Les nombres premiers: mystères et consolation

Jean-Marie De Koninck
Université Laval

Avril 2004

§1. Introduction

Que peut bien avoir d'intéressant le nombre

$$2^{20996011} - 1 \qquad ?$$

Eh bien! c'est le plus grand nombre premier connu: il est fait de 6 320 430 chiffres et il a été découvert le 17 novembre 2003. Il aura fallu 25 000 années de temps calcul partagé sur les ordinateurs de 211 000 volontaires répartis sur la planète. Il faut croire que la recherche de nombres premiers a quelque chose de très fascinant, n'est-ce pas ?

Histoire de s'assurer que nous parlons bien de la même chose: un *nombre premier* est un nombre plus grand que 1 qui n'est divisible que par 1 et par lui-même. Ainsi 7 est un nombre premier parce que ses seuls diviseurs sont 1 et 7, tandis que 6 n'est pas premier parce qu'à part 1 et 6, il a aussi comme diviseur le nombre 2. On peut s'amuser à construire la liste des nombres premiers inférieurs à 100:

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

Cette notion de *nombre premier* existe depuis des milliers d'années et depuis ce temps, elle n'a cessé de fasciner tous ceux et celles qui l'ont étudiée. C'est que la répartition des nombres premiers renferme de nombreux mystères.

Par exemple, on sait depuis Euclide (300 ans avant Jésus-Christ) qu'il existe une infinité de nombres premiers (voir la preuve dans l'encadré). Mais lorsqu'on examine de plus près la suite des nombres premiers, on peut se demander s'il existe une infinité de nombres premiers p tels que $p+2$ est aussi premier. Autrement dit, la suite de couples

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73),\ (101,103),\ldots$$

est-elle infinie ?

Tous les mathématiciens sont convaincus que la réponse à cette question est "OUI", mais une démonstration rigoureuse de cette affirmation leur échappe... pour le moment. On appelle ce résultat la *conjecture des nombres premiers jumeaux*. Cette incapacité à démontrer cette conjecture est d'autant plus frustrante que, aussi loin qu'on aille dans la suite des nombres premiers, on trouve toujours des nombres premiers jumeaux. Ainsi, en 2002, Papp et Gallot ont trouvé les nombres premiers jumeaux

$$33218925 \times 2^{169690} - 1 \text{ et } 33218925 \times 2^{169690} + 1,$$

chacun de ces nombres premiers étant fait de 51090 chiffres.

L'infinitude des nombres premiers

On suppose qu'il existe seulement un nombre fini de nombres premiers, disons $p_1 < p_2 < \ldots < p_k$; on considère alors le nouveau nombre $n = p_1 p_2 \ldots p_k + 1$; ou bien n est premier, ou bien il est composé; s'il est premier, on a une contradiction puisque $n > p_k$; par contre si n est composé, il existe un nombre premier p qui divise n, et comme p doit être un des p_i $(1 \le i \le k)$, disons $p = p_{i_0}$, on a $p_{i_0} | p_1 \ldots p_{i_0} \ldots p_k + 1$ et par conséquent $p_{i_0} | 1$, ce qui n'a pas de sens; ainsi dans les deux cas, on obtient une contradiction et l'infinitude des nombres premiers est démontrée.

§2. Le théorème de raréfaction des nombres premiers

Les mathématiciens ont tout de même réussi à relever certains défis entourant la répartition des nombres premiers. Ainsi, tout à fait naturellement, ils se sont demandés s'il y avait une façon rapide de calculer la quantité de nombres premiers contenus dans l'intervalle $[1, x]$ pour un nombre x donné, une quantité qu'on a convenu d'appeler $\pi(x)$. Par exemple, $\pi(10) = 4$, car il y a exactement quatre nombres premiers dans l'intervalle $[1, 10]$. De même, $\pi(100) = 25$ comme en fait foi l'énumération ci-dessus.

Ainsi depuis longtemps, on s'est demandé s'il existe une fonction simple $f(x)$ telle que

$$(*) \qquad \lim_{x\to\infty} \frac{\pi(x)}{f(x)} = 1.$$

Vers la fin du XVIII^e siècle, le mathématicien français Adrien-Marie Legendre (1752-1833) et le mathématicien allemand Carl Friedrich Gauss (1777-1855) ont affirmé (sans toutefois pouvoir le démontrer) que la quantité $\pi(x)$ était approximativement $x/\log x$, suggérant ainsi que $(*)$ était vraie avec $f(x) = x/\log x$. D'ailleurs, les données numériques allaient dans ce sens, comme semble le confirmer le tableau ci-dessous.

x	$\pi(x)$	$[x/\log x]$	$\dfrac{\pi(x)}{x/\log x}$
10	4	4	1.00
10^2	25	21	1.19
10^3	168	144	1.16
10^4	1229	1085	1.13
10^5	9592	8685	1.10
10^6	78498	72382	1.08
10^7	664579	620420	1.07

(Ici, on a écrit $[y]$ pour signifier le plus grand entier inférieur ou égal à y.)

Mais Legendre et Gauss n'ont pas réussi à démontrer que $\lim_{x\to\infty} \dfrac{\pi(x)}{x/\log x} = 1$, un résultat appelé aujourd'hui le *théorème de raréfaction des nombres premiers* ou tout simplement le *théorème des nombres premiers*. Vers le milieu du XIX^e siècle, le Russe Pafnouti Tchebychev (1821-1894) (dont le nom est bien connu en théorie des probabilités) vient tout près de démontrer ce fameux théorème, puisqu'il arrive à démontrer qu'il existe des constantes $a < 1 < b$ telles que, si x est assez grand, le quotient $\dfrac{\pi(x)}{x/\log x}$ est compris entre a et b.

Ce n'est qu'en 1896 que le mathématicien français Jacques Hadamard (1865-1963) et le mathématicien belge Charles-Jean de la Vallée Poussin (1866-1962) ont réussi à démontrer (indépendamment, à quelques mois d'intervalle) le théorème des nombres premiers. Pour ce faire, ils ont étudié le comportement analytique de la fonction zêta de Riemann

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \dots,$$

une fonction d'abord étudiée vers 1750 par le Suisse Leonhard Euler (1707-1783) pour des valeurs réelles de s et ensuite vers 1850 par l'Allemand Bernhard Riemann (1826-1866) pour des valeurs complexes de s. En réalité, Hadamard et de la Vallée Poussin ont réussi à compléter le travail d'analyse complexe amorcé 40 ans auparavant par Riemann.

Légende ou réalité ?

Au XIX^e siècle, la légende voulait que quiconque réussirait à démontrer le théorème des nombres premiers vivrait au moins 100 ans. Il faut croire que cette fabulation avait un brin de fondement, puisque les deux mathématiciens qui en ont réalisé la preuve ont vécu très vieux, du moins pour leur époque, soit Hadamard jusqu'à 98 ans et de la Vallée Poussin jusqu'à 96 ans.

Le lien entre la fonction $\zeta(s)$ et $\pi(x)$ vient du fait que, pour chaque nombre réel $s > 1$, on a

$$(1) \qquad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \frac{1}{p^{4s}} + \frac{1}{p^{5s}} + \dots\right) = \prod_p \left(1 - \frac{1}{p}\right)^{-1},$$

où le produit infini parcourt tous les nombres premiers p dans l'ordre croissant.

Le lien entre $\pi(x)$ et $\zeta(s)$

Il existe un lien direct entre $\pi(x)$ et $\zeta(s)$, soit celui donné par la formule

$$\log \zeta(s) = s \int_2^\infty \frac{\pi(x)}{x(x^s-1)}\, dx. \tag{2}$$

Voici une esquisse de la preuve. En utilisant l'intégrale de Stieltjes, on peut démontrer ce lien de la façon suivante. On a d'après la relation (**??**),

$$\begin{aligned}
\log \zeta(s) &= -\log \prod_p \left(1-\frac{1}{p^s}\right) = -\sum_p \log\left(1-\frac{1}{p^s}\right) \\
&= -\int_{2^-}^\infty \log\left(1-\frac{1}{x^s}\right)\, d\pi(x) \\
&= \log\left(1-\frac{1}{x^s}\right)^{-1} \pi(x)\Big|_2^\infty + s\int_2^\infty \frac{\pi(x)}{x(x^s-1)}dx,
\end{aligned}$$

ce qui prouve (**??**), car d'une part $\pi(2^-)=0$, alors que d'autre part $\log\left(1-\frac{1}{x^s}\right)^{-1} < \frac{2}{x^s}$ de sorte que $\pi(x)/x^s$ tend vers 0 lorsque $x \to \infty$.

L'idée de Riemann

Riemann est le premier à avoir eu l'idée d'utiliser les fonctions d'une variable complexe pour démontrer le théorème des nombres premiers. Le produit infini (de même que la série) qui représente la fonction zêta (voir (**??**)) ne converge que si $s > 1$, la raison étant que la série $\sum_{n=1}^\infty \frac{1}{n}$ diverge. Pour contourner cet obstacle, Riemann eut l'idée d'étendre le domaine de définition de la fonction zêta. Dans un premier temps, on peut facilement démontrer que $\zeta(s)$ peut s'écrire sous la forme

$$\zeta(s) = \frac{1}{1-2^{1-s}} \sum_{n=1}^\infty \frac{(-1)^{n+1}}{n^s},$$

où cette fois la série converge pour tout $s > 0$. Armée de cette nouvelle représentation, la fonction $\zeta(s)$ a maintenant un sens pour tout nombre réel $s > 0$, sauf au point $s = 1$ où elle a un pôle (une sorte d'explosion). Avec un peu d'effort, on peut continuer ce processus et prolonger la fonction $\zeta(s)$ à tout le plan complexe.

§3. Des formules simples pour livrer des nombres premiers ?

La formule $f(n) = 17n$ nous donne le n-ième multiple de 17. Existe-t-il une formule tout aussi "simple" et efficace qui donnerait le n-ième nombre premier ? On en cherche une depuis des siècles ! Tout ce qu'on a trouvé jusqu'ici, ce sont des formules en apparence efficaces, mais en réalité sans grand intérêt.

Donnons un premier exemple. Soit donc p_n le n-ième nombre premier et considérons la formule

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left[\frac{n}{1+\pi(m)}\right]^{1/n}\right],$$

où $\pi(m)$ désigne le nombre de nombres premiers $\le m$. Par exemple, on peut la vérifier dans le cas de $n = 2$:

$$p_2 = 1 + \left[\left[\frac{2}{1+\pi(1)}\right]^{1/2}\right] + \left[\left[\frac{2}{1+\pi(2)}\right]^{1/2}\right] + 0+0+0+0+0+0 = 1+1+1 = 3.$$

Mais, voilà qui n'est pas très commode, d'autant plus que cela présuppose qu'on connaît à l'avance les valeurs $\pi(1)$, $\pi(2)$, …, $\pi(2^n)$.

Et si on était moins exigeant ! Plutôt que de chercher une formule qui donne tous les nombres premiers, peut-on en exhiber une qui ne donnerait que des nombres premiers ? Une première tentative a été faite par Euler en 1772. Il a considéré l'expression $n^2 - n + 41$ pour $n = 1, 2, 3, \ldots$ Pour $0 \le n \le 40$, on obtient les nombres

$$41, 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461,$$

$$503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601,$$

lesquels sont tous premiers. Malheureusement, pour $n = 41$, on obtient $n^2 - n + 41 = 41^2 - 41 + 41 = 41^2$ qui n'est pas premier. Un échec ! Mais si on avait choisi un autre polynôme ? Aucune chance ! En effet, peu importe le polynôme $P(x)$ à coefficients entiers, on peut démontrer que nécessairement, il existe un entier positif n tel que $P(n)$ est composé, à moins bien sûr de considérer un polynôme constant, comme $P(n) = 19$ qui ne donne trivialement rien d'autre que des nombres premiers ! Mais, avouns-le, ce n'est pas un résultat intéressant !

En 1947, W.H. Mills en surprenait plus d'un en démontrant qu'il existe une constante positive θ telle que l'expression $\left[\theta^{3^n}\right]$ représente un nombre premier pour tout entier $n \geq 1$.

En prenant $\theta = 1,306377883863080690468614492 6$, on obtient $[\theta^{3^1}] = 2$, $[\theta^{3^2}] = 11$, $[\theta^{3^3}] = 1361$, $[\theta^{3^4}] = 2521008887$, et tout semble bien aller... jusqu'à ce qu'on calcule $[\theta^{3^5}] = 16022362040098181318313201 75$, un multiple de 5. C'est qu'il aurait fallu préciser davantage la *constante de Mills* θ. Mais comment y arrive-t-on ? En fait, lorsqu'on examine la façon dont la constante θ est construite, on s'aperçoit que l'on doit connaître à l'avance la suite p_n, de sorte qu'on n'est pas plus avancé ... En réalité, il s'agit d'un résultat d'un intérêt théorique, mais pas du tout pratique pour trouver de nouveaux nombres premiers.

Donnons un 2^e exemple où le subterfuge est encore plus évident, et qui plus est, cette fois, on obtient même chaque nombre premier p_n. Considérons d'abord la constante

$$s = \frac{2}{10} + \frac{3}{10^4} + \frac{5}{10^9} + \frac{7}{10^{16}} + \frac{11}{10^{25}} + \ldots = 0,200300005000000700000001 10\ldots$$

On peut assez facilement démontrer que

$$p_n = \left[10^{n^2} s\right] - 10^{2n-1}\left[10^{(n-1)^2} s\right]. \tag{3}$$

(Ici, encore une fois, $[y]$ désigne le plus grand entier $\leq y$; par exemple, $[4.1] = 4$, $[11.9] = 11$ et $[\pi] = 3$.) Bravo ! Mais comme p_n apparaît déjà dans la formule qui donne la valeur exacte de la constante s, la formule (**??**) n'est pas d'un intérêt pratique, car en réalité elle présuppose que l'on connaît déjà p_n. Bel effort...

Et si on considérait des polynômes à deux variables, ou trois, ou... En fait, il découle des travaux de Yuri Matijasevitch dans sa résolution en 1970 du 10^e problème de Hilbert qu'il existe un polynôme à coefficients entiers à 26 variables tel que, si on limite les valeurs des variables aux nombres entiers, alors l'ensemble des valeurs strictement positives du polynôme est égal à l'ensemble des nombres premiers. En 1976, les mathématiciens Jones, Sato, Wada et Wiens ont réussi à construire un tel polynôme et le voici:

$$\begin{aligned}
&(k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
&- [2n + p + q + z - e]^2 - [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\
&- [e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 \\
&- [16r^2y^4(a^2-1) + 1 - u^2]^2 - [((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 \\
&+ 1 - (x + cu)^2]^2 - [n + \ell + v - y]^2 - [(a^2-1)\ell^2 + 1 - m^2]^2 - [ai + k + 1 - \ell - i]^2 \\
&- [p + \ell(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
&- [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - [z + p\ell(a - p) + t(2ap - p^2 - 1) - pm]^2\}.
\end{aligned}$$

Peu commode, vous direz ! Mais alors, y a-t-il moyen d'obtenir un polynôme avec les mêmes propriétés mais avec moins de variables ? Oui, mais à un coût quant au degré du polynôme. En effet, il est possible d'obtenir un polynôme à 12 variables (plutôt que 26), mais alors son degré est 13697. Dommage !

Des encadrements précis pour $\pi(x)$ et pour p_n

En 1962, Rosser et Schoenfeld ont démontré que, pour $x \geq 67$, on a

$$\frac{x}{\log x - \frac{1}{2}} < \pi(x) < \frac{x}{\log x - \frac{3}{2}}.$$

En 2000, Panaitopol a obtenu encore mieux, soit que pour $x \geq 59$,

$$\frac{x}{\log x - 1 + \frac{1}{\sqrt{\log x}}} < \pi(x) < \frac{x}{\log x - 1 - \frac{1}{\sqrt{\log x}}}.$$

On peut démontrer que le théorème des nombres premiers est équivalent à $\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$. Mais à quel point la quantité p_n est-elle proche de son approximation $n \log n$? À ce sujet, en 1983, Guy Robin a démontré que pour tout entier $n \geq 7022$, on a

$$n(\log n + \log\log n - 1) < p_n < n(\log n + \log\log n - 0,9385).$$

Cet encadrement annonce par exemple que si $n = 10^8$, on aura $2033415473 < p_n < 2039565473$, ce qui est tout de même assez juste, puisque $p_{10^8} = 2038074743$.

§4. Les tests de primalité

Depuis qu'on étudie les nombres premiers, on cherche des méthodes efficaces pour les reconnaître, i.e. des méthodes permettant d'établir si un nombre donné est premier ou pas. On les appelle des "tests de primalité".

Le test de primalité le plus naturel est sûrement celui de la division par les petits nombres premiers. Par exemple, pour savoir si 143 est premier, on examine sa divisibilité par 2, 3, 5, et ainsi de suite. Ici, 143 est "dénoncé" par 11, puisqu'il est divisible par 11. Ce test est relativement efficace pour des "petits nombres", parce que si un nombre n'est pas premier, il sera toujours "dénoncé" par un de ses diviseurs premiers qui est $\leq \sqrt{n}$. Ainsi, étant donné un nombre $n < 10^{12}$, en utilisant un logiciel de calcul, on peut tester rapidement (soit en quelques secondes) sa divisibilité par tous les nombres premiers $< 10^6$; si aucun diviseur $< 10^6$ n'est trouvé, alors le nombre n est déclaré "premier". Pour des nombres plus grands, disons de l'ordre de 10^{20}, cette méthode n'est plus efficace... à moins que l'on soit très patient !

Un test de primalité bien connu et facile à formuler est le *théorème de Wilson*, selon lequel si n est un entier positif,

$$n \text{ est un nombre premier } \iff (n-1)! \equiv -1 \pmod{n}.$$

(Ici $a \equiv b \pmod{m}$ veut dire "$a - b$ est un multiple de m".) Toutefois, puisque le calcul de $(n-1)!$ est laborieux (même en réduisant modulo n à chaque étape), il s'avère que ce test de primalité n'est pas du tout pratique.

Rappelons maintenant le *petit théorème de Fermat*, un résultat qui date de plus de trois siècles.

Petit théorème de Fermat. *Soit p un nombre premier et soit a un entier relativement premier avec p. Alors*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Si la réciproque du petit théorème de Fermat était vraie, alors on aurait un critère de primalité très efficace. Mais malheureusement, la réciproque est fausse. En effet, si on prend $a = 2$ et $n = 341 = 11 \cdot 31$, on a

$$2^{340} \equiv 1 \pmod{341},$$

et pourtant 341 est un nombre composé. Par contre, le petit théorème de Fermat fournit un critère de "non primalité" fort commode, et on l'énonce ainsi:

Soit $n > 1$ et soit $(a, n) = 1$. Si $a^{n-1} \not\equiv 1 \pmod{n}$, alors n est composé.

Par exemple, soit $n = 2796238380562974519433$. Comme

$$2^{n-1} \equiv 2706340698865264344859 \not\equiv 1 \pmod{n},$$

on conclut que n est composé.

REMARQUE. Signalons que le calcul de $2^{n-1} \pmod{n}$ (i.e. du reste de la division de 2^{n-1} par n) est très rapide: en fait, il est possible de démontrer que le nombre d'opérations que nécessite l'évaluation de $2^{n-1} \pmod{n}$ est de l'ordre de $\log^3 n$.

En pratique, si un nombre est composé, il est fort probable que cela sera confirmé par la réciproque du test de Fermat. Par contre, s'il n'est pas dénoncé par ce test, on ne peut pas conclure qu'il est premier. Dans un tel cas, pourquoi ne pas tester à nouveau le nombre n en utilisant le nombre 3 plutôt que 2 ? Ainsi, si on avait $3^{n-1} \not\equiv 1 \pmod{n}$, on pourrait alors conclure que n n'est pas premier. L'idée est excellente. Toutefois, il existe des nombres composés n très sournois qui "passent tous ces tests", i.e. des nombres composés n pour lesquels $a^n \equiv 1 \pmod{n}$ pour tout entier a n'ayant aucun facteur en commun avec n. Ces nombres exceptionnels, on les appelle des *nombres de Carmichael*, et malheureusement on sait depuis 1992 (grâce à W. Alford, A. Granville et C. Pomerance) qu'ils sont en nombre infini. D'où le besoin de développer des tests de primalité davantage fiables.

L'un des premiers tests de primalité s'appliquant à tous les nombres, et par surcroît très efficace, est celui introduit par Edouard Lucas en 1891. Dans les décennies qui ont suivi, une foule de tests tant soit peu meilleurs que celui de Lucas ont pris forme. Ici, nous nous contentons d'expliquer le test de Lucas.

Le test de primalité de Lucas

L'énoncé

Soit a et n deux entiers positifs tels que

$$a^{n-1} \equiv 1 \pmod{n}$$

et supposons que

$$a^{(n-1)/p} \not\equiv 1 \pmod{n}$$

pour chaque facteur premier p de $n-1$. Alors n est premier.

Un exemple

Soit $n = 947$ et $a = 2$. On a $946 = 2 \cdot 11 \cdot 43$ et $2^{946} \equiv 1 \pmod{n}$. Or

$$\begin{aligned} 2^{946/2} &= 2^{473} \equiv 946 \pmod{947}, \\ 2^{946/11} &= 2^{86} \equiv 215 \pmod{947}, \\ 2^{946/43} &= 2^{22} \equiv 41 \pmod{947}, \end{aligned}$$

et c'est pourquoi on peut conclure que 947 est premier.

REMARQUE. Ce test comporte deux inconvénients. Le premier (pas trop grave) est qu'il faut trouver un a pour lequel le test sera positif (si n est premier, bien sûr). Le deuxième est qu'il faut tout de même être capable de factoriser $n-1$, ce qui n'est pas toujours facile. Dans le cas où n est un nombre de Fermat, cela est évidemment très facile: c'est l'objet du test de Pépin.

Effectivement, certains tests de primalité ne s'appliquent qu'à une certaine catégorie de nombres. C'est le cas du test de Lucas-Lehmer qui ne s'applique qu'aux nombres de Mersenne, soit les nombres de la forme $2^p - 1$, où p est premier. C'est aussi le cas du test de Pépin qui ne s'applique qu'aux nombres de Fermat.

Le test de primalité de Lucas-Lehmer

L'algorithme le plus utilisé pour établir la primalité d'un nombre de Mersenne, i.e. d'un nombre de la forme $2^p - 1$ où p est premier, est celui dû à Lucas et, comme il a été amélioré par la suite par Lehmer, il est aujourd'hui appelé le *test de Lucas-Lehmer*.

L'énoncé

Soit $M_p = 2^p - 1$, où p est un nombre premier impair. Soit $s_1 = 4$ et, pour $k \geq 2$, soit $s_k \equiv s_{k-1}^2 - 2 \pmod{M_p}$. Alors

$$M_p \text{ est premier } \iff M_p | s_{p-1}.$$

La programmation avec Mathematica

```
p=...;s=4;j=1;mp=2^p-1;
While[j<p-1,{r=Mod[s^2-2,mp];s=r;j++}];
If[Mod[r,mp]==0,Print["2^",p,"−1 est
premier"],
Print["2^",p,"−1 est compose"]]
```

Le test de Pépin

Énoncé et exemples

Soit k un entier positif et $F_k = 2^{2^k} + 1$. Alors

$$3^{\frac{F_k - 1}{2}} \equiv -1 \pmod{F_k} \iff F_k \text{ est premier.}$$

Ainsi $F_2 = 17$ est premier, parce que $3^{2^{2^2-1}} = 3^8 \equiv -1 \pmod{17}$. Par contre, $F_5 = 4294967297$ est composé, car

$$3^{2^{2^5-1}} = 3^{2^{31}} \equiv -4284642994 \not\equiv -1 \pmod{F_5}.$$

Voulez-vous gagner 500$?

Le plus petit nombre de Fermat dont on ne connaît aucun facteur premier est F_{14}, et cela même si Selfridge et Hurwitz, en 1963, ont réussi à établir, en utilisant le test de Pépin, qu'il est composé. *Perfectly Scientific Inc.* offre un prix de 500$US à quiconque trouvera un facteur premier de F_{14}. Sans vouloir décourager qui que ce soit, mentionnons que F_{14} est fait de 4933 chiffres !

Comment mesure-t-on la rapidité d'un algorithme ?

Que veut-on dire quand on dit qu'un algorithme qui teste la primalité d'un nombre n (ou encore livre sa factorisation) peut s'effectuer dans un temps polynomial ou exponentiel ou encore sous-exponentiel ?

On dit qu'un algorithme est polynomial si sa complexité (i.e. le nombre d'opérations que nécessite son exécution) n'excède pas r^c pour une certaine constante $c > 0$, où r est la longueur du nombre n en base 2 (i.e. $r \approx \log_2 n$). Par exemple, la multiplication d'un nombre n de r chiffres (en base 2) avec un nombre m de s chiffres requiert essentiellement rs opérations, i.e. environ $\log_2 n \log_2 m$. Il en est de même pour la division. Par contre, l'addition ou la soustraction de ces deux nombres en nécessite environ $O(\max(r, s))$. Les opérations élémentaires sont donc polynomiales (en temps d'exécution).

Si un algorithme est de complexité $c^{f(n)}$, où $c > 0$ et $f(n)$ est un polynôme en $\log n$, alors on dit que cet algorithme est de temps exponentiel. Par exemple, le test de primalité d'un nombre n par une vérification avec tous les nombres premiers $p \leq \sqrt{n}$ utilise environ $\sqrt{n}$ étapes. Or $\sqrt{n} = 2^{\log_2 n} = 2^{(\log_2 n)/2}$. Voilà pourquoi on dit que ce test est exponentiel.

Si un algorithme est de complexité $\exp\{c(\log_2 n)^a (\log_2 \log_2 n)^{1-a}\}$, où $0 < a < 1$ et c est une constante, on dit que cet algorithme est sous-exponentiel. En général, un bon algorithme de factorisation est sous-exponentiel. On ne connaît pas d'algorithme de factorisation polynomial.

Un test probabiliste: le test de primalité de Miller-Rabin

Pour des raisons pratiques, on pourrait parfois se contenter d'un test qui nous garantit qu'un nombre impair donné est premier avec une certitude de presque 100%, surtout si ce test prend moins d'une seconde à exécuter. C'est la nature du test de Miller-Rabin. Essentiellement, l'idée est que pour réaliser le test sur un nombre impair $n > 3$, on choisit au hasard un entier $a \in [2, n-2]$; si a est un "témoin" pour n (voir ci-contre), alors n est déclaré composé; sinon, il y a environ trois chances sur 4 que n soit premier.

Ainsi, supposons que, pour un nombre impair $n > 3$, l'on ne trouve aucun témoin pour n après avoir effectué k fois le test de Miller-Rabin (pour différents choix de a); alors la probabilité que n soit premier est d'environ $1 - \dfrac{1}{4^k}$.

Par exemple, étant donné un entier positif impair, supposons qu'on effectue 200 fois le test de Miller-Rabin, et supposons que le test "annonce" que n est premier, alors la probabilité qu'on fasse erreur est de l'ordre de

$$\frac{1}{4^{200}} \approx \frac{1}{10^{120}},$$

une quantité très proche de 0, auquel cas on peut effectivement affirmer qu'on est presque 100% certain que n est premier.

Le test de Miller-Rabin

Soit $n > 3$ un entier impair. On peut donc l'écrire sous la forme $n - 1 = 2^s d$ pour un certain entier $s \geq 0$ et un certain nombre impair d. Soit $1 < a < n$ n'ayant aucun facteur en commun avec n (ce qui est facile à vérifier en utilisant l'algorithme d'Euclide). Alors on dit que a est un *témoin* pour n si $a^d \not\equiv 1 \pmod{n}$ et $a^{2^j d} \not\equiv -1 \pmod{n}$ pour chaque nombre j tel que $0 \leq j < s$. S'il s'avère que a est un témoin pour n, alors on peut conclure que n est composé. Autrement dit, un témoin pour n est "quelqu'un" qui dénonce n en confirmant qu'il est composé. Sinon, c'est-à-dire si a n'est pas un témoin, on peut conclure avec une probabilité de $1 - \frac{1}{4} = \frac{3}{4}$ que n est premier. En effectuant le test une 2^e fois avec un autre nombre a qui n'a aucun facteur en commun avec n et en supposant encore une fois que ce nombre a n'est pas un témoin, alors on est maintenant certain avec une probabilité de $1-(\frac{1}{4})^2 = \frac{15}{16}$ que n est premier. Et ainsi de suite.

Le test de Miller-Rabin est si efficace et "fiable" que le logiciel de calcul MATHEMATICA l'utilise pour confirmer la primalité d'un nombre premier avec la commande `PrimeQ[ ]`. Il reste que c'est un test probabiliste et non déterministe: il ne peut pas affirmer avec une certitude de 100% qu'un nombre est premier (même s'il est effectivement premier !). Par surcroît, on est incapable de démontrer qu'il s'agit d'un test qui s'exécute en temps polynomial.

Il faut mentionner qu'une des méthodes parmi les plus efficaces pour tester la primalité d'un nombre en est une qui utilise une généralisation du petit théorème de Fermat aux courbes elliptiques. Une courbe elliptique est le lieu des points (x, y) qui satisfont une équation de la forme $y^2 = x^3 + ax + b$, où a et b sont des nombres rationnels. Les premiers tests de primalité utilisant les courbes elliptiques ont été mis au point par S. Goldwasser et J. Kilian en 1986. On peut constater qu'en pratique, le temps d'exécution d'un tel test est en moyenne de l'ordre de $\log^6 n$, donc polynomial; mais on est incapable de le démontrer.

Jusqu'en l'an 2002, le test qui s'approchait le plus d'un temps d'exécution polynomial était celui établi en 1983 par Adleman, Pomerance et Rumely: leur test est "presque polynomial", car son temps de calcul est de l'ordre de $(\log n)^{\log\log\log n}$.

C'était l'époque où on se demandait si on arriverait enfin un jour à trouver un test de primalité déterministe dont le temps d'exécution est polynomial. Mais à l'été 2002, l'histoire des mathématiques allait prendre un important virage ...

Enfin un test de primalité en temps polynomial !

On cherche depuis longtemps un test pouvant déterminer si un entier positif n est premier ou non en un temps polynomial, i.e. polynomial comme fonction du nombre de chiffres de n. Depuis des décennies, on connaît des tests de primalité probabilistes (i.e. qui déterminent avec une certitude proche de 100% qu'un nombre est premier ou non) s'effectuant en temps polynomial, mais malheureusement de tels tests ne sont pas déterministes. Parmi les tests probabilistes très efficaces, on retrouve celui utilisant les courbes elliptiques, qui permet d'établir (avec certitude!) la primalité d'un nombre de 2 000 chiffres.

Au début du mois d'août 2002, trois chercheurs de l'*Indian Institute of Technology*, soit le professeur Manindra Agrawal et ses deux étudiants Neeraj Kayal et Nitin Saxena, ont annoncé la découverte d'un test de primalité dont le nombre d'étapes est borné approximativement par d^{12}, où d est le nombre de chiffres du nombre testé. En 2004, ils ont réduit ce nombre d'étapes à d^6.

Ce nouveau test des trois Indiens est d'autant plus remarquable qu'il n'utilise que des notions de théorie élémentaire des nombres, soit le petit théorème de Fermat ($a^p \equiv a \pmod p$ pour tout entier positif a et tout nombre premier p) et le fait que $(x+y)^p \equiv x^p + y^p \pmod p$ pour tout nombre premier p.

Leur manuscrit est disponible sur le WEB à l'adresse `www.cse.iitk.ac.in/primality.pdf`.

§5. Les algorithmes de factorisation

5.1. Le test de factorisation de Fermat

Pierre de Fermat (1601-1665) est l'auteur d'un test de factorisation qui porte son nom: étant donné un entier positif impair composé n, ce test consiste à utiliser le fait qu'il existe des entiers positifs a et b tels que $n = a^2 - b^2$, auquel cas $n = (a-b)(a+b)$ fournit une factorisation de n. Il s'agit d'une méthode efficace si l'entier n possède deux diviseurs relativement près l'un de l'autre. Voici cette méthode. D'abord le fait que de tels entiers a et b existent toujours découle du fait que si $n = rs$, avec $1 < r < s$, alors les nombres $a = (r+s)/2$ et $b = (s-r)/2$ font l'affaire. Le test consiste donc à chercher deux entiers positifs $a > b$ tels que $n = a^2 - b^2$. Comme $n = a^2 - b^2 < a^2$ et ainsi $a > \sqrt{n}$, il est certain que $a \geq [\sqrt{n}] + 1$. On commence donc par poser $a = [\sqrt{n}] + 1$; si $a^2 - n$ est un carré parfait, disons $a^2 - n = b^2$, alors on a trouvé a et b comme souhaité; sinon on pose $a = [\sqrt{n}] + 2$, et ainsi de suite, jusqu'à ce que l'on trouve un entier positif k tel que le nombre $a = [\sqrt{n}] + k$ a la propriété que $a^2 - n$ est un carré parfait que l'on écrira b^2. Par ailleurs, ce processus a une fin, en ce sens que l'on va nécessairement trouver un b tel que $b^2 = a^2 - n$, parce que $b = (s-r)/2$.

Programmé avec MATHEMATICA, cette méthode peut être formulée ainsi:

```
n = ...; a = Floor[Sqrt[n]] + 1; While[!IntegerQ[b = Sqrt[a^2 - n]], a++];
Print[a, " ", b, "⟶ n =", a - b, " × ", a + b]
```

L'exemple donné par Fermat est celui de la factorisation de $n = 2027651281$. Il calcule d'abord $[\sqrt{n}] = 45029$. Il commence avec $a = 45029 + 1 = 45030$; comme $45030^2 - 2027651281 = 49619$ n'est pas un carré parfait, il pose ensuite $a = 45031$, ce qui ne donne toujours pas un carré parfait, et ainsi de suite, jusqu'à ce qu'il arrive à $a = 45041$, ce qui donne $b = \sqrt{45041^2 - 2027651281} = \sqrt{1040400} = 1020$. Il suit alors que

$$n = 2027651281 = 45041^2 - 1020^2 = (45041 - 1020)(45041 + 1020) = 46061 \cdot 44021.$$

En 1920, Maurice Kraitchik a développé une amélioration de la méthode des "différences de carrés" de Fermat, et c'est ce développement qui est aujourd'hui à la base de plusieurs algorithmes de factorisation modernes.

5.2. Le temps de factorisation d'un nombre – un court aperçu historique

Quel est le temps nécessaire à la factorisation d'un nombre n ? La réponse dépend de deux choses: l'algorithme utilisé et la puissance de l'ordinateur sur lequel il est implanté.

La méthode	le nombre d'opérations	l'année	l'auteur	le nombre de chiffres
La division par de petits nombres premiers	$\frac{2\sqrt{n}}{\log n}$	l'an 0		20
Test de Fermat (différence de carrés)	rapide pour $n = pq$, avec p et q proches	1650	Pierre de Fermat	20
$x^2 \equiv y^2 \pmod{n}$ (amélioration du test de Fermat)	$e^{\sqrt{2 \log n \log\log n}}$	1920	Kraitchik	30
Méthode des fractions continues	$e^{\sqrt{2 \log n \log\log n}}$	1979	J. Brillhart M. Morisson	50
Crible quadratique	$e^{\sqrt{\log n \log\log n}}$	1990	C. Pomerance	116
Number Field Sieve (pour les nombres n de la forme $n = p^a + b$)	$e^{(\log n)^{1/3}(\log\log n)^{2/3}}$	1996	H. Lenstra	130
Courbes elliptiques (trouve les facteurs de moins de 40 chiffres)	$e^{\sqrt{\log n \log\log n}}$	1985	H. Lenstra	150

Le plus grand nombre factorisé

En 1999, une équipe de recherche d'Amsterdam a réussi à relever le défi RSA-155 en factorisant un nombre de 155 chiffres. Ils ont démontré que le nombre n de 155 chiffres

$$n = 109417386415705274218097073220403576120037329454492059909138421320520088215418$$
$$44440751004247835336877365348729210124008017337821724869685910203793354333897$$

peut se factoriser comme

$$n = p \times q \ ,$$

où

$$p = 10263959282974110577205419657399167590071656780803806680334193352719071130777 9$$
$$q = 10660348838016845482092722036001287867920795857598929152227060823719306280864 3$$

sont deux nombres premiers de 78 chiffres.

Une citation regrettable

The obvious mathematical breakthrough would be the development of an easy way to factor large prime numbers.

Bill Gates, The Road Ahead, Viking Penguin (1995).

5.3. La méthode RSA

En 1977, trois mathématiciens du M.I.T., R.L. Rivest, A. Shamir et L. Adleman, ont l'idée d'utiliser les nombres premiers pour construire un code qui ne pouvait être déchiffré par un intercepteur même à l'aide d'un ordinateur très puissant. La méthode "RSA" (qualifié de méthode "à clé publique") repose essentiellement sur le fait qu'il est pratiquement impossible de factoriser un nombre de 200 chiffres fait de deux facteurs premiers eux-mêmes constitués d'environ 100 chiffres chacun.

Supposons donc qu'un groupe d'individus désirent s'envoyer des messages secrets. D'abord chacun se trouve deux nombres premiers p et q d'environ 100 chiffres. Chaque membre du groupe publie dans un bottin (accessible à n'importe qui) le nombre $n = p \times q$ correspondant, ainsi qu'un nombre a qui n'a aucun facteur en commun avec $p-1$, ni avec $q-1$, de sorte que $\text{pgcd}(a, (p-1)(q-1)) = 1$. Par exemple, supposons qu'Alice veut envoyer un message à Bob ...

Alice veut envoyer un message secret à **Bob**

- -

BOB

$p = 2038074743$, $q = 2059519669$:	(secret)
$n = 4197455020100620067$, $a = 13$:	(public)
$x = 3228811550771558197$, $y = -10$: (tels que $ax + \phi(n)y = 1$)	(secret)

ALICE

Alice veut envoyer le message:
"napoleon"
Elle écrit alors le message en chiffres en utilisant la règle
$A = 01$, $B = 02$, ..., $Z = 26$,
ce qui donne le message chiffré
$m = 1401161512051514$.
Elle envoie donc le nombre m^a modulo n,
i.e. le reste de la division de m^a par n,
i.e. le nombre $c = 4048910886833826061$.

BOB

Bob calcule le reste de la division de c^x par n,
ce qui lui donnera le message original m

- -

La raison pour laquelle Bob obtient m découle de l'enchaînement suivant:

$$c^x \equiv (m^a)^x = m^{ax} = m^{1-\phi(n)y} = m^{1+\phi(n)(-y)} = m \times (m^{\phi(n)})^{-y} \equiv m \times 1^{-y} = m \pmod{n},$$

car $m^{\phi(n)} \equiv 1 \pmod{n}$.

5.4. La méthode de factorisation avec les courbes elliptiques – un aperçu

On a vu que la méthode RSA utilisée dans le système de clé publique s'est avérée très sécuritaire en cryptographie. Rappelons que l'efficacité de la méthode RSA repose essentiellement sur deux phénomèmes:

- d'une part, on connaît des tests de primalité très efficaces, en ce sens qu'ils permettent d'établir en quelques secondes si un nombre de 100 chiffres est premier ou composé;
- d'autre part, on ne connaît pas d'algorithme permettant de factoriser en un temps raisonnable un nombre de 200 chiffres qui est produit de deux nombres premiers d'environ 100 chiffres chacun.

Toutefois, son grand inconvénient est qu'elle nécessite beaucoup d'espace-mémoire pour sauvegarder la clé privée. Or ce n'est pas le cas avec la méthode des courbes elliptiques de H. Lenstra, laquelle assure pratiquement le même niveau de sécurité avec cette fois des clés beaucoup plus petites.

Ainsi, revenons à la méthode de Rivest, Shamir et Adleman pour la comparer avec celle de Lenstra. La méthode RSA repose sur la fonction de multiplication (ici $\mathcal{P}$ désigne l'ensemble des nombres premiers impairs)

$$\begin{array}{rccl} f & : & \mathcal{P}\times\mathcal{P} & \to & \mathbf{N} \\ & & (p,q) & \mapsto & n=pq, \end{array}$$

qui, à deux nombres premiers p, q associe leur produit $n = pq$. Or le calcul de f^{-1} est en général très difficile, voire même quasi-impossible pour de grands nombres n qui sont produits de deux nombres premiers également très grands.

La méthode des courbes elliptiques considère un point rationnel P pris sur une courbe elliptique E définie sur un corps fini (en l'occurence $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$), et applique alors la fonction

$$\begin{array}{rccl} g & : & \mathbf{N} & \to & E \\ & & k & \mapsto & kP, \end{array} \tag{1}$$

où kP est tout simplement le point P additionné k fois, jusqu'à ce que l'addition mène à une impasse. Or, tout comme dans le cas de RSA, la fonction inverse de (**??**) est très difficile à calculer: c'est ce qu'on appelle le *problème du logarithme discret*.

Alors que le plus récent "défi RSA", qui consistait à factoriser un nombre de 155 chiffres, a récemment été relevé avec succès (voir le double encadré de la page **??**), le défi courant pour calculer l'inverse de (**??**) concerne un nombre k de 33 chiffres. La raison est que l'on dispose d'une foule d'algorithmes relativement efficaces pour factoriser un nombre n donné (disons, de moins de 100 chiffres), alors qu'on en connaît très peu pour résoudre le problème du logarithme discret.

6. Le problème P $\neq$ NP

Examinons d'abord quelques problèmes typiques pour lesquels il peut être commode de disposer d'un algorithme permettant d'obtenir la résolution:

1. Problème de tri: Étant donné un ensemble d'entiers, les ranger en ordre croissant.
2. Problème de l'emploi du temps: Étant donnée une liste de cours devant être offerts, la grille de disponibilité des étudiants et celle des professeurs, construire un emploi du temps qui ne contient aucun conflit d'horaire.

3. Problème du commis voyageur: Étant donné un certain nombre de villes, trouver l'itinéraire le plus court permettant de traverser chacune d'elle, une et une seule fois.

Il s'agit là de problèmes d'optimisation combinatoire.

Dans chaque cas, il faut minimiser une certaine fonction $f(x)$, i.e. une grandeur $f(x)$. Par exemple, dans le premier problème, on cherche à minimiser le nombre d'entiers mal classés, alors que dans le dernier, on cherche à minimiser la distance totale parcourue.

On désigne par **P** la classe des problèmes que l'on peut résoudre au moyen d'un algorithme dans un temps polynomial.

On désigne par **NP** la classe des problèmes que l'on peut résoudre au moyen d'un algorithme non déterministe et vérifier sa solution en un temps polynomial.

De toute évidence, tout problème **P** est aussi **NP**. On se demande si l'inverse est vrai. Autrement dit si on peut vérifier une solution dans un temps polynomial, peut-on la trouver dans un temps polynomial ? Donnons à cet effet deux exemples:

- Considérons le problème de la factorisation d'un entier positif donné n. Si on nous donne ses deux facteurs premiers p et q, alors on est capable de vérifier en temps polynomial qu'effectivement $n = pq$. Par contre, on est encore incapable à ce jour de trouver en temps polynomial les nombres premiers p et q tels que $n = pq$.

- Vous arrivez à un party où il y a 200 personnes. Vous vous demandez si vous connaissez quelqu'un à ce party. Lors de votre arrivée, l'organisateur vous avise que vous connaissez Louise qui est là tout au fond de la salle: d'un seul coup d'oeil, vous pouvez constater qu'effectivement, Louise, une de vos connaissances, est en effet présente. Sans cette information, il vous aurait fallu faire le tour des personnes présentes pour être en mesure de vérifier que vous êtes effectivement en pays de connaissance, une opération qui risque de prendre beaucoup plus de temps.

On se doute bien que $\mathbf{P} \neq \mathbf{NP}$. Toutefois, il s'agit encore aujourd'hui d'un problème non résolu. Ce qui fait que ce problème est si difficile, c'est qu'il est difficile de démontrer qu'un problème ne peut pas être résolu dans un temps polynomial. En effet, pour ce faire, il faudrait être capable d'envisager tous les algorithmes possibles et de démontrer qu'ils sont tous inefficaces. À titre d'exemples de démonstrations de non existence, mentionnons le problème de la quadrature du cercle, celui de la résolution par radicaux de l'équation du 5^e degré ou celle d'une démonstration de l'hypothèse du continu.

Conclusion: du mystère à la consolation !

Les nombres premiers sont donc très mystérieux. Mais il est ironique de constater que, finalement, c'est notre incapacité à saisir leur comportement qui nous a permis de développer des méthodes de cryptographie qui pour le moment sont parfaitement sécuritaires. Nous pouvons donc nous considérer comme consolés ...

Lectures recommandées

- R. Crandall et C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, 2000.
- J.M. De Koninck et A. Mercier, *Introduction à la théorie des nombres*, Modulo, 1994.
- J.P. Delahaye, *Merveilleux nombres premiers*, Belin - Pour la Science, 2000.
- R.A. Mollin, *An Introduction to Cryptography*, CRC Press, 2000.
- P. Ribenboim, *The New Book of Prime Number Records*, Springer, 1996.

Le coin des problèmes ouverts

Existe-t-il une infinité de nombres premiers de Mersenne ?

Autrement dit, existe-t-il une infinité de nombres premiers de la forme $2^n - 1$? À ce jour, on en connaît 40: les 5 plus petits sont $2^2 - 1$, $2^3 - 1$, $2^5 - 1$, $2^7 - 1$ et $2^{13} - 1$; les 4 plus grands connus sont

$$2^{3012377} - 1, \quad 2^{6972593} - 1, \quad 2^{13466917} - 1 \text{ et } 2^{20996011} - 1.$$

Ce dernier nombre est le plus grand nombre premier connu. Un prix de 100 000$ US est offert à la première personne qui trouvera un nombre premier ayant au moins un million de chiffres. Chacun peut participer à la recherche de nombres premiers de Mersenne en visitant le site `www.mersenne.org`.

Existe-t-il une infinité de nombres premiers de Fermat ?

Les nombres de Fermat sont les nombres de la forme $2^{2^n} + 1$. À ce jour, les seuls connus qui soient premiers sont

$$\begin{aligned} 2^{2^0} + 1 &= 3 \\ 2^{2^1} + 1 &= 5 \\ 2^{2^2} + 1 &= 17 \\ 2^{2^3} + 1 &= 257 \\ 2^{2^4} + 1 &= 65537 \end{aligned}$$

Existe-t-il une infinité de nombres de Fibonacci qui soient premiers ?

Les 12 plus petits nombres de Fibonacci qui sont premiers sont

$$2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437, 2971215073, 99194853094755497.$$

Rappelons que la suite des nombres de Fibonacci est la suite 1, 1, 2, 3, 5, 8, 13, 21, 34,..., où chaque terme (à partir du 3^e) est la somme des deux précédents.

Une citation

"En observant les nombres premiers, on éprouve le sentiment d'être en présence d'un des plus inexplicables secrets de la création."

Arthur Hennessy

Existe-t-il une infinité de nombres premiers de la forme $n^2 + 1$?

Les nombres premiers 2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, ... sont tous de la forme $n^2 + 1$. Nous sommes tous convaincus que cette suite est infinie, mais une preuve nous échappe. Toutefois, en 1998, John Friedlander et Henryk Iwaniec ont démontré qu'il existait une infinité de nombres premiers de la forme $a^2 + b^4$ (malheureusement, dans leur preuve, il n'est pas clair qu'on peut prendre $b = 1$ infiniment souvent.)

Les nombres de la forme $n! + 1$

Le nombre $n! + 1$ est premier lorsque n vaut 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1477, 6380 et 26951. Y en a-t-il d'autres ? Sûrement !

Les nombres de la forme $n! - 1$

Le nombre $n! - 1$ est premier lorsque n vaut 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1963, 3507, 3610, 3697, 21480 et 34790. Y en a-t-il d'autres ? Qu'en pensez-vous ?

Les fascinants nombres premiers de Wieferich

D'après le petit théorème de Fermat, on sait que si p est un nombre premier impair, alors $2^{p-1} \equiv 1 \pmod{p}$ (ce qui veut dire que p divise $2^{p-1} - 1$). Existe-t-il des nombres premiers p tels que $2^{p-1} \equiv 1 \pmod{p^2}$? Oui! On en connaît deux, soit 1093 et 3511. Tout nombre premier $p > 2$ qui satisfait la congruence $2^{p-1} \equiv 1 \pmod{p^2}$ est appelé un *nombre premier de Wieferich* (en l'honneur de A. Wieferich qui y a vu un lien avec le *dernier théorème de Fermat*). À part 1093 et 3511, on sait qu'il n'y a aucun autre nombre premier de Wieferich inférieur à 10^{15}. On croit qu'il en existe une infinité, mais on ne sait pas le démontrer. On a même des raisons de croire que la quantité de nombres premiers de Wieferich $\leq x$ est environ $\log\log x$. Ce qui est particulièrement troublant, c'est qu'on ne sait même pas démontrer qu'il y a une infinité de nombres premiers qui ne sont pas des nombres premiers de Wieferich !