

Furstenberg's Proof of the Infinitude of Primes in Naproche

Andrei Paskevich, Marcel Schütz

2025

This is a formalization of Furstenberg's topological proof of the infinitude of primes [1, p. 353].

The central idea of Furstenberg's proof is to define a certain topology on \mathbb{N} from the properties of which we can deduce that the set of primes is infinite.¹

Let n, m, k denote natural numbers. Let p, q denote nonzero natural numbers.

Definition 1. Let A be a subset of \mathbb{N} . $A^c := \mathbb{N} \setminus A$.

Let the complement of A stand for A^c .

Lemma 2. The complement of any subset of \mathbb{N} is a subset of \mathbb{N} .

Towards a suitable topology on \mathbb{N} let us define *arithmetic sequences* $N_{n,q}$ on \mathbb{N} .

Definition 3. $N_{n,q} := \{m \in \mathbb{N} \mid m \equiv n \pmod{q}\}$.

This allows us to define the *evenly spaced natural number topology* on \mathbb{N} , whose open sets are defined as follows.

Definition 4. Let U be a subset of \mathbb{N} . U is open iff for any $n \in U$ there exists a q such that $N_{n,q} \subset U$.

Definition 5. A system of open sets is a system of sets S such that every element of S is an open subset of \mathbb{N} .

Lemma 6. Every system of open sets is a set.

¹Actually, Furstenberg's proof makes use of a topology on \mathbb{Z} . But this topology can as well be restricted to \mathbb{N} without substantially changing the proof.

Proof. Let S be a system of open sets. Then $S \subset \mathcal{P}(\mathbb{N})$. Hence S is a set. ■

We can show that the open sets indeed form a topology on \mathbb{N} .

Lemma 7. \mathbb{N} and \emptyset are open.

Lemma 8. Let U, V be open subsets of \mathbb{N} . Then $U \cap V$ is open.

Proof. Let $n \in U \cap V$. Take a q such that $N_{n,q} \subset U$. Take a p such that $N_{n,p} \subset V$. Then $p \cdot q \neq 0$.

Let us show that $N_{n,p \cdot q} \subset U \cap V$. Let $m \in N_{n,p \cdot q}$. We have $m \equiv n \pmod{p \cdot q}$. Hence $m \equiv n \pmod{p}$ and $m \equiv n \pmod{q}$. Thus $m \in N_{n,p}$ and $m \in N_{n,q}$. Therefore $m \in U$ and $m \in V$. Consequently $m \in U \cap V$. End. ■

Lemma 9. Let S be a system of open sets. Then $\bigcup S$ is open.

Proof. Let $n \in \bigcup S$. Take a set M such that $n \in M \in S$. Consider a q such that $N_{n,q} \subset M$. Then $N_{n,q} \subset \bigcup S$. ■

Now that we have a topology of open sets on \mathbb{N} , we can continue with a characterization of closed sets whose key property is that they are closed under finite unions.

Definition 10. Let A be a subset of \mathbb{N} . A is closed iff A^c is open.

Definition 11. A system of closed sets is a system of sets S such that every element of S is a closed subset of \mathbb{N} .

Lemma 12. Every system of closed sets is a set.

Proof. Let S be a system of closed sets. Then $S \subset \mathcal{P}(\mathbb{N})$. $\mathcal{P}(\mathbb{N})$ is a set. Hence S is a set. ■

Lemma 13. Let S be a finite system of closed sets. Then $\bigcup S$ is closed.

Proof. Define $C := \{X \mid X \text{ is a closed subset of } \mathbb{N}\}$.

Let us show that $A \cup B \in C$ for any $A, B \in C$. Let $A, B \in C$. Then A, B are closed subsets of \mathbb{N} . We have $(A \cup B)^c = A^c \cap B^c$. A^c and B^c are open. Hence $A^c \cap B^c$ is open. Thus $A \cup B$ is a closed subset of \mathbb{N} . End.

Therefore C is closed under finite unions. Consequently $\bigcup S \in C$. Indeed S is a subset of C . ■

An important step towards Furstenberg's proof is to show that arithmetic sequences are closed.

Lemma 14. $N_{n,q}$ is closed.

Proof. Let $m \in N_{n,q}^c$.

Let us show that $N_{m,q} \subset N_{n,q}^c$. Let $k \in N_{m,q}$. Assume $k \notin N_{n,q}^c$. Then $k \equiv m \pmod{q}$ and $n \equiv k \pmod{q}$. Hence $m \equiv n \pmod{q}$. Therefore $m \in N_{n,q}$. Contradiction. End. ■

Identifying each prime number p with the arithmetic sequence $N_{0,p}$ yields a bijection between the set \mathbb{P} of all prime numbers and the set P of all such sequences $N_{0,p}$. Thus to show that there are infinitely many primes it suffices to show that P is infinite.

Definition 15. $P := \{N_{0,p} \mid p \in \mathbb{P}\}$.

Lemma 16. P is a system of closed sets.

Proof. $N_{0,p}$ is a closed subset of \mathbb{N} for every $p \in \mathbb{P}$. ■

Lemma 17. P is a set that is equinumerous to \mathbb{P} .

Proof. (1) P is a set. Indeed $P \subset \mathcal{P}(\mathbb{N})$.

(2) P is equinumerous to \mathbb{P} .

Proof. Define $f(p) := N_{0,p}$ for $p \in \mathbb{P}$.

Let us show that f is injective. Let $p, q \in \mathbb{P}$. Assume $f(p) = f(q)$. Then $N_{0,p} = N_{0,q}$. We have $N_{0,p} = \{m \in \mathbb{N} \mid m \equiv 0 \pmod{p}\}$ and $N_{0,q} = \{m \in \mathbb{N} \mid m \equiv 0 \pmod{q}\}$.

We can show that for all $m \in \mathbb{N}$ we have $p \mid m$ iff $q \mid m$. Let $m \in \mathbb{N}$. Then $m \equiv 0 \pmod{p}$ iff $m \equiv 0 \pmod{q}$. Thus $m \bmod p = 0 \bmod p$ iff $m \bmod q = 0 \bmod q$. We have $0 \bmod p = 0 = 0 \bmod q$. Hence $m \bmod p = 0$ iff $m \bmod q = 0$. Therefore $p \mid m$ iff $q \mid m$. End.

Consequently $p = q$. End.

f is surjective onto P . Thus f is a bijection between \mathbb{P} and P . □ ■

Theorem 18 (Furstenberg). \mathbb{P} is infinite.

Proof. $\bigcup P$ is a subset of \mathbb{N} .

Let us show that for any $n \in \mathbb{N}$ we have $n \in \bigcup P$ iff n has a prime divisor. Let $n \in \mathbb{N}$.

If n has a prime divisor then n belongs to $\bigcup P$.

Proof. Assume n has a prime divisor. Take a prime divisor p of n . We have $N_{0,p} \in P$. Hence $n \in N_{0,p}$. □

If n belongs to $\bigcup P$ then n has a prime divisor.

Proof. Assume that n belongs to $\bigcup P$. Take a prime number r such that $n \in N_{0,r}$. Hence $n \equiv 0 \pmod{r}$. Thus $n \bmod r = 0 \bmod r = 0$. Therefore r is a prime divisor of n . \square End.

Hence For all $n \in \mathbb{N}$ we have $n \in \bigcup P^{\complement}$ iff n has no prime divisor. 1 has no prime divisor and any natural number having no prime divisor is equal to 1. Therefore $\bigcup P^{\complement} = \{1\}$. Indeed $\bigcup P^{\complement} \subset \{1\}$ and $\{1\} \subset \bigcup P^{\complement}$.

P is infinite.

Proof by contradiction. Assume that P is finite. Then $\bigcup P$ is closed and $\bigcup P^{\complement}$ is open. Take a p such that $N_{1,p} \subset \bigcup P^{\complement}$. $1+p$ is an element of $N_{1,p}$. Indeed $1+p \equiv 1 \pmod{p}$ (by congruency of sum). $1+p$ is not equal to 1. Hence $1+p \notin \bigcup P^{\complement}$. Contradiction. \square ■

References

- [1] Harry Furstenberg. “On the Infinitude of Primes”. In: *The American Mathematical Monthly* 62.1 (1955).

Copyright

© Andrei Paskevich (2008), Marcel Schütz (2021–2025).