Prime numbers

Webster's New Collegiate Dictionary defines prime as follows.
prime \'prim\ *n* [**ME**, fr. **MF**, fem. of *prin* first, **L** primus ; akin to **L** prior]

1. : first in time : ORIGINAL

2. (a) : having no factor except itself and one ⟨*3 is a ~number*⟩

   (b) : having no common factor except one ⟨*12 and 25 are relatively ~*⟩

3. (a) : first in rank, authority or significance : PRINCIPAL

   (b) : having the highest quality or value ⟨*~television time*⟩

Each of Webster's definitions may be applied to this page, but the most operative is **2a** : *An integer greater than one is* ***prime*** *if its only positive divisors are itself and one* (otherwise it is **composite**). For example : 15 is composite because it has the two prime divisors 3 and 5.

Un article traduit du SCIENCE NEWS de Washington

in COURRIER INTERNATIONAL N°628 DU 14 AU 20 NOVEMBRE 2002

Des chercheurs indiens viennent d'annoncer la mise au point d'un algorithme capable de déterminer, à coup sûr et en un temps raisonnable, si un nombre est premier.

Les nombres premiers sont au coeur de certaines des interrogations les plus anciennes et les plus complexes des mathématiques. Ces nombres, qui sont divisibles seulement par un et par eux-mêmes, sont les éléments de base des nombres entiers. Depuis quelques décennies, les nombres premiers occupent une place de tout premier plan dans la recherche mathématique, car ce sont des éléments de codage particulièrement appréciés et largement utilisés pour assurer la sécurité de messages numérisés. Bien qu'il en existe une quantité infinie, ils sont relativement rares et leur répartition au sein des nombres entiers est aléatoire. Seuls 1 091 987 405 - environ 4 % - des 25 premiers milliards de nombres entiers sont des nombres premiers. Et plus les nombres sont grands, plus la proportion diminue. Leur distribution dans la suite des nombres entiers ne suit aucun modèle, ce qui les rend difficiles à identifier. Exemple 687 532 127 est-il un nombre premier ? II n'y a aucun moyen de le savoir de prime abord. Il est évident qu'il n'est divisible ni par 2 ni par aucun autre nombre pair. Mais est-il divisible par 3 ? par 5 ? par 7 ? par 26 203 ? En fait, 687 532 127 n'est divisible que par lui-même et par 1. C'est donc un nombre premier.

DU CRIBLE D'ERATOSTHÈNE AU PETIT THÉORÈME DE FERMAT

Cette élimination par des divisions successives est à la base du procédé inventé par Eratosthène (mathématicien grec du III^{e} siècle ante C.). Le crible d'Eratosthène est une méthode permettant de vérifier de façon systématique si un nombre est premier ou non, en le divisant par tous les nombres premiers, en commençant par 2 et en allant jusqu'à la racine carrée du nombre étudié. S'il ne peut être divisé sans reste par aucun nombre entier, c'est un nombre premier. Mais, pour les très grands nombres, ces divisions sont extrêmement fastidieuses et prennent beaucoup de temps. Pourtant, ces opérations de base sont de plus en plus nécessaires à cause de l'utilisation de plus en plus courante de la cryptographie. S'il est relativement simple de multiplier de grands nombres premiers, il est considérablement plus difficile de décomposer le résultat de cette opération en produit de facteurs et de retrouver les nombres premiers originaux. Or ces opérations sont précisément celles qui permettent de décoder les messages cryptés. Cette méthode exige d'avoir sous la main une réserve de nombres premiers élevés, et c'est pourquoi elle a incité mathématiciens et informaticiens à chercher des méthodes de plus en plus efficaces pour les identifier. Une équipe de l'Institut indien de technologie (IIT), à Kanpur, vient d'imaginer un nouveau moyen de les détecter. Ce procédé novateur résout un problème auquel la théorie des nombres et l'informatique sont confrontées depuis longtemps, en apportant une amélioration fort attendue à l'efficacité théorique des algorithmes d'authentification. "C'est un résultat superbe, qui donne un coup de fouet à la théorie algorithmique des nombres", estime Carl Pomerance, théoricien des nombres aux laboratoires Bell, à Murray Hill, dans le New jersey. L'équipe de l'IIT, composée de Manindra Agrawal, de Neeraj Kayal et de Nitin Saxena, a publié sa découverte en août dernier. La validité des résultats n'a pas tardé à être confirmée par des mathématiciens, et certains chercheurs ont déjà réussi à améliorer le procédé. L'efficacité du vénérable crible d'Eratosthène est liée au nombre de divisions nécessaires pour appliquer un test de prima-

lité à un nombre entier. Le problème, c'est que ce nombre de divisions augmente de façon exponentielle en fonction du nombre de chiffres composant le nombre entier. Donc, même si cette méthode se révèle fort pratique pour identifier les nombres premiers inférieurs à 10 milliards (comportant 9 chiffres), elle n'est d'aucune utilité pour les nombres à 25 chiffres ou plus. En revanche, les procédures informatisées, aujourd'hui très répandues en la matière, se fondent sur un principe mathématique découvert au XVII^{e} siècle par Pierre de Fermat, magistrat et mathématicien français. Son "petit théorème", comme on l'appelle communément, exprime une relation surprenante concernant les nombres premiers : soit p un nombre premier et a un entier quelconque ; en divisant a^p et a par p, on obtient un résultat donnant le même reste. Par exemple, si $p = 7$ (un nombre premier) et $a = 9$, lorsqu'on divise 9^7 par 7, le reste est égal à 2 : $[9^7 = 4\,782\,969 = (7 \times 683\,281) + 2]$, comme lorsqu'on divise 9 par 7 : $[9 = (7 \times 1) + 2]$. Tout nombre entier qui ne passe pas ce test n'est pas un nombre premier. Cependant, comme de rares nombres composés [résultats de la multiplication de plusieurs facteurs premiers] satisfont eux aussi à cette condition, la méthode n'est pas un test infaillible pour détecter un nombre premier. Dans le cadre d'applications pratiques, ce test est suffisant. Les algorithmes les plus efficaces créés sur la base du petit théorème de Fermat testent le nombre entier avec une valeur de a prise au hasard. Lorsqu'un nombre entier réussit le test de Fermat, il n'y a qu'une très faible probabilité pour que ce ne soit pas un nombre premier. S'il réussit un nouveau test avec une autre valeur de a prise au hasard, cette probabilité est encore plus faible. En répétant le test un nombre de fois suffisant, on peut ramener cette probabilité d'erreur à une valeur proche de zéro. Ce qui suffit dans le cadre d'un système cryptographique. Pourtant, ces algorithmes ont le défaut d'être extrêmement lents.

UNE JOURNÉE POUR IDENTIFIER UN NOMBRE DE 30 CHIFFRES

En 1999, Manindra Agrawal s'est essayé à une méthode relativement simple, mais négligée par les autres chercheurs. Il demanda leur aide à Neeraj Kayal et à Nitin Saxena, qui, à l'époque, étaient encore étudiants. Et l'été dernier l'équipe amis au point une méthode complète et une preuve mathématique établissant son efficacité théorique. L'équipe de l'IIT a découvert une version nouvelle, généralisée, du petit théorème de Fermat, dans laquelle les nombres entiers a et a^p sont remplacés par les expressions polynomiales $(x - a)$ et $(x^p - a)$. Sur cette base, ils ont formulé un algorithme et prouvé que ce dernier donnait la réponse en temps raisonnable. Les experts qui se sont longuement penchés sur l'algorithme d'Agrawal, de Kayal et de Saxena lui ont déjà apporté des améliorations. L'une de ces variantes a été mise au point par Hendrik W. Lenstra, de l'université de Californie, à Berkeley. Richard E. Crandall a démontré récemment qu'un ordinateur programmé avec cette variante peut authentifier un nombre premier de 30 chiffres en un jour environ, contre plusieurs années avec la version originale de l'algorithme de l'IIT. Si c'est un progrès significatif en matière de performance, on est encore loin de la vitesse nécessaire pour identifier, par exemple, des nombres de 1 000 chiffres. Mais il y a de l'espoir. Une étape primordiale de l'algorithme modifié de Lenstra peut être aisément fractionnée entre un grand nombre d'ordinateurs. Un projet dans lequel les ordinateurs de volontaires du monde entier se partageraient les calculs pourrait facilement, estime Richard E. Crandall, traiter un nombre premier ayant 1 000 chiffres en un an environ. D'autres améliorations de l'algorithme d'Agrawal, de Kayal et de Saxena sont peut-être à attendre. "En laissant aux théoriciens des nombres une année pour étudier cet algorithme, on devrait en savoir beaucoup plus quant à son avenir", dit Chris K. Caldwell, de l'université du Tennessee, à Martin. Précision, Fermat est plus connu pour un autre théorème que celui qui est décrit ci-contre, le grand théorème". Il énonce que, si n est supérieur à 2, il n'y a pas d'entiers x,

y et z non nuls pour lesquels $x^p + y^p = z^p$. Il a été démontré en 1995 par le Britannique Andrew Willes. Le "petit théorème" a été démontré au XVII^e siècle par le mathématicien lui-même. Moins médiatisé que son grand frère, Il est d'une efficacité qui n'est pas moins redoutable.

Les questions

Certaines questions ont leur réponse, ou la base de l'argumentation, dans le texte : il faut alors citer le paragraphe et le numéro de ligne.

1. What's a prime number (write your answer in the same langage) ?
2. Recopie le crible d'Eratosthène pour les 100 premiers entiers en expliquant le moyen de son obtention.
3. Quel est le premier nombre premier supérieur à 1 000 (justifie la réponse) ?
4. À quoi peuvent bien servir les nombres premiers ?
5. Qu'est-ce que la *cryptographie* ?
6. Parmi les cent premiers nombres entiers, y a-t-il *proportionnellement* autant de nombres premiers que dans les 25 premiers milliards de nombres entiers (justifie la réponse) ?
7. Combien faut-il effectuer, au minimum, de divisions pour tester si 97 est un nombre premier (détailler) ?
8. Explique, numériquement et graphiquement, le terme *exponentiel* trouvé dans :
   «Le problème, c'est que ce nombre de divisions augmente *de façon exponentielle* en fonction du nombre de chiffres composant le nombre entier.»
9. Peux-tu trouver trois nombres entiers naturels distincts x, y et z tels que : $x^2 + y^2 = z^2$ (justifie la réponse) ?
   Et tels que : $x^3 + y^3 = z^3$ (justifie la réponse) ?
10. Donne un exemple d'application du *petit théorème de Fermat* (autre que celui cité dans le texte) en expliquant son utilité.

Et pour terminer, quatre références sur la toile mondiale :
`http://fr.wikipedia.org/wiki/Nombre_premier`
`http://primes.utm.edu/`
`http://perso.wanadoo.fr/yoda.guillaume/Vocabula/GlosP/Premier.htm`
`http://www.mathgoodies.com/francais/volume3/prime_composite_fr.html`