# Lecture 3:
# Chebyshev's prime number theorem

Karl Dilcher

Dalhousie University, Halifax, Canada

December 15, 2018

## 1. Introduction

We begin with a basic definition.

**Definition 1**

An integer $p > 1$ is called a *prime number*, or simply a *prime*, if it has only 1 and itself as divisors.

## 1. Introduction

We begin with a basic definition.

**Definition 1**

An integer $p > 1$ is called a *prime number*, or simply a *prime*, if it has only 1 and itself as divisors.
An integer that is not a prime number is called *composite*.

## 1. Introduction

We begin with a basic definition.

**Definition 1**

An integer $p > 1$ is called a *prime number*, or simply a *prime*, if it has only 1 and itself as divisors.
An integer that is not a prime number is called *composite*.

Obvious question: How many primes are there?

## 1. Introduction

We begin with a basic definition.

**Definition 1**

An integer $p > 1$ is called a *prime number*, or simply a *prime*, if it has only 1 and itself as divisors.
An integer that is not a prime number is called *composite*.

Obvious question: How many primes are there?

**Theorem 2 (Euclid)**

*There are infinitely many primes.*

**Proof:** Suppose there were only finitely mny primes, namely $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$.

**Proof:** Suppose there were only finitely mny primes, namely $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$.

Now form the number

$$n = p_1 p_2 \cdots p_r + 1.$$

**Proof:** Suppose there were only finitely mny primes, namely $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$.

Now form the number

$$n = p_1 p_2 \cdots p_r + 1.$$

$n$ is not divisible by
$p_1$: remainder 1 upon division;
$p_2$: remainder 1 upon division;
. . .
$p_r$: remainder 1 upon division.

**Proof:** Suppose there were only finitely mny primes, namely $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$.

Now form the number

$$n = p_1 p_2 \cdots p_r + 1.$$

$n$ is not divisible by
$p_1$: remainder 1 upon division;
$p_2$: remainder 1 upon division;
...
$p_r$: remainder 1 upon division.

Hence any prime divisor of $n$ must be distinct from the $p_1, p_2, \ldots, p_r$, but this is a contradiction.

**Remark:** Further to Euclid's theorem, the following is noteworthy.

**Remark:** Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof: There are infinitely many primes of the form $4k + 1$, or $4k - 1$, or $6k - 1$.

**Remark:** Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof: There are infinitely many primes of the form $4k + 1$, or $4k - 1$, or $6k - 1$.

(b) More generally, what about $p = ak + b$, where $(a, b) = 1$?

**Remark:** Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof: There are infinitely many primes of the form $4k+1$, or $4k-1$, or $6k-1$.

(b) More generally, what about $p = ak+b$, where $(a,b)=1$?

There are infinitely many primes in each class.

**Remark:** Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof: There are infinitely many primes of the form $4k+1$, or $4k-1$, or $6k-1$.

(b) More generally, what about $p = ak + b$, where $(a, b) = 1$?

There are infinitely many primes in each class.
First proved by P. G. Lejeune-Dirichlet (1805–1859) in 1837; this marked the beginning of analytic number theory.

**Remark:** Further to Euclid's theorem, the following is noteworthy.

(a) Variants of Euclid's proof: There are infinitely many primes of the form $4k+1$, or $4k-1$, or $6k-1$.

(b) More generally, what about $p = ak + b$, where $(a, b) = 1$?

There are infinitely many primes in each class.
First proved by P. G. Lejeune-Dirichlet (1805–1859) in 1837; this marked the beginning of analytic number theory.

(c) The prime numbers are both very regularly and very irregularly distributed.

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes:

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes: Consider the integers

$$k! + 2, k! + 3, \ldots, k! + k - 1, k! + k;$$

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes: Consider the integers

$$k! + 2, k! + 3, \dots, k! + k - 1, k! + k;$$

all these $k - 1$ consecutive integers are composite because clearly

$$j \mid k! + j \quad \text{for} \quad j = 2, 3, \dots, k.$$

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes: Consider the integers

$$k! + 2, k! + 3, \ldots, k! + k - 1, k! + k;$$

all these $k - 1$ consecutive integers are composite because clearly

$$j \mid k! + j \quad \text{for} \quad j = 2, 3, \ldots, k.$$

Second, there are the **twin primes**, namely pairs $p, p + 2$ of primes, such as

$$3, 5 \quad 5, 7 \quad 11, 13 \quad 17, 19 \quad \ldots$$

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes: Consider the integers

$$k! + 2, k! + 3, \dots, k! + k - 1, k! + k;$$

all these $k - 1$ consecutive integers are composite because clearly

$$j \mid k! + j \quad \text{for} \quad j = 2, 3, \dots, k.$$

Second, there are the **twin primes**, namely pairs $p, p + 2$ of primes, such as

$$3, 5 \quad 5, 7 \quad 11, 13 \quad 17, 19 \quad \dots$$

Are there infinitely many such pairs?

(c) The prime numbers are both very regularly and very irregularly distributed.

(i) “irregularity": two extreme situations.

First, there are “gaps" of arbitrary length between primes: Consider the integers

$$k!+2, k!+3, \ldots, k!+k-1, k!+k;$$

all these $k-1$ consecutive integers are composite because clearly

$$j \mid k!+j \quad \text{for} \quad j=2,3,\ldots,k.$$

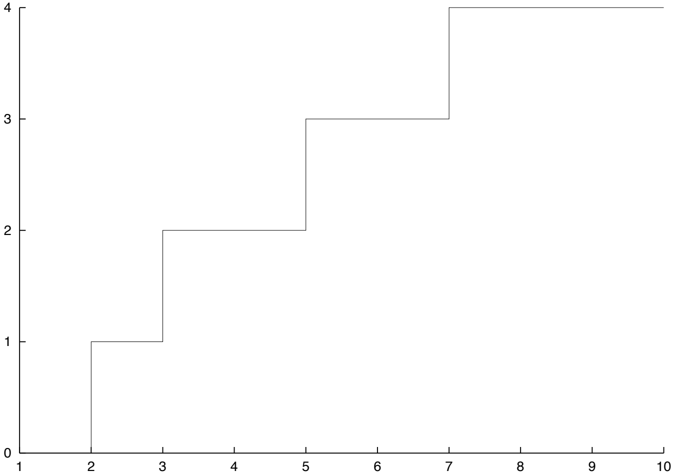
Second, there are the **twin primes**, namely pairs $p, p+2$ of primes, such as

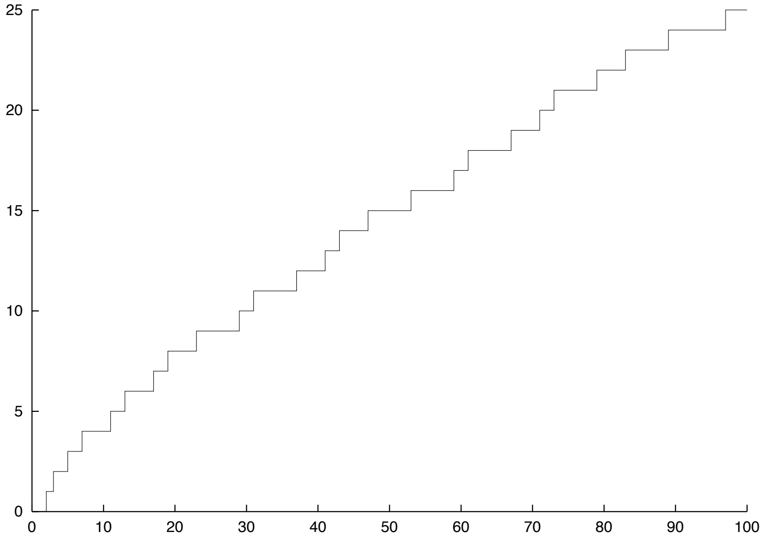
$$3,5 \quad 5,7 \quad 11,13 \quad 17,19 \quad \ldots$$

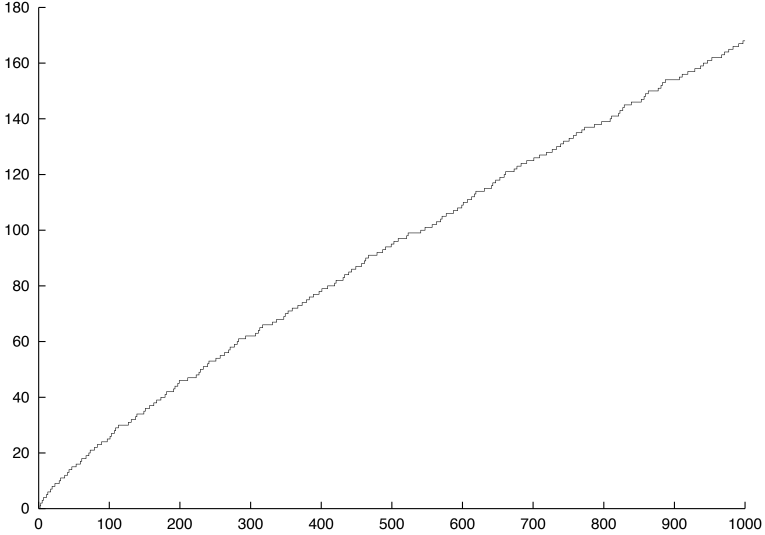
Are there infinitely many such pairs?
Not known: The **twin-prime conjecture**, one of the most famous unsolved problems in number theory.

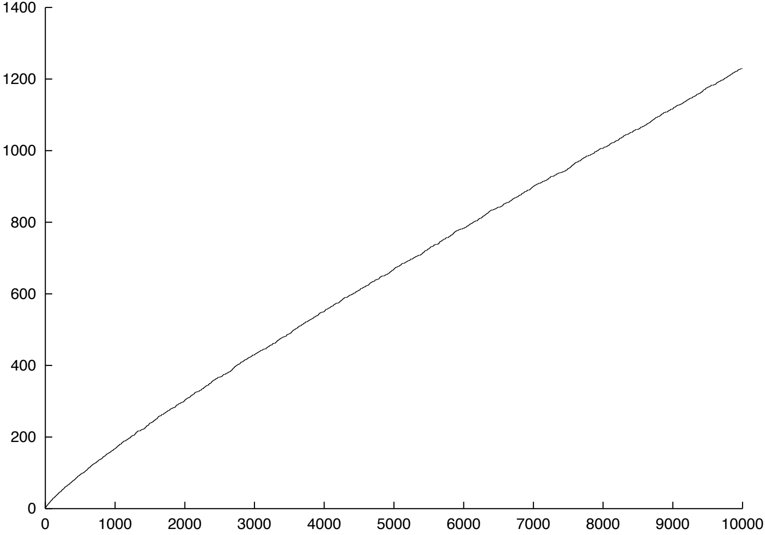
(ii) “Regularity": Let’s look at the “Prime counting function" $\pi(x)$:

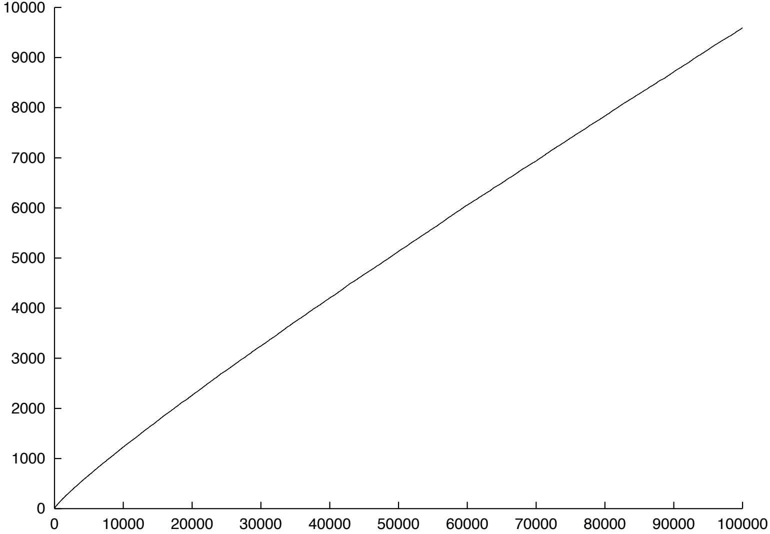
(ii) “Regularity": Let’s look at the “Prime counting function" $\pi(x)$:

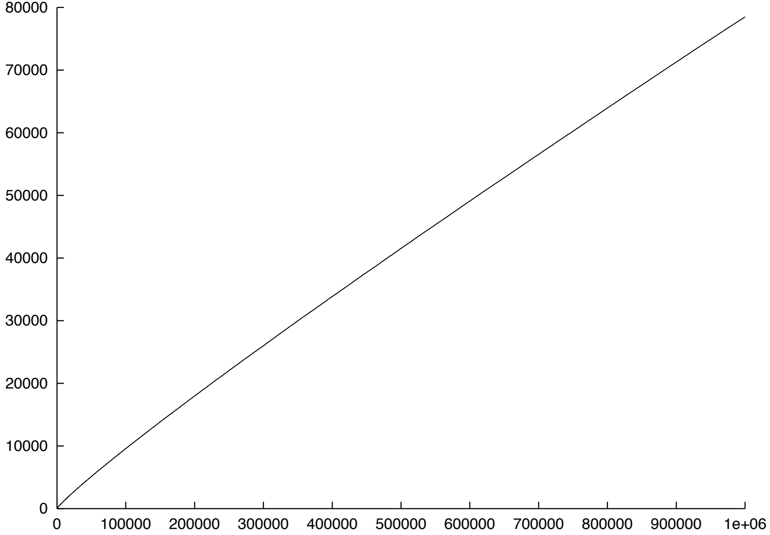



0
5
10
15
20
25
0
10
20
30
40
50
60
70
80
90
100


180
160
140
120
100
80
60
40
20
0
0
100
200
300
400
500
600
700
800
900
1000


1400
1200
1000
800
600
400
200
0
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000


10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
0
10000
20000
30000
40000
50000
60000
70000
80000
90000
100000


80000
70000
60000
50000
40000
30000
20000
10000
0
0
100000
200000
300000
400000
500000
600000
700000
800000
900000
1e+06

What is this function?

What is this function?
The *prime number theorem* shows that the primes are very regularly behaved “in the large".

What is this function?

The *prime number theorem* shows that the primes are very regularly behaved “in the large".

More exactly, we define the function

$$\pi(x) = \sum_{p \le x} 1 = \#\{p \le x \mid p \text{ prime}\}.$$

What is this function?
The *prime number theorem* shows that the primes are very regularly behaved “in the large".

More exactly, we define the function

$$\pi(x) = \sum_{p \le x} 1 = \#\{p \le x \mid p \text{ prime}\}.$$

It was proved by Jacques Hadamard (1865–1963) and (independently) Charles de la Vallée Poussin (1866–1962) in 1896 that

$$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty,$$

What is this function?
The *prime number theorem* shows that the primes are very regularly behaved “in the large".

More exactly, we define the function

$$\pi(x) = \sum_{p \le x} 1 = \#\{p \le x \mid p \text{ prime}\}.$$

It was proved by Jacques Hadamard (1865–1963) and (independently) Charles de la Vallée Poussin (1866–1962) in 1896 that

$$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty,$$

which is a short form for writing

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

Proof relies heavily on complex analysis and is beyond the scope of these lectures.

Proof relies heavily on complex analysis and is beyond the scope of these lectures.

However, a weaker version, which still shows how the primes behave “in the large", is easier to obtain.

Proof relies heavily on complex analysis and is beyond the scope of these lectures.

However, a weaker version, which still shows how the primes behave “in the large", is easier to obtain.

This will be the main objective of this lecture.

Before the eventual proof in 1896, the most important advance was made by the Russian mathematician Pavnutii Lvovich Chebyshev (1821–1894) in 1850.

Proof relies heavily on complex analysis and is beyond the scope of these lectures.

However, a weaker version, which still shows how the primes behave “in the large", is easier to obtain.

This will be the main objective of this lecture.

Before the eventual proof in 1896, the most important advance was made by the Russian mathematician Pavnutii Lvovich Chebyshev (1821–1894) in 1850.

## Theorem 3

*For all $n \geq 2$,*

$$\frac{1}{8} \leq \frac{\pi(n)}{n/\log n} \leq 12.$$

## Theorem 3

*For all* $n \geq 2$,

$$\frac{1}{8} \leq \frac{\pi(n)}{n/\log n} \leq 12.$$

To prove this theorem, we first state another one:

## Theorem 4

*For all* $n \geq 2$,

$$\frac{1}{8} \leq \pi(n)\frac{H(n)}{n} < 6,$$

*where*

$$H(n) = \sum_{j=2}^{n} \frac{1}{j}.$$

## Theorem 3

*For all* $n \geq 2$,

$$\frac{1}{8} \leq \frac{\pi(n)}{n/\log n} \leq 12.$$

To prove this theorem, we first state another one:

## Theorem 4

*For all* $n \geq 2$,

$$\frac{1}{8} \leq \pi(n)\frac{H(n)}{n} < 6,$$

*where*

$$H(n) = \sum_{j=2}^{n} \frac{1}{j}.$$

In other words: $\pi(n)$ is of the same order of magnitude as the reciprocal of the average of $(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots, \frac{1}{n})$.

**Proof of Theorem 3** For $n \geq 2$ we have

$$\log \frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

**Proof of Theorem 3** For $n \geq 2$ we have

$$\log \frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

For $n \geq 4$ we have

$$\log \frac{n}{2} \geq \frac{1}{2} \log n,$$

**Proof of Theorem 3** For $n \geq 2$ we have

$$\log \frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

For $n \geq 4$ we have

$$\log \frac{n}{2} \geq \frac{1}{2} \log n,$$

and also

$$\frac{1}{2} \log 3 \leq \frac{1}{2} + \frac{1}{3}, \qquad \frac{1}{2} \log 2 \leq \frac{1}{2}.$$

**Proof of Theorem 3** For $n \geq 2$ we have

$$\log \frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

For $n \geq 4$ we have

$$\log \frac{n}{2} \geq \frac{1}{2} \log n,$$

and also

$$\frac{1}{2} \log 3 \leq \frac{1}{2} + \frac{1}{3}, \qquad \frac{1}{2} \log 2 \leq \frac{1}{2}.$$

Hence for all $n \geq 2$,

$$\frac{1}{2} \log n \leq H(n) \leq \log n,$$

and therefore Theorem 3 follows from Theorem 4.

**Remarks:** (1) The numbers $H(n)$ are closely related to the **harmonic numbers**

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}.$$

**Remarks:** (1) The numbers $H(n)$ are closely related to the **harmonic numbers**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

(2) In view of the first line of the above proof it is of interest to note that the limit

$$\gamma := \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$$

actually exists.

**Remarks:** (1) The numbers $H(n)$ are closely related to the **harmonic numbers**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

(2) In view of the first line of the above proof it is of interest to note that the limit

$$\gamma := \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$$

actually exists. $\gamma$ is called **Euler's constant**, also known as the **Euler-Mascheroni constant.**

**Remarks:** (1) The numbers $H(n)$ are closely related to the **harmonic numbers**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

(2) In view of the first line of the above proof it is of interest to note that the limit

$$\gamma := \lim_{n \to \infty} \left( 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \right)$$

actually exists. $\gamma$ is called **Euler's constant**, also known as the **Euler-Mascheroni constant.**

After the numbers $\pi$ and $e$ it is probably the most important special constant in mathematics, and it is also closely related to the **Gamma function** $\Gamma(x)$.

In preparation for the proof of Theorem 4, we first prove several lemmas.

In preparation for the proof of Theorem 4, we first prove several lemmas.

### Lemma 5

$$\pi\left(2^{k+1}\right) \leq 2^k.$$

In preparation for the proof of Theorem 4, we first prove several lemmas.

**Lemma 5**

$$\pi\left(2^{k+1}\right) \leq 2^k.$$

**Proof.** Even numbers cannot be primes, except 2.

In preparation for the proof of Theorem 4, we first prove several lemmas.

## Lemma 5

$$\pi\left(2^{k+1}\right) \leq 2^k.$$

**Proof.** Even numbers cannot be primes, except 2.
For $n > 9$ we clearly have $\pi(n) \leq n/2$.

In preparation for the proof of Theorem 4, we first prove several lemmas.

## Lemma 5

$$\pi\left(2^{k+1}\right) \le 2^k.$$

**Proof.** Even numbers cannot be primes, except 2.
For $n > 9$ we clearly have $\pi(n) \le n/2$.
For the smaller cases we count the primes:

$$\pi(2) = 1 = 2^0, \quad \pi(4) = 2 = 2^1, \quad \pi(8) = 4 = 2^2.$$

## Lemma 6

$$\frac{1}{2}l \leq H(2^l) \leq l.$$

## Lemma 6

$$\frac{1}{2}l \le H(2^l) \le l.$$

**Proof:** Group the terms of the sum $H(2^l)$ in 2 different ways:

$$\begin{aligned}
H(2^l) &= \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\
&\quad + \left(\frac{1}{2^{l-1}+1} + \cdots + \frac{1}{2^l}\right) \\
&\ge \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\
&\quad + \left(\frac{1}{2^l} + \cdots + \frac{1}{2^l}\right) \\
&= \frac{1}{2}l.
\end{aligned}$$

On the other hand,

$$\begin{aligned} H(2^l) &= \left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)+\cdots+\frac{1}{2^l} \\ &\le \left(\frac{1}{2}+\frac{1}{2}\right)+\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right)+\cdots \\ &\quad +\left(\frac{1}{2^{l-1}}+\cdots+\frac{1}{2^{l-1}}+\frac{1}{2^l}\right) \\ &\le l. \end{aligned}$$

## Lemma 7

*The canonical factorization of $n!$ is*

$$n! = \prod_{p \le n} p^{\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}.$$

## Lemma 7

*The canonical factorization of $n!$ is*

$$n! = \prod_{p \le n} p^{\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}.$$

**Proof:** Only primes $p \le n$ can occur in the factorization of $n!$.

## Lemma 7

*The canonical factorization of* $n!$ *is*

$$n! = \prod_{p \le n} p^{\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}.$$

**Proof:** Only primes $p \le n$ can occur in the factorization of $n!$. Fix such a prime $p$. In the sequence of factors

$$1,\ 2,\ 3,\ \ldots, n-1,\ n \quad \text{of} \quad n!,$$

– every $p$th number (namely $p, 2p, \ldots$) is divisible by $p$; there are $\lfloor n/p \rfloor$ of them;

## Lemma 7

*The canonical factorization of* $n!$ *is*

$$n! = \prod_{p \le n} p^{\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}.$$

**Proof:** Only primes $p \le n$ can occur in the factorization of $n!$.
Fix such a prime $p$. In the sequence of factors

$$1,\ 2,\ 3,\ \ldots, n-1,\ n \quad \text{of} \quad n!,$$

– every $p$th number (namely $p, 2p, \ldots$) is divisible by $p$;
there are $\lfloor n/p \rfloor$ of them;
– every $p^2$th number (namely $p, 2p, \ldots$) is divisible by another $p$;
there are $\lfloor n/p^2 \rfloor$ of them;

## Lemma 7

*The canonical factorization of $n!$ is*

$$n! = \prod_{p \le n} p^{\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots}.$$

**Proof:** Only primes $p \le n$ can occur in the factorization of $n!$. Fix such a prime $p$. In the sequence of factors

$$1,\ 2,\ 3,\ \ldots, n-1,\ n \quad \text{of} \quad n!,$$

– every $p$th number (namely $p, 2p, \ldots$) is divisible by $p$; there are $\lfloor n/p \rfloor$ of them;
– every $p^2$th number (namely $p, 2p, \ldots$) is divisible by another $p$; there are $\lfloor n/p^2 \rfloor$ of them;
– and so on, so that the power of $p$ in $n!$ is

$$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots$$

## Lemma 8

*The power of a prime p in* $\binom{N}{n}$ *is*

$$\sum_{m\geq 1}\left(\left\lfloor\frac{N}{p^m}\right\rfloor-\left\lfloor\frac{n}{p^m}\right\rfloor-\left\lfloor\frac{N-n}{p^m}\right\rfloor\right).$$

## Lemma 8

*The power of a prime p in* $\binom{N}{n}$ *is*

$$\sum_{m\geq 1}\left(\left\lfloor\frac{N}{p^m}\right\rfloor-\left\lfloor\frac{n}{p^m}\right\rfloor-\left\lfloor\frac{N-n}{p^m}\right\rfloor\right).$$

**Proof:** We use the fact that

$$\binom{N}{n}=\frac{N!}{n!(N-n)!}$$

and apply Lemma 7.

## Proof of Theorem 4

**Proof of Theorem 4**

(i) We begin with the following assertion:

$$\prod_{n<p\leq 2n} p \,\Big|\, \binom{2n}{n} \qquad \text{and} \qquad \binom{2n}{n} \,\Big|\, \prod_{p^r\leq 2n<p^{r+1}} p^r. \tag{1}$$

**Proof of Theorem 4**

(i) We begin with the following assertion:

$$\prod_{n<p\le 2n} p \,\Big|\, \binom{2n}{n} \qquad \text{and} \qquad \binom{2n}{n} \,\Big|\, \prod_{p^r\le 2n<p^{r+1}} p^r. \qquad (1)$$

**Proof:** We use the fact that

$$\binom{2n}{n} = \frac{(2n!)}{n!n!}.$$

**Proof of Theorem 4**

(i) We begin with the following assertion:

$$\prod_{n<p\leq 2n} p \,\Big|\, \binom{2n}{n} \qquad \text{and} \qquad \binom{2n}{n} \,\Big|\, \prod_{p^r\leq 2n<p^{r+1}} p^r. \qquad (1)$$

**Proof:** We use the fact that

$$\binom{2n}{n} = \frac{(2n!)}{n!n!}.$$

If $n < p \leq 2n$ then $p \mid (2n)!$, while $p \nmid n!$.

**Proof of Theorem 4**

(i) We begin with the following assertion:

$$\prod_{n<p\le 2n} p \,\Big|\, \binom{2n}{n} \qquad \text{and} \qquad \binom{2n}{n} \,\Big|\, \prod_{p^r\le 2n<p^{r+1}} p^r. \qquad (1)$$

**Proof:** We use the fact that

$$\binom{2n}{n} = \frac{(2n!)}{n!n!}.$$

If $n < p \le 2n$ then $p \mid (2n)!$, while $p \nmid n!$.

This proves the left part of (1).

On the other hand, by Lemma 8 the power of $p$ in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left( \left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\leq 1} \leq r.$$

On the other hand, by Lemma 8 the power of $p$ in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left( \left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\leq 1} \leq r.$$

This proves the right part of (1).

On the other hand, by Lemma 8 the power of $p$ in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left( \left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\leq 1} \leq r.$$

This proves the right part of (1).

(ii) Changing divisibility in (1) into inequalities, we get for $n \geq 1$,

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p^r \leq 2n < p^{r+1}} p^r \leq (2n)^{\pi(2n)}. \quad (2)$$

On the other hand, by Lemma 8 the power of $p$ in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left( \left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\leq 1} \leq r.$$

This proves the right part of (1).

(ii) Changing divisibility in (1) into inequalities, we get for $n \geq 1$,

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p^r\leq 2n<p^{r+1}} p^r \leq (2n)^{\pi(2n)}. \quad (2)$$

Left inequality follows from: $\pi(2n) - \pi(n)$ primes between $n$ and $2n$, and the smallest one is at least $n$.

On the other hand, by Lemma 8 the power of $p$ in $\binom{2n}{n}$ is

$$\sum_{m=1}^{r} \underbrace{\left( \left\lfloor \frac{2n}{p^n} \right\rfloor - 2 \left\lfloor \frac{n}{p^n} \right\rfloor \right)}_{\leq 1} \leq r.$$

This proves the right part of (1).

(ii) Changing divisibility in (1) into inequalities, we get for $n \geq 1$,

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p^r \leq 2n < p^{r+1}} p^r \leq (2n)^{\pi(2n)}. \quad (2)$$

Left inequality follows from: $\pi(2n) - \pi(n)$ primes between $n$ and $2n$, and the smallest one is at least $n$.

Right inequality follows from: Number of $p$ in the preceding product is $\pi(2n)$, while each factor $p^r$ is at most $2n$.

Now

$$
\begin{aligned}
\binom{2n}{n} &= \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1} \\
&= 2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{j}{n-j}\right)\cdots\left(2+\frac{n-1}{1}\right) \\
&\geq 2^n,
\end{aligned}
$$

Now

$$\begin{aligned}\binom{2n}{n} &= \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1} \\ &= 2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{j}{n-j}\right)\cdots\left(2+\frac{n-1}{1}\right) \\ &\geq 2^n,\end{aligned}$$

and

$$\binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}.$$

Now

$$\begin{aligned}\binom{2n}{n} &= \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}\\ &= 2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{j}{n-j}\right)\cdots\left(2+\frac{n-1}{1}\right)\\ &\geq 2^n,\end{aligned}$$

and

$$\binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}.$$

Hence, with (2) we get for $n \geq 1$,

$$n^{\pi(2n)-\pi(n)} < 2^{2n}, \qquad 2^{2n} \leq (2n)^{\pi(2n)}.$$

Now let $n = 2^k$, $k = 0, 1, 2, \ldots$.

Now let $n = 2^k$, $k = 0, 1, 2, \ldots$.
Then the last inequalities become

$$2^{k(\pi(2^{k+1})-\pi(2^k))} < 2^{2^{k+1}}, \qquad 2^{2^k} \le 2^{(k+1)\pi(2^{k+1})},$$

Now let $n = 2^k$, $k = 0, 1, 2, \ldots$.
Then the last inequalities become

$$2^{k(\pi(2^{k+1})-\pi(2^k))} < 2^{2^{k+1}}, \qquad 2^{2^k} \leq 2^{(k+1)\pi(2^{k+1})},$$

or

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1}, \qquad 2^k \leq (k+1)\pi(2^{k+1}). \qquad (3)$$

Now

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k,$$

where the first inequality follows from (3), and the second one from Lemma 5.

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k$$

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k$$

Replace $k$ successively by $0, 1, \ldots, k$ and add.

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k$$

Replace $k$ successively by $0, 1, \ldots, k$ and add.
On the left we have a “telescoping sum" so that

$$(k+1)\pi(2^{k+1}) < 3\left(2^0 + 2^1 + \cdots + 2^k\right) < 3 \cdot 2^{k+1}.$$

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \le 3 \cdot 2^k$$

Replace $k$ successively by $0, 1, \ldots, k$ and add.
On the left we have a “telescoping sum" so that

$$(k+1)\pi(2^{k+1}) < 3\left(2^0 + 2^1 + \cdots + 2^k\right) < 3 \cdot 2^{k+1}.$$

Using this and (3), we find

$$\frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \le \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}.$$

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \le 3 \cdot 2^k$$

Replace $k$ successively by $0, 1, \ldots, k$ and add.
On the left we have a “telescoping sum" so that

$$(k+1)\pi(2^{k+1}) < 3\left(2^0 + 2^1 + \cdots + 2^k\right) < 3 \cdot 2^{k+1}.$$

Using this and (3), we find

$$\frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \le \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}.$$

Now let $n \in \mathbb{N}$, $n > 1$, be such that

$$2^{k+1} \le n < 2^{k+2}.$$

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leq 3 \cdot 2^k$$

Replace $k$ successively by $0, 1, \ldots, k$ and add.
On the left we have a “telescoping sum" so that

$$(k+1)\pi(2^{k+1}) < 3\left(2^0 + 2^1 + \cdots + 2^k\right) < 3 \cdot 2^{k+1}.$$

Using this and (3), we find

$$\frac{1}{2} \cdot \frac{2^{k+1}}{k+1} \leq \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}.$$

Now let $n \in \mathbb{N}$, $n > 1$, be such that

$$2^{k+1} \leq n < 2^{k+2}.$$

Then

$$\pi(n) \leq \pi(2^{k+2}) < 3\frac{2^{k+2}}{k+2} \leq 6\frac{2^{k+1}}{H(2^{k+2})} \leq 6\frac{n}{H(n)},$$

where we have used Lemma 6 in the third inequality.

On the other hand,

$$\pi(n) \geq \pi(2^{k+1}) \geq \frac{1}{2} \cdot \frac{2^{k+1}}{k+1} = \frac{1}{8} \cdot \frac{2^{k+2}}{\frac{1}{2}(k+1)}$$
$$\geq \frac{1}{8} \cdot \frac{2^{k+2}}{H(2^{k+1})} \geq \frac{1}{8} \cdot \frac{n}{H(n)},$$

where we have used Lemma 6 for the second-last inequality.

On the other hand,

$$\pi(n) \geq \pi(2^{k+1}) \geq \frac{1}{2} \cdot \frac{2^{k+1}}{k+1} = \frac{1}{8} \cdot \frac{2^{k+2}}{\frac{1}{2}(k+1)}$$
$$\geq \frac{1}{8} \cdot \frac{2^{k+2}}{H(2^{k+1})} \geq \frac{1}{8} \cdot \frac{n}{H(n)},$$

where we have used Lemma 6 for the second-last inequality.

Putting the last two strings of inequalities together, we finally obtain the statement of Theorem 4.

Consequence of Chebyshev's theorem:

Proof of a famous and at that time unsolved problem, namely

**Bertrand's Postulate:** (J. L. F. Bertrand, 1845)

*If* $x \in \mathbb{R}$*,* $x > 1$*, then there is at least one prime in the open interval* $(x, 2x)$*.*

Consequence of Chebyshev's theorem:

Proof of a famous and at that time unsolved problem, namely

**Bertrand's Postulate:** (J. L. F. Bertrand, 1845)

*If $x \in \mathbb{R}$, $x > 1$, then there is at least one prime in the open interval $(x, 2x)$.*

Chebyshev said,
And I'll say it again,
There's always a prime
Between n and 2n.