Compter les nombres premiers

Nicolas Billerey

Laboratoire de mathématiques Blaise Pascal
Université Clermont Auvergne

Lycée de Mauriac – Vendredi 2 mars 2018

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48 car $48 = 12 \times 4$;

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48 car $48 = 12 \times 4$;
- 5 n'est pas un diviseur de 21

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48 car $48 = 12 \times 4$;
- 5 n'est pas un diviseur de 21

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48 car $48 = 12 \times 4$;
- 5 n'est pas un diviseur de 21 car $5 \times 4 < 21 < 5 \times 5$:

Divisibilité dans les entiers

On dit qu'un entier non nul d divise un entier n s'il existe un entier k tel que

$$n = d \times k.$$

On dit aussi que d est un diviseur de n.

Exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$;
- 12 est un diviseur de 48 car $48 = 12 \times 4$;
- 5 n'est pas un diviseur de 21 car $5 \times 4 < 21 < 5 \times 5$:

$$21 = 5 \times 4 + 1.$$

Diviseurs des entiers ≤ 30

entier n	diviseurs de n	entier n	diviseurs de n
1	1	16	1, 2, 4, 8, 16
2	1, 2	17	1, 17
3	1, 3	18	1, 2, 3, 6, 9, 18
4	1, 2, 4	19	1, 19
5	1, 5	20	1, 2, 4, 5, 10, 20
6	1, 2, 3, 6	21	1, 3, 7, 21
7	1, 7	22	1, 2, 11, 22
8	1, 2, 4, 8	23	1, 23
9	1, 3, 9	24	1, 2, 3, 4, 6, 8, 12, 24
10	1, 2, 5, 10	25	1, 5, 25
11	1, 11	26	1, 2, 13, 26
12	1, 2, 3, 4, 6, 12	27	1, 3, 9, 27
13	1, 13	28	1, 2, 4, 7, 14, 28
14	1, 2, 7, 14	29	1, 29
15	1, 3, 5, 15	30	1, 2, 3, 5, 6, 10, 15, 30

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43 \text{ et } 47.$$

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

- Le nombre 200560490130 admet 2048 diviseurs.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

- Le nombre 200560490130 admet 2048 diviseurs.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

- Le nombre 200560490130 admet 2048 diviseurs. Le nombre 200560490131 n'en a que deux.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

- Le nombre 200560490130 admet 2048 diviseurs. Le nombre 200560490131 n'en a que deux.
- Tout entier s'écrit comme un produit de nombres premiers.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

- Le nombre 200560490130 admet 2048 diviseurs. Le nombre 200560490131 n'en a que deux.
- Tout entier s'écrit comme un produit de nombres premiers.

Nombres premiers

- Un entier $n \geq 2$ est dit premier si ses seuls diviseurs sont 1 et n.
- Les nombres premiers inférieurs à 50 sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43 \text{ et } 47.$$

- Le nombre 200560490130 admet 2048 diviseurs. Le nombre 200560490131 n'en a que deux.
- Tout entier s'écrit comme un produit de nombres premiers. De plus, cette décomposition est unique (à l'ordre près).

Devinettes

- Existe-t-il un nombre premier > 50 ?

Devinettes

- Existe-t-il un nombre premier > 50 ? Réponse : oui ! Par exemple, $53,\ 59,\ 61,\ 67$ sont premiers.

Devinettes

- Existe-t-il un nombre premier > 50 ? Réponse : oui ! Par exemple, $53,\ 59,\ 61,\ 67$ sont premiers.
- Existe-t-il un nombre premier > 100 ?

Devinettes

- Existe-t-il un nombre premier > 50 ? Réponse : oui ! Par exemple, $53,\ 59,\ 61,\ 67$ sont premiers.
- Existe-t-il un nombre premier > 100 ? Réponse : oui ! Par exemple, $101,\ 103,\ 107$ sont premiers.

Devinettes

- Existe-t-il un nombre premier > 50 ? Réponse : oui ! Par exemple, $53,\ 59,\ 61,\ 67$ sont premiers.
- Existe-t-il un nombre premier > 100 ? Réponse : oui ! Par exemple, $101,\ 103,\ 107$ sont premiers.
- Existe-t-il un nombre premier > 1000 ?

Devinettes

- Existe-t-il un nombre premier > 50 ? Réponse : oui ! Par exemple, $53,\ 59,\ 61,\ 67$ sont premiers.
- Existe-t-il un nombre premier > 100 ? Réponse : oui ! Par exemple, $101,\ 103,\ 107$ sont premiers.
- Existe-t-il un nombre premier > 1000 ? On ne demande pas d'en donner, mais juste de montrer qu'il en existe au moins un.

Un nombre premier > 1000 ?

On pose $N = 1 \times 2 \times 3 \times \cdots \times 999 \times 1000 + 1$.

Un nombre premier > 1000 ?

On pose $N = 1 \times 2 \times 3 \times \cdots \times 999 \times 1000 + 1$.

- L'entier N est divisible par un nombre premier p.

Un nombre premier > 1000 ?

On pose $N = 1 \times 2 \times 3 \times \cdots \times 999 \times 1000 + 1$.

- L'entier N est divisible par un nombre premier p.
- Si $p \leq 1000$, on a une contradiction.

Un nombre premier > 1000 ?

On pose $N = 1 \times 2 \times 3 \times \cdots \times 999 \times 1000 + 1$.

- L'entier N est divisible par un nombre premier p.
- Si $p \leq 1000$, on a une contradiction.
- Donc $p > 1000$ et on a gagné !

Infinitude des nombres premiers

Détail de *L'École d'Athène* par Raphaël (1483–1520)

Stanza della Segnatura, Palazzi Pontifici, Vatican

Théorème (Euclide, troisième siècle avant J.C.)

Il existe une infinité de nombres premiers.

Le plus grand nombre premier...

Le plus grand nombre premier... n'existe pas !

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier. Les seuls premiers F_n connus sont $F_0, \ldots, F_4$.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier. Les seuls premiers F_n connus sont $F_0, \ldots, F_4$.

- Le polynôme $n^2 + n + 41$ prend des valeurs premières pour tous les entiers compris entre 0 et 39.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier. Les seuls premiers F_n connus sont $F_0, \ldots, F_4$.

- Le polynôme $n^2 + n + 41$ prend des valeurs premières pour tous les entiers compris entre 0 et 39.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier. Les seuls premiers F_n connus sont $F_0, \ldots, F_4$.

- Le polynôme $n^2 + n + 41$ prend des valeurs premières pour tous les entiers compris entre 0 et 39. Mais, on ne connaît aucun polynôme de degré > 1 en une variable qui prend une infinité de valeurs premières.

Le plus grand nombre premier... n'existe pas !

Pourtant, trouver un « grand » nombre premier est un problème difficile.

- Fermat ($17^{\text{ième}}$ siècle) pensait que tous les entiers de la forme

$$\left\{F_n = 2^{2^n} + 1,\ n \geq 0\right\} = \{3,\ 5,\ 17,\ 257,\ 65\,537,\ 4\,294\,967\,297, \ldots\}$$

étaient premiers. Euler (1707-1783) montra que

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

n'est pas premier. Les seuls premiers F_n connus sont $F_0, \ldots, F_4$.

- Le polynôme $n^2 + n + 41$ prend des valeurs premières pour tous les entiers compris entre 0 et 39. Mais, on ne connaît aucun polynôme de degré > 1 en une variable qui prend une infinité de valeurs premières.
- Il existe un polynôme en 26 variables de degré 25 dont l'ensemble des valeurs positives sur $\mathbb{N}^{26}$ est précisément l'ensemble des nombres premiers.

Le plus grand nombre premier. . . connu

Le plus grand nombre premier... connu

Le plus grand nombre premier connu à l'heure actuelle est

$$2^{77\,232\,917} - 1 = \underbrace{2 \times \cdots \times 2}_{77\,232\,917 \text{ termes}} - 1$$

Le plus grand nombre premier... connu

Le plus grand nombre premier connu à l'heure actuelle est

$$2^{77\,232\,917} - 1 = \underbrace{2 \times \cdots \times 2}_{77\,232\,917 \text{ termes}} - 1$$

- Il a été « découvert » le 26 décembre 2017 par The Great Internet Mersenne Prime Search (GIMPS) ;

Le plus grand nombre premier... connu

Le plus grand nombre premier connu à l'heure actuelle est

$$2^{77\,232\,917} - 1 = \underbrace{2 \times \cdots \times 2}_{77\,232\,917 \text{ termes}} - 1$$

- Il a été « découvert » le 26 décembre 2017 par The Great Internet Mersenne Prime Search (GIMPS) ;
- Son écriture décimale a 23 249 425 chiffres ;

Le plus grand nombre premier... connu

Le plus grand nombre premier connu à l'heure actuelle est

$$2^{77\,232\,917} - 1 = \underbrace{2 \times \cdots \times 2}_{77\,232\,917 \text{ termes}} - 1$$

- Il a été « découvert » le 26 décembre 2017 par The Great Internet Mersenne Prime Search (GIMPS) ;
- Son écriture décimale a 23 249 425 chiffres ;
- Le fichier (format .txt) le contenant a une taille de 23,7 Mo ;

Le plus grand nombre premier... connu

Le plus grand nombre premier connu à l'heure actuelle est

$$2^{77\,232\,917} - 1 = \underbrace{2 \times \cdots \times 2}_{77\,232\,917 \text{ termes}} - 1$$

- Il a été « découvert » le 26 décembre 2017 par The Great Internet Mersenne Prime Search (GIMPS) ;
- Son écriture décimale a 23 249 425 chiffres ;
- Le fichier (format .txt) le contenant a une taille de 23,7 Mo ;
- En écrivant 5 chiffres par seconde et chaque chiffre dans une case de 0,5 cm, il faudrait 54 jours et 116 km de papier pour le recopier.

There are two facts about the distribution of prime numbers [. . .]. The first is that [. . .] the prime numbers belong to the most arbitrary and ornery objects studied by mathematicians : they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite : that the prime numbers exhibit stunning regularity, that there are laws governing their behaviour, and that they obey these laws with almost military precision.

— *Don Zagier, The First* 50 *Million Prime Numbers*

Crible d'Ératosthène (troisième siècle avant J.C.)

Principe

- si n est un entier (différent de 1), alors les entiers $2n$, $3n$, $4n$, ... ne sont pas premiers ;

Crible d'Ératosthène (troisième siècle avant J.C.)

Principe

- si n est un entier (différent de 1), alors les entiers $2n$, $3n$, $4n$, ... ne sont pas premiers ;
- si un entier n (différent de 1) n'est pas de la forme $2q$ ou $3q$ ou $4q$ etc. avec q valant au moins 2 alors n est premier.

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

Crible d'Ératosthène (troisième siècle avant J.C.)

Mise en œuvre

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

La fonction $\pi(x)$

Pour tout nombre réel positif x, on note $\pi(x)$ le nombre de nombres premiers $\leq x$.

La fonction $\pi(x)$

Pour tout nombre réel positif x, on note $\pi(x)$ le nombre de nombres premiers $\leq x$.

On a

$$\pi(2) = 1, \quad \pi(3) = \pi(4) = 2, \quad \pi(5) = \pi(6) = 3,$$

$$\pi(x) = 4, \quad \text{pour tout } x \in]7, 11[, \quad \pi(100) = 25.$$

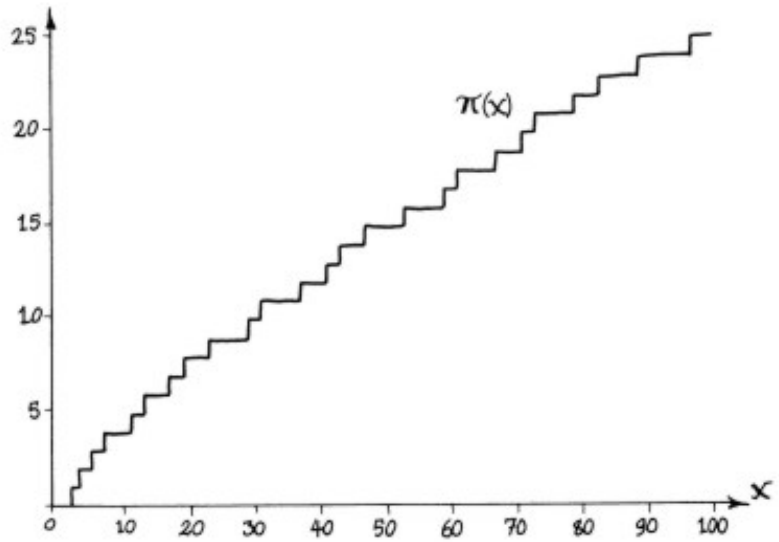
La fonction $\pi(x)$

Pour tout nombre réel positif x, on note $\pi(x)$ le nombre de nombres premiers $\leq x$.

On a

$$\pi(2) = 1, \quad \pi(3) = \pi(4) = 2, \quad \pi(5) = \pi(6) = 3,$$

$$\pi(x) = 4, \quad \text{pour tout } x \in]7, 11[, \quad \pi(100) = 25.$$



Graphe de la fonction π sur l'intervalle [0, 100] – Matthew R. Martin

Énumérer les nombres premiers

x	$\pi(x)$
100	25
1 000	168
10 000	1 229
100 000	9 592
1 000 000	78 498
10 000 000	664 579
100 000 000	5 761 455

Énumérer les nombres premiers

x	$\pi(x)$	proportion $\mathrm{P}(x) = \frac{\pi(x)}{x}$
100	25	0,25
1 000	168	0,17
10 000	1 229	0,12
100 000	9 592	0,096
1 000 000	78 498	0,0785
10 000 000	664 579	0,066
100 000 000	5 761 455	0,058

Énumérer les nombres premiers

x	$\pi(x)$	proportion $\mathrm{P}(x) = \frac{\pi(x)}{x}$	proportion inversée $\frac{1}{\mathrm{P}(x)}$
100	25	0,25	4
1 000	168	0,17	5,95
10 000	1 229	0,12	8,14
100 000	9 592	0,096	10,42
1 000 000	78 498	0,0785	12,74
10 000 000	664 579	0,066	15,05
100 000 000	5 761 455	0,058	17,36

Énumérer les nombres premiers

x	$\pi(x)$	proportion $\mathrm{P}(x) = \frac{\pi(x)}{x}$	proportion inversée $\frac{1}{\mathrm{P}(x)}$	écart $\frac{1}{\mathrm{P}(10x)} - \frac{1}{\mathrm{P}(x)}$
100	25	0,25	4	1,95
1 000	168	0,17	5,95	2,19
10 000	1 229	0,12	8,14	2,28
100 000	9 592	0,096	10,42	2,32
1 000 000	78 498	0,0785	12,74	2,31
10 000 000	664 579	0,066	15,05	2,31
100 000 000	5 761 455	0,058	17,36	

À la recherche d'un équivalent

Le tableau précédent suggère que pour les grandes valeurs de x, la fonction $1/\mathrm{P}$ vérifie :

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

À la recherche d'un équivalent

Le tableau précédent suggère que pour les grandes valeurs de x, la fonction $1/\mathrm{P}$ vérifie :

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

Il existe une fonction qui a cette propriété :

À la recherche d'un équivalent

Le tableau précédent suggère que pour les grandes valeurs de x, la fonction $1/\mathrm{P}$ vérifie :

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

Il existe une fonction qui a cette propriété : la fonction logarithme népérien.

Tour d'horizon de la fonction ln

Version TS

Définition

La fonction logarithme népérien, notée ln, est définie sur $]0, +\infty[$.
Elle associe à tout nombre x strictement positif l'unique nombre y, noté $\ln(x)$, dont l'exponentielle est x.

Tour d'horizon de la fonction ln

Version TS

Définition

La fonction logarithme népérien, notée ln, est définie sur $]0,\ +\infty[$.
Elle associe à tout nombre x strictement positif l'unique nombre y, noté $\ln(x)$, dont l'exponentielle est x.

Autrement dit, pour tout nombre réel positif x et tout nombre réel y,

$$\ln(x) = y \quad \text{équivaut à} \quad x = e^y.$$

Tour d'horizon de la fonction ln

Version 1ère S

Définition

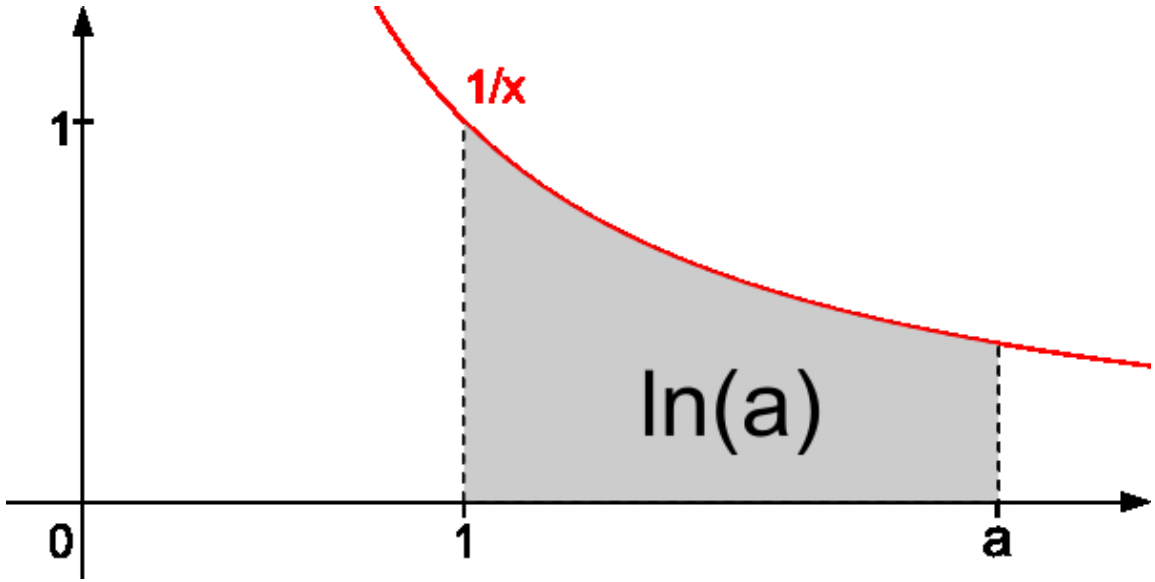
La fonction logarithme népérien, notée ln, est définie sur $]0, +\infty[$.
Elle associe à tout nombre $a > 0$ l'aire de la surface comprise entre l'axe des abscisses, les droites verticales d'équation $x = 1$ et $x = a$ et la courbe représentative de la fonction $1/x$. (On a $\ln(a) \leq 0$ si $0 < a \leq 1$.)

Tour d'horizon de la fonction ln

Version 1ère S

Définition

La fonction logarithme népérien, notée ln, est définie sur $]0, +\infty[$.
Elle associe à tout nombre $a > 0$ l'aire de la surface comprise entre l'axe des abscisses, les droites verticales d'équation $x = 1$ et $x = a$ et la courbe représentative de la fonction $1/x$. (On a $\ln(a) \leq 0$ si $0 < a \leq 1$.)



Source : Wikipédia

Tour d'horizon de la fonction ln

Propriétés

Tour d'horizon de la fonction ln

Propriétés

- On a

$$\ln(1) = 0 \; ; \quad \ln(e) = 1 \; ; \quad \ln(10) \approx 2,3.$$

Tour d'horizon de la fonction ln

Propriétés

- On a
$$\ln(1) = 0 \; ; \quad \ln(e) = 1 \; ; \quad \ln(10) \approx 2,3.$$
- Pour tous réels positifs x et y, on a
$$\ln(xy) = \ln(x) + \ln(y).$$

Tour d'horizon de la fonction ln

Propriétés

- On a
$$\ln(1) = 0 \; ; \quad \ln(e) = 1 \; ; \quad \ln(10) \approx 2,3.$$
- Pour tous réels positifs x et y, on a
$$\ln(xy) = \ln(x) + \ln(y).$$
- Pour tout entier strictement positif x,
$$\ln(x) \approx 2,3 \times (\text{nombre de chiffres de } x \text{ (en base 10)} - 1)$$

Le théorème des nombres premiers

Le rapport du nombre de nombres premiers inférieurs et de $\frac{x}{\pi(x)}$ se rapproche de 1 lorsque x grandit :

Le théorème des nombres premiers

Le rapport du nombre de nombres premiers inférieurs et de $\frac{x}{\pi(x)}$ se rapproche de 1 lorsque x grandit :

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

Le théorème des nombres premiers

Le rapport du nombre de nombres premiers inférieurs et de $\frac{x}{\pi(x)}$ se rapproche de 1 lorsque x grandit :

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

Cet équivalent a été conjecturé par Gauss en 1792.

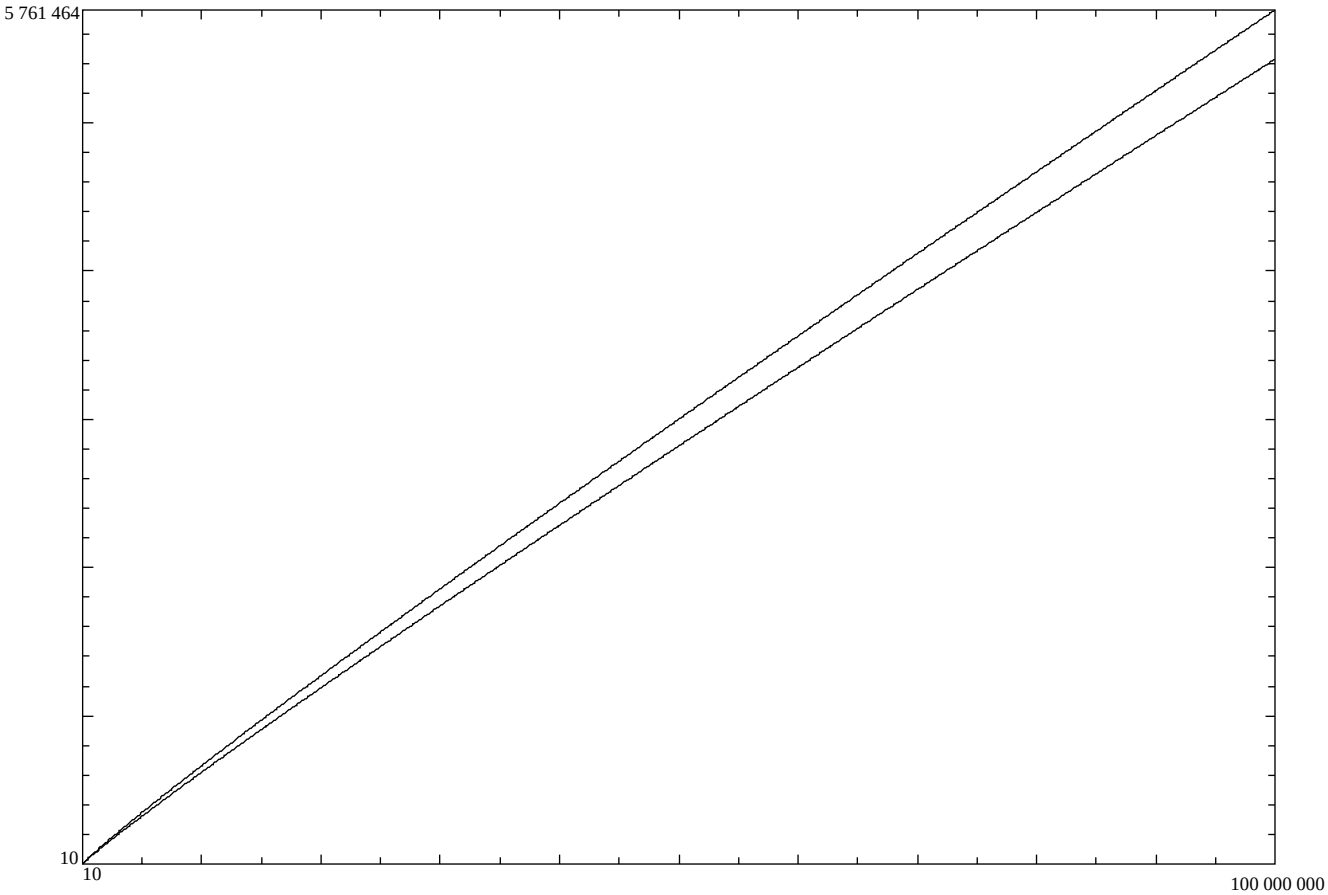
Le théorème des nombres premiers

Le rapport du nombre de nombres premiers inférieurs et de $\frac{x}{\pi(x)}$ se rapproche de 1 lorsque x grandit :

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

Cet équivalent a été conjecturé par Gauss en 1792. Il avait alors 15 ans...

Vue de loin



Représentation graphique des fonctions $\pi(x)$ et $x/\ln(x)$

Le théorème de Hadamard et de La Vallée Poussin

La conjecture de Gauss a été démontrée en 1896 par Hadamard et De La Vallée Poussin.

Le théorème de Hadamard et de La Vallée Poussin

La conjecture de Gauss a été démontrée en 1896 par Hadamard et De La Vallée Poussin.

La fonction ζ de Riemann

- La preuve de Hadamard et De La Vallée Poussin utilise l'analyse complexe, c'est-à-dire l'étude des fonctions définies sur le plan complexe.

La fonction ζ de Riemann

- La preuve de Hadamard et De La Vallée Poussin utilise l'analyse complexe, c'est-à-dire l'étude des fonctions définies sur le plan complexe.
- En particulier, la fonction ζ de Riemann (1826-1866) joue un rôle fondamental :

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} \cdots \quad (s \text{ nombre complexe})$$

La fonction ζ de Riemann

- La preuve de Hadamard et De La Vallée Poussin utilise l'analyse complexe, c'est-à-dire l'étude des fonctions définies sur le plan complexe.
- En particulier, la fonction ζ de Riemann (1826-1866) joue un rôle fondamental :

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} \cdots \quad (s \text{ nombre complexe})$$

- Le Clay Mathematics Institute offre un million de dollars à qui montrera que les zéros complexes « non triviaux » de cette fonction sont tous situés sur une même droite verticale ($s = \frac{1}{2} + it$).

La fonction ζ de Riemann

- La preuve de Hadamard et De La Vallée Poussin utilise l'analyse complexe, c'est-à-dire l'étude des fonctions définies sur le plan complexe.
- En particulier, la fonction ζ de Riemann (1826-1866) joue un rôle fondamental :

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} \cdots \quad (s \text{ nombre complexe})$$

- Le Clay Mathematics Institute offre un million de dollars à qui montrera que les zéros complexes « non triviaux » de cette fonction sont tous situés sur une même droite verticale ($s = \frac{1}{2} + it$).
- Un tel résultat donnerait - entre autres - une estimation précise du terme d'erreur dans le théorème de Hadamard et De La Vallée Poussin.

Une assertion hardie

No elementary proof of the prime number theorem is known, and one may ask whether it is reasonable to expect one. [. . .] A proof of such a theorem [. . .] seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way ; but one thing seems quite clear. We have certain views about the logic of the theory ; we think that some theorems, as we say "lie deep" and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten.

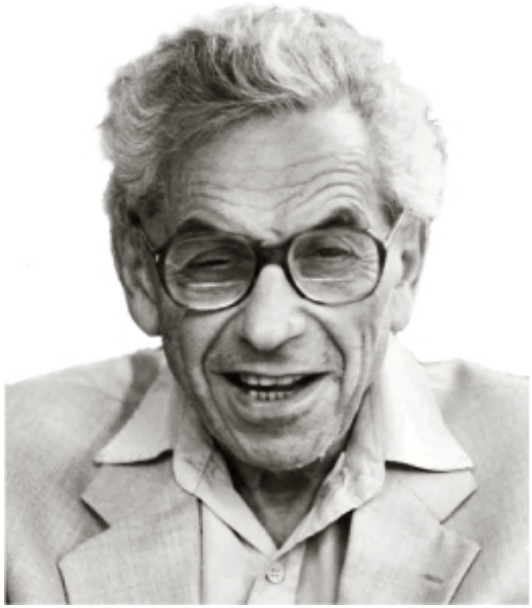
— G. H. Hardy (1921), Lecture to Mathematical Society of Copenhagen.

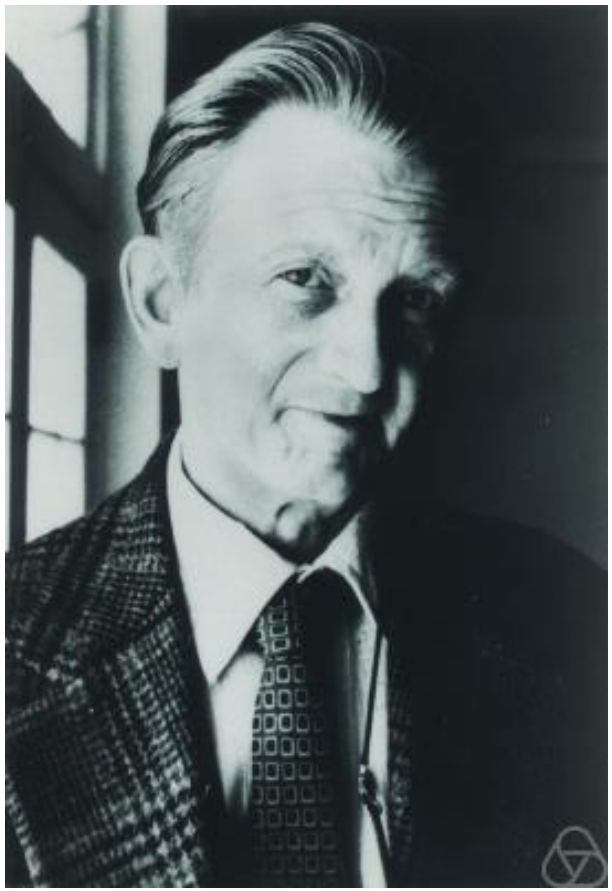
Une preuve élémentaire

En 1949, Erdös et Selberg ont donné une preuve élémentaire du théorème des nombres premiers.

Une preuve élémentaire

En 1949, Erdös et Selberg ont donné une preuve élémentaire du théorème des nombres premiers.





Merci pour votre attention !