Furstenberg's proof of the infinitude of primes

Naproche formalization:

Andrei Paskevich (2007),
Marcel Schütz (2021 - 2022)

This is a formalization of Furstenberg's topological proof of the infinitude of primes [1, p. 353]. On mid-range hardware Naproche needs approximately 5 Minutes to verify this formalization plus approximately 30 minutes to verify the library files it depends on.

[readtex `arithmetic/sections/10_primes.ftl.tex`]

[readtex `foundations/sections/13_equinumerosity.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.[1]

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

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

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

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* $\mathrm{N}_{n,q}$ on $\mathbb{N}$.

Definition 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.

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 $\mathrm{N}_{n,q} \subseteq U$.

Definition 5. A system of open sets is a system of sets S such that every

[1] 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.

element of S is an open subset of $\mathbb{N}$.

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

Lemma 6. $\mathbb{N}$ and $\emptyset$ are open.

Lemma 7. 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 $\mathrm{N}_{n,q} \subseteq U$. Take a p such that $\mathrm{N}_{n,p} \subseteq V$. Then $p \cdot q \neq 0$.

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 8. 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 $\mathrm{N}_{n,q} \subseteq M$. 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 plus the fact that sets which are equinumerous to an infinite set are also infinite is all we need to know about the notion of finiteness to prove that there are infinitely many primes.

Definition 9. Let A be a subset of $\mathbb{N}$. A is closed iff $A^{\complement}$ is open.

Definition 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 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 12. Let X be a class. X is finite is an atom.

Let X is infinite stand for X is not finite.

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

Axiom 14. Let X, Y be classes. If X is infinite and X is equinumerous to Y then Y is infinite.

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

Lemma 15. $\mathrm{N}_{n,q}$ is closed.
Proof. 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. □

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

Definition 16. $\mathrm{P} = \{\mathrm{N}_{0,p} \mid p \in \mathbb{P}\}$.

Lemma 17. P is a system of closed sets.

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

Lemma 18. P is a set that is equinumerous to $\mathbb{P}$.

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

(2) P is equinumerous to $\mathbb{P}$.
Proof. Define $f(p) = \mathrm{N}_{0,p}$ for $p \in \mathbb{P}$.

Let us show that f is injective. Let $p, q \in \mathbb{P}$. Assume $f(p) = f(q)$. Then $\mathrm{N}_{0,p} = \mathrm{N}_{0,q}$. We have $\mathrm{N}_{0,p} = \{m \in \mathbb{N} \mid m \equiv 0 \pmod p\}$ and $\mathrm{N}_{0,q} = \{m \in \mathbb{N} \mid m \equiv 0 \pmod q\}$. Hence for all $m \in \mathbb{N}$ we have $m \equiv 0 \pmod p$ iff $m \equiv 0 \pmod q$. Thus for all $m \in \mathbb{N}$ we have $m \bmod p = 0 \bmod p$ iff $m \bmod q = 0 \bmod q$. We have $0 \bmod p = 0 = 0 \bmod q$. Hence for all $m \in \mathbb{N}$ we have $m \bmod p = 0$ iff $m \bmod q = 0$. Thus for all $m \in \mathbb{N}$ we have $p \mid m$ iff $q \mid m$. Therefore $p = q$. End.

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

Theorem 19 (Furstenberg). $\mathbb{P}$ is infinite.

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

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

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

If n belongs to $\bigcup \mathrm{P}$ then n has a prime divisor.
Proof. Assume that n belongs to $\bigcup \mathrm{P}$. 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.

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

equal to 1.

P is infinite.
Proof by contradiction. Assume that P is finite. Then $\bigcup \mathrm{P}$ is closed and $(\bigcup \mathrm{P})^{\complement}$ is open. Take a p such that $\mathrm{N}_{1,p} \subseteq (\bigcup \mathrm{P})^{\complement}$. $1 + p$ is an element of $\mathrm{N}_{1,p}$. Indeed $1 + p \equiv 1 \pmod{p}$ (by 8.12). $1 + p$ is not equal to 1. Hence $1 + p \notin (\bigcup \mathrm{P})^{\complement}$. Contradiction. Qed. □

References

[1] Harry Furstenberg (1955), *On the Infinitude of Primes*; The American Mathematical Monthly, vol. 62, no. 5