Furstenberg's Topology And His Proof of the Infinitude of Primes

Manuel Eberl

March 17, 2025

Abstract

This article gives a formal version of Furstenberg's topological proof of the infinitude of primes. He defines a topology on the integers based on arithmetic progressions (or, equivalently, residue classes). Using some fairly obvious properties of this topology, the infinitude of primes is then easily obtained.

Apart from this, this topology is also fairly 'nice' in general: it is second countable, metrizable, and perfect. All of these (well-known) facts are formally proven, including an explicit metric for the topology given by Zulfeqarr.

Contents

1 Furstenberg's topology and his proof of the infinitude of primes

theory *Furstenberg-Topology*
  imports
    HOL−Real-Asymp.Real-Asymp
    HOL−Analysis.Analysis
    HOL−Number-Theory.Number-Theory
begin

This article gives a formal version of Furstenberg's topological proof of the infinitude of primes [2]. He defines a topology on the integers based on arithmetic progressions (or, equivalently, residue classes).

Apart from yielding a short proof of the infinitude of primes, this topology is also fairly 'nice' in general: it is second countable, metrizable, and perfect. All of these (well-known) facts will be formally proven below.

1.1 Arithmetic progressions of integers

We first define 'bidirectional infinite arithmetic progressions' on $\mathbb{Z}$ in the sense that to an integer a and a positive integer b, we associate all the integers x such that $x \equiv a \pmod{b}$, or, equivalently, $\{a + nb \mid n \in \mathbb{Z}\}$.

definition *arith-prog* :: *int* ⇒ *nat* ⇒ *int set* **where**
  arith-prog a b = {*x*. [*x* = *a*] (*mod int b*)}

lemma *arith-prog-0-right* [*simp*]: *arith-prog a 0* = {*a*}
  ⟨*proof*⟩

lemma *arith-prog-Suc-0-right* [*simp*]: *arith-prog a* (*Suc 0*) = *UNIV*
  ⟨*proof*⟩

lemma *in-arith-progI* [*intro*]: [*x* = *a*] (*mod b*) ⟹ *x* ∈ *arith-prog a b*
  ⟨*proof*⟩

Two arithmetic progressions with the same period and noncongruent starting points are disjoint.

lemma *arith-prog-disjoint*:
  assumes [*a* ≠ *a'*] (*mod int b*) **and** *b* > *0*
  shows *arith-prog a b* ∩ *arith-prog a' b* = {}
  ⟨*proof*⟩

Multiplying the period gives us a subset of the original progression.

lemma *arith-prog-dvd-mono*: *b dvd b'* ⟹ *arith-prog a b'* ⊆ *arith-prog a b*
  ⟨*proof*⟩

The following proves the alternative definition mentioned above.

lemma *bij-betw-arith-prog*:
  assumes $b > 0$
  shows $bij\text{-}betw\ (\lambda n.\ a + int\ b * n)\ UNIV\ (arith\text{-}prog\ a\ b)$
$\langle proof \rangle$

lemma *arith-prog-altdef*: $arith\text{-}prog\ a\ b = range\ (\lambda n.\ a + int\ b * n)$
$\langle proof \rangle$

A simple corollary from this is also that any such arithmetic progression is infinite.

lemma *infinite-arith-prog*: $b > 0 \Longrightarrow infinite\ (arith\text{-}prog\ a\ b)$
  $\langle proof \rangle$

1.2 The Furstenberg topology on $\mathbb{Z}$

The typeclass-based topology is somewhat nicer to use in Isabelle/HOL, but the integers, of course, already have a topology associated to them. We therefore need to introduce a type copy of the integers and furnish them with the new topology. We can easily convert between them and the 'proper' integers using Lifting and Transfer.

typedef $fbint = UNIV :: int\ set$
  morphisms *int-of-fbint fbint* $\langle proof \rangle$

setup-lifting *type-definition-fbint*

lift-definition $arith\text{-}prog\text{-}fb :: int \Rightarrow nat \Rightarrow fbint\ set$ **is** *arith-prog* $\langle proof \rangle$

instantiation $fbint :: topological\text{-}space$
begin

Furstenberg defined the topology as the one generated by all arithmetic progressions. We use a slightly more explicit equivalent formulation that exploits the fact that the intersection of two arithmetic progressions is again an arithmetic progression (or empty).

lift-definition $open\text{-}fbint :: fbint\ set \Rightarrow bool$ **is**
  $\lambda U.\ (\forall x \in U.\ \exists b > 0.\ arith\text{-}prog\ x\ b \subseteq U)$ $\langle proof \rangle$

We now prove that this indeed forms a topology.

instance $\langle proof \rangle$

end

Since any non-empty open set contains an arithmetic progression and arithmetic progressions are infinite, we obtain that all nonempty open sets are infinite.

lemma *open-fbint-imp-infinite*:

fixes U :: *fbint set*
assumes *open* U **and** $U \neq \{\}$
shows *infinite* U
$\langle proof \rangle$

lemma *not-open-finite-fbint* [*simp*]:
assumes *finite* (U :: *fbint set*) $U \neq \{\}$
shows $\neg$*open* U
$\langle proof \rangle$

More or less by definition, any arithmetic progression is open.

lemma *open-arith-prog-fb* [*intro*]:
assumes $b > 0$
shows *open* (*arith-prog-fb* a b)
$\langle proof \rangle$

Slightly less obviously, any arithmetic progression is also closed. This can be seen by realising that for a period b, we can partition the integers into b congruence classes and then the complement of each congruence class is the union of the other $b - 1$ classes, and unions of open sets are open.

lemma *closed-arith-prog-fb* [*intro*]:
assumes $b > 0$
shows *closed* (*arith-prog-fb* a b)
$\langle proof \rangle$

1.3 The infinitude of primes

The infinite of the primes now follows quite obviously: The multiples of any prime form a closed set, so if there were only finitely many primes, the union of all of these would also be open. However, since any number other than ± 1 has a prime divisor, the union of all these sets is simply $\mathbb{Z} \setminus \{\pm 1\}$, which is obviously *not* closed since the finite set $\{\pm 1\}$ is not open.

theorem *infinite* $\{p::nat.\ prime\ p\}$
$\langle proof \rangle$

1.4 Additional topological properties

Just for fun, let us also show a few more properties of Furstenberg's topology. First, we show the equivalence to the above to Furstenberg's original definition (the topology generated by all arithmetic progressions).

theorem *topological-basis-fbint*: *topological-basis* $\{$*arith-prog-fb* a b $|a\ b.\ b > 0\}$
$\langle proof \rangle$

lemma *open-fbint-altdef*: *open* = *generate-topology* $\{$*arith-prog-fb* a b $|a\ b.\ b > 0\}$
$\langle proof \rangle$

From this, we can immediately see that it is second countable:

instance *fbint* :: *second-countable-topology*
⟨*proof*⟩

A trivial consequence of the fact that nonempty open sets in this topology are infinite is that it is a perfect space:

instance *fbint* :: *perfect-space*
⟨*proof*⟩

It is also Hausdorff, since given any two distinct integers, we can easily construct two non-overlapping arithmetic progressions that each contain one of them. We do not *really* have to prove this since we will get it for free later on when we show that it is a metric space, but here is the proof anyway:

instance *fbint* :: *t2-space*
⟨*proof*⟩

Next, we need a small lemma: Given an additional assumption, a T_2 space is also T_3:

lemma *t2-space-t3-spaceI*:
assumes $\bigwedge(x :: {'a} :: \mathit{t2\text{-}space})\ U.\ x \in U \Longrightarrow \mathit{open}\ U \Longrightarrow$
$\exists\, V.\ x \in V \wedge \mathit{open}\ V \wedge \mathit{closure}\ V \subseteq U$
shows $\mathit{OFCLASS}({'a},\ \mathit{t3\text{-}space\text{-}class})$
⟨*proof*⟩

Since the Furstenberg topology is T_2 and every arithmetic progression is also closed, we can now easily show that it is also T_3 (i. e. regular). Again, we do not really need this proof, but here it is:

instance *fbint* :: *t3-space*
⟨*proof*⟩

1.5 Metrizability

The metrizability of Furstenberg's topology (i. e. that it is induced by some metric) can be shown from the fact that it is second countable and T_3 using Urysohn's Metrization Theorem, but this is not available in Isabelle yet. Let us therefore give an *explicit* metric, as described by Zulfeqarr [3]. We follow the exposition by Dirmeier [1].

First, we define a kind of norm on the integers. The norm depends on a real parameter $q > 1$. The value of q does not matter in the sense that all values induce the same topology (which we will show). For the final definition, we then simply pick $q = 2$.

locale *fbnorm* =
fixes q :: *real*
assumes *q-gt-1*: $q > 1$
begin

definition N :: *int* $\Rightarrow$ *real* **where**
$N\ n = (\sum k.\ if\ k = 0 \vee int\ k\ dvd\ n\ then\ 0\ else\ 1\ /\ q\ \widehat{}\ k)$

lemma *N-summable*: $summable\ (\lambda k.\ if\ k = 0 \vee int\ k\ dvd\ n\ then\ 0\ else\ 1\ /\ q\ \widehat{}\ k)$
⟨*proof*⟩

lemma *N-sums*: $(\lambda k.\ if\ k = 0 \vee int\ k\ dvd\ n\ then\ 0\ else\ 1\ /\ q\ \widehat{}\ k)\ sums\ N\ n$
⟨*proof*⟩

lemma *N-nonneg*: $N\ n \geq 0$
⟨*proof*⟩

lemma *N-uminus* [*simp*]: $N\ (-n) = N\ n$
⟨*proof*⟩

lemma *N-minus-commute*: $N\ (x - y) = N\ (y - x)$
⟨*proof*⟩

lemma *N-zero* [*simp*]: $N\ 0 = 0$
⟨*proof*⟩

lemma *not-dvd-imp-N-ge*:
assumes $\neg n\ dvd\ a\ n > 0$
shows $N\ a \geq 1\ /\ q\ \widehat{}\ n$
⟨*proof*⟩

lemma *N-lt-imp-dvd*:
assumes $N\ a < 1\ /\ q\ \widehat{}\ n$ **and** $n > 0$
shows $n\ dvd\ a$
⟨*proof*⟩

lemma *N-pos*:
assumes $n \neq 0$
shows $N\ n > 0$
⟨*proof*⟩

lemma *N-zero-iff* [*simp*]: $N\ n = 0 \longleftrightarrow n = 0$
⟨*proof*⟩

lemma *N-triangle-ineq*: $N\ (n + m) \leq N\ n + N\ m$
⟨*proof*⟩

lemma *N-1*: $N\ 1 = 1\ /\ (q * (q - 1))$
⟨*proof*⟩

It follows directly from the definition that norms fulfil a kind of monotonicity property with respect to divisibility: the norm of a number is at most as large as the norm of any of its factors:

lemma *N-dvd-mono*:

assumes $m\ dvd\ n$
shows $N\ n \leq N\ m$
⟨*proof*⟩

In particular, this means that 1 and -1 have the greatest norm.

lemma *N-le-N-1*: $N\ n \leq N\ 1$
⟨*proof*⟩

Primes have relatively large norms, almost reaching the norm of 1:

lemma *N-prime*:
assumes *prime p*
shows $N\ p = N\ 1 - 1\ /\ q\ \hat{}\ nat\ p$
⟨*proof*⟩

lemma *N-2*: $N\ 2 = 1\ /\ (q\ \hat{}\ 2 * (q - 1))$
⟨*proof*⟩

lemma *N-less-N-1*:
assumes $n \neq 1\ n \neq -1$
shows $N\ n < N\ 1$
⟨*proof*⟩

Composites, on the other hand, do not achieve this:

lemma *nonprime-imp-N-lt*:
assumes $\neg$*prime-elem* $n\ |n| \neq 1\ n \neq 0$
shows $N\ n < N\ 1 - 1\ /\ q\ \hat{}\ nat\ |n|$
⟨*proof*⟩

This implies that one can use the norm as a primality test:

lemma *prime-iff-N-eq*:
assumes $n \neq 0$
shows *prime-elem* $n \longleftrightarrow N\ n = N\ 1 - 1\ /\ q\ \hat{}\ nat\ |n|$
⟨*proof*⟩

Factorials, on the other hand, have very small norms:

lemma *N-fact-le*: $N\ (fact\ m) \leq 1\ /\ (q - 1) * 1\ /\ q\ \hat{}\ m$
⟨*proof*⟩

lemma *N-prime-mono*:
assumes *prime p prime p'* $p \leq p'$
shows $N\ p \leq N\ p'$
⟨*proof*⟩

lemma *N-prime-ge*:
assumes *prime p*
shows $N\ p \geq 1\ /\ (q^2 * (q - 1))$
⟨*proof*⟩

lemma *N-prime-elem-ge*:
assumes *prime-elem p*
shows $N\ p \geq 1\ /\ (q^2 * (q - 1))$
⟨*proof*⟩

Next, we use this norm to derive a metric:

lift-definition *dist* :: *fbint* ⇒ *fbint* ⇒ *real* **is**
$\lambda x\ y.\ N\ (x - y)$ ⟨*proof*⟩

lemma *dist-self* [*simp*]: $dist\ x\ x = 0$
⟨*proof*⟩

lemma *dist-sym* [*simp*]: $dist\ x\ y = dist\ y\ x$
⟨*proof*⟩

lemma *dist-pos*: $x \neq y \Longrightarrow dist\ x\ y > 0$
⟨*proof*⟩

lemma *dist-eq-0-iff* [*simp*]: $dist\ x\ y = 0 \longleftrightarrow x = y$
⟨*proof*⟩

lemma *dist-triangle-ineq*: $dist\ x\ z \leq dist\ x\ y + dist\ y\ z$
⟨*proof*⟩

Lastly, we show that the metric we defined indeed induces the Furstenberg topology.

theorem *dist-induces-open*:
$open\ U \longleftrightarrow (\forall x \in U.\ \exists e > 0.\ \forall y.\ dist\ x\ y < e \longrightarrow y \in U)$
⟨*proof*⟩

end

We now show that the Furstenberg space is a metric space with this metric (with $q = 2$), which essentially only amounts to plugging together all the results from above.

interpretation *fb*: *fbnorm 2*
⟨*proof*⟩

instantiation *fbint* :: *dist*
begin

definition *dist-fbint* **where** *dist-fbint* = *fb.dist*

instance ⟨*proof*⟩

end

instantiation *fbint* :: *uniformity-dist*
begin

definition *uniformity-fbint* :: (*fbint* $\times$ *fbint*) *filter* **where**
uniformity-fbint = (*INF* *e*∈{*0* <..}. *principal* {(*x*, *y*). *dist* *x* *y* < *e*})

instance ⟨*proof*⟩

end

instance *fbint* :: *open-uniformity*
⟨*proof*⟩

instance *fbint* :: *metric-space*
⟨*proof*⟩

In particular, we can now show that the sequence $n!$ tends to 0 in the Furstenberg topology:

lemma *tendsto-fbint-fact*: (λn. *fbint* (*fact* *n*)) $\longrightarrow$ *fbint* *0*
⟨*proof*⟩

end

References

[1] A. Dirmeier. On metrics inducing the Fürstenberg topology on the integers. https://arxiv.org/abs/1912.11663, 2019.

[2] H. Furstenberg. On the infinitude of primes. *The American Mathematical Monthly*, 62(5):353, May 1955.

[3] F. Zulfeqarr. Some interesting consequences of Furstenberg topology. *Resonance*, 24(7):755–765, July 2019.