THE "TOPOLOGICAL" PROOF OF THE INFINITUDE OF PRIMES

KEITH CONRAD

1. Introduction

In 1955, Furstenberg published a proof that there are infinitely many primes using properties of a topology on $\mathbf{Z}$ based on arithmetic progressions. His paper [1] (see also [2]) is less than half a page. We will review the proof and then see how it is based on the same idea as Euclid's proof of the infinitude of primes.

2. The proof

Define a topology on $\mathbf{Z}$ as follows: a nonempty subset $U \subset \mathbf{Z}$ will be called *open* if for each $a \in U$ there is an arithmetic progression $a + m\mathbf{Z}$ for some $m \geq 1$ such that $a + m\mathbf{Z} \subset U$.[1] Including $\emptyset$ as an open subset of $\mathbf{Z}$ too, let's check that these open subsets fit the conditions to be a topology:

(1) By definition $\emptyset$ is open, and also $\mathbf{Z} = 0 + 1\mathbf{Z}$ is open.

(2) If $\{U_i\}$ is an arbitrary collection of open subsets of $\mathbf{Z}$ then their union $\bigcup_i U_i$ is open, since for each $a \in \bigcup_i U_i$ we have $a \in U_i$ for some i, so $a + m\mathbf{Z} \subset U_i$ for some $m \geq 1$. Then $a + m\mathbf{Z} \subset \bigcup_i U_i$.

(3) To show openness is preserved under finite intersections, let $U_1, \ldots, U_k$ be finitely many open subsets. Without loss of generality assume $\bigcap_{i=1}^k U_i \neq \emptyset$. For $a \in \bigcap_{i=1}^k U_i$, there are arithmetic progressions $a + m_i\mathbf{Z} \subset U_i$ where $m_i \geq 1$. Then $a + m_1 \cdots m_k\mathbf{Z}$ is an arithmetic progression contained in each $a + m_i\mathbf{Z}$, so $a + m_1 \cdots m_k\mathbf{Z} \subset \bigcap_{i=1}^k U_i$. Thus each element of $\bigcap_{i=1}^k U_i$ is contained in an arithmetic progression that's entirely in $\bigcap_{i=1}^k U_i$, so $\bigcap_{i=1}^k U_i$ is open.

This topology on $\mathbf{Z}$ has the following two properties:

- Every nonempty open subset of $\mathbf{Z}$ is infinite, since a nonempty open subset contains an arithmetic progression.
- Every arithmetic progression $a + m\mathbf{Z}$ is both open and closed. To show it is open, for each $a + mb$ in $a + m\mathbf{Z}$ we have $a + mb + m\mathbf{Z} = a + m\mathbf{Z}$. To show it is closed, we show its complement is open: the complement is the finite union of arithmetic progressions $r + m\mathbf{Z}$ for $0 \leq r \leq m - 1$ and $r \not\equiv a \bmod m$. Each $r + m\mathbf{Z}$ is open, so a union of $m - 1$ such progressions is open.

Remark 2.1. This topology on $\mathbf{Z}$ has a Wikipedia page about it under the label "evenly spaced integer topology," and this terminology is used in the famous book "Counterexamples in Topology" [3] (originally published in 1970), but the name for this topology used by mathematicians who don't consider it weird or exotic is the profinite topology. This type of topology had been introduced in the 1920s by Krull in his work on infinite Galois theory,

[1] For our purposes, the term "arithmetic progression" always means an infinite arithmetic progression going in both directions.

although the name "profinite" only came much later. Such a topology can be defined using the subgroups of finite index in any group, and a similar idea leads to a topology using cosets of powers of an ideal I in a commutative ring, called the I-adic topology on the ring.

Now we are ready to give Furstenberg's proof. Consider the union over prime numbers $\bigcup_p p\mathbf{Z}$. Since each integer other than ±1 has a prime factor,

$$\bigcup_p p\mathbf{Z} = \mathbf{Z} - \{\pm 1\}, \tag{2.1}$$

where the union runs over all prime numbers. In $\mathbf{Z}$ the subset $\{\pm 1\}$ is not open (since it is finite and nonempty), so its complement in $\mathbf{Z}$, namely $\bigcup_p p\mathbf{Z}$, is not closed. Each $p\mathbf{Z}$ is closed, and a union of finitely many closed subsets is closed, so the union $\bigcup_p p\mathbf{Z}$ in (2.1) can't be running over only finitely many primes p. The union runs over all primes, so the set of prime numbers is infinite. That completes Furstenberg's proof.

3. Relationship with Euclid's proof

Furstenberg's proof does not use anything about topology other than its most basic terminology. Let's unravel its use of open and closed subsets relative to the topology on $\mathbf{Z}$ to see what is going on.

Why is each $p\mathbf{Z}$ closed? Let's show the complement $\mathbf{Z} - p\mathbf{Z} = \{a \in \mathbf{Z} : p \nmid a\}$ is open: if $p \nmid a$ then no integer in the arithmetic progression $a + p\mathbf{Z}$ is divisible by p, so $a + p\mathbf{Z} \subset \mathbf{Z} - p\mathbf{Z}$.

For finitely many primes $p_1, \ldots, p_k$, why is the union $p_1\mathbf{Z} \cup \cdots \cup p_k\mathbf{Z}$ closed? Let's show the complement $\bigcap_{i=1}^k (\mathbf{Z} - p_i\mathbf{Z}) = \{a \in \mathbf{Z} : p_i \nmid a \text{ for } i = 1, \ldots, k\}$ is open. It is not empty since it contains the number 1. If $a \in \mathbf{Z}$ is not divisible by any of $p_1, \ldots, p_k$ then the integers in $a + p_1 \cdots p_k\mathbf{Z}$ are not divisible by any p_i (if some p_i divides an integer in this progression then it would divide a too), so $a + p_1 \cdots p_k\mathbf{Z} \subset \bigcap_{i=1}^k (\mathbf{Z} - p_i\mathbf{Z})$.

We now formulate Furstenberg's proof without mentioning a topology on $\mathbf{Z}$. Since the only integers not divisible by any prime are ±1,

$$\bigcap_p (\mathbf{Z} - p\mathbf{Z}) = \{\pm 1\},$$

where the intersection runs over all prime numbers. (This equation is the complement of (2.1).) The set $\{\pm 1\}$ contains no arithmetic progressions, so $\bigcap_p (\mathbf{Z} - p\mathbf{Z})$ contains none either. An intersection of finitely many $\mathbf{Z} - p\mathbf{Z}$ does contain an arithmetic progression, so $\bigcap_p (\mathbf{Z} - p\mathbf{Z})$ can't be running over only finitely many p. This intersection runs over all primes, so there are infinitely many primes.

The key idea in this proof is that for a finite set of primes $p_1, \ldots, p_k$, the intersection $\bigcap_{i=1}^k (\mathbf{Z} - p_i\mathbf{Z})$ contains arithmetic progressions while $\{\pm 1\}$ does not. More precisely, since 1 is in $\bigcap_{i=1}^k (\mathbf{Z} - p_i\mathbf{Z})$, the arithmetic progression $1 + p_1p_2 \cdots p_k\mathbf{Z}$ is too. This says *every integer of the form* $1 + p_1p_2 \ldots p_kb$ *for* $b \in \mathbf{Z}$ *is not divisible by any* p_i. That is the exact same idea as in Euclid's proof of the infinitude of the primes: given a finite list of primes $p_1, p_2, \ldots, p_k$, the number $1 + p_1p_2 \cdots p_k$ (or any $1 + p_1p_2 \cdots p_kb$) is not divisible by any p_i.

References

[1] H. Furstenberg, "On the Infinitude of Primes," Amer. Math. Monthly **62** (1955), 353.

[2] https://en.wikipedia.org/wiki/Furstenberg's_proof_of_the_infinitude_of_primes.

[3] L. A. Steen and J. A. Seebach, Jr., *Counterexamples in Topology*, Dover, 1995.