Why are there so many prime numbers?

Doug Ravenel

University of Rochester

October 15, 2008

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Some theorems about primes that every mathematician should know

Theorem 1 (Euclid, 300 BC)

There are infinitely many prime numbers.

Euclid's proof is very elementary, and we will give it shortly.

In 1737 Euler found a completely different proof that requires calculus. His method is harder to use but more powerful. We will outline it later if time permits.

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Some theorems about primes that every mathematician should know

Theorem 1 (Euclid, 300 BC)

There are infinitely many prime numbers.

Euclid's proof is very elementary, and we will give it shortly.

In 1737 Euler found a completely different proof that requires calculus. His method is harder to use but more powerful. We will outline it later if time permits.

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Some theorems about primes that every mathematician should know

Theorem 1 (Euclid, 300 BC)

There are infinitely many prime numbers.

Euclid's proof is very elementary, and we will give it shortly.

In 1737 Euler found a completely different proof that requires calculus. His method is harder to use but more powerful. We will outline it later if time permits.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Dirichlet's theorem

Theorem 2 (Dirichlet, 1837, Primes in arithmetic progressions)

Let a and b be relatively prime positive integers. Then there are infinitely primes of the form $am + b$.

Example. For $a = 10$, b could be 1, 3, 7 or 9. The theorem says there are infinitely many primes of the form $10m + 1$, $10m + 3$, $10m + 7$ and $10m + 9$. For other values of b not prime to 10, there is at most one such prime.

Dirichlet's proof uses functions of a complex variable.

We will see how some cases of it can be proved with more elementary methods.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Dirichlet's theorem

Theorem 2 (Dirichlet, 1837, Primes in arithmetic progressions)

Let a and b be relatively prime positive integers. Then there are infinitely primes of the form $am + b$.

Example. For $a = 10$, b could be 1, 3, 7 or 9. The theorem says there are infinitely many primes of the form $10m + 1$, $10m + 3$, $10m + 7$ and $10m + 9$. For other values of b not prime to 10, there is at most one such prime.

Dirichlet's proof uses functions of a complex variable.

We will see how some cases of it can be proved with more elementary methods.

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Dirichlet's theorem

Theorem 2 (Dirichlet, 1837, Primes in arithmetic progressions)

Let a and b be relatively prime positive integers. Then there are infinitely primes of the form $am + b$.

Example. For $a = 10$, b could be 1, 3, 7 or 9. The theorem says there are infinitely many primes of the form $10m + 1$, $10m + 3$, $10m + 7$ and $10m + 9$. For other values of b not prime to 10, there is at most one such prime.

Dirichlet's proof uses functions of a complex variable.

We will see how some cases of it can be proved with more elementary methods.

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Dirichlet's theorem

Theorem 2 (Dirichlet, 1837, Primes in arithmetic progressions)

Let a and b be relatively prime positive integers. Then there are infinitely primes of the form $am + b$.

Example. For $a = 10$, b could be 1, 3, 7 or 9. The theorem says there are infinitely many primes of the form $10m + 1$, $10m + 3$, $10m + 7$ and $10m + 9$. For other values of b not prime to 10, there is at most one such prime.

Dirichlet's proof uses functions of a complex variable.

We will see how some cases of it can be proved with more elementary methods.

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

The prime number theorem

Theorem 3 (Hadamard and de la Valle Poussin, 1896, Assyptotic distribution of primes)

Let $\pi(x)$ denote the number of primes less than x. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln x} = 1.$$

In other words, the number of primes less than x is roughly $x/\ln x$.

A better approximation is to $\pi(x)$ is the logarithmic integral

$$li(x) = \int_0^x \frac{dt}{\ln(t)}.$$

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

The prime number theorem

Theorem 3 (Hadamard and de la Valle Poussin, 1896, Assyptotic distribution of primes)

Let $\pi(x)$ *denote the number of primes less than* x*. Then*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

In other words, the number of primes less than x is roughly $x/\ln x$.

A better approximation is to $\pi(x)$ is the logarithmic integral

$$li(x) = \int_0^x \frac{dt}{\ln(t)}.$$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m-1$
Primes of the form $4m+1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

The prime number theorem

Theorem 3 (Hadamard and de la Valle Poussin, 1896, Assymptotic distribution of primes)

Let $\pi(x)$ *denote the number of primes less than* x*. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

In other words, the number of primes less than x is roughly $x/\ln x$.

A better approximation is to $\pi(x)$ is the logarithmic integral

$$li(x) = \int_0^x \frac{dt}{\ln(t)}.$$

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

The omniscient being proof of Theorem 1

Here is God's proof that there are infinitely many primes:

- Look at the positive integers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- See which of them are primes

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- Notice that there are infinitely many of them.

QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

The omniscient being proof of Theorem 1

Here is God's proof that there are infinitely many primes:

- Look at the positive integers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- See which of them are primes

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- Notice that there are infinitely many of them.

QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m-1$
Primes of the form $4m+1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

The omniscient being proof of Theorem 1

Here is God's proof that there are infinitely many primes:

- Look at the positive integers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- See which of them are primes

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- Notice that there are infinitely many of them.

QED

The omniscient being proof of Theorem 1

Here is God's proof that there are infinitely many primes:

- Look at the positive integers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- See which of them are primes

$$1, \color{green}{2}, \color{green}{3}, 4, \color{green}{5}, 6, \color{green}{7}, 8, 9, 10, \color{green}{11}, \ldots$$

- Notice that there are infinitely many of them.

QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

The omniscient being proof of Theorem 1

Here is God's proof that there are infinitely many primes:

- Look at the positive integers

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- See which of them are primes

$$1, {\color{green}2}, {\color{green}3}, 4, {\color{green}5}, 6, {\color{green}7}, 8, 9, 10, {\color{green}11}, \ldots$$

- Notice that there are infinitely many of them.

QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euclid's proof

Without God's omniscience, we have to work harder.

Euclid's proof relies on the *Fundamental Theorem of Arithmetic* (FTA for short), which says that every positive integer can be written as a product of primes in a unique way.

For example,

$$2008 = 2^3 \cdot 251 \qquad (251 \text{ is a prime})$$

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof

Without God's omniscience, we have to work harder.

Euclid's proof relies on the *Fundamental Theorem of Arithmetic* (FTA for short), which says that every positive integer can be written as a product of primes in a unique way.

For example,

$$2008 = 2^3 \cdot 251 \qquad (251 \text{ is a prime})$$

Euclid's proof

Without God's omniscience, we have to work harder.

Euclid's proof relies on the *Fundamental Theorem of Arithmetic* (FTA for short), which says that every positive integer can be written as a product of primes in a unique way.

For example,

$$2008 = 2^3 \cdot 251 \qquad \text{(251 is a prime)}$$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euclid's proof that there are infinitely many primes

Here is Euclid's wonderfully elegant argument:

- Let $S = \{p_1, p_2, \ldots, p_n\}$ be a finite set of primes.
- Let $N = p_1 p_2 \ldots p_n$, the product of all the primes in S.
- The number N is divisible by every prime in S.
- The number $N + 1$ is *not* divisible by any prime in S.
- By the FTA, $N + 1$ is a product of one or more primes not in the set S.
- Therefore S is not the set of all the prime numbers.

This means there are infinitely many primes.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Primes of the form $4m-1$

We can use Euclid's method to show there are infinitely many prime of the form $4m-1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N-1$ is not divisible by any of the primes in S.
- Therefore $4N-1$ is the product of some primes not in S, all of which are odd and not all of which have the form $4m+1$.
- Therefore S is not the set of all primes of the form $4m-1$.

Primes of the form $4m - 1$

We can use Euclid's method to show there are infinitely many prime of the form $4m - 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N - 1$ is not divisible by any of the primes in S.
- Therefore $4N - 1$ is the product of some primes not in S, all of which are odd and not all of which have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m - 1$.

Primes of the form $4m - 1$

We can use Euclid's method to show there are infinitely many prime of the form $4m - 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N - 1$ is not divisible by any of the primes in S.
- Therefore $4N - 1$ is the product of some primes not in S, all of which are odd and not all of which have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m - 1$.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Primes of the form $4m - 1$

We can use Euclid's method to show there are infinitely many prime of the form $4m - 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N - 1$ is not divisible by any of the primes in S.
- Therefore $4N - 1$ is the product of some primes not in S, all of which are odd and not all of which have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m - 1$.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Primes of the form $4m - 1$

We can use Euclid's method to show there are infinitely many prime of the form $4m - 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N - 1$ is not divisible by any of the primes in S.
- Therefore $4N - 1$ is the product of some primes not in S, all of which are odd and not all of which have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m - 1$.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Primes of the form $4m + 1$

We can try a similar approach to primes of the form $4m + 1$.

- Let $S = \{p_1, \dots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N + 1$ is not divisible by any of the primes in S.
- Therefore $4N + 1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m - 1$, eg $21 = 3 \cdot 7$. OOPS.

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Primes of the form $4m + 1$

We can try a similar approach to primes of the form $4m + 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N + 1$ is not divisible by any of the primes in S.
- Therefore $4N + 1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m - 1$, eg $21 = 3 \cdot 7$. OOPS.

Primes of the form $4m + 1$

We can try a similar approach to primes of the form $4m + 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N + 1$ is not divisible by any of the primes in S.
- Therefore $4N + 1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m - 1$, eg $21 = 3 \cdot 7$. OOPS.

Primes of the form $4m + 1$

We can try a similar approach to primes of the form $4m + 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N + 1$ is not divisible by any of the primes in S.
- Therefore $4N + 1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m - 1$, eg $21 = 3 \cdot 7$. OOPS.

Primes of the form $4m + 1$

We can try a similar approach to primes of the form $4m + 1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N + 1$ is not divisible by any of the primes in S.
- Therefore $4N + 1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m - 1$, eg $21 = 3 \cdot 7$. OOPS.

Primes of the form $4m+1$

We can try a similar approach to primes of the form $4m+1$.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N+1$ is not divisible by any of the primes in S.
- Therefore $4N+1$ is the product of some primes not in S, all of which are odd.
- However it could be the product of an even number of primes of the form $4m-1$, eg $21 = 3 \cdot 7$. OOPS.

How to fix this problem

It turns out that the number $4N^2+1$ (instead of $4N+1$) has to be the product of primes of the form $4m+1$.

Here are some examples.

N	$4N^2+1$	N	$4N^2+1$
1	5	9	$325 = 5^2 \cdot 13$
2	17	10	401
3	37	11	$485 = 5 \cdot 97$
4	$65 = 5 \cdot 13$	12	577
5	101	13	677
6	$145 = 5 \cdot 29$	14	$785 = 5 \cdot 157$
7	197	15	$901 = 17 \cdot 53$
8	257	16	$1025 = 5^2 \cdot 41$

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

How to fix this problem

It turns out that the number $4N^2+1$ (instead of $4N+1$) has to be the product of primes of the form $4m+1$.

Here are some examples.

N	$4N^2+1$	N	$4N^2+1$
1	5	9	$325 = 5^2 \cdot 13$
2	17	10	401
3	37	11	$485 = 5 \cdot 97$
4	$65 = 5 \cdot 13$	12	577
5	101	13	677
6	$145 = 5 \cdot 29$	14	$785 = 5 \cdot 157$
7	197	15	$901 = 17 \cdot 53$
8	257	16	$1025 = 5^2 \cdot 41$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m-1$
Primes of the form $4m+1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

How to fix this problem (continued)

It turns out that the number $4N^2 + 1$ (instead of $4N + 1$) has to be the product of primes of the form $4m + 1$.

To prove this we need some help from Pierre de Fermat, who is best known for his “Last Theorem.”

Theorem (Fermat’s Little Theorem, 1640)

If p is a prime, then $x^p - x$ is divisible by p for any integer x.

Since $x^p - x = x(x^{p-1} - 1)$, if x is not divisible by p, then $x^{p-1} - 1$ is divisible by p. In other words, $x^{p-1} \equiv 1$ modulo p.

Why are there so many prime numbers?
Outline
Three big theorems about prime numbers
Euclid’s theorem
Dirichlet’s theorem
The prime number theorem
Two proofs of Theorem 1
God’s proof
Euclid’s proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet’s theorem
Euler’s proof of Theorem 1
The Riemann hypothesis

How to fix this problem (continued)

It turns out that the number $4N^2 + 1$ (instead of $4N + 1$) has to be the product of primes of the form $4m + 1$.

To prove this we need some help from Pierre de Fermat, who is best known for his "Last Theorem."

Theorem (Fermat's Little Theorem, 1640)

If p is a prime, then $x^p - x$ is divisible by p for any integer x.

Since $x^p - x = x(x^{p-1} - 1)$, if x is not divisible by p, then $x^{p-1} - 1$ is divisible by p. In other words, $x^{p-1} \equiv 1$ modulo p.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

How to fix this problem (continued)

It turns out that the number $4N^2 + 1$ (instead of $4N + 1$) has to be the product of primes of the form $4m + 1$.

To prove this we need some help from Pierre de Fermat, who is best known for his "Last Theorem."

Theorem (Fermat's Little Theorem, 1640)

If p is a prime, then $x^p - x$ is divisible by p for any integer x.

Since $x^p - x = x(x^{p-1} - 1)$, if x is not divisible by p, then $x^{p-1} - 1$ is divisible by p. In other words, $x^{p-1} \equiv 1$ modulo p.

How to fix this problem (continued)

It turns out that the number $4N^2 + 1$ (instead of $4N + 1$) has to be the product of primes of the form $4m + 1$.

To prove this we need some help from Pierre de Fermat, who is best known for his "Last Theorem."

Theorem (Fermat's Little Theorem, 1640)

If p is a prime, then $x^p - x$ is divisible by p for any integer x.

Since $x^p - x = x(x^{p-1} - 1)$, if x is not divisible by p, then $x^{p-1} - 1$ is divisible by p. In other words, $x^{p-1} \equiv 1$ modulo p.

How to fix this problem (continued)

It turns out that the number $4N^2 + 1$ (instead of $4N + 1$) has to be the product of primes of the form $4m + 1$.

To prove this we need some help from Pierre de Fermat, who is best known for his "Last Theorem."

Theorem (Fermat's Little Theorem, 1640)

If p is a prime, then $x^p - x$ is divisible by p for any integer x.

Since $x^p - x = x(x^{p-1} - 1)$, if x is not divisible by p, then $x^{p-1} - 1$ is divisible by p. In other words, $x^{p-1} \equiv 1$ modulo p.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ is a product of primes of the form $4m + 1$.

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ is a product of primes of the form $4m + 1$.

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Lemma

Any number of the form $4N^2+1$ is a product of primes of the form $4m+1$.

Proof: Let $x = 2N$, so our number is x^2+1. Suppose it is divisible by a prime of the form $p = 4m+3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2+1$ is not divisible by any prime of the form $4m+3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m-1$
Primes of the form $4m+1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ *is a product of primes of the form* $4m + 1$.

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ is a product of primes of the form $4m + 1$.

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ *is a product of primes of the form* $4m + 1$.

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Lemma

Any number of the form $4N^2 + 1$ *is a product of primes of the form* $4m + 1$*.*

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Lemma

Any number of the form $4N^2 + 1$ *is a product of primes of the form* $4m + 1$*.*

Proof: Let $x = 2N$, so our number is $x^2 + 1$. Suppose it is divisible by a prime of the form $p = 4m + 3$. This means $x^2 \equiv -1$ modulo p.

Then $x^{4m} = (x^2)^{2m} \equiv (-1)^{2m} = 1$.

Fermat's Little Theorem tell us that $x^{p-1} = x^{4m+2} \equiv 1$, but $x^{4m+2} = x^{4m} \cdot x^2 \equiv 1 \cdot -1 = -1$, so we have a contradiction.

Hence $4N^2 + 1$ is not divisible by any prime of the form $4m + 3$. QED

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Primes of the form $4m + 1$ again

Here is our second attempt to use Euclid's method, this time with some help from Fermat.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N^2 + 1$ is not divisible by any of the primes in S.
- Therefore $4N^2 + 1$ is the product of some primes not in S, all of which must have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m + 1$.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Primes of the form $4m + 1$ again

Here is our second attempt to use Euclid's method, this time with some help from Fermat.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N^2 + 1$ is not divisible by any of the primes in S.
- Therefore $4N^2 + 1$ is the product of some primes not in S, all of which must have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m + 1$.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Primes of the form $4m + 1$ again

Here is our second attempt to use Euclid's method, this time with some help from Fermat.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N^2 + 1$ is not divisible by any of the primes in S.
- Therefore $4N^2 + 1$ is the product of some primes not in S, all of which must have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m + 1$.

Primes of the form $4m + 1$ again

Here is our second attempt to use Euclid's method, this time with some help from Fermat.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N^2 + 1$ is not divisible by any of the primes in S.
- Therefore $4N^2 + 1$ is the product of some primes not in S, all of which must have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m + 1$.

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Primes of the form $4m + 1$ again

Here is our second attempt to use Euclid's method, this time with some help from Fermat.

- Let $S = \{p_1, \ldots, p_n\}$ be a set of such primes, and let N be the product of all of them.
- The number $4N^2 + 1$ is not divisible by any of the primes in S.
- Therefore $4N^2 + 1$ is the product of some primes not in S, all of which must have the form $4m + 1$.
- Therefore S is not the set of all primes of the form $4m + 1$.

Some other cases of Dirichlet's theorem

Similar methods (involving algebra but no analysis) can be used to prove some but not all cases of Dirichlet's theorem. For example,

- We can show there are infinitely many primes of the forms $3m+1$ and $3m-1$.
- We can show there are infinitely many primes of the forms $5m+1$ and $5m-1$.
- We can show there are infinitely many primes of the forms $5m+2$ or $5m+3$, *but not that there are infinitely many of either type alone.*

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Some other cases of Dirichlet's theorem

Similar methods (involving algebra but no analysis) can be used to prove some but not all cases of Dirichlet's theorem. For example,

- We can show there are infinitely many primes of the forms $3m+1$ and $3m-1$.
- We can show there are infinitely many primes of the forms $5m+1$ and $5m-1$.
- We can show there are infinitely many primes of the forms $5m+2$ or $5m+3$, *but not that there are infinitely many of either type alone.*

Some other cases of Dirichlet's theorem

Similar methods (involving algebra but no analysis) can be used to prove some but not all cases of Dirichlet's theorem. For example,

- We can show there are infinitely many primes of the forms $3m + 1$ and $3m - 1$.
- We can show there are infinitely many primes of the forms $5m + 1$ and $5m - 1$.
- We can show there are infinitely many primes of the forms $5m + 2$ or $5m + 3$, *but not that there are infinitely many of either type alone.*

Some other cases of Dirichlet's theorem

Similar methods (involving algebra but no analysis) can be used to prove some but not all cases of Dirichlet's theorem. For example,

- We can show there are infinitely many primes of the forms $3m + 1$ and $3m - 1$.
- We can show there are infinitely many primes of the forms $5m + 1$ and $5m - 1$.
- We can show there are infinitely many primes of the forms $5m + 2$ or $5m + 3$, *but not that there are infinitely many of either type alone.*

Some other cases of Dirichlet's theorem

Similar methods (involving algebra but no analysis) can be used to prove some but not all cases of Dirichlet's theorem. For example,

- We can show there are infinitely many primes of the forms $3m + 1$ and $3m - 1$.
- We can show there are infinitely many primes of the forms $5m + 1$ and $5m - 1$.
- We can show there are infinitely many primes of the forms $5m + 2$ or $5m + 3$, *but not that there are infinitely many of either type alone.*

Euler's proof that there are infinitely many primes

Euler considered the infinite series

$$\sum_{n\geq 1} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

From calculus we know that it converges for $s > 1$ (by the integral test) and diverges for $s = 1$ (by the comparison test), when it is the harmonic series.

Using FTA, Euler rewrote the series as a product

$$\begin{aligned} \sum_{n\geq 1} \frac{1}{n^s} &= \prod_{p \text{ prime}} \left(\sum_{k\geq 0} \frac{1}{p^{ks}} \right) \\ &= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right)\dots \end{aligned}$$

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euler's proof that there are infinitely many primes

Euler considered the infinite series

$$\sum_{n\geq 1} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

From calculus we know that it converges for $s > 1$ (by the integral test) and diverges for $s = 1$ (by the comparison test), when it is the harmonic series.

Using FTA, Euler rewrote the series as a product

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(\sum_{k\geq 0} \frac{1}{p^{ks}} \right)$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right)\dots$$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euler's proof that there are infinitely many primes

Euler considered the infinite series

$$\sum_{n\geq 1} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

From calculus we know that it converges for $s > 1$ (by the integral test) and diverges for $s = 1$ (by the comparison test), when it is the harmonic series.

Using FTA, Euler rewrote the series as a product

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(\sum_{k\geq 0} \frac{1}{p^{ks}} \right)$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right)\dots$$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euler's proof that there are infinitely many primes

Euler considered the infinite series

$$\sum_{n\geq 1} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

From calculus we know that it converges for $s > 1$ (by the integral test) and diverges for $s = 1$ (by the comparison test), when it is the harmonic series.
Using FTA, Euler rewrote the series as a product

$$\begin{aligned} \sum_{n\geq 1} \frac{1}{n^s} &= \prod_{p \text{ prime}} \left(\sum_{k\geq 0} \frac{1}{p^{ks}} \right) \\ &= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right)\dots \end{aligned}$$

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

Euler's proof (continued)

Each factor in this product is a geometric series. The pth factor converges to $1/(1-p^{-s})$, whenever $s > 0$. Hence

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

If there were only finitely many primes, this would give a finite answer for $s = 1$, contradicting the divergence of the harmonic series.

Dirichlet used some clever variations of this method to prove his theorem 100 years later.

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euler's proof (continued)

Each factor in this product is a geometric series. The *p*th factor converges to $1/(1-p^{-s})$, whenever $s > 0$. Hence

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

If there were only finitely many primes, this would give a finite answer for $s = 1$, contradicting the divergence of the harmonic series.

Dirichlet used some clever variations of this method to prove his theorem 100 years later.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euler's proof (continued)

Each factor in this product is a geometric series. The pth factor converges to $1/(1 - p^{-s})$, whenever $s > 0$. Hence

$$\sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

If there were only finitely many primes, this would give a finite answer for $s = 1$, contradicting the divergence of the harmonic series.

Dirichlet used some clever variations of this method to prove his theorem 100 years later.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Euler's proof (continued)

Each factor in this product is a geometric series. The pth factor converges to $1/(1-p^{-s})$, whenever $s > 0$. Hence

$$\sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

If there were only finitely many primes, this would give a finite answer for $s = 1$, contradicting the divergence of the harmonic series.

Dirichlet used some clever variations of this method to prove his theorem 100 years later.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Epilogue: The Riemann zeta function.

In his famous 1859 paper *On the Number of Primes Less Than a Given Magnitude*, Riemmann studied Euler's series

$$\sum_{n\geq 0} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

as a function of a complex variable s, which he called $\zeta(s)$.

He showed that the series converges whenever s has real part greater than 1, and that it can be extended as a complex analytic function to all values of s other than 1, where the function has a pole.

He showed that the behavior of this function is intimately connected with the distribution of prime numbers.
To learn more about this connection, ask Steve Gonek to give a talk.

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Epilogue: The Riemann zeta function.

In his famous 1859 paper *On the Number of Primes Less Than a Given Magnitude*, Riemann studied Euler's series

$$\sum_{n\geq 0} \frac{1}{n^s} = \prod_{p\,\text{prime}} \frac{1}{1-p^{-s}}$$

as a function of a complex variable s, which he called $\zeta(s)$.

He showed that the series converges whenever s has real part greater than 1, and that it can be extended as a complex analytic function to all values of s other than 1, where the function has a pole.

He showed that the behavior of this function is intimately connected with the distribution of prime numbers.
To learn more about this connection, ask Steve Gonek to give a talk.

Epilogue: The Riemann zeta function.

In his famous 1859 paper *On the Number of Primes Less Than a Given Magnitude*, Riemann studied Euler's series

$$\sum_{n\geq 0} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

as a function of a complex variable s, which he called $\zeta(s)$.

He showed that the series converges whenever s has real part greater than 1, and that it can be extended as a complex analytic function to all values of s other than 1, where the function has a pole.

He showed that the behavior of this function is intimately connected with the distribution of prime numbers.
To learn more about this connection, ask Steve Gonek to give a talk.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

Epilogue: The Riemann zeta function.

In his famous 1859 paper *On the Number of Primes Less Than a Given Magnitude*, Riemann studied Euler's series

$$\sum_{n\geq 0} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

as a function of a complex variable s, which he called $\zeta(s)$.

He showed that the series converges whenever s has real part greater than 1, and that it can be extended as a complex analytic function to all values of s other than 1, where the function has a pole.

He showed that the behavior of this function is intimately connected with the distribution of prime numbers.
To learn more about this connection, ask Steve Gonek to give a talk.

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem

Two proofs of Theorem 1
God's proof
Euclid's proof

Primes of the form $4m-1$

Primes of the form $4m+1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$.

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$.

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers
- Euclid's theorem
- Dirichlet's theorem
- The prime number theorem

Two proofs of Theorem 1
- God's proof
- Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$.

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m-1$
Primes of the form $4m+1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$*.*

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$.

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Outline
Three big theorems about prime numbers
Euclid's theorem
Dirichlet's theorem
The prime number theorem
Two proofs of Theorem 1
God's proof
Euclid's proof
Primes of the form $4m - 1$
Primes of the form $4m + 1$
Other cases of Dirichlet's theorem
Euler's proof of Theorem 1
The Riemann hypothesis

When does $\zeta(s)$ vanish?

Riemann showed that $\zeta(s) = 0$ for $s = -2$, $s = -4$, $s = -6$ and so on. These are called the *trivial zeros*.

The *Riemann hypothesis* is concerned with the non-trivial zeros, and states that:

> *The real part of any non-trivial zero of the Riemann zeta function is* $1/2$.

This is the most famous unsolved problem in mathematics.

A million dollar prize has been offered for its solution.

Go home and watch the debate!

Why are there so many prime numbers?

Outline

Three big theorems about prime numbers

Euclid's theorem

Dirichlet's theorem

The prime number theorem

Two proofs of Theorem 1

God's proof

Euclid's proof

Primes of the form $4m - 1$

Primes of the form $4m + 1$

Other cases of Dirichlet's theorem

Euler's proof of Theorem 1

The Riemann hypothesis