Furstenberg's proof of the infinitude of primes

Naproche formalization:

Andrei Paskevich (2007),
Marcel Schütz (2021)

Furstenberg's proof of the infinitude of primes is a topological proof of the fact that there are infinitely many primes. It was published 1955 while Furstenberg was still an undergraduate student.[1] The following formalization of his proof is based on the notions of natural numbers and sets provided by the following files:

[readtex `arithmetic/sections/03_divisibility/03_modular-arithmetic.ftl.tex`]

[readtex `arithmetic/sections/03_divisibility/04_primes.ftl.tex`]

[readtex `set-theory/sections/01_sets/02_powerset.ftl.tex`]

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.[2] To do so, let us begin with a few preliminaries about natural numbers.

Axiom 0.1. $\mathbb{N}$ is a set.

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

Definition 0.2. Let A be a subset of $\mathbb{N}$. $A^{\complement} = \mathbb{N} \setminus A$.

Let the complement of A stand for $A^{\complement}$.

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

Definition 0.3. $\mathrm{N}_{n,q} = \{m \in \mathbb{N} \mid m \equiv n \pmod{q}\}$.

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

[1] Furstenberg, Harry. 'On the Infinitude of Primes'. The American Mathematical Monthly, vol. 62, no. 5, 1955, pp. 353–353

[2] Actually, 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.

Definition 0.4. Let U be a subset of $\mathbb{N}$. U is open iff for any $n \in U$ there exists a q such that $\mathrm{N}_{n,q} \subseteq U$.

Definition 0.5. A system of open sets is a system of sets S such that every element of S is an open subset of $\mathbb{N}$.

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

Lemma 0.6. $\mathbb{N}$ and $\emptyset$ are open.

Lemma 0.7. Let U, V be open subsets of $\mathbb{N}$. Then $U \cap V$ is open.

Proof. $U \cap V$ is a subset of $\mathbb{N}$. Let $n \in U \cap V$. Take q such that $\mathrm{N}_{n,q} \subseteq U$. Take p such that $\mathrm{N}_{n,p} \subseteq V$.

Let us show that $\mathrm{N}_{n,p\cdot q} \subseteq U \cap V$. Let $m \in \mathrm{N}_{n,p\cdot q}$. We have $m \equiv n \pmod{p \cdot q}$. Hence $m \equiv n \pmod{p}$ and $m \equiv n \pmod{q}$. Thus $m \in \mathrm{N}_{n,p}$ and $m \in \mathrm{N}_{n,q}$. Therefore $m \in U$ and $m \in V$. Consequently $m \in U \cap V$. End. □

Lemma 0.8. Let S be a system of open sets. Then $\bigcup S$ is an open set.

Proof. Let $n \in \bigcup S$. Take a set M such that $n \in M \in S$. Consider a q such that $\mathrm{N}_{n,q} \subseteq M$. Then $\mathrm{N}_{n,q} \subseteq \bigcup S$. □

Now that we have a topology of open sets on $\mathbb{N}$, we can continue with a characterization of closed sets. Their key property is that they are closed under *finite* unions. Since we cannot provide a proper definition of finiteness in the context of this formalization, we cannot prove this closedness condition. All we can do is to prove that the union of *two* closed sets remains closed. Having shown this little fact we will introduce the notion of finiteness axiomatically and state that every finite union of closed sets is indeed closed. Actually this condition is all we need to know about finiteness to prove that there are infinitely many primes.

Definition 0.9. Let A be a subset of $\mathbb{N}$. A is closed iff $A^{\complement}$ is open.

Definition 0.10. 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 0.11. Let A, B be closed subsets of $\mathbb{N}$. Then $A \cup B$ is closed.

Proof. We have $((A \cup B)^{\complement}) = A^{\complement} \cap B^{\complement}$. $A^{\complement}$ and $B^{\complement}$ are open. Hence $A^{\complement} \cap B^{\complement}$ is open. Thus $A \cup B$ is closed. □

Signature 0.12. Let X be a set. X is finite is a relation.

Let X is infinite stand for X is not finite.

Axiom 0.13. Let S be a finite system of closed sets. Then $\bigcup S$ is closed.

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

Lemma 0.14. $\mathrm{N}_{n,q}$ is a closed subset of $\mathbb{N}$.

Proof. Proof by contradiction. Let $m \in (\mathrm{N}_{n,q})^{\complement}$.

Let us show that $\mathrm{N}_{m,q} \subseteq (\mathrm{N}_{n,q})^{\complement}$. Let $k \in \mathrm{N}_{m,q}$. Assume $k \notin (\mathrm{N}_{n,q})^{\complement}$. Then $k \equiv m \pmod{q}$ and $n \equiv k \pmod{q}$. Hence $m \equiv n \pmod{q}$. Therefore $m \in \mathrm{N}_{n,q}$. Contradiction. End. □

Finally, to show that there are infinitely many primes we identify a prime number p with the arithmetic sequence $\mathrm{N}_{0,p}$. In fact we could prove that there exists a bijection between the set of all prime numbers and the set of all arithmetic sequences of this form. But this would go beyond the scope of this formalization.

Definition 0.15. $\mathbb{P} = \{\mathrm{N}_{0,p} \mid p \text{ is a prime number}\}$.

Lemma 0.16. $\mathbb{P}$ is a set.

Proof. Every element of $\mathbb{P}$ is a subset of $\mathbb{N}$. Hence every element of $\mathbb{P}$ is contained in $\mathcal{P}(\mathbb{N})$. Thus $\mathbb{P}$ is a set. □

Theorem 0.17 (Furstenberg). $\mathbb{P}$ is infinite.

Proof. Proof by contradiction.

Let us show that for any natural number n n belongs to $\bigcup \mathbb{P}$ iff n has a prime divisor. Let n be a natural number.

If n has a prime divisor then n belongs to $\bigcup \mathbb{P}$.
Proof. Assume n has a prime divisor. Take a prime divisor p of n. We have $\mathrm{N}_{0,p} \in \mathbb{P}$. Hence $n \in \mathrm{N}_{0,p}$. Qed.

If n belongs to $\bigcup \mathbb{P}$ then n has a prime divisor.
Proof. Assume that n belongs to $\bigcup \mathbb{P}$. Take a prime number r such that $n \in \mathrm{N}_{0,r}$. Hence $n \equiv 0 \pmod{r}$. Thus $n \bmod r = 0 \bmod r = 0$. Therefore r is a prime divisor of n. Qed. End.

Thus we have $(\bigcup \mathbb{P})^{\complement} = \{1\}$. Indeed for any natural number n if n has no prime divisor then we have $n = 1$. Assume that $\mathbb{P}$ is finite. Then $\bigcup \mathbb{P}$ is closed and $(\bigcup \mathbb{P})^{\complement}$ is open. Take a p such that $\mathrm{N}_{1,p} \subseteq (\bigcup \mathbb{P})^{\complement}$. $1 + p$ is an element of $\mathrm{N}_{1,p}$. Indeed $1 + p \equiv 1 \pmod{p}$. $1 + p$ is not equal to 1. Hence $1 + p \notin (\bigcup \mathbb{P})^{\complement}$. Contradiction. □