Hands-on PVS for mathematicians!

Case of Study:

The infinitude of primes by Fürstenberg's topological argument

PVS for Mathematicians - Tutorial CICM+LSFA 2025

Thaynara Arielly de Lima (IME)

UFG

Mauricio Ayala-Rincón (IE)

UnB

Funded by the Brazilian agencies CAPES, CNPq, and FAPDF

Brasília D.F., Oct 6, 2025

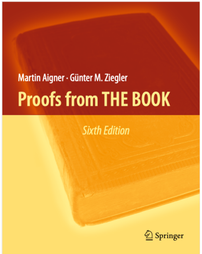
Plan

Infinitude of Primes:

Fürstenberg's Topological Argument [2], [1]

Goal: formalize the Infinitude of Primes following Fürstenberg's topological argumentation.

Let's see the pen-and-paper proof.



Infinitude of Primes:

Fürstenberg's Topological Argument

Topology

A topology over a set X is a collection τ of subsets of X satisfying the following properties:

i) $\emptyset$ and X belong to τ;

ii) The union of elements of any sub-collection of τ belongs to τ;

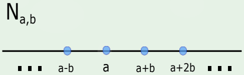
iii) The intersection of elements of a finite sub-collection of τ belongs to τ.

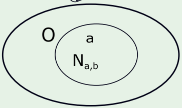
- A set X equipped with a topology τ is called a **topological space**.
- A subset U of a topological space X, that belongs to the collection τ, is called an **open set of** X.

Fürstenberg's Topological Argument

Example

Consider the sets $X = \mathbb{Z}$ and $N_{a,b} = \{a + n \cdot b; n \in \mathbb{Z}\}$, $a, b \in \mathbb{Z}$, where $b > 0$. A set $O \subseteq \mathbb{Z}$ is called open if and only if $O = \emptyset$ or for every $a \in O$, there is an integer $b > 0$ such that $N_{a,b} \subseteq O$.





The collection τ, induced by the open sets of type O, is a topology over $\mathbb{Z}$:

i) $\emptyset$ and $\mathbb{Z}$ belong to τ;

ii) By the definition of elements of τ, the arbitrary union of subsets of τ belongs to τ;

iii) If O_1 and O_2 belong to τ then $O_1 \cap O_2$ belongs to τ.

- In fact, consider $a \in O_1 \cap O_2$. There are b_1 and b_2 such that $N_{a,b_1} \subseteq O_1$ e $N_{a,b_2} \subseteq O_2$. Logo, $N_{a,b_1 \cdot b_2} \subseteq O_1 \cap O_2$.

Fürstenberg's Topological Argument

- **Statement 1:** Any nonempty open set is infinite.
  - Proof: if $O \neq$ then $N_{a,b} \subset O$, for some $a \in O$ and $b > 0$.
- **Statement 2:** For any $a \in \mathbb{Z}$ and $b > 0$, $N_{a,b}$ is an open set.

Fürstenberg's Topological Argument

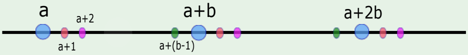
- **Statement 1:** Any nonempty open set is infinite.
  - Proof: if $O \neq$ then $N_{a,b} \subset O$, for some $a \in O$ and $b > 0$.
- **Statement 2:** For any $a \in \mathbb{Z}$ and $b > 0$, $N_{a,b}$ is an open set.

Closed sets

A subset A of a topological space X is called a closed set if and only if its complement A^c is an open set in X.

- **Statement 3:** For any $a \in \mathbb{Z}$ and $b > 0$, $N_{a,b}$ is closed.

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$



and $\bigcup_{i=1}^{b-1} N_{a+i,b}$ is an open set.

Fürstenberg's Topological Argument

Some properties of closed sets

If X is a topological space then:

P1. $\emptyset$ and X are closed sets;

P2. The finite union of closed sets is a closed set;

- Consider A_i, $1 \leq i \leq n$ closed sets. Thus,

$$X \setminus \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (X \setminus A_i) \text{ is an open set}$$

P3. The arbitrary intersection of closed sets is a closed set.

- Consider A_α, a family of closed sets. Thus,

$$X \setminus \bigcap A_\alpha = \bigcup (X \setminus A_\alpha) \text{ is an open set}$$

Fürstenberg's topological argument

- **Statement 4:** Consider k an integer number such that $k \neq 1$ and $k \neq -1$. Therefore, k has a prime divisor p and, consequently, $k \in N_{0,p}$.
  Also,

  $$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}, \text{ where } \mathbb{P} \text{ denotes the set of prime numbers.}$$

If $\mathbb{P}$ is finite then:

- $\bigcup_{p \in \mathbb{P}} N_{0,p}$ is a closed set (**Statement 3 + P2**);
- Thus, $\{-1, 1\}$ is an open set (**By the definition of a closed set)**.
- Consequently $\{-1, 1\}$ is an infinite set. (**Statement 1**)

Therefore, the set $\mathbb{P}$ of the prime numbers is infinite.

References

Aigner, Martin and Ziegler, Günter M. Proofs from THE BOOK. 6th.Springer (2018)

Hillel Fürstenberg. On the Infinitude of Primes. Amer. Math, Monthly. **62**(5) (1955)

Hands-on!

Upload the exercise files.