Nombres premiers

Lycée Français International de Hong Kong

Emmanuel Royer

Laboratoire de mathématiques
CNRS & Université Blaise Pascal
Clermont-Ferrand

Avril 2016

Opérations

Divisibilité

Qu'est-ce qu'un diviseur ?

Opérations

Divisibilité

Choisissez deux nombres entiers,

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second.

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Exemple

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Exemple

4 20

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Exemple

$$4 \times 5 = 20$$

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Exemple

$4 \times 5 = 20$ $\quad$ 4 est un diviseur de 20

Opérations

Divisibilité

Choisissez deux nombres entiers, appelez d le premier et n le second. S'il existe un troisième entier k tel que

$$d \times k = n$$

on dit que d est un **diviseur** de n.

Exemple

$4 \times 5 = 20$ $\quad$ 4 est un diviseur de 20

Exemple

Un autre exemple ?

Opérations

Divisibilité

Chaque nombre entier (différent de 1) a au moins deux diviseurs : 1 et lui même.

Opérations

Divisibilité

Chaque nombre entier (différent de 1) a au moins deux diviseurs : 1 et lui même.

Exemple

- $1 \times 20 = 20$ donc 1 divise 20

Opérations

Divisibilité

Chaque nombre entier (différent de 1) a au moins deux diviseurs : 1 et lui même.

Exemple

- $1 \times 20 = 20$ donc 1 divise 20
- $20 \times 1 = 20$ donc 20 divise 20

Certains nombres n'ont que deux diviseurs,

Deux grands nombres...

- 1 719 620 105 458 406 433 483 340 568 317 543 019 584 575 635 895 742 560 438 771 105 058 321 655 238 562 613 083 979 651 479 555 788 009 994 557 822 024 565 226 932 906 295 208 262 756 822 275 663 694 111 n'a que deux diviseurs ;

Opérations

Divisibilité

Certains nombres n'ont que deux diviseurs, d'autres ont beaucoup de diviseurs,

Deux grands nombres...

- 1 719 620 105 458 406 433 483 340 568 317 543 019 584 575 635 895 742 560 438 771 105 058 321 655 238 562 613 083 979 651 479 555 788 009 994 557 822 024 565 226 932 906 295 208 262 756 822 275 663 694 111 n'a que deux diviseurs ;
- 1 719 620 105 458 406 433 483 340 568 317 543 019 584 575 635 895 742 560 438 771 105 058 321 655 238 562 613 083 979 651 479 555 788 009 994 557 822 024 565 226 932 906 295 208 262 756 822 275 663 694 110 a 37 778 931 862 957 161 709 568 diviseurs ;

Opérations

Divisibilité

Certains nombres n'ont que deux diviseurs, d'autres ont beaucoup de diviseurs,

Deux grands nombres...

- 1 719 620 105 458 406 433 483 340 568 317 543 019 584 575 635 895 742 560 438 771 105 058 321 655 238 562 613 083 979 651 479 555 788 009 994 557 822 024 565 226 932 906 295 208 262 756 822 275 663 694 111
  n'a que deux diviseurs ;
- 1 719 620 105 458 406 433 483 340 568 317 543 019 584 575 635 895 742 560 438 771 105 058 321 655 238 562 613 083 979 651 479 555 788 009 994 557 822 024 565 226 932 906 295 208 262 756 822 275 663 694 110
  a 37 778 931 862 957 161 709 568 diviseurs

Combien les nombres suivants ont-ils de diviseurs ?

Opérations

Divisibilité

Combien les nombres suivants ont-ils de diviseurs ?

- 3 ?

Opérations

Divisibilité

Combien les nombres suivants ont-ils de diviseurs ?

- 3 a 2 diviseurs

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 ?

Opérations

Divisibilité

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 a 3 diviseurs

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 a 3 diviseurs
- 12 ?

Opérations

Divisibilité

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 a 3 diviseurs
- 12 a 6 diviseurs

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 a 3 diviseurs
- 12 a 6 diviseurs
- 13 ?

Opérations

Divisibilité

Combien les nombres suivants ont-ils de diviseurs ?

À vous !

- 3 a 2 diviseurs
- 4 a 3 diviseurs
- 12 a 6 diviseurs
- 13 a 2 diviseurs

Qu'est-ce qu'un nombre premier ?

Définition

Un nombre premier est un nombre entier naturel qui n'a que deux diviseurs.

Exemples

- Les nombres 2, 3, 5, 7, 11 sont premiers ;

Exemples

- Les nombres 2, 3, 5, 7, 11 sont premiers ;
- vous pouvez le vérifier en divisant par tous les entiers plus petits que ces nombres.

Exemples

- Les nombres 2, 3, 5, 7, 11 sont premiers ;
- vous pouvez le vérifier en divisant par tous les entiers plus petits que ces nombres.
- Les nombres 4, 9, 12 ne sont pas premiers ;

Exemples

- Les nombres 2, 3, 5, 7, 11 sont premiers ;
- vous pouvez le vérifier en divisant par tous les entiers plus petits que ces nombres.
- Les nombres 4, 9, 12 ne sont pas premiers ;
- Le nombre $2^{74\,207\,281} - 1$ est premier ;

Exemples

- Les nombres 2, 3, 5, 7, 11 sont premiers ;
- vous pouvez le vérifier en divisant par tous les entiers plus petits que ces nombres.
- Les nombres 4, 9, 12 ne sont pas premiers ;
- Le nombre $2^{74\,207\,281} - 1$ est premier ;
- ce nombre a 22 338 618 chiffres, c'est le plus grand nombre premier connu à ce jour. Il a été « trouvé » en janvier 2016.

Le plus grand... connu

Le plus grand nombre premier connu à ce jour a

22 338 618 chiffres.

Le fichier texte (format .txt) le contenant a une taille de

22,8 Mo.

Pour l'imprimer, il faudrait

3 304 feuilles

imprimées recto-verso comme celle que je vous présente, soit

16 kilogrammes de papier.

Crible d'Ératosthène

Troisième siècle av. J.-C.

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

Crible d'Ératosthène

Principe

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

Crible d'Ératosthène

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Une infinité...

- Donnez moi une liste de nombres

Une infinité...

- Donnez moi une liste de nombres
- puis-je vous garantir qu'il existe un nombre plus grand que le plus grand de votre liste ?

Une infinité...

- Donnez moi une liste de nombres
- puis-je vous garantir qu'il existe un nombre plus grand que le plus grand de votre liste ?

OUI

Une infinité...

- Donnez moi une liste de nombres
- puis-je vous garantir qu'il existe un nombre plus grand que le plus grand de votre liste ?

OUI

Il suffit de trouver le plus grand des nombres que vous m'avez donnés et de l'augmenter de 1.

Une infinité...

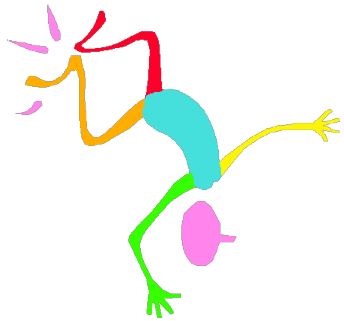
- Donnez moi une liste de nombres premiers,

Une infinité...

- Donnez moi une liste de nombres premiers,
- puis-je vous garantir qu'il existe un nombre premier plus grand que le plus grand de votre liste ?

Une infinité...

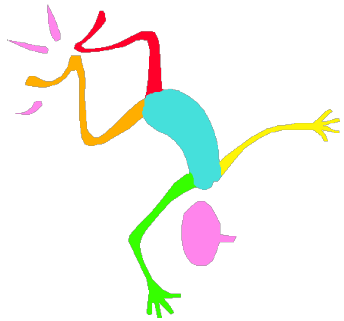
- Donnez moi une liste de nombres premiers,
- puis-je vous garantir qu'il existe un nombre premier plus grand que le plus grand de votre liste ?



OUI

Une infinité...

- Donnez moi une liste de nombres premiers,
- puis-je vous garantir qu'il existe un nombre premier plus grand que le plus grand de votre liste ?

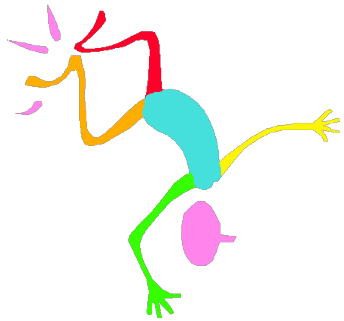


OUI

On dit qu'il y a une infinité de nombres premiers.

Une infinité...

- Donnez moi une liste de nombres premiers,
- puis-je vous garantir qu'il existe un nombre premier plus grand que le plus grand de votre liste ?

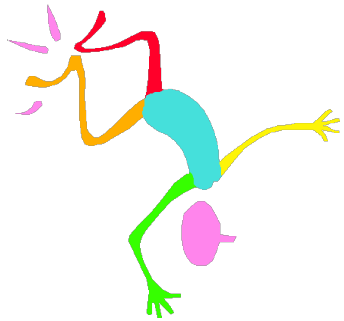


OUI

On dit qu'il y a une infinité de nombres premiers.
Si vous choisissez une liste trop longue, il me sera malgré tout très difficile de construire un tel nombre premier.

Une infinité...

- Donnez moi une liste de nombres premiers,
- puis-je vous garantir qu'il existe un nombre premier plus grand que le plus grand de votre liste ?



On dit qu'il y a une infinité de nombres premiers.
Si vous choisissez une liste trop longue, il me sera malgré tout très difficile de construire un tel nombre premier.
Ça n'empêche pas de savoir qu'il en existe un.

Une infinité...

La preuve d'Euclide (Troisième siècle av. J.-C.)

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

Une infinité...

La preuve d'Euclide

Donnez moi une liste de nombres premiers, grâce au crible d'Érathostène on construit la liste de tous les nombres premiers inférieurs au plus grand de votre liste :

$$p_1 < p_2 < p_3 < \cdots < p_k.$$

BUT : montrer qu'il existe un nombre premier strictement supérieur à p_k.

Une infinité...

La preuve d'Euclide

Un cas particulier

Un homme ne connaît que les nombres premiers 2, 3, 5 et 11. Avec le crible d'Érathostène il construit :

$$2 < 3 < 5 < 7 < 11.$$

Il a énormément de mal à calculer, au point qu'utiliser crible d'Érathostène pour trouver un nombre premier plus grand que 11 est impensable. En revanche, il sait raisonner !

BUT : se convaincre qu'il existe un nombre premier strictement supérieur à 11.

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

2. Soit il est premier : il convient car $n > p_k$;

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

2. Soit il est premier : il convient car $n > p_k$;
3. soit il n'est pas premier : dans ce cas, il admet un diviseur premier q ;

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

2. Soit il est premier : il convient car $n > p_k$;
3. soit il n'est pas premier : dans ce cas, il admet un diviseur premier q ;
4. ce nombre premier q n'est pas dans la liste $p_1, \ldots, p_k$, sinon il diviserait à la fois le nombre n et le nombre $p_1 \times p_2 \times p_3 \times \cdots \times p_k$,

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

2. Soit il est premier : il convient car $n > p_k$;
3. soit il n'est pas premier : dans ce cas, il admet un diviseur premier q ;
4. ce nombre premier q n'est pas dans la liste $p_1, \ldots, p_k$, sinon il diviserait à la fois le nombre n et le nombre $p_1 \times p_2 \times p_3 \times \cdots \times p_k$,
5. il diviserait donc 1 ce qui est impossible ;

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

1. Construisons le nombre

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1.$$

2. Soit il est premier : il convient car $n > p_k$;
3. soit il n'est pas premier : dans ce cas, il admet un diviseur premier q ;
4. ce nombre premier q n'est pas dans la liste $p_1, \ldots, p_k$, sinon il diviserait à la fois le nombre n et le nombre $p_1 \times p_2 \times p_3 \times \cdots \times p_k$,
5. il diviserait donc 1 ce qui est impossible ;
6. ainsi q est un nombre premier supérieur à p_k.

Mon premier théorème !

Il existe une infinité de nombres premiers : pour tout nombre entier n, il existe un nombre premier plus grand que n.

Une infinité...

La preuve d'Euclide : un nombre strictement plus grand que le plus grand...

Un cas particulier

- Notre homme construit le nombre

$$n = 2 \times 3 \times 5 \times 7 \times 11 + 1.$$

Il ne sait pas le calculer.

- S'il est premier, alors c'est un nombre premier plus grand que 11.
- S'il n'est pas premier, ce nombre à un diviseur qui est lui-même premier.
- Ce diviseur ne peut pas être 2, ni 3, ni 5, ni 7 ni 11.
- Ce diviseur est donc un nombre premier plus grand que 11.

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;
- il y a 1229 nombres premiers inférieurs à 10000 ;

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;
- il y a 1229 nombres premiers inférieurs à 10000 ;
- il y a 9592 nombres premiers inférieurs à 100000 ;

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;
- il y a 1229 nombres premiers inférieurs à 10000 ;
- il y a 9592 nombres premiers inférieurs à 100000 ;
- il y a 78498 nombres premiers inférieurs à 1000000 ;

Combien ?

Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;
- il y a 1229 nombres premiers inférieurs à 10000 ;
- il y a 9592 nombres premiers inférieurs à 100000 ;
- il y a 78498 nombres premiers inférieurs à 1000000 ;
- il y a 664579 nombres premiers inférieurs à 10000000.

Combien ?

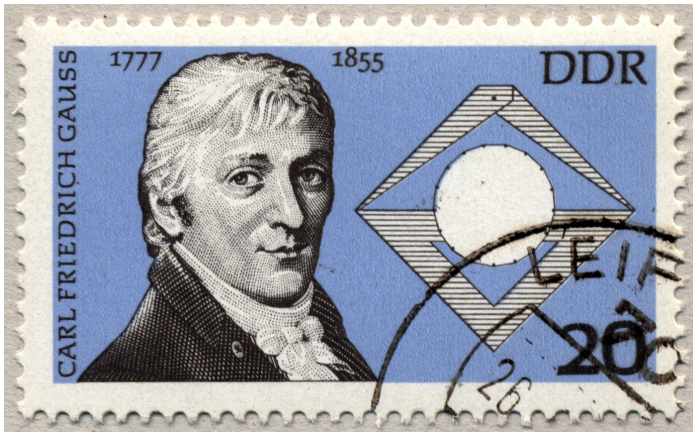
Une infinité, oui mais...

- Il y a 25 nombres premiers inférieurs à 100 ;
- il y a 168 nombres premiers inférieurs à 1000 ;
- il y a 1229 nombres premiers inférieurs à 10000 ;
- il y a 9592 nombres premiers inférieurs à 100000 ;
- il y a 78498 nombres premiers inférieurs à 1000000 ;
- il y a 664579 nombres premiers inférieurs à 10000000.

Quelle régularité ?

Combien ?

Une infinité, oui mais...



Le décompte des nombres premiers évoqués précédemment a été fait par Gauss à la main.

Combien ?

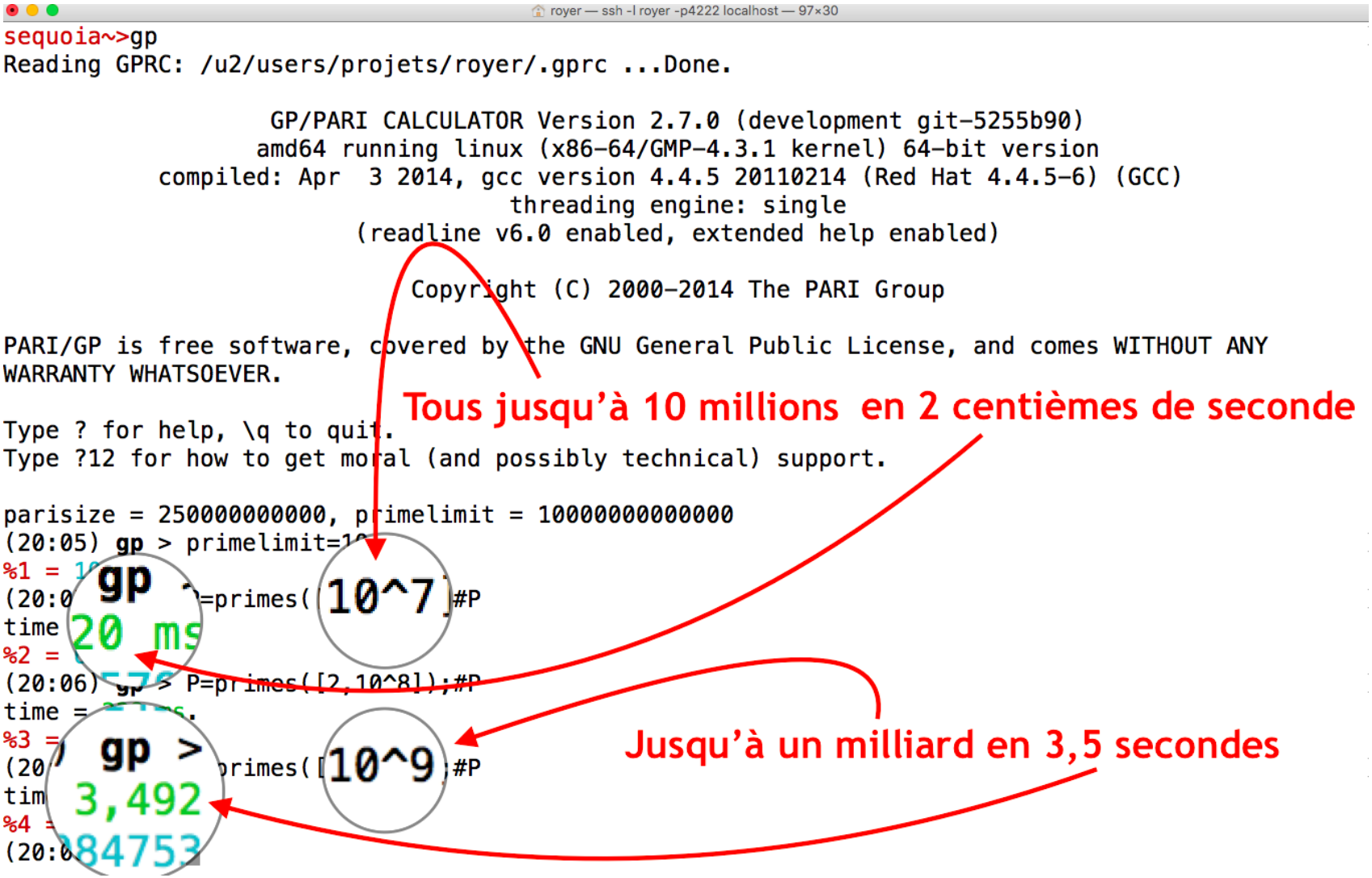
Une infinité, oui mais...

De nos jours, on utilise plutôt des applications informatiques telles que pari-gp.

```
royer — ssh -l royer -p4222 localhost — 97×30
sequoia~>gp
Reading GPRC: /u2/users/projets/royer/.gprc ...Done.

                GP/PARI CALCULATOR Version 2.7.0 (development git-5255b90)
              amd64 running linux (x86-64/GMP-4.3.1 kernel) 64-bit version
         compiled: Apr  3 2014, gcc version 4.4.5 20110214 (Red Hat 4.4.5-6) (GCC)
                                threading engine: single
                      (readline v6.0 enabled, extended help enabled)

                           Copyright (C) 2000-2014 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and comes WITHOUT ANY
WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

parisize = 250000000000, primelimit = 10000000000000
(20:05) gp > primelimit=10
%1 = 10
(20:05) gp > P=primes([2,10^7]);#P
time = 20 ms.
%2 = 664579
(20:06) gp > P=primes([2,10^8]);#P
time = 238 ms.
%3 = 5761455
(20:06) gp > P=primes([2,10^9]);#P
time = 3,492 ms.
%4 = 50847534
(20:06) gp >
```

Combien ?

Une infinité, oui mais...



Combien ?

Une infinité, oui mais...

Combien ?

Une infinité, oui mais...

x	Nombre de premiers inférieurs à x
100	25
1000	168
10000	1229
100000	9592
1000000	78498
10000000	664579
100000000	5761455

Combien ?

Une infinité, oui mais...

x	Nombre de premiers inférieurs à x	Proportion
100	25	0,25
1000	168	0,17
10000	1229	0,12
100000	9592	0,1
1000000	78498	0,08
10000000	664579	0,07
100000000	5761455	0,06

Combien ?

Une infinité, oui mais...

x	Nombre de premiers inférieurs à x	Proportion	Proportion inverse
100	25	0,25	4
1000	168	0,17	5,95
10000	1229	0,12	8,14
100000	9592	0,1	10,43
1000000	78498	0,08	12,74
10000000	664579	0,07	15,05
100000000	5761455	0,06	17,36

Combien ?

Une infinité, oui mais...

x	Nombre de premiers inférieurs à x	Proportion	Proportion inverse	Écart
100	25	0,25	4	
1000	168	0,17	5,95	1,95
10000	1229	0,12	8,14	2,18
100000	9592	0,1	10,43	2,29
1000000	78498	0,08	12,74	2,31
10000000	664579	0,07	15,05	2,31
100000000	5761455	0,06	17,36	2,31

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

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

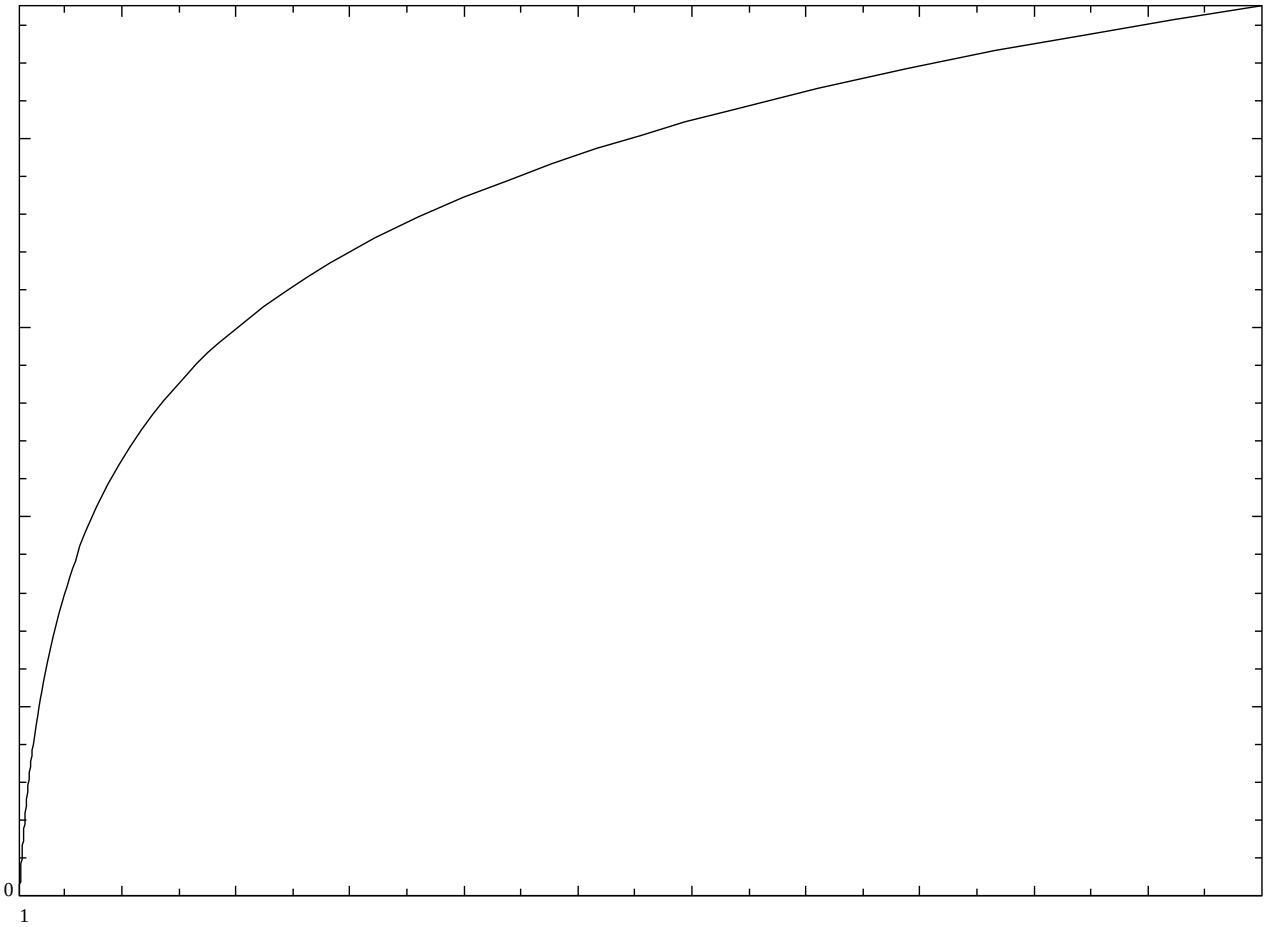
Le tableau précédent semble montrer que, lorsque x est suffisamment grand,

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

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

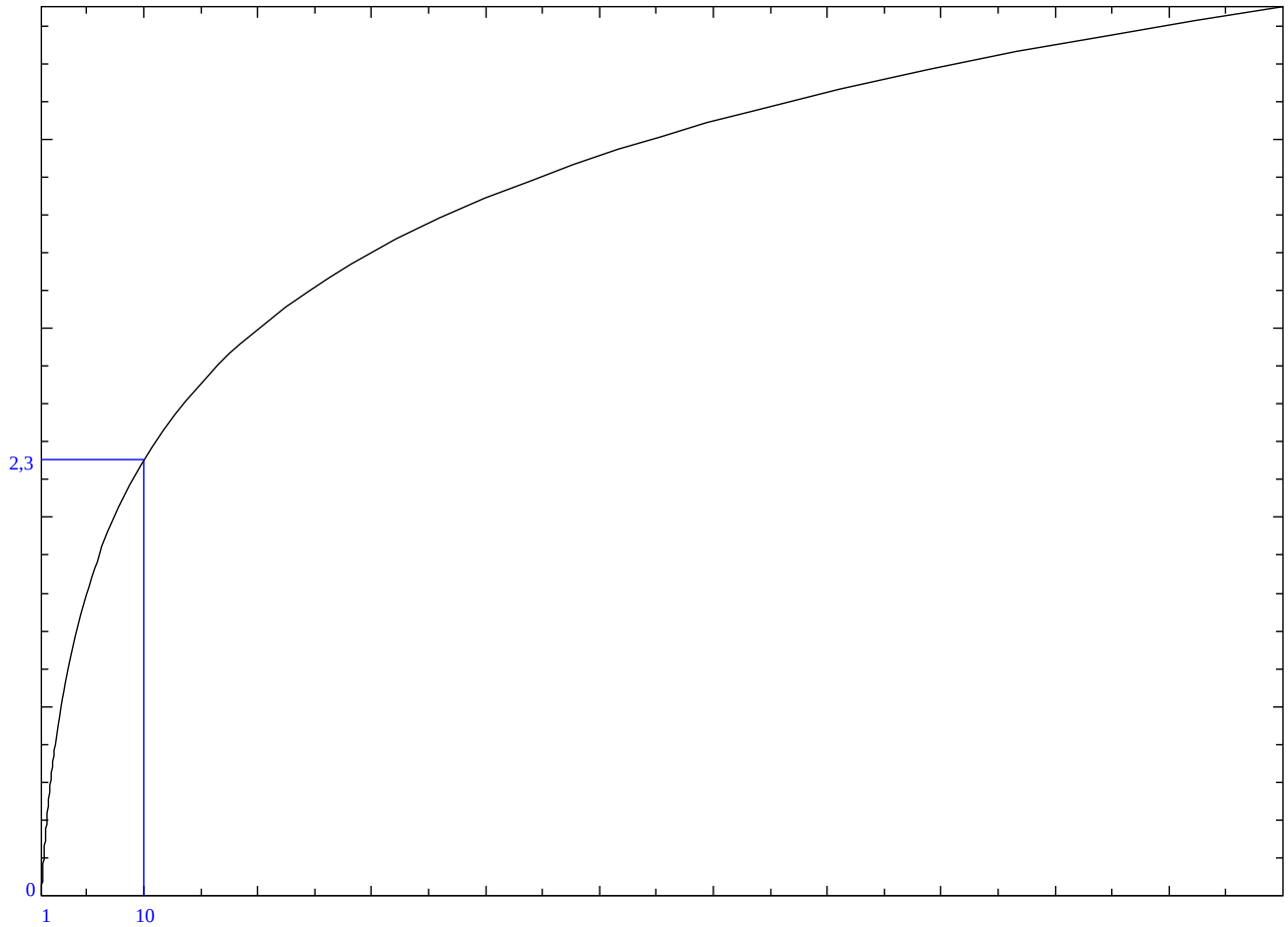
Combien ?

Une infinité, oui mais...



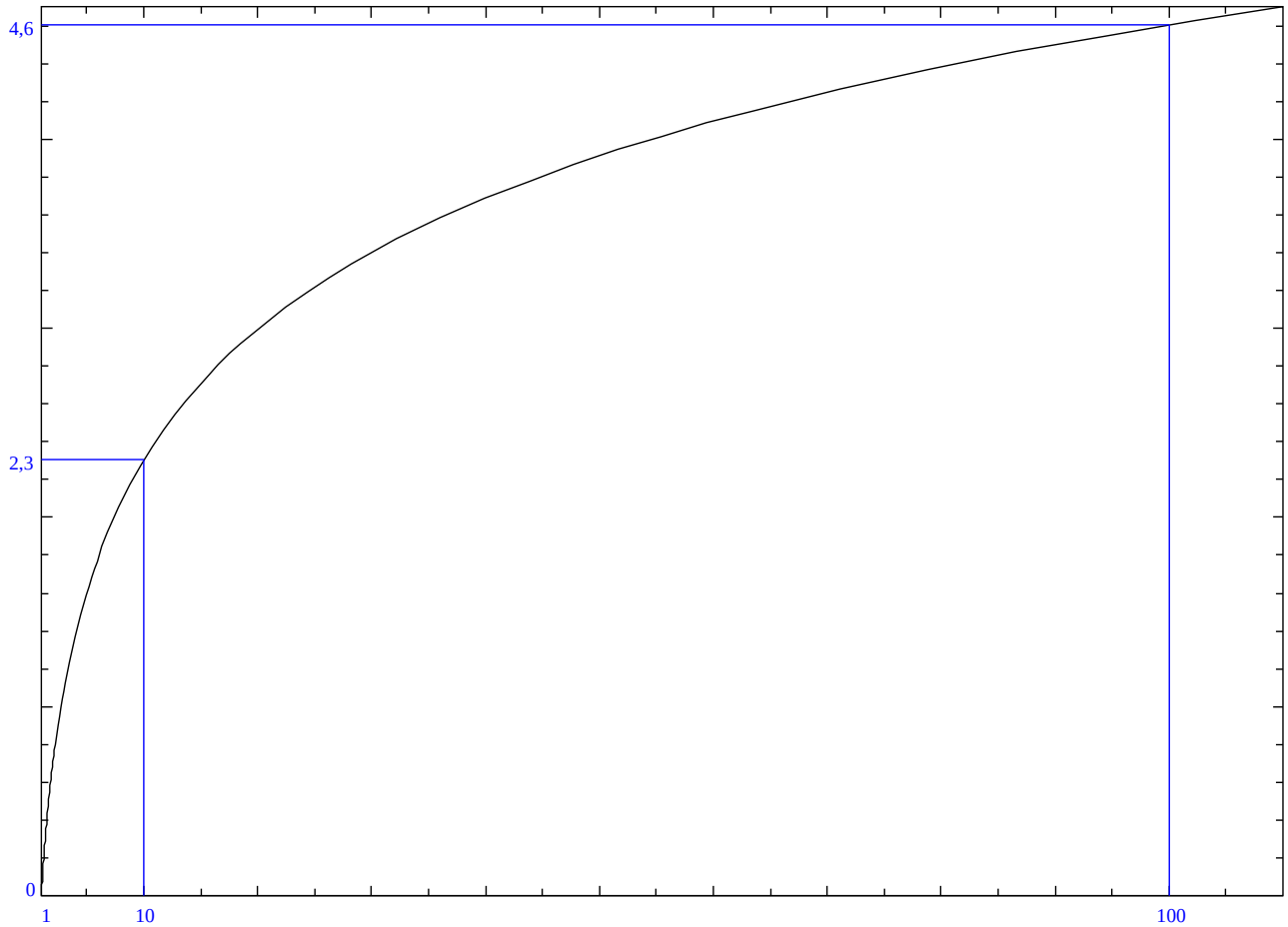
Combien ?

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.

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...

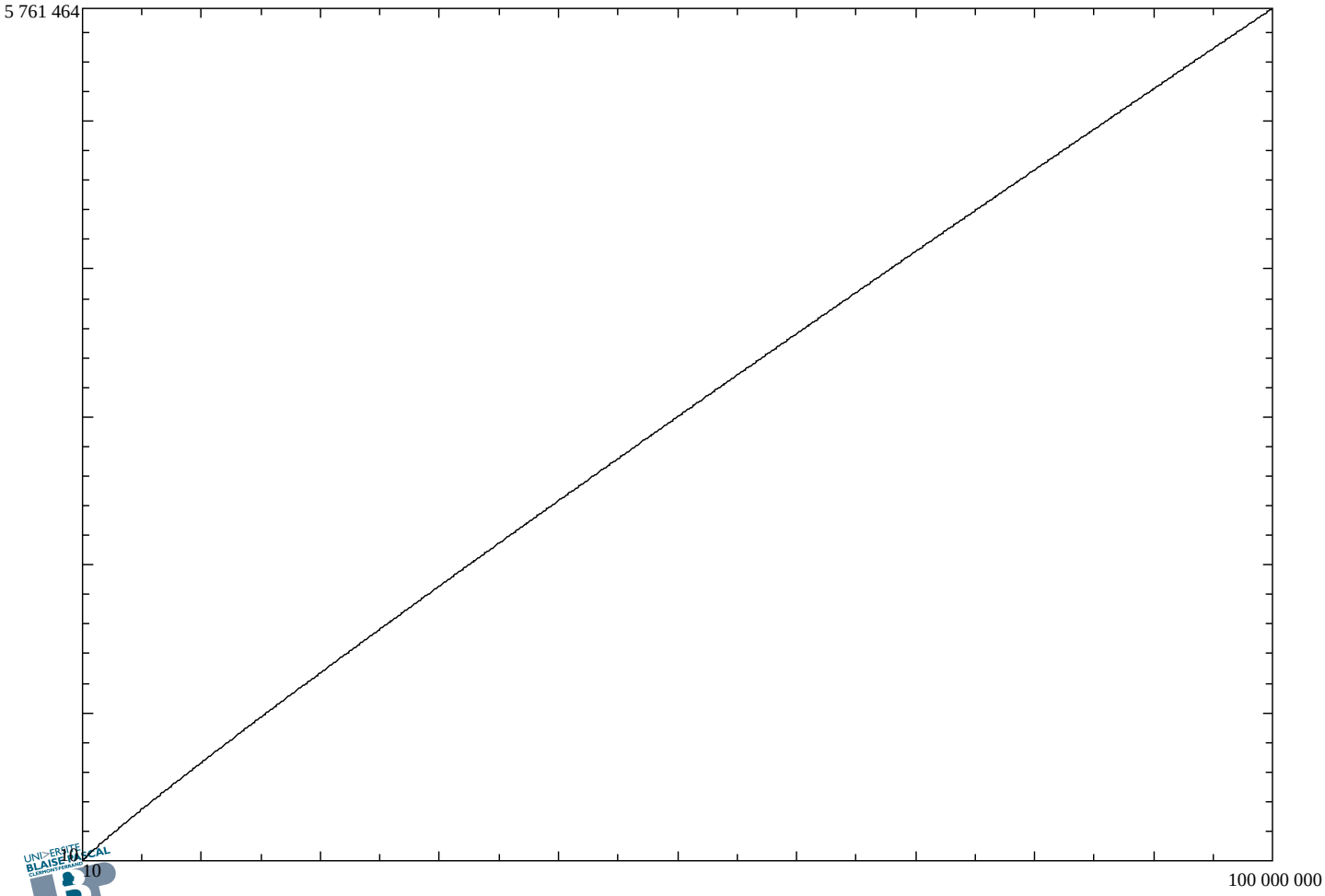
Il semble donc que le rapport du nombre de nombres premiers inférieurs à x et de $\frac{x}{\ln x}$ se rapproche de 1 quand x grandit.

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

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

Combien ?

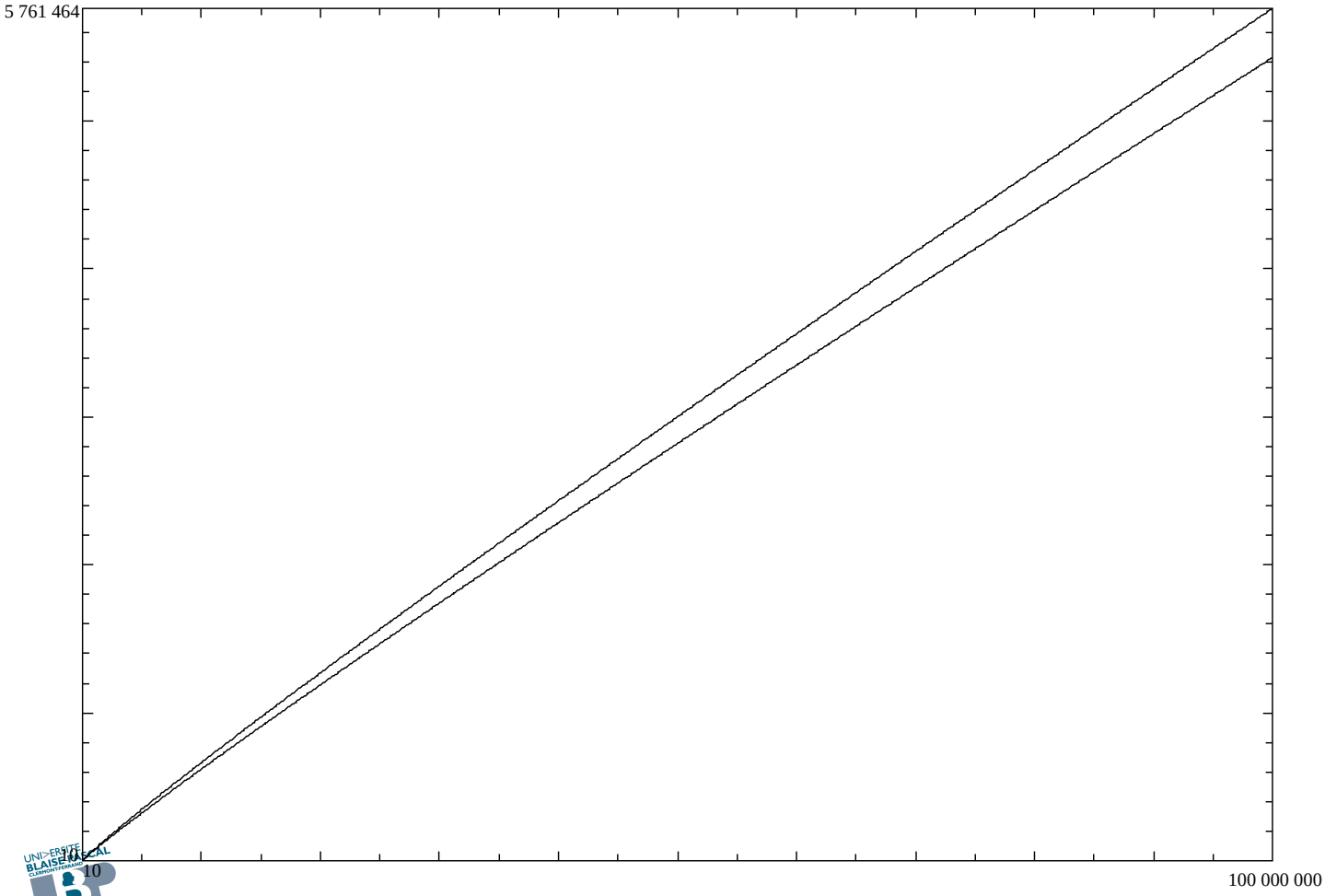
Qualité de l'estimation du jeune Gauss...



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

Combien ?

Qualité de l'estimation du jeune Gauss...



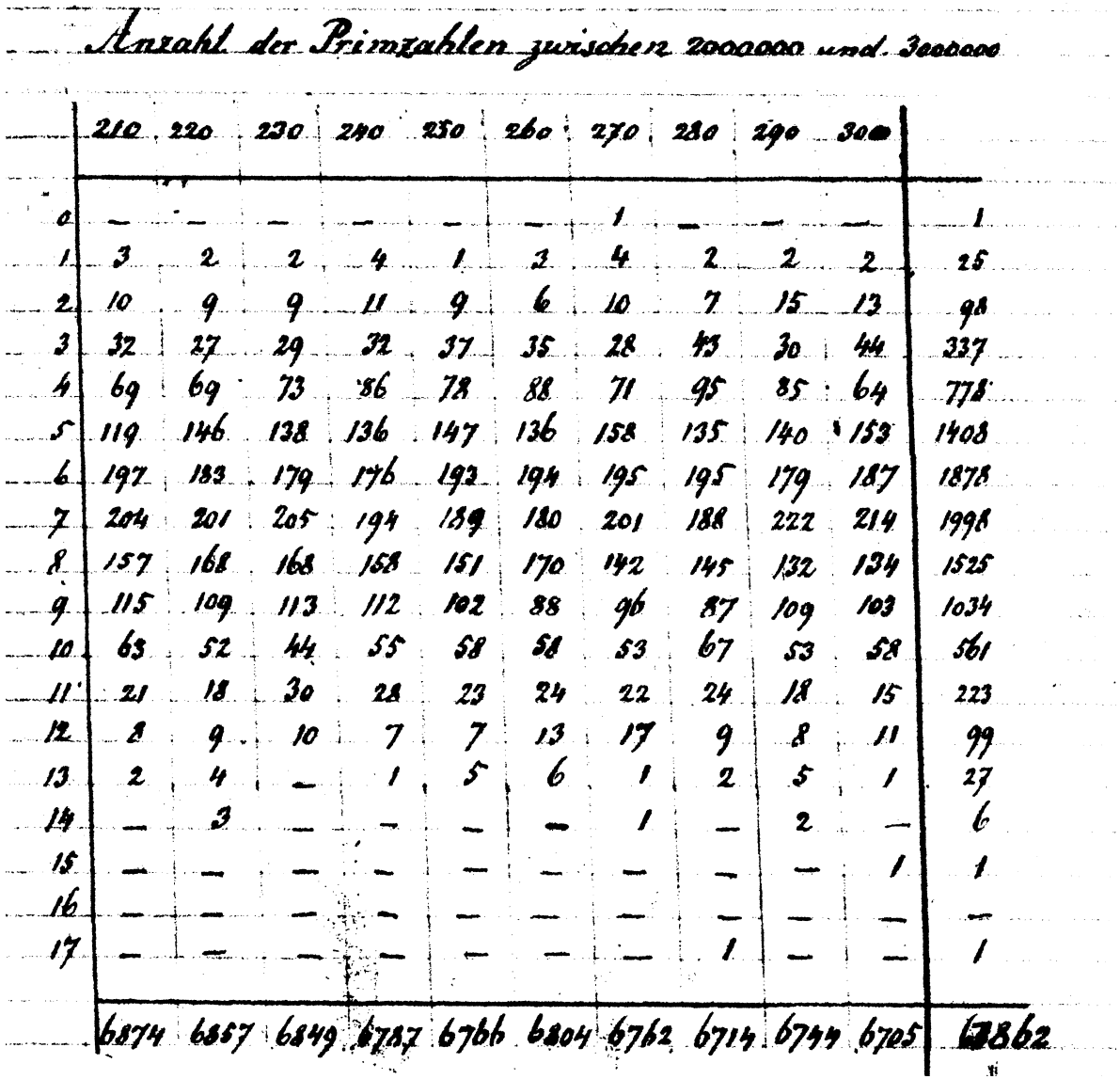
$$x \mapsto \pi(x)$$

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


Il est temps de partir,
mais
l'histoire ne fait que commencer...
AQUALUNA
Encore 225 ans de mathématiques à parcourir...

Combien ?

Une estimation 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

Combien ?

Une estimation du vieux Gauss...

und ich habe (da ich zu einer enthaltenden 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 ~~Decbr~~ 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 ?

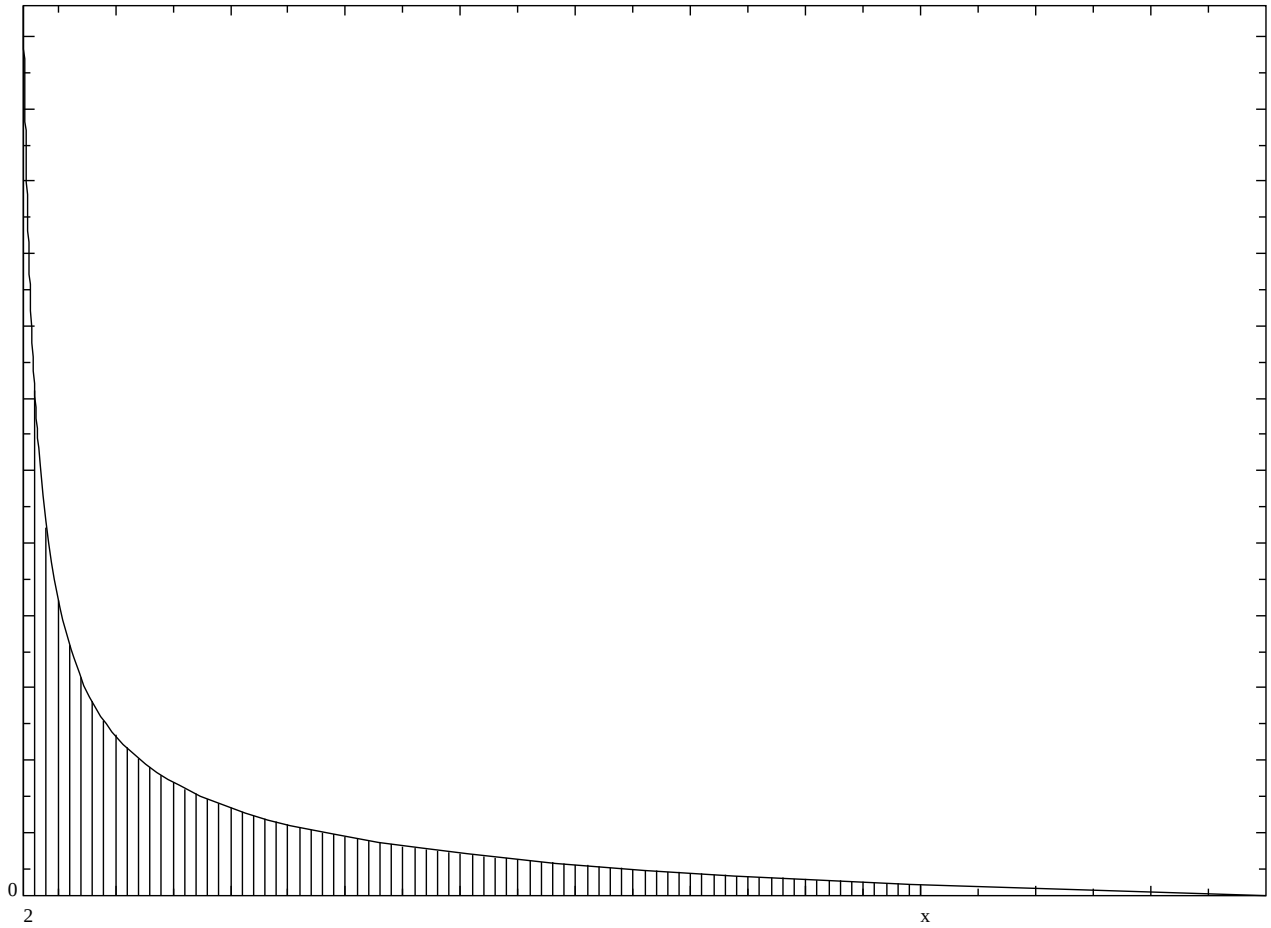
Une estimation du vieux Gauss...

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.

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

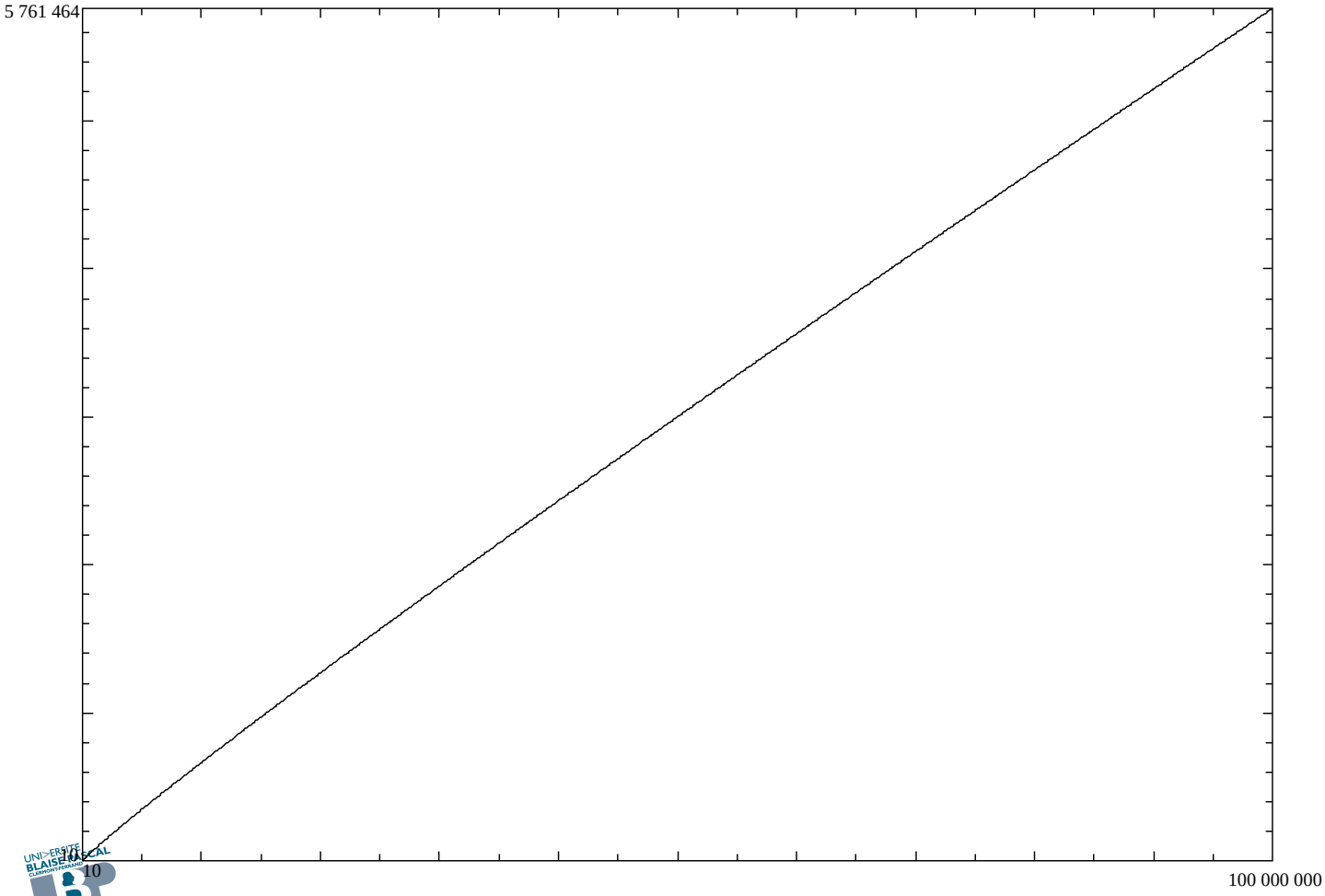
Combien ?

Une estimation du vieux Gauss...



Combien ?

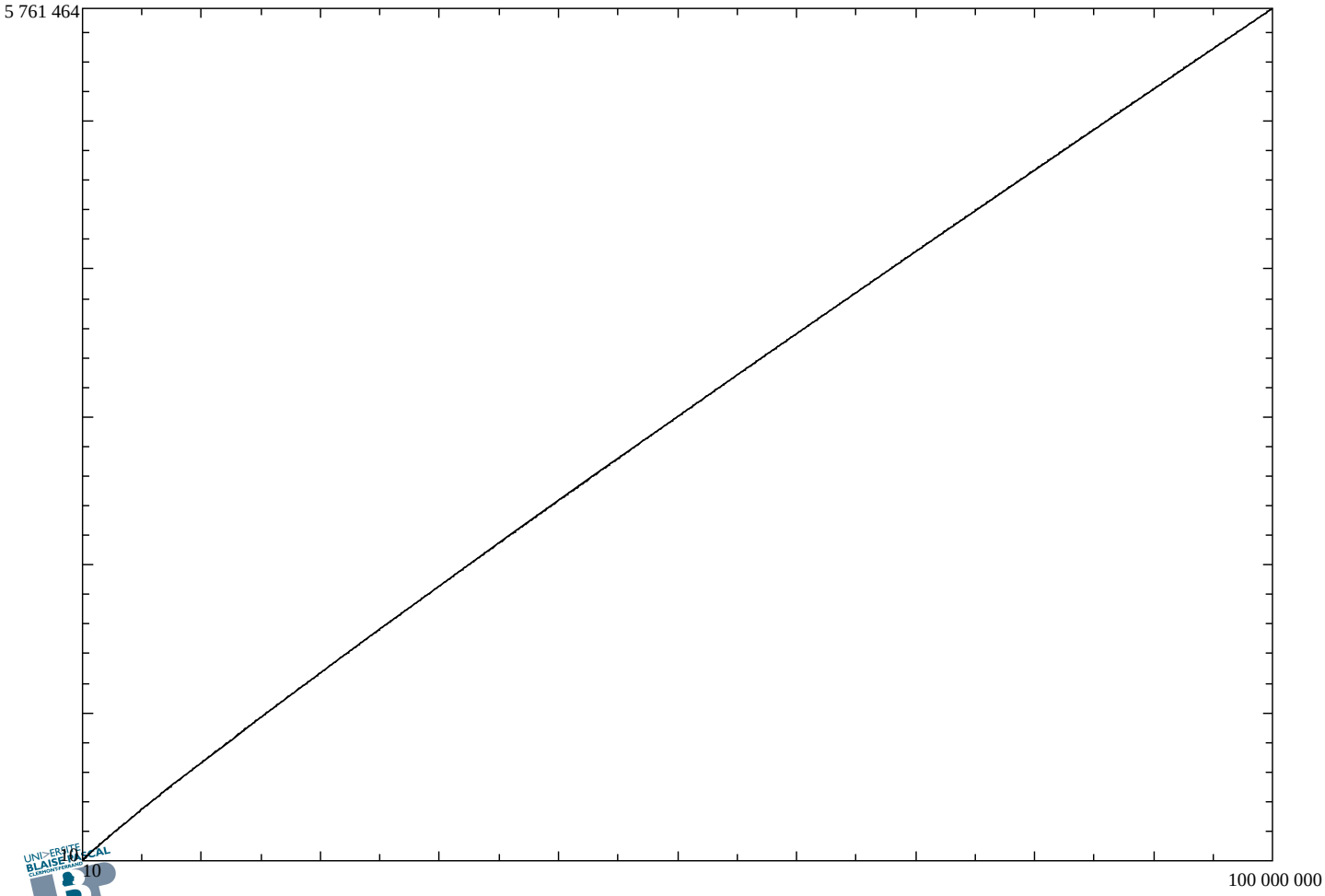
Qualité de l'estimation du vieux Gauss...



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

Combien ?

Qualité de l'estimation du vieux Gauss...

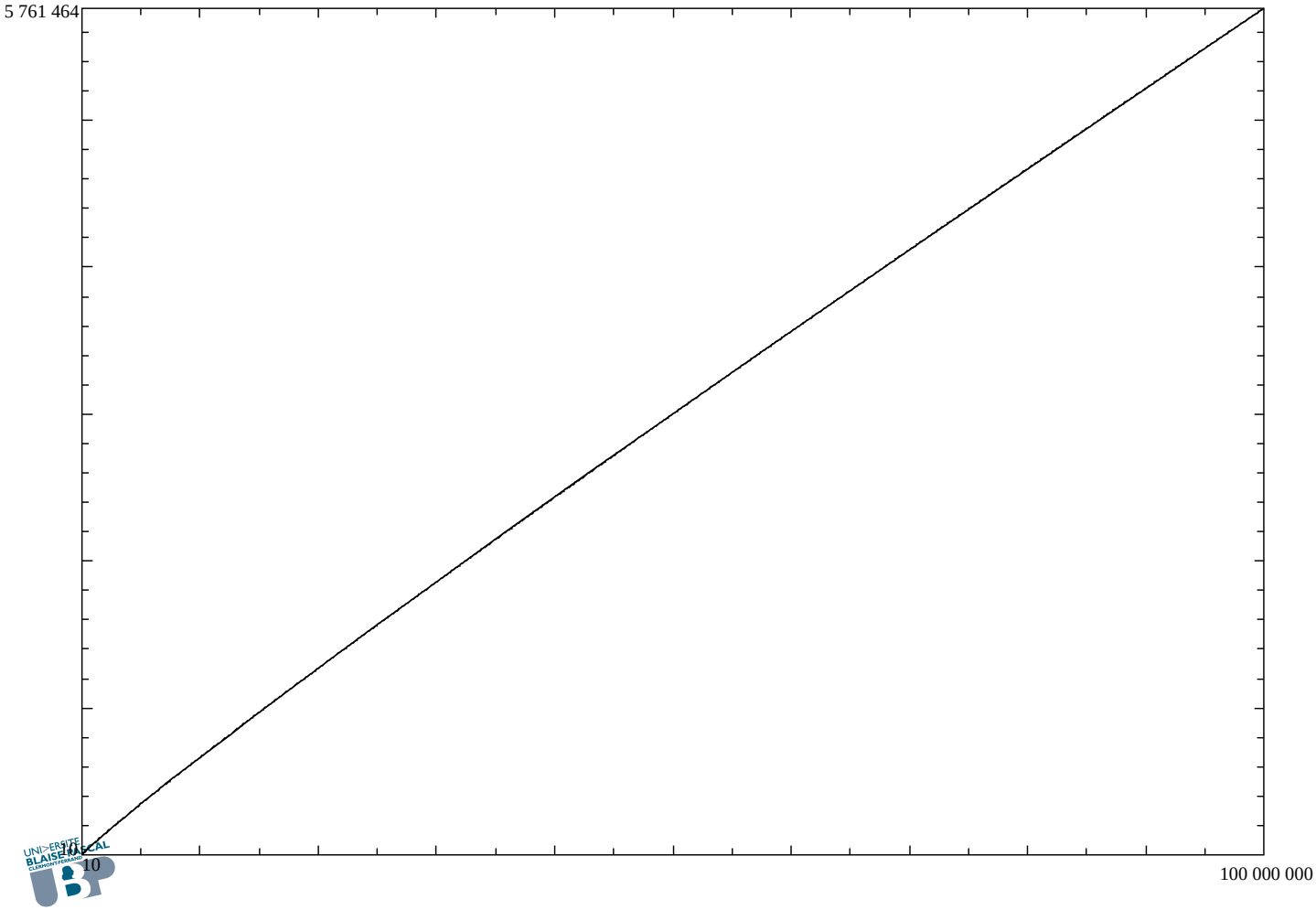


$$x \mapsto \pi(x)$$

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

Combien ?

Qualité de l'estimation du vieux Gauss...



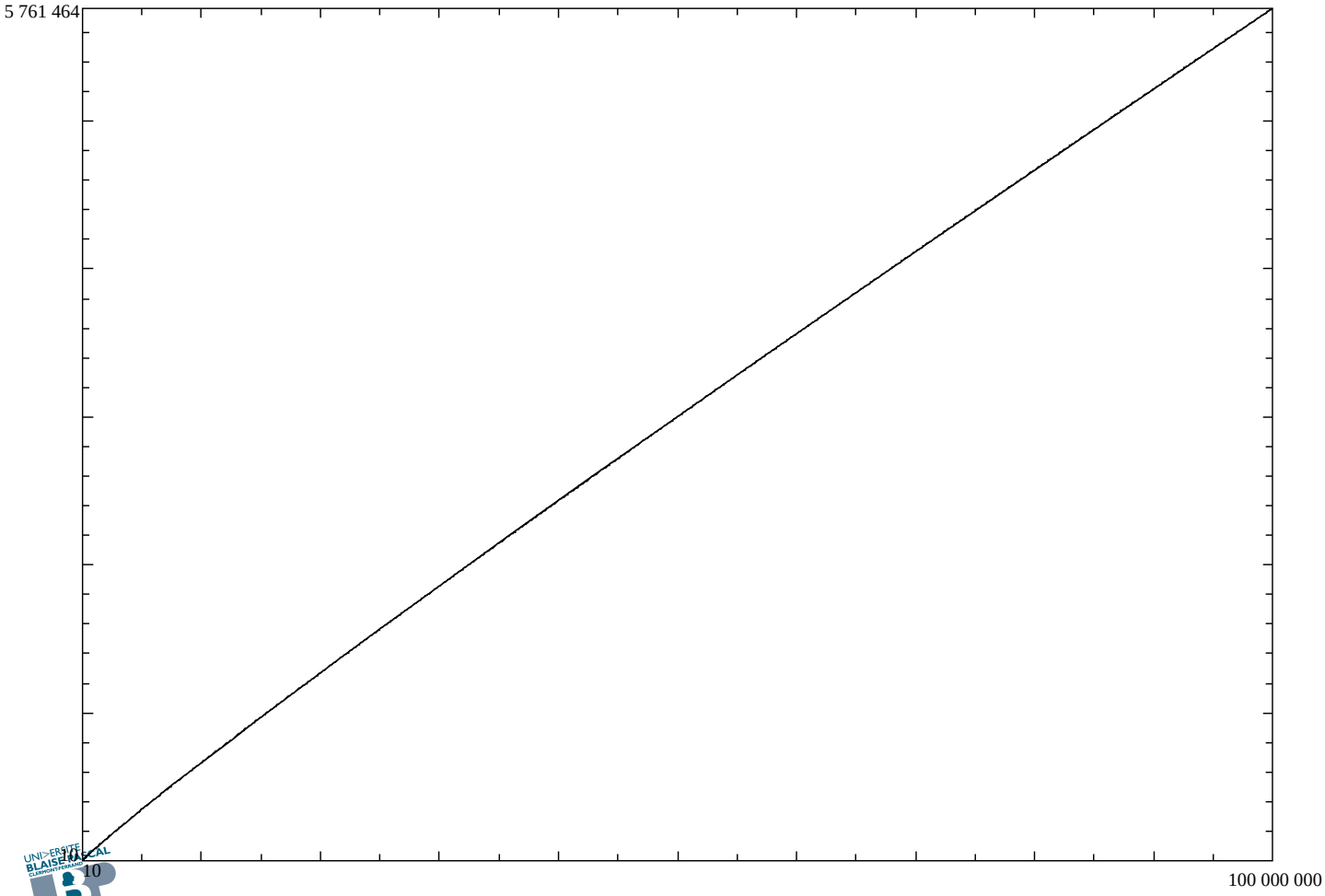
$$x \mapsto \pi(x)$$

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

Voyez-vous une différence ?

Combien ?

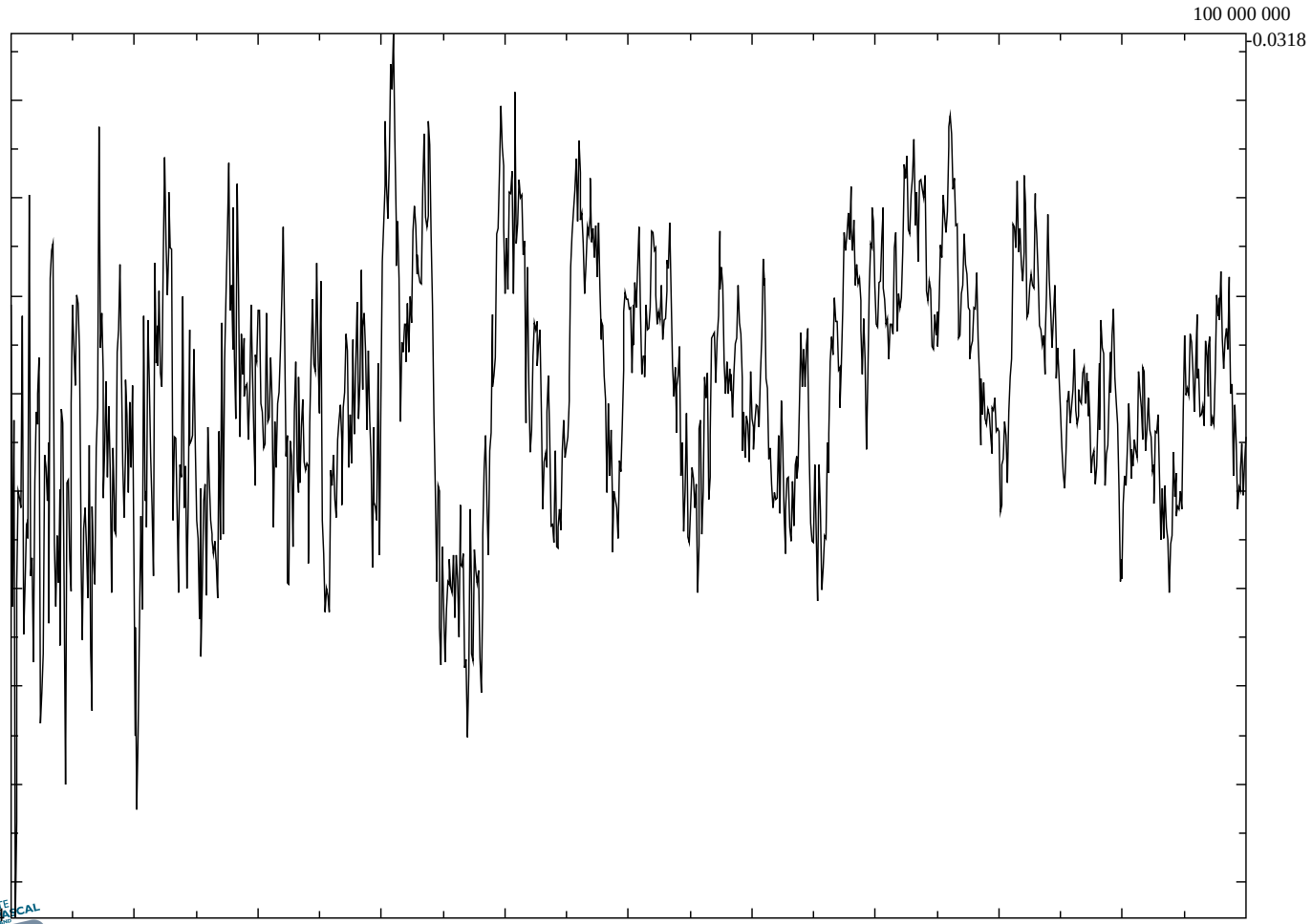
Qualité de l'estimation du vieux Gauss...



Comment distinguer ?

Combien ?

Qualité de l'estimation du vieux Gauss...



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

Vous voyez une différence !

Combien ?

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

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.

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

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

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 on donné une estimation de l'erreur.

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 on donné une estimation de l'erreur. Un thème de recherche de la théorie analytique des nombres est d'améliorer ce terme d'erreur.

Combien ?

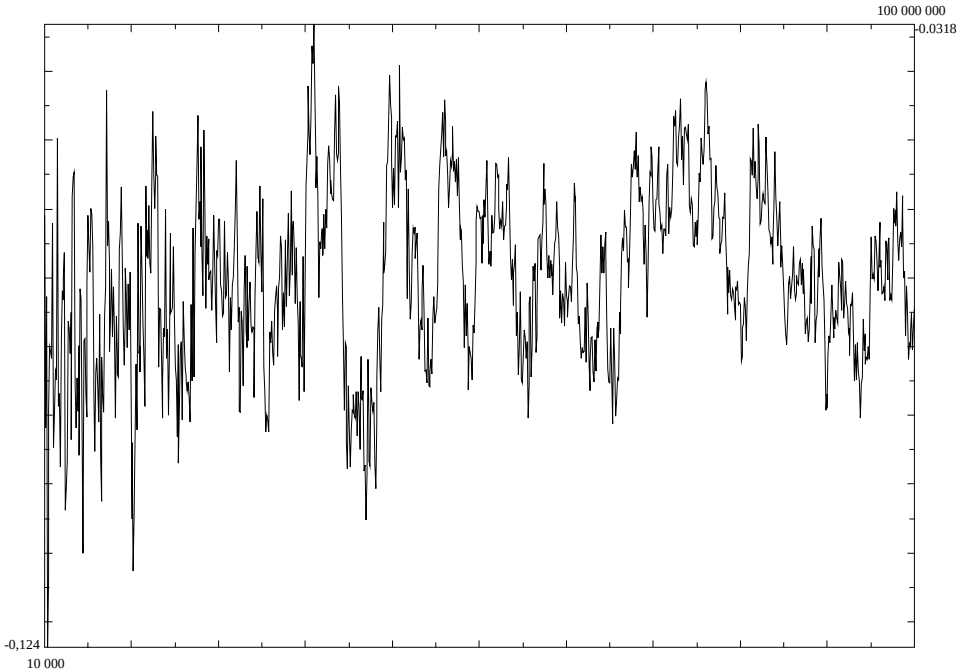
Le terme d'erreur

En particulier, on aimerait savoir montrer que le bon ordre de grandeur de l'erreur est (un peu plus grand que) $\sqrt{x}$).

Combien ?

Le terme d'erreur

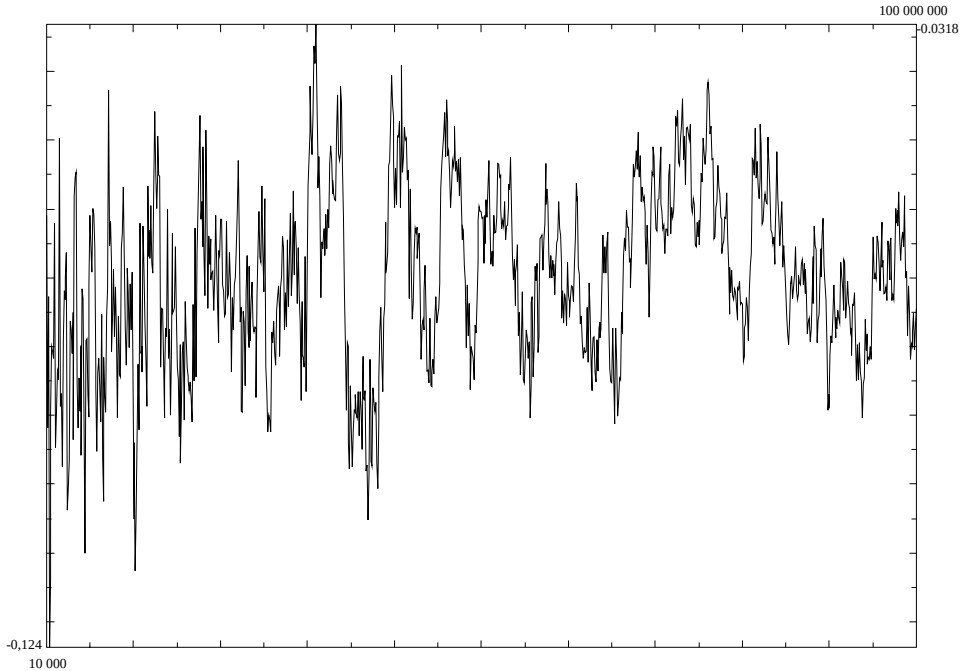
En particulier, on aimerait savoir montrer que le bon ordre de grandeur de l'erreur est (un peu plus grand que) $\sqrt{x}$).



Combien ?

Le terme d'erreur

En particulier, on aimerait savoir montrer que le bon ordre de grandeur de l'erreur est (un peu plus grand que) $\sqrt{x}$).



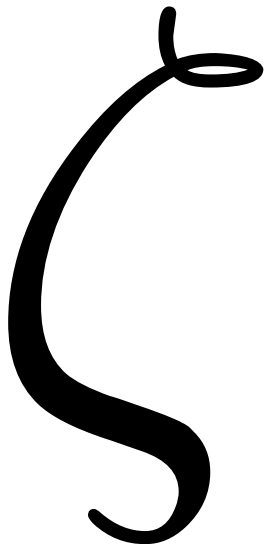
donc que la courbe ne sort que très lentement de la bande horizontale tracée.

La fonction ζ de Riemann

Le terme d'erreur conjecturé serait connu si on connaissait suffisamment la mystérieuse fonction

La fonction ζ de Riemann

Le terme d'erreur conjecturé serait connu si on connaissait suffisamment la mystérieuse fonction



La fonction ζ de Riemann

Le terme d'erreur conjecturé serait connu si on connaissait suffisamment la mystérieuse fonction

ζ

Le premier a faire un lien entre les nombres premiers et l'analyse complexe est Riemann en 1859.

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2}$$

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2} + \frac{1}{2^2}$$

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2}$$

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}$$

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2}$$

La fonction ζ de Riemann

Aux entiers

Calculons

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2}$$

pour n de plus en plus grand.

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111
100	1,634983900

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111
100	1,634983900
1000	1,643934567

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111
100	1,634983900
1000	1,643934567
5000	1,644734087

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111
100	1,634983900
1000	1,643934567
5000	1,644734087
10000	1,644834072

La fonction ζ de Riemann

Aux entiers

n	somme
1	1,000000000
2	1,250000000
3	1,361111111
4	1,423611111
100	1,634983900
1000	1,643934567
5000	1,644734087
∞	$\zeta(2)$

La fonction ζ de Riemann

Aux entiers

On procède de même pour tous les entiers valant au moins 2 :

La fonction ζ de Riemann

Aux entiers

On procède de même pour tous les entiers valant au moins 2 :

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \simeq 1,2020569\ldots$$

La fonction ζ de Riemann

Aux entiers

On procède de même pour tous les entiers valant au moins 2 :

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \simeq 1,2020569\ldots$$

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \cdots \simeq 1.0823232\ldots$$

La fonction ζ de Riemann

Aux entiers

On procède de même pour tous les entiers valant au moins 2 :

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \simeq 1,2020569\ldots$$

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \cdots \simeq 1.0823232\ldots$$

$$\zeta(5) = \frac{1}{1^5} + \frac{1}{2^5} + \frac{1}{3^5} + \cdots \simeq 1.0369278\ldots$$

La fonction ζ de Riemann

Aux entiers

On procède de même pour tous les entiers valant au moins 2 :

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \cdots \simeq 1,2020569\ldots$$

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \cdots \simeq 1.0823232\ldots$$

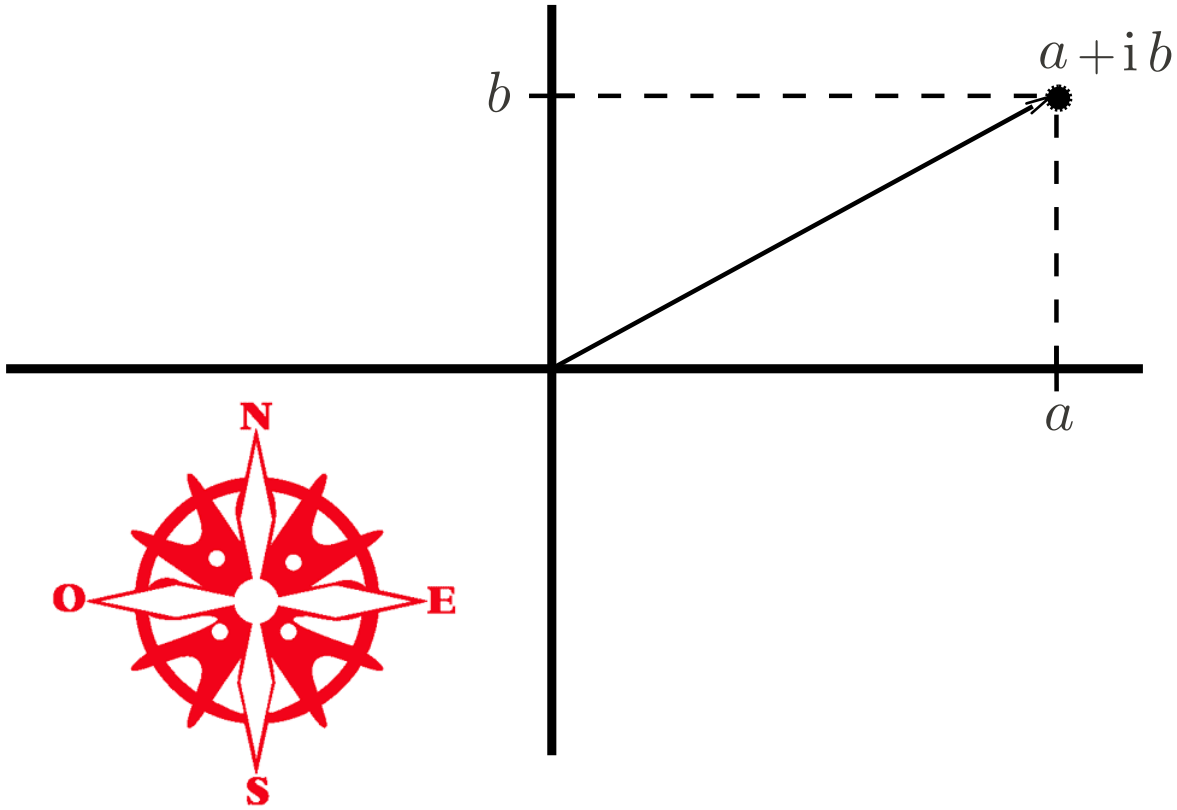
$$\zeta(5) = \frac{1}{1^5} + \frac{1}{2^5} + \frac{1}{3^5} + \cdots \simeq 1.0369278\ldots$$

On connaît une façon de donner un sens à ces calculs pour tous les nombres complexes différents de 1.

La fonction ζ de Riemann

Le plan complexe

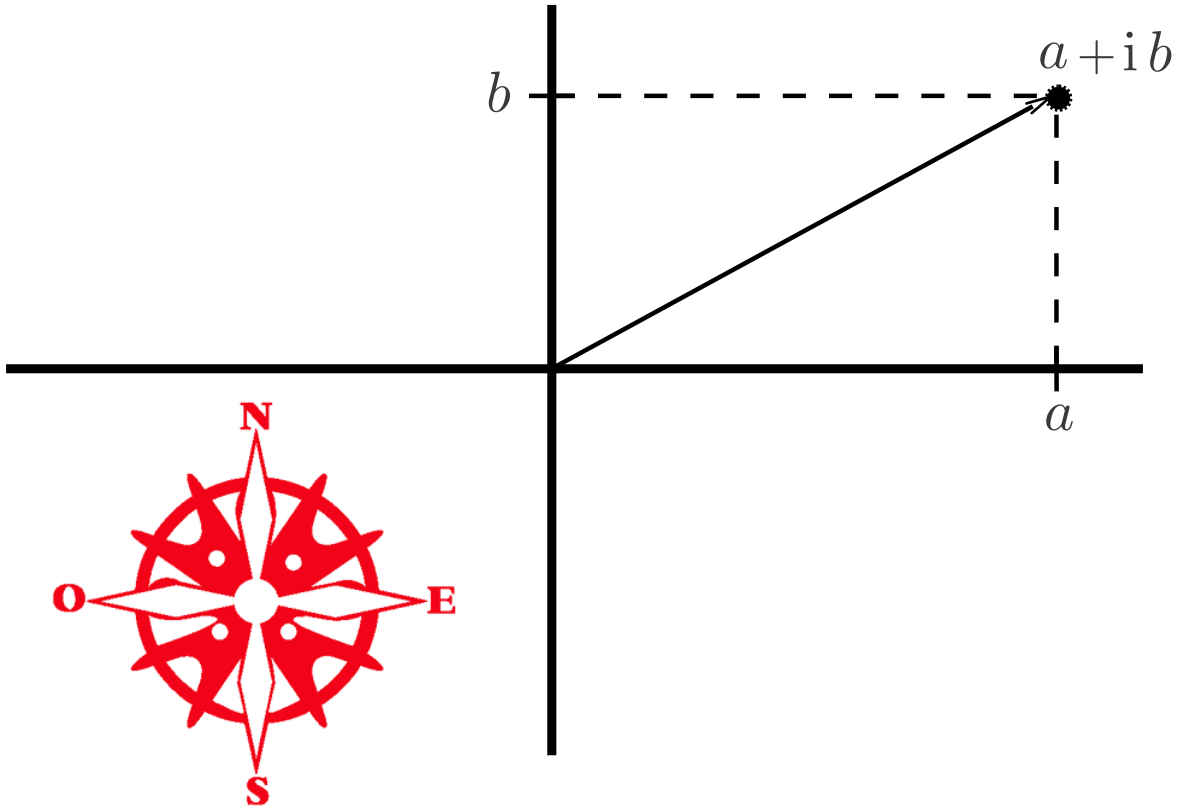
Les nombres complexes sont les points du plan,



La fonction ζ de Riemann

Le plan complexe

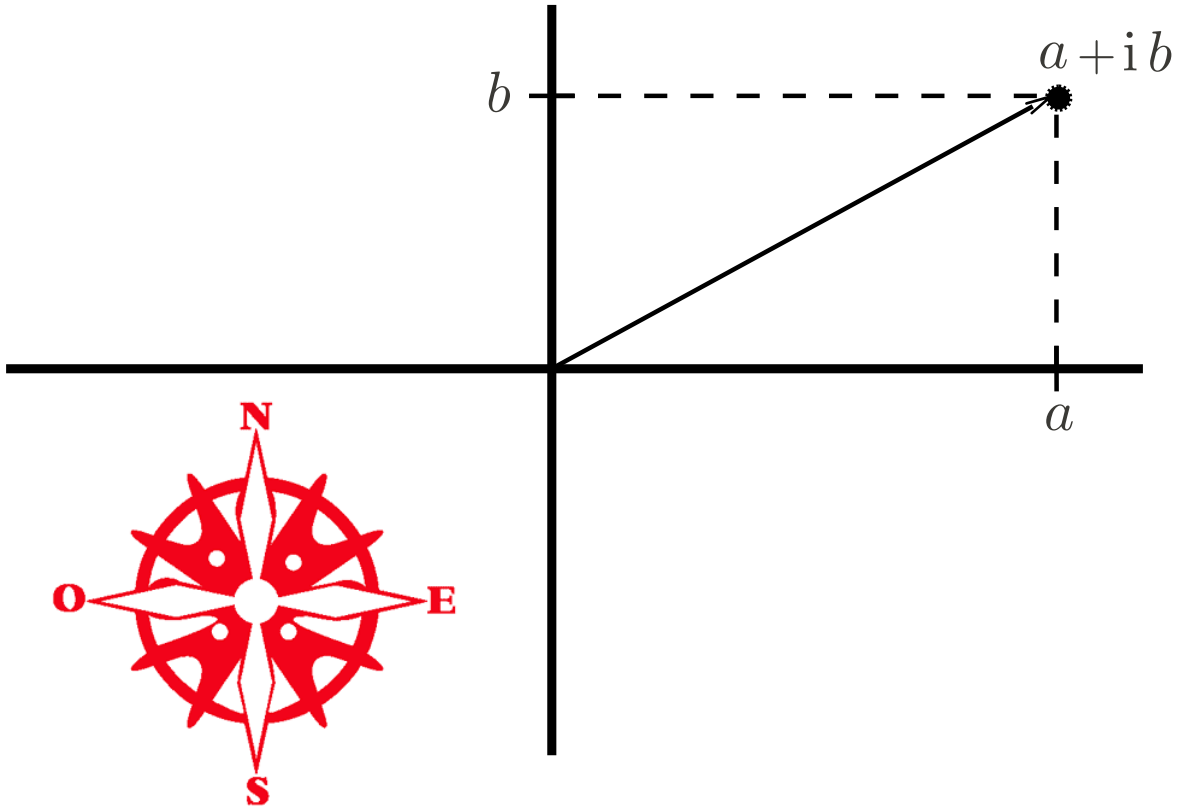
Les nombres complexes sont les points du plan, mais on sait les additionner



La fonction ζ de Riemann

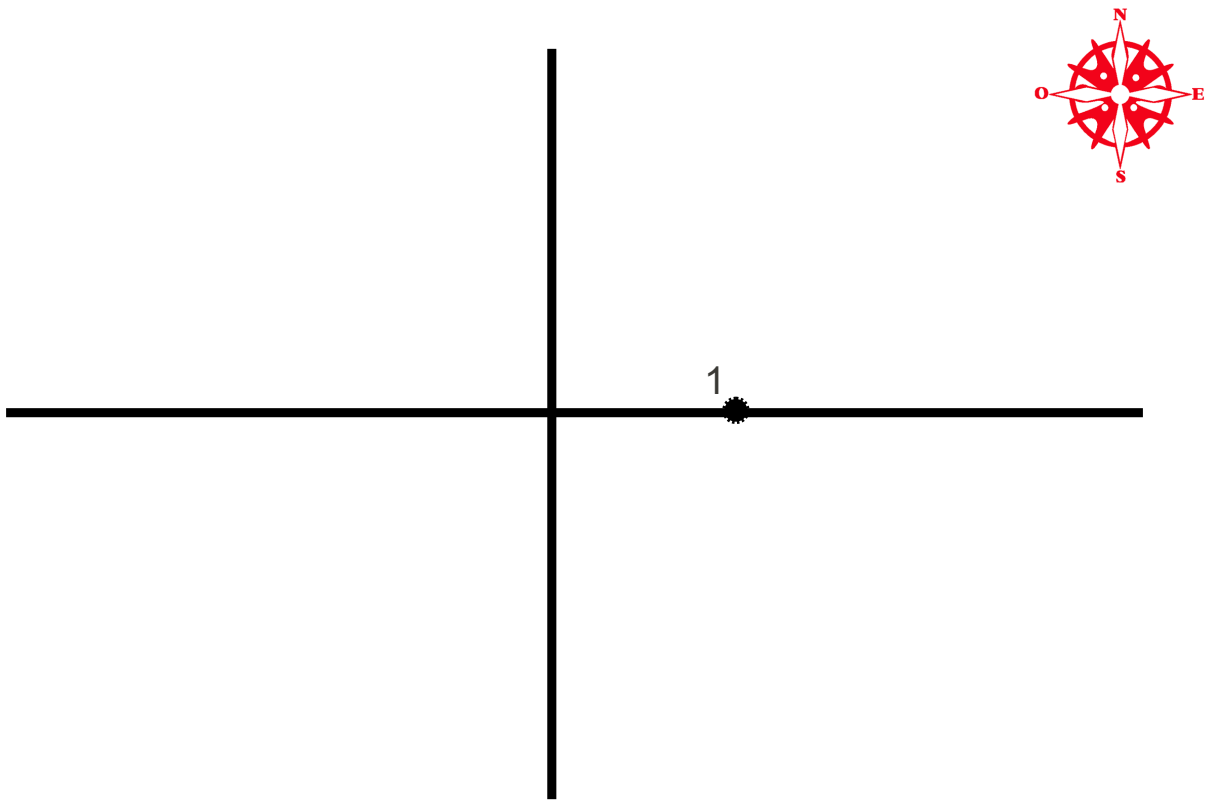
Le plan complexe

Les nombres complexes sont les points du plan, mais on sait les additionner et même les multiplier !



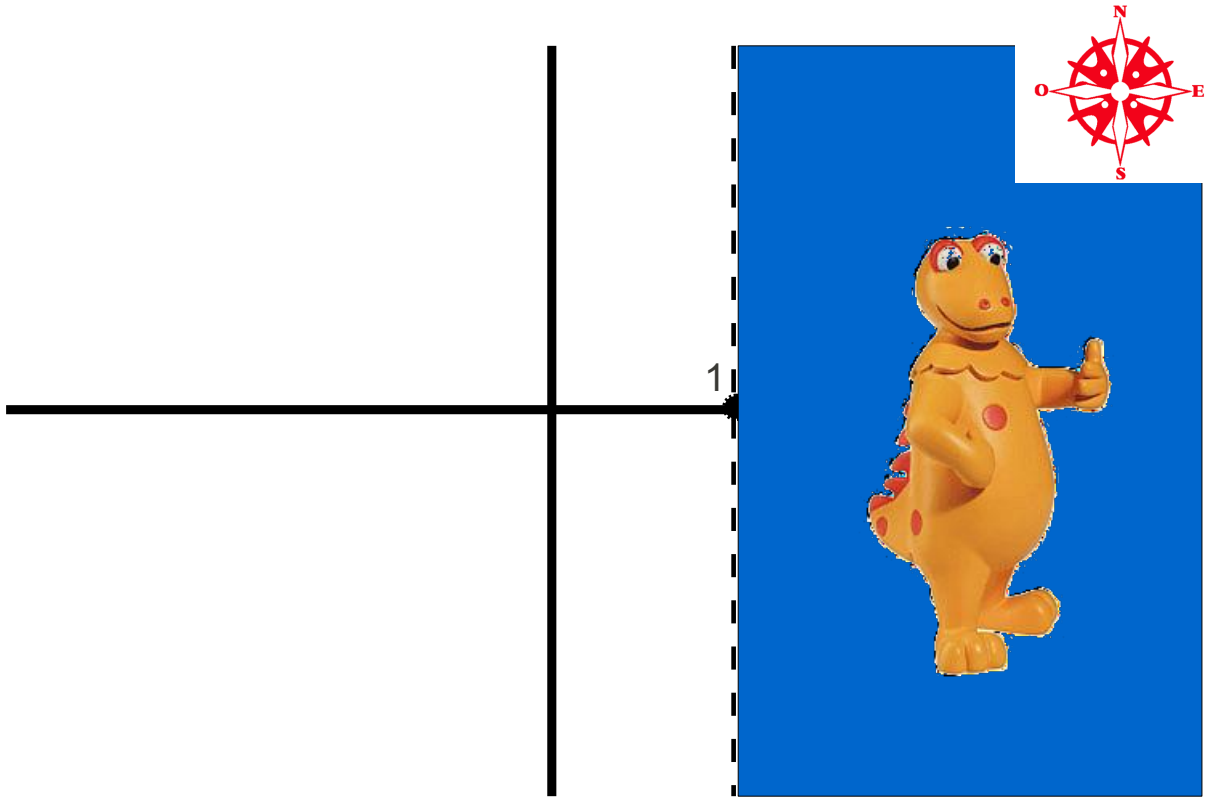
La fonction ζ de Riemann

On sait calculer $\zeta(z)$ pour tous les nombres complexes sauf pour 1.



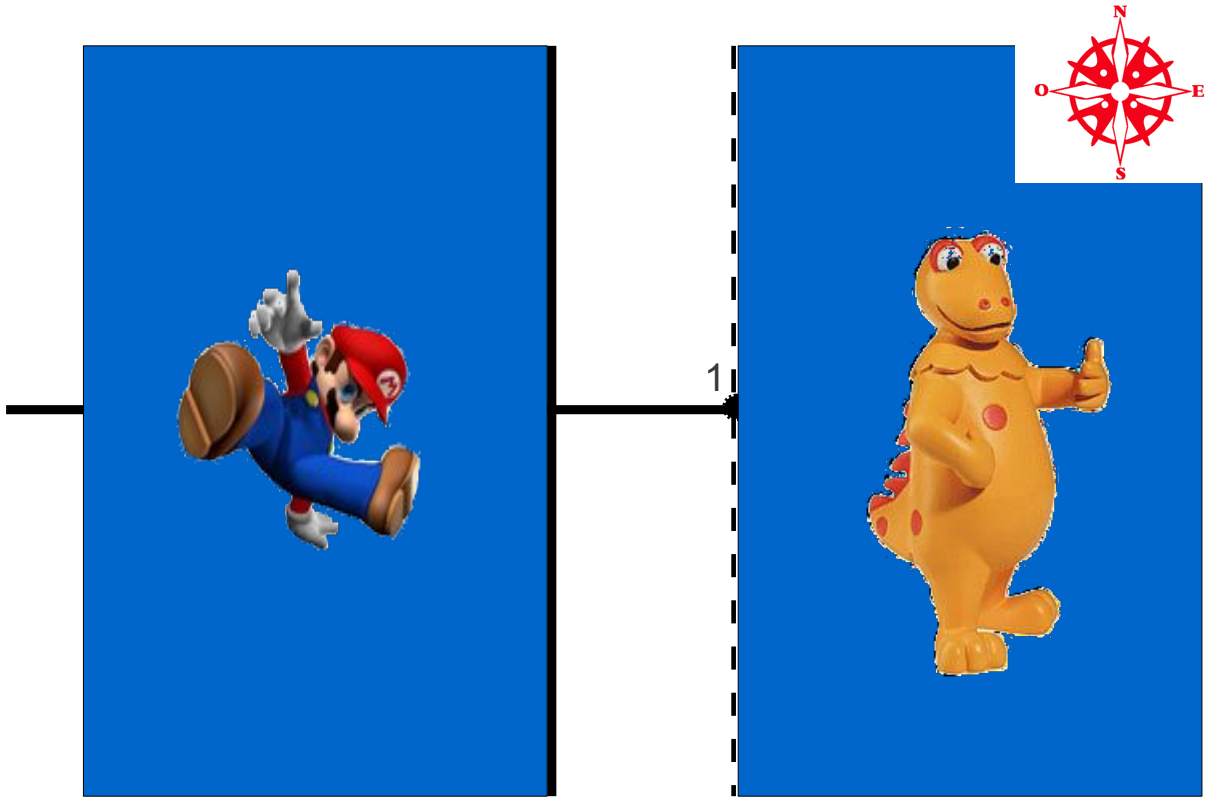
La fonction ζ de Riemann

On sait calculer $\zeta(z)$ pour tous les nombres complexes sauf pour 1. Pour les nombres complexes à l'Est de 1, c'est facile.



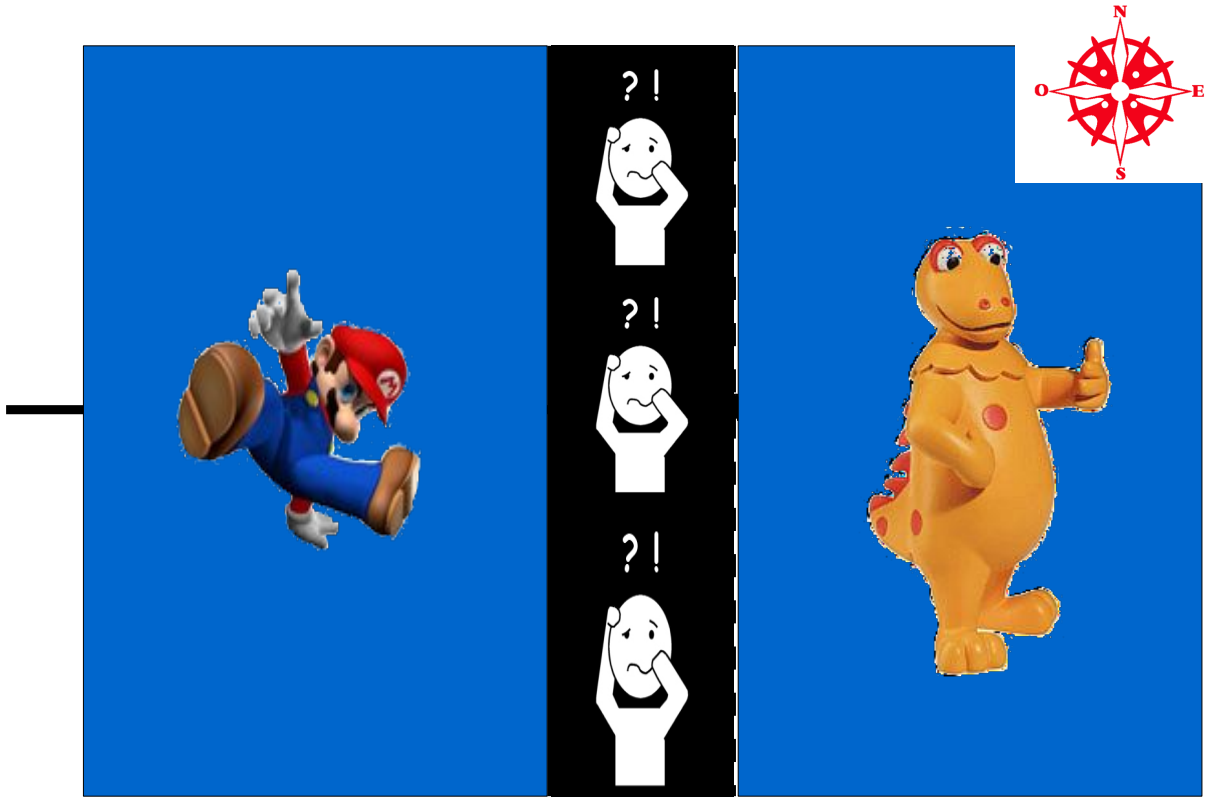
La fonction ζ de Riemann

On sait calculer $\zeta(z)$ pour tous les nombres complexes sauf pour 1. Pour les nombres complexes à l'Est de 1, c'est facile. Pour les nombres complexes à l'Ouest de 0, c'est facile.



La fonction ζ de Riemann

On sait calculer $\zeta(z)$ pour tous les nombres complexes sauf pour 1. Pour les nombres complexes à l'Est de 1, c'est facile. Pour les nombres complexes à l'Ouest de 0, c'est facile. Dans la région du milieu, c'est très difficile.



La fonction ζ de Riemann

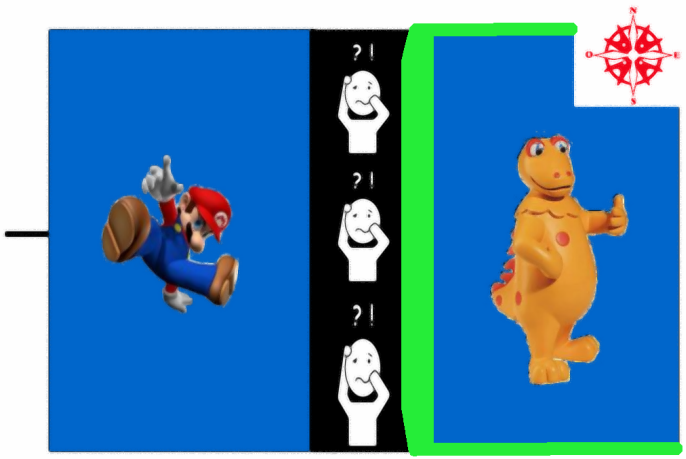
Hadamard & de la Vallée Poussin

Le travail de Hadamard et de la Vallée Poussin a consisté a explorer une petite région à l'Ouest de 1

La fonction ζ de Riemann

Hadamard & de la Vallée Poussin

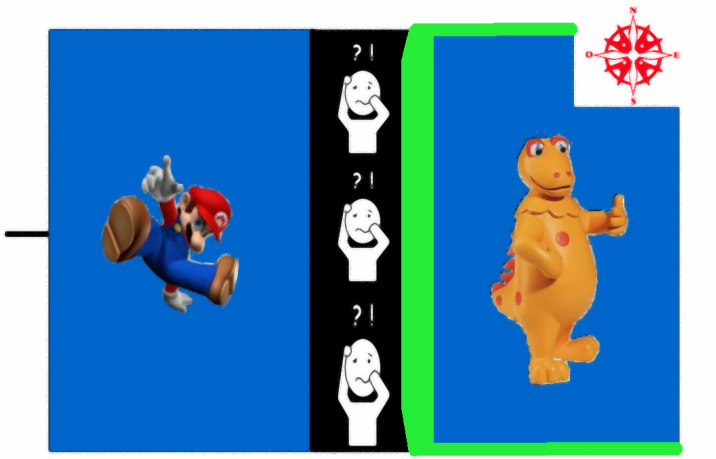
Le travail de Hadamard et de la Vallée Poussin a consisté a explorer une petite région à l'Ouest de 1 et à comprendre le Pic du Un.

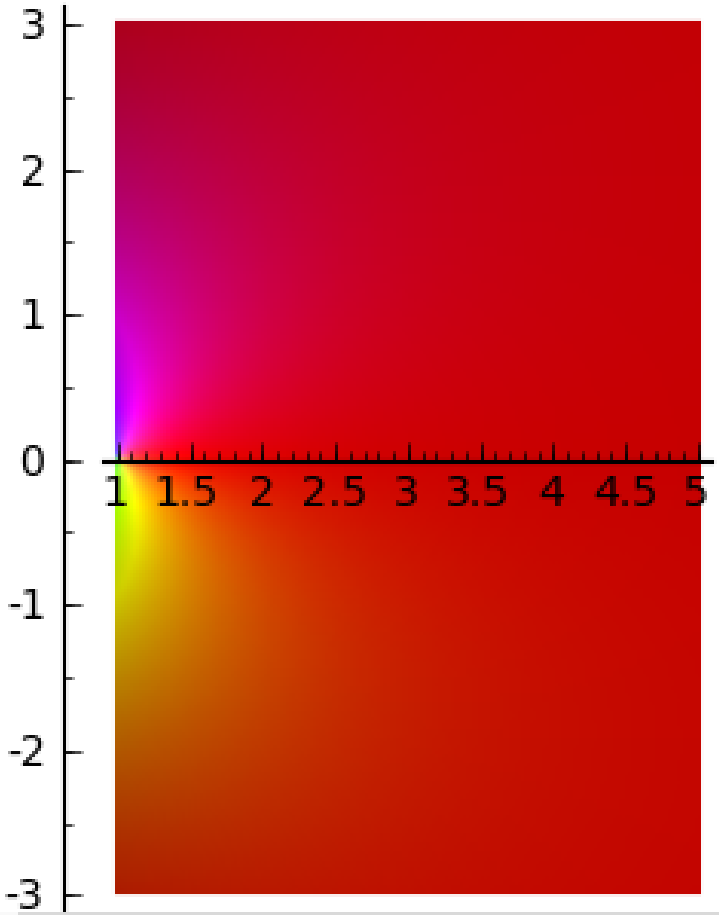


La fonction ζ de Riemann

Hadamard & de la Vallée Poussin

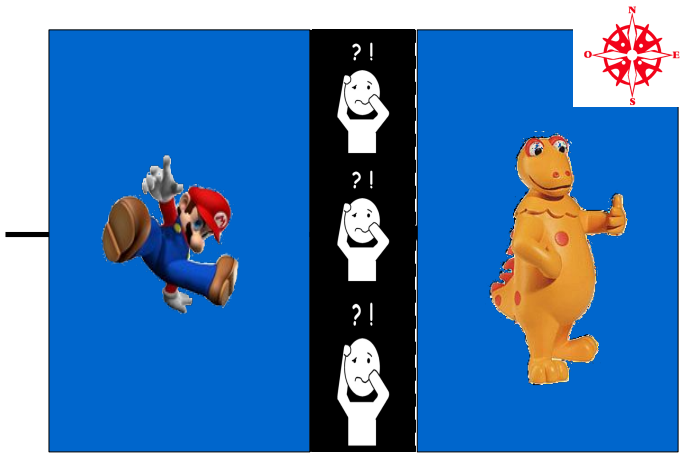
Le travail de Hadamard et de la Vallée Poussin a consisté a explorer une petite région à l'Ouest de 1 et à comprendre le Pic du Un.





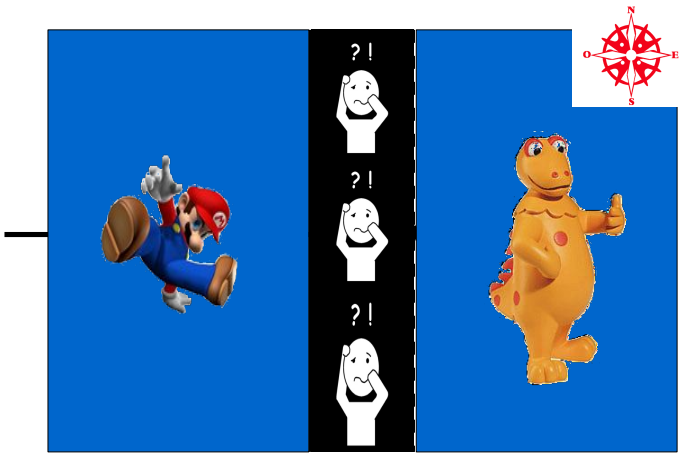
La fonction ζ de Riemann

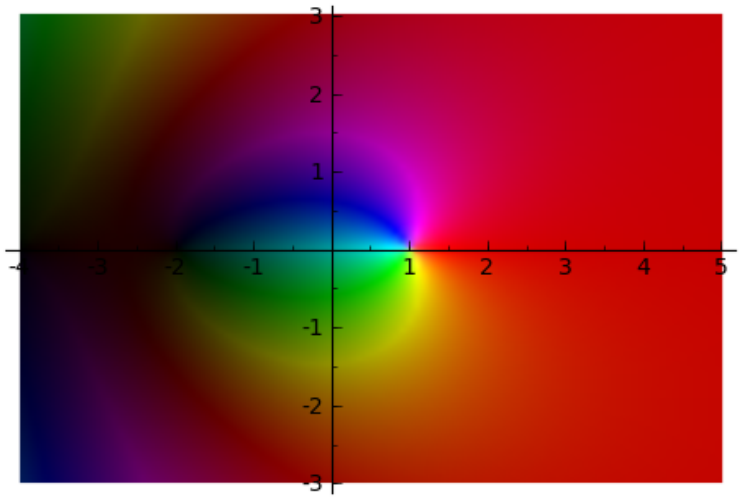
Partout



La fonction ζ de Riemann

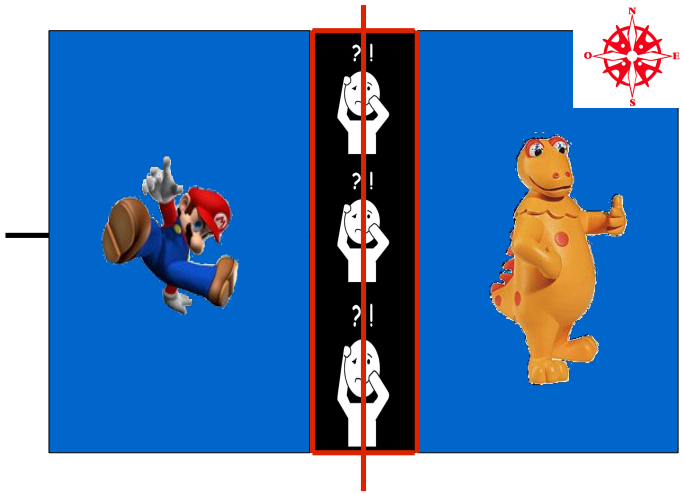
Partout





La fonction ζ de Riemann

Ce qui reste à explorer



La fonction ζ de Riemann

Ce qui reste à explorer