Furstenberg's Proof of the Infinitude of Primes

Andrei Paskevich (2007), Steffen Frerix (2018), 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].

1 Integers

The central idea of Furstenberg's proof is to define a certain topology on $\mathbb{Z}$ from the properties of which we can deduce that the set of primes is infinite. So first we have to introduce the ring $\mathbb{Z}$ of integers. In fact, we do not need to give a full axiomatization of integer arithmetic; it suffices to assume that $\mathbb{Z}$ is an integral domain.

Let us start by introducing the signature of the ring of integers.

[read `examples/preliminaries.ftl.tex`]

Signature 1. An integer is an object.

Let $a, b, c, d, i, j, k, l, m, n$ stand for integers.

Signature 2. 0 is an integer.

Signature 3. 1 is an integer.

Signature 4. $-a$ is an integer.

Signature 5. $a + b$ is an integer.

Signature 6. $a \cdot b$ is an integer.

Let $a - b$ stand for $a + (-b)$.

Moreover, we assume $(\mathbb{Z}, 0, +, -)$ to be an abelian group and $(\mathbb{Z}, 1, \cdot)$ to be a commutative monoid which satisfy the distribution laws.

Axiom 7. $a + (b + c) = (a + b) + c$.

Axiom 8. $a + b = b + a$.

Axiom 9. $a + 0 = a = 0 + a$.

Axiom 10. $a - a = 0 = -a + a$.

Axiom 11. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Axiom 12. $a \cdot b = b \cdot a$.

Axiom 13. $a \cdot 1 = a = 1 \cdot a$.

Axiom 14. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Lemma 15. $a \cdot 0 = 0 = 0 \cdot a$.

Proof. $a \cdot 0 = a \cdot (1 - 1) = a - a = 0$. □

Lemma 16. $-1 \cdot a = -a = a \cdot -1$.

Proof. $(-1 \cdot a) + a = 0$. □

Furthermore, we assume that our ring is not trivial and that there are no non-trivial zero divisors.

Axiom 17. $0 \neq 1$.

Axiom 18. $a \neq 0 \wedge b \neq 0 \implies a \cdot b \neq 0$.

Lemma 19. $-(-a)$ is an integer.

Let us continue with the notion of divisors and congruency.

Let a is nonzero stand for $a \neq 0$. Let p, q stand for nonzero integers.

Definition 20. A divisor of b is a nonzero integer a such that for some n $(a \cdot n = b)$.

Let a divides b stand for a is a divisor of b. Let $a \mid b$ stand for a is a divisor of b.

Definition 21. $a = b \pmod{q}$ iff $q \mid a - b$.

Lemma 22. $a = a \pmod{q}$.

Lemma 23. $a = b \pmod{q} \implies b = a \pmod{q}$.

Proof. Assume that $a = b \pmod{q}$.

(1) Take n such that $q \cdot n = a - b$.

$q \cdot (-n). = (-1) \cdot (q \cdot n)$ (by MulMinOne, MulAsso, MulComm) $. = (-1) \cdot (a - b)$ (by 1). □

Lemma 24. $a = b \pmod{q} \wedge b = c \pmod{q} \implies a = c \pmod{q}$.

Proof. Assume that $a = b \pmod{q} \wedge b = c \pmod{q}$. Take n such that $q \cdot n = a - b$. Take m such that $q \cdot m = b - c$. We have $q \cdot (n + m) = a - c$. □

Lemma 25. $a = b \pmod{p \cdot q} \implies a = b \pmod{p} \wedge a = b \pmod{q}$.

Proof. Assume that $a = b \pmod{p \cdot q}$. Take m such that $(p \cdot q) \cdot m = a - b$. We have $p \cdot (q \cdot m) = a - b = q \cdot (p \cdot m)$. □

Note that up to now every finite field could be a model of our theory. But since we want to prove that there are *infinitely* many primes we must eventually add some axiom which eliminates such models.

This is done by introducing the notion of prime integers. All we need to know about them for Furstenberg's proof is that every integer n has a prime divisor iff $n \neq 1$ and $n \neq -1$.

Signature 26. a is prime is an atom.

Let a prime stand for a prime nonzero integer.

Axiom 27. n has a prime divisor iff $n \neq 1 \wedge n \neq -1$.

Let us assume that some finite field is a model of our current theory. Recall that in any finite field every non-zero element is a divisor of 1. Let us rephrase axiom *PrimeDivisor*:

$$n \text{ has no prime divisor iff } n = 1 \vee n = -1.$$

Then we immediately see that 1 has no prime divisor. But since every non-zero element is a divisor of 1, no non-zero element is prime. Hence 0 has also no prime divisor (recall that any divisor must be non-zero). But then, again by the axiom, we get $0 = 1 \vee 0 = -1$, a contradiction (by *NonTriv*).

2 Finite classes

Another important notion is that of finite subsets of $\mathbb{Z}$. We leave the characterization of what it means for a set to be finite for the next sections.

Let S, T stand for classes.

Signature 28. S is finite is an atom.

Let S is infinite stand for S is not finite.

3 Sets of integers

Since Furstenberg's proof is a topological proof we have to define unions, intersections and also complements of sets.

Definition 29. $\mathbb{Z}$ is the class of integers.

Axiom 30. $\mathbb{Z}$ is a set.

Let A, B, C, D stand for subclasses of $\mathbb{Z}$.

Definition 31. A family of integer sets is a class S such that every element of S is a subset of $\mathbb{Z}$.

Definition 32. Let S be a family of integer sets. $\bigcup S = \{x \in \mathbb{Z} \mid x \text{ belongs to some element of } S\}$.

Lemma 33. Let S be a family of integer sets. $\bigcup S$ is a subset of $\mathbb{Z}$.

Definition 34. $\overline{A} = \{x \in \mathbb{Z} \mid x \text{ does not belong to } A\}$.

Lemma 35. $\overline{A}$ is a subset of $\mathbb{Z}$.

4 Introducing topology

In our next step towards a suitable topology on $\mathbb{Z}$ let us define arithmetic sequences, i.e. sets of the form $q\mathbb{Z} + a$.

Let a, b, c denote integers. Let p, q stand for nonzero integers. Let A, B, C stand for subsets of $\mathbb{Z}$.

Definition 36. $q\mathbb{Z} + a = \{b \in \mathbb{Z} \mid b = a \pmod{q}\}$.

Lemma 37. $q\mathbb{Z} + a$ is a set.

This allows us to define the so-called *evenly spaced integer topology* where its open sets are defined as follows:

Definition 38. A is open iff $A = \mathbb{Z}$ or for any $a \in A$ there exists q such that $q\mathbb{Z} + a \subseteq A$.

Note that we have declared q as a *non-zero* integer. Otherwise, every set A would be open since $0\mathbb{Z} + a = \{a\} \subseteq A$ for every $a \in A$.

Definition 39. A is closed iff $\overline{A}$ is open.

Definition 40. An family of open sets is a family of integer sets S such that every element of S is open.

We can easily check that the open sets really form a topology on $\mathbb{Z}$.

Lemma 41. Let S be an family of open sets. $\bigcup S$ is open.

Proof. Let $x \in \bigcup S$. Take a set M such that (M is an element of S and $x \in M$). Take q such that $q\mathbb{Z} + x \subseteq M$. Then $q\mathbb{Z} + x \subseteq \bigcup S$. □

Lemma 42. Let A, B be open subsets of $\mathbb{Z}$. Then $A \cap B$ is a subset of $\mathbb{Z}$ and $A \cap B$ is open.

Proof. $A \cap B$ is a subset of $\mathbb{Z}$. Let $x \in A \cap B$. Then x is an integer. Take q such that $q\mathbb{Z} + x \subseteq A$. Take p such that $p\mathbb{Z} + x \subseteq B$.

Let us show that $p \cdot q$ is a nonzero integer and $(p \cdot q)\mathbb{Z} + x \subseteq A \cap B$. $p \cdot q$ is a nonzero integer. Let $a \in (p \cdot q)\mathbb{Z} + x$.

$a \in p\mathbb{Z} + x$ and $a \in q\mathbb{Z} + x$.
Proof. x is an integer and $a = x \pmod{p \cdot q}$. $a = x \pmod{p}$ and $a = x \pmod{q}$ (by EquModMul). Qed.

Therefore $a \in A$ and $a \in B$. Hence $a \in A \cap B$. End. □

Lemma 43. Let A, B be closed subsets of $\mathbb{Z}$. $A \cup B$ is closed.

Proof. We have $\overline{A}, \overline{B} \subseteq \mathbb{Z}$. $\overline{A \cup B} = \overline{A} \cap \overline{B}$. □

Now we state a consequence of finiteness:

Axiom 44. Let S be a finite family of integer sets such that all elements of S are closed subsets of $\mathbb{Z}$. $\bigcup S$ is closed.

This characterization allows us to prove that a family S of closed sets is infinite by assuming S to be finite and deriving a contradiction from this assumption together with the statement that $\bigcup S$ is closed. In Furstenberg's proof we will use this method to show that the family $\{r\mathbb{Z} \mid r \text{ is prime}\}$ is infinite. To use the above argument we thus have to prove that any $r\mathbb{Z}$ – or more general any $q\mathbb{Z} + a$ – is closed.

Lemma 45. $q\mathbb{Z} + a$ is a closed subset of $\mathbb{Z}$.

Proof by contradiction. $q\mathbb{Z} + a$ is a subset of $\mathbb{Z}$. Let $b \in \overline{q\mathbb{Z} + a}$.

Let us show that $q\mathbb{Z} + b \subseteq \overline{q\mathbb{Z} + a}$. Let $c \in q\mathbb{Z} + b$. Assume $c \notin \overline{q\mathbb{Z} + a}$. Then $c = b \pmod{q}$ and $a = c \pmod{q}$. Hence $b = a \pmod{q}$. Therefore $b \in q\mathbb{Z} + a$. Contradiction. End. □

To prove that there are infinitely many primes we identify a prime number r with the set $r\mathbb{Z}$ and show that the set $S = \{r\mathbb{Z} \mid r \text{ is a prime}\}$ is infinite. It is easy to see that $\bigcup S = \{\text{integer } n \mid n \text{ has a prime divisor}\} = \mathbb{Z} \setminus \{1, -1\}$. So if S is finite then $\bigcup S$ is closed (by *UnionClosed*) and hence $\{1, -1\}$ is open. But then some arithmetic sequence $p\mathbb{Z} + 1$ (where p is non-zero) is contained in $\{1, -1\}$ which obviously cannot be.

Theorem 46 (Fuerstenberg). Let $S = \{r\mathbb{Z} + 0 \mid r \text{ is a prime}\}$. S is infinite.

Proof by contradiction. S is a family of integer sets.

We have $\overline{\bigcup S} = \{1, -1\}$.
Proof. Let us show that for any integer n n belongs to $\bigcup S$ iff n has a prime divisor. Let n be an integer.

If n has a prime divisor then n belongs to $\bigcup S$.
Proof. Assume n has a prime divisor. Take a prime divisor p of n. $p\mathbb{Z}+0 \in$

S. $n \in p\mathbb{Z} + 0$. Qed.

If n belongs to $\bigcup S$ then n has a prime divisor.
Proof. Assume n belongs to $\bigcup S$. Take a prime r such that $n \in r\mathbb{Z} + 0$. Then r is a prime divisor of n. Qed. End. Qed.

Assume that S is finite. Then $\bigcup S$ is closed and $\overline{\bigcup S}$ is open.

Take p such that $p\mathbb{Z} + 1 \subseteq \overline{\bigcup S}$.

$p\mathbb{Z} + 1$ has an element x such that neither $x = 1$ nor $x = -1$.
Proof. $1 + p$ and $1 - p$ are integers. $1 + p$ and $1 - p$ belong to $p\mathbb{Z} + 1$. Indeed $1 + p = 1 \pmod p$ and $1 - p = 1 \pmod p$. $1 + p \neq 1 \wedge 1 - p \neq 1$. $1 + p \neq -1 \vee 1 - p \neq -1$. Qed.

We have a contradiction. □

Note that we cannot define $q\mathbb{Z}$ as $q\mathbb{Z} + 0$ in our formalization since then any term of the form $q\mathbb{Z} + a$ would be ambiguous: It could either be interpreted as $q\mathbb{Z} + a$ or as $(q\mathbb{Z} + 0) + a$. This is a result of some kind of overloading of the symbol $+$. We use $+$ on the one hand to denote integer addition and on the other hand it is part of the operator $\cdot\, \mathbb{Z} + \,\cdot$.

References

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