Dîner avec les nombres premiers

Collège Stanislas, Montréal

Emmanuel Royer

Laboratoire international de recherches mathématiques
CRM - CNRS, IRL3457
CNRS & CRM
Montréal, Québec, Canada

12 février 2025

Qu'est-ce qu'un nombre premier ?

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

▸▸ Pas trop de topologie...

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. Pour tous entiers $a \geqslant 0$ et $b > 0$, on note $N_{a,b}$ l'ensemble des entiers congrus à a modulo b, c'est-à-dire : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$. Par exemple l'ensemble $N_{0,p}$ des multiples d'un entier p est ouvert

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$
3. Par exemple, $N_{a,b}$ est ouvert si $a + bm \in N_{a,b}$, alors $N_{a,b}$ contient $N_{a+bm,b}$ puisque les éléments de $N_{a+bm,b}$ sont de la forme $a + bm + bn = a + b(m + n)$ et donc dans $N_{a,b}$

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$
3. Par exemple, $N_{a,b}$ est ouvert
4. La réunion d'ensembles ouverts est un ouvert : si un ensemble contient un ensemble $N_{a,b}$ pour tout $a \geqslant 0$, cela reste vrai si j'ajoute des éléments à cet ensemble

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$
3. Par exemple, $N_{a,b}$ est ouvert
4. La réunion d'ensembles ouverts est un ouvert
5. Par exemple $N_{a+1,b} \cup \cdots \cup N_{a+b-1,b}$ est ouvert : en effet, $N_{a,b}$ est infini

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$
3. Par exemple, $N_{a,b}$ est ouvert
4. La réunion d'ensembles ouverts est un ouvert
5. Par exemple $N_{a+1,b} \cup \cdots \cup N_{a+b-1,b}$ est ouvert
6. L'intersection d'un nombre fini d'ouverts est un ouvert : si N_{a,b_1} est inclus dans $\mathcal{O}_1$ et si N_{a,b_2} est inclus dans $\mathcal{O}_2$ alors N_{a,b_1} est inclus dans $\mathcal{O}_1 \cap \mathcal{O}_2$

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

1. $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$
2. On appelle ouvert tout ensemble qui est soit vide soit vérifie la propriété suivante : si a est dans cet ensemble, il contient au moins un ensemble $N_{a,b}$
3. Par exemple, $N_{a,b}$ est ouvert
4. La réunion d'ensembles ouverts est un ouvert
5. Par exemple $N_{a+1,b} \cup \cdots \cup N_{a+b-1,b}$ est ouvert
6. L'intersection d'un nombre fini d'ouverts est un ouvert
7. Un ensemble ouvert est soit vide soit infini.

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7 On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert
9. Par exemple $\mathbb{Z} \setminus \left(N_{a+1,b} \cup \cdots \cup N_{a+b-1,b}\right)$ est fermé. Or modulo b, tout entier vaut soit a, soit $a+1$, soit..., soit $a+b-1$ et donc $\mathbb{Z} \setminus \left(N_{a+1,b} \cup \cdots \cup N_{a+b-1,b}\right) = N_{a,b}$. Ainsi, $N_{a,b}$ est fermé

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert
9. $N_{a,b}$ est fermé
10. Une réunion d'un nombre fini de fermés est fermée : $(Z \setminus \mathcal{O}_1) \cup (Z \setminus \mathcal{O}_2) = \mathbb{Z} \setminus (\mathcal{O}_1 \cap \mathcal{O}_2)$

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert
9. $N_{a,b}$ est fermé
10. Une réunion d'un nombre fini de fermés est fermée
11. $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}$: tout nombre premier différent de -1 ou 1 admet un diviseur premier donc $\{-1, 1\} = \mathbb{Z} \setminus \bigcup_{p \in \mathcal{P}} N_{0,p}$

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert
9. $N_{a,b}$ est fermé
10. Une réunion d'un nombre fini de fermés est fermée
11. $\{-1,1\} = \mathbb{Z} \setminus \bigcup_{p\in\mathcal{P}} N_{0,p}$
12. S'il n'y a qu'un nombre fini de nombres premiers, alors $\bigcup_{p\in\mathcal{P}} N_{0,p}$ est une réunion finie de fermés, c'est donc un fermé et donc $\{-1,1\}$ est un ouvert

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Une infinité de nombres premiers

Une preuve... topologique (Fürstenberg, 1955)

7. On appelle fermé tout ensemble qui est obtenu en retirant à $\mathbb{Z}$ un ensemble ouvert
8. En retirant à $\mathbb{Z}$ un ensemble fermé on obtient donc un ensemble ouvert
9. $N_{a,b}$ est fermé
10. Une réunion d'un nombre fini de fermés est fermée
11. $\{-1,1\} = \mathbb{Z} \setminus \bigcup_{p \in \mathcal{P}} N_{0,p}$
12. S'il n'y a qu'un nombre fini de nombres premiers, $\{-1,1\}$ est un ouvert
13. Mais, $\{-1,1\}$ n'est ni vide, ni infini.

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

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.

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Construire des premiers est compliqué

Quelles méthodes connaissez-vous ?

Construire des premiers est compliqué

Quelles méthodes connaissez-vous ?

Divisions successives par les entiers inférieurs

Crible d'Eratsothène
(3^{e} siècle avant notre ère)

Érathostène enseignant à Alexandrie par Bernardo Strozzi (1581–1644) (inv. 1959.1225)
Avec l'aimable autorisation du Musée des Beaux-Arts de Montréal

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Construire des premiers est compliqué

Tests de primalité

Les meilleurs tests de primalité... n'en sont pas tout à fait

Ils sont comme des filtres qui laissent passer tous les nombres premiers, retiennent la plupart des nombres non premiers mais en laissent passer quelques un. Seulement très peu et de très grands seulement.

Ces tests reposent sur les remarques suivantes, liées au petit théorème de Fermat.

Petit théorème de Fermat

Si p est un nombre premier et si a est un entier premier à p, alors $a^{p-1} - 1$ est un multiple de p :

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

Construire des premiers est compliqué

Tests de primalité

Petit théorème de Fermat (∗)

Si p est un nombre premier alors $a^p - a$ est un multiple de p pour tout entier a :

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

Construire des premiers est compliqué

Tests de primalité

Petit théorème de Fermat (*)

Si p est un nombre premier alors $a^p - a$ est un multiple de p pour tout entier a :

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

Question

La réciproque est-elle vraie ? Un entier n vérifiant $a^n \equiv a \pmod{n}$ pour tout a est-il premier ?

Nombre de Carmichael

Un entier n non premier vérifiant $a^n \equiv a \pmod{n}$ pour tout a s'appelle un nombre de Carmichael.

Construire des premiers est compliqué

Tests de primalité

Imaginons donc un « grand » filtre construit à partir de plusieurs « petits » filtres superposés, chaque petit filtre ayant pour numéro une valeur de a entre 1 et $n-1$:

1. pour chaque valeur de a , l'entier n passe le petit filtre numéro a si n divise $a^n - a$;
2. dès qu'on a trouvé une valeur de a pour laquelle n ne passe pas le petit filtre numéro a, on sait que cet entier n ne passe pas le grand filtre et on arrête les calculs ;
3. si n passe tous les petits filtres, alors il passe le grand filtre.

Efficacité

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Construire des premiers est compliqué

Tests de primalité

Imaginons donc un « grand » filtre construit à partir de plusieurs « petits » filtres superposés, chaque petit filtre ayant pour numéro une valeur de a entre 1 et $n-1$. Un entier qui passe le grand filtre est :

- soit un nombre premier ;
- soit un nombre de Carmichael (un escroc qui se prétend premier mais ne l'est pas...).

Existe-t-il beaucoup de nombres de Carmichael ?

Construire des premiers est compliqué

Tests de primalité

ChatGPT 4.1

CRM-CNRS
International Research Lab

cnrs

Construire des premiers est compliqué

Nombres de Carmichael

Nombre de Carmichael

Un entier n vérifiant $a^n \equiv a \pmod{n}$ pour tout a s'appelle un nombre de Carmichael.

Alford, Granville et Pomerance (1994)

Il existe une infinité de nombre de Carmichael : la réciproque du théorème de Fermat est fausse une infinité de fois.

Les plus petits nombres de Carmichael sont 561, 1105, 1729, 2645, 2821, 6601, 8911...

Construire des premiers est compliqué

Nombres de Carmichael

Annals of Mathematics, 140 (1994), 703–722

There are infinitely many Carmichael numbers

By W.R. Alford, Andrew Granville and Carl Pomerance*

Dedicated to Paul Erdős on the occasion of his 80th birthday

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Le plus grand connu

Le plus grand nombre premier connu est depuis 2024 le nombre

$$p = 2^{136\ 279\ 841} - 1.$$

Ce nombre a 41 024 320 chiffres décimaux.

« L'essor des GPU. Ce nombre premier marque la fin d'une ère de 28 ans durant laquelle des ordinateurs personnels ordinaires étaient capables de découvrir ces immenses nombres premiers. [...] Au moment de la découverte, son « superordinateur cloud » comprenait des milliers de GPU de serveurs répartis sur 24 centres de données, dans 17 pays. Après près d'un an de tests, Luke a enfin trouvé le nombre premier tant recherché. Le 11 octobre, un GPU NVIDIA A100 basé à Dublin, en Irlande, a signalé que M136279841 était probablement premier. Le 12 octobre, un NVIDIA H100 situé à San Antonio, Texas, USA, a confirmé la primalité à l'aide du test de Lucas-Lehmer. ». Avis personnel

`https://www.mersenne.org/primes/?press=M136279841`

Couloir entre deux rangées du supercalculateur Jean Zay

CENTRE DE RECHERCHES MATHÉMATIQUES — CRM-CNRS International Research Lab — cnrs

Compter les nombres premiers

Une infinité, oui mais...

x	Premiers inférieurs à x
100	25
1000	168
10000	1229
100000	9592
1000000	78498
10000000	664579
100000000	5761455
1000000000	50847534
10000000000	455052511
100000000000	4118054813
1000000000000	37607912018

Compter les nombres premiers

Une infinité, oui mais...

x	Premiers inférieurs à x	Proportion
100	25	0,250
1000	168	0,168
10000	1229	0,123
100000	9592	0,096
1000000	78498	0,078
10000000	664579	0,066
100000000	5761455	0,058
1000000000	50847534	0,051
10000000000	455052511	0,046
100000000000	4118054813	0,041
1000000000000	37607912018	0,038

Compter les nombres premiers

Une infinité, oui mais...

x	Premiers inférieurs à x	Proportion	Proportion inverse
100	25	0,250	4,00
1000	168	0,168	5,95
10000	1229	0,123	8,14
100000	9592	0,096	10,43
1000000	78498	0,078	12,74
10000000	664579	0,066	15,05
100000000	5761455	0,058	17,36
1000000000	50847534	0,051	19,67
10000000000	455052511	0,046	21,98
100000000000	4118054813	0,041	24,28
1000000000000	37607912018	0,038	26,59

Compter les nombres premiers

Une infinité, oui mais...

x	Premiers inférieurs à x	Proportion	Proportion inverse	Écart
100	25	0,250	4,00	
1000	168	0,168	5,95	1,952
10000	1229	0,123	8,14	2,184
100000	9592	0,096	10,43	2,289
1000000	78498	0,078	12,74	2,314
10000000	664579	0,066	15,05	2,308
100000000	5761455	0,058	17,36	2,310
1000000000	50847534	0,051	19,67	2,310
10000000000	455052511	0,046	21,98	2,309
100000000000	4118054813	0,041	24,28	2,308
1000000000000	37607912018	0,038	26,59	2,307

Combien ?

Une infinité, oui mais...

Notons $\pi(x)$ le nombre de nombres premiers plus petits que x. La proportion des nombres premiers plus petits que x est

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

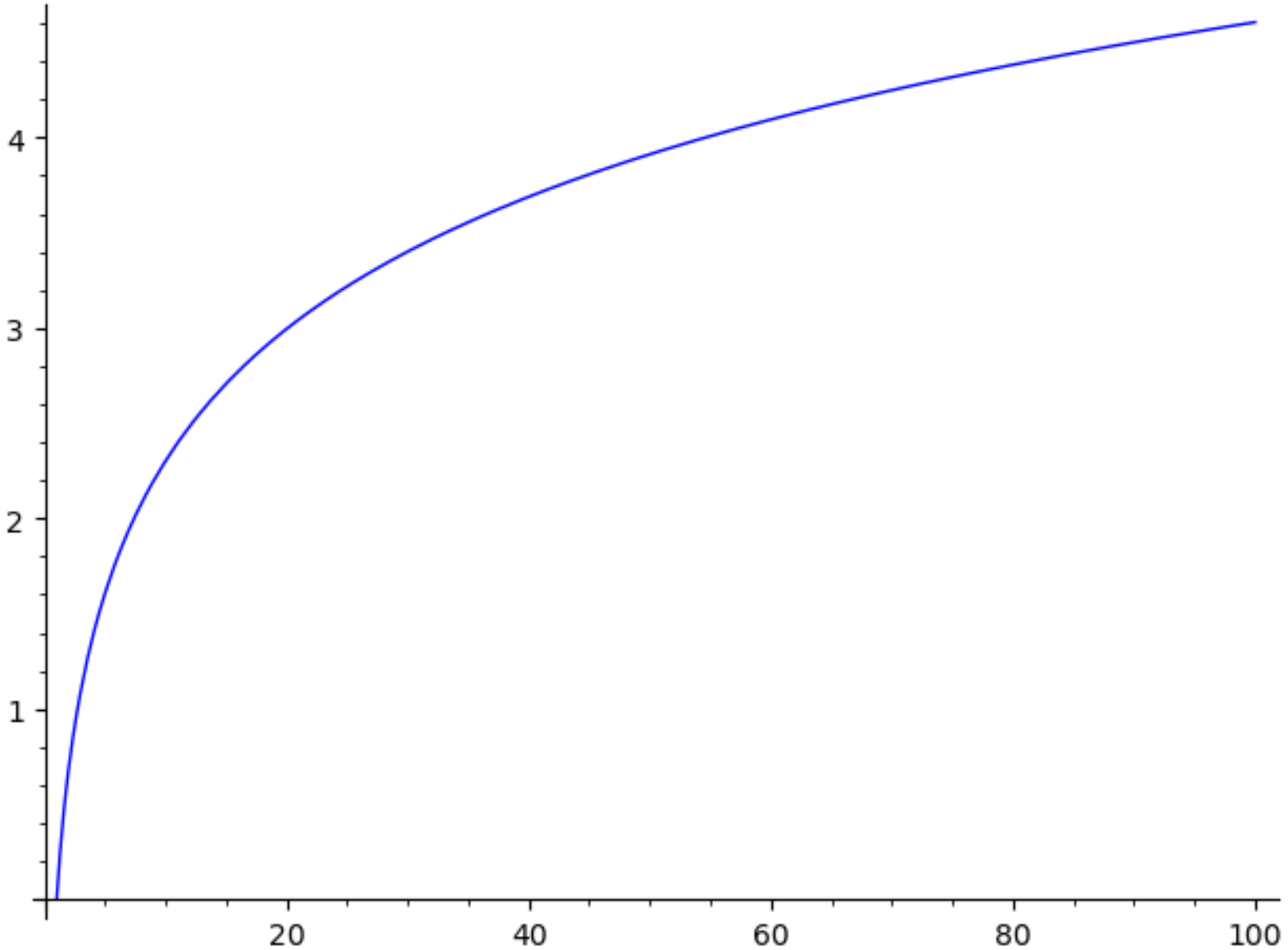
Le tableau précédent semble montrer que, lorsque x est suffisamment grand,

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

Il existe une fonction qui a cette propriété : la fonction logarithme, qu'on note ln.

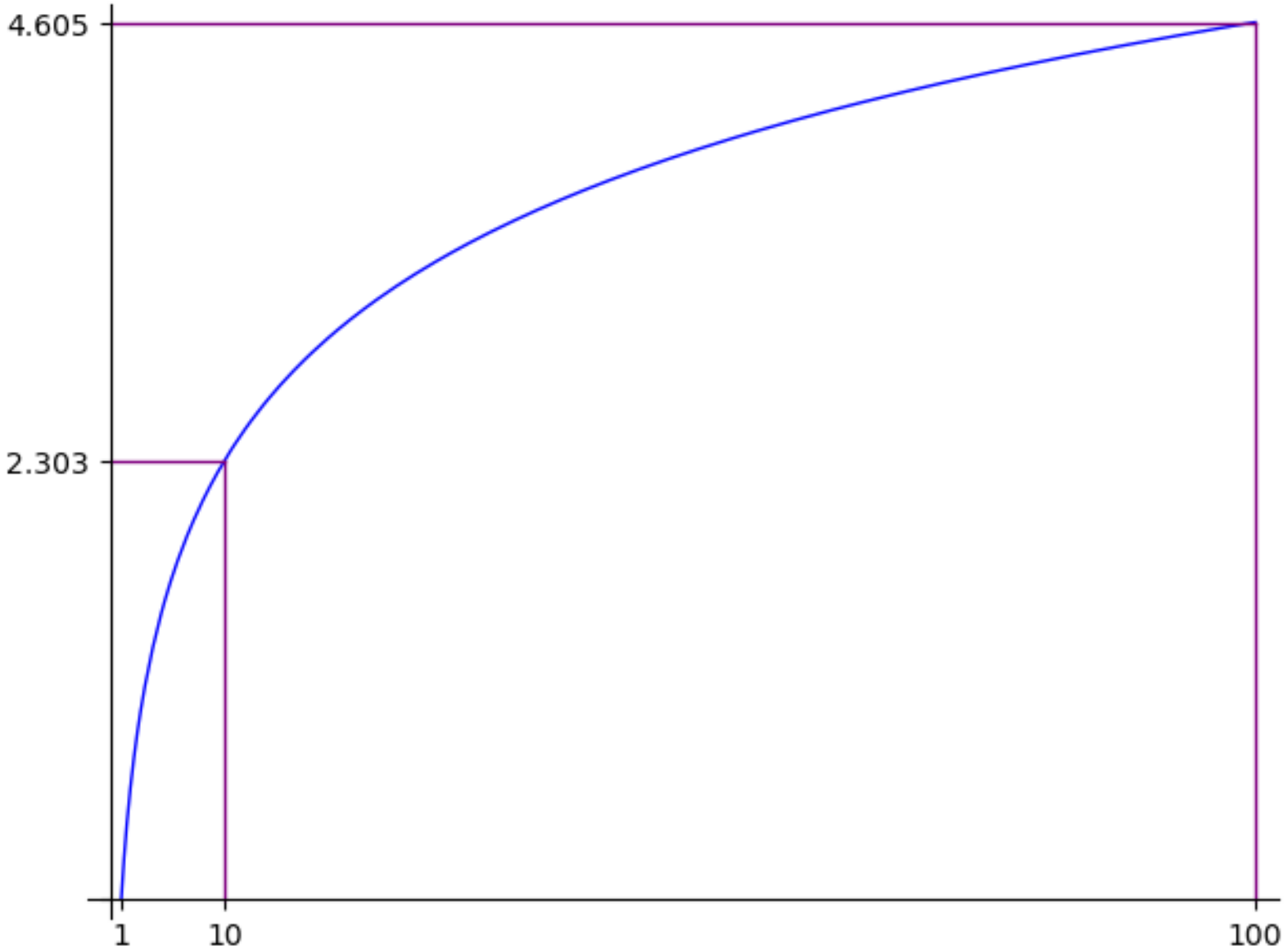
Combien ?

Une infinité, oui mais...



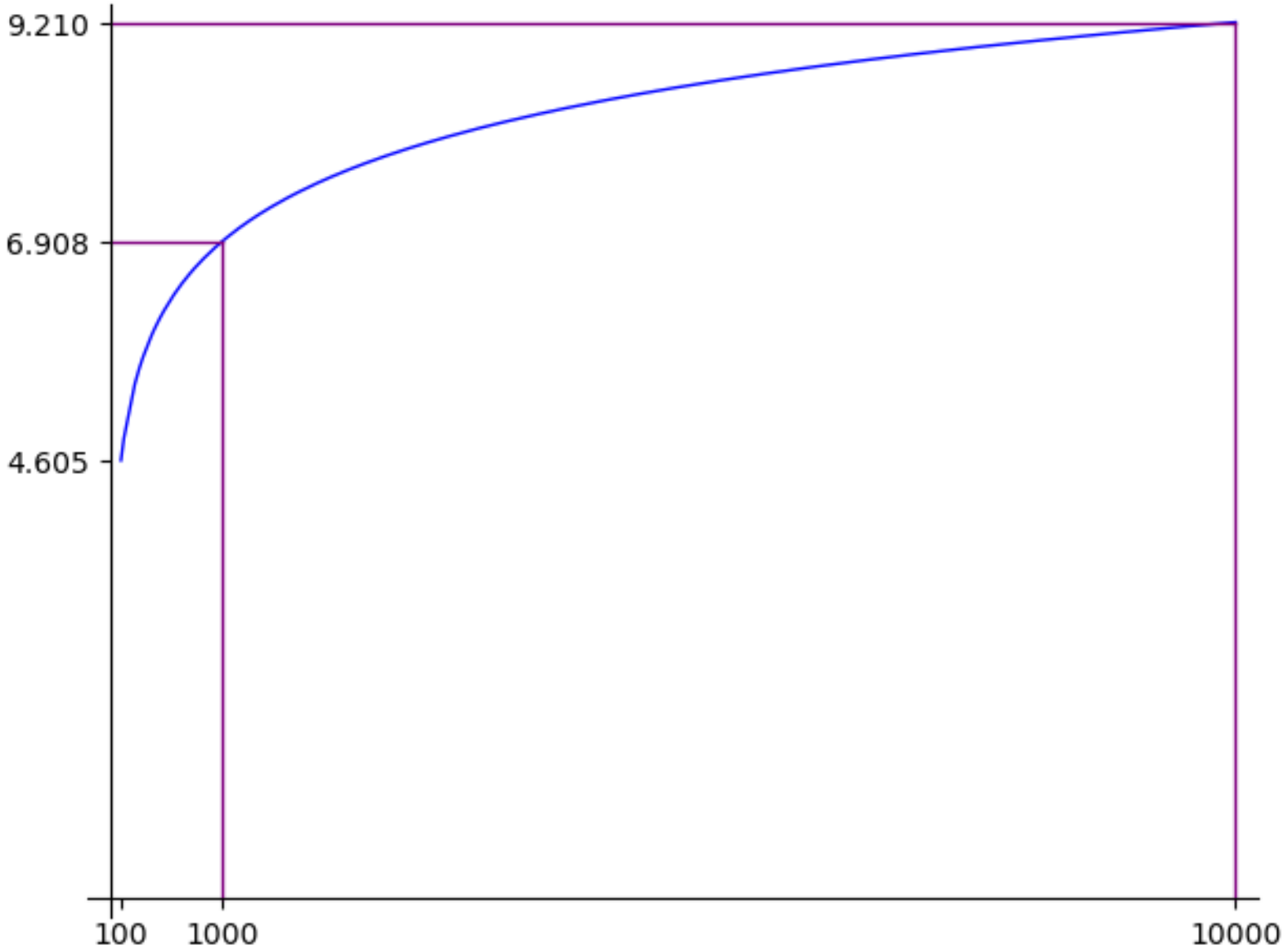
Combien ?

Une infinité, oui mais...



Combien ?

Une infinité, oui mais...



Combien ?

Une estimation du jeune Gauss...

Il semble donc que le rapport du nombre de nombres premiers inférieurs à x et de $\frac{x}{\ln x}$ se rapproche de 1 quand x grandit :

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

Combien ?

Une estimation du jeune Gauss...

Il semble donc que le rapport du nombre de nombres premiers inférieurs à x et de $\frac{x}{\ln x}$ se rapproche de 1 quand x grandit :

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

Gauss a donné cette approximation en 1792, il avait 15 ans !

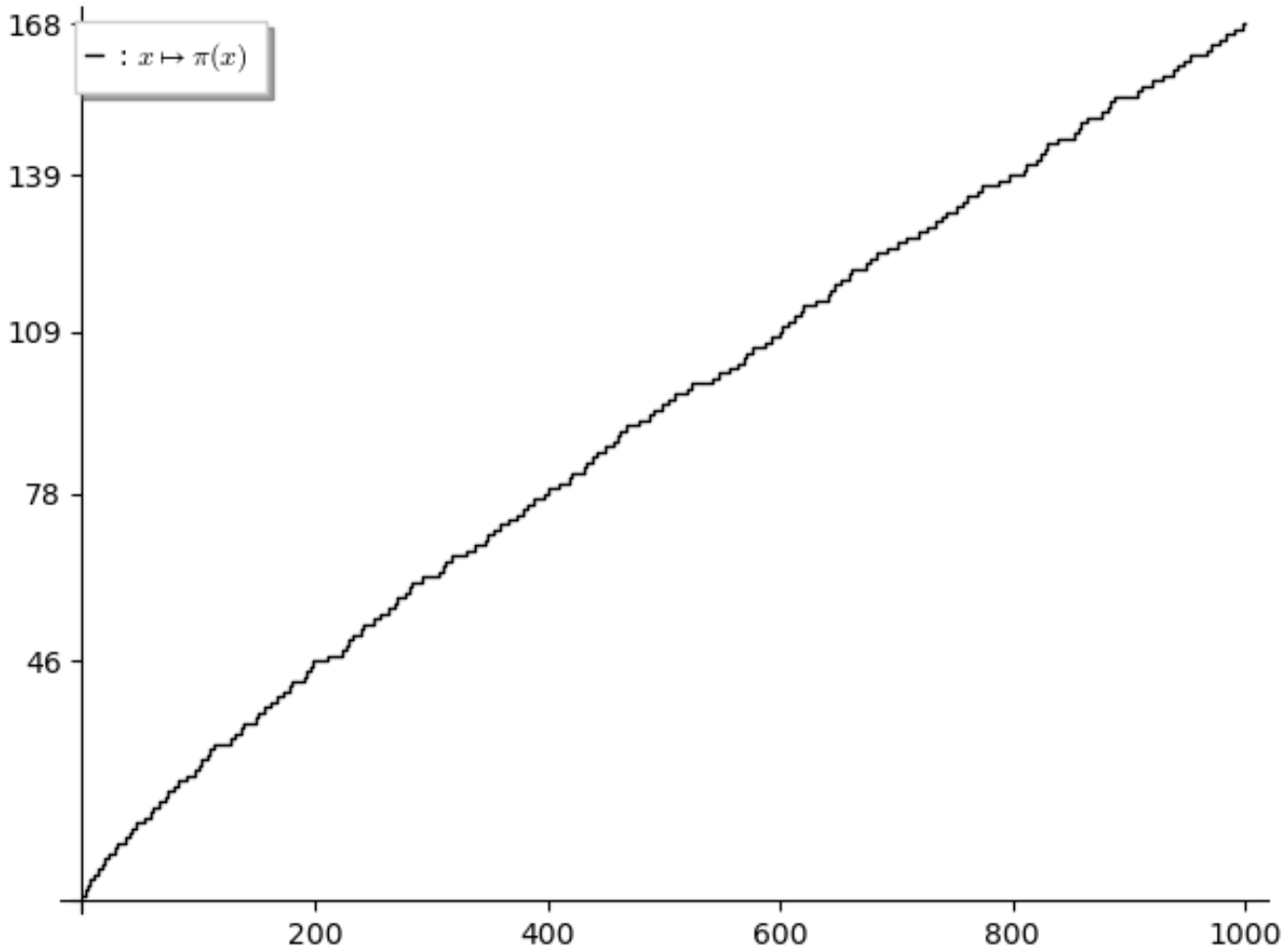
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du jeune Gauss...



$$x \mapsto \pi(x)$$

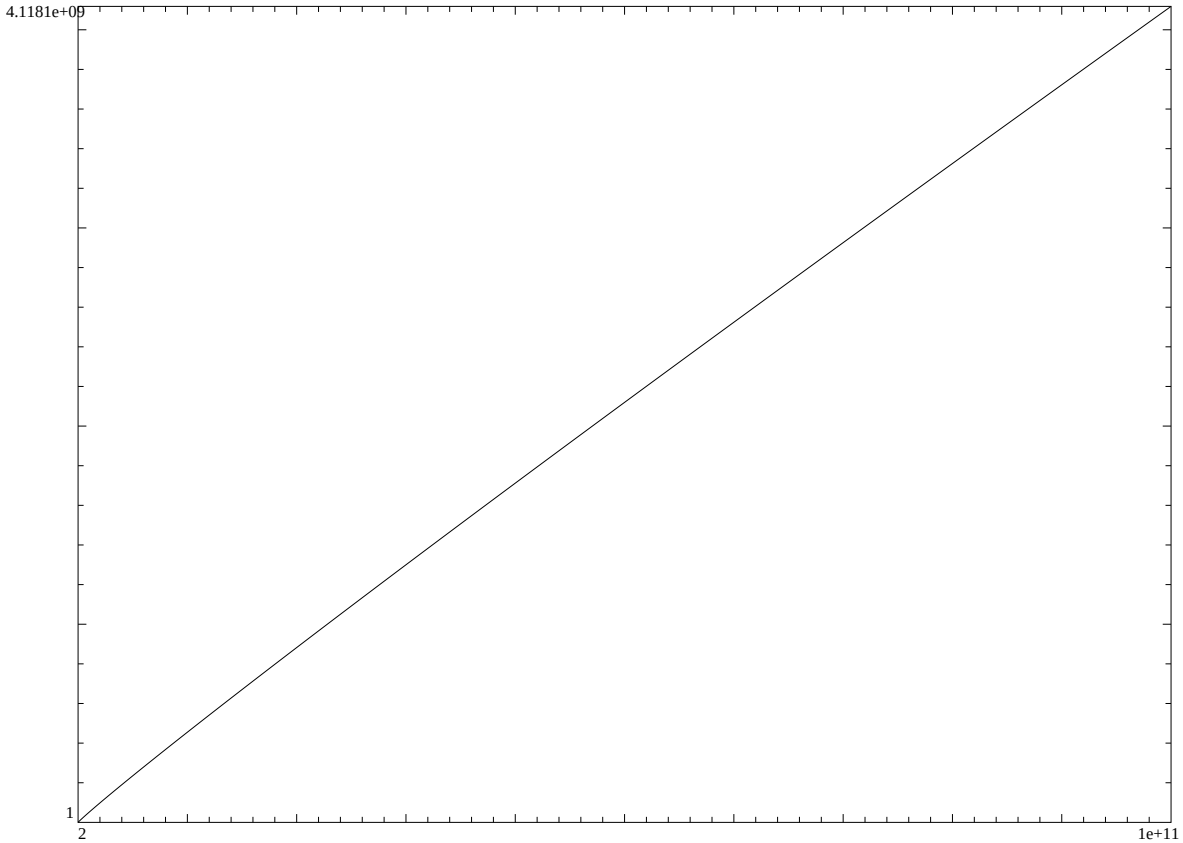
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du jeune Gauss...



$$x \mapsto \pi(x)$$

$$(x \leqslant 10^{11})$$

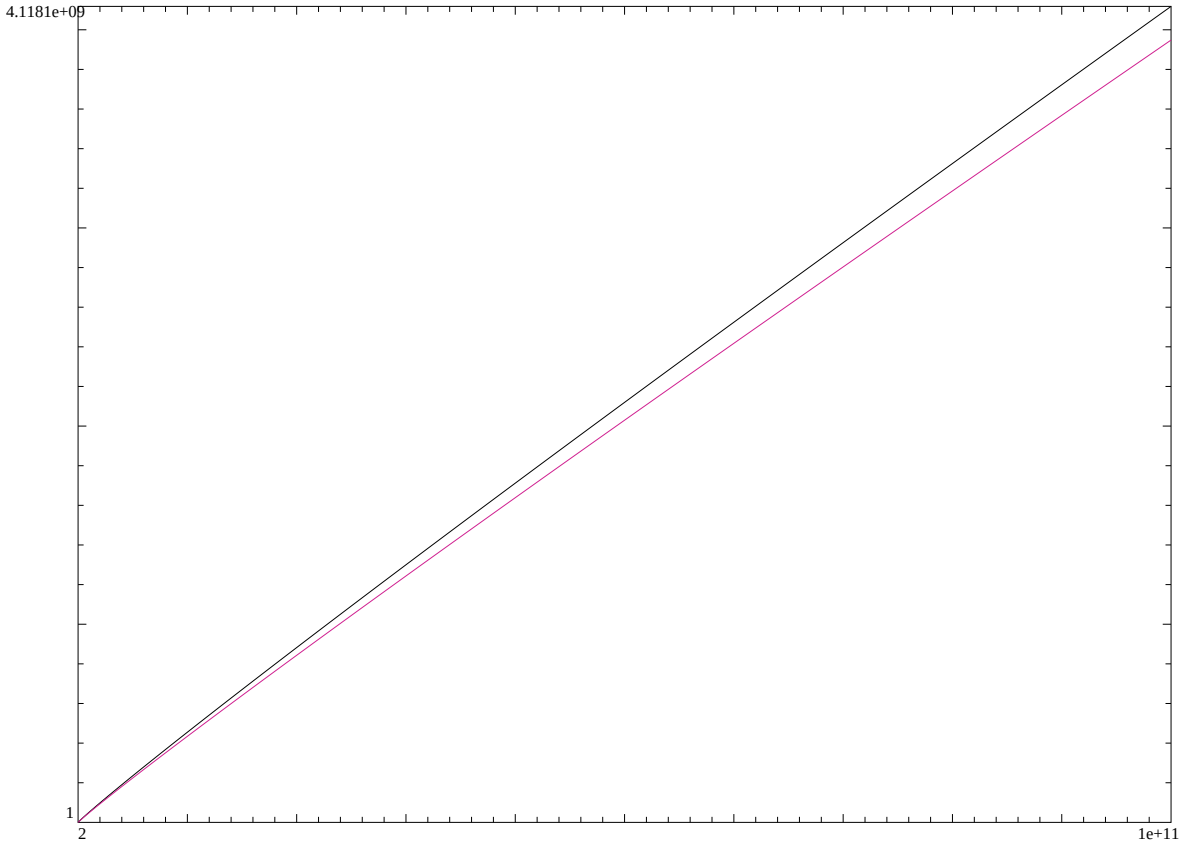
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du jeune Gauss...



$$x \mapsto \pi(x)$$

$$(x \leqslant 10^{11})$$

$$x \mapsto x/\ln(x)$$

HdlVP

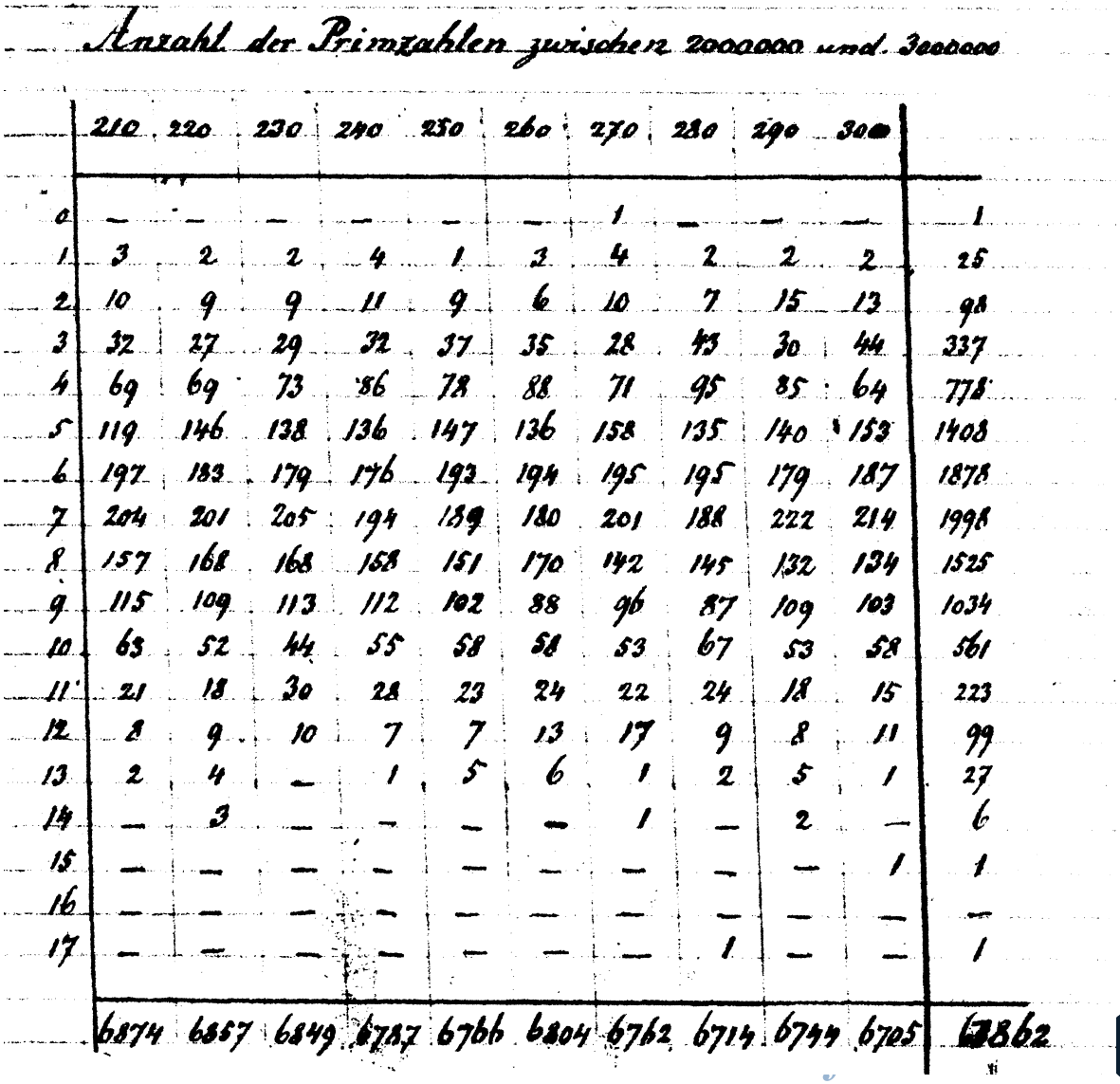
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Une estimation 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	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

CRM-CNRS International Research Lab

Combien ?

Une estimation du vieux Gauss...

und ich habe (da ich zu einer anhaltenderen 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 ~~Dec~~ December 1849

Stets der Ihrige
C. F. Gauss

Combien ?

Une estimation du vieux Gauss...

Le « vieux » Gauss (64 ans) conjecture donc que le nombre de nombres premiers inférieurs à x est bien approché par la surface sous la courbe de $t \mapsto \frac{1}{\ln t}$ entre 2 et x.

Combien ?

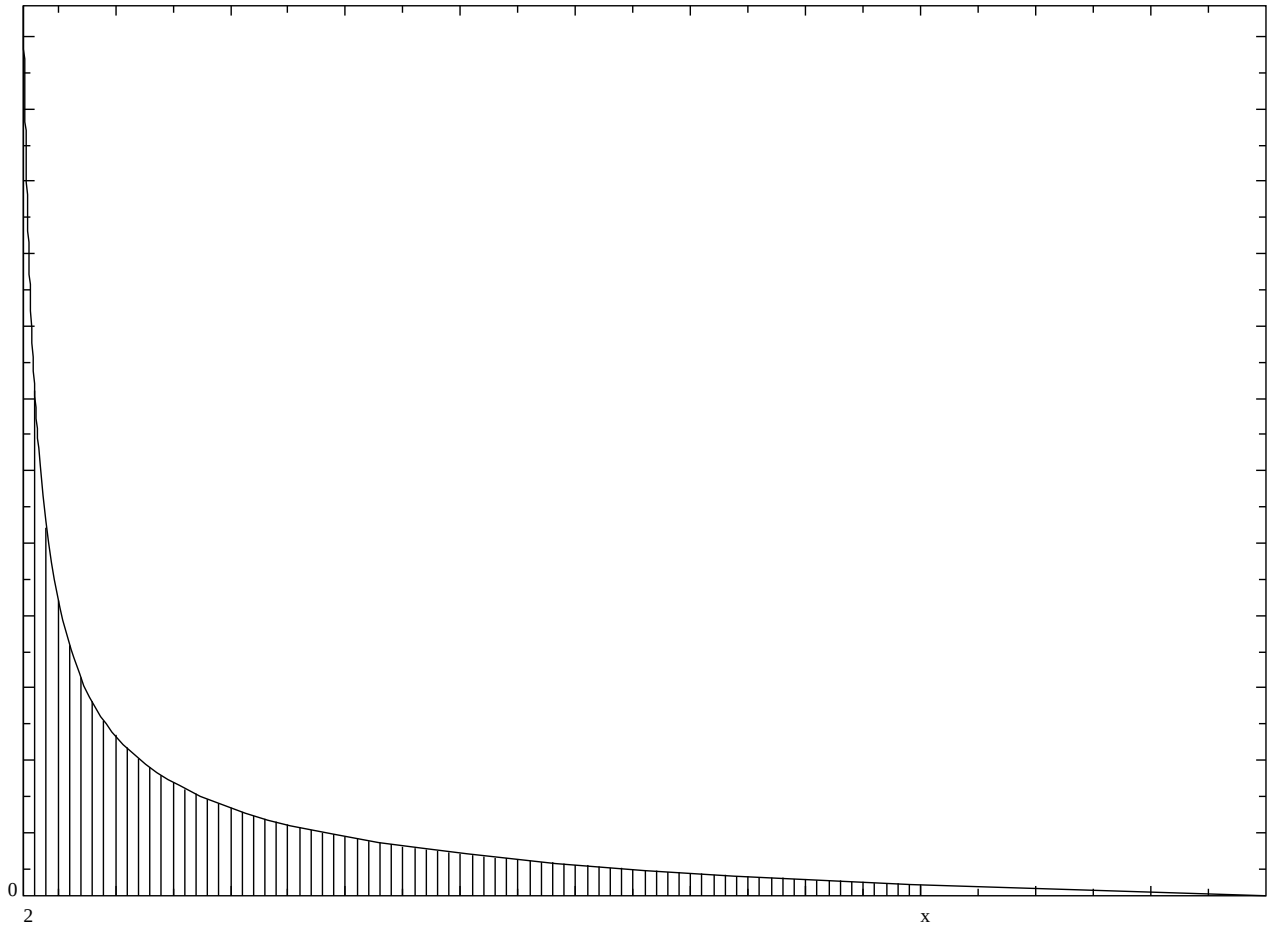
Une estimation du vieux Gauss...

Le « vieux » Gauss (64 ans) conjecture donc que le nombre de nombres premiers inférieurs à x est bien approché par la surface sous la courbe de $t \mapsto \frac{1}{\ln t}$ entre 2 et x.

$$\pi(x) \sim \int_2^x \frac{1}{\ln t} \mathrm{d}t.$$

Combien ?

Une estimation du vieux Gauss...



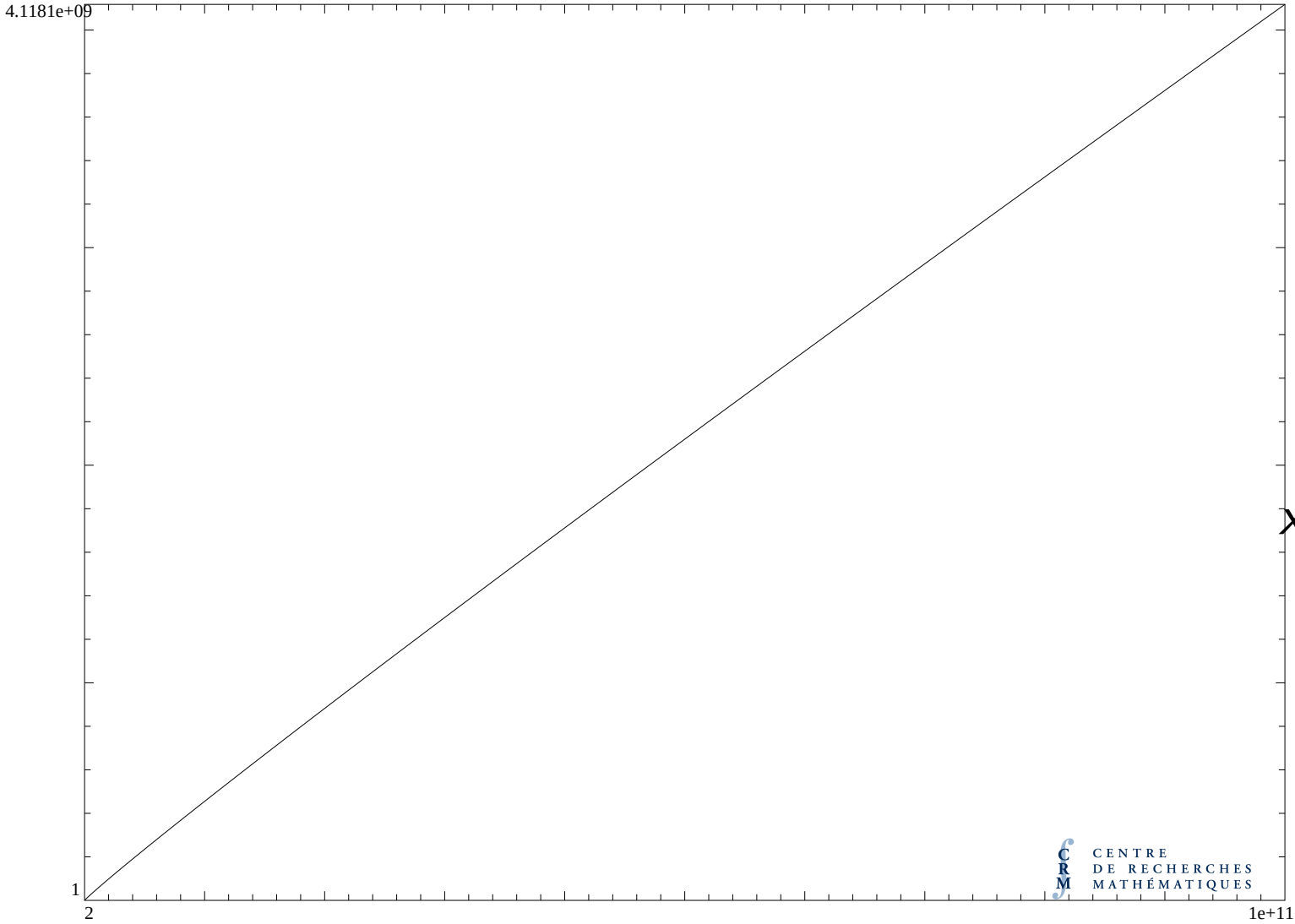
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du vieux Gauss...



$x \mapsto \pi(x)$

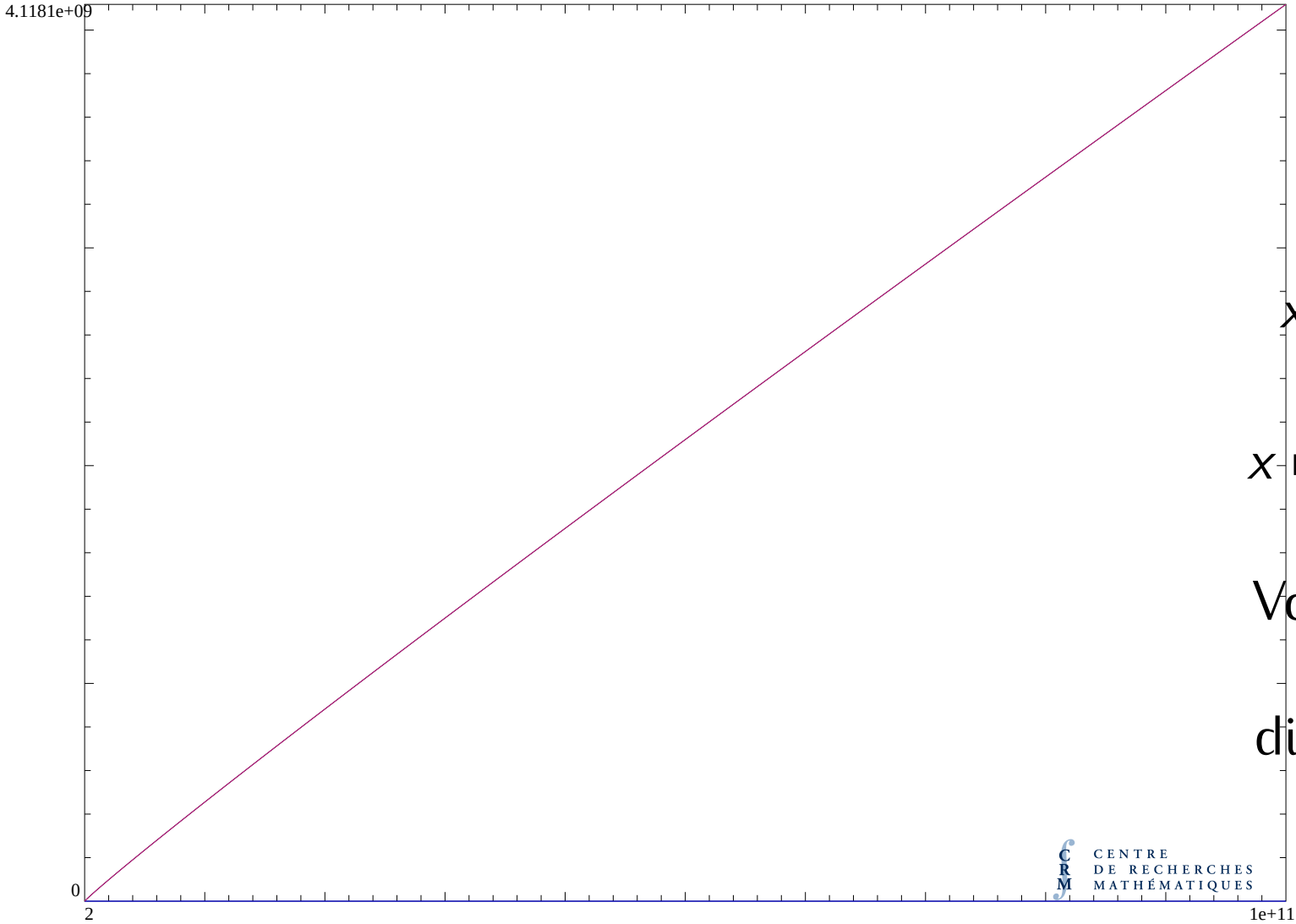
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du vieux Gauss...



$$x \mapsto \pi(x)$$

$$x \mapsto \int_2^x \frac{\mathrm{d}t}{\ln(t)}$$

Voyez-vous une différence ?

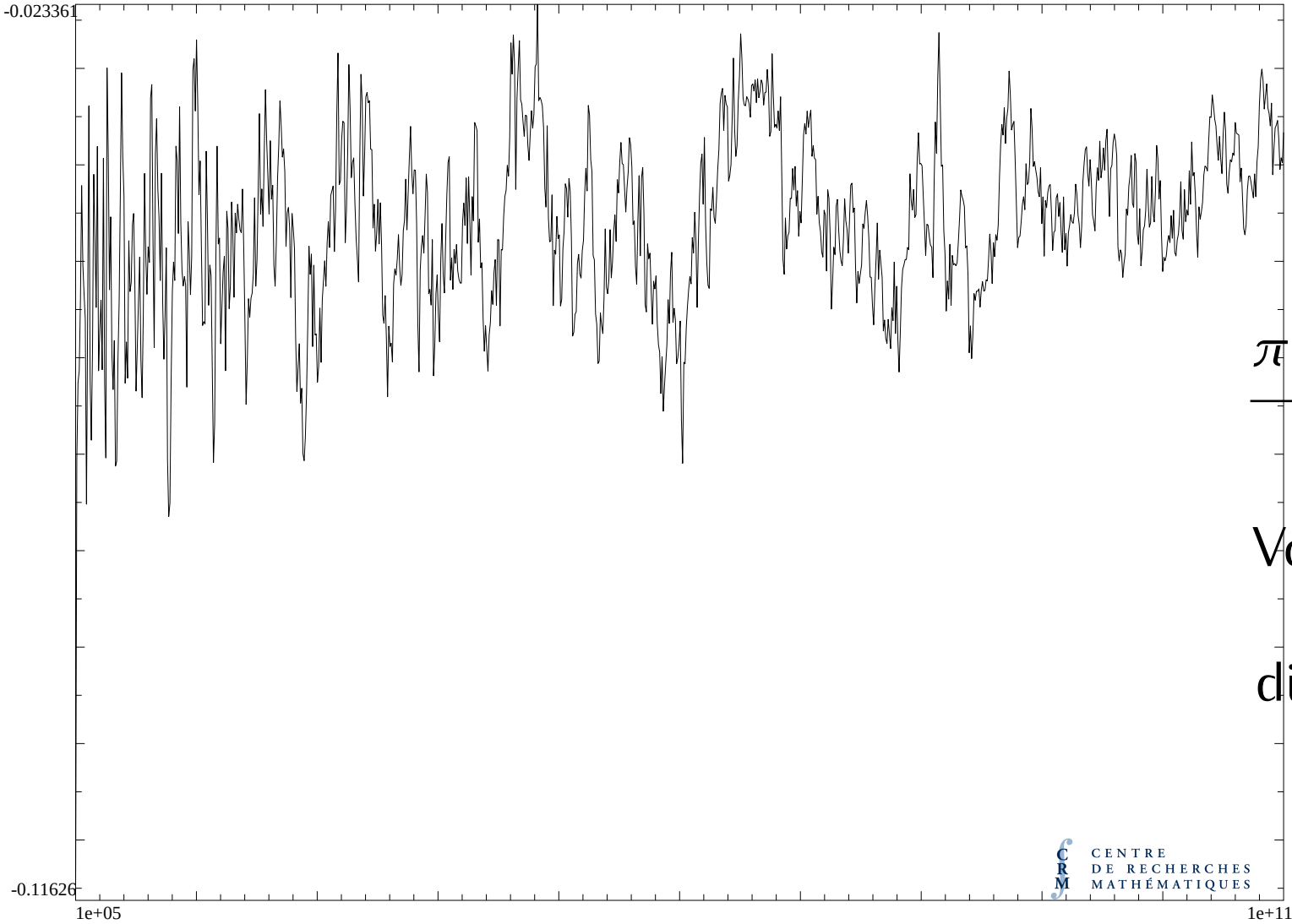
CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Qualité de l'estimation du vieux Gauss...



$$\frac{\pi(x) - \int_2^x \frac{dt}{\ln(t)}}{\sqrt{x}}$$

Vous voyez une différence !

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Le théorème de Hadamard et De La Vallée Poussin (1896)

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Combien ?

Le théorème de Hadamard et De La Vallée Poussin (1896)

Le résultat conjecturé par Gauss en 1849 a été démontré par Hadamard et De La Vallée Poussin en 1896.

Ils ont montré que $\pi(x)$ est bien approchée par $\int_2^x \frac{\mathrm{d}t}{\ln(t)}$ et ont donné une estimation de l'erreur.

Un thème de recherche (un défi majeur !) de la théorie analytique des nombres est d'améliorer ce terme d'erreur.

Germain

Un nouveau défi

Les nombres premiers jumeaux

Si $2 < p < q$ sont deux nombres premiers alors, ils sont tous deux impairs et leur différence vaut au moins 2.

Il existe des couples de nombres premiers entre eux vaut 2 :

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61)$$

ou encore

$$(10000139, 10000141),\ (10000451, 10000453),\ (10000721, 10000723)$$

Un nouveau défi

Les nombres premiers jumeaux

Existe-t-il une infinité de couples de nombres premiers (p, q) avec $q - p \leqslant 2$?

Personne ne sait encore répondre : on conjecture que oui.

Alors on simplifie et, on cherche à avoir le plus petit entier m pour lequel on sait démontrer qu'il existe une infinité de couples de nombres premiers (p, q) avec

$$q - p \leqslant m.$$

Un nouveau défi

Les nombres premiers jumeaux

James Maynard a obtenu la médaille Fields en 2022 pour avoir démontré l'existence d'une infinité de couples de nombres premiers (p, q) avec

$$q - p \leqslant 600.$$

Un nouveau défi

Les nombres premiers jumeaux

James Maynard a obtenu la médaille Fields en 2022 pour avoir démontré l'existence d'une infinité de couples de nombres premiers (p, q) avec

$$q - p \leqslant 600.$$

CRM-CNRS International Research Lab

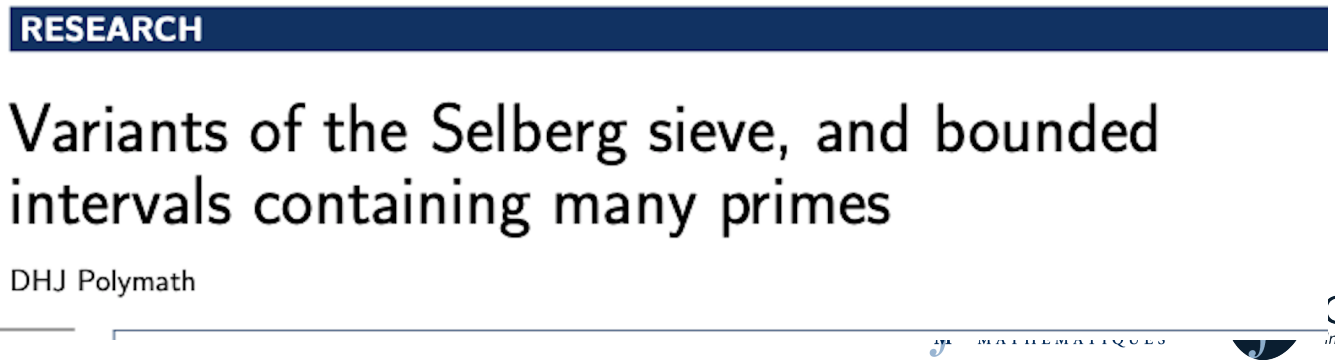
Un nouveau défi

Les nombres premiers jumeaux

James Maynard a obtenu la médaille Fields en 2022 pour avoir démontré l'existence d'une infinité de couples de nombres premiers (p, q) avec

$$q - p \leqslant 600.$$

Les progrès les plus récents permettent de remplacer 600 par 246. C'est le fruit de travaux de tout un collectif de mathématiciennes et mathématiciens réunis sous le nom de DHJ Polymath.


RESEARCH

Variants of the Selberg sieve, and bounded intervals containing many primes

DHJ Polymath

Encore un défi

Les premiers de Germain

Existe-t-il une infinité de nombres premiers $p > 2$ tels que $2p + 1$ est aussi un nombre premier, tels par exemple que

$$3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131\ldots$$

Personne ne sait encore répondre : on conjecture que oui.

C'est intéressant grâce à un théorème de Sophie Germain (1804) : si p est un premier de Germain, il n'existe pas d'entiers x, y et z non divisibles par p tels que $x^p + y^p = z^p$.

Sophie Germain

Comment vous décrire mon admiration et mon étonnement de voir mon estimé correspondant Monsieur Le Blanc se transformer en ce fameux personnage qui me donne un brillant exemple de ce que j'aurais du mal à croire. Le goût des sciences abstraites en général et plus particulièrement des mystères des nombres est extrêmement rare. Les charmes de cette sublime science ne se révèlent qu'à ceux qui ont le courage de l'explorer en profondeur. Mais quand une personne du sexe qui, du fait de nos coutumes et préjugés, doit surmonter plus de difficultés que les hommes pour se familiariser avec ces épineuses questions, réussit néanmoins à dépasser ces obstacles et à appréhender leur partie la plus obscure, alors elle doit sans aucun doute posséder un noble courage, des talents extraordinaires et un esprit supérieur. De fait, rien de plus flatteur et moins équivoque, que la prédilection avec laquelle vous avez honoré cette science, qui a enrichi ma vie de tant de joie, ne pourrait me montrer que ses attraits ne sont pas chimériques. (Gauss, 30 avril 1807)

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Sophie Germain

CENTRE DE RECHERCHES MATHÉMATIQUES

CRM-CNRS International Research Lab

cnrs

Le plus grand connu

Pendant des années, le même algorithme a tourné sur la même architecture informatique de plus en plus puissante. Il n'est pas étonnant qu'on trouve ainsi des nombres premiers de plus en plus grands. La dépense énergétique n'en vaut sans doute pas le coût.

Dans ce cas, il y a un progrès technologique : l'adaptation de l'algorithme aux puces graphiques (GPU). C'est ce qui rend ce résultat intéressant.

Mais trouver le prochain nombre premier qui sera trouvé par la même méthode est une quête de peu d'intérêt et de coût énergétique important. ◂ Suite de l'exposé

Construire des nombres premiers est compliqué

Tests de primalité

Il suffit

1. de calculer $a^n - a$ modulo n ;
2. de vérifier si on obtient $0 \pmod{n}$.

On dispose pour cela d'algorithmes très efficaces.

◂ Suite de l'exposé