Prime Numbers

Pf. Euclid of Alexandria euclid@alexandria.edu

Alexandria University

March 11, 2022

Table of contents

Table of contents

Table of contents

Table of contents

Division

Definition

An integer number $d \in \mathbb{Z}$ divides another integer number $D \in \mathbb{Z}$ if there exists $k \in \mathbb{Z}$ such that $D = dk$.

Division

Definition

An integer number $d \in \mathbb{Z}$ divides another integer number $D \in \mathbb{Z}$ if there exists $k \in \mathbb{Z}$ such that $D = dk$.

In this case we write $d|D$. We also refer to d as a divisor of D.

Prime numbers

Definition

A number $p \in \mathbb{Z}$ is called prime if $p \neq \pm 1$ and $\{\pm 1, \pm p\}$ are its only divisors.

Interesting Questions

- How many prime numbers are there?

Interesting Questions

- How many prime numbers are there?
- Do they have interesting properties?

Interesting Questions

- How many prime numbers are there?
- Do they have interesting properties?
- How easy are they to detect?

Interesting Questions

- How many prime numbers are there?
- Do they have interesting properties?
- How easy are they to detect?
- Are they constructible?

Interesting Questions

- How many prime numbers are there?
- Do they have interesting properties?
- How easy are they to detect?
- Are they constructible?
- Can you make money out of them?

Pascal Triangle

Theorem

If p is a prime number, then $\binom{p}{n}$ is a multiple of p.

Pascal Triangle

Theorem

If p is a prime number, then $\binom{p}{n}$ is a multiple of p.

Proof.

Pascal Triangle

Theorem

If p is a prime number, then $\binom{p}{n}$ is a multiple of p.

Proof.

$$\binom{p}{n}$$

Pascal Triangle

Theorem

If p is a prime number, then $\binom{p}{n}$ is a multiple of p.

Proof.

$$\binom{p}{n} = \frac{p(p-1)\dots(p-n+1)}{n(n-1)\dots 2}.$$

Pascal Triangle

Theorem

If p is a prime number, then $\binom{p}{n}$ *is a multiple of p.*

Proof.

$$\binom{p}{n} = \frac{p(p-1)\dots(p-n+1)}{n(n-1)\dots 2}.$$

The result follows since p is prime and hence not divisible by any factor in the denominator. □

The Euler Zeta Function

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Remark

$$\theta(s) \quad = \quad 1 \quad + \quad \tfrac{1}{2^s} \quad + \quad \tfrac{1}{3^s} \quad + \quad \tfrac{1}{4^s} \quad + \quad \tfrac{1}{5^s} \quad + \dots$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Remark

$$\begin{aligned} \theta(s) &= 1 + \tfrac{1}{2^s} + \tfrac{1}{3^s} + \tfrac{1}{4^s} + \tfrac{1}{5^s} + \dots \\ \tfrac{1}{2^s}\theta(s) &= \tfrac{1}{2^s} + \tfrac{1}{4^s} + \dots \end{aligned}$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Remark

$$\begin{aligned}
\theta(s) &= 1 + \tfrac{1}{2^s} + \tfrac{1}{3^s} + \tfrac{1}{4^s} + \tfrac{1}{5^s} + \dots \\
\tfrac{1}{2^s}\theta(s) &= \tfrac{1}{2^s} + \tfrac{1}{4^s} + \dots
\end{aligned}$$

$$\left(1 - \frac{1}{2^s}\right)\theta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \dots$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Remark

$$\begin{aligned} \theta(s) &= 1 + \tfrac{1}{2^s} + \tfrac{1}{3^s} + \tfrac{1}{4^s} + \tfrac{1}{5^s} + \dots \\ \tfrac{1}{2^s}\theta(s) &= \tfrac{1}{2^s} + \tfrac{1}{4^s} + \dots \end{aligned}$$

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\theta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \dots$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Remark

$$\begin{aligned}
\theta(s) &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots \\
\frac{1}{2^s}\theta(s) &= \frac{1}{2^s} + \frac{1}{4^s} + \dots
\end{aligned}$$

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right) \theta(s) = 1$$

The Euler Zeta Function

Definition

The Euler Zeta Function is defined as follows

$$\theta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Euler Sieve Property

$$\theta(s) = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right)$$

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number . . .

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number . . .

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number ...

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number … not in the first p numbers!!

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number . . . not in the first p numbers!!

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number ... not in the first p numbers!!!

□

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number ... not in the first p numbers!!! □

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem (_, 300 BC)

There are infinitely many prime numbers.

Proof.

1. Suppose there were finitely many prime numbers.
2. Consider p the largest prime number.
3. Let $q = p!$ be the product of the first p numbers.
4. Then $q + 1$ is not divisible by any of them.
5. But $q + 1$ is greater than p, thus divisible by some prime number . . . not in the first p numbers!!! □

Prime Number Theorem

Let $\pi(n) := \#\{\text{prime numbers smaller than } n\}$.

Prime Number Theorem

Let $\pi(n) := \#\{\text{prime numbers smaller than } n\}$.
For example $\pi(10) = 4$, $\pi(100) = 25, \ldots$

Prime Number Theorem

Let $\pi(n) := \#\{\text{prime numbers smaller than } n\}$.
For example $\pi(10) = 4$, $\pi(100) = 25, \ldots$

Theorem (Prime Number Theorem)

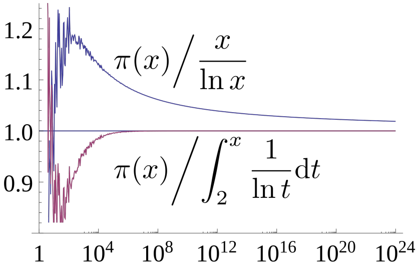
$$\pi(n) \sim \frac{n}{\log(n)}$$

Prime Number Theorem

Let $\pi(n) := \#\{\text{prime numbers smaller than } n\}$.
For example $\pi(10) = 4$, $\pi(100) = 25, \ldots$

Theorem (Prime Number Theorem)

$$\pi(n) \sim \frac{n}{\log(n)}$$



Sieve of Eratosthenes, 200 BC

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieve of Eratosthenes, 200 BC

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

$$11^2 = 121 > 100$$

Sieve of Eratosthenes, 200 BC

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

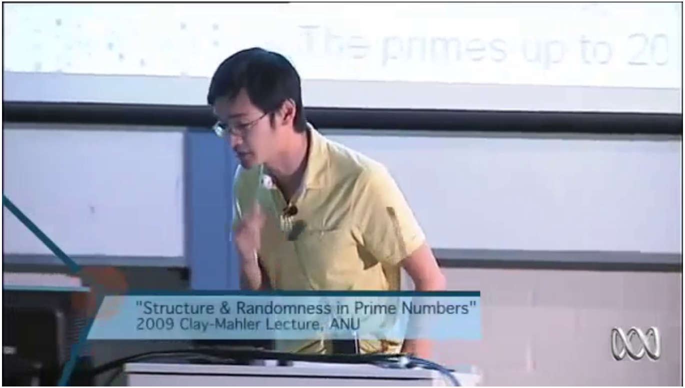
$$11^2 = 121 > 100$$

Goldbach Conjecture

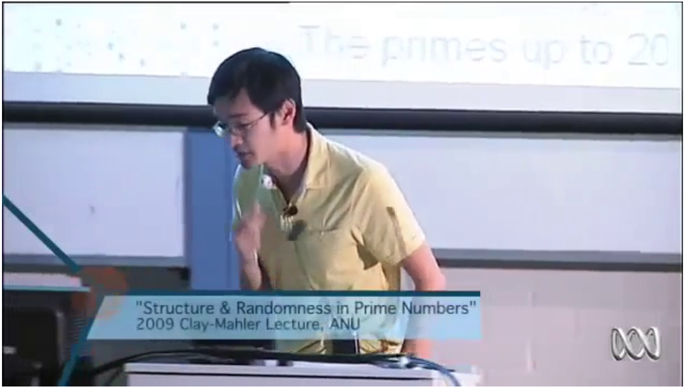
Goldbach, 1742

Every even integer greater than 2 can be expressed as the sum of two primes.

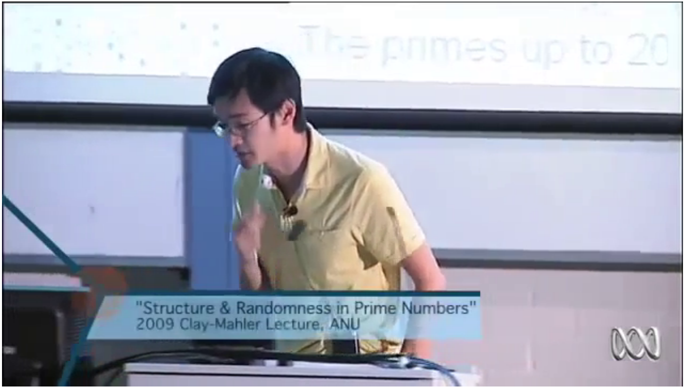
Local video file



External player



External player (href)



https://www.youtube.com/watch?v=lqKSXk5Xwg8

remote (YouTube player)

https://www.youtube.com/watch?v=1qKSXk5Xwg8