Les nombres premiers

E. Kowalski

ETH Zürich / S.M.O-Tag 2009

28 Mars 2009

Was sind und was sollen die Primzahlen?

Les nombres premiers

Un entier positif $p > 1$ est un *nombre premier* si il n'est pas possible de l'écrire sous la forme

$$p = a \times b$$

où a et b sont eux-mêmes des entiers $a > 1$, $b > 1$.

Les nombres premiers

Un entier positif $p > 1$ est un *nombre premier* si il n'est pas possible de l'écrire sous la forme

$$p = a \times b$$

où a et b sont eux-mêmes des entiers $a > 1$, $b > 1$.

Par exemple :

$$2, \quad 3, \quad 5, \quad 7, \ldots, 641, \ldots, 2^{43112609}-1, \ldots$$

Les nombres premiers

Un entier positif $p > 1$ est un *nombre premier* si il n'est pas possible de l'écrire sous la forme

$$p = a \times b$$

où a et b sont eux-mêmes des entiers $a > 1$, $b > 1$.

Par exemple :

$$2, \quad 3, \quad 5, \quad 7, \ldots, 641, \ldots, 2^{43112609}-1, \ldots$$

mais pas

$$5007 = 3 \cdot 1669, \qquad 156839 = 2209 \cdot 71, \qquad 8102008 = 8 \cdot 1012751.$$

(Le nombre $2^{43112609} - 1$ est le plus grand nombre premier connu, découvert en Août 2008.)

Factorisation

L'importance des nombres premiers découle du fait que chaque entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers, avec éventuellement des répétitions.

Factorisation

L'importance des nombres premiers découle du fait que chaque entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers, avec éventuellement des répétitions.

Par exemple :

$$17179869175 = 5 \cdot 5 \cdot 7 \cdot 7 \cdot 53 \cdot 107 \cdot 2473.$$

Factorisation

L'importance des nombres premiers découle du fait que chaque entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers, avec éventuellement des répétitions.

Par exemple :

$$17179869175 = 5 \cdot 5 \cdot 7 \cdot 7 \cdot 53 \cdot 107 \cdot 2473.$$

Si on ordonne les nombres premiers qui apparaissent par ordre croissant, ils sont déterminés de manière unique par n, ainsi que le nombre de répétition de chacun.

Combien y-a-t-il de nombres premiers ?

EUCLIDE avait déjà prouvé qu'il existe une infinité de nombres premiers !

Il existe beaucoup de preuves de cette propriété fondamentale, et en voici une particulièrement élégante, due apparemment à un certain Hacks aux alentours de 1890.

Une preuve du théorème d'Euclide

Première étape. Euler a montré vers 1735 que le produit

$$\frac{1}{1-\frac{1}{4}} \times \frac{1}{1-\frac{1}{9}} \times \cdots \times \frac{1}{1-\frac{1}{p^2}} \times \cdots$$

portant sur tout les nombres premiers a un sens,

Une preuve du théorème d'Euclide

Première étape. Euler a montré vers 1735 que le produit

$$\frac{1}{1-\frac{1}{4}} \times \frac{1}{1-\frac{1}{9}} \times \cdots \times \frac{1}{1-\frac{1}{p^2}} \times \cdots$$

portant sur tout les nombres premiers a un sens, et que sa valeur est la même que celle de la somme infinie

$$\frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} + \cdots$$

portant sur tout les carrés d'entiers $n \geq 1$,

Une preuve du théorème d'Euclide

Première étape. Euler a montré vers 1735 que le produit

$$\frac{1}{1-\frac{1}{4}} \times \frac{1}{1-\frac{1}{9}} \times \cdots \times \frac{1}{1-\frac{1}{p^2}} \times \cdots = \frac{\pi^2}{6}$$

portant sur tout les nombres premiers a un sens, et que sa valeur est la même que celle de la somme infinie

$$\frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} + \cdots = \frac{\pi^2}{6}$$

portant sur tout les carrés d'entiers $n \geq 1$, laquelle vaut $\pi^2/6$.

(suite)

Deuxième étape. LEGENDRE a montré en 1794 que le nombre

$$\frac{\pi^2}{6}$$

est irrationnel : il ne peut pas être écrit sous la forme p/q où p et $q \neq 0$ sont des entiers.

(suite)

Deuxième étape. LEGENDRE a montré en 1794 que le nombre

$$\frac{\pi^2}{6}$$

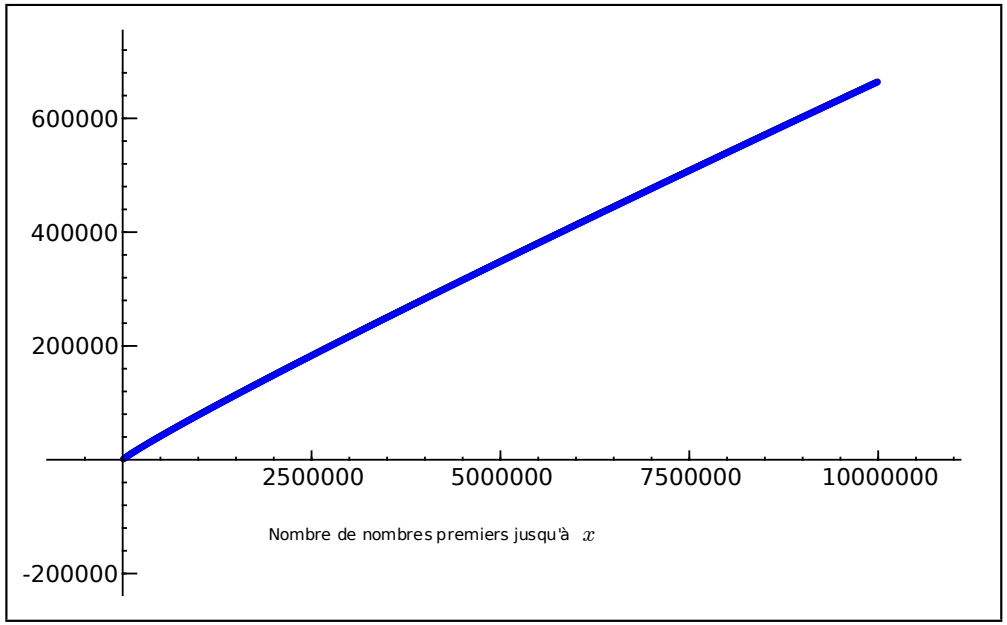
est irrationnel : il ne peut pas être écrit sous la forme p/q où p et $q \neq 0$ sont des entiers.

Fin. Mais si l'ensemble des nombres premiers était fini, avec p_m le plus grand d'entre eux, le produit d'Euler

$$\frac{1}{1-\frac{1}{4}}\frac{1}{1-\frac{1}{9}}\cdots\frac{1}{1-\frac{1}{p_m^2}} = \frac{4}{3}\cdot\frac{9}{8}\cdots\frac{p_m^2}{p_m^2-1}$$

serait certainement rationnel ! *Contradiction*.

Quelques résultats, anciens...



Le nombre $\pi(x)$ de nombres premiers plus petits que x a un comportement régulier quand x grandit.

Le Théorème des nombres premiers, conjecturé par Gauss et prouvé par Hadamard et de la Vallée Poussin en 1896, dit que

$$\pi(x) \sim \frac{x}{\log x}.$$

... et moderne

B. Green et T. Tao ont démontré en 2004 que, pour tout $k \geq 1$, arbitrairement grand, on peut trouver une infinité de nombres premiers p et d'entiers $h \geq 1$, tels que

$$p, \quad p+h, \quad p+2h, \quad \ldots, \quad p+(k-1)h$$

sont *tous* premiers ("il y a des progressions arithmétiques arbitrairement longues de nombres premiers").

... et moderne

B. Green et T. Tao ont démontré en 2004 que, pour tout $k \geq 1$, arbitrairement grand, on peut trouver une infinité de nombres premiers p et d'entiers $h \geq 1$, tels que

$$p, \quad p+h, \quad p+2h, \quad \ldots, \quad p+(k-1)h$$

sont *tous* premiers ("il y a des progressions arithmétiques arbitrairement longues de nombres premiers").

Par exemple, pour $k = 6$,

$$121,174,811 + 30 \cdot i \text{ est premier si } 0 \leq i \leq 5$$

(mais le terme suivant est divisible par 7^2).

Beaucoup de questions, peu de réponses

La répartition des nombres premiers parmi les entiers semble aléatoire, et reste très mystérieuse même aujourd'hui. Par l'observation et des raisonnements heuristiques, on peut facilement deviner certaines propriétés frappantes... et parfois les démontrer.

Beaucoup de questions, peu de réponses

La répartition des nombres premiers parmi les entiers semble aléatoire, et reste très mystérieuse même aujourd'hui. Par l'observation et des raisonnements heuristiques, on peut facilement deviner certaines propriétés frappantes... et parfois les démontrer.

P. de Fermat : Un nombre premier p est de la forme $n^2 + m^2$, avec n et m entiers, si et seulement si on peut l'écrire $p = 4q + 1$, avec q entier. Par exemple,

$$196561 = 156^2 + 415^2 = 4 \cdot 49140 + 1.$$

Il faut parfois faire attention...

P. de Fermat : Si n est un entier ≥ 1, alors $2^{2^n}+1$ est premier ! En effet, 3, 17, 257, 65537 sont premiers...

Il faut parfois faire attention...

P. de Fermat : Si n est un entier ≥ 1, alors $2^{2^n}+1$ est premier ! En effet, 3, 17, 257, 65537 sont premiers...

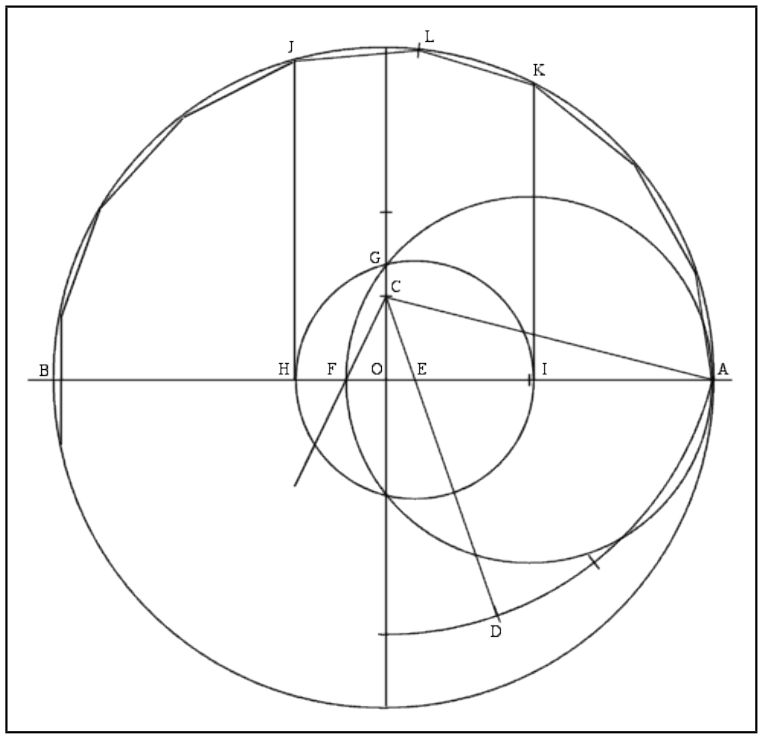
Euler : Pas si vite ! Le nombre $2^{2^5}+1 = 4,294,967,297$ n'est pas premier ; en effet,

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$$

divise $5^4 \cdot 2^{28} + 2^{32}$ et $5^4 \cdot 2^{28} - 1$, donc aussi la différence $2^{32}+1$...

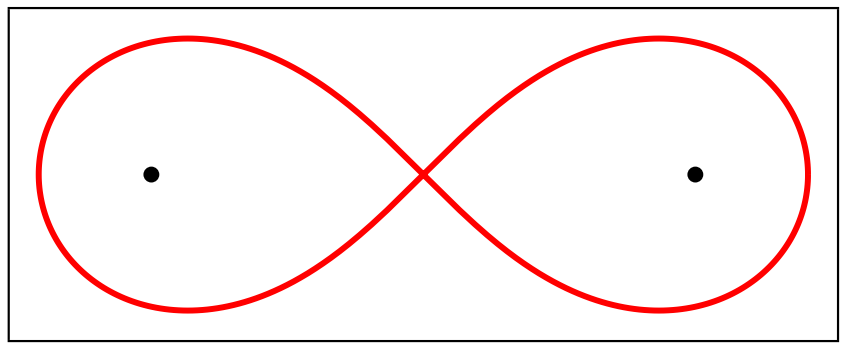
Les bonnes idées ne sont jamais perdues...

C.F. Gauss : Si m est un entier ≥ 1, alors on peut découper un gâteau circulaire en m parts égales à la règle et au compas *si et seulement si* m est un produit de nombres de Fermat premiers distincts, et d'une puissance de 2.



Les bonnes idées ne sont jamais perdues...

C.F. Gauss : Si m est un entier ≥ 1, alors on peut découper un gâteau circulaire en m parts égales à la règle et au compas *si et seulement si* m est un produit de nombres de Fermat premiers distincts, et d'une puissance de 2.



Et la même propriété est vraie pour un gâteau en forme de lemniscate de Bernoulli : $(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$

Petits...

C. Goldbach (1742) : Tout entier pair $n \geq 4$ est-il la somme de deux nombres premiers ? Par exemple,

$$10^7 + 2 = 200033 + 9799969.$$

Petits...

C. Goldbach (1742) : Tout entier pair $n \geq 4$ est-il la somme de deux nombres premiers ? Par exemple,

$$10^7 + 2 = 200033 + 9799969.$$

A. de Polignac (1848) : Existe-t-il une infinité de *nombres premiers jumeaux*, c'est-à-dire de p premiers tels que $p + 2$ soit également premier ? Par exemple,

$$p = 10000139, \quad p + 2 = 10000141.$$

Petits...

C. Goldbach (1742) : Tout entier pair $n \geq 4$ est-il la somme de deux nombres premiers ? Par exemple,

$$10^7 + 2 = 200033 + 9799969.$$

A. de Polignac (1848) : Existe-t-il une infinité de *nombres premiers jumeaux*, c'est-à-dire de p premiers tels que $p + 2$ soit également premier ? Par exemple,

$$p = 10000139, \quad p + 2 = 10000141.$$

On ne sait pas !

... et grands mystères

Le plus grand mystère : est-il vrai qu'il existe un nombre C tel que

$$|\sum_{p \leq x} \log p - x| \leq C\sqrt{x}(\log x)^2 \quad ?$$

Cet énoncé est l'Hypothèse de RIEMANN, le plus célèbre problème ouvert en mathématiques à l'heure actuelle.

... et grands mystères

Le plus grand mystère : est-il vrai qu'il existe un nombre C tel que

$$|\sum_{p \leq x} \log p - x| \leq C\sqrt{x}(\log x)^2 \quad ?$$

Cet énoncé est l'Hypothèse de RIEMANN, le plus célèbre problème ouvert en mathématiques à l'heure actuelle.

Une conséquence : si cette hypothèse est vraie, alors il y a toujours un nombre premier entre x et $x + \sqrt{x}(\log x)^2$, si x est assez grand du moins.

Pourquoi les nombres premiers sont-ils intéressants ?

Réponse moderne. Il est relativement facile de construire des nombres premiers assez grands, ou de vérifier qu'un entier est premier.

Pourquoi les nombres premiers sont-ils intéressants ?

Réponse moderne. Il est relativement facile de construire des nombres premiers assez grands, ou de vérifier qu'un entier est premier.

```
? p1=16347336458092538484431338838650908598417836700330923121811108 5
23893331001045081512121181675115 79;
? isprime(p1)
time = 137 ms.
%1= 1
? p2=19008712816648221131268515739354139754718967899685154936666385
39088027103802104498957191261465571;
time = 0 ms.
? isprime(p2)
time = 136 ms.
%2 = 1
```

Suite

Mais il est très difficile de représenter un entier de taille comparable (qui n'est pas premier !) comme produit de facteurs premiers.

Suite

Mais il est très difficile de représenter un entier de taille comparable (qui n'est pas premier !) comme produit de facteurs premiers.

```
? factor(p1*p2)
^C  *** factor: user interrupt after 1hr, 53mn, 39,129 ms.
```

Suite

Mais il est très difficile de représenter un entier de taille comparable (qui n'est pas premier !) comme produit de facteurs premiers.

```
? factor(p1*p2)
^C  *** factor: user interrupt after 1hr, 53mn, 39,129 ms.
```

Défi RSA : Le calcul des facteurs p_1 et p_2 de $p_1 \cdot p_2$ (sans connaître p_1 et p_2 !) a demandé l'équivalent de trente années de calcul sur un ordinateur personnel en 2005.

Suite

Mais il est très difficile de représenter un entier de taille comparable (qui n'est pas premier !) comme produit de facteurs premiers.

```
? factor(p1*p2)
^C  *** factor: user interrupt after 1hr, 53mn, 39,129 ms.
```

Défi RSA : Le calcul des facteurs p_1 et p_2 de $p_1 \cdot p_2$ (sans connaître p_1 et p_2 !) a demandé l'équivalent de trente années de calcul sur un ordinateur personnel en 2005.

Cette difficulté est la base de la plupart des protocoles de sécurité utilisés de nos jours en informatique (internet, etc).

Transmettre la confiance

Supposons que l'Agence **A** doit envoyer l'Espion **B** dans un pays hostile pour rencontrer le Contact **C**. Comment s'assurer que that **B** est **B** et **C** est **C** ?

Transmettre la confiance

Supposons que l'Agence **A** doit envoyer l'Espion **B** dans un pays hostile pour rencontrer le Contact **C**. Comment s'assurer que that **B** est **B** et **C** est **C** ?

Une possibilité est de donner $p_1 p_2$ à **B** (sans dévoiler p_1 ou p_2) et de communiquer p_1 seulement à **C**.

Transmettre la confiance

Supposons que l'Agence **A** doit envoyer l'Espion **B** dans un pays hostile pour rencontrer le Contact **C**. Comment s'assurer que that **B** est **B** et **C** est **C** ?

Une possibilité est de donner $p_1 p_2$ à **B** (sans dévoiler p_1 ou p_2) et de communiquer p_1 seulement à **C**.

Quand ils se rencontrent, **B** donne $n = p_1 p_2$ à **C**, qui peut s'identifier en retournant immediatement p_1 (que **C** connait déjà) et $p_2 = n/p_1$.

Transmettre la confiance

Supposons que l'Agence **A** doit envoyer l'Espion **B** dans un pays hostile pour rencontrer le Contact **C**. Comment s'assurer que that **B** est **B** et **C** est **C** ?

Une possibilité est de donner $p_1 p_2$ à **B** (sans dévoiler p_1 ou p_2) et de communiquer p_1 seulement à **C**.

Quand ils se rencontrent, **B** donne $n = p_1 p_2$ à **C**, qui peut s'identifier en retournant immediatement p_1 (que **C** connait déjà) et $p_2 = n/p_1$.

Si **C** était un imposteur, il ne pourrait pas factoriser n facilement en l'absence de p_1 et ne pourrait pas convaincre **B**.

Plus d'information...

Il y a énormément de ressources disponibles sur internet pour en apprendre plus. On peut aussi utiliser des logiciels de calcul libres pour explorer à sa guise l'univers des nombres premiers et des mathématiques.

– Le logiciel **Pari/GP** : `pari.math.u-bordeaux.fr`
– Le logiciel **Sage** : `www.sagemath.org`
– Le blog de Terry Tao : `terrytao.wordpress.com`
– Si vous voulez retrouver cet exposé :
`www.math.ethz.ch/~kowalski/expose-smo.pdf`