## Lecture 1



3

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ ○

Yuri Tschinkel tschinke@cims.nyu.edu

#### Course webpage:

 $\tt cims.nyu.edu/^{\sim} tschinke/teaching/Spring24/number.html$ 

< 回 > < 回 > < 回 > <

Yuri Tschinkel tschinke@cims.nyu.edu

#### Course webpage:

 $\tt cims.nyu.edu/^{\sim} tschinke/teaching/Spring24/number.html$ 

Grader: Zhijia Zhang zhijia.zhang@cims.nyu.edu

A (1) > A (2) > A (2) > A

Yuri Tschinkel tschinke@cims.nyu.edu

#### Course webpage:

 $\tt cims.nyu.edu/^{\sim} tschinke/teaching/Spring24/number.html$ 

Grader: Zhijia Zhang zhijia.zhang@cims.nyu.edu

### Grading:

- Homework: 20%
- Midterm March 11: 30%
- Final May 6 50%

• • = • • = •



• Elementary number theory, residues, quadratic reciprocity

э

イロト イボト イヨト イヨト

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations

э

イロト イボト イヨト イヨト

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations
- *p*-adic numbers

- 4 回 ト 4 三 ト 4 三 ト

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations
- *p*-adic numbers
- Distribution of primes

▲ □ ▶ ▲ □ ▶ ▲ □ ▶

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations
- *p*-adic numbers
- Distribution of primes
- L-functions, primes in arithmetic progressions

A B b A B b

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations
- *p*-adic numbers
- Distribution of primes
- L-functions, primes in arithmetic progressions
- Basic algebraic number theory: number fields, rings of integers, class groups

- Elementary number theory, residues, quadratic reciprocity
- Diophantine equations
- *p*-adic numbers
- Distribution of primes
- L-functions, primes in arithmetic progressions
- Basic algebraic number theory: number fields, rings of integers, class groups
- Transcendence of e and  $\pi$

## Integers

 $\dots, -2, -1, 0, 1, 2, \dots$ 

イロト イポト イミト イミト 一日



#### $\ldots,-2,-1,0,1,2,\ldots$

#### Leopold Kronecker (1823-1891)

Integers were created by God, the rest is human labor.

(1日) (1日) (日) (日)

Integers are a group with respect to addition, a semigroup with respect to multiplication -a ring.

・ 同 ト ・ ヨ ト ・ ヨ ト

Integers are a group with respect to addition, a semigroup with respect to multiplication – a ring. Number theory investigates the structure of this ring.

▲ □ ▶ ▲ □ ▶ ▲ □ ▶

Integers are a group with respect to addition, a semigroup with respect to multiplication – a ring. Number theory investigates the structure of this ring.

Seems trivial: what is there to study?

• • = • • = •

### Adding is easy / multiplying is difficult.

æ

イロト イヨト イヨト イヨト

Adding is easy / multiplying is difficult.

Today, we don't even know accurate lower bounds for the complexity of multiplication.

イロト イボト イヨト イヨト

Adding is easy / multiplying is difficult.

Today, we don't even know accurate lower bounds for the complexity of multiplication.

Trivially, multiplying two *n*-digit integers takes  $O(n^2)$  steps. Best known bound is

 $O(n \log(n) \log(\log(n))).$ 

A (10) × (10)

# Number Theory

One of the oldest branches of mathematics.

э

イロト イボト イヨト イヨト

One of the oldest branches of mathematics.

**Gauss:** *Mathematics is the queen of the sciences – and number theory is the queen of mathematics.* 

• • = • • = •

One of the oldest branches of mathematics.

**Gauss:** Mathematics is the queen of the sciences – and number theory is the queen of mathematics.

Why?

- Elegant, simply stated problems
- Deep, difficult proofs that stimulate the development of new areas of mathematics

A B A A B A

• Algebra: manipulations of equations

▲ □ ▶ ▲ □ ▶ ▲ □ ▶

- Algebra: manipulations of equations
- Metric properties of numbers  $\mathbb{Q} \subset \mathbb{R},$  distance, Geometry of Numbers

A B A A B A

- Algebra: manipulations of equations
- Metric properties of numbers  $\mathbb{Q} \subset \mathbb{R},$  distance, Geometry of Numbers
- Complex numbers

A B K A B K

- Algebra: manipulations of equations
- Metric properties of numbers  $\mathbb{Q} \subset \mathbb{R},$  distance, Geometry of Numbers
- Complex numbers
- Harmonic analysis over  $\mathbb{R}$  (and  $\mathbb{Q}_p$ ), special functions

- Algebra: manipulations of equations
- Metric properties of numbers  $\mathbb{Q} \subset \mathbb{R},$  distance, Geometry of Numbers
- Complex numbers
- Harmonic analysis over  $\mathbb{R}$  (and  $\mathbb{Q}_p$ ), special functions
- Complex variables

- Algebra: manipulations of equations
- Metric properties of numbers  $\mathbb{Q} \subset \mathbb{R},$  distance, Geometry of Numbers
- Complex numbers
- Harmonic analysis over  $\mathbb{R}$  (and  $\mathbb{Q}_p$ ), special functions
- Complex variables
- Approximation theory

## Primes

### Definition

A positive integer  $p \ge 2$  is called prime if it is divisible only by itself and 1.

A B A A B A

## Primes

### Definition

A positive integer  $p \ge 2$  is called prime if it is divisible only by itself and 1.

### Example

primes: 2, 3, 5, 7, 11, 13, . . .

not primes: 1, 4, 6, 8, 9, 10, 12, 15, ....

Primes are **atoms** in the ring of integers, a free basis of the multiplicative semigroup.

< 同 ト < 三 ト < 三 ト

#### Theorem

Every positive integer is a product of prime factors

 $n=p_1\cdots p_r$ .

These prime factors are uniquely determined, up to permutation.

・ 同 ト ・ ヨ ト ・ ヨ ト

#### Theorem

Every positive integer is a product of prime factors

 $n=p_1\cdots p_r$ .

These prime factors are uniquely determined, up to permutation.

Proof: Use Euclidean algorithm.

伺 ト イ ヨ ト イ ヨ ト

#### Theorem

There are infinitely many primes.

Proof by contradiction. Assume that there are finitely many primes  $p_1, \ldots, p_n$ . None of these can divide the number

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Thus there exists another prime. Contradiction to the assumption.

## 888 AD., Bodleian Library, Oxford



イロト イポト イヨト イヨト

# To know and use

• Division with remainder

э

イロト イヨト イヨト イヨト

# To know and use

- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$

э

イロト イボト イヨト イヨト
- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$
- Finding x, y, d recursively (Euclidean algorithm)

• • = • • = •

- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$
- Finding x, y, d recursively (Euclidean algorithm)
- Congruences:  $a \equiv b \pmod{m}$  iff  $m \mid (a b)$

- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$
- Finding x, y, d recursively (Euclidean algorithm)
- Congruences:  $a \equiv b \pmod{m}$  iff  $m \mid (a b)$
- Solving congruences  $ax \equiv b \pmod{m}$

- E > - E >

- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$
- Finding x, y, d recursively (Euclidean algorithm)
- Congruences:  $a \equiv b \pmod{m}$  iff  $m \mid (a b)$
- Solving congruences  $ax \equiv b \pmod{m}$
- Euler function  $\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^{\times}$

• 
$$\varphi(p^n) = (p-1)p^{n-1}$$

•  $\varphi(ab) = \varphi(a) \cdot \varphi(b)$  if (a, b) = 1

・ 同 ト ・ ヨ ト ・ ヨ ト …

- Division with remainder
- gcd(a, b) = ax + by, for some  $x, y \in \mathbb{Z}$
- Finding x, y, d recursively (Euclidean algorithm)
- Congruences:  $a \equiv b \pmod{m}$  iff  $m \mid (a b)$
- Solving congruences  $ax \equiv b \pmod{m}$
- Euler function  $\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^{\times}$

$$\sum_{d|m}\varphi(d)=m$$

• Fermat's Little Theorem:

$$(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

э

• Fermat's Little Theorem:

$$(a,m)=1\Rightarrow a^{arphi(m)}\equiv 1\pmod{m}$$

In particular, if p is a prime, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

The converse is not true! There exist composite numbers m such that for all a one has

 $a^m \equiv a \pmod{m}$ .

< 回 > < 回 > < 回 >

The converse is not true! There exist composite numbers m such that for all a one has

 $a^m \equiv a \pmod{m}$ .

Theorem (Alford, Granville, Pomerance 1994)

There are infinitely many Carmichael numbers.

## First results about primes

### Theorem

### Assume that p > 2 satisfies $p \mid a^2 + b^2$ . Then $p \equiv 1 \pmod{4}$ .

・ 同 ト ・ ヨ ト ・ ヨ ト

## First results about primes

### Theorem

Assume that p > 2 satisfies  $p \mid a^2 + b^2$ . Then  $p \equiv 1 \pmod{4}$ .

**Proof:** 

• 
$$(p, a) = (p, b) = 1$$

・ 同 ト ・ ヨ ト ・ ヨ ト

## First results about primes

### Theorem

Assume that p > 2 satisfies  $p \mid a^2 + b^2$ . Then  $p \equiv 1 \pmod{4}$ .

#### **Proof:**

• 
$$(p, a) = (p, b) = 1$$
  
•  $a^2 \equiv -1 \cdot b^2 \Rightarrow (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot (b^2)^{\frac{p-1}{2}} \pmod{p}$   
•  $1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$   
• Thus,  $\frac{p-1}{2}$  is even, and  $p \equiv 1 \pmod{4}$ .

・ 何 ト ・ ヨ ト ・ ヨ ト

### **Corollary:** There are infinitely many primes $\equiv 1 \pmod{4}$ .

イロト 不得下 イヨト イヨト

**Corollary:** There are infinitely many primes  $\equiv 1 \pmod{4}$ .

**Proof:** Assume that there are finitely many  $p_1, \ldots, p_r$ . Consider

$$N:=4\prod_{j=1}^r p_j^2+1$$

- 4 回 ト 4 ヨ ト 4 ヨ ト

**Corollary:** There are infinitely many primes  $\equiv 1 \pmod{4}$ .

**Proof:** Assume that there are finitely many  $p_1, \ldots, p_r$ . Consider

$$N:=4\prod_{j=1}^r p_j^2+1$$

Every prime dividing N is of the form 4m + 1, so must be one of the listed primes, contradiction.

<日<br />
<</p>

## Representations as sums of squares

### Theorem

$$p \equiv 1 \pmod{4} \Rightarrow p = x^2 + y^2, \quad x, y \in \mathbb{Z}$$

э

伺 ト イヨト イヨト

## Proof

(1) Given  $r \not\equiv 0 \pmod{p}$  and e, f with ef > p there exists a representation

$$r = \pm x/y, \quad 1 \le y < f, \quad 1 \le x < e.$$

Indeed, we have  $e \cdot f$  numbers of the form  $y \cdot r + x$ , at least two have to be equal (mod p)

$$y'r + x' \equiv y''r + x'' \pmod{p}$$
$$(y' - y'')r \equiv x'' - x' \pmod{p}$$
$$r \equiv \pm \frac{x'' - x'}{y'' - y'} \pmod{p}$$

< ロ > < 同 > < 回 > < 回 > < 回 > <

## Proof

(2) Assume there exists an r with  $r^2 \equiv -1 \pmod{p}$ . We can represent it as

$$r \equiv \pm \frac{x}{y}, \quad 1 \le x, y \le \left[\sqrt{p}\right] + 1.$$

#### Then we have

$$x^2 + y^2 \equiv 0 \pmod{p} \Rightarrow x^2 + y^2 = mp$$
, with  $m = 1, 2$ 

If m = 1 we are done, if m = 2, we can write

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = p.$$

イロト イポト イヨト イヨト

# Representations by polynomials

### Theorem (Friedlander-Iwaniec 1998)

There are infinitely many primes of the form  $x^2 + y^4$ .

• • = • • = •

### Theorem (Friedlander-Iwaniec 1998)

There are infinitely many primes of the form  $x^2 + y^4$ .

### Theorem (Heath-Brown 2001)

There are infinitely many primes of the form  $x^3 + 2y^3$ .

A B A A B A

# Integral part

۲

۲

• [x] - integral part:

$$\label{eq:stars} \begin{split} [x] \leq x < [x] + 1 \\ \{x\} \text{ - fractional part, } \{x+1\} = \{x\}, \end{split}$$

$$x = [x] + \{x\}$$

$$[\frac{[x]}{m}] = [\frac{x}{m}] \quad \forall m \in \mathbb{N}, x \in \mathbb{R}.$$

(prove this at home)

æ

イロン イ理 とく ヨン イ ヨン

For an integer m > 1 write

$$m!=p_1^{\nu_1}\cdots p_s^{\nu_s}.$$

Then

$$\nu_j = \left[\frac{m}{p_j}\right] + \left[\frac{m}{p_j^2}\right] + \cdots$$

æ

<ロト <回ト < 回ト < 回ト < 回ト -

# Applications

Proof: List

$$1, 2, \ldots, m,$$
  
 $p, 2p, \ldots, k_1p,$ 

we have

$$k_1p \leq m < (k_1+1)p \Rightarrow k_1 = [rac{m}{p}].$$

Then

$$\nu = k_1 + \cdots$$

2

<ロト <回ト < 回ト < 回ト < 回ト -

# Applications

Proof: List

$$1, 2, \ldots, m,$$
$$p, 2p, \ldots, k_1p,$$

we have

$$k_1p \leq m < (k_1+1)p \Rightarrow k_1 = [rac{m}{p}].$$

Then

$$\nu = k_1 + \cdots$$

List

$$1, 2, \ldots, k_1$$

and repeat the process:  $k_2 = \left[\frac{k_1}{p}\right]$ .

э

Inductively,

$$\nu_p(m!) = \left[\frac{m}{p}\right] + \left[\frac{k_1}{p}\right] + \dots + \left[\frac{k_n}{p}\right], \quad \text{with} \quad \left[\frac{k_n}{p}\right] = \left[\frac{\left[\frac{k_{n-1}}{p}\right]}{p}\right].$$

2

<ロト <回ト < 回ト < 回ト < 回ト -

Inductively,

$$\nu_p(m!) = \left[\frac{m}{p}\right] + \left[\frac{k_1}{p}\right] + \dots + \left[\frac{k_n}{p}\right], \quad \text{with} \quad \left[\frac{k_n}{p}\right] = \left[\frac{\left[\frac{k_{n-1}}{p}\right]}{p}\right].$$

Now apply the lemma.

æ

<ロト <回ト < 回ト < 回ト < 回ト -

# Applications

How to use this?

#### **Example:** Find the maximal $\nu$ such that

 $3^{\nu} \mid 1000!$ 

э

イロト イボト イヨト イヨト

## Applications

How to use this?

#### **Example:** Find the maximal $\nu$ such that

 $3^{\nu} \mid 1000!$ 

#### Solution:

$$\nu = \left[\frac{1000}{3}\right] + \left[\frac{1000}{9}\right] + \left[\frac{1000}{27}\right] + \left[\frac{1000}{81}\right] + \left[\frac{1000}{243}\right] + \left[\frac{1000}{729}\right]$$
  
= 333 + 111 + 37 + 12 + 4 + 1  
= 498

э

イロト イボト イヨト イヨト

Let  $n \ge 9$  be an odd integer. Put

$$N_0 := n$$
,  $N_1 = N_0 + 1$ ,  $N_2 = N_1 + 3$ ,  $N_s := N_{s-1} + (2s - 1)$ 

with

$$1 \le s \le \left[\frac{n-9}{6}\right].$$

2

<ロト <回ト < 回ト < 回ト < 回ト -

## Tricks

### Theorem

*n* is composite iff for some *s*,  $N_s = t^2$ .

2

イロト イヨト イヨト イヨト

## Tricks

### Theorem

*n* is composite iff for some *s*,  $N_s = t^2$ .

#### **Proof:**

$$N_s = n+1+3+\cdots(2s-1)$$
$$n+s^2$$

If  $N_s = n + s^2 = t^2$  then

$$n = t^2 - s^2 = (t - s)(t + s).$$

æ

イロト イポト イヨト イヨト

Since 
$$s \le (n-9)/6$$
 we have  
 $n \ge 6s+9 > 2s+1, \quad t^2 = n^2 + s^2 > (s+1)^2,$   
 $t > (s+1) \Rightarrow (t-s) > 1,$ 

i.e., *n* is composite.

3

## Tricks

Conversely, suppose  $n = a \cdot b$ , with a, b odd. Then

$$3 \le a \le \sqrt{n}, \quad \sqrt{n} \le b \le n/3.$$

Put

$$s := \frac{b-a}{2} \Rightarrow N_s = n + s^2 = ab + \left(\frac{b-a}{2}\right)^2 = \left(\frac{b+a}{2}\right)^2$$

with

$$0 \leq \frac{b-a}{2} \leq \frac{1}{2}(\frac{n}{3}-3) \Rightarrow \frac{b-a}{2} \leq [\frac{n-9}{6}].$$

æ

How to use this? Let's try to factor 391:

 $N_0 = 391, \quad N_1 = 392, \quad N_2 = 395, \quad N_3 = 400 = 20^2.$ 

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

How to use this? Let's try to factor 391:

$$N_0 = 391$$
,  $N_1 = 392$ ,  $N_2 = 395$ ,  $N_3 = 400 = 20^2$ .

Thus

$$s = 3, t = 20 \Rightarrow 391 = (20 - 3)(20 + 3) = 17 \cdot 23.$$

æ

## Residues modulo primes: reminder

### • $(\mathbb{Z}/p\mathbb{Z})^{ imes}$ is cyclic, $\varphi(p-1)$ primitive roots (generators)

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <
(ℤ/pℤ)<sup>×</sup> is cyclic, φ(p − 1) primitive roots (generators)
Legendre symbol:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

(ℤ/pℤ)<sup>×</sup> is cyclic, φ(p − 1) primitive roots (generators)
Legendre symbol:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}, \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

(日)

(ℤ/pℤ)<sup>×</sup> is cyclic, φ(p − 1) primitive roots (generators)
Legendre symbol:

$$\begin{pmatrix} a \\ p \end{pmatrix} \equiv a^{\frac{p-1}{2}} \pmod{p}, \quad \begin{pmatrix} ab \\ p \end{pmatrix} = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} b \\ p \end{pmatrix}.$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(日)

• Quadratic reciprocity

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

э

• • = • • = •

Let *p* and *q* be odd primes. Put  $\zeta := e^{\frac{2\pi i}{p}}$  and consider the Gauss sum:

$$\tau_{p} := \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{j}.$$

Let *p* and *q* be odd primes. Put  $\zeta := e^{\frac{2\pi i}{p}}$  and consider the Gauss sum:

$$\tau_p := \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^j.$$

One has

$$\tau_p^2 = \sum_{j,k} \left(\frac{jk}{p}\right) \zeta^{j+k} = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \sum_{\substack{j=0\\j=0}}^{p-1} \zeta^{j(1+k)} \begin{cases} 0 \quad k \neq -1\\ p \quad k = -1 \end{cases}$$
$$= \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$$

$$\begin{aligned} \tau_p^q &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \cdot \tau_p \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \tau_p \pmod{q} \\ &\equiv \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{jq} \equiv \left(\frac{q}{p}\right) \tau_p \pmod{q} \end{aligned}$$

э

イロト イボト イヨト イヨト

$$egin{aligned} & au_p^q = (-1)^{rac{p-1}{2}\cdot rac{q-1}{2}} \cdot p^{rac{q-1}{2}} \cdot au_p \equiv (-1)^{rac{p-1}{2}\cdot rac{q-1}{2}} \left(rac{p}{q}
ight) au_p \pmod{q} \ &\equiv \sum_{j=1}^{p-1} \left(rac{j}{p}
ight) \zeta^{jq} \equiv \left(rac{q}{p}
ight) au_p \pmod{q} \end{aligned}$$

It follows that

$$\left(rac{q}{p}
ight) = (-1)^{rac{p-1}{2}\cdotrac{q-1}{2}}\left(rac{p}{q}
ight).$$

э

イロト イボト イヨト イヨト

# Logarithmus: John Napier(1550-1617)

### Mirifici Logarithmorum Canonis Descriptio (1614)

$$\log(a \cdot b) = \log(a) + \log(b)$$

・ 同 ト ・ ヨ ト ・ ヨ ト

# Logarithmus: John Napier(1550-1617)

### Mirifici Logarithmorum Canonis Descriptio (1614)

$$\log(a \cdot b) = \log(a) + \log(b)$$

Napier: Logarithms are artificial numbers and antilogarithms - natural numbers.

<日<br />
<</p>

- 1617 H. Briggs: *n* ≤ 1000
- 1628 A. Vlacq: n ≤ 100000
- 1795 G. Vega: logarithms of primes  $\leq$  10000

< ロ > < 同 > < 回 > < 回 > < 回 > <

81

(日) (四) (코) (코) (코) (코)



Abb. 10 Gauß' erste Logarithmentafel, ein Geschenk des braunschweigischen Herzogs Carl Wilhelm Ferdinand an den Vierzehnjährigen (D 2)

# G. Vega: Thesaurus logarithmorum completus

Bestseller: more than 100 editions.

イロト 不得 トイヨト イヨト

#### Bestseller: more than 100 editions.

### Gauss (1851)

Vega scheint sich nun mit der Hoffnung geschmeichelt zu haben, dass seine Tafeln fast fehlerfrei geworden seien, und verspricht, für die erste Anzeige eines Fehlers eine Prämie von einem Dukaten zu bezahlen. ...

Unter 568 geprüften irrationalen Logarithmen haben sich 301 als richtig und 267 als unrichtig ausgewiesen. Dürfte man dies Verhältnis als durchschnittlich zutreffend betrachten, so würden unter den 68038 irrationalen Logarithmen des Vega'schen Thesaurus ... nach der Wahrscheinlichkeit etwa 31983 fehlerhafte anzunehmen sein.

▲ □ ▶ ▲ □ ▶ ▲ □ ▶

# Distribution of primes

### Definition

#### $\pi(x) :=$ number of primes less than or equal to x.

э

イロト イヨト イヨト イヨト

# Distribution of primes

### Definition

 $\pi(x) :=$  number of primes less than or equal to x.

The pi-function for small values



### The pi-function for $x \le 100$



э

### The pi-function for $x \le 1000$



э

<ロト <回ト < 回ト < 回ト < 回ト -

### The pi-function for $x \leq 10$ million



э

イロト イポト イヨト イヨト

#### Goal: Find a simple formula for the pi-function.

æ

<ロト <回ト < 回ト < 回ト < 回ト -

## pi-function and the logarithm



A D N A B N A B N A B N

# pi-function and $x / \log(x)$



э

<ロト < 四ト < 三ト < 三ト

# pi-function divided by $x / \log(x)$



э

イロト イポト イヨト イヨト

### pi-function and integral-log for $x \le 1000$



イロン イ理 とくほとう ほんし

### pi-function and integral-log for $x \le 10000$



A D N A B N A B N A B N

Gouys 3. Eache 5 Briefe

Hochraverebrender Freund

75

Vorablen statle ich Shnen für die gewyentliche Ulersondung des Jahrbuchs von 1852 meinen verbendlich sten Back al.

Die gubige Arthlendung Jeen, Brunnen den ogen niches dere Programen der Brimsenklen sil mis ein proch alse einer Bessichness ihrungsauf generen lich haben miss männe äynen Bestähligtung ei mit dennichten Agenetischen ihr brimsenung gebracht, deren verk defärgesissienetekonsferet. Die falsen, von John 1972 under 1979, miss ihr die Landersträchsuchgedemacht, weich degenählenenspaßelen angesechnift hult. Sesser and alse ist mit falsen Untersteinung auf die haben Arthbeatht. Sesser and alse ist mit falsen Untersteinung auf die haben Arthbeathte und die alterekten ist einer ersteine seich geschählt, mein. Brighenertsneht und die alterekten ist weise der Vermanklan zu wichten, zu ersehen Versaund die alterekten ist die angebren Untersteinung verschlen. Die Arthoente lauf die haben altere abgebren Übeischen weiselchen ist. Herentbeaten die Jahen der alter alter angebren übeischen weisellen zu die Arten der die Aufen unter alter erstenderen zu dies verschlahen. Die Artenete lauf Aufen unter alter abgebren übeischen die verschlahen die Arten der der Aufen unter alter erstender zu geschlahen. Die Artenete laufe Ander angelechner zu geschlahen alter der Artenete der der Ander angelechner verschlahen zu die isten der der der Arten alter alter erstender zu geschlahen der der der Artenete der der Annachten unter einer professen Greegen zu die der Artenete der der Annachten unter einer professen geschlahen der der der Artenete der der Artenete der der der Artenete der der der Artenete der der Artenete der der Artenete der der der Artenete der der Artenete der der der Artenete der Artenete

I dan

aussericht under, some des hyperbehinde Lynnikhen verstunden werde. Se spielen Verte der ihr die is Verse Tehen (vom 1996) bater abgerricht Lith bis avonges bekande mehnen, staket ihr meise Abstehlung werte, aus, Eth jone, Verträtnig sestähligte. Eine geregte Franke meinhet mir 180 die Berschnieus von Obernass ertebrum, ausst als Abele (das nacher underschunden Aberschaftigte Wierstehlung der Althatte) sehe ohte eingelne underschaftigte Wierstehlunken versensch, um teht die bete dort eine Childese absurählten ; der als Chief, einer Aufter on genen liegen, oder aufte der Millein gener beteilt versensch, undet en genen liegen, oder aufte Millein gener beteilt der necht sellen-Lichen ist der An Millenmate (Lichtenskert (Medi die necht sellen-Lichen, ist erschn finklichen ungefühlt, Judie same Bueltaust Tafelachen Chiefen ausste fortuneten - In sind (same Am teh wieden Jahren) der Ansten isten abgesählt zu auft am Ausschaften versen Jahren Abeite beste abgester ausschaften ausschaften ausschaften besten Jahren Jahren der Auften isten abgeste abgestellt aus der Ausschaften ausschaften besten. Abeite hen aussten fortuneten - In sind (same Ausschaften Jahren) abeiten An eine Ausschaften Erschaften ausschaften ausschaften besten. Abeite hen um einen Kleinen Erschaften eine Ausschaften fahlen.

Abueich Differ Formel Prinzahla Unter 41 556 41806,4 + 50,4 41596.9 +40,9 500000 78 501 78627,5 +126,5 78672,7 +171,7 1000 000 114263,1 + 151,1 114374,0 +264,0 1500 000 194112 148883 149054.8 +171.8 149233.0 + 350.0 2000 000 2500 000 183016 183245,0 +229,0 183495,1 +479,1 3000 000 216745 216970.6+225.6 217308.5+563.6 Dass Legendre such unt mit diesem Gegenstande beschaf. tigt hat, was mir nicht bekannt ; auf Neranlassung threes Briefes habe it in seiner Theorie des Nombres nachzeschen, und in der gweiten ausgabe einige darauf berügliche Seiten gefunden, die ich früher überschen (oder seitdem verges. sen ) haben mufs , Legendre gebraucht die Formet legn - A 200 A cine Constante sein soll, fier welche ar 1.08366 setzt. Noch einer flichtig on Rechnung fin de ich danach in digen Fällen die Abweichungen - 23.3 +422 + 68,1 + 92.8 +159.1 +167.6 Diese Defferensen sind noch Kleiner als die nach den Integral, lie scheinen aber bei gunchmeniem n stille 1 hadles ne wachson als diese, to days leicht moglat ware, dass bei viel weiteres Fortsetning jene die letden über. trafen. Um Lablury und Formed in iller ein thing go brigen might man respective an statt A = 1,08366 sets on 1.09040 1.07682 407582 1,07529 1,07179 1,07297

<ロト (四) (三) (三)

Erscheint, daß bei wachsendem n der Durchschnettes) Werth von A abrimmit, ob aber die Grenze beim Wachsen des n ins Unendliche 1 oder eine von I verschiedene Griffe som wird dariber wage ich Keine Vernuthung. Ich kann nuht sagen, dass ene Betugnifs da est, einen gang ein frihen Greng werth zu er warten; von der andern Sette unhant der Ubarschups des A aber 1 gang frigheit ein John von der Ordnung - 19 sen. Ih wurde geneigt ein moglander, dass dass Differentel 19 ver der betriffender Function einfander son maß, als die Function sellert; Inden inform In voraus gesetet habe, wurde Legendres Fore cine Differential function wrausselys, die etwo - 2n Thre Tormel ubrigans winde fus in schr 5 . so, log - (A-1) n als mit  $logn - 1\frac{1}{2k} = 1$ iberein timment behachtet werden Konner, work der Modulas der Briggischen Loyarithmen ist, also mit Legendres Formel. wenn man  $A = \frac{1}{16} = 1,1513$  selft. Endlich will it much bemerken ; dass ich zwischen Abren Ab-zählungen und den meinigen ein Paux Differenzen bemerkthabe, Zwishen 59000 u. 60000 haben Sic 95 ich 94 101000 102000 94 93 Die orthe Differenzy hat vielleuht ihren Grund darin, dass in Lam berts Suppl. die Primzahl 59023 zweimahl aufzahihrt ist. Die Chiliade von 101000 - 102000 avimmelt in Lamberts Supplementer un Fehlern juk habe in meinem Exemplare 7 Lablen auszerhrichen die keine Primrahlen sind, u. dagezin 2 fehlende eingeschattet. Könnten Sie nicht den jungen Dase vormloffen, daße er die Frimzahlen in der fitzenden Millionen aus denjenizen bei der Akademie befindlichen Tafch abrabilite, die wie ich fürchte das Publicum nicht besitren soll? Fürdiesen Fell bemerke ich, das inder 2. u. 3 Million die abrahlung auf meine Vurschaft noch einem besondern Schema gemacht ist, welchy it selbst auch schon bei einen Theile lig erste million enjewant hatte. Die alzählungen von je 100000

49 stehes out ting (klein) Octavisate in 10 Columnen, je de sich auf Eine myriede bozichend; dazu Konunt noch eine Columne devor planks und eine dahinter rechts); jene geigtan als Beuput hier eine Vertical columne u. die beiden Quesatz alumnes aus dem 2 lavell 1000000 - 1100000 Un Erlanterung diere j A die the honjoulal rate ۲ In la myriade 1000000 4 21 hi 1010000 mid 100 54 Heraton haden ; dorunter Δ r 114 \$ 6 u ist I die nur eine Prim. 171 Jahl enthalt ; gar keine 14 mit 2 ver 3; 2 that 7 26 217 mit je 4 Prinizablen ; 8 164 19 ú ní 11 Auch mit je 5 u.s.w. 9 71 alle gusann yeber 752. 10 8 39 11 6 =1.1+4.2+5.11+ n 12 6.14 + 4.3. 00 Die letyle Columne of 6 erthalt die appregate 14 ausden 10 ein johnin . 16 Die Zahlen 14.15.16 m dy enter Vertical raise 1752 17210 Achen hier our Jun Weflups, la keine Hecatontala mit so violen Prinzables votkommen ; sie aber auf den folynden Mallen bekommen sie Geltung. Unletzt werden wieder die 10 Suiten in 1 veringt, w. umfossen so die gange 2" Moly Dach os il Peit abrubreches. Jek sage noch meinen he gluphe Deak für ghor mitteilunge über den Forburge die der tryin offent Justande. noch sicht man tienen answez pus dem Laborguth in des uns die Nachäfferie des Franssen sessort hat. Hate herz lichen Wunschen für Ihr Wohlbefindes Jottingen 24 Statt December Puts & Physics (849 C. F. Gands

▲ロ▶ ▲舂▶ ▲臣▶ ▲臣▶ 三臣 - のへの

My distinguished friend,

Your remarks concerning the frequency of primes were of interest to me in more ways than one. You have reminded me of my own endeavors in this field which began in the very distant past, in 1792 or 1793, after I had acquired the Lambert supplements to the logarithmic tables. Even before I had begun my more detailed investigations into higher arithmetic, one of my first projects was to turn my attention to the decreasing frequency of primes, to which end I counted the primes in several chiliads and recorded the results on the attached white pages. I soon recognized that behind all of its fluctuations, this frequency is on the average inversely proportional to the logarithm, so that the number of primes below a given bound n is approximately equal to

 $\int \frac{dn}{\log(n)},$ 

where the logarithm is understood to be hyperbolic.

Later on, when I became acquainted with the list in Vega's tables (1796) going up to 400031, I extended my computation further, confirming that estimate. In 1811, the appearance of Chernau's cribrum gave me much pleasure and I have frequently (since I lack the patience for a continuous count) spent an idle quarter of an hour to count another chiliad here and there; although I eventually gave it up without quite getting through a million. Only some time later did I make use of the diligence of Goldschmidt to fill some of the remaining gaps in the first million and to continue the computation according to Burkhardt's tables. Thus (for many years now) the first three million have been counted and checked against the integral.

	1	1		. 1	਼	1	-	1		1				1		1			
1	168	51	89	101	81	151	85	201	77	251	71	301	85	351	74	401	70	451	92
2	135	52	97	102	93	152	90	202	87	252	88	302	83	552	80	402	71	452	70
4	127	50	0y	103	an a	155	88	203	78	253	81	304	84	354	76	A04	75	450	20
1.5	119	55	90	105	91	155	84	205	77	255	76	305	88	355	87	405	70	455	74
16	114	56	93	106	82	156	85	206	85	256	87	306	80	356	79	406	83	456	82
7	117	57	99	107	92	157	76	207	83	257	72	907	82	357	67	407	67	457	73
1 9	110	59	90	108	76	158	87	208	87	258	78	308	75	359	83	409	79	459	75
10	112	60	94	110	88	160	85	210	88	260	76	310	80	360	71	410	82	460	68
11	106	61	88	111	89	161	85	211	84	261	77	311	79	361	68	411	73	461	27
12	103	62	87	112	84	162	84	212	86	262	73	312	69	362	79	412	81	462	69
14	105	64	93	114	88	164	83	214	81	264	84	314	86	364	84	415	60	464	74
15	102	65	80	115	82	165	77	215	86	265	80	315	76	965	77	415	90	465	85
16	198	66	98	116	93	166	80	216	74	266	78	316	77	366	77	416	80	466	74
17	98	67	84	117	81	168	81	217	76	267	87	317	84	367	85	417	67	467	69
19	94	69	80	119	24	169	73	219	84	269	36	319	84	269	72	419	85	469	85
20	102	70	81	120	\$7	170	87	220	91	270	78	320	86	370	68	420	75	470	72
21	98	71	98	121	38	171	87	221	78	271	84	321	79	\$71	70	421	75	471	87
22	104	72	95	122	86	172	81	222	80	272	78	323	81	372	76	422	73	472	78
24	104	74	83	12.4	88	174	79	224	80	274	71	324	71	374	73	A24	83	474	78
25	94	75	92	125	83	175	83	225	\$3	275	80	325	87	375	82	425	81	475	80
26	98	76	91	126	54	196	75	226	84	276	83	326	85	376	85	426	74	476	86
27	101	77	83	127	83	177	95	227	76	297	83	327	73	377	80	427	71	477	25
29	98	19	84	129	89	179	89	229	89	279	81	320	73	379	77	429	71	479	85
30	92	80	91	130	83	180	94	230	88	280	73	330	81	380	83	430	89	480	71
31	95	81	88	131	85	181	71	231	8.4	281	87	331	80	381	72	431	76	481	77
33	92	82.	92	133	87	183	41	232	78	282	77	332	72	382 383	76	432	19 8A	484	78
34	100	84	84	194	82	184	79	234	71	28.4	72	334	80	384	81	434	80	484	75
95	94	85	87	135	80	185	83	235	87	285	9ø	\$35	77	385	78	435	85	485	63
36	92	86	85	136	39	186	91	136	13	286	71	336	77	386	180	436	82	486	63
37	99	88	93	138	80	188	3	138	13	288	71	338	80	388	69	438	70	488	28
39	90	89	76	139	85	189	80	239	87	289	85	339	17	389	7 <i>\$</i>	439	75	489	83
40	96	90	94	140	84	196	88	240	79	290	84	340	68	390	84	440	75	490	78
41	88	91	89	141	87	191	30	241	80	291	84	341	84	391	81	441	79	491	78
43	102	93	97	143	82	193	89	243	76	293	78	343	77	393	86	443	85	493	67
44	25	94	86	44	77	194	84	244	27	294	68	344	80	394	87	444	88	494	8
45	96	95	87	45	79	195	74	245	78	295	85	345	80	395	75	445	82	495	80
46	86	96	95	146	84	196	85	246	80	296	73	347	80	396 397	72 75	446 447	68	496	6
47	95	98	82	148	83	148	87	248	79	298	73	348	82	398	75	448	73	498	8
49	89	99	87	149	83	199	96	2.49	88	299	73	349	77	397	82	449	70	499	73
50	98	100	87	150	91	200	77	250	00	1000	18	330	8,2	400	81	450	80	500	8

(山)の「(間))(目)、(目))

- 12

÷.,		-÷	-	<u> </u>	-		-	- ¥ -		<u> </u>			-	-	- +	-+-	-			Υ.
501	78	551	79	601	75	651	61	701	75	751	68	801	85	851	70	901	74	951	76	
\$02	74	552	75	602	73	652	74	702	71	752.	85	802	66	852	77	902	73	952	70	
509	67	\$53	71	603	83	653	85	703	81	753	73	803	90	853	74	1903	70	953	78	1.1
604	76	254	80	604	76	654	64	704	71	25A	71	80A	64	854	66	904	63	454	65	
\$05	76	85	77	605	73	645	78	705	87	755	83	805	78	855	21	905	81	455	73	
1.1		611	1.	6.6	-	64	10	Hal	10	1141	-	0.1	70	856	73	land	170	1.7		
500	44	530		600	74	030	"	100	08	100	4	300	12	857	78	acr	100	950	76	
,07	10	257	00	607	12	1007	71	101	114		200	807	0.8	100	14	P.".	1.00	1957	58	
508	25	558	68	608	78	1458	70	703	74	158	68	808	70	858	76	908	80	958	69	
\$09	70	339	74	609	78	059	12	109	77	139	79	809	09	1009	09	209	19	959	77	
510	75	\$60	77	610	80	660	73	710	77	760	77	\$10	78	860	71	910	9.2	960	69	
3.11	72	561	86	611	73	661	83	711	78	761	77	811	78	861	77	911	62	961	68	
512	82	562	61	612	71	662	70	712	76	762	80	812.	72	862	74	912	81	462	88	•
513	70	563	83	613	76	663	74	713	12	763	68	813	69	863	83	913	71	l463	31	
514	77	564	67	614	79	664	77	714	23	764	79	814	72.	564	60	1914	54	964	74	
515	81	565	77	615	71	665	77	715	66	765	n	815	78	865	80	915	73	465	74	
eif.	41	666	70	61	25	64	77	716	83	264	\$2	811	60	861	80	la.C.	70	144	20	
310	00	640	18	12.	10	144	73	1717	6	767	100	0.0		106.7	60	1200	20	1.00	10	
217	03	1007	1/2	217		100	70	1 110	14	101	12	217	15	060	79	12.2	12	967	13	
518	22	\$68	72	018		008	13	17"	100	168	108	218	13	008	10	1718	19	968	06	
,19	76	569	71	619	67	669	66	519	07	769	177	\$19	62	1869	80	919	75	969	75	
\$20	78	570	30	620	73	670	74	720	74	170	/4	820	83	870	73	920	171	970	73	
21	73	571	85	621	77	671	75	721	78	771	77	821	75	871	79	921	72	971	76	
522	83	572	72	622	70	172	76	722	77	172	75	\$22	72	872	58	922	72	472	78	
523	79	573	85	623	74	673	76	723	19	773	70	823	84	873	76	923	72	473	74	
52.4	69	574	72	624	75	674	27	1984	186	774	76	824	78	874	65	1924	81	474	63	
525	11	575	70	625	68	675	64	725	75	775	72	\$25	71	875	25	1925	76	475	85	
\$26	70	676	-	44	60	676	75	nob	60	1996	67	001	81	876	80	1026	100	1.	1	
C47	19	1	110	140	29	672	70	1,20	69	110	100	\$24	28	877	00	120	1.0	976	70	
	04	100	10	1.7	100	6	14	140	76	111	120	1 828	60	1.0	10	P.*/	174	977	66	
248	72	r	17	618	70	620	.2	128	75	178	10	100	2	878	107	228	63	175	60	•
249	10	279	16	100	75	6/9	02	1000	1/6	179	81	049	179	079	08	1929	170	1979	80	
2.20	18	380	"	Car	10	000	03	1.50	15	780	11	3.30	08	880	75	930	80	980	05	
31	80	581	73	631	67	1881	75	731	69	781	70	\$31	76	881	80	931	69	981	67	
532	68	382	79	632	81	682	78	732	76	782	82	832	79	882	69	432.	64	982	75	
533	79	583	79	633	77	683	66	733	71	789	68	835	82	883	72	633	76	683	70	
34	74	584	78	634	70	684	78	734	75	784	74	834	68	884	73	634	60	Ľ.	70	
535	72	585	72	635	82	685	72	735	74	785	75	835	67	885	69	1935	81	12.	194	
\$96	71	586	81	616	78	686	74	736	70	786	77	836	73	281.	77	096	60	17.22	26	
ca.4	\$7	1007	70	697	11	6.07	24	797	60	787	20	837	71	887	76	637	21	730	46	
(10)	10	100	19	20	15	1200	17	120	1 70	1.00		1928	64	888	171	2	121	124	12	
100	70	500	87	028	74	088	82	190	10	100	10	\$30	80	440	177	1928	74	788	12	
2.29	10	100	13	139	29	689	74	139	,0	109	40	0.79	60	009	16	1939	12	989	12	
.40	71	390	08	100	14	090	19	140	81	790	08	840	09	890	68	940	68	9.90	72	
541	73	591	71	641	77	691	60	741	67	791	78	841	70	\$91	68	941	74	991	171	
\$42	77	592	67	642	71	692	79	742	74	192	71	842	69	892	80	942	79	992	79	
543	78	593	80	643	68	693	77	743	73	793	82	843	83	893	69	943	72	6.	68	
\$44	81	\$94	77.	644	70	694	73	744	67	794	71	844	68	894	72	944	76	604	68	
\$45	68	595	78	6.45	86	695	76	745	64	795	73	845	78	895	74	945	73	995	78	
\$46	68	596	77	646	75	696	77	746	67	796	79	846	70	846	80	446	66	046	60	
547	73	507	74	647	74	697	23	747	76	707	77	867	60	807	60	447	22	1790	109	
48	76	100	23	648	74	698	79	748	71	200	72	840	27	800	75	440	ú	1797	09	
40	77	170	72.	640	73	640	62	749	76	1700	21	800	11	200	26	140	1.	998	83	
real	78	22	12	650	100	700	72	200	100	277	<i>.</i>	100	2	10.99	6	749	20	999	74	
	10	000	10	- 10	-4	,00	12	1,50	12	1000	01	1050	08	1980	0	1950	15	1000	65	

			9	ð un	aa	hte	n				
		vo	n 1	0000	00	bi.	110	000	ođ.		
	0.	4.	2.	3.	A	5.	6	7.	8	و	1
1.	1.		-	1		1	-	1			1.
2.		1.				4.		4.	۹.		4.
з.		4.	2.	2.	3.	1.	2.	. 3.	3.	1.	٤١.
4	2.	8.	5.	4.	3	6	.9.	4.	5.	8.	\$4.
5	H.	10.	8.	18.	12.	10	10.	12.	15.	8	114
6	14.	14.	18.	25.	16.	22.	19.	15	17.	15.	171.
7.	26	(7.	23	23.	24	24	17.	22	20.	24.	217.
8.	19.	19.	24.	7.	14.	15.	20.	17.	15.	17.	164.
9.	H.	13	.a.	13	14.	14.	12.	13.	11,	16.	126.
10	8.	6.	8.	5.	9.	5.	5.	9.	7.	9.	71.
11.	6.	6.	4.	6.	з.	4.	з.	4.	4.	5.	39.
12.	1.	1.	2.	1.	4.	1.	2.	2.	4.		12.
13	1.	٠ł.			ı.	1	1.	5.	1.		6.
14											
15.											
16											1
	752	719	732.	700.	734.	698	743.	722.	706.	737	7210

<□> <0>
<□> <0</p>
<□> <0</p>
<0</p>

Gauss Math 18

444/3 3

Primzahlen von 1100000 bis 1200000. 0. 1. 2. 4. 5 6. 7. 8. 9. ø 1. 4. 5 1. 1 4. 3. 3 3. 3. 3. 3. 2 1. 25 6. 7. 6. 5. 5. 6. 57 4 9 4. 4 8.1 13. 10. 12. 15. . 9 ' 12. 11. 12 9 117 14. 20. 17. 20. 17. 19 18 6 16 17. 14. 170. 19. 22. 19. 24. 20. 18 20. 27 217 24. 24. 10. 12. 40. 18 20. 17 19. 8 9. 20 160 6. 10. 10. 2. 2. 5. 0 16 17. 7. 11. 16 44 12 15. 134 6. .9 8 77 h 11 1. 4. 4. 5. 9. 2. 32 1 1 1. 2. 3. 1. 2. \$5. 13 1. 5 1. 2.1 736 710 746 743 692 725 720 723 725 740 7194 J dax ...... 7165.9! a starter 438 .

4

#### ◆□▶ ◆□▶ ◆三▶ ◆三▶ ○□ の々で

Math 18

(4) ##af #

<ロ> (四) (四) (三) (三)

æ

Jumzahlen. in 1200000 tis 1300000 . 0. 1. 2. 3. 4. 5. 6. 7. 8 9. 12. 1 2. 2 з. 32 62 化育动的 120 .15 9.17 49. 16 160 166 15 2ů 14 209 240 219 15 22. 4 4 169 165 22. 15 14 410. 111 13 0 73 76 10 **3**, 5. 16 35 \$ 2. 3. 3 3. 36 2? 4 1. 1. ч. 9. 13 1. 14 4. 16 604 207 693 693 79 712 716 76 ş J dar = 2123,35.
gung , Math 18. . . . 5. 444 5



1200 000 - 1300 000



1300 000 --- 1400 000

#### ◆□▶ ◆□▶ ◆三▶ ◆三▶ ○□ の々で

Math 18 6º 440/ 6 Primrahlen von 100000 bis 1400000 4. 2. э. A.) 5. 6 6 6 11. 6. 8. 7. 6. 6. 5. 6 4. 11. 14. 15 12. 8. 8. 14. 10. 11. 10. 11. 4.1 1. 14 4 109 200 21 200 6 12 248 20 21 625 207 70 94 7/3 7/3 723 J dx - 50 84, 48

《曰》 《聞》 《臣》 《臣》 三臣

F) #4 4 7 Math 18 1400000 bis 1500000 141 . 142 . 143 . 144 . 145 . 146 . 147 . 148 . 149 . 150 o 183 179 183 22 14 ío 680 117 .723 703 701 716 705 706 698 7028 1 da = 1048. 78186 

#### (ロ) (型) (E) (E) (E) (の)(C)

1500000 his 1600000 151 152 133 154 155 156 157 188 189 160 ~ 10 28 77 124 1999 1749 124 63 29 17 6 17 22 20 119  $\ddot{\eta}_{l}$ ź íL 731 702 bgi 630 701 693 675 698 714 12x = 7015, 78776 80.4T.

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○□ の々で

1600000 his 1700000 161. 162 163 164 165 166 167 168 169 170 0 \_\_\_\_\_ 18 203 13 14 12 19 174 13 130 9 63 3 26 21, \_ 119 bg4 710 bg2 bg2 100 716 702 b75 712 7012 france = 6985, 13714

<ロ> (四)、(四)、(三)、(三)、

- 2

1700000 his 1800000 171 172 173 174 175 176 177 178 179 150 íо 695 685 691 689 706 684 679 700 689 713 6921 Juneo Logar = basb, 53562 NIEDERSXCHS. STAATS-U.UNIV: BIBLIOTHEK GUTTINGEN

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○□ の々で

Math 18. 1800000 bis 1900000 (9) ##a/ 9 181 . 182 . 183 . 184 . 185 . 186 . 187 . 188 . 189 . 190 ~ 175 206 161 23 ź2 \_ 704 b72 718 by4 700 707 703 b89 b97 b91 b955 12x = 6929, 73917 

1900000 his 2000000 191 . 192 . 193 . 194 . 195 . 196 . 197 . 198 . 199 . 200 2 7 12 10 31 20 6 16 20 17 15 18 21 8 15 20 10 148 .9 \$ ío -689 . 697 . 711 . 683 . 692 . 685 . 673 . Tyo . 688 . 114 6902 Jagr 6904, 54424 NIEDERSACHS. STAATS- U. UNIV: BIBLIOTHEK GUTTINGEN

<ロト (四) (三) (三)

- E

Angahl des Vingablen gwischen 200000 and 2100000 . 40 201 202 203 204 205 206 207 208 209 210 /3 23 25 /3 22 204 19 157 4 11 12 11 14 . // ío 15 11 6 11 6 63 - 21 5 3 - 1 3 . 3 - 8 13 1 691 671 671 694 694 694 1. 6874. Li = 6880.780 Angabel der Primzahlen zwischen 2100000 und 2200000 211. 212 213 214 215 216 217 214 219 220 /\$3 <u>\_\_\_</u> F E 3 3 5 3 6057. Li - 6058. apr. ۲ş - 4

<ロト (四) (三) (三)

æ

Anzahl der Frinzahlen wiechen 2200000 und 200000 221 222 223 224 225 226 227 228 229 230 List IS .11 701 660 bys beo bes bes 701 by4 662 bes being 1.1. 6536.977 Ungahi der Bringahlen zwischen 200000 und 2400000 231 232 233 234 235 236 237 238 239 240 \$6 'n. mi i 640 662 672 671 666 690 691 660 705 650 6787 S.i. 6016.700 NIEDERSTCHS STAATS- U. UNIV BIBLIOTHEK CUTTINGEN

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

Angahl der Trimjahlen juischen Horsoo und 20000 the At 11) 241 242 243 244 245 266 267 248 249 250 x Ś 600 690 672 657 701 687 666 672 687 670 6766 Li. 6797.394 Angahl der Primyablen wischen 250000 und 260000 251 252 253 254 255 256 257 258 259 260 4.68 \$\$ /3 677 675 696 670 670 671 678 693 693 676 6804 Li. 6778.960 NIEDERSXCHS. STAATS U. UNIV BIBLIOTHEK GUTTINGEN

◆□▶ ◆□▶ ◆三▶ ◆三▶ ● □ ● ●



◆□▶ ◆□▶ ◆三▶ ◆三▶ ● □ ● ●

281 282 283 284 285 286 287 249 4 4 7 8 19.16 14 7 14 14 . 18 18 17 20 13 29 . 15 . 21 179 11 20 20 27. 22 23 . 21 22 222 4 20 13 12 9 12 12 14 17 12 12 10 11 log 7 4 8 3 3 3 12 2 1 2 14 1 - - 1 - -- 2 690 695 667 704 671 654 672 653 676 662 6744. Li 6728,220 ... Anguhl der Pringahlon justchen 2900000 and Boorooo 291 292 293 298 295 296 297 298 299 300 #**7** . 17 15 . 23 11 14.19 . 11 . : 1 12 13 . 11 // -------600 663 671 680 649 652 694 650 671 687 6705 L: 6712.64

▲ロト ▲御ト ▲ヨト ▲ヨト 三ヨ - のへで

Anzahl der Primzahlen zwischen 2000000 und Bootooo 210 . 220 230 240 250 260 270 280 290 300 \$\$ лġ. 146 138 1 /53 197 183 . 179 201 205 157 168 £ 115 109 113 st 1 \$3 śз \_\_\_\_\_/'` . 14 . 15 6874 6857 6849 \$787 6766 6804 6762 6714 6744 6705 Jas = 67915,733 Die sharg to lealade onthill heine Primpa ll Die 17050 & Contade enthalt 17 Primpollon NIEDERSACHS. STAATS- U. UNIV: BIBLIOTHEK GUTTINGEN

(日) (部) (注) (注)

훈

..... 

(日) (四) (三) (三) (三)

- 12

Guns Math 18 1000000 bis 2000000 (13) 44af 13 110 120 130 140 160, 160 170 Ma 190 200 1 1 - 1 5 10 **21** 25 32 19 19 57 57 63 69 72 114 107 120 119 129 77 124 29 30 22 34 68 76 71 67 120 152 135 136 11 170 160 173 183 199 173 183 199 189 174 175 182 207 179 172 203 194 206 221 161 183 199 174 147 161 148 113 103 s . . / Ì\$ ĸ ∫dx = 70427.78 110----

(日) (四) (三) (三) (三)

- 2

	1210	1220	1230	, 124 ,	125	, 126	. 127	. 128	129	. 130	4
/								1	/		2
2	2		2	/		-	-	-	-		6
3	3	2	4	5	- 4	3	1	4	3	3	32
4	7	7	7	3	5	7	12	2	3	10	63
5	15	12	12	15	lo	14	9	15-	6	12	120
6	16	/1/	13	19	17	16	16	15	20	- 14	160
7	24	15	25	24	21	20	15	22	24	24	214
8	17	19	16	1	17	15	22	18	19	14	168
9	8	12	¥7	10	12	13	14	13	13	9	111
10	3	//	10	8	10	4	5	3	9	10	73
11	3	ł	3	2	з	5	3	6	1	3	35
12	1	1	1	-	2	/	3	1	1		9
13	1	1		1	-	2	-				5
14				1	-		_				1
15					-	***					
 16					1	_	-				1

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへで

20	1.	1 23		23 1	29 1	25 1	292	31.2	11.2	35 2	
34	. 3	34	ۏ	45 4	45 4	45 4	45 4	47.4	47.4	49.4	
\$7	8	\$7	8	87 8	91 9	100 10	100 10	100.40	100.40	100.40	S .
15	4	45	4	49 4	50 4	50 4	50 4	50.4	84	52.4	2
45	4	45	. 4	45 4	45 4	45 4	45.4	47.4	47.4	48.4	31
17	- <u>(</u> -	20	1	20 1	22 1	221	26 1	28 1	28.1	34.2	5.
19	S. 1	21	1	21 1	21 1	26 2	26 2	28 2	28.2	29 2	20
/8	12 I	20	1 1	26 L	26 2	26 2	26 2	26 2	12.2	33.2	2
19	/	21	1 1	21 1	21 1	25 1	27 1	33 2	322	34.2	0.0
100	10	100	10	100 10	100 10	100 10	100 10	100 10	100.00	100.10	
404	34	416	34	437 36	444 37	464 39	474 40	440 41	446.41	\$14.42	,
27 May.2	Aug. 14	1818 Min	2) Mire 17	Marz 25	Mai 6	Ma: 13	Mai 18	Main	Jun 14	Jun 29	
38.2	44. 3	46.3	48 3	58.4	60.4	62.4	66.4	72.5	74.5	74.5	
52.4	54.4	\$6.4	59 4	60.4	60.4	60.4	66.4	66.4	68.5	70.5	
100.10	100.10	100.10	100 10	100.40	100.10	100.10	100.10	100.10	100.10	100.10	
54 4	56.5	58.5	58.5	59.5	60 5	60.5 +	04.5	08.5	68.5	90.5	
49 4	49.4	51.4	51.4	53.4	60.4	60.4	60.4	66.4	70.5	70.5	
36 2	40 3	42.3	42.3	52.4	60.4	60.4	60.4	60.4	64.5	70.5	
912	34 2	A0 2	46 3	54:4	60.4	60.4	60.A	60.4	64.5	70.5	
\$4.2	362	38 2.	44 3	50.4	52.4	60.4	60.4	60.4	62.5	62.5	
35.2	36,2	38.2	44 3	50.4	52.4	60.4	00.4	00.4	66.5	06.5	
	100.10	100.10	100.10	100.10	100.10	100.10	100.10	100.10	100 40	100.10	
2 6 9.42	349.45	569.45	5 <b>92.</b> 48	630.53	664.53	082.53	1 696.53	712.54	756.60	\$ 752.6	o
										*	
									- (G	U.G	
										- Sa	•,
ALC: NO.			1.1							$\sim$	

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

3	1824 Jal.	1.46	augel	Septis	1890	40	Mai 17	Ma2 26	Jun 14	7	fels	1000	ine là	100
e.	88.8	90.8	94 8	100.10	100.10	100.10	100.10	100.50	92.6	94.7	96.5		100 10	1
	70.5	70.5	70.5	10.5	100.10	100.10	100.10	100.10	82.5	100.10	86.5	88.6	88 6	
	70.5	70.5	70.5	70.5	72.5	72.5	76.5	76.5	80.5	80.5	86.5	86.5	865	
į.	70.5	70.9	70.5	70.5	72.5	12.5	76.5	76.5	78.5	78.5	78.5	78.5	78 5	÷
ų.	70.5	70.5	70.5	70.5	72.5	74.5	76.5	76.5	76.5	78.5	78.5	78.5	78 5	
	66.5	68.9	72 5	72.5	74.5	76.5	76.5	76.5	100.10	100.10	100.10	100. 10	1 100.0	. 73
	100.10	100.10	100.10	100.10	814 6	6 822.6	6 842:65	850.6	6 \$60,6	\$ \$72.6	7 84.	890.5	5/094	

77 2.63 776.63 786,65 79

4

a, b

<ロ> (四)、(四)、(三)、(三)、

æ

0.715) 6 40.812 - 0.0263 0.7122 . 2772 0.7128 0.2465 94687 -0.7944+0.4777 +0.1855 - 0.165 +0.4691 . 0.7102 猢 +a+618 . +0.535 -00171 8 645// 1/2400/ 17 2820/ 2649 1649 1049 1049 1049 1049 1040 00000070 esservit 0.002241 0.022241 energy a 1002081 120000 ¢ \*\*\*\*\*\* annaat × "7)"tong

(日) (四) (三) (三)

- E

1.10		20	-20		41	12.6	<u>۱</u>	6	61 - 3	11'	. 74	19	41	1 25		0-105		101-121		1 4	12.15		10 14		.48	× 16	10-10	165	N
		Ż,			<i>zi</i> ,			140			1. A.			2	1		4.0			20			3. 10 2.4.9 2.4.9			28			1. 10 2. 10 2. 19
+							h							1.4			÷;						1.0						
11														1.1	<b>1</b>														
	- 4																												
+	- 1			- 1							1						-												
11																							1						
				_			81.																						
																							i						
				- 1				£															- · · · · ·						
				-				-	÷																			-	
				_																									
																												-	
								1																					
	_			- 1																									
-1-	-																												
-				- 1										1															
													r	1															
-1-				- 1										1 .															
- 1-														1															

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

S locure	ak 29. 80904						
Loccon	18036.05216	+ 8400.24312	355.60305				
Jacoco	26086,69223	8050. 69007	214.71030*	140.89275	78. 32915		
400000	33922,62200	7835.92977	152.14670	62.56360	27 77793	50.55122	\$4.78461
aborre.	41606.40507	7683.78307	117.36103	\$9.78 567	12.01132	15.70001	11.14331
600000	44112.82711	7566 42384	44.58668	22-77435	7.38802	4.62330	1.299.00
Forece	58649,66247	7.471.83536	74.20035	15.38633	4.06372	3.32430	1.07819
800000	64037.20748	7392.63501	67.81774	11-32261	2.70761	1.35611	0.50042
400000	7/362.05975	7324.75727	59.26274	8.61500	1. 45242	0.85519	0.22424
1000000	78627.54928	7265.49453	\$2.50016	6.76298	1.32147	0.53095	0.18252
1100000	35840.54365	7212.99437	47.05905	5.44111	097304	0,34843	0.112.73
1200000	91006, 47897	7105.93532	4259998	4, 46807	0.73734	0,13570	0.071.07
1300000	100129, 82331	7125, 34434	36.86025	3, 73093	0.57271	0,16463	0.04181
1400000	107214,30740	7084, 48409	35.70223	3, 16802	0.44989	0,12282	0.03758
1500000	114263.45926	7948. 78186	52 94610	2,70813	0.36465	0.08524	0.01497
1600000	121 278,87702	7015,78770	30. 85062	2. 34345	0.20438	0.07027	0.01992
1700000	128 264,01416	6985, 13714	. 28.60152	2.04910	0.24403	0.05035	0.10937
1800000	135 220, 54978	6956 53562	26,74645	1.8050	0 20355	c.c.9.c.98	• / /
1400000	142150,28895	6929. 73917	25, 14493	1.6015	2		
2000000	140054 83310	6904.5442	4 799°				

NIEDERSACHS. STAATS U. UNIV: BIBLIOTHEK GUTTINGEN

69100 - 18910 99974 99999

æ

1		4.9	24 rd	134			ŕ
- 010	100000	9590	9594	logy		1	
	200000	18002					
	500000	20014					
	100000	41552	Lunc.				
	600000	agut	41590.9	41000,4	22	39.9	- 1
	7	49111		19172.8 1	-37.8		
	8 20000	12000		50044.7	74 9		
	A	00401		712 621	10.5		
	1000000	75400	++6+2 +	70 600 6	125.64	1747	
	1100000	85708	100/2.1	10021.7	Tos.	1	<b>T</b> .
	12 00000	01001		434465	100.5		
	13 00000	0 0000		1			
	14 00000	107081				-	
1	1800000	11 4100	11112740	114263.1	150 1 1	140	4
	1600000	121080		121278.0	104.9		
	1700000	128002					
1	10 00000	135023					1
0	1900000	141978					
	20 00000	14 8880	144233.0	14.9054.833	170.8	349.0	+
	2100000	153764		13593 5.613	177.6	<i>v</i> .	
	2200000	162611		162793.905	178.9		
	2500000	169460		169630 \$82	166.9		
	24 00000	176247		176447.588	196.6		
	25 00000	183013	183495.1	183244.981	228.0	47811	4
	2600000	189817		190023.944	202,9		
	2700000	196579		196785.271	202,3		
	2800000	203293		203529.70	- 2327		
	2900000	210037		210257.92	2 1169		-
	3000000	216742	217308.5	216970,56	6 2246	562,5	+1

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

## B. Riemann 1849



< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

$$\zeta(s) := 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{n^s} + \dots = \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

Analytic properties of this function carry information about the distribution of primes.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 >

$$\zeta(s) := 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{n^s} + \dots = \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

Analytic properties of this function carry information about the distribution of primes.

#### **Riemann Conjecture**

All nontrivial zeroes of this function have real part  $\Re(s) = 1/2$ .

• • = • • = •

### Manuscript by B. Riemann

Men des Angest des Pringelles ander aren gigition grines ( Bulson donated miche, 18 59 , Non and t) Anon Deres fir der Angelatung, wilde une der her dennes deard des Aufralme under des Conseponsthe same had you That and a laren, glande out and bedan deduces go exerning aget a dans us mades had and establemen Extent was hald god get read markendered Tothe day ever beleventing the do the formet der Prinzelle; an Jeger hand, willter deres ber 1/ Amere, adden Games and Divicelas demulta langers fit governed lab, one exchan chitteen Eng viale nes mill go again and is a metaint Building Later quanter death and als danger of points JI 1 = 2 1 ment for po alle Promyalles, for malle garage fallquerty and Don Fared on der & mylener kartater later &, well devel dens hat a during a large An anany my bergestells and by an ist durch 2(0). Bern any in may a bay ar well This man a guinerreb. fort; which and man harde on in gills burnder had mender history from Dans According der Guinens 1" - my side - Thean endle mer quinted JI (a.1) . 2(a) - 5 " Routed mer un 200 Filyne J Casta nort & bio + a ponto un frieng that evolved withen die ben he a char miner and in the which you the will dis Franken aster dass July pulgadan no 70 more water to , as any it a we down have gland (1 - The a The) \$ " at the , remegerety , bass or der vielbund ogen Trive toon (-1) - (0-1) b(-1) de , Ly - temes on - x asherbirt when not, Denses firs in regulirax reell wird have

э

## Manuscript by B. Riemann

343.+++24 24 :  $+\frac{1}{16}\frac{1}{1-10}$  $-\frac{3}{5\cdot6} + \frac{9}{2\cdot6\cdot16}$  $-\frac{5}{6\cdot16}$ - 285 + . 71 - 41  $f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{1}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}})} + f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{1}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}})} + f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{1}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}})} + f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}})} + f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}})} + f_{0}^{\mu_{0}} \frac{1}{1(t_{1}^{\mu_{0}} t_{1}^{\mu_{0}} t_{1}^{\mu_{0}}$  $+\frac{1}{2}\left(\int_{0}^{0}\frac{1}{n^{2}}\frac{1}{n^{2}}\partial_{n}h^{2}h^{2}+\int_{0}^{0}\frac{1}{n^{2}}\frac{1}{n^{2}}\frac{1}{n^{2}}+\int_{0}^{0}\frac{1}{n^{2}}\frac{1}{n^{2}}+\int_{0}^{0}\frac{n}{n^{2}}\frac{1}{n^{2}}h^{2}h^{2}h^{2}\right)$ 1 - H. 1. C.7 41 12.6 - +++6 /\*\* - 191 3067 1936  $\begin{array}{c} 4^{1}_{1} \pm^{3}_{1,6} \\ 3^{1}_{1,7} \\ a_{1,7} \\ a$ And the set of the set + 1.11 mg  $-\frac{11.13}{1.1^3}$   $-\frac{11.13}{1.1^3}$  $= \frac{a_{1}(5) + 5}{(a_{1}(1)^{2})^{2} a_{1}(1)^{2}} \left| \frac{a_{1}(2, 6, a_{2}) + \frac{a_{1}(5, 1)}{12} \frac{a_{1}(1)}{2} + (b_{1})(1, 5) + 50}{a_{2}(1, 2)^{2} \frac{b_{1}(1, 2)}{2} \frac{b_{$ 17 Ban-13h+6 (IA-601-4) (8-5)-12 +(0-1)(0-1)(5+(0-1))19 +10  $\frac{e^{2N}}{(n+1)^2} = \frac{2N+1}{(n+1)^2} \frac{2^{N+1}}{4(n+1)^2} + \frac{(n+1)^2}{(n+1)^2} \frac{($ 1-++++++ for fair a fair and and a fair and a fair and and and a fair a fai 21-1 (A(1-1)+5-4 + ( ") (1+6) 1+4 5617,144

$$\pi(x) := \{p \le x\} \sim \frac{x}{\log(x)}, \quad x \to \infty$$

- Gauss conjecture
- Riemann's approach via the zeta function
- Hadamard, de la Vallee-Poussin
- Selberg "elementary" proof

(B)

Proof of  $\gg$ 

$$\nu_p(n) := p$$
-power dividing  $n$ 

2

イロト イヨト イヨト イヨト

Proof of  $\gg$ 

 $\nu_p(n) := p$ -power dividing n

$$\nu_p(n!) = \sum_{k \ge 1} \left[ \frac{n}{p^k} \right]$$

イロト イポト イヨト イヨト 二日

#### Proof of $\gg$

 $u_p(n) := p$ -power dividing n  $u_p(n!) = \sum_{k>1} \left[ \frac{n}{p^k} \right]$ 

Apply to

$$N = \binom{2m}{m} = \frac{(2m)!}{(m!)^2}$$
$$\nu_p(N) = \sum_{k \ge 1} \left[\frac{2m}{p^k}\right] - 2\left[\frac{m}{p^k}\right]$$

3

イロト イヨト イヨト イヨト

$$N=(\frac{m+1}{1})(\frac{m+2}{2})\cdots(\frac{m+m}{m})$$

Thus

$$N \geq 2^m$$
,  $p \mid N \Rightarrow p \leq 2m$ .

The summand in  $\nu_p(N)$  vanishes if  $k > \frac{\log(2m)}{\log(p)}$ , and is at most 1, in other cases. It follows that

$$u_p(N) \leq rac{\log(2m)}{\log(p)}$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

We find

$$\pi(2m)\log(2m) = \sum_{p \leq 2m} \frac{\log(2m)}{\log(p)} \cdot \log(p)$$

$$\geq \sum_{p\leq 2m} 
u_p(N) \cdot \log(p) = \log(N)$$

$$\geq m \log(2)$$

Thus

$$\pi(2m) \geq \frac{1}{2}\log(2)\frac{2m}{\log(2m)}$$

3

イロト イヨト イヨト イヨト
#### Primes in arithmetic progressions

$$(a, m) = 1 \quad \Rightarrow$$
  
 $\#\{p \equiv a \pmod{m}, p \leq x\} \sim \frac{1}{\varphi(m)} \frac{x}{\log(x)}$ 

æ

イロン イ理 とく ヨン イ ヨン

#### Primes in arithmetic progressions

E.g.

$$(a, m) = 1 \quad \Rightarrow$$
  
 $\#\{p \equiv a \pmod{m}, p \leq x\} \sim \frac{1}{\varphi(m)} \frac{x}{\log(x)}$   
 $q \mid (\prod p_j)^2 + 1 \Rightarrow q \equiv 1 \pmod{4}$ 

æ

イロン イ理 とく ヨン イ ヨン

#### Theorems of Green-Tao

- 2
- 2,3
- 3,5,7
- 5,11,17,23
- 5,11,17,23,29

3

イロト イボト イヨト イヨト

#### Theorems of Green-Tao

- 2
- 2,3
- 3,5,7
- 5,11,17,23
- 5,11,17,23,29
- no infinitely long arithmetic progressions in primes (trivial)
- van der Corput 1939: ∃ infinitely many arithmetic progressions of length 3 in primes
- Green-Tao 2004: there exist arbitrarily long arithmetic progressions in primes
- Tao-Ziegler 2006: P<sub>1</sub>,..., P<sub>k</sub> ∈ ℤ[x], P<sub>j</sub>(0) = 0, ⇒ Π ⊃ infinitely many progressions of the form

$$n + P_1(r), \ldots, n + P_k(r)$$

< 回 > < 三 > < 三 > -

 Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes.

э

(4 回 ) (4 回 ) (4 回 )

 Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)

▲ □ ▶ ▲ □ ▶ ▲ □ ▶

- Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)
- Are there infinitely many prime twins: 11, 13 or 17, 19, ... ?

. . . . . . . .

- Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)
- Are there infinitely many prime twins: 11, 13 or 17, 19, ... ? Recently proved that there are infinitely many pairs of primes p, q such that p − q ≤ 246 (after Yitang Zhang 2013 + Polymath)

. . . . . . . .

- Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)
- Are there infinitely many prime twins: 11, 13 or 17, 19, ... ? Recently proved that there are infinitely many pairs of primes p, q such that  $p - q \le 246$  (after Yitang Zhang 2013 + Polymath)

• 
$$p = n^2 + 1?$$

. . . . . . . .

- Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)
- Are there infinitely many prime twins: 11, 13 or 17, 19, ... ? Recently proved that there are infinitely many pairs of primes p, q such that  $p - q \le 246$  (after Yitang Zhang 2013 + Polymath)

• 
$$p = n^2 + 1?$$

• p = f(n),  $f \in \mathbb{Z}[x]$ , unitary, irreducible, coprime coefficients

イロト イヨト イヨト ・

- Goldbach conjecture (1742): every even number ≥ 4 is a sum of two primes. Recently solved: every odd number ≥ 7 is a sum of three primes (Helfgott 2013)
- Are there infinitely many prime twins: 11, 13 or 17, 19, ... ? Recently proved that there are infinitely many pairs of primes p, q such that  $p - q \le 246$  (after Yitang Zhang 2013 + Polymath)
- $p = n^2 + 1?$
- p = f(n),  $f \in \mathbb{Z}[x]$ , unitary, irreducible, coprime coefficients
- Schinzel's hypothesis = same for systems of equations  $f_1, \ldots, f_r \in \mathbb{Z}[x] \ldots \Rightarrow \exists \infty$ -many  $n \mid f_j(n) = p_j$  e.g.,  $x, x + 2 \ldots$