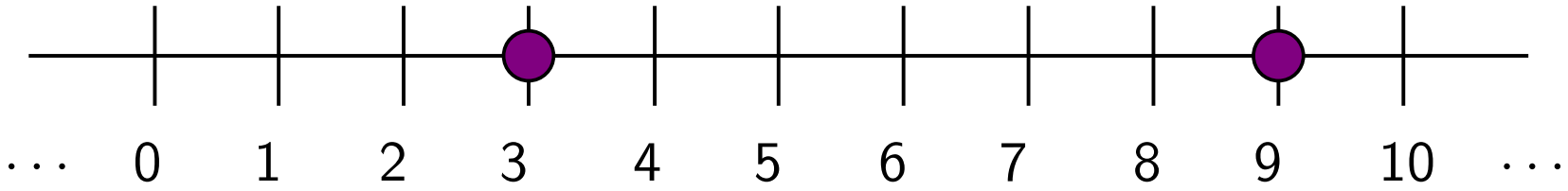
$N(1, 2)$



$N(0, 3)$



$N(1, 2) \cap N(0, 3) = N(3, \text{lcm}(2, 3)) = N(3, 6)$



Remarks on Our Newfound Topology (Pt. 1)

- Thus $\mathcal{B} = \{N(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ generates a unique topology on $\mathbb{Z}$.
- Each $N(a, b)$ is a neighborhood of a, hence the notation.
- A subset of the integers is open iff it is a (possibly empty) union of arithmetic sequences.

Example

The set $N(0, 3) \cup N(2, 4) =$
$\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \cup \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\} =$
$\{\ldots, -10, -9, -6, -3, -2, 0, 2, 3, 6, 9, 10, \ldots\}$ is open in $\mathbb{Z}$.

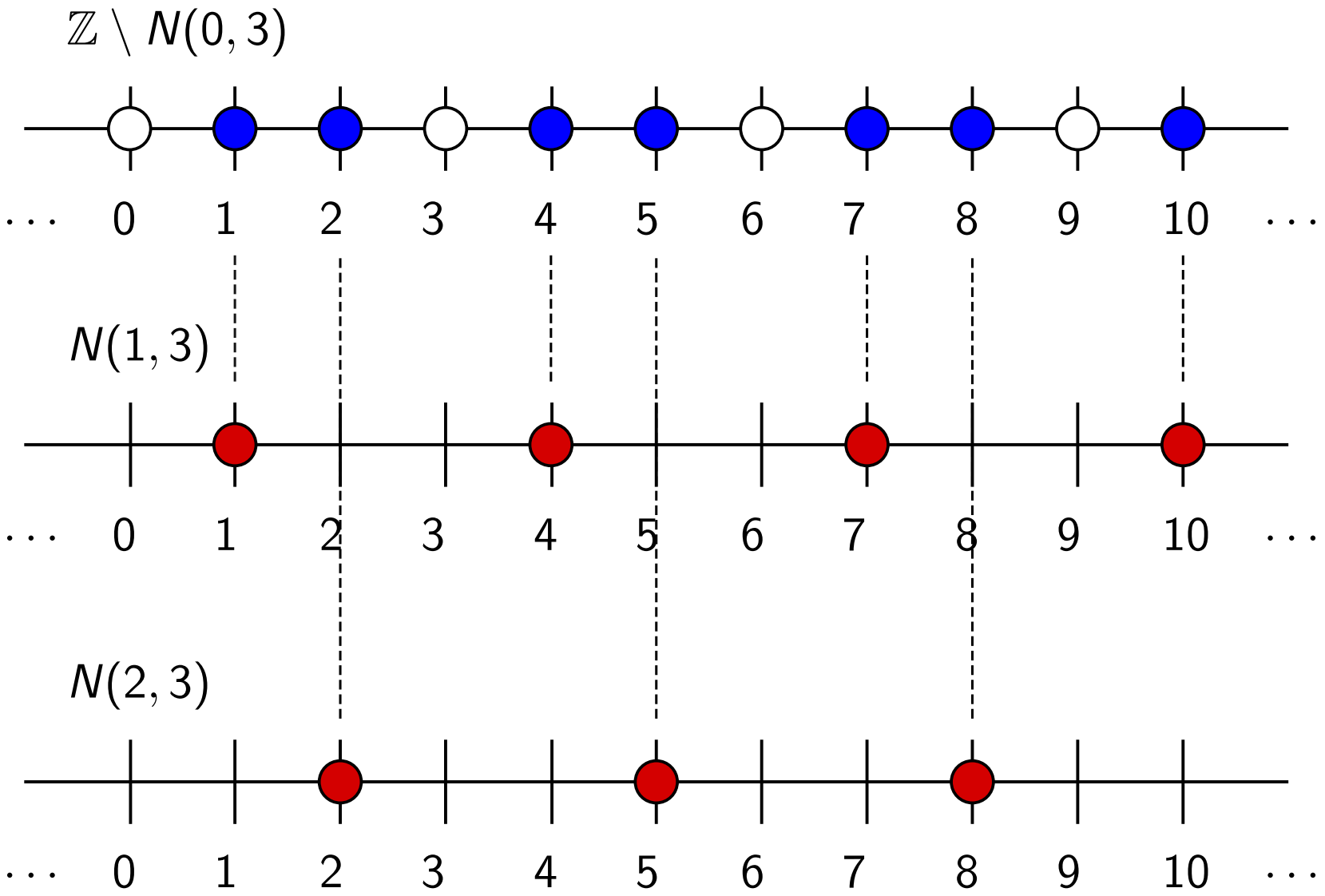
Remarks on Our Newfound Topology (Pt. 2)

- Any non-empty open set is infinite.
- Equivalently, the complement of a finite set cannot be closed.
- The basis sets $N(a, b)$ are closed as well as open. Indeed, we can write them as complements of open sets:

$$N(a, b) = \mathbb{Z} \setminus \bigcup_{i=1}^{|b|-1} N(a + i, b)$$

Example

$N(0, 3) = \{\ldots, -6, -3, 0, 3, 6, \ldots\} =$
$\mathbb{Z} \setminus (\{\ldots, -5, -2, 1, 4, 7, \ldots\} \cup \{\ldots, -4, -1, 2, 5, 8, \ldots\}) =$
$\mathbb{Z} \setminus \bigcup_{i=1}^{|3|-1} N(0 + i, 3)$.


$\mathbb{Z} \setminus N(0,3)$
$N(1,3)$
$N(2,3)$
$\cdots$ 0 1 2 3 4 5 6 7 8 9 10 $\cdots$

The Theorem

We can now easily prove Euclid's Theorem!

Theorem

There are infinitely many prime numbers.

The Proof

Proof.

Assume by way of contradiction that there are finitely many primes. The only integers that aren't multiples of prime numbers are 1 and -1, so

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

- The left-hand side, as a complement of a finite set, cannot be closed.
- However the right-hand side is a finite union of closed sets, which is closed.

Therefore there must be an infinitude of primes. □