Compter les nombres premiers... jusqu'au chaos quantique

Lycée Blaise Pascal

Emmanuel Royer

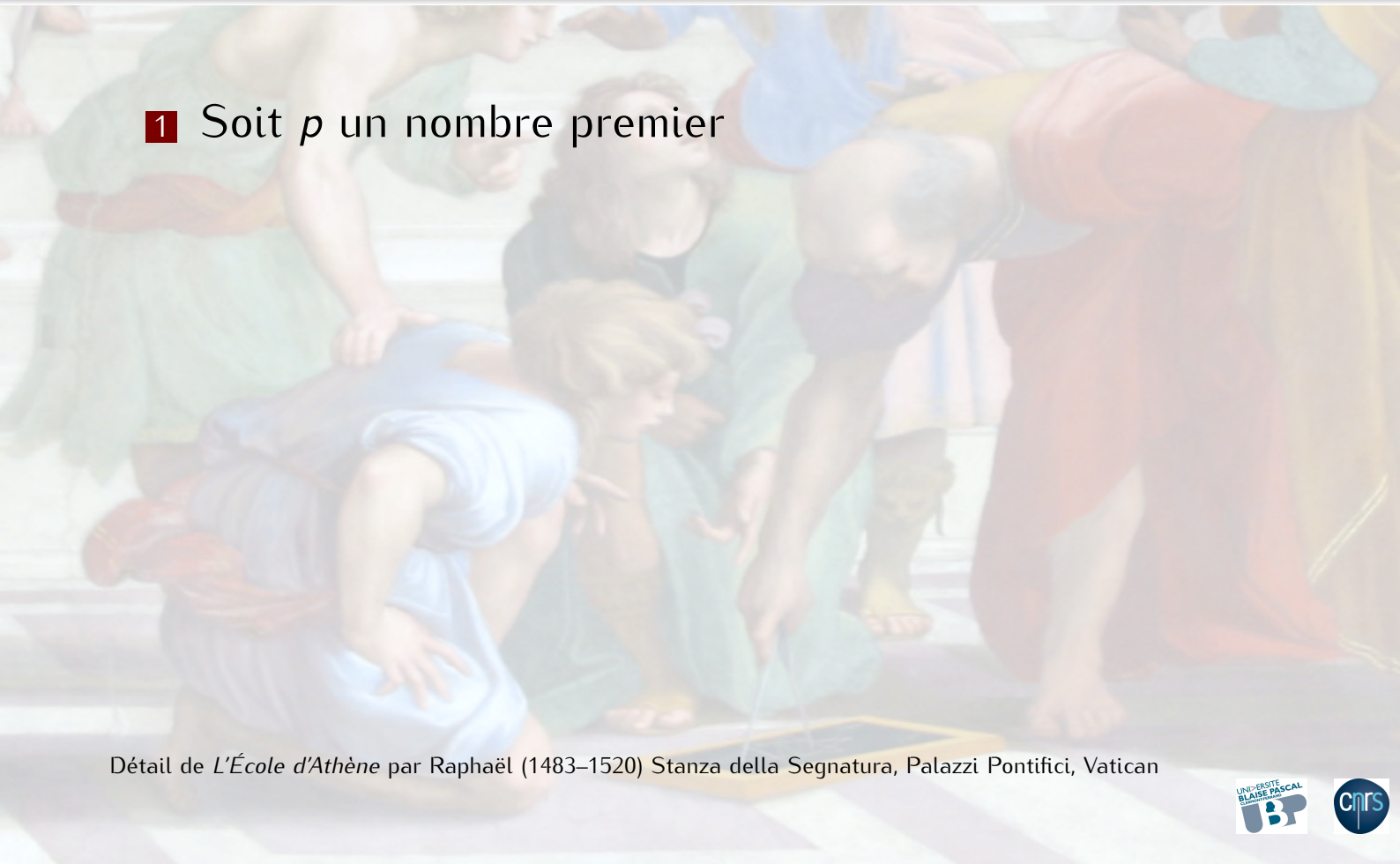
Laboratoire de mathématiques
UMR 6620
Université Blaise Pascal
Clermont-Ferrand

6 février 2013

Une infinité de nombres premiers

La preuve d'Euclide (−325 −265)

1. Soit p un nombre premier

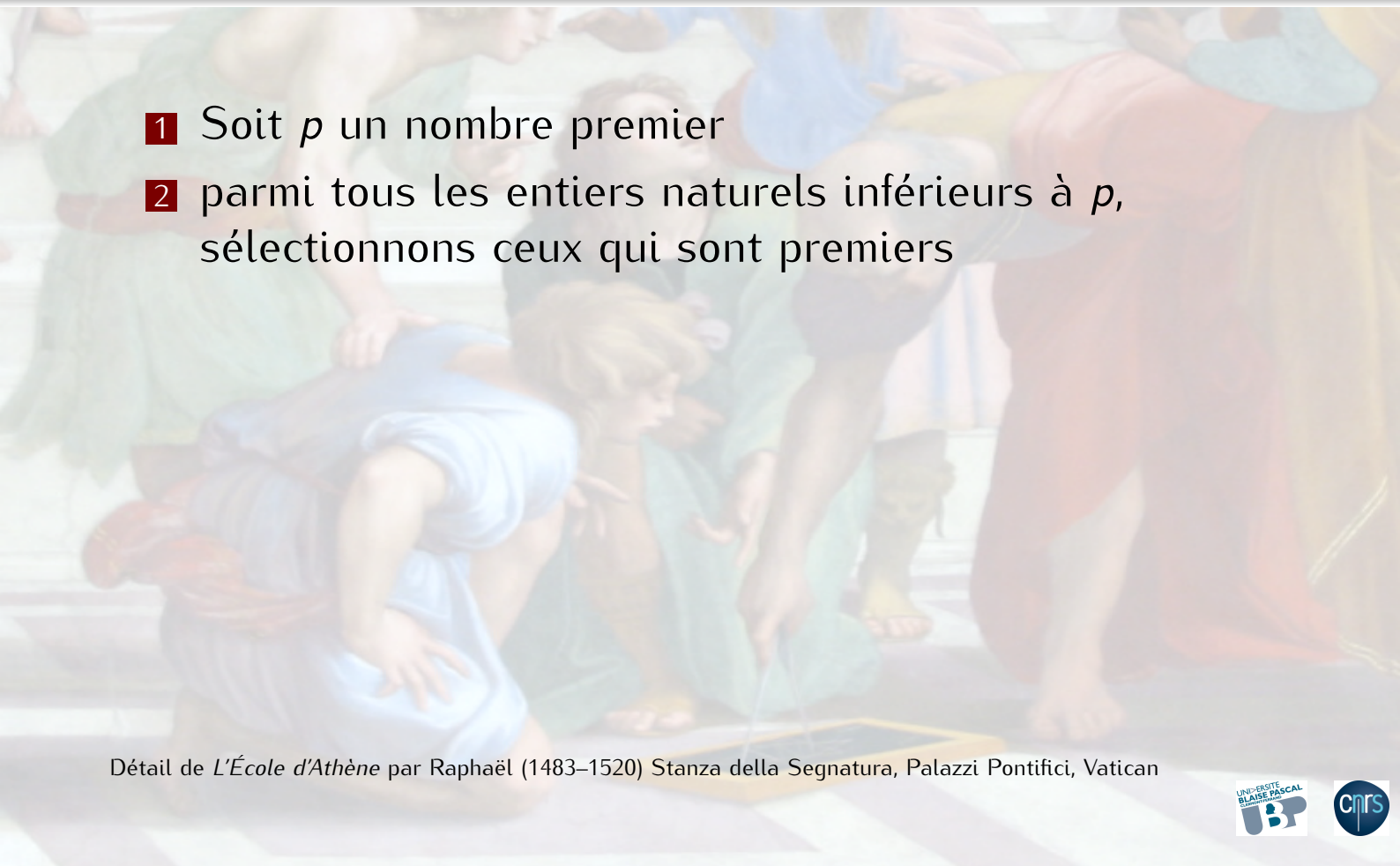


Détail de *L'École d'Athène* par Raphaël (1483–1520) Stanza della Segnatura, Palazzi Pontifici, Vatican

Une infinité de nombres premiers

La preuve d'Euclide (−325 −265)

1. Soit p un nombre premier
2. parmi tous les entiers naturels inférieurs à p, sélectionnons ceux qui sont premiers



Détail de *L'École d'Athène* par Raphaël (1483–1520) Stanza della Segnatura, Palazzi Pontifici, Vatican

Une infinité de nombres premiers

La preuve d'Euclide (−325 −265)

1. Soit p un nombre premier
2. parmi tous les entiers naturels inférieurs à p, sélectionnons ceux qui sont premiers
3. on en fait le produit et on ajoute un

Détail de *L'École d'Athène* par Raphaël (1483–1520) Stanza della Segnatura, Palazzi Pontifici, Vatican

Une infinité de nombres premiers

La preuve d'Euclide (−325 −265)

1. Soit p un nombre premier
2. parmi tous les entiers naturels inférieurs à p, sélectionnons ceux qui sont premiers
3. on en fait le produit et on ajoute un
   - soit le nombre obtenu est premier : on obtient un nombre premier strictement supérieur à p

Détail de *L'École d'Athène* par Raphaël (1483–1520) Stanza della Segnatura, Palazzi Pontifici, Vatican

Une infinité de nombres premiers

La preuve d'Euclide (−325 −265)

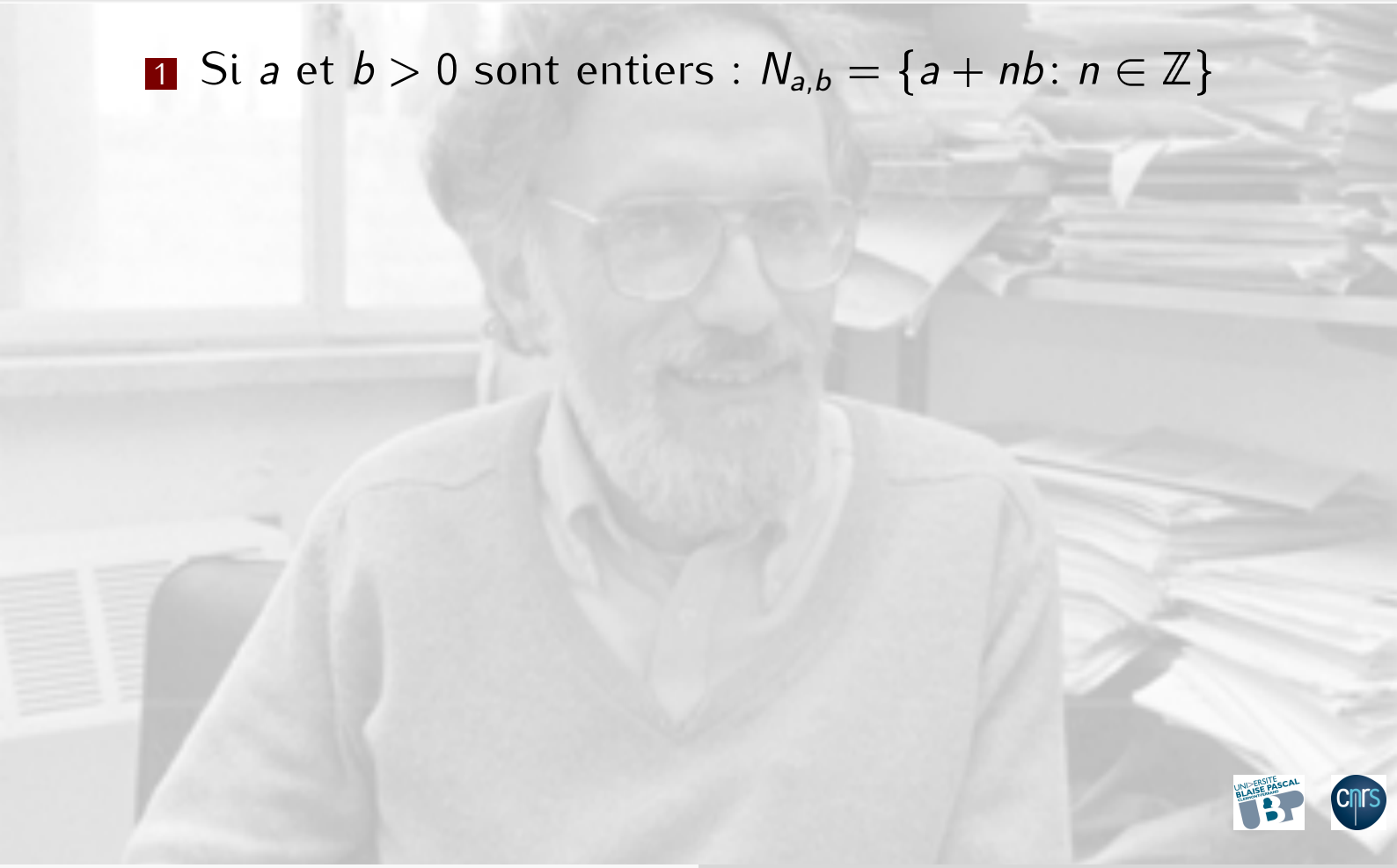
1. Soit p un nombre premier
2. parmi tous les entiers naturels inférieurs à p, sélectionnons ceux qui sont premiers
3. on en fait le produit et on ajoute un
   - soit le nombre obtenu est premier : on obtient un nombre premier strictement supérieur à p
   - soit le nombre premier obtenu n'est pas premier, il est alors divisible par un nombre premier qui ne peut pas être inférieur à p : on obtient un nombre premier strictement supérieur à p.

Détail de *L'École d'Athène* par Raphaël (1483–1520) Stanza della Segnatura, Palazzi Pontifici, Vatican

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Si a et $b > 0$ sont entiers : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$



Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Si a et $b > 0$ sont entiers : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. Topologie sur $\mathbb{Z}$: $\mathcal{O}$ est ouvert si $\mathcal{O} = \emptyset$ ou si

$$\forall a \in \mathcal{O}\,, \exists b > 0 : N_{a,b} \in \mathcal{O}$$

(un ouvert non vide est donc infini)

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Si a et $b > 0$ sont entiers : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. Topologie sur $\mathbb{Z}$: $\mathcal{O}$ est ouvert si $\mathcal{O} = \emptyset$ ou si

$$\forall a \in \mathcal{O}\,, \exists b > 0 : N_{a,b} \in \mathcal{O}$$

(un ouvert non vide est donc infini)

- une réunion quelconque d'ouverts est un ouvert

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Si a et $b > 0$ sont entiers : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. Topologie sur $\mathbb{Z}$: $\mathcal{O}$ est ouvert si $\mathcal{O} = \emptyset$ ou si

$$\forall a \in \mathcal{O}\,, \exists b > 0 : N_{a,b} \in \mathcal{O}$$

(un ouvert non vide est donc infini)

- une réunion quelconque d'ouverts est un ouvert
- si $\mathcal{O}_1$ et $\mathcal{O}_2$ sont ouverts, soit $a \in \mathcal{O}_1 \cap \mathcal{O}_2$ alors $N_{a,b_1} \subset \mathcal{O}_1$ et $N_{a,b_2} \subset \mathcal{O}_2$ donc $N_{a,b_1 b_2} \subset \mathcal{O}_1 \cap \mathcal{O}_2$.

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Si a et $b > 0$ sont entiers : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. Topologie sur $\mathbb{Z}$: $\mathcal{O}$ est ouvert si $\mathcal{O} = \emptyset$ ou si

$$\forall a \in \mathcal{O}\,, \exists b > 0 : N_{a,b} \in \mathcal{O}$$

(un ouvert non vide est donc infini)

- une réunion quelconque d'ouverts est un ouvert
- si $\mathcal{O}_1$ et $\mathcal{O}_2$ sont ouverts, soit $a \in \mathcal{O}_1 \cap \mathcal{O}_2$ alors $N_{a,b_1} \subset \mathcal{O}_1$ et $N_{a,b_2} \subset \mathcal{O}_2$ donc $N_{a,b_1 b_2} \subset \mathcal{O}_1 \cap \mathcal{O}_2$.

3. $N_{a,b}$ est fermé (et ouvert !) :

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

4 Tout nombre premier différent de -1 ou 1 admet un diviseur premier :

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}.$$

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

4. Tout nombre premier différent de -1 ou 1 admet un diviseur premier :

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}.$$

5. Si $\mathcal{P}$ est fini alors

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

4. Tout nombre premier différent de -1 ou 1 admet un diviseur premier :

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}.$$

5. Si $\mathcal{P}$ est fini alors
   - $\mathbb{Z} \setminus \{-1, 1\}$ est fermé

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

4. Tout nombre premier différent de -1 ou 1 admet un diviseur premier :

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}.$$

5. Si $\mathcal{P}$ est fini alors
   - $\mathbb{Z} \setminus \{-1, 1\}$ est fermé
   - donc $\{-1, 1\}$ est ouvert

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

4. Tout nombre premier différent de -1 ou 1 admet un diviseur premier :

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}.$$

5. Si $\mathcal{P}$ est fini alors
   - $\mathbb{Z} \setminus \{-1, 1\}$ est fermé
   - donc $\{-1, 1\}$ est ouvert
   - or, $\{-1, 1\}$ n'est ni vide ni infini.

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

ON THE INFINITUDE OF PRIMES

HARRY FURSTENBERG, Yeshiva University

In this note we would like to offer an elementary "topological" proof of the infinitude of the prime numbers. We introduce a topology into the space of integers S, by using the arithmetic progressions (from $-\infty$ to $+\infty$) as a basis. It is not difficult to verify that this actually yields a topological space. In fact, under this topology, S may be shown to be normal and hence metrizable. Each arithmetic progression is closed as well as open, since its complement is the union of other arithmetic progressions (having the same difference). As a result, the union of any finite number of arithmetic progressions is closed. Consider now the set $A = \bigcup A_p$, where A_p consists of all multiples of p, and p runs through the set of primes $\geqq 2$. The only numbers not belonging to A are -1 and 1, and since the set $\{-1, 1\}$ is clearly not an open set, A cannot be closed. Hence A is not a finite union of closed sets which proves that there are an infinity of primes.

Harry Furstenberg, The American Mathematical Monthly, Vol. 62, No. 5 (May, 1955), p. 353.

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

1. Dans le développement du produit

$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$

il y a tous les entiers de la forme $\dfrac{1}{p_1^{v_1}\cdots p_\omega^{v_\omega}}$ où $p_1,\ldots,p_\omega$ sont premiers inférieurs à N et $v_1,\ldots,v_\omega$ sont entiers naturels.

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

1. Dans le développement du produit

$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}} \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$

il y a tous les entiers de la forme $\dfrac{1}{p_1^{v_1}\cdots p_\omega^{v_\omega}}$ où $p_1,\ldots,p_\omega$ sont premiers inférieurs à N et $v_1,\ldots,v_\omega$ sont entiers naturels.

2. Réciproquement, tout tel entier, et en particulier tout entier inférieur à N s'y retrouve.

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

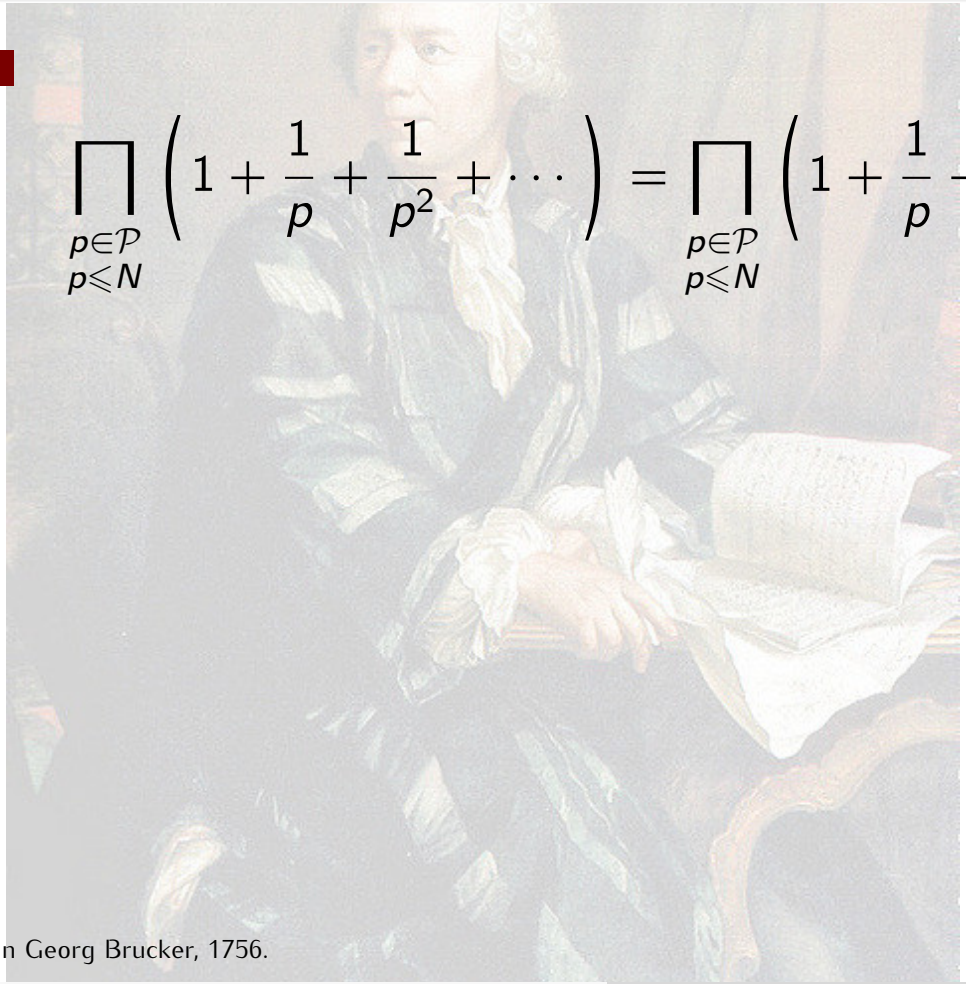
1. Dans le développement du produit
$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$
il y a tous les entiers de la forme $\dfrac{1}{p_1^{v_1}\cdots p_\omega^{v_\omega}}$ où $p_1,\ldots,p_\omega$ sont premiers inférieurs à N et $v_1,\ldots,v_\omega$ sont entiers naturels.
2. Réciproquement, tout tel entier, et en particulier tout entier inférieur à N s'y retrouve.
3. $$\sum_{n=1}^{N}\frac{1}{n}\leqslant\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right).$$

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

1

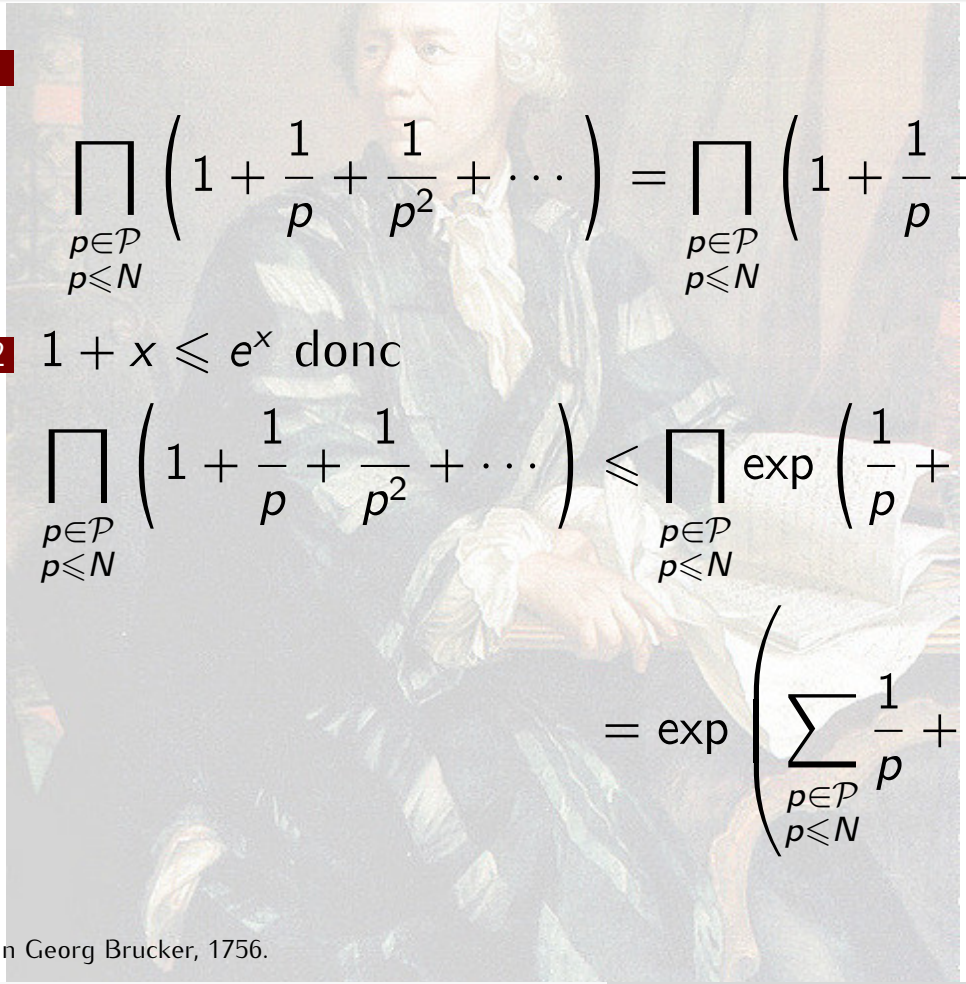
$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p(p-1)}\right).$$



Johann Georg Brucker, 1756.

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)



1

$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p(p-1)}\right).$$

2 $1+x\leqslant e^x$ donc

$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\leqslant\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\exp\left(\frac{1}{p}+\frac{1}{p(p-1)}\right)$$

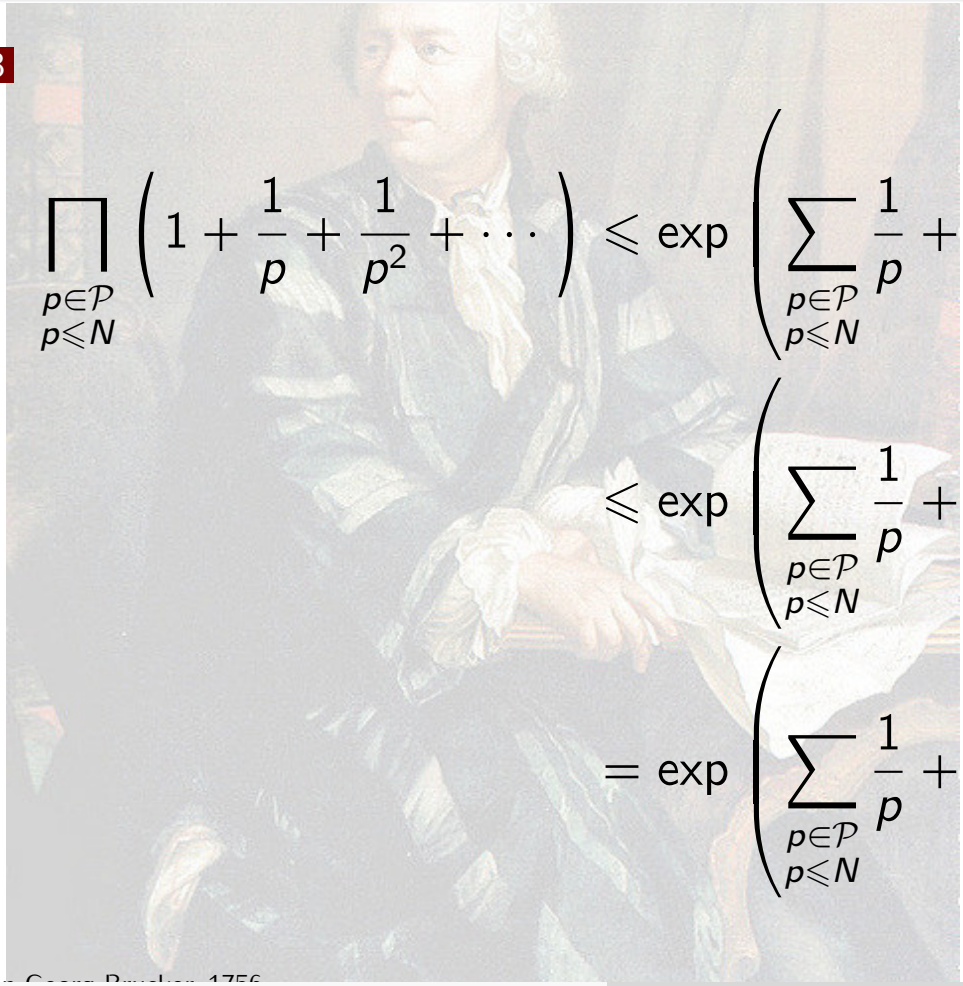
$$=\exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p(p-1)}\right)$$

Johann Georg Brucker, 1756.

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

3



$$\prod_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p(p-1)}\right)$$

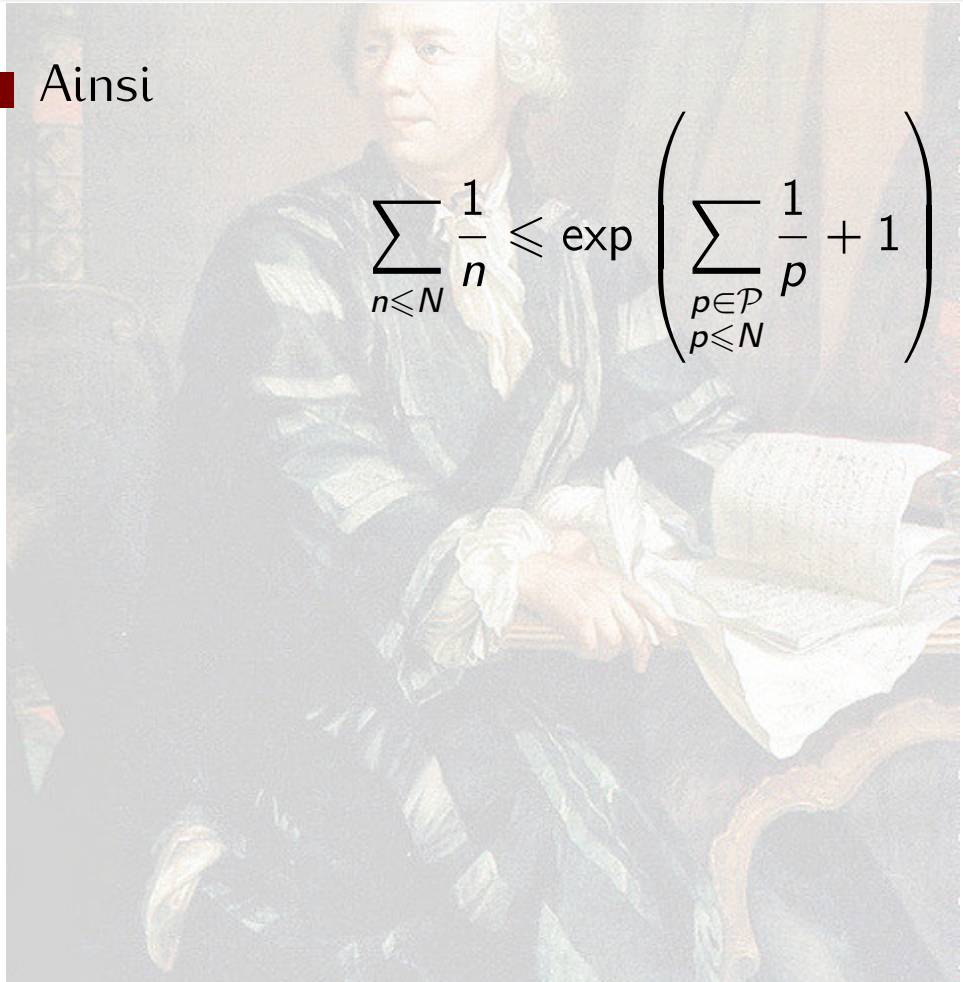
$$\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+\sum_{n\geqslant 2}\frac{1}{n(n-1)}\right)$$

$$= \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+1\right)$$

Johann Georg Brucker, 1756

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)

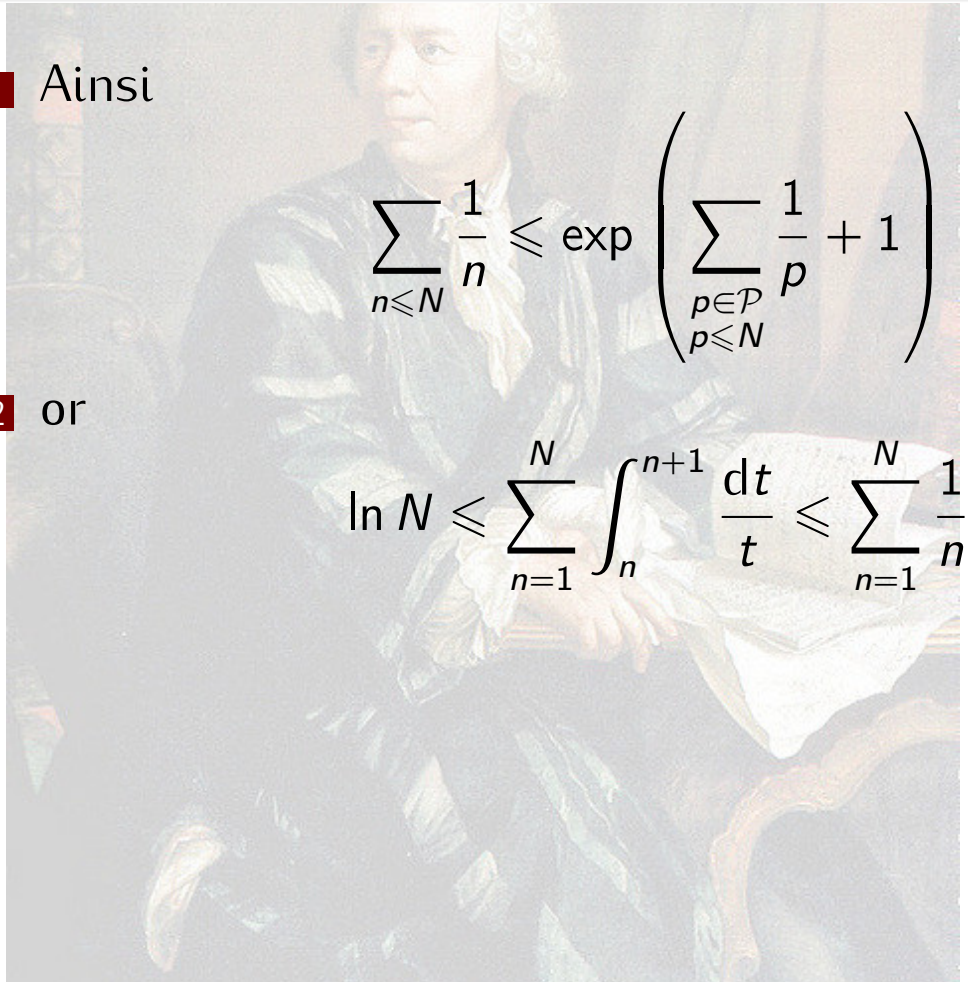


1. Ainsi

$$\sum_{n\leqslant N}\frac{1}{n}\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+1\right)$$

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)



1. Ainsi

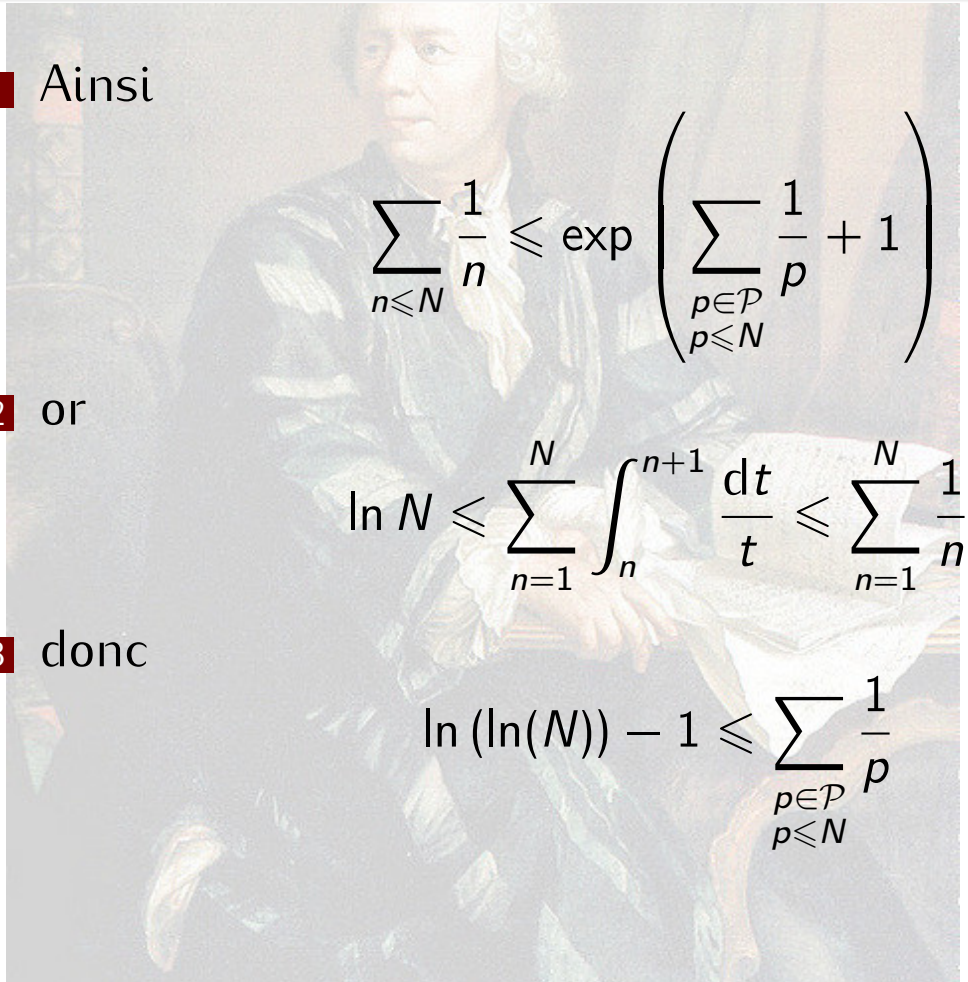
$$\sum_{n\leqslant N}\frac{1}{n}\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+1\right)$$

2. or

$$\ln N\leqslant \sum_{n=1}^{N}\int_{n}^{n+1}\frac{\mathrm{d}t}{t}\leqslant \sum_{n=1}^{N}\frac{1}{n}$$

Une infinité de nombres premiers

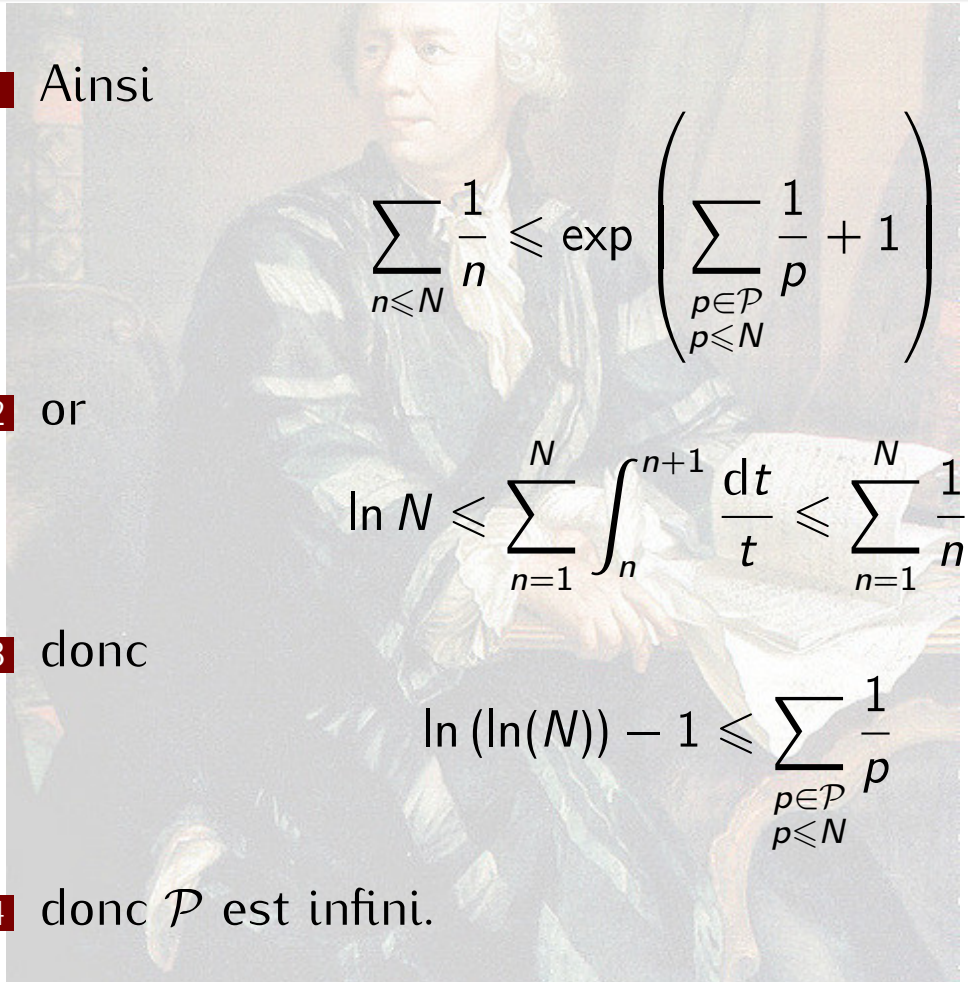
Une preuve analytique (Euler 1707–1783)



1. Ainsi
$$\sum_{n\leqslant N}\frac{1}{n}\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+1\right)$$
2. or
$$\ln N\leqslant \sum_{n=1}^{N}\int_{n}^{n+1}\frac{\mathrm{d}t}{t}\leqslant \sum_{n=1}^{N}\frac{1}{n}$$
3. donc
$$\ln\left(\ln(N)\right)-1\leqslant \sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}$$

Une infinité de nombres premiers

Une preuve analytique (Euler 1707–1783)



1. Ainsi
$$\sum_{n\leqslant N}\frac{1}{n}\leqslant \exp\left(\sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}+1\right)$$
2. or
$$\ln N\leqslant \sum_{n=1}^{N}\int_{n}^{n+1}\frac{\mathrm{d}t}{t}\leqslant \sum_{n=1}^{N}\frac{1}{n}$$
3. donc
$$\ln\left(\ln(N)\right)-1\leqslant \sum_{\substack{p\in\mathcal{P}\\ p\leqslant N}}\frac{1}{p}$$
4. donc $\mathcal{P}$ est infini.

Compter les nombres premiers

La fonction de comptage

Si $x \geqslant 2$ est réel, on note $\pi(x) = \#\{p \in \mathcal{P} : p \leqslant x\}$.

Compter les nombres premiers

La fonction de comptage

Si $x \geqslant 2$ est réel, on note $\pi(x) = \#\{p \in \mathcal{P} : p \leqslant x\}$. De

$$\ln(\ln(N)) - 1 \leqslant \sum_{\substack{p \in \mathcal{P} \\ p \leqslant N}} \frac{1}{p}$$

on déduit

$$\pi(x) \geqslant 2 \ln(\ln\lfloor x \rfloor) - 2.$$

Compter les nombres premiers

La fonction de comptage

Si $x \geqslant 2$ est réel, on note $\pi(x) = \#\{p \in \mathcal{P} : p \leqslant x\}$. De

$$\ln(\ln(N)) - 1 \leqslant \sum_{\substack{p \in \mathcal{P} \\ p \leqslant N}} \frac{1}{p}$$

on déduit

$$\pi(x) \geqslant 2 \ln(\ln\lfloor x \rfloor) - 2.$$

Comment être plus précis ?

Compter les nombres premiers

Un peu d'expérimentation

N	$\pi(N)$
10	4
10^2	25
10^3	168
10^4	1 229
10^5	9 592
10^6	78 498
10^7	664 579
10^8	5 761 455
10^9	50 847 534
10^{10}	455 052 511

```
sequoia~>sage
--------------------------------------------------------------------------------
| Sage Version 5.2, Release Date: 2012-07-25                                   |
| Type "notebook()" for the browser-based notebook interface.                  |
| Type "help()" for help.                                                      |
--------------------------------------------------------------------------------
sage: time P=prime_range(10^10)
Time: CPU 60.31 s, Wall: 60.37 s
sage:
```

Compter les nombres premiers

Un peu d'expérimentation

N	$\pi(N)$	$N/\pi(N)$
10	4	2,5
10^2	25	4
10^3	168	5,95
10^4	1 229	8,13
10^5	9 592	10,42
10^6	78 498	12,73
10^7	664 579	15,04
10^8	5 761 455	17,35
10^9	50 847 534	19,66
10^{10}	455 052 511	21,97

```
sequoia~>sage
--------------------------------------------------------------------------------
| Sage Version 5.2, Release Date: 2012-07-25                                   |
| Type "notebook()" for the browser-based notebook interface.                  |
| Type "help()" for help.                                                      |
--------------------------------------------------------------------------------
sage: time P=prime_range(10^10)
Time: CPU 60.31 s, Wall: 60.37 s
sage:
```

Compter les nombres premiers

Un peu d'expérimentation

N	$\pi(N)$	$N/\pi(N)$	Écarts
10	4	2,5	
10^2	25	4	1,50
10^3	168	5,95	1,95
10^4	1 229	8,13	2,18
10^5	9 592	10,42	2,28
10^6	78 498	12,73	2,31
10^7	664 579	15,04	2,30
10^8	5 761 455	17,35	2,30
10^9	50 847 534	19,66	2,30
10^{10}	455 052 511	21,97	2,30

```
sequoia~>sage
--------------------------------------------------------------------
| Sage Version 5.2, Release Date: 2012-07-25                       |
| Type "notebook()" for the browser-based notebook interface.      |
| Type "help()" for help.                                          |
--------------------------------------------------------------------
sage: time P=prime_range(10^10)
Time: CPU 60.31 s, Wall: 60.37 s
sage:
```

Compter les nombres premiers

Un peu d'expérimentation

Notons

$$P(x) = \frac{\pi(x)}{x}.$$

Lorsque x devient grand, il semble donc que

$$\frac{1}{P}(10x) - \frac{1}{P}(x) = 2{,}3\ldots$$

Compter les nombres premiers

Un peu d'expérimentation

Notons

$$P(x) = \frac{\pi(x)}{x}.$$

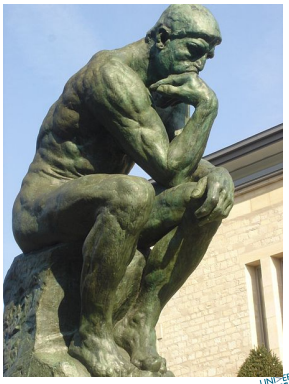
Lorsque x devient grand, il semble donc que

$$\frac{1}{P}(10x) - \frac{1}{P}(x) = 2{,}3\ldots$$

Connaissez-vous une fonction f vérifiant

$$f(10x) - f(x) = 2{,}3\ldots$$

pour tout $x > 0$?



Rodin, Le penseur.
Musée Rodin, Paris.

Compter les nombres premiers

Un peu d'expérimentation

Notons

$$P(x) = \frac{\pi(x)}{x}.$$

Lorsque x devient grand, il semble donc que

$$\frac{1}{P}(10x) - \frac{1}{P}(x) = 2{,}3\ldots$$

Connaissez-vous une fonction f vérifiant

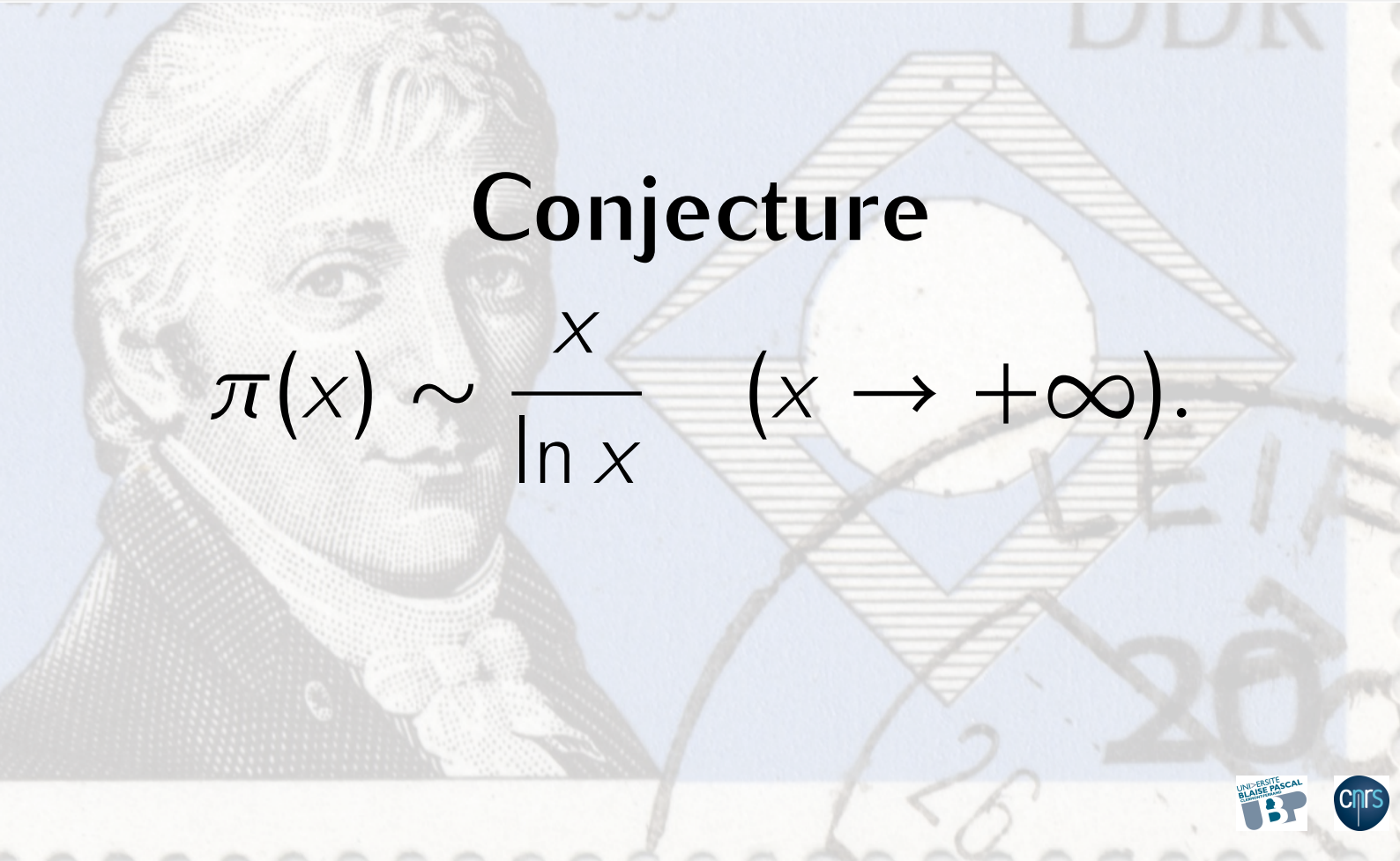
$$f(10x) - f(x) = 2{,}3\ldots$$

pour tout $x > 0$? La fonction ln !

Portrait de Neper.
Université d'Edinburgh

Compter les nombres premiers

Une conjecture du jeune Gauss (1777-1855)



Conjecture

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \to +\infty).$$

Compter les nombres premiers

Une conjecture du jeune Gauss (1777-1855)

Conjecture

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \to +\infty).$$

Gauss avait 15 ans lorsqu'il fit les calculs précédents et devina cette première version du théorème des nombres premiers.

Compter les nombres premiers

Une conjecture du jeune Gauss (1777-1855)

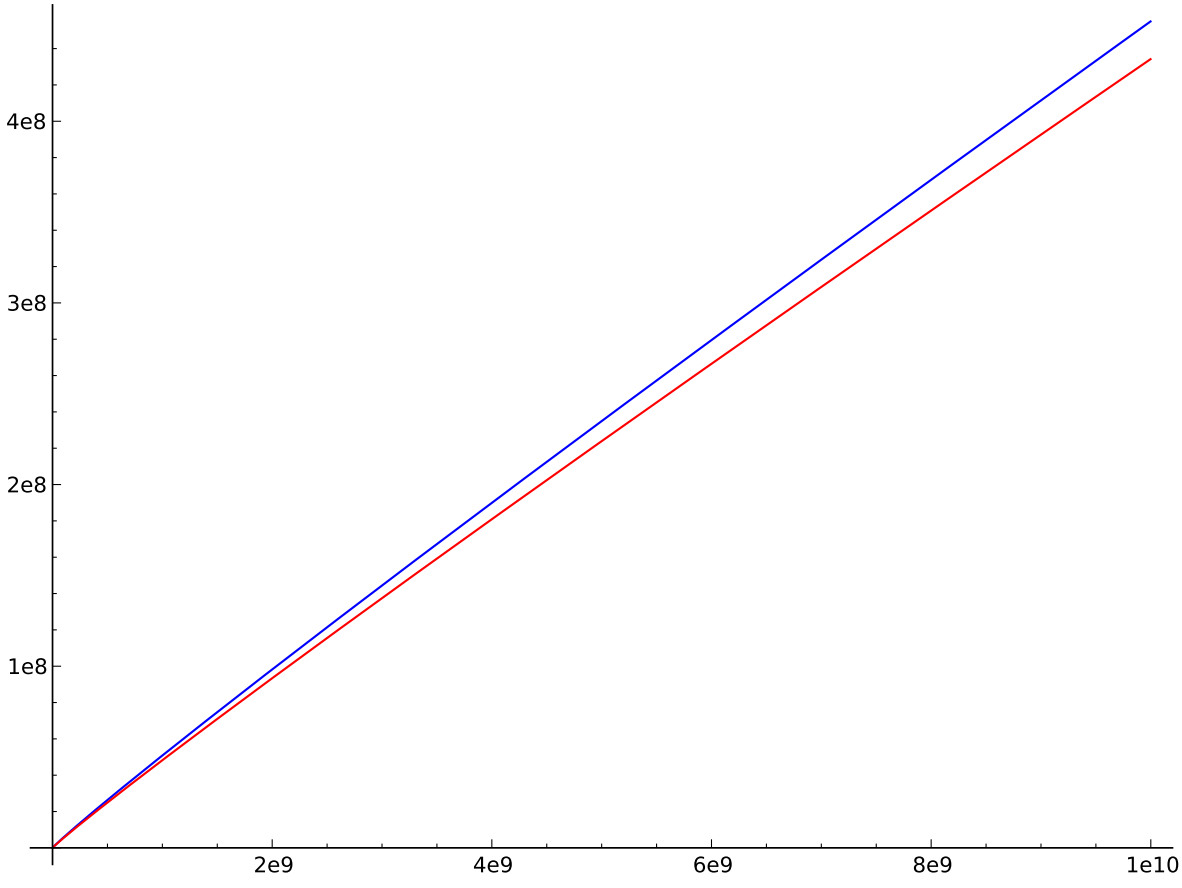
Conjecture

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \to +\infty).$$

Gauss avait 15 ans lorsqu'il fit les calculs précédents et devina cette première version du théorème des nombres premiers. Il n'annonça jamais cette conjecture, n'ayant pas de preuve.

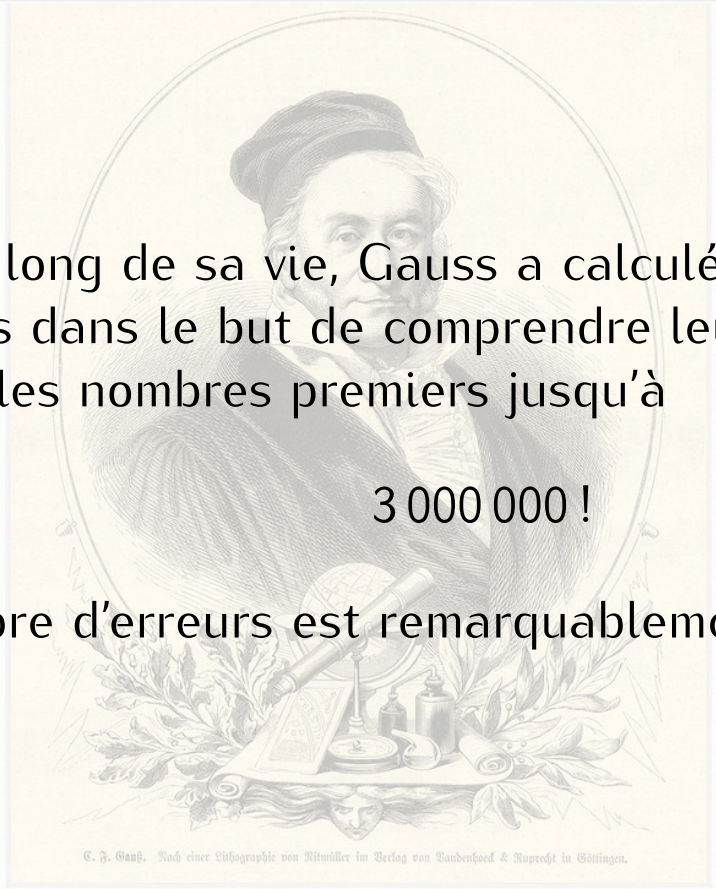
Compter les nombres premiers

Précision de la conjecture du jeune Gauss



Compter les nombres premiers

Une conjecture du vieux Gauss



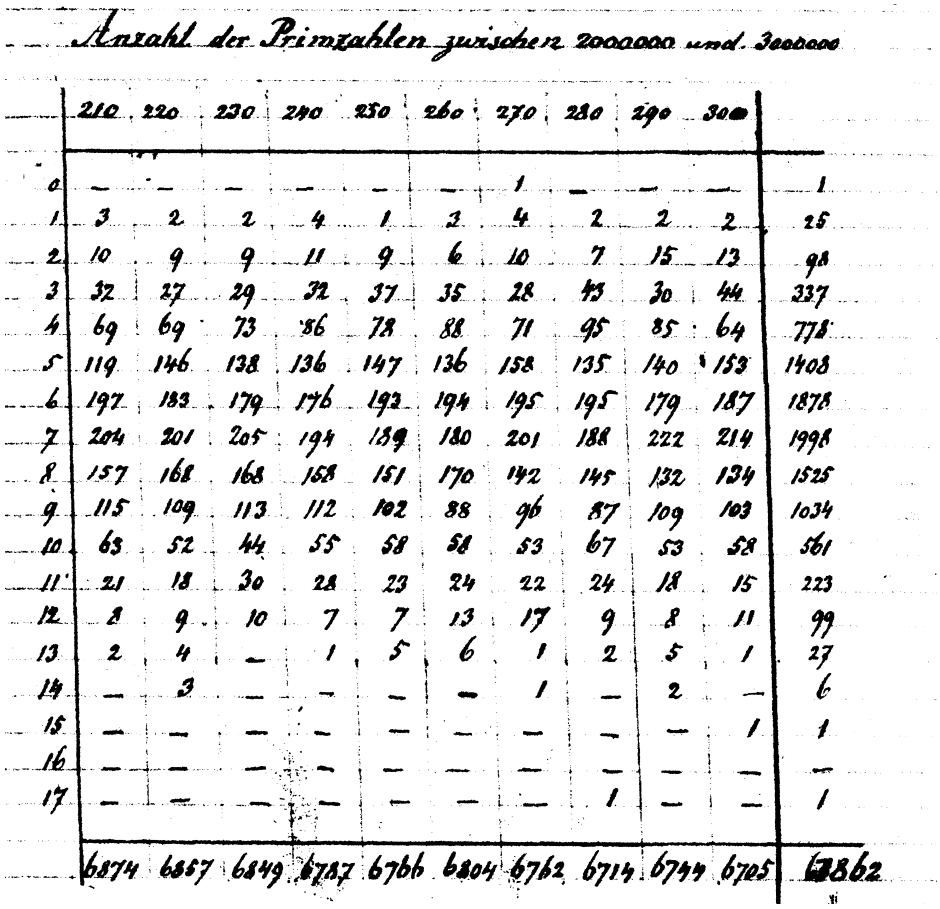
Tout au long de sa vie, Gauss a calculé des nombres premiers dans le but de comprendre leur distribution. Il a compté les nombres premiers jusqu'à

$$3\,000\,000\,!$$

Le nombre d'erreurs est remarquablement faible.

Compter les nombres premiers

Une conjecture du vieux Gauss

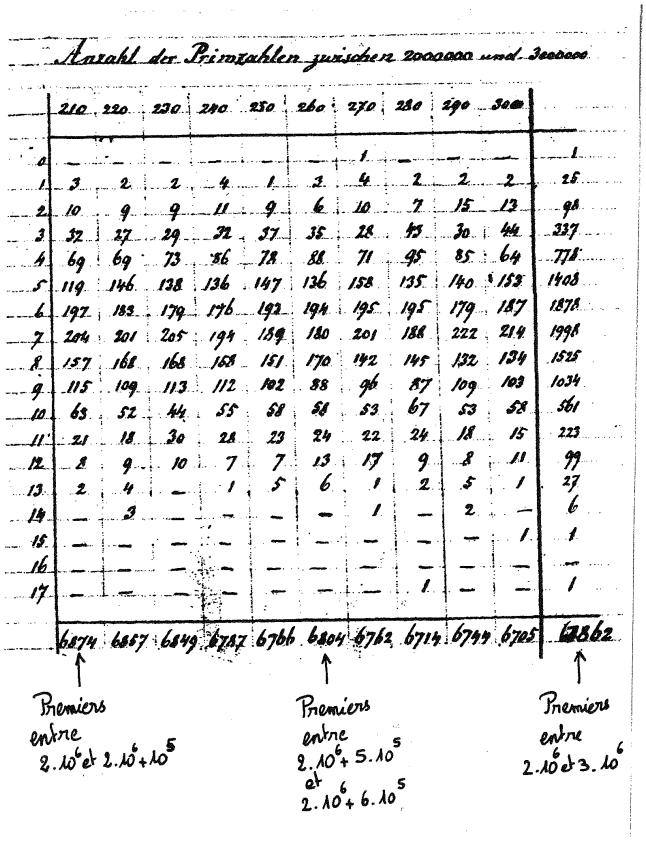


Anzahl der Primzahlen zwischen 2000000 und 3000000

	210	220	230	240	250	260	270	280	290	300	
0	—	—	—	—	—	—	1	—	—	—	1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	11	9	6	10	7	15	13	98
3	32	27	29	32	37	35	28	43	30	44	337
4	69	69	73	86	78	88	71	95	85	64	778
5	119	146	138	136	147	136	158	135	140	153	1408
6	197	183	179	176	192	194	195	195	179	187	1878
7	204	201	205	194	189	180	201	188	222	214	1998
8	157	168	168	158	151	170	142	145	132	134	1525
9	115	109	113	112	102	88	96	87	109	103	1034
10	63	52	44	55	58	58	53	67	53	58	561
11	21	18	30	28	23	24	22	24	18	15	223
12	8	9	10	7	7	13	17	9	8	11	99
13	2	4	—	1	5	6	1	2	5	1	27
14	—	3	—	—	—	—	1	—	2	—	6
15	—	—	—	—	—	—	—	—	—	1	1
16	—	—	—	—	—	—	—	—	—	—	—
17	—	—	—	—	—	—	—	1	—	—	1
	6874	6857	6849	6787	6766	6804	6762	6714	6744	6705	67862

Compter les nombres premiers

Une conjecture du vieux Gauss



Anzahl der Primzahlen zwischen 2000000 und 3000000

	2100	2200	2300	2400	2500	2600	2700	2800	2900	3000	
0	—	—	—	—	—	—	1	—	—	—	1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	11	9	6	10	7	15	12	98
3	32	27	29	32	37	35	28	45	30	44	337
4	69	69	73	56	78	88	71	95	85	64	778
5	119	146	138	136	147	136	158	135	140	153	1408
6	197	183	179	176	192	194	195	195	179	187	1878
7	204	201	205	194	159	180	201	188	222	214	1998
8	157	168	168	158	151	170	142	145	132	134	1525
9	115	109	113	112	102	88	96	87	109	103	1034
10	63	52	44	55	58	58	53	67	53	58	561
11	21	18	30	28	23	24	22	24	18	15	223
12	8	9	10	7	7	13	17	9	8	11	99
13	2	4	—	1	5	6	1	2	5	1	27
14	—	3	—	—	—	—	1	—	2	—	6
15	—	—	—	—	—	—	—	—	—	1	1
16	—	—	—	—	—	—	—	—	—	—	—
17	—	—	—	—	—	—	—	1	—	—	1
	6874	6857	6849	6727	6766	6804	6762	6714	6749	6705	67862

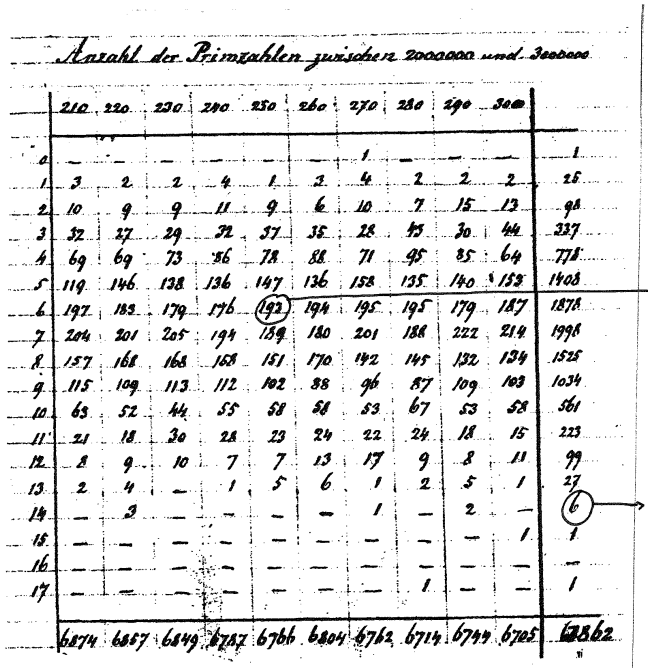
Premiers entre 2.10^6 et 2.10^6+10^5

Premiers entre $2.10^6+5.10^5$ et $2.10^6+6.10^5$

Premiers entre 2.10^6 et 3.10^6

Compter les nombres premiers

Une conjecture du vieux Gauss



Anzahl der Primzahlen zwischen 2000000 und 3000000

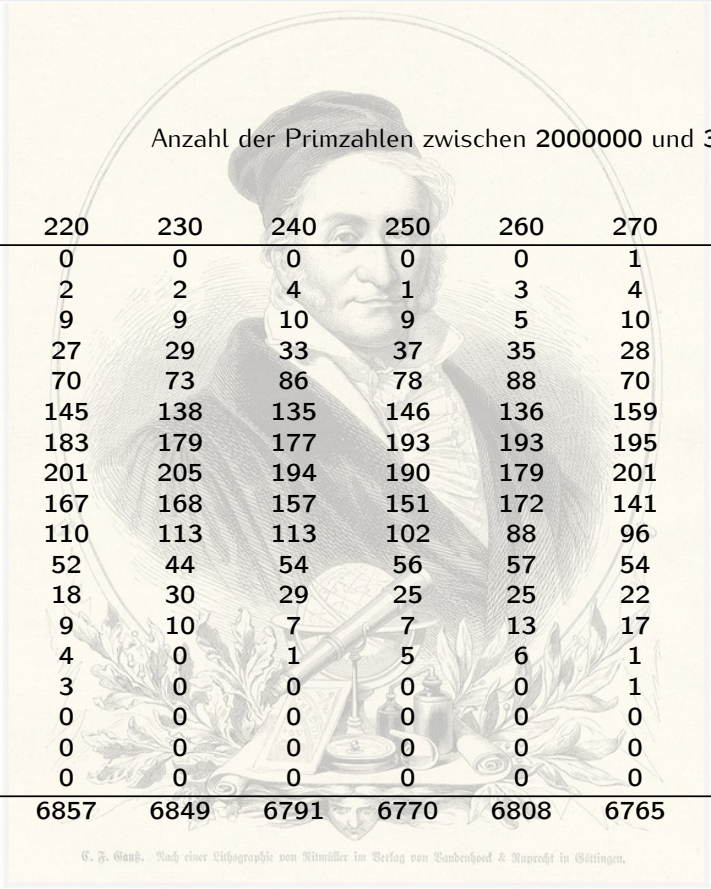
	210	220	230	240	250	260	270	280	290	300	
0	—	—	—	—	—	—	1	—	—	—	1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	11	9	6	10	7	15	13	98
3	32	27	29	32	37	35	28	43	30	44	337
4	69	69	73	56	78	88	71	95	85	64	778
5	119	146	138	136	147	136	158	135	140	153	1408
6	197	183	179	176	(193)	194	195	195	179	187	1878
7	204	201	205	194	159	180	201	188	222	214	1998
8	157	168	168	158	151	170	142	145	132	134	1525
9	115	109	113	112	102	88	96	87	109	103	1034
10	63	52	44	55	58	58	53	67	53	58	561
11	21	18	30	28	23	24	22	24	18	15	223
12	8	9	10	7	7	13	17	9	8	11	99
13	2	4	—	1	5	6	1	2	5	1	27
14	—	3	—	—	—	—	1	—	2	—	(6)
15	—	—	—	—	—	—	—	—	—	1	1
16	—	—	—	—	—	—	—	—	—	—	—
17	—	—	—	—	—	—	—	1	—	—	1
	6874	6857	6849	6787	6766	6804	6762	6714	6749	6705	67862

Il y a 193 intervalles de la forme $[240.10^4+100k, 240.10^4+100k+100[$ inclus dans $[240.10^4, 250.10^4[$ et contenant exactement 6 nombres premiers

Il y a 6 intervalles de la forme $[200.10^4+100k, 200.10^4+100k+100[$ inclus dans $[200.10^4, 300.10^4[$ contenant exactement 14 nombres premiers.

Compter les nombres premiers

Une conjecture du vieux Gauss

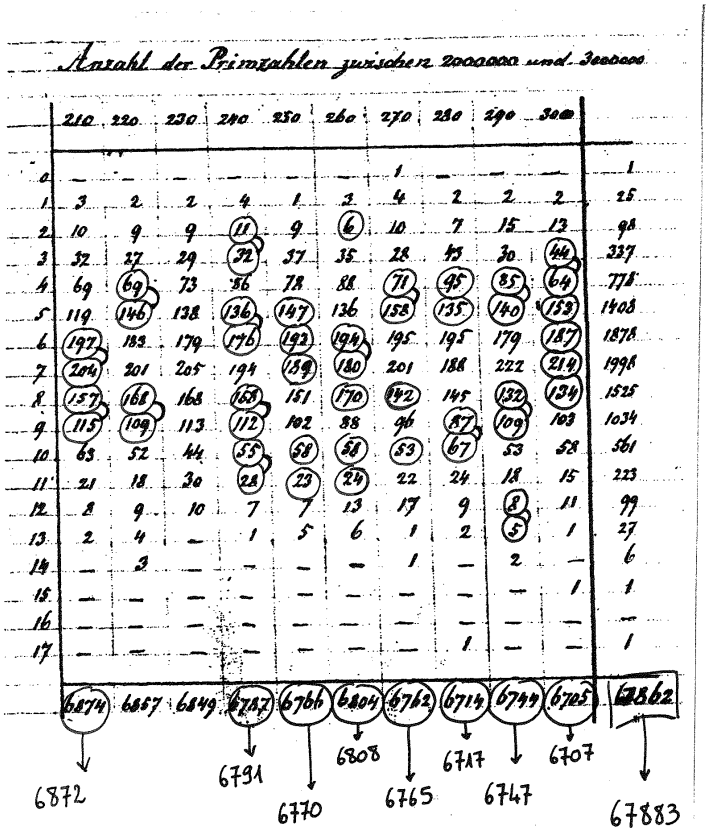


Anzahl der Primzahlen zwischen **2000000** und **3000000**

	210	220	230	240	250	260	270	280	290	300	
0	0	0	0	0	0	0	1	0	0	0	1
1	3	2	2	4	1	3	4	2	2	2	25
2	10	9	9	10	9	5	10	7	15	13	97
3	32	27	29	33	37	35	28	43	30	43	337
4	69	70	73	86	78	88	70	93	84	65	776
5	119	145	138	135	146	136	159	137	141	152	1408
6	198	183	179	177	193	193	195	195	179	189	1881
7	203	201	205	194	190	179	201	188	222	212	1995
8	158	167	168	157	151	172	141	145	131	135	1525
9	114	110	113	113	102	88	96	86	110	103	1035
10	63	52	44	54	56	57	54	68	53	58	559
11	21	18	30	29	25	25	22	24	18	15	227
12	8	9	10	7	7	13	17	9	7	11	98
13	2	4	0	1	5	6	1	2	6	1	28
14	0	3	0	0	0	0	1	0	2	0	6
15	0	0	0	0	0	0	0	0	0	1	1
16	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	1
	6872	6857	6849	6791	6770	6808	6765	6717	6747	6707	67883

Compter les nombres premiers

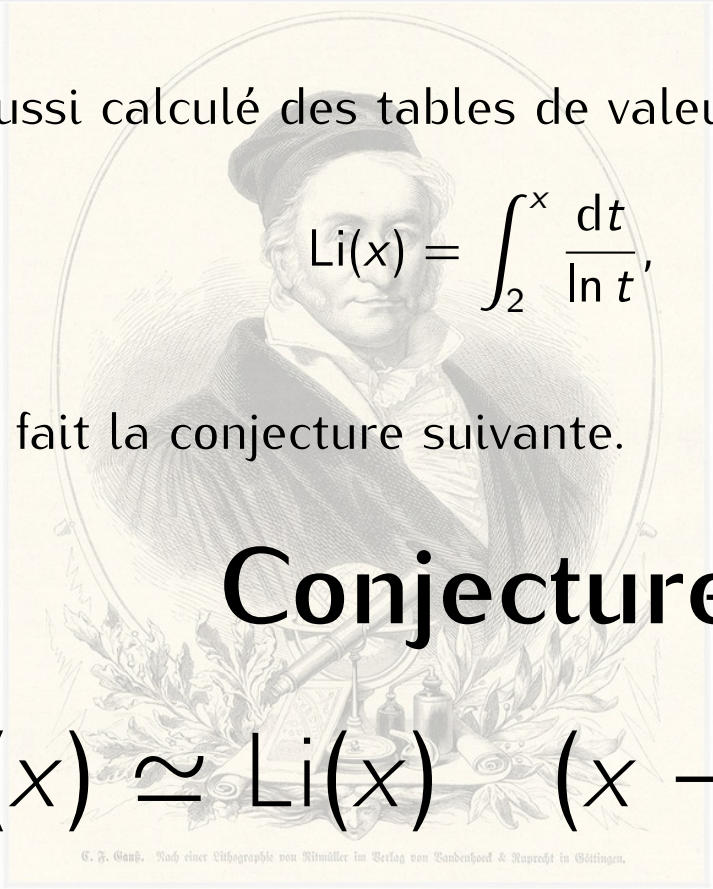
Une conjecture du vieux Gauss



8 : l'un des nombres entourés est trop grand de 1, l'autre étant trop petit de 1. Il s'agit probablement d'une erreur de décompte d'intervalle plutôt que de calcul des premiers.

Compter les nombres premiers

Une conjecture du vieux Gauss



Ayant aussi calculé des tables de valeurs de

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t},$$

Gauss a fait la conjecture suivante.

Conjecture

$$\pi(x) \simeq \mathrm{Li}(x) \quad (x \to +\infty).$$

Compter les nombres premiers

Une conjecture du vieux Gauss

und ich habe (da ich zu einer enthaltenderen Abzählung der Reihe nach keine Geduld hatte) sehr oft einzelne unbeschäftigte Viertelstunden verwandt, um bald hie bald dort eine Chiliade abzuzählen

Ich erkannte bald, dass unter allen Schwankungen diese Frequenz durchschnittlich nahe dem Logarithmen verkehrt proportional sei, so dass die Anzahl aller Primzahlen unter einer gegebenen Grenze n nahe durch das Integral

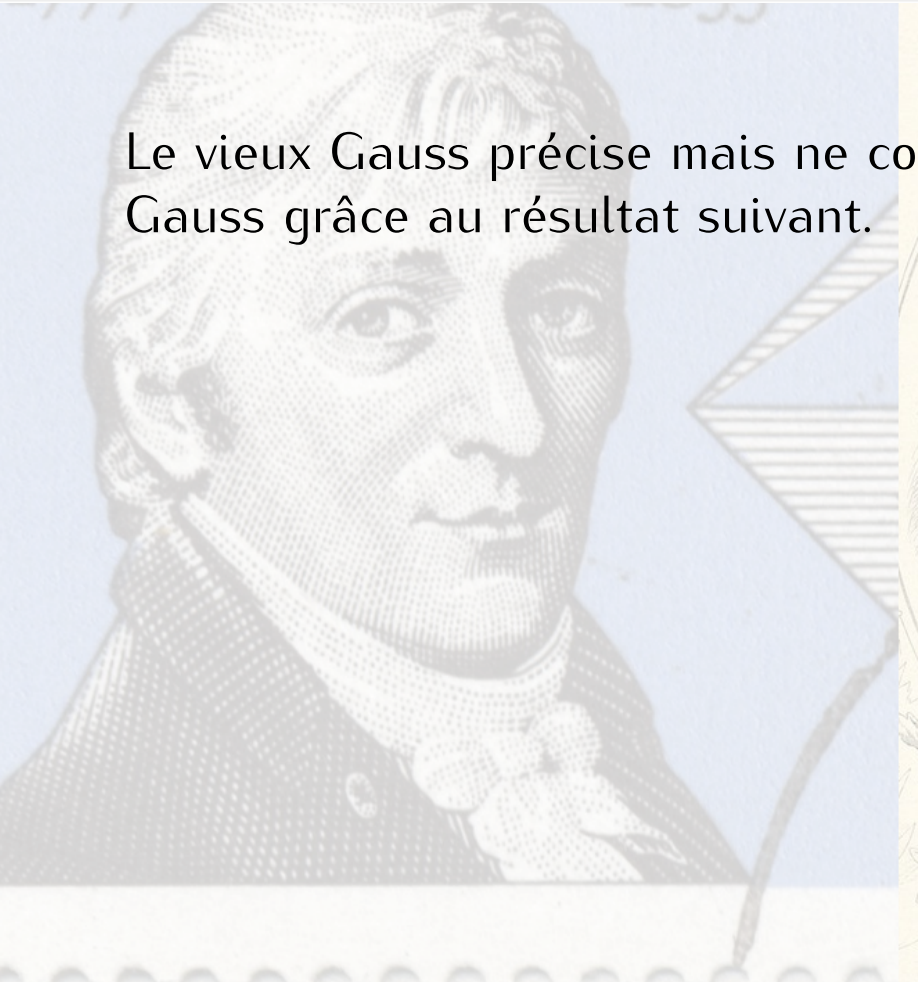
$$\int \frac{dn}{\log n}$$

Göttingen 24 ~~Octbr~~ December 1849

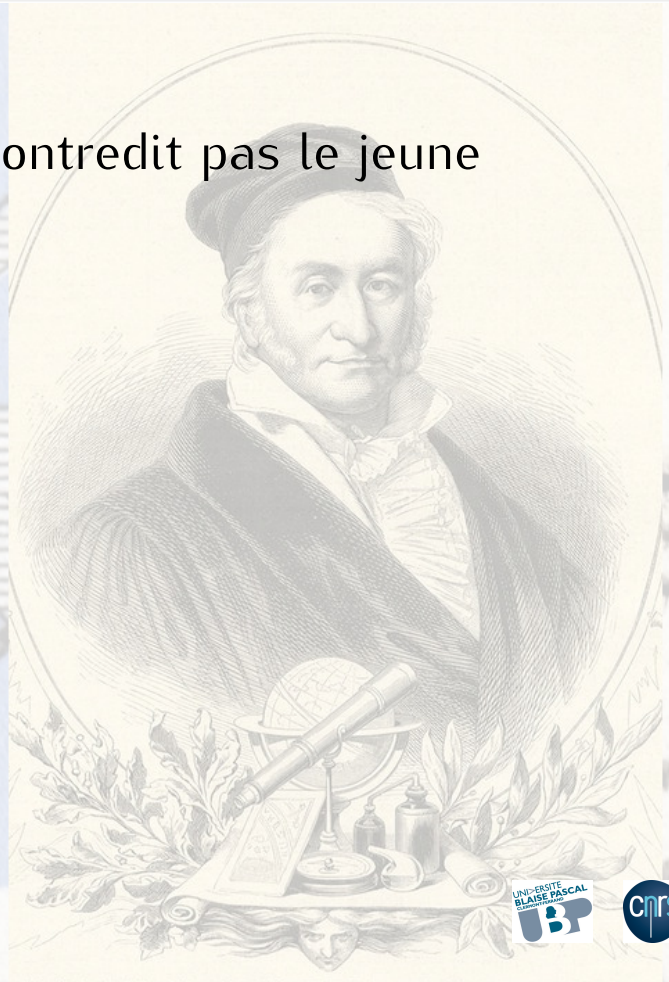
Stets der Ihrige
C. F. Gauss

Compter les nombres premiers

Une conjecture du vieux Gauss



Le vieux Gauss précise mais ne contredit pas le jeune Gauss grâce au résultat suivant.



Compter les nombres premiers

Une conjecture du vieux Gauss

Le vieux Gauss précise mais ne contredit pas le jeune Gauss grâce au résultat suivant.

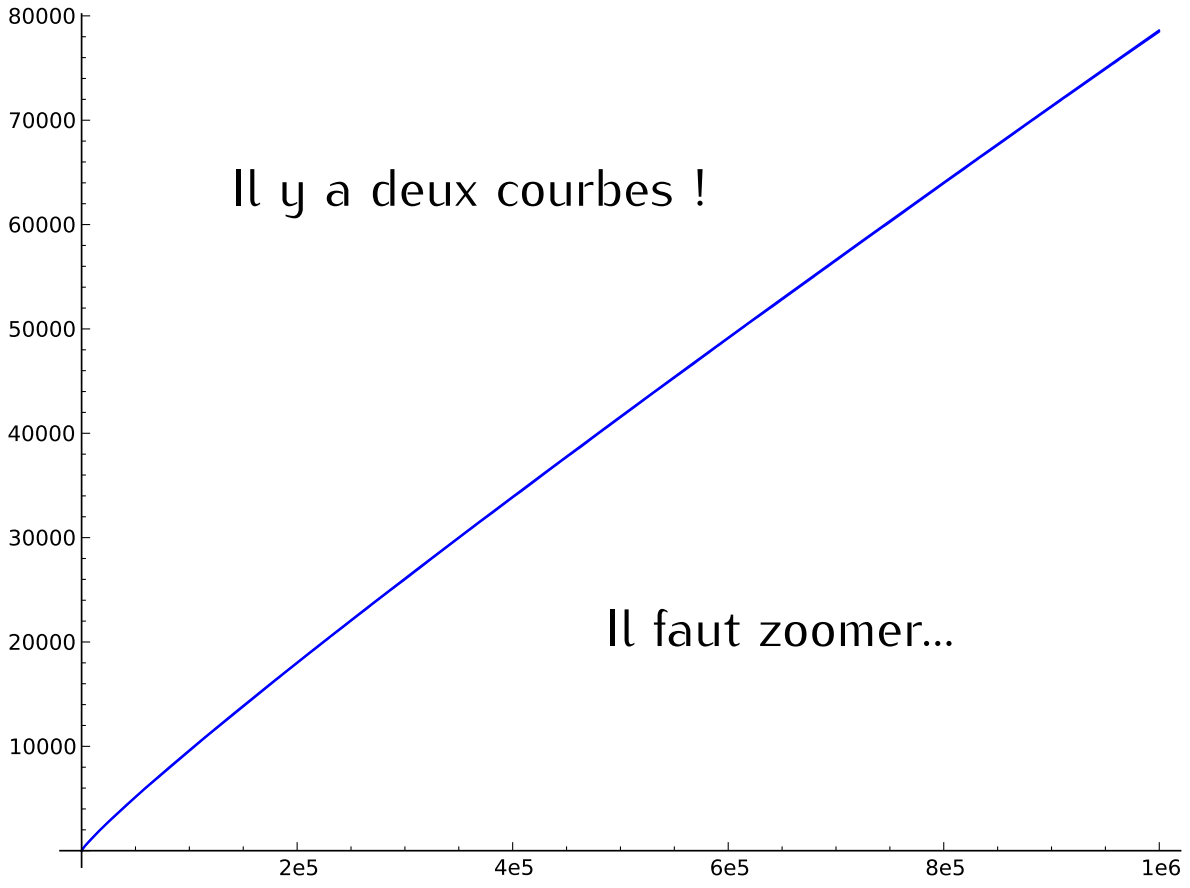
Exercice

Pour tout entier $n \geqslant 1$, il existe une fonction ε de limite nulle à l'infini telle que

$$\mathrm{Li}(x) = \frac{x}{\ln x}\left(1 + \sum_{k=1}^{n} \frac{k!}{\ln^k x}\right) + \frac{x}{\ln^{n+1} x}\varepsilon(x).$$

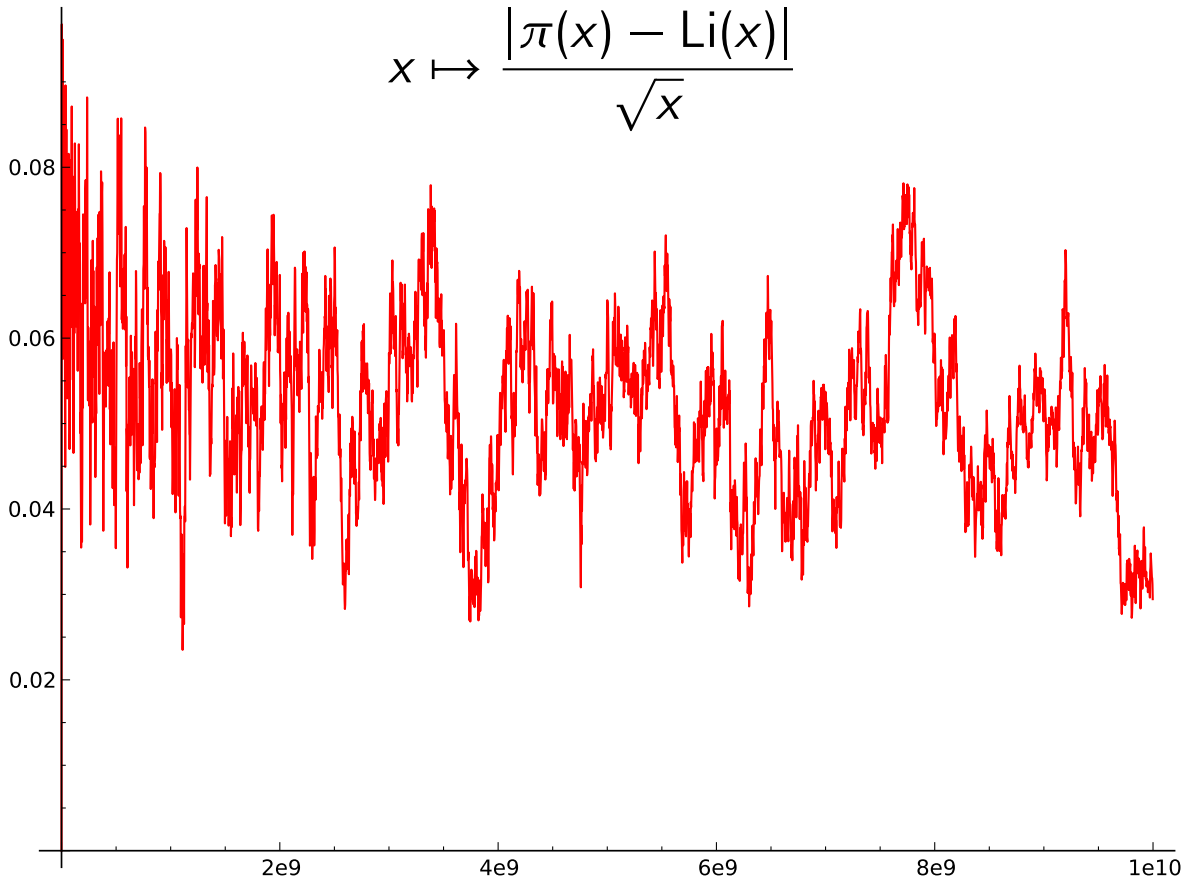
Compter les nombres premiers

Une conjecture du vieux Gauss



Compter les nombres premiers

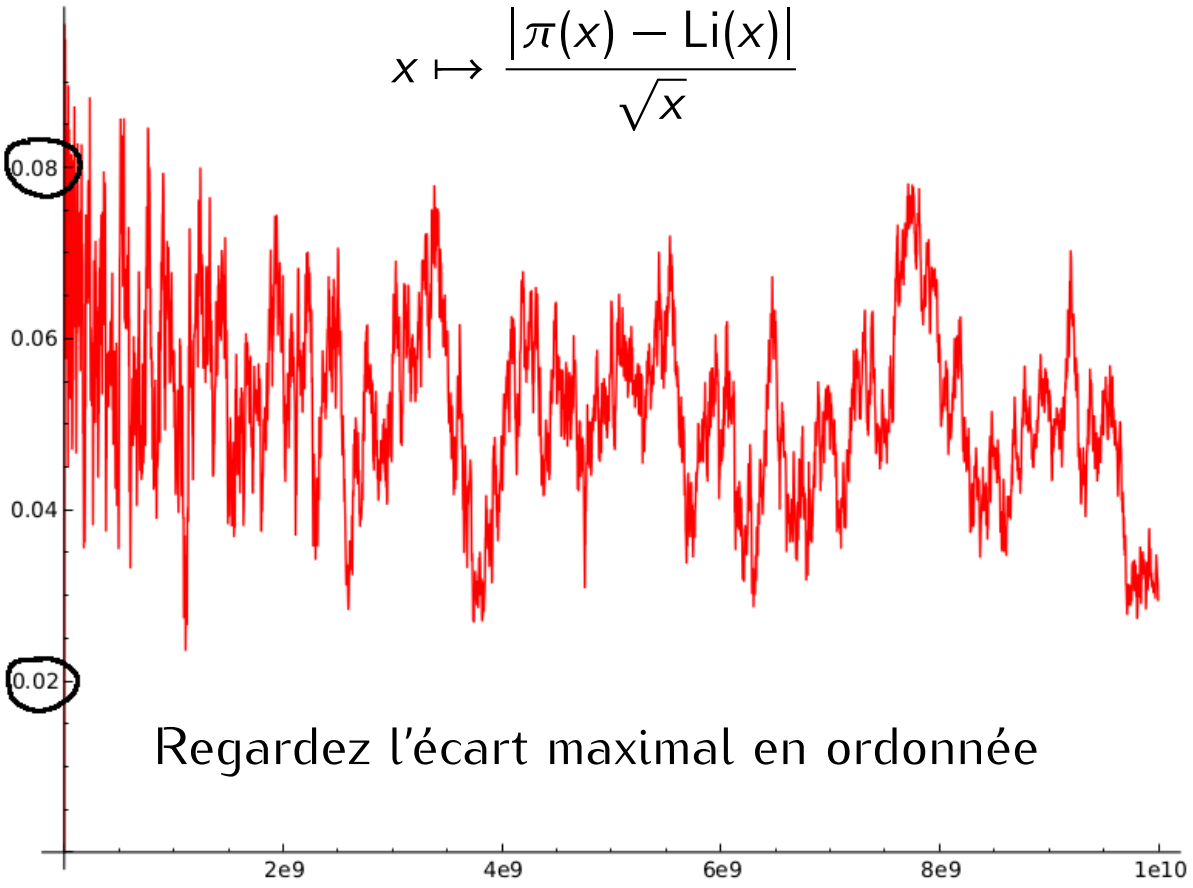
Une conjecture du vieux Gauss



Compter les nombres premiers

Une conjecture du vieux Gauss

$$x \mapsto \frac{|\pi(x) - \mathrm{Li}(x)|}{\sqrt{x}}$$



Regardez l'écart maximal en ordonnée

Compter les nombres premiers

L'idée de genie de Riemann (1859)

La série

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

converge normalement sur tout compact de

$$\{s \in \mathbb{R} : s > 1\}.$$

Elle définit sur cet ensemble une fonction C^∞. C'est la fonction ζ de Riemann.

Compter les nombres premiers

L'idée de genie de Riemann (1859)

La série

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

converge normalement sur tout compact de

$$\{s \in \mathbb{R} : s > 1\}.$$

Elle définit sur cet ensemble une fonction C^∞. C'est la fonction ζ de Riemann. La décomposition des entiers en produit de nombres premiers implique

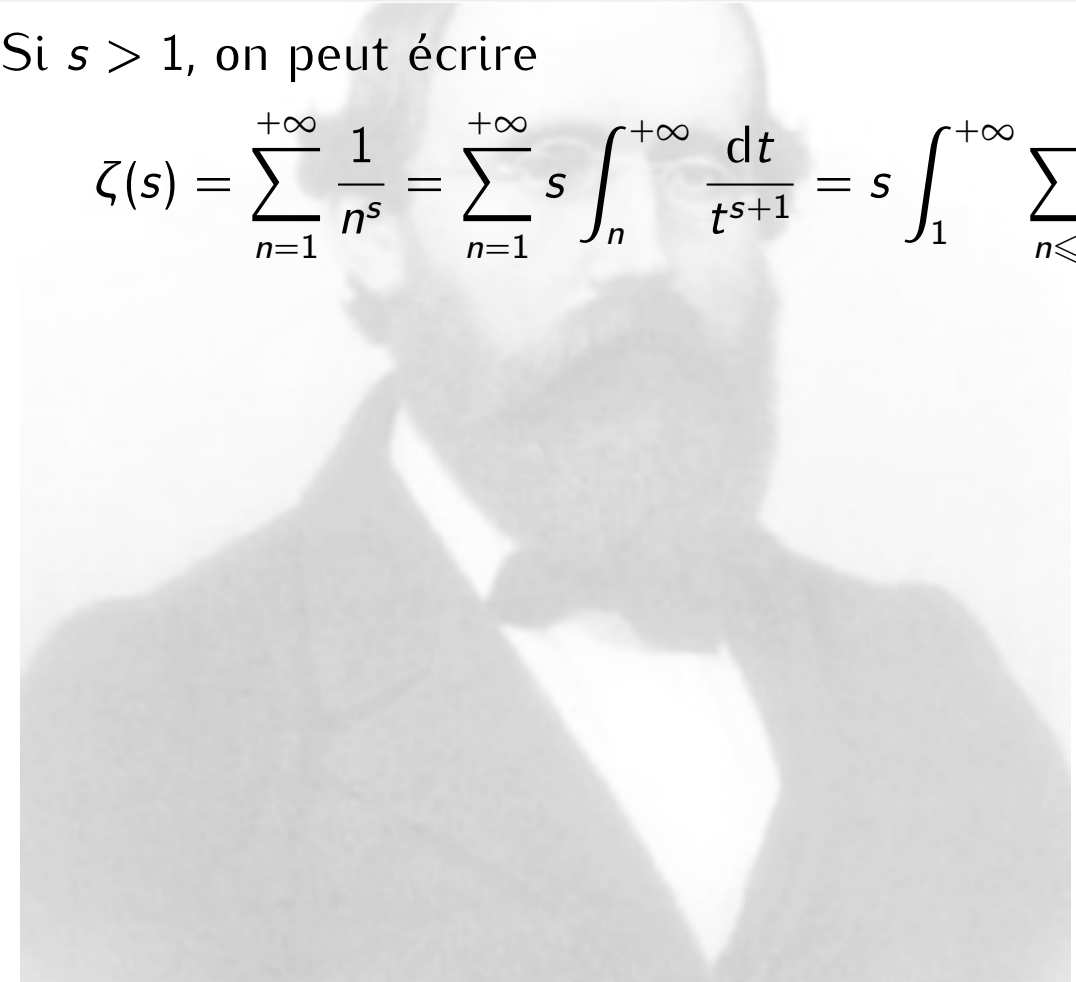
$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \lim_{N \to +\infty} \prod_{\substack{p \in \mathcal{P} \\ p \leqslant N}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Compter les nombres premiers

L'idée de genie de Riemann (1859)

Si $s > 1$, on peut écrire

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{n=1}^{+\infty} s \int_n^{+\infty} \frac{\mathrm{d}t}{t^{s+1}} = s \int_1^{+\infty} \sum_{n \leqslant t} 1 \frac{\mathrm{d}t}{t^{s+1}}.$$



Compter les nombres premiers

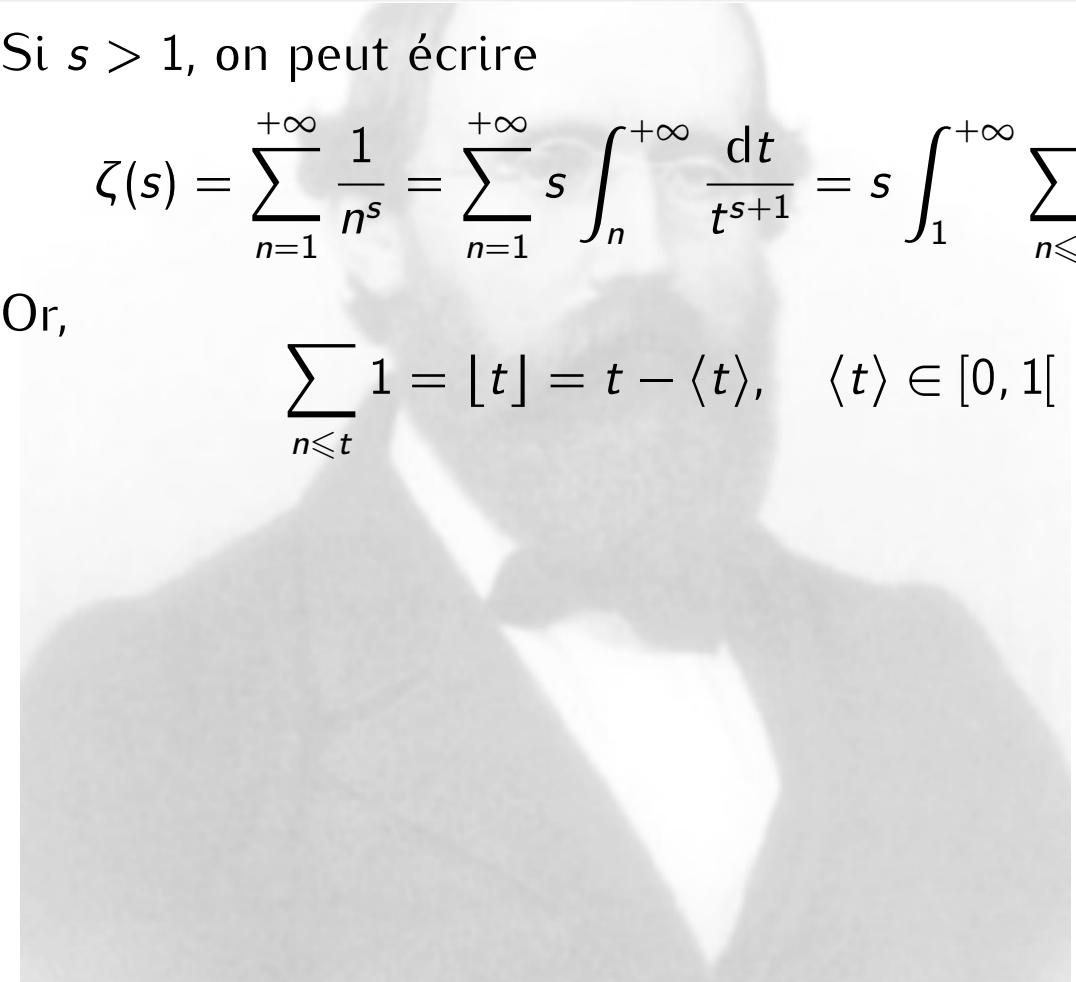
L'idée de genie de Riemann (1859)

Si $s > 1$, on peut écrire

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{n=1}^{+\infty} s \int_n^{+\infty} \frac{\mathrm{d}t}{t^{s+1}} = s \int_1^{+\infty} \sum_{n \leqslant t} 1 \frac{\mathrm{d}t}{t^{s+1}}.$$

Or,

$$\sum_{n \leqslant t} 1 = \lfloor t \rfloor = t - \langle t \rangle, \quad \langle t \rangle \in [0, 1[$$



Compter les nombres premiers

L'idée de genie de Riemann (1859)

Si $s > 1$, on peut écrire

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{n=1}^{+\infty} s \int_n^{+\infty} \frac{\mathrm{d}t}{t^{s+1}} = s \int_1^{+\infty} \sum_{n \leqslant t} 1 \frac{\mathrm{d}t}{t^{s+1}}.$$

Or,

$$\sum_{n \leqslant t} 1 = \lfloor t \rfloor = t - \langle t \rangle, \quad \langle t \rangle \in [0, 1[$$

donc

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\langle t \rangle}{t^{s+1}} \, \mathrm{d}t.$$

Compter les nombres premiers

L'idée de genie de Riemann (1859)

Si $s > 1$, on peut écrire

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{n=1}^{+\infty} s \int_n^{+\infty} \frac{\mathrm{d}t}{t^{s+1}} = s \int_1^{+\infty} \sum_{n \leqslant t} 1 \frac{\mathrm{d}t}{t^{s+1}}.$$

Or,

$$\sum_{n \leqslant t} 1 = \lfloor t \rfloor = t - \langle t \rangle, \quad \langle t \rangle \in [0, 1[$$

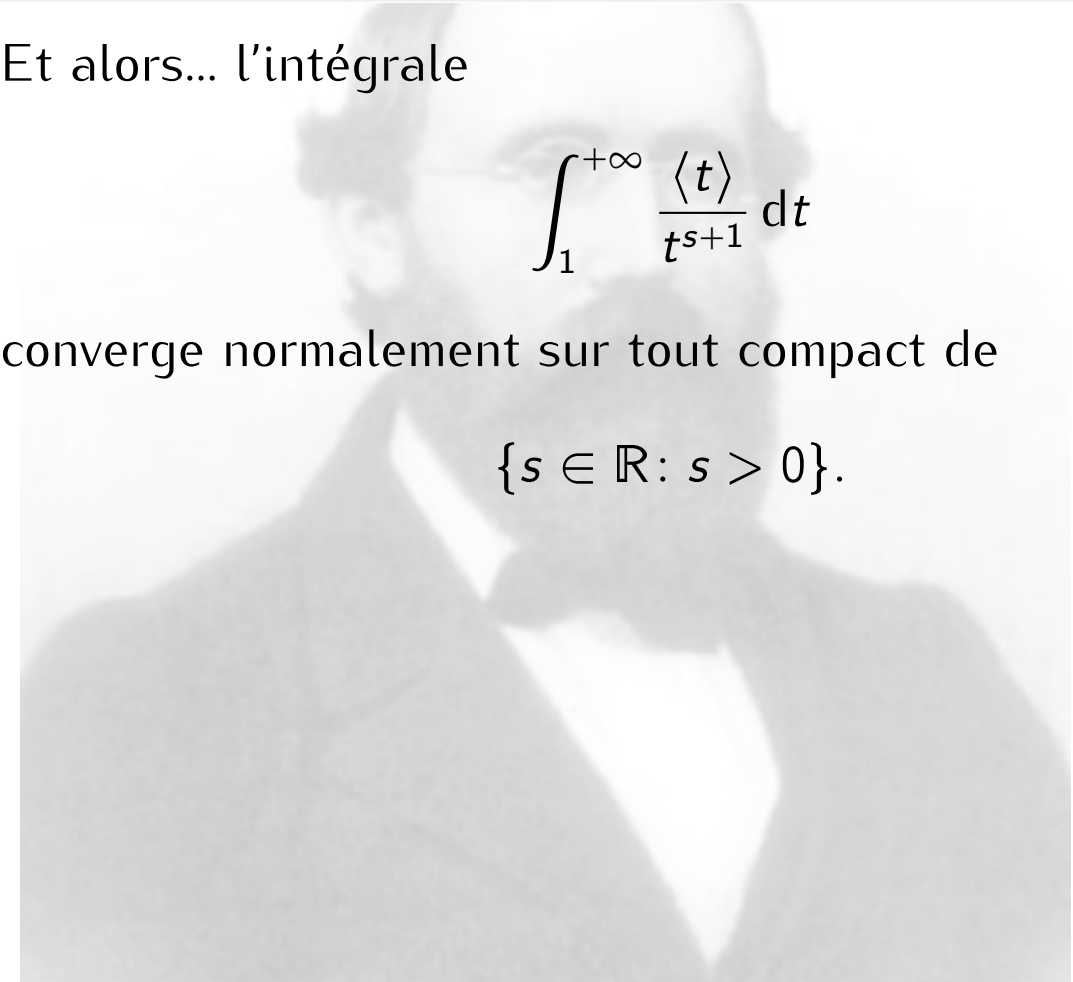
donc

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\langle t \rangle}{t^{s+1}} \, \mathrm{d}t.$$

Roy Lichtenstein

Compter les nombres premiers

L'idée de genie de Riemann (1859)



Et alors... l'intégrale

$$\int_1^{+\infty} \frac{\langle t \rangle}{t^{s+1}}\, \mathrm{d}t$$

converge normalement sur tout compact de

$$\{s \in \mathbb{R} : s > 0\}.$$

Compter les nombres premiers

L'idée de genie de Riemann (1859)

Et alors... l'intégrale

$$\int_1^{+\infty} \frac{\langle t \rangle}{t^{s+1}}\, \mathrm{d}t$$

converge normalement sur tout compact de

$$\{s \in \mathbb{R} : s > 0\}.$$

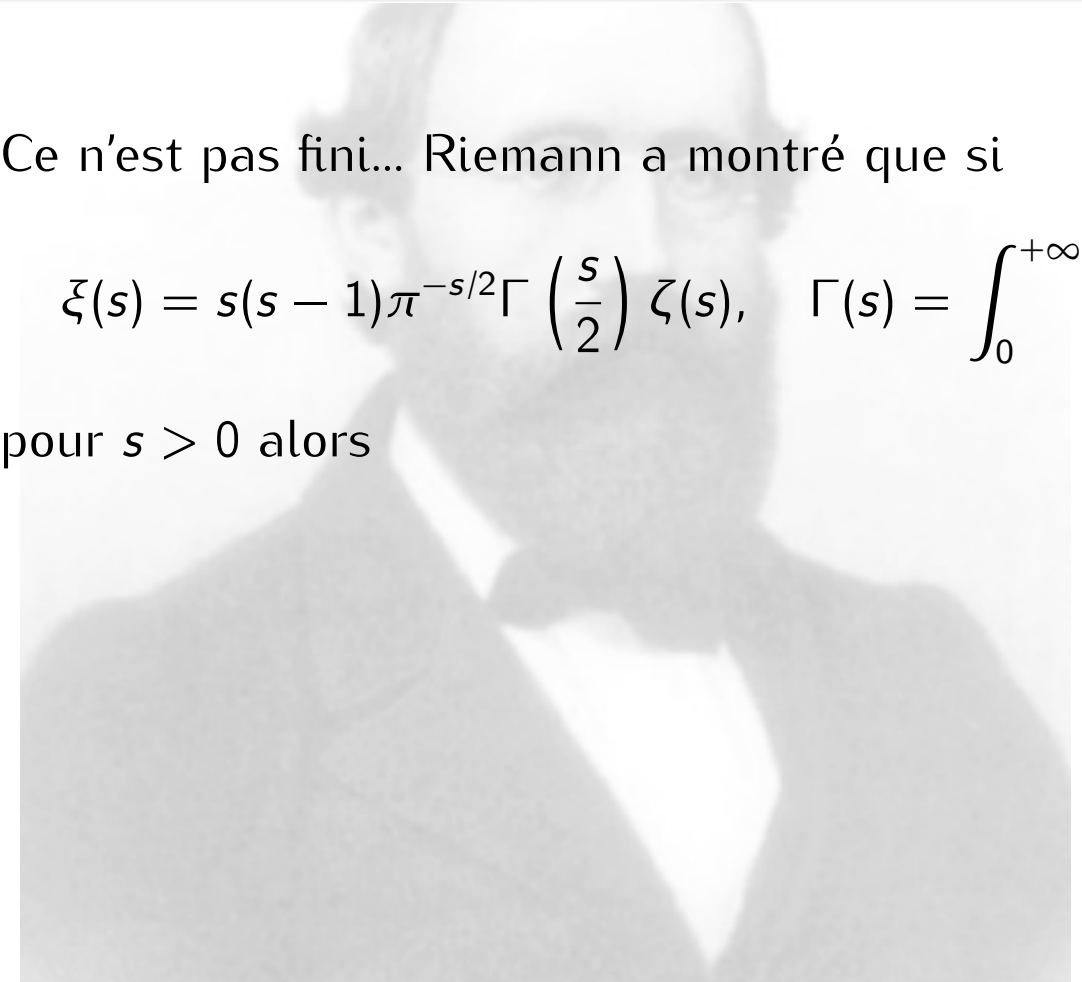
Autrement, dit l'équation

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\langle t \rangle}{t^{s+1}}\, \mathrm{d}t.$$

définit sur $\{s \in \mathbb{R} : s > 0,\ s \neq 1\}$ un prolongement de ζ en fonction C^∞.

Compter les nombres premiers

L'idée de genie de Riemann (1859)



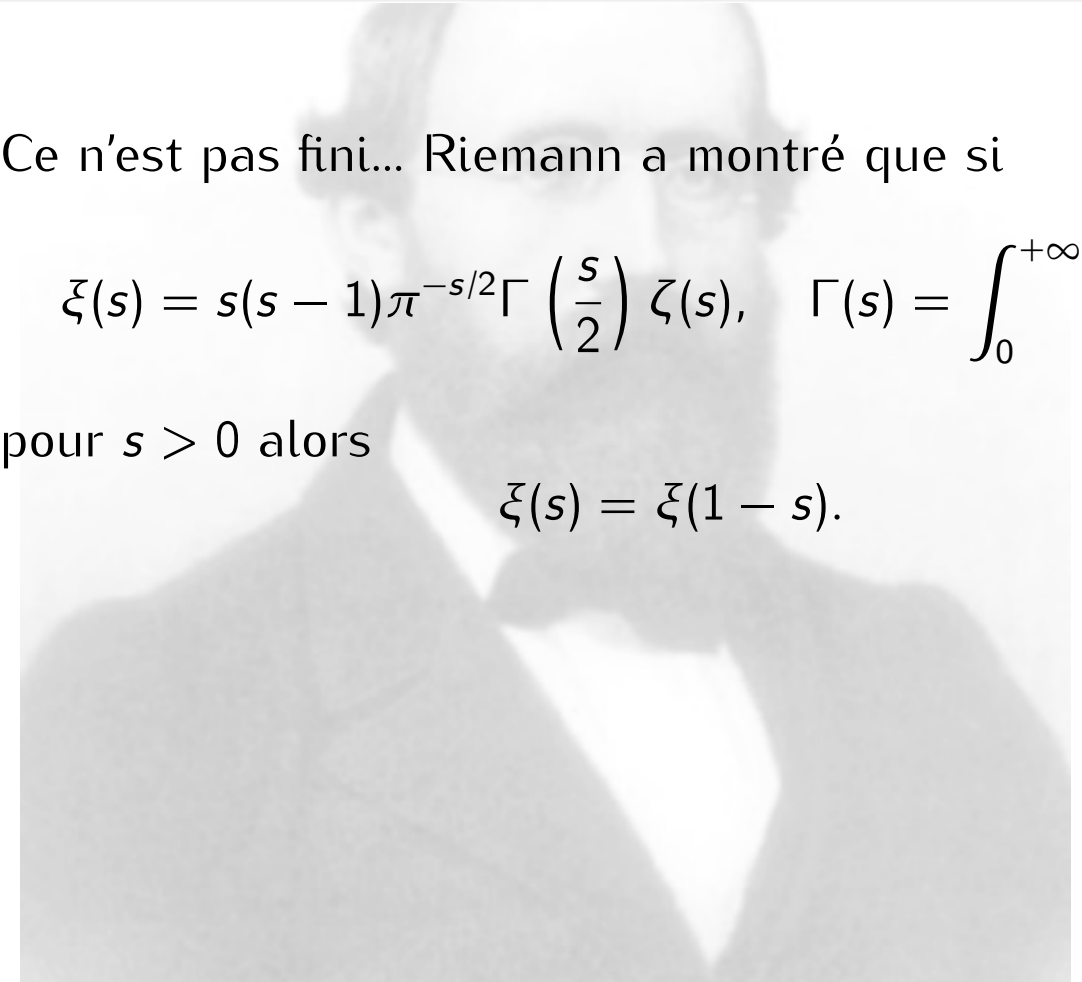
Ce n'est pas fini... Riemann a montré que si

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s), \quad \Gamma(s) = \int_0^{+\infty} x^s e^{-x}\frac{\mathrm{d}x}{x}$$

pour $s > 0$ alors

Compter les nombres premiers

L'idée de genie de Riemann (1859)



Ce n'est pas fini... Riemann a montré que si

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s), \quad \Gamma(s) = \int_0^{+\infty} x^s e^{-x}\frac{\mathrm{d}x}{x}$$

pour $s > 0$ alors

$$\xi(s) = \xi(1-s).$$

Compter les nombres premiers

L'idée de genie de Riemann (1859)

Ce n'est pas fini... Riemann a montré que si

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s), \quad \Gamma(s) = \int_0^{+\infty} x^s e^{-x}\frac{\mathrm{d}x}{x}$$

pour $s > 0$ alors

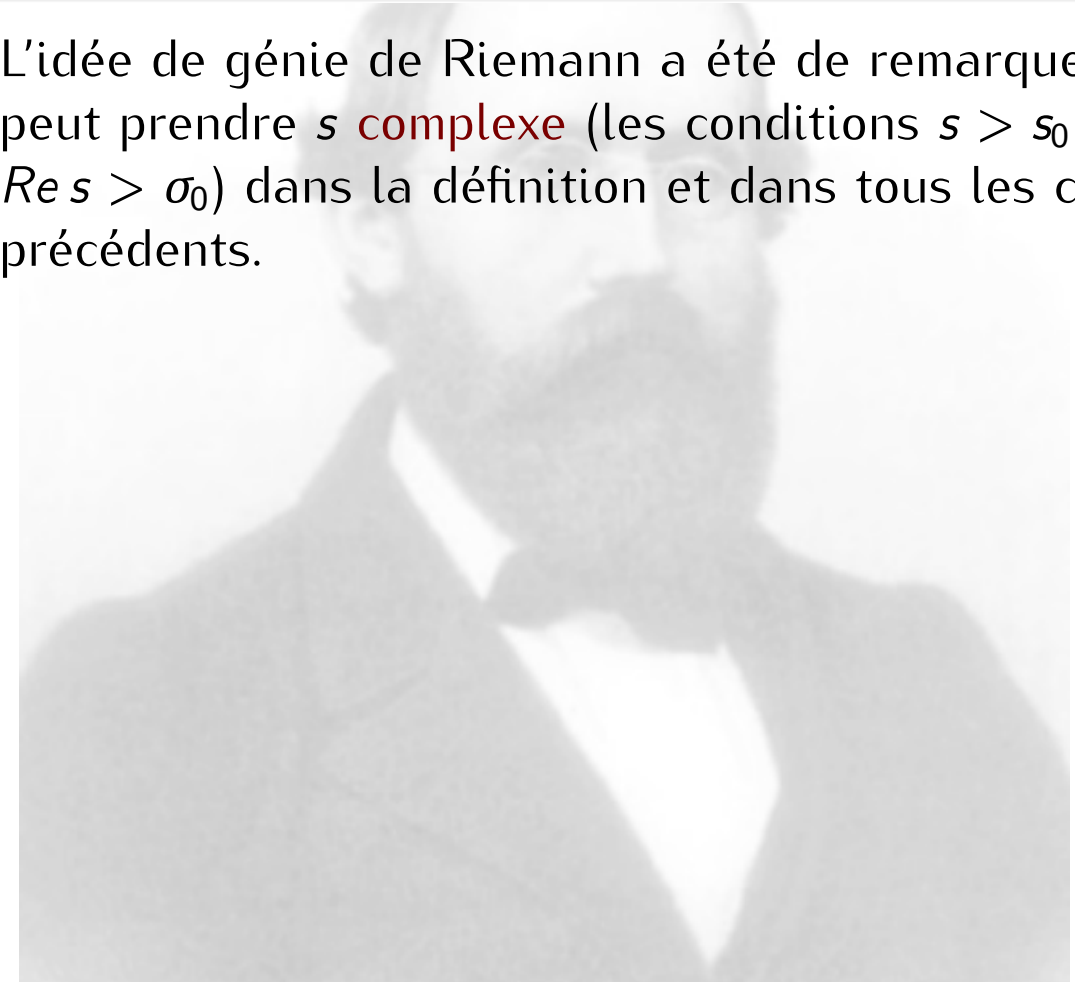
$$\xi(s) = \xi(1-s).$$

Comme Γ peut-être prolongée en une fonction C^∞ sur $\mathbb{R}$ privé des entiers négatifs (grâce à $\Gamma(s+1) = s\Gamma(s)$) on en déduit une définition de ζ sur $\mathbb{C} \setminus \{0, 1\}$ (et on peut par ailleurs définir $\zeta(0)$ par passage à la limite).

Compter les nombres premiers

L'idée de genie de Riemann (1859)

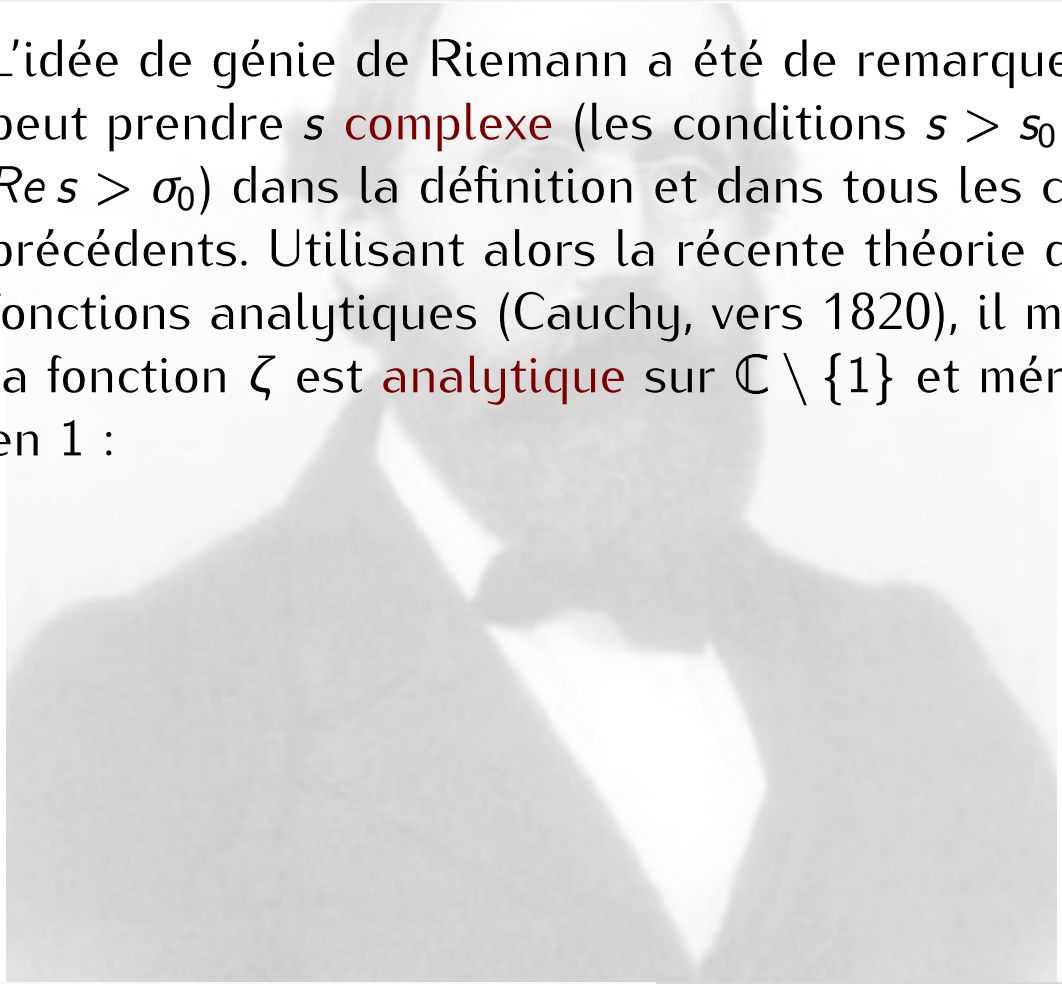
L'idée de génie de Riemann a été de remarquer qu'on peut prendre s complexe (les conditions $s > s_0$ devenant $Re\, s > \sigma_0$) dans la définition et dans tous les calculs précédents.



Compter les nombres premiers

L'idée de genie de Riemann (1859)

L'idée de génie de Riemann a été de remarquer qu'on peut prendre s complexe (les conditions $s > s_0$ devenant $Re\, s > \sigma_0$) dans la définition et dans tous les calculs précédents. Utilisant alors la récente théorie des fonctions analytiques (Cauchy, vers 1820), il montre que la fonction ζ est analytique sur $\mathbb{C} \setminus \{1\}$ et méromorphe en 1 :



Compter les nombres premiers

L'idée de genie de Riemann (1859)

L'idée de génie de Riemann a été de remarquer qu'on peut prendre s complexe (les conditions $s > s_0$ devenant $Re\, s > \sigma_0$) dans la définition et dans tous les calculs précédents. Utilisant alors la récente théorie des fonctions analytiques (Cauchy, vers 1820), il montre que la fonction ζ est analytique sur $\mathbb{C} \setminus \{1\}$ et méromorphe en 1 :

$$\zeta(s) = \sum_{n=0}^{+\infty} a_n (s - s_0)^n \quad \text{au voisinage de } s_0 \neq 1$$

et

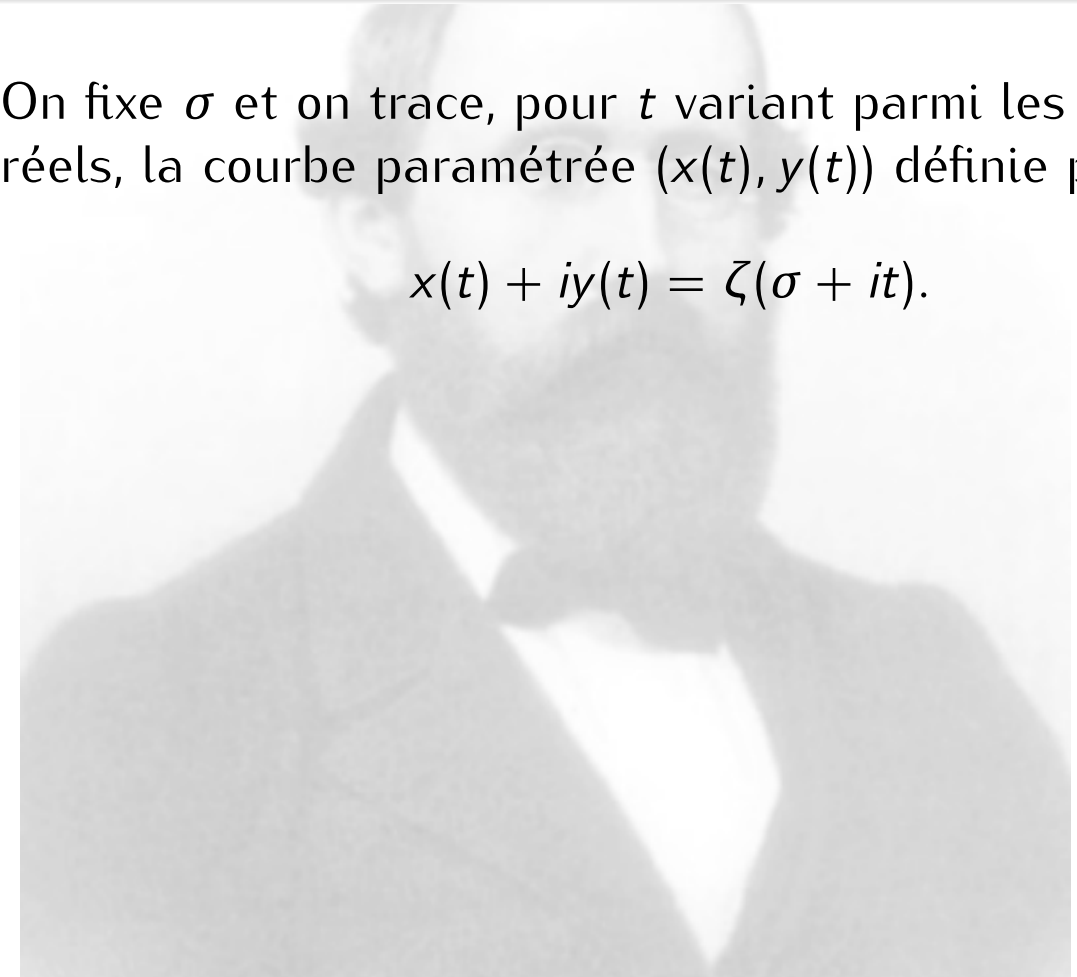
$$\zeta(s) = \frac{1}{s} + \sum_{n=0}^{+\infty} a_n (s-1)^n \quad \text{au voisinage de } 1.$$

Compter les nombres premiers

À quoi ressemble ζ ?

On fixe σ et on trace, pour t variant parmi les nombres réels, la courbe paramétrée $(x(t), y(t))$ définie par

$$x(t) + iy(t) = \zeta(\sigma + it).$$



Compter les nombres premiers

À quoi ressemble ζ ?

On fixe σ et on trace, pour t variant parmi les nombres réels, la courbe paramétrée $(x(t), y(t))$ définie par

$$x(t) + iy(t) = \zeta(\sigma + it).$$

Si la courbe passe par l'origine, c'est en une valeur de t où $\zeta(\sigma + it) = 0$. Traçons les différentes courbes pour différentes valeurs de σ.

`izeta.mov`

Compter les nombres premiers

À quoi ressemble ζ ?

On fixe σ et on trace, pour t variant parmi les nombres réels, la courbe paramétrée $(x(t), y(t))$ définie par

$$x(t) + iy(t) = \zeta(\sigma + it).$$

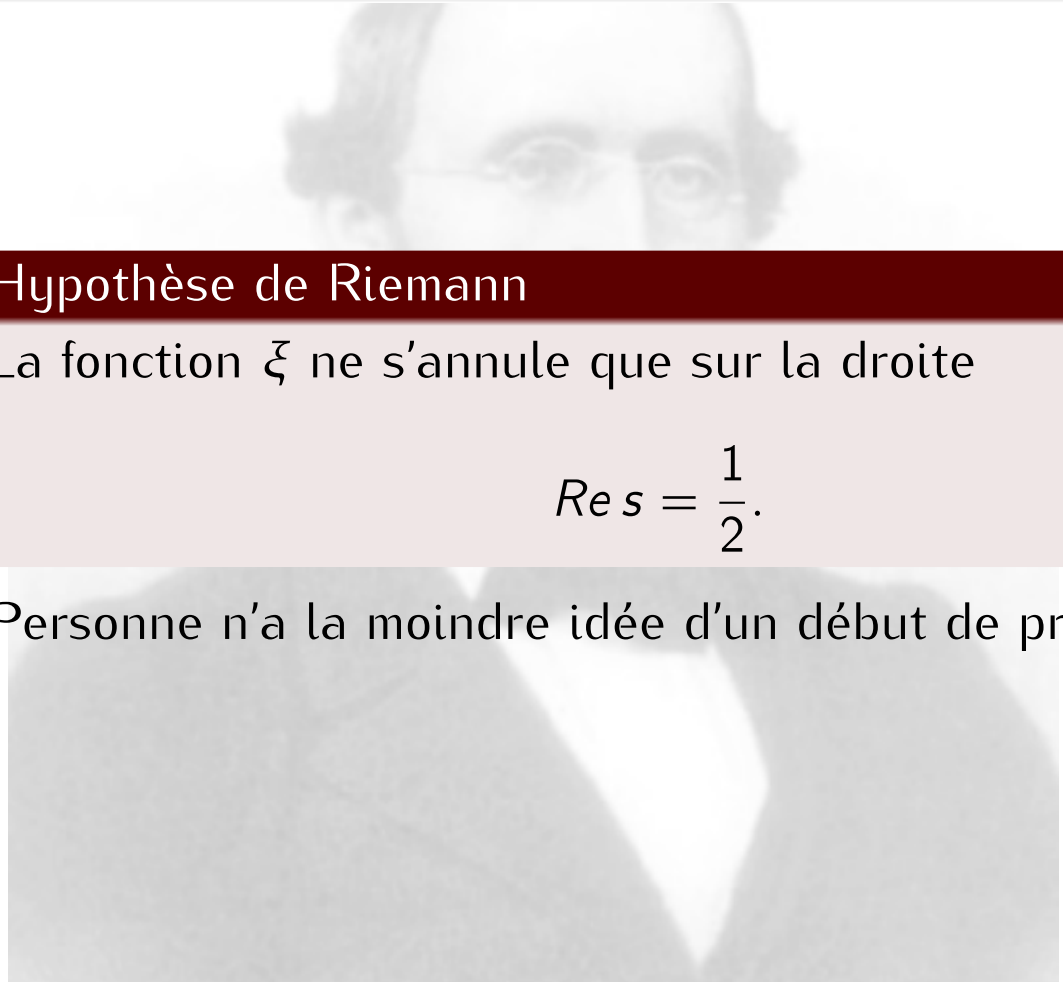
Si la courbe passe par l'origine, c'est en une valeur de t où $\zeta(\sigma + it) = 0$. Traçons les différentes courbes pour différentes valeurs de σ.

`izeta.mov`

On remarque que la courbe ne passe à l'origine que pour $\sigma = \frac{1}{2}$. Traçons la courbe correspondante.

`iargzeta.mov`

Films : Jeffrey Stopple



Hypothèse de Riemann

La fonction ξ ne s'annule que sur la droite

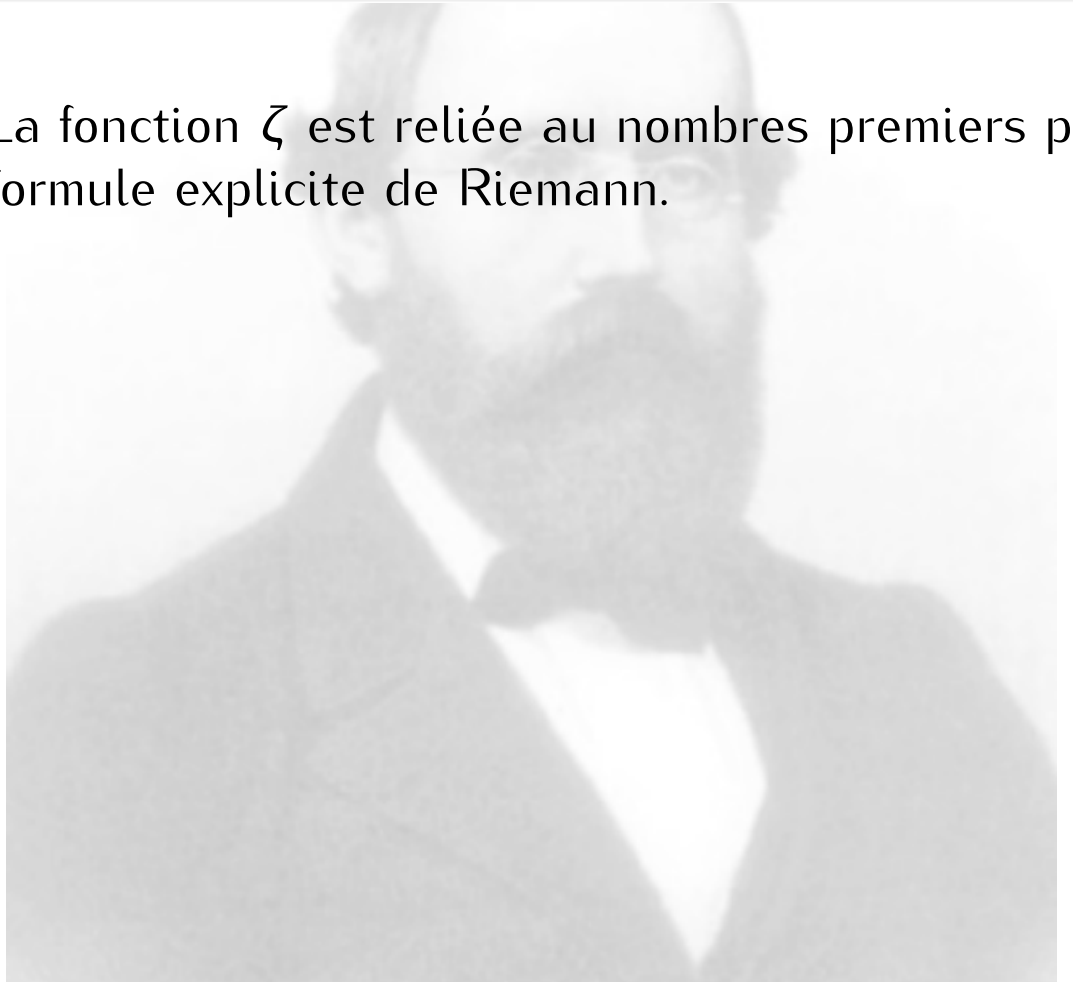
$$Re\, s = \frac{1}{2}.$$

Personne n'a la moindre idée d'un début de preuve...

Compter les nombres premiers

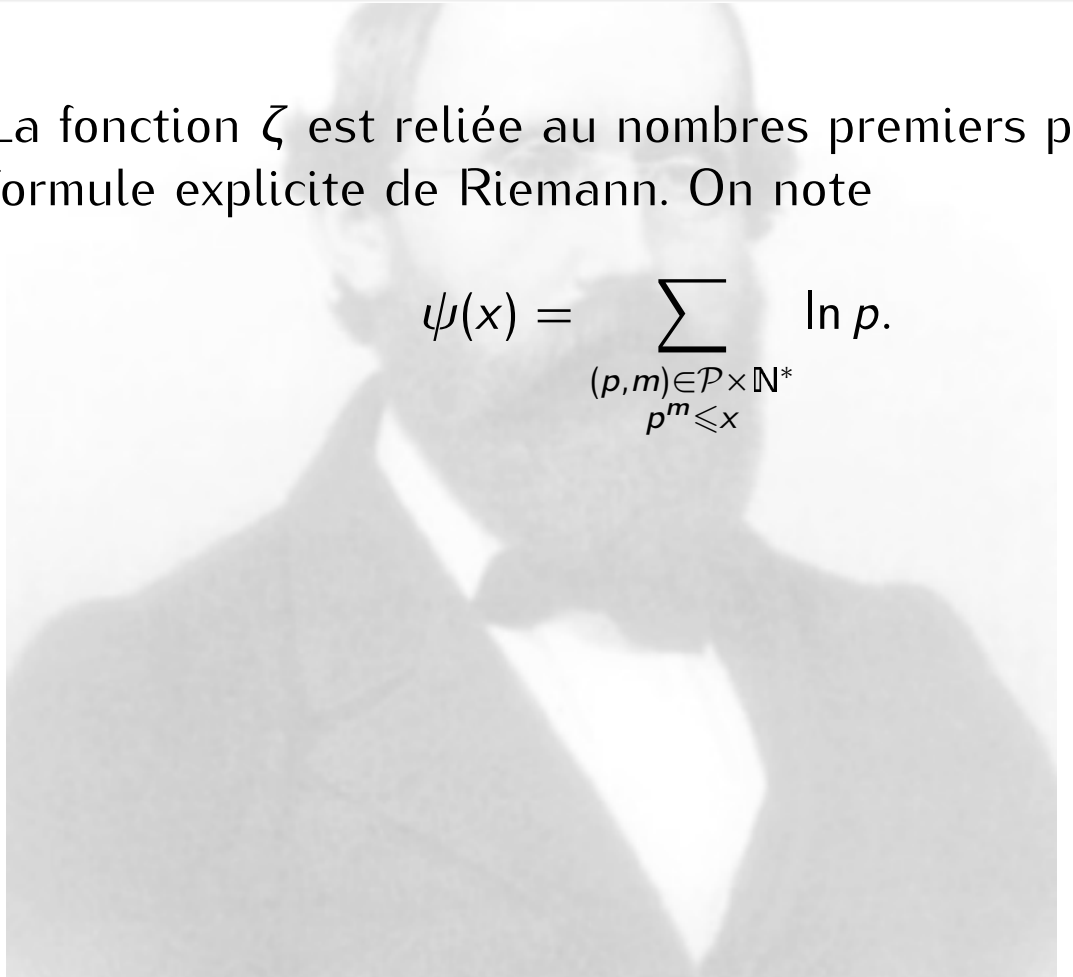
De ζ à π

La fonction ζ est reliée au nombres premiers par la formule explicite de Riemann.



Compter les nombres premiers

De ζ à π



La fonction ζ est reliée au nombres premiers par la formule explicite de Riemann. On note

$$\psi(x) = \sum_{\substack{(p,m)\in\mathcal{P}\times\mathbb{N}^* \\ p^m\leqslant x}} \ln p.$$

Compter les nombres premiers

De ζ à π

La fonction ζ est reliée au nombres premiers par la formule explicite de Riemann. On note

$$\psi(x) = \sum_{\substack{(p,m)\in\mathcal{P}\times\mathbb{N}^* \\ p^m\leqslant x}} \ln p.$$

Alors, Riemann a montré que

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right)$$

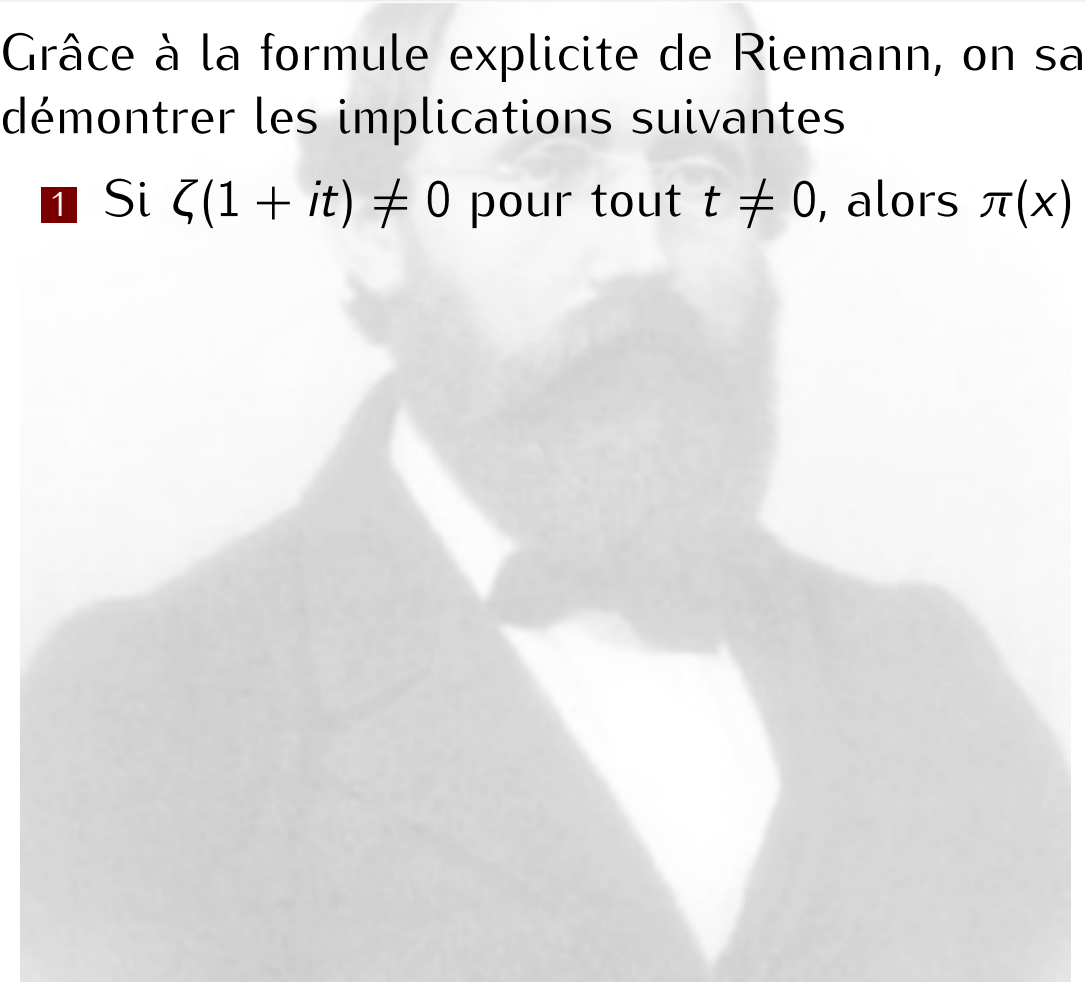
où ρ parcourt l'ensemble des zéros de ξ.

Compter les nombres premiers

De ζ à π

Grâce à la formule explicite de Riemann, on sait démontrer les implications suivantes

1. Si $\zeta(1+it) \neq 0$ pour tout $t \neq 0$, alors $\pi(x) \sim \dfrac{x}{\ln x}$.



Compter les nombres premiers

De ζ à π

Grâce à la formule explicite de Riemann, on sait démontrer les implications suivantes

1. Si $\zeta(1+it) \neq 0$ pour tout $t \neq 0$, alors $\pi(x) \sim \dfrac{x}{\ln x}$.
2. Si ϑ est le sup des parties réelles de zéros de ξ, alors il existe une constante C telle que, pour tout $x \geqslant 2$ on a

$$|\pi(x) - \mathrm{Li}(x)| \leqslant C x^{\vartheta} \ln x.$$

Compter les nombres premiers

De ζ à π

Grâce à la formule explicite de Riemann, on sait démontrer les implications suivantes

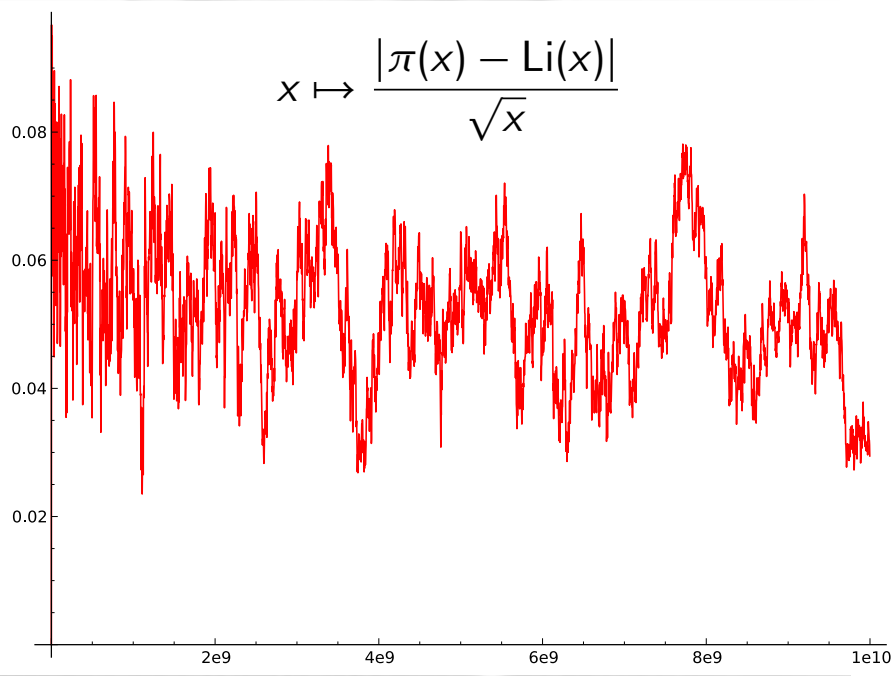
1. Si $\zeta(1+it) \neq 0$ pour tout $t \neq 0$, alors $\pi(x) \sim \dfrac{x}{\ln x}$.
2. Si ϑ est le sup des parties réelles de zéros de ξ, alors il existe une constante C telle que, pour tout $x \geqslant 2$ on a
$$|\pi(x) - \mathrm{Li}(x)| \leqslant C x^{\vartheta} \ln x.$$
3. En particulier, si l'hypothèse de Riemann est vraie, alors il existe une constante C telle que, pour tout $x \geqslant 2$ on a
$$|\pi(x) - \mathrm{Li}(x)| \leqslant C \sqrt{x} \ln x.$$

Compter les nombres premiers

De ζ à π

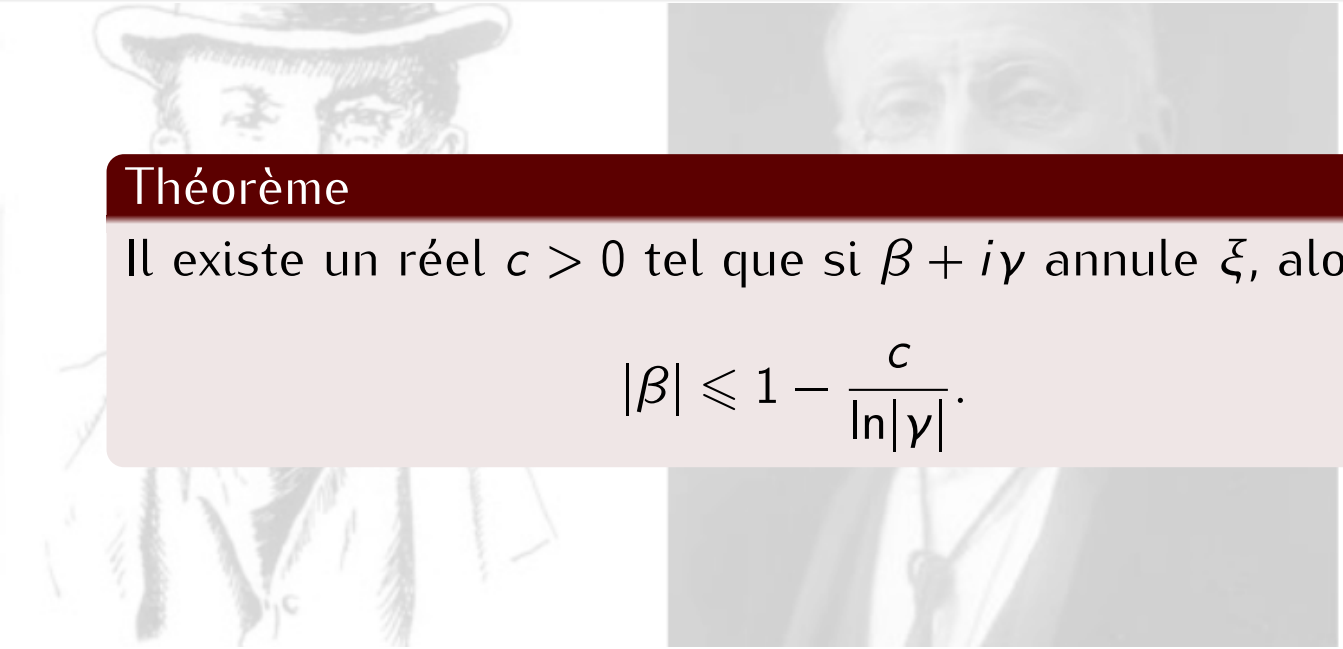
Si l'hypothèse de Riemann est vraie, alors il existe une constante C telle que, pour tout $x \geqslant 2$ on a

$$|\pi(x) - \mathrm{Li}(x)| \leqslant C\sqrt{x}\ln x.$$



Compter les nombres premiers

La première preuve : Hadamard et La Vallée Poussin (1896–1898)



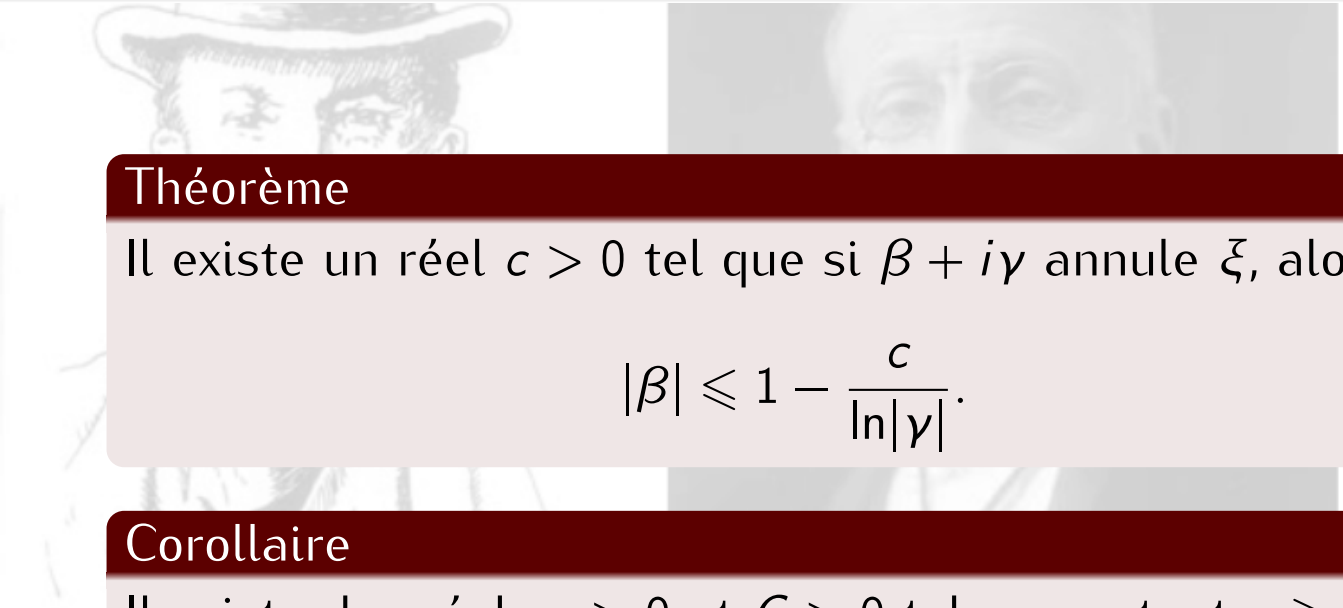
Théorème

Il existe un réel $c > 0$ tel que si $\beta + i\gamma$ annule ξ, alors

$$|\beta| \leqslant 1 - \frac{c}{\ln|\gamma|}.$$

Compter les nombres premiers

La première preuve : Hadamard et La Vallée Poussin (1896–1898)



Théorème

Il existe un réel $c > 0$ tel que si $\beta + i\gamma$ annule ξ, alors

$$|\beta| \leqslant 1 - \frac{c}{\ln|\gamma|}.$$

Corollaire

Il existe des réels $a > 0$ et $C > 0$ tels, pour tout $x \geqslant 2$, on a

$$|\pi(x) - \mathrm{Li}(x)| \leqslant Cxe^{-a\sqrt{\ln x}}.$$

Compter les nombres premiers

Le meilleur résultat à ce jour : Korobov et La Vinogradov (1958)

Théorème

Il existe un réel $c > 0$ tel que si $\beta + i\gamma$ annule ξ, alors

$$|\beta| \leqslant 1 - \frac{c}{\ln|\gamma|^{2/3}(\ln\ln|\gamma|)^{1/3}}.$$

Compter les nombres premiers

Le meilleur résultat à ce jour : Korobov et La Vinogradov (1958)

Théorème

Il existe un réel $c > 0$ tel que si $\beta + i\gamma$ annule ξ, alors

$$|\beta| \leqslant 1 - \frac{c}{\ln|\gamma|^{2/3}(\ln\ln|\gamma|)^{1/3}}.$$

Corollaire

Il existe des réels $a > 0$ et $C > 0$ tels, pour tout $x \geqslant 2$, on a

$$|\pi(x) - \mathrm{Li}(x)| \leqslant Cxe^{-a\ln(x)^{3/5}/(\ln\ln x)^{1/5}}.$$

Un soupçon de matrices aléatoires

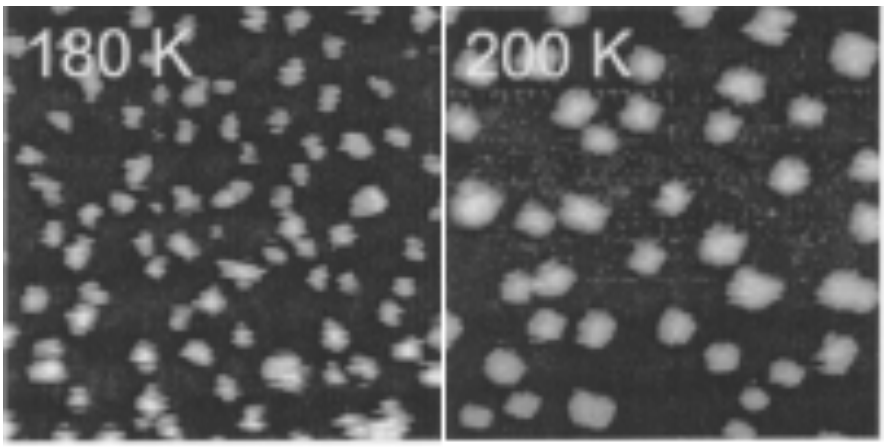
En physique

Les physiciens étudient la formation des atomes d'aluminium en îles.

Un soupçon de matrices aléatoires

En physique

Les physiciens étudient la formation des atomes d'aluminium en îles.

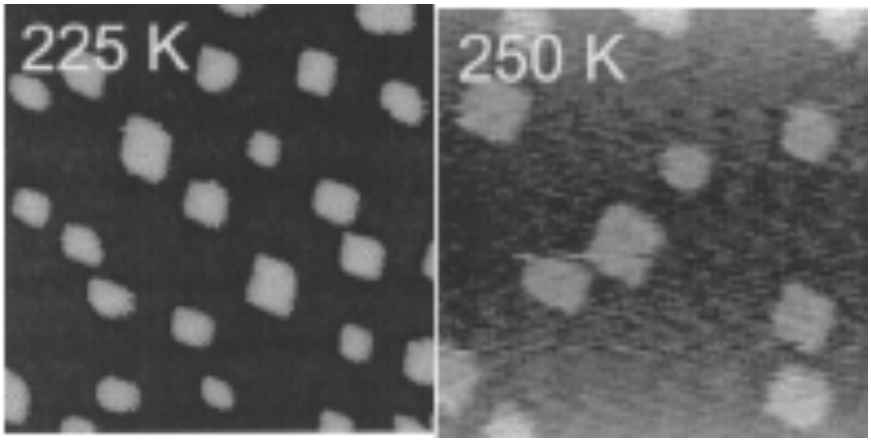


Frank, Wedler, Behm, Rottler, Maass, Caspersen, Stoldt, Thiel & Evans, Physical Review B 66 155435 (2002).

Un soupçon de matrices aléatoires

En physique

Les physiciens étudient la formation des atomes d'aluminium en îles.

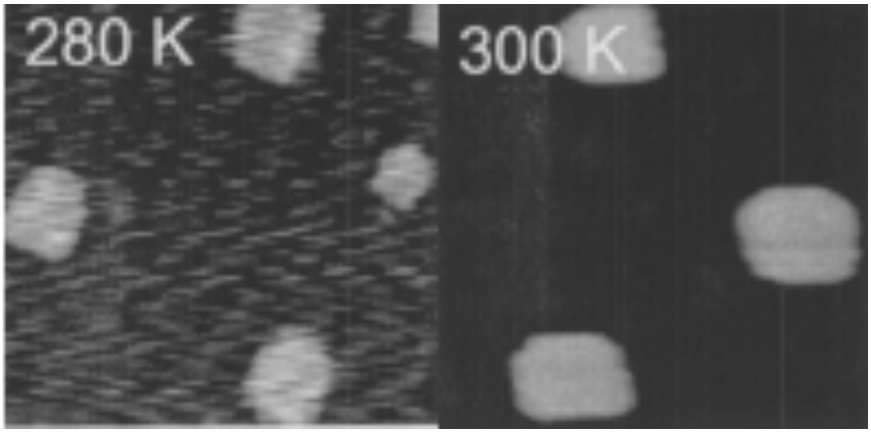


Frank, Wedler, Behm, Rottler, Maass, Caspersen, Stoldt, Thiel & Evans, Physical Review B 66 155435 (2002).

Un soupçon de matrices aléatoires

En physique

Les physiciens étudient la formation des atomes d'aluminium en îles.

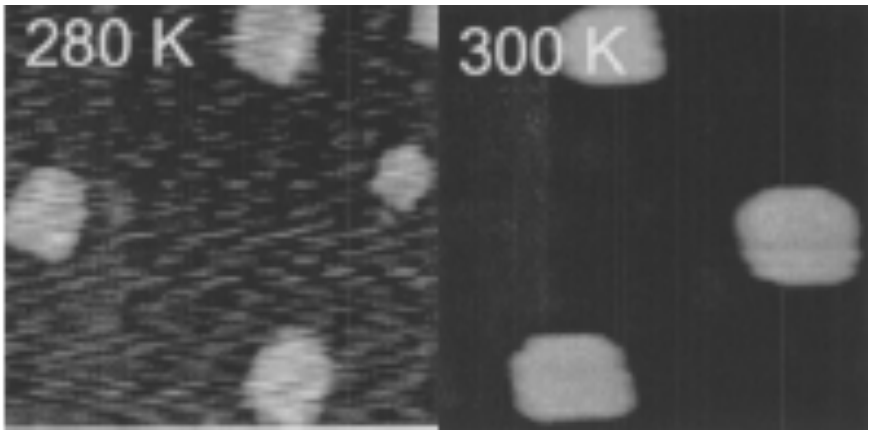


Frank, Wedler, Behm, Rottler, Maass, Caspersen, Stoldt, Thiel & Evans, Physical Review B 66 155435 (2002).

Un soupçon de matrices aléatoires

En physique

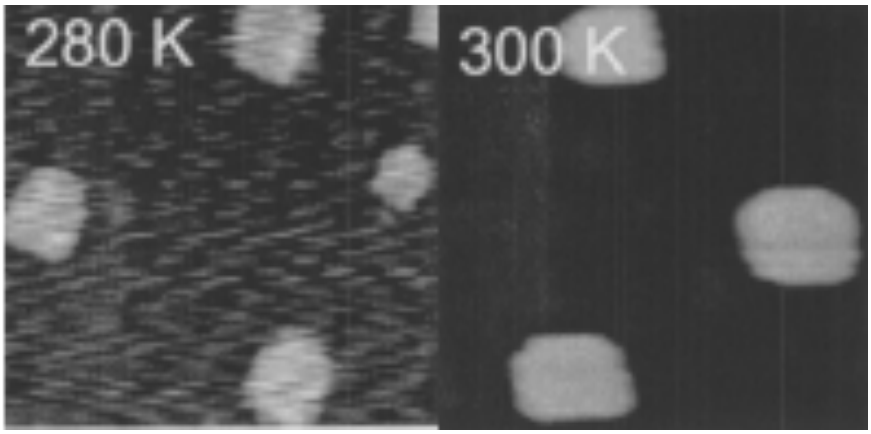
Chaque île définit une zone de capture : tout nouvel atome dans la zone de capture d'une île est capté par cette île.



Un soupçon de matrices aléatoires

En physique

Chaque île définit une zone de capture : tout nouvel atome dans la zone de capture d'une île est capté par cette île.

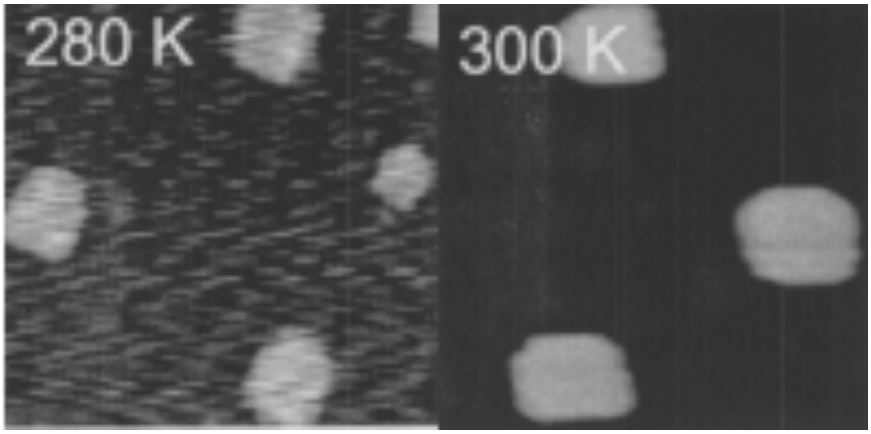


La taille de la zone de capture est, en quelque sorte, la distance à l'île la plus proche.

Un soupçon de matrices aléatoires

En physique

On étudie alors la distribution des tailles de zone de capture : combien en existe-t'il dont la taille est inférieure à une taille donnée ?



Un soupçon de matrices aléatoires

En théorie des nombres

Les arithméticiens étudient les zéros de ζ.

Les physiciens étudient la formation des atomes d'aluminium en îles.

Un soupçon de matrices aléatoires

En théorie des nombres

Les arithméticiens étudient les zéros de ζ.
Les physiciens étudient la formation des atomes d'aluminium en îles.
Chaque zéro définit une distance au plus proche : c'est la distance au plus proche des autres zéros de ζ.
Chaque île définit une zone de capture.

Un soupçon de matrices aléatoires

En théorie des nombres

Les arithméticiens étudient les zéros de ζ.
Les physiciens étudient la formation des atomes d'aluminium en îles.
Chaque zéro définit une distance au plus proche : c'est la distance au plus proche des autres zéros de ζ.
Chaque île définit une zone de capture.
Les arithméticiens étudient la distribution des distances au plus proche : combien de zéros sont distants de moins qu'une distance donnée d'un autre zéro de ζ ?
Les physiciens étudient la distribution des tailles des zones de capture

Un soupçon de matrices aléatoires

Universalité

Les distributions trouvées par les arithméticiens et les physiciens sont les mêmes !