# A Surprising Connection between Two Proofs of the Infinitude of Primes 

Nathan Carlson<br>California Lutheran University

CMC ${ }^{3}$ April 23, 2016

## Euclid and History

Euclid's Proof of the Infinitude of Primes
Furstenberg's Proof
Mercer's Variation
A Connection

## Euclid of Alexandria, 300BC



## Euclid...

- is considered the "Father of Geometry"


## Euclid...

- is considered the "Father of Geometry"
- wrote The Elements, one of the most influential works in the history of mathematics, serving as the main textbook for geometry from the time of its publication until the late 19th or early 20th century.


## Euclid...

- is considered the "Father of Geometry"
- wrote The Elements, one of the most influential works in the history of mathematics, serving as the main textbook for geometry from the time of its publication until the late 19th or early 20th century.
- deduced, in The Elements, the principles of what is now called Euclidean geometry from a small set of axioms.


## Euclid...

- is considered the "Father of Geometry"
- wrote The Elements, one of the most influential works in the history of mathematics, serving as the main textbook for geometry from the time of its publication until the late 19th or early 20th century.
- deduced, in The Elements, the principles of what is now called Euclidean geometry from a small set of axioms.
- other non-Euclidean geometries emerged in the late 19th century.

one of the oldest surviving fragments of The Elements, 100AD

Euclid and History
Euclid's Proof of the Infinitude of Primes
Furstenberg's Proof
Mercer's Variation
A Connection

## Euclid, depicted in Rafael's School of Athens (1510)



## The Infinitude of Primes

Let's recall:
Definition

Note the number 1 is neither a prime nor composite. It is generally referred to as a unit.

## The Infinitude of Primes

Let's recall:

## Definition

- A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.

Note the number 1 is neither a prime nor composite. It is generally referred to as a unit.

## The Infinitude of Primes

## Let's recall:

## Definition

- A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.
- A composite number is a natural number greater than 1 that is not prime.

Note the number 1 is neither a prime nor composite. It is generally referred to as a unit.

# In Book 9 of The Elements, Euclid established the following. 

## Main Theorem

There exists an infinite number of primes.

## Besides Euclid's original proof, several other proofs of this fundamental result have been given by <br> - Euler (18th century)

# Besides Euclid's original proof, several other proofs of this fundamental result have been given by <br> - Euler (18th century) <br> - Erdös (20th century) 

Besides Euclid's original proof, several other proofs of this fundamental result have been given by

- Euler (18th century)
- Erdös (20th century)
- Furstenberg (1955) (a topological proof)

Besides Euclid's original proof, several other proofs of this fundamental result have been given by

- Euler (18th century)
- Erdös (20th century)
- Furstenberg (1955) (a topological proof)
- Pinasco (2009)

Besides Euclid's original proof, several other proofs of this fundamental result have been given by

- Euler (18th century)
- Erdös (20th century)
- Furstenberg (1955) (a topological proof)
- Pinasco (2009)
- Whang (2010)

Besides Euclid's original proof, several other proofs of this fundamental result have been given by

- Euler (18th century)
- Erdös (20th century)
- Furstenberg (1955) (a topological proof)
- Pinasco (2009)
- Whang (2010)
- and more.


## Euclid's Proof (300BC)

First we recall the all-important ...

## Fundamental Theorem of Arithmetic

For all $n \in \mathbb{Z}$ such that $n>1, n$ can be represented uniquely as the product of primes.

For example, the set $\{\ldots,-11,-4,3,10,17,24, \ldots\}$ is an arithmetic progression, where $a=7$ and $m=3$.

## Euclid's Proof (300BC)

First we recall the all-important ...
Fundamental Theorem of Arithmetic
For all $n \in \mathbb{Z}$ such that $n>1, n$ can be represented uniquely as the product of primes.

## Definition

Let $a, m \in \mathbb{Z}$. An arithmetic sequence is a set of integers of the form

$$
a+m \mathbb{Z}=\{a+m n: n \in \mathbb{Z}\}
$$

For example, the set $\{\ldots,-11,-4,3,10,17,24, \ldots\}$ is an arithmetic progression, where $a=7$ and $m=3$.

## Lemma

For all integers $m$ not equal to -1 or 1 ,

$$
m \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(m \mathbb{Z})
$$

I.e., one more than a multiple of $m$ is not a multiple of $m$.

## Lemma

For all integers $m$ not equal to -1 or 1 ,

$$
m \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(m \mathbb{Z})
$$

I.e., one more than a multiple of $m$ is not a multiple of $m$.

## Proof.

Let $m k+1 \in m \mathbb{Z}+1$ for some $k \in \mathbb{Z}$. Suppose by way of contradiction that $m k+1$ is a multiple of $m$. Then there exists $n \in \mathbb{Z}$ such that $m k+1=m n$. Thus $1=m(n-k)$ and $m$ divides 1 . So $m$ must be either -1 or 1 , which is contradiction. We conclude $m \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(m \mathbb{Z})$.

## Proof of the Infinitude of Primes (Euclid).

## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.
- If $p \notin F$, then there is prime not on our list and we're done.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.
- If $p \notin F$, then there is prime not on our list and we're done.
- Otherwise, $p \in F$ and note $N \in p \mathbb{Z}+1$.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.
- If $p \notin F$, then there is prime not on our list and we're done.
- Otherwise, $p \in F$ and note $N \in p \mathbb{Z}+1$.
- As $p>1$, it follows by the Lemma that $N \in p \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(p \mathbb{Z})$.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.
- If $p \notin F$, then there is prime not on our list and we're done.
- Otherwise, $p \in F$ and note $N \in p \mathbb{Z}+1$.
- As $p>1$, it follows by the Lemma that $N \in p \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(p \mathbb{Z})$.
- This is contradiction since $p$ divides $N$. We conclude $N$ is a prime, and furthermore it cannot be on our list $F$.


## Proof of the Infinitude of Primes (Euclid).

- Let $F=\left\{p_{1}, \ldots, p_{n}\right\}$ be any finite list of primes. We show there is a prime not on our list $F$.
- Suppose that $N=p_{1} p_{2} \ldots p_{n}+1$ were not prime.
- As $N>1$, by the FTA there exists a prime $p$ that divides $N$.
- If $p \notin F$, then there is prime not on our list and we're done.
- Otherwise, $p \in F$ and note $N \in p \mathbb{Z}+1$.
- As $p>1$, it follows by the Lemma that $N \in p \mathbb{Z}+1 \subseteq \mathbb{Z} \backslash(p \mathbb{Z})$.
- This is contradiction since $p$ divides $N$. We conclude $N$ is a prime, and furthermore it cannot be on our list $F$.
- Since for any finite list $F$ of primes there is a prime not on our list, we conclude the set $P$ of primes is infinite.


## Hillel Furstenberg



- discovered a topological proof of the Infinitude of Primes in 1955, while an undergraduate at Yeshiva University
- discovered a topological proof of the Infinitude of Primes in 1955, while an undergraduate at Yeshiva University
- a curious and unusual proof, seemingly very different than any other proofs out there
- discovered a topological proof of the Infinitude of Primes in 1955, while an undergraduate at Yeshiva University
- a curious and unusual proof, seemingly very different than any other proofs out there
- published in the American Mathematical Monthly
- discovered a topological proof of the Infinitude of Primes in 1955, while an undergraduate at Yeshiva University
- a curious and unusual proof, seemingly very different than any other proofs out there
- published in the American Mathematical Monthly
- currently at Hebrew University of Jerusalem, works in differential geometry and ergodic theory

Euclid and History Euclid's Proof of the Infinitude of Primes Furstenberg's Proof
Mercer's Variation A Connection


## The Evenly-Spaced Integer Topology on $\mathbb{Z}$

## Definition

The evenly-spaced integer topology on $\mathbb{Z}$ consists of the following collection of open sets:

$$
\{U \subseteq \mathbb{Z}: a \mathbb{Z}+b \subseteq U \text { for some } a, b \in \mathbb{Z}\}
$$

In other words, a non-empty set of integers is open in this space if and only if it contains an arithmetic sequence.

This amazing thing about this topology is that it actually is a topology! To help see why, let's consider this question:

## Question

What can we say about the intersection of finitely many arithmetic sequences? That is, what are the possibilities for

$$
\bigcap_{i=1}^{n}\left(a_{i}+m_{i} \mathbb{Z}\right)
$$

where $a_{1}, \ldots, a_{n}$ and $m_{1}, \ldots, m_{n}$ are integers?

## We see that:

## Lemma

A finite intersection of arithmetic sequences is an arithmetic sequence (and thus infinite), or empty.

We see that:

## Lemma

A finite intersection of arithmetic sequences is an arithmetic sequence (and thus infinite), or empty.

- It follows from the previous Lemma that the finite intersection of open sets is open in the Evenly-Spaced Integer Topology.

We see that:

## Lemma

A finite intersection of arithmetic sequences is an arithmetic sequence (and thus infinite), or empty.

- It follows from the previous Lemma that the finite intersection of open sets is open in the Evenly-Spaced Integer Topology.
- Other conditions for a topology are also satisfied.

Two curious properties of this space:
(0) an arithmetic sequence is both open and closed (clopen) Why?

Two curious properties of this space:

- an arithmetic sequence is both open and closed (clopen) Why?
(2) a finite set is not open (unless it is empty) as it cannot contain an infinite arithmetic sequence.


## Proof (Furstenberg, 1955).

## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.


## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.
- By the Fundamental Theorem of Arithmetic,

$$
\bigcup_{p \text { prime }} p \mathbb{Z}=\mathbb{Z} \backslash\{-1,1\} .
$$

## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.
- By the Fundamental Theorem of Arithmetic,

$$
\bigcup_{p \text { prime }} p \mathbb{Z}=\mathbb{Z} \backslash\{-1,1\} .
$$

- For each prime $p$, the arithmetic sequence $p \mathbb{Z}$ is closed.


## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.
- By the Fundamental Theorem of Arithmetic,

$$
\bigcup_{p \text { prime }} p \mathbb{Z}=\mathbb{Z} \backslash\{-1,1\} .
$$

- For each prime $p$, the arithmetic sequence $p \mathbb{Z}$ is closed.
- As the finite union of closed sets is closed, the set on the left above is closed.


## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.
- By the Fundamental Theorem of Arithmetic,

$$
\bigcup_{p \text { prime }} p \mathbb{Z}=\mathbb{Z} \backslash\{-1,1\} .
$$

- For each prime $p$, the arithmetic sequence $p \mathbb{Z}$ is closed.
- As the finite union of closed sets is closed, the set on the left above is closed.
- Hence, the set on the right is closed, implying $\{-1,1\}$ is open.


## Proof (Furstenberg, 1955).

- Suppose by way of contradiction that the set of primes were finite.
- By the Fundamental Theorem of Arithmetic,

$$
\bigcup_{p \text { prime }} p \mathbb{Z}=\mathbb{Z} \backslash\{-1,1\} .
$$

- For each prime $p$, the arithmetic sequence $p \mathbb{Z}$ is closed.
- As the finite union of closed sets is closed, the set on the left above is closed.
- Hence, the set on the right is closed, implying $\{-1,1\}$ is open.
- This is a contradiction since finite sets cannot be open.


## Mercer's Variation

In 2009, Mercer "unpackaged" the topology in Furstenberg's proof to uncover the underlying number theory. We give Mercer's proof, also published in the Monthly.

## Lemma

If $m \geq 2$, then

$$
\mathbb{Z} \backslash(m \mathbb{Z})=(1+m \mathbb{Z}) \cup \ldots \cup((m-1)+m \mathbb{Z})
$$

I.e., $\mathbb{Z} \backslash(m \mathbb{Z})$ is a finite union of arithmetic sequences.

## Proof of the Infinitude of Primes (Mercer's Unpackaging).

## Proof of the Infinitude of Primes (Mercer's Unpackaging).

- Suppose that the set of primes were finite, and let $p_{1}, \ldots, p_{n}$ represent all the prime numbers.


## Proof of the Infinitude of Primes (Mercer's Unpackaging).

- Suppose that the set of primes were finite, and let $p_{1}, \ldots, p_{n}$ represent all the prime numbers.
- the FTA implies that every integer other than 1 and -1 are multiples of some prime. Put another way, the numbers 1 and -1 are the only integers that are not multiples of any prime.


## Proof of the Infinitude of Primes (Mercer's Unpackaging).

- Suppose that the set of primes were finite, and let $p_{1}, \ldots, p_{n}$ represent all the prime numbers.
- the FTA implies that every integer other than 1 and -1 are multiples of some prime. Put another way, the numbers 1 and -1 are the only integers that are not multiples of any prime.
- it follows that

$$
\{-1,1\}=\mathbb{Z} \backslash\left(p_{1} \mathbb{Z}\right) \cap \mathbb{Z} \backslash\left(p_{2} \mathbb{Z}\right) \cap \cdots \cap \mathbb{Z} \backslash\left(p_{n} \mathbb{Z}\right)
$$

## Proof of the Infinitude of Primes (Mercer's Unpackaging).

- Suppose that the set of primes were finite, and let $p_{1}, \ldots, p_{n}$ represent all the prime numbers.
- the FTA implies that every integer other than 1 and -1 are multiples of some prime. Put another way, the numbers 1 and -1 are the only integers that are not multiples of any prime.
- it follows that

$$
\{-1,1\}=\mathbb{Z} \backslash\left(p_{1} \mathbb{Z}\right) \cap \mathbb{Z} \backslash\left(p_{2} \mathbb{Z}\right) \cap \cdots \cap \mathbb{Z} \backslash\left(p_{n} \mathbb{Z}\right)
$$

- each $\mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)$ above is a finite union of arithmetic sequences, by the previous Lemma.

Proof of the Infinitude of Primes (Mercer's Unpackaging).

- Suppose that the set of primes were finite, and let $p_{1}, \ldots, p_{n}$ represent all the prime numbers.
- the FTA implies that every integer other than 1 and -1 are multiples of some prime. Put another way, the numbers 1 and -1 are the only integers that are not multiples of any prime.
- it follows that

$$
\{-1,1\}=\mathbb{Z} \backslash\left(p_{1} \mathbb{Z}\right) \cap \mathbb{Z} \backslash\left(p_{2} \mathbb{Z}\right) \cap \cdots \cap \mathbb{Z} \backslash\left(p_{n} \mathbb{Z}\right)
$$

- each $\mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)$ above is a finite union of arithmetic sequences, by the previous Lemma.
- so $\{-1,1\}$ is then a finite intersection of finite unions of arithmetic sequences.


## Proof, con't.

## Proof, con't.

- finite intersections distribute over finite unions


## Proof, con't.

- finite intersections distribute over finite unions
- $\{-1,1\}$ is then a finite union of finite intersections of arithmetic sequences.


## Proof, con't.

- finite intersections distribute over finite unions
- $\{-1,1\}$ is then a finite union of finite intersections of arithmetic sequences.
- By a previous lemma, finite intersections of arithmetic sequences are empty or infinite, and so then will unions of these intersections.


## Proof, con't.

- finite intersections distribute over finite unions
- $\{-1,1\}$ is then a finite union of finite intersections of arithmetic sequences.
- By a previous lemma, finite intersections of arithmetic sequences are empty or infinite, and so then will unions of these intersections.
- thus $\{-1,1\}$ is either empty or infinite which, on most days of the week, it is decidely not.


## Proof, con't.

- finite intersections distribute over finite unions
- $\{-1,1\}$ is then a finite union of finite intersections of arithmetic sequences.
- By a previous lemma, finite intersections of arithmetic sequences are empty or infinite, and so then will unions of these intersections.
- thus $\{-1,1\}$ is either empty or infinite which, on most days of the week, it is decidely not.
- this is a contradiction, showing that the primes are infinite.


## A Connection Between the Proofs

- Suppose the set of primes $P$ where finite. Let $P=\left\{p_{1}, \ldots, p_{n}\right\}$.


## A Connection Between the Proofs

- Suppose the set of primes $P$ where finite. Let $P=\left\{p_{1}, \ldots, p_{n}\right\}$.
- Let $A \subseteq \mathbb{Z}$ be all the integers that are not multiples of any prime. Then,

$$
A=\bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

## A Connection Between the Proofs

- Suppose the set of primes $P$ where finite. Let $P=\left\{p_{1}, \ldots, p_{n}\right\}$.
- Let $A \subseteq \mathbb{Z}$ be all the integers that are not multiples of any prime. Then,

$$
A=\bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

- The Fundamental Theorem of Arithmetic says that

$$
A=\{-1,1\} .
$$

## A Connection Between the Proofs

- Suppose the set of primes $P$ where finite. Let $P=\left\{p_{1}, \ldots, p_{n}\right\}$.
- Let $A \subseteq \mathbb{Z}$ be all the integers that are not multiples of any prime. Then,

$$
A=\bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

- The Fundamental Theorem of Arithmetic says that

$$
A=\{-1,1\} .
$$

- Observe that in Mercer's variation on Furstenberg's proof, the key idea is to show that $A$ is infinite, contradicting that $A=\{-1,1\}$. (Thus there must be an infinitude of primes).

A straightforward way to see that $A$ is infinite (if the set of primes $P=\left\{p_{1}, \ldots p_{n}\right\}$ were finite):

- Let $m \in \mathbb{Z}$.

A straightforward way to see that $A$ is infinite (if the set of primes $P=\left\{p_{1}, \ldots p_{n}\right\}$ were finite):

- Let $m \in \mathbb{Z}$.
- Notice that for any prime $p_{i}$, the product $m p_{1} p_{2} \cdots p_{n}$ is a multiple of $p_{i}$.

A straightforward way to see that $A$ is infinite (if the set of primes $P=\left\{p_{1}, \ldots p_{n}\right\}$ were finite):

- Let $m \in \mathbb{Z}$.
- Notice that for any prime $p_{i}$, the product $m p_{1} p_{2} \cdots p_{n}$ is a multiple of $p_{i}$.
- By a previous Lemma, it follows that

$$
m p_{1} p_{2} \cdots p_{n}+1 \in \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

A straightforward way to see that $A$ is infinite (if the set of primes $P=\left\{p_{1}, \ldots p_{n}\right\}$ were finite):

- Let $m \in \mathbb{Z}$.
- Notice that for any prime $p_{i}$, the product $m p_{1} p_{2} \cdots p_{n}$ is a multiple of $p_{i}$.
- By a previous Lemma, it follows that

$$
m p_{1} p_{2} \cdots p_{n}+1 \in \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

- So,

$$
m p_{1} p_{2} \cdots p_{n}+1 \in \bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=A
$$

A straightforward way to see that $A$ is infinite (if the set of primes $P=\left\{p_{1}, \ldots p_{n}\right\}$ were finite):

- Let $m \in \mathbb{Z}$.
- Notice that for any prime $p_{i}$, the product $m p_{1} p_{2} \cdots p_{n}$ is a multiple of $p_{i}$.
- By a previous Lemma, it follows that

$$
m p_{1} p_{2} \cdots p_{n}+1 \in \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)
$$

- So,

$$
m p_{1} p_{2} \cdots p_{n}+1 \in \bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=A
$$

- Since the above holds for any $m \in \mathbb{Z}$, we see that $A$ is infinite.

Now let's go back and look at Euclid's original proof. We see that

- A finite set of primes $\left\{p_{1}, \ldots, p_{n}\right\}$ and the number $N=p_{1} p_{2} \cdots p_{n}+1$ is considered.

Now let's go back and look at Euclid's original proof. We see that

- A finite set of primes $\left\{p_{1}, \ldots, p_{n}\right\}$ and the number $N=p_{1} p_{2} \cdots p_{n}+1$ is considered.
- In essence, it is shown in that proof that

$$
p_{1} p_{2} \cdots p_{n}+1 \in \bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=A .
$$

Now let's go back and look at Euclid's original proof. We see that

- A finite set of primes $\left\{p_{1}, \ldots, p_{n}\right\}$ and the number $N=p_{1} p_{2} \cdots p_{n}+1$ is considered.
- In essence, it is shown in that proof that

$$
p_{1} p_{2} \cdots p_{n}+1 \in \bigcap_{i=1}^{n} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=A .
$$

- But $p_{1} p_{2} \cdots p_{n}+1>1$ and $A=\{-1,1\}$. This is a contradiction.

In summary, we see that both proofs are very similar, in the following way:

- Suppose the set of primes $P=\left\{p_{1}, \ldots, p_{n}\right\}$ were finite.

In summary, we see that both proofs are very similar, in the following way:

- Suppose the set of primes $P=\left\{p_{1}, \ldots, p_{n}\right\}$ were finite.
- Then the Fundamental Theorem of Arithmetic guarantees that

$$
A=\bigcap_{i=1}^{m} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=\{-1,1\}
$$

In summary, we see that both proofs are very similar, in the following way:

- Suppose the set of primes $P=\left\{p_{1}, \ldots, p_{n}\right\}$ were finite.
- Then the Fundamental Theorem of Arithmetic guarantees that

$$
A=\bigcap_{i=1}^{m} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=\{-1,1\}
$$

- The Furstenberg/Mercer proof is the observation that if $P$ were finite then $A$ would be infinite.

In summary, we see that both proofs are very similar, in the following way:

- Suppose the set of primes $P=\left\{p_{1}, \ldots, p_{n}\right\}$ were finite.
- Then the Fundamental Theorem of Arithmetic guarantees that

$$
A=\bigcap_{i=1}^{m} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=\{-1,1\}
$$

- The Furstenberg/Mercer proof is the observation that if $P$ were finite then $A$ would be infinite.
- Euclid's proof is the observation that if $P$ were finite then $p_{1} p_{2} \cdots p_{n}+1 \in A$

In summary, we see that both proofs are very similar, in the following way:

- Suppose the set of primes $P=\left\{p_{1}, \ldots, p_{n}\right\}$ were finite.
- Then the Fundamental Theorem of Arithmetic guarantees that

$$
A=\bigcap_{i=1}^{m} \mathbb{Z} \backslash\left(p_{i} \mathbb{Z}\right)=\{-1,1\}
$$

- The Furstenberg/Mercer proof is the observation that if $P$ were finite then $A$ would be infinite.
- Euclid's proof is the observation that if $P$ were finite then $p_{1} p_{2} \cdots p_{n}+1 \in A$
- Both observations contradict that $A=\{-1,1\}$.

围 N. A. Carlson, A Connection between Furstenberg's and Euclid's proofs of the Infinitude of Primes, Amer. Math. Monthly 121 (2014), 444.

Thank you!

