On Fürstenberg's topological proof of the infinitude of primes

Martin Klazar[1]

February 9, 2010

Fürstenberg's proof [5], via topological arguments, that the set of primes $P = \{2, 3, 5, 7, 11, \dots\}$ is infinite enjoys constant popularity, see, e.g., Baaz et al. [2], Mercer [6] and, to name only three textbooks, Aigner and Ziegler [1, p. 5], Everest and Ward [4, p. 40] and Pollack [7, p. 12]. Most of other proofs work with properties of individual integers but this one is a second order proof as it deals with properties of sets of integers. We want to explain it from the first principles, without topology. This was recently nicely done by Mercer [6] but we think it still worthwhile to point out explicitly a simple combinatorial property of sets of integers on which it rests, which we have not seen done in the literature.

Let $\mathbb{Z}$ be the integers and $\mathbb{N} = \{1, 2, \dots\}$. (Everything can be formulated in $\mathbb{N}$, as it is done in [2], but from tradition we will stay in $\mathbb{Z}$.) The main idea of Fürstenberg's proof is the set identity

$$\mathbb{Z}\backslash\{-1, 1\} = \bigcup_{p \in P} p\mathbb{Z},$$

which follows from the fact -1 and 1 are the only integers not divisible by any prime. We write S for this set of integers. What is the property that, for finite P, by one side of the identity S has but by the other has not? In the topological rendering of Fürstenberg's proof it is *closedness* in certain topology on $\mathbb{Z}$. This topology has arithmetic progressions $m + n\mathbb{Z}$, $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, as a base of open sets. Then each of these progressions is also closed because its complement can be expressed as a union of (even finitely many) arithmetic progressions. Thus if P is finite, by the right side is S closed. On the other hand, every nonempty open set in this topology is infinite as it contains an arithmetic progression. Thus every closed set, distinct from $\mathbb{Z}$, is coinfinite, complement of an infinite set. But then the left side shows that S is not closed, which is a contradiction.

How would you explain the proof to someone not knowledgeable of topology? It is actually quite simple—another property that S has and at the same time has not is *periodicity*. Clearly, $\mathbb{Z}\backslash\{-1, 1\}$ is not a periodic set. On the other hand, arithmetic progressions $p\mathbb{Z}$ are periodic and so is their finite union over P. Thus we have a contradiction. Let us see the details.

A set $X \subset \mathbb{Z}$ is *periodic* if for some $a \in \mathbb{N}$, called the *period* of X,

$$\forall x \in \mathbb{Z} : \; x \in X \iff x + a \in X.$$

Note the following properties of periodicity, all very easy to prove.

1. If X is periodic with period a, then any multiple na, $n \in \mathbb{N}$, is also a period of X.

[1]klazar@kam.mff.cuni.cz

2. X is periodic if and only if $\mathbb{Z}\backslash X$ is periodic.

3. Finite set X is periodic if and only if $X = \emptyset$.

4. Every arithmetic progression $X = m + n\mathbb{Z}$, $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, is periodic.

5. If X and Y are periodic then so is $X \cup Y$ (and $X \cap Y$).

We justify only the last property, crucial for the proof. Let X and Y be periodic with periods a and b, respectively. We set $c = ab$ and consider generic $x \in \mathbb{Z}$. If $x \in X$ then $x + c \in X$ by 1 as c is a multiple of a. Similarly if $x \in Y$ then $x + c \in Y$. If x is neither in X nor in Y, then $x + c$ is neither in X nor in Y by 1 because c is a multiple of both a and b. Therefore $X \cup Y$ (and $X \cap Y$) is periodic with period c.

Now $S = \mathbb{Z}\backslash\{-1, 1\}$ is not periodic by properties 2 and 3. On the other hand, for finite P is $S = \bigcup_{p \in P} p\mathbb{Z}$ periodic by properties 4 and 5. We have a contradiction.

Let us close with the remark that this combinatorial reformulation is quite in the spirit of fundamental work of H. Fürstenberg.

Post scriptum. A more thorough search of the Internet revealed that this combinatorial version of Fürstenberg's proof via periodicity is due already to Cass and Wildenberg [3]. Their beautiful proof definitely deserves to be much better known!

References

[1] M. Aigner and G. Ziegler, *Proofs from THE BOOK*, Springer, 2001.

[2] M. Baaz, S. Hetzl, A. Leitsch, C. Richter and H. Spohr, CERES: An analysis of Fürstenberg's proof of the infinity of primes, *Theoret. Comput. Sci.* **403** (2008) 160–175.

[3] D. Cass and G. Wildenberg, Math bite: A novel proof of the infinitude of primes, revisited, *Mathematics Magazine* **76** (2003) 203.

[4] G. Everest and T. Ward, *An Introduction to Number Theory*, Springer, 2005.

[5] H. Furstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955) 353.

[6] I. D. Mercer, On Furstenberg's proof of the infinitude of primes, *Amer. Math. Monthly* **116** (2009) 355–356.

[7] P. Pollack, *Not Always Burried Deep. A Second Course in Elementary Number Theory*, AMS, 2009.