Les nombres premiers ne sont pas si aléatoires

Annamaria Iezzi

Institut des Mathématiques de Marseille, Université d'Aix-Marseille

A travers champs - Hasard, 6 Juin 2014

Définition

Un **nombre premier** est un entier naturel plus grand que 1 qui admet exactement deux diviseurs positifs, 1 et lui même.

Définition

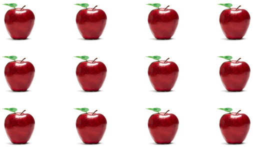
Un **nombre premier** est un entier naturel plus grand que 1 qui admet exactement deux diviseurs positifs, 1 et lui même.

$$1 \times 12$$

Définition

Un **nombre premier** est un entier naturel plus grand que 1 qui admet exactement deux diviseurs positifs, 1 et lui même.

1×12

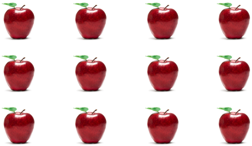


3×4

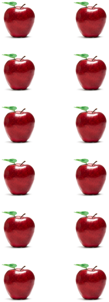
Définition

Un **nombre premier** est un entier naturel plus grand que 1 qui admet exactement deux diviseurs positifs, 1 et lui même.

1×12



3×4



6×2

Définition

Un **nombre premier** est un entier naturel plus grand que 1 qui n'admet autre diviseur positive que 1 et lui même.

Définition

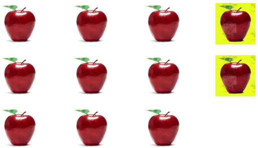
Un **nombre premier** est un entier naturel plus grand que 1 qui n'admet autre diviseur positive que 1 et lui même.

$$1 \times 11$$

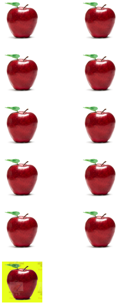
Définition

Un **nombre premier** est un entier naturel plus grand que 1 qui n'admet autre diviseur positive que 1 et lui même.

$$1 \times 11$$



$$3 \times 3 + 2$$



$$5 \times 2 + 1$$

Théorème fondamental de l'arithmétique

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

Théorème fondamental de l'arithmétique

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

$$7956 = 2^2 \times 3^2 \times 13 \times 17 = 2 \times 3 \times 13 \times 17 \times 2 \times 3$$

Théorème fondamental de l'arithmétique

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

$$7956 = 2^2 \times 3^2 \times 13 \times 17 = 2 \times 3 \times 13 \times 17 \times 2 \times 3$$

"Les nombres premiers sont les atomes mêmes de l'arithmétique. [...] Ils sont les pierres précieuses enchâssées dans l'immense étendue de l'univers infini des nombres, que les mathématiciens explorent depuis des siècles. Ils sont pour eux une source d'émerveillement : 2, 3, 5, 7, 11, 13, 17, 19, 23... nombres hors du temps qui existent dans un monde indépendant de notre réalité physique. Pour le mathématicien, ils sont un don de la Nature." - Marcus du Sautoy

Théorème (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

Théorème (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

$$\Downarrow$$

Il n'existe pas de plus grand nombre premier.

Théorème (Théorème d'Euclide)

Il existe une infinité de nombres premiers.

$$\Downarrow$$

Il n'existe pas de plus grand nombre premier.
Cependant beaucoup de mathématiciens "s'amusent" à chercher le plus grand nombre premier connu.

RECORD ACTUEL

25 janvier 2013: $\mathbf{2^{57.885.161} - 1}$

Cet objet mathématique est composé de plus de 17 millions de chiffres et remplirait près de 20 livres de 500 pages environ.

- Liste des nombres premiers inférieurs à 100:

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

- Liste des nombres premiers inférieurs à 100:

  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

- Liste des nombres premiers parmi les 100 nombres précédant 10.000.000:

  9.999.901, 9.999.907, 9.999.929, 9.999.31, 9.999.937, 9.999.943,
  9.999.971, 9.999.973, 9.999.991

- Liste des nombres premiers parmi les 100 nombres suivant 10.000.000:

  10.000.019, 10.000.079

- Liste des nombres premiers inférieurs à 100:

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

- Liste des nombres premiers parmi les 100 nombres précédant 10.000.000:

  $9.999.901, 9.999.907, 9.999.929, 9.999.31, 9.999.937, 9.999.943,$
  $9.999.971, 9.999.973, 9.999.991$

- Liste des nombres premiers parmi les 100 nombres suivant 10.000.000:

  $10.000.019, 10.000.079$

A première vue on s'aperçoit que le rythme avec lequel ils se succèdent est irrégulier et imprévisible...

Considérons la suite des nombres carrés:

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$$

Considérons la suite des nombres carrés:

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$$

C'est facile de déterminer le n-ème nombre carré, qui est donné par la simple formule n^2.

Considérons la suite des nombres carrés:

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$$

C'est facile de déterminer le n-ème nombre carré, qui est donné par la simple formule n^2.
On peut aussi considérer des suites plus compliquées, comme celle des nombres triangulaires:

$$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, \ldots$$

et trouver que le n-ème nombre triangulaire est donné par $\frac{n(n+1)}{2}$.

Considérons la suite des nombres carrés:

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$$

C'est facile de déterminer le n-ème nombre carré, qui est donné par la simple formule n^2.
On peut aussi considérer des suites plus compliquées, comme celle des nombres triangulaires:

$$1, 3, 6, 10, 15, 21, 28, 36, 45, 55, \ldots$$

et trouver que le n-ème nombre triangulaire est donné par $\frac{n(n+1)}{2}$.

Existe-il, similairement, une fonction " efficace" qui associe à un entier n le n-ème nombre premier?
Ce problème de déterminer une formule magique pour le n-ème nombre premier passionne les têtes mathématiciennes depuis plusieurs siècles et il n'a pas encore trouvé une solution.

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{\sum_{j=1}^{m} F(j)} \right\rfloor^{\frac{1}{n}} \right\rfloor,$$

où

$$F(j) = \left\lfloor \cos^2 \left[\pi \frac{(j-1)!+1}{j} \right] \right\rfloor = \begin{cases} 1 & \text{si } j = 1 \text{ ou } j \text{ premier} \\ 0 & \text{sinon} \end{cases}$$

Pour souligner cette imprévisibilité dans la suite des nombres premiers, on peut citer le résultat suivant:

Suite de composés consécutifs

Pour tout $N > 1$, il existe une succession d'au moins N entiers consécutifs non premiers.

N	**1**	**3**	**5**	**7**	**13**	**17**
	1	8	24	90	114	524
		9	25	91	115	525
		10	26	92	116	526
			27	93	117	527
			28	94	118	528
				95	119	529
				96	120	530
					121	531
					122	532
					123	533
					124	534
					125	535
					126	536
						537
						538
						539
						540

Pour souligner cette imprévisibilité dans la suite des nombres premiers, on peut citer le résultat suivant:

Suite de composés consécutifs

Pour tout $N > 1$, il existe une succession d'au moins N entiers consécutifs non premiers.

N	**1**	**3**	**5**	**7**	**13**	**17**
	1	8	24	90	114	524
		9	25	91	115	525
		10	26	92	116	526
			27	93	117	527
			28	94	118	528
				95	119	529
				96	120	530
					121	531
					122	532
					123	533
					124	534
					125	535
					126	536
						537
						538
						539
						540

En général

$$\begin{array}{ll} N! + 2 & \text{divisible par } 2 \\ N! + 3 & \text{divisible par } 3 \\ N! + 4 & \text{divisible par } 4 \\ & \vdots \\ N! + i & \text{divisible par } i \\ & \vdots \\ N! + N & \text{divisible par } N \end{array}$$

D'autre part, on peut trouver des nombres premiers très proches:

$$41, 43$$

$$881, 883$$

$$2003663613 \cdot 2^{195000} \pm 1$$

On appelle **nombres premiers jumeaux** ces couples de nombres premiers qui diffèrent de 2.

Conjecture des nombres premiers jumeaux

Il existe une infinité de nombres premiers jumeaux.

Dans cette perspective il semblerait alors normal d'affirmer que les nombres premiers sont distribués au **hasard** dans l'ensemble des nombres naturels, où le mot hasard exprime cette impossibilité de trouver une structure, une régularité, une logique interne dans la suite qu'ils définissent.

Mais appelle-t-on simplement "hasard" la limite intellectuelle qui nous empêche de comprendre leur structure?

"God may not play dice with the universe, but something strange is going on with the prime numbers." - Paul Erdös

"It is evident that the primes are randomly distributed but, unfortunately, we don't know what 'random' means." - Bob Vaughan

Changement de perspective

Johann Carl Friedrich Gauss (1777-1855)

Changement de perspective

Johann Carl Friedrich Gauss (1777-1855)

Plutôt que d'essayer de prédire quels nombres sont premiers, on peut se demander combien de nombres sont premiers parmi les N premiers nombres...

N	Nombre de nombres premiers compris entre 1 et N	Distance "moyenne" entre deux nombres premiers consécutifs
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

"As a boy I considered the problem of how many primes there are up to a given point. From my computations, I determined that the density of primes around x, is about $\frac{1}{\log x}$." - C.F. Gauss

"As a boy I considered the problem of how many primes there are up to a given point. From my computations, I determined that the density of primes around x, is about $\frac{1}{\log x}$." - C.F. Gauss

Théorème des nombres premiers (Hadamard, de La Vallée Poussin - 1896)

Pour n assez grand, la probabilité qu'un nombre "autour" de n soit premier est $\frac{1}{\log n}$.

Even though number theory is a deterministic subject (one does not need to roll any dice to factorise a number, or figure out if a number is prime), one expects to get a good asymptotic prediction for the answers to many number-theoretic questions by pretending that various number-theoretic assertions E (e.g. that a given number n is prime) are probabilistic events (with a probability $P(E)$ that can vary between 0 and 1) rather than deterministic events (that are either always true or always false). - Terence Tao

"Individual primes are believed to behave randomly, but the collective behaviour of the primes is believed to be quite predictable." - Terence Tao

"Every fool can ask questions about prime numbers that the wisest man cannot answer" - G.H. Hardy