CRM-CNRS
International Research Lab

Nombres premiers

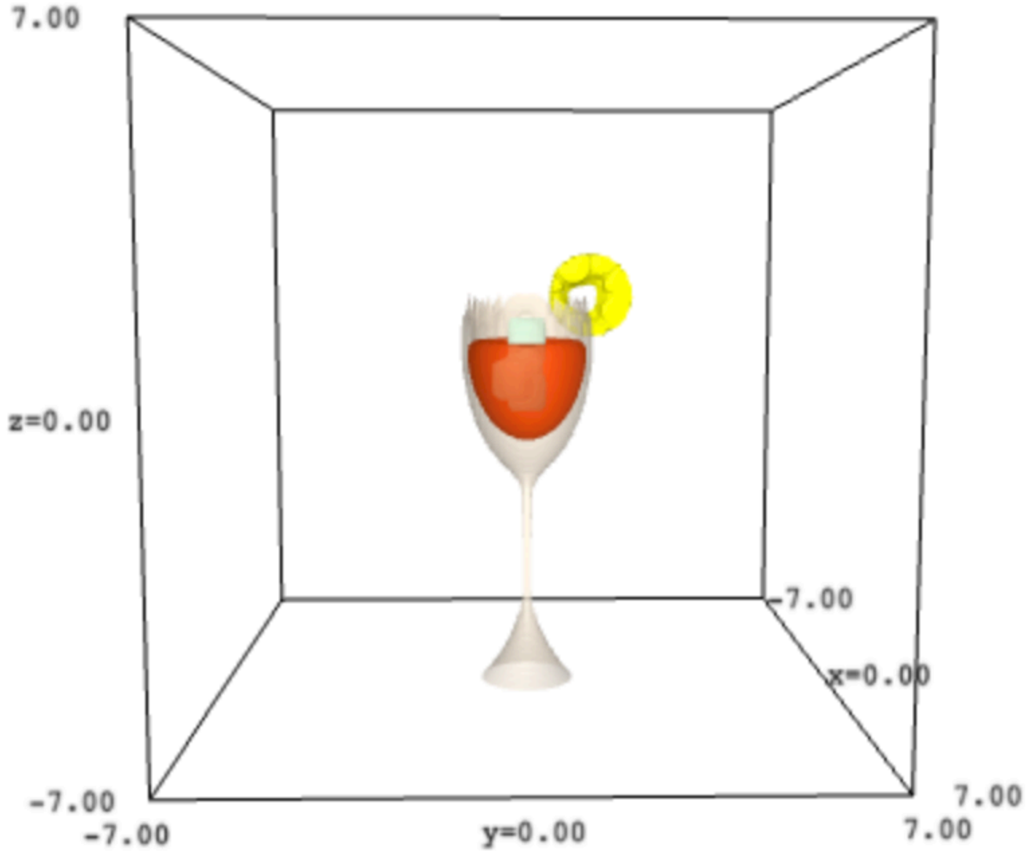
Collège Stanislas, Montréal - 4è - 19 février 2025

Emmanuel Royer, CNRS, Université Clermont-Auvergne

Nombres premiers

Qu’est-ce qu’un nombre premier ?

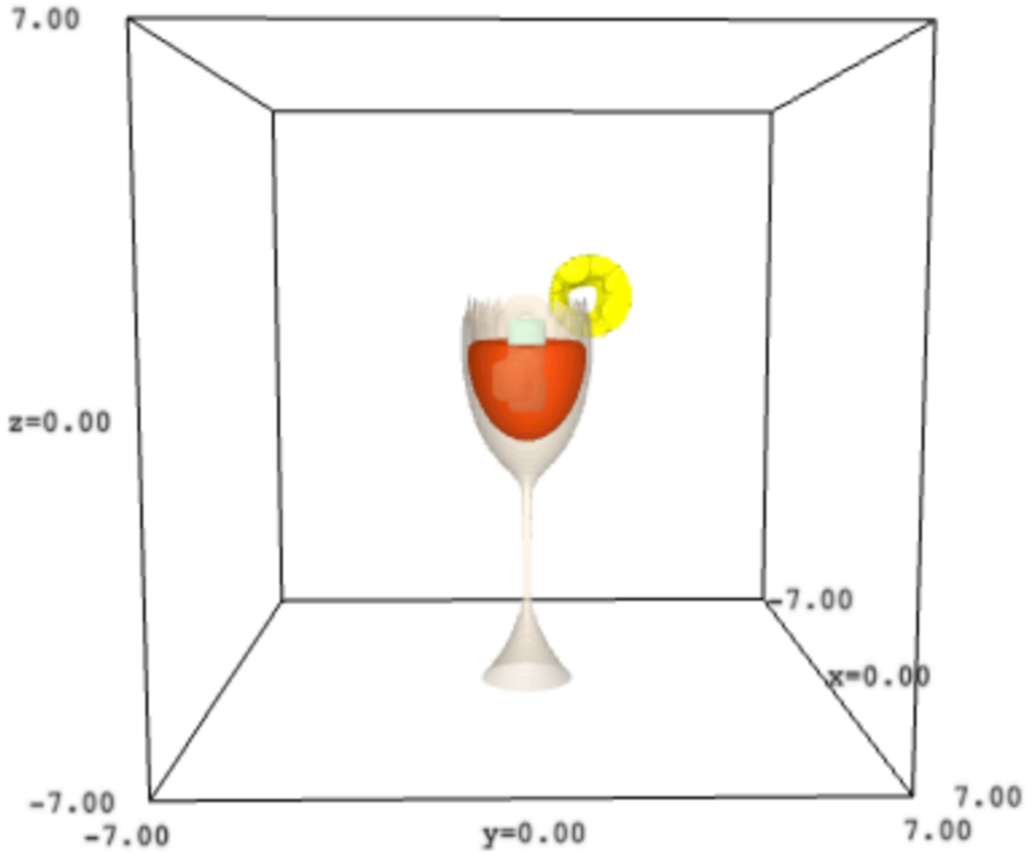
- Qu’est-ce qu’un nombre premier ?
- 1 est-il un nombre premier ?
- Existe-t-il des nombres premiers pairs ?



Nombres premiers

Qu’est-ce qu’un nombre premier ?

- Comment détecter si un nombre est premier ?
- 12 est-il un nombre premier ?
- Et 17 ?



Nombres premiers

Comment trouver tous les nombres premiers jusqu’à 100 ?

Nombres premiers

Comment trouver tous les nombres premiers jusqu’à 100 ?

Ératosthène enseignant à Alexandrie par Bernardo Strozzi (vers 1635).

Nombres premiers

Comment trouver tous les nombres premiers jusqu’à 100 ?

Installation *Mathémalchimie*
(extrait)

Visible à l’Université du Québec à Montréal jusqu’au 2 mai 2025

https://evenements.uqam.ca/evenements/mathemalchimie/29641

Nombres premiers

Comment trouver tous les nombres premiers jusqu’à 100 ?

	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

Réalisé avec Chat GPT

Nombres premiers

Comment trouver tous les nombres premiers jusqu'à 100 ?

	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

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

Nombres premiers

Comment trouver tous les nombres premiers jusqu'à 100 ?

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

Nombres premiers

Comment trouver tous les nombres premiers jusqu'à 100 ?

	2	3		5		7		
11		13				17		19
		23		25				29
31				35		37		
41		43				47		49
		53		55				59
61				65		67		
71		73				77		79
		83		85				89
91				95		97		

	2	3		5		7		
11		13				17		19
		23						29
31						37		
41		43				47		49
		53						59
61						67		
71		73				77		79
		83						89
91						97		

Nombres premiers

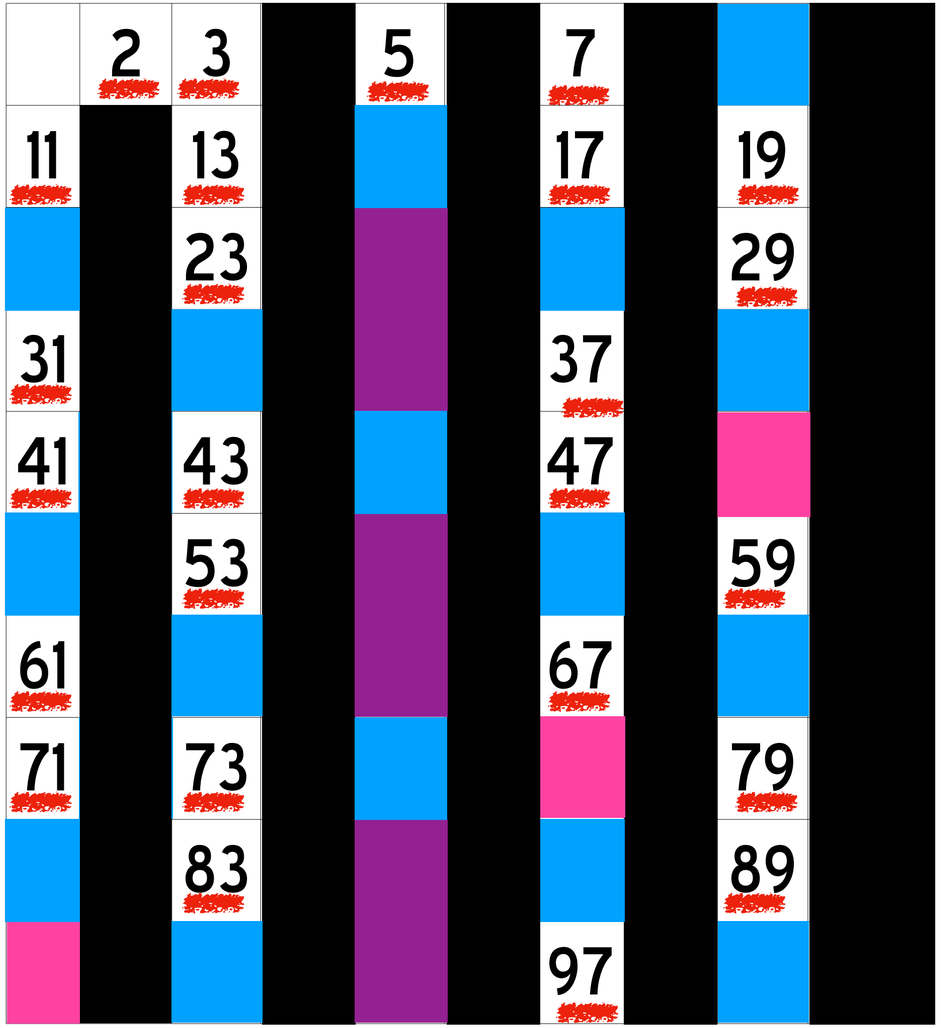
Comment trouver tous les nombres premiers jusqu'à 100 ?

	2	3		5		7		
11		13				17	19	
		23					29	
31						37		
41		43				47	49	
		53					59	
61						67		
71		73				77	79	
		83					89	
91						97		

	2	3		5		7		
11		13				17	19	
		23					29	
31						37		
41		43				47		
		53					59	
61						67		
71		73					79	
		83					89	
						97		

Nombres premiers

Comment trouver tous les nombres premiers jusqu'à 100 ?



Nombres premiers

Combien ?

Un ou une camarade vous donne un nombre entier.

Réalisé avec Chat GPT

Comment pouvez-vous lui donner un nombre plus grand ?

Nombres premiers

Combien ?

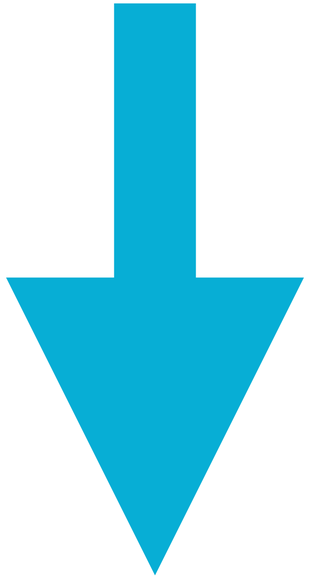
Un ou une camarade vous donne un nombre entier. Vous lui en donner un plus grand

Réalisé avec Chat GPT

Nombres premiers

Combien ?

Chaque fois qu’on vous donne un nombre entier, vous pouvez en trouver un strictement plus grand.

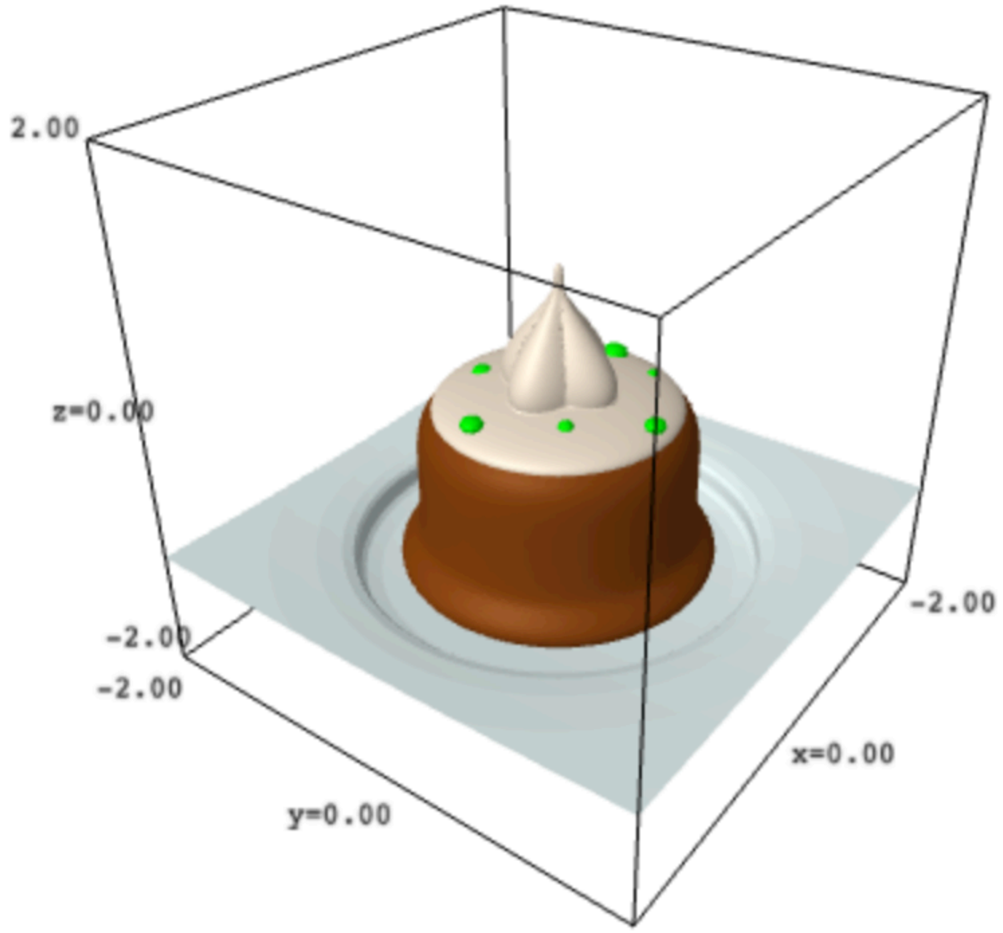


Il y a une infinité de nombres entiers.

Nombres premiers

Combien ?

Existe-t-il une infinité de nombres pairs ?



Nombres premiers

Combien ?

Un ou une camarade vous donne un nombre premier.

Pouvez-vous lui donner un nombre premier plus grand ?

Nombres premiers

Combien ?

Le plus grand nombre premier connu est depuis 2024 le nombre

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

Ce nombre a 41 024 320 chiffres décimaux.

Sans réfléchir, j'écris environ 120 chiffres en une minute. **Pour écrire ce nombre**, il me faudrait donc, à condition d'avoir mémorisé tous ses chiffres (!!!) : **237 jours**.

En les écrivant sur une bande, celle-ci mesurerait **143 km**

Couloir entre deux rangées du supercalculateur Jean Zay

Nombres premiers

- ✓ Donnez-moi un nombre premier
- ✓ Grâce au crible d'Ératosthène, je sais construire tous les nombres premiers plus petit
- ✓ Je fais le produit de tous ces nombres premiers que j'ai trouvé et j'ajoute 1
  - ✤ Soit le nombre que j'ai construit est premier : j'ai construit un nombre premier plus grand que le vôtre
  - ✤ Soit le nombre que j'ai construit n'est pas premier, je sais qu'il est divisible par un nombre premier, ça ne peut pas être un des nombres premiers que j'ai construit avec le crible d'Eratosthène à le deuxième étape : je sais donc qu'il existe un nombre premier plus grand que le vôtre (mais je ne sais pas donner sa valeur !)

Nombres premiers

Une infinité !

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

Euclide : 325 à 265 avant notre ère.

Nombres premiers

Un défi

Si p = 3 alors 2p+1 = 7 est premier

Si p = 5 alors 2p+1 = 11 est premier

Si p = 11 alors 2p+1 = 23 est premiers

Existe-t-il une infinite de nombre premiers p tels que 2p+1 est premier ?

C’est une question compliquée : en tout cas, je ne connais pas la réponse est ne connais personne qui la connaisse.

Ces nombres s’appellent nombres de Germain, en l’honneur de SOPHIE GERMAIN qui a réalisé des travaux montrant l’utilité de tels nombres.

Cryptographie

Factoriser est difficile, vérifier est facile

«Lors de la réunion d'octobre 1903 à New York de l'*American Mathematical Society*, Cole avait un exposé au programme avec le titre modeste *On the factorization of large numbers*. Lorsque le président lui a demandé de présenter sa communication, Cole — qui a toujours été un homme de peu de mots — s'est dirigé vers le tableau et, sans rien dire, a commencé à tracer à la craie les calculs pour élever 2 à la puissance 67. Puis il soustrait soigneusement 1. Sans un mot, il se dirigea vers un espace libre sur le tableau et multiplia, à la main $193\,707\,721 \times 761\,838\,257\,287$. Les deux calculs concordent... Pour la première et unique fois dans les annales, le public de l'*American Mathematical Society* a vigoureusement applaudi l'auteur d'un article présenté devant lui. Cole a pris place sans avoir prononcé un mot. Personne ne lui a posé de question.»

https://thatsmaths.com/2016/06/30/lecture-sans-paroles-the-factors-of-m67/

Cryptographie

Factoriser est difficile, vérifier est facile

Le nombre entier

$$2^{67} - 1 = 193\,707\,721 \times 761\,838\,257\,287$$

n’est pas premier

```
√ ~ % gp
Reading GPRC: /Users/emmanuel.royer/.gprc
GPRC Done.

                GP/PARI CALCULATOR Version 2.18.1 (development 29965-b1b821b1e0)
                 arm64 running darwin (aarch64/GMP-6.3.0 kernel) 64-bit version
               compiled: Feb  7 2025, Apple clang version 16.0.0 (clang-1600.0.26.6)
                             threading engine: pthread, nbthreads = 10
                           (readline v8.2 enabled, extended help enabled)

                                Copyright (C) 2000-2025 The PARI Group

? factor(2^67-1)
cpu time = 3 ms, real time = 3 ms.
%1 =
[   193707721 1]

[761838257287 1]
```

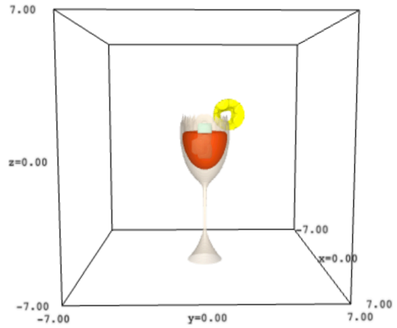
ON THE FACTORING OF LARGE NUMBERS.

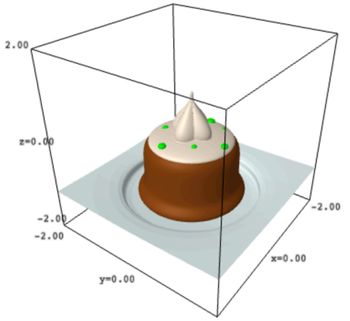
BY PROFESSOR F. N. COLE.

(Read before the American Mathematical Society, October 31, 1903.)

Les dessins

Rien à voir avec les premiers





Mais tous ont avoir avec les mathématiques : ils sont décrits par des équations dues à Valentina GALATA et disponible sur le site internet d'imaginary.org

Le verre

$$((x^2+y^2+(0.5z-0.6)^2-2)^2+(0.1z-0.2))(11x^2+11y^2+0.05(z+4)^5-0.09)-1=0$$

La tranche

$$\begin{aligned}&((5x+3)^6+(y-1.5)^2+(z-2)^2-1)((y-1.5)^2+(x+0.5)^2-0.00000001)\\&\times((z-2)^2+(x+0.5)^2-0.00000001)((y-z+0.6)^2+(x+0.5)^2-0.00000001)\\&\times((y+z-3.2)^2+(x+0.5)^2-0.00000001)+0.0002=0\end{aligned}$$

Le liquide

$$(x^2+y^2+(0.6z-0.6)^2-2)(x^2+y^2+(z-1.99)^6-2)+0.37=0$$

Les glaçons

$$\left(x^6+y^6+(z+0.2)^6-0.01\right)\left(\left(0.5(x-1)+z\right)^6+y^6+\left((0.5(z-0.5)-x-0.7\right)^6-0.01\right)=0$$

D'autres glaçons

$$((0.5x-1*z+1)^6+y^6+(0.5z+x-0.6)^6-0.01)((0.5x+y+0.1)^6+(0.5y-x+0.59)^6+(z-0.1)^6-0.01)=0$$