Nombres premiers : pour l'amour des maths et le goût du secret

En janvier dernier, David Slowinski et Paul Gage, deux chercheurs de la société Cray Research ont connu leur heure de gloire. Ils venaient de découvrir un nombre premier de 258 716 chiffres après avoir fait tourner pendant sept heures un de leurs supercalculateurs. 258 716 chiffres, cela représenterait une bonne centaine de pages d'*Isotopes*, et la découverte a suscité une admiration légitime : l'idée qu'un si long nombre ne puisse être divisé (si ce n'est par lui même et par 1) imposait le respect. Pourtant, dénicher de très grands nombres premiers constitue encore un exercice relativement facile...

Une formule du 17ème siècle épuise les ordinateurs géants

Les mathématiciens de Cray Research se sont en effet contentés de faire tourner l'algorithme de Lucas et Lehmer, qui teste les nombres obtenus avec la formule de Mersenne. Ce dernier, un père jésuite contemporain de Pascal et Descartes, avait avancé dès le 17ème siècle que si le nombre p était premier, la formule $2(p)-1$ pouvait donner un nombre premier. Quatre siècles de recherches lui ont donné raison : on connaît à ce jour 32 valeurs de p, dont la plus élevée, 859 433, vient d'être découverte... Et l'utilisation de l'algorithme de Lucas et Lehmer sur cette formule vieille de 300 ans est si éprouvante pour un supercalculateur qu'elle sert de test de "rodage" avant livraison pour tous les calculateurs Cray !

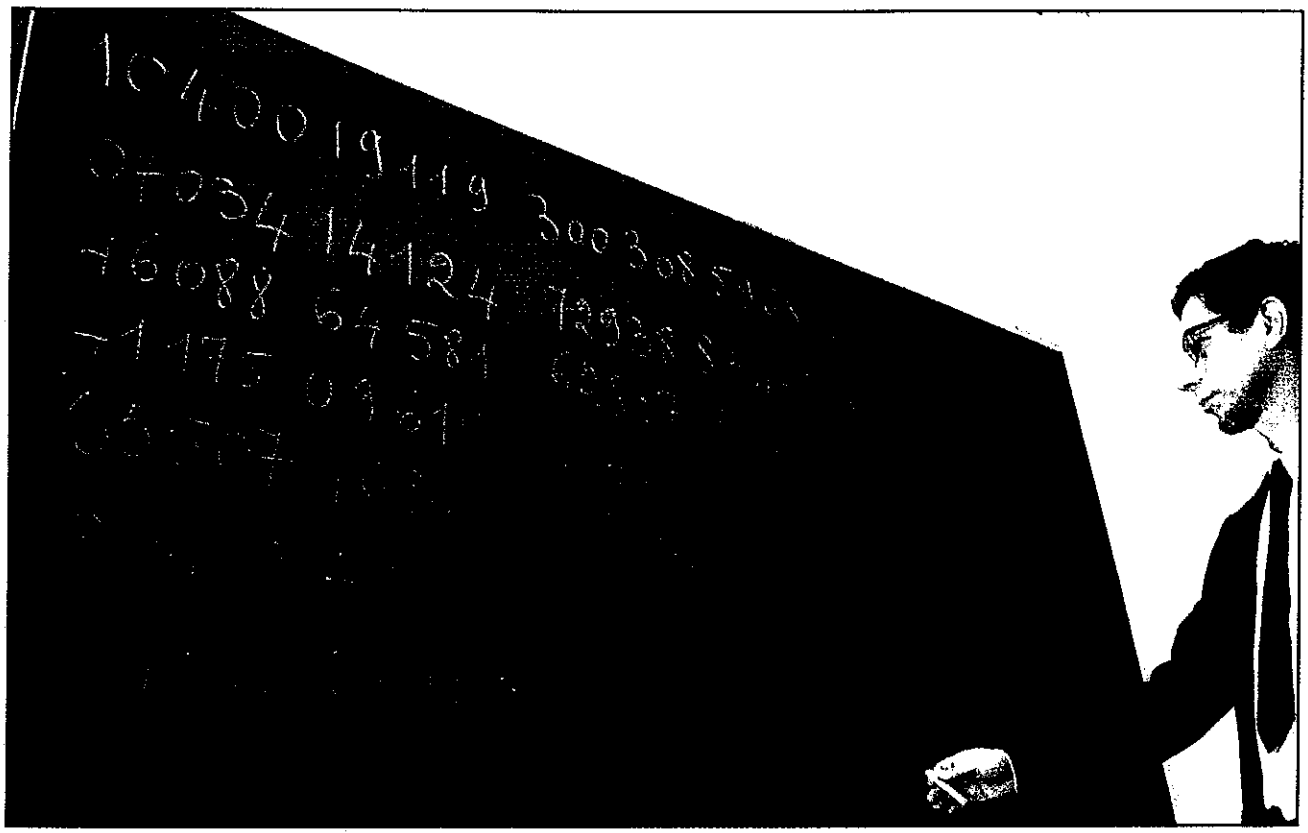
Dans l'univers très rationnel des mathématiques, les nombres premiers constituent un domaine énigmatique. Plus on avance et plus l'horizon s'élargit : on compte 4 nombres premiers entre 1 et 10 (par convention, 1 n'est pas premier), 21 entre 10 et 100, 143 entre 100 et 1000... Plus on cherche et plus on tâtonne : la primalité d'un nombre se démontre par défaut, en constatant l'absence de diviseurs (autres que le nombre et 1), et comment démontrer l'absence ? Plus on explore l'histoire, et plus on découvre l'obstination de quelques passionnés : un autre Lehmer, père du précédent, avait publié dès 1900, la liste des nombres premiers inférieurs à 10 millions !

L'annonce très médiatique de grands nombres premiers n'est que la partie émergée de l'iceberg. Avec plus de discrétion, les chercheurs travaillent sur des sujets autrement difficiles : comment décompter les nombres premiers au sein d'un ensemble d'entiers ? Comment démontrer la primalité ou la non-primalité d'un nombre ? Comment "factoriser" un grand nombre, c'est-à-dire retrouver ses diviseurs ? Autant de questions qui portent sur des nombres de plusieurs dizaines à plusieurs centaines de chiffres, bien au-delà de nos capacités de perception...

Le décompte des nombres premiers compris entre 1 et n s'enseigne à l'école, avec l'apprentissage du crible d'Eratosthène : on écrit tous les entiers entre 2 et n ; 2 est le premier nombre premier, on supprime tous les multiples de 2 ; le premier nombre non rayé est 3, c'est le deuxième nombre premier, on supprime tous les multiples de 3 ; etc, etc.

Inconvénient majeur de cette technique : c'est long ! Pour "passer au crible" un nombre de 20 chiffres, il faudrait un temps supérieur à la durée de vie probable de l'univers... C'est pourquoi les mathématiciens se sont tournés rapidement vers d'autres techniques.

En 1985, trois américains, Lagarias, Miller et Odlyzko, mettent au point une formule qui leur permet de



Si impressionnant soit-il, ce nombre premier compte à peine deux cents chiffres

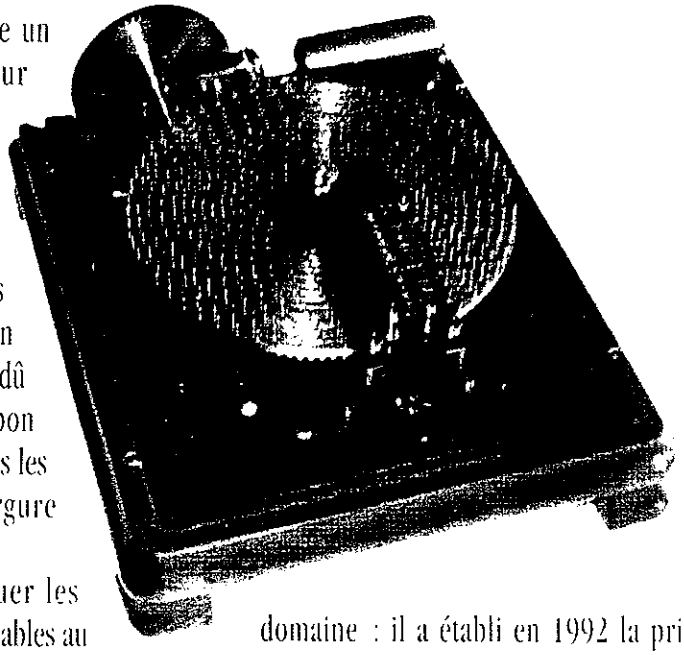
comptabiliser les nombres premiers jusqu'à $4x10^{16}$. Cette formule est également valable pour de plus grands nombres, mais l'ordinateur ne peut suivre : il manque de puissance et ne peut gérer davantage de chiffres !

Nouvelle étape en 1993 : Marc Deléglise et Joël Rivat, deux chercheurs du Laboratoire de Logique, Mathématiques Discrètes, Informatique - LMDI[1], divisent par 20 le temps de traitement en améliorant la "mise en informatique" de la formule. Et découvrent qu'il existe 24 739 954 287 740 860 nombres premiers entre 2 et 10^{18}. Pourtant, à nouveau, les cerveaux humains et électroniques se heurtent à la barrière du temps : il a fallu 15 jours à une station de travail Hewlett-Packard pour accoucher de ce résultat ! Et il lui faudrait trois mois pour traiter les premiers jusqu'à 10^{19}. Inutile d'aller plus loin, d'autant que la recherche sur les nombres premiers a bien d'autres facettes. Avec la recherche de la primalité d'un nombre et sa factorisation, on sort des travaux de connaissance pure pour aborder les applications industrielles. Depuis une quinzaine d'années, les nombres premiers deviennent la pierre d'angle des systèmes de cryptographie qui garantissent la confidentialité des transmissions militaires, des réseaux informatiques, des opérations bancaires, des cartes de crédit... Exit les codages à base de lettres, que les linguistes et les informaticiens percent trop facilement : les nombres premiers de cent chiffres et plus constituent un rempart autrement efficace.

Militaires et banquiers confient leurs secrets au talent des mathématiciens

Si de nombreux systèmes ont été mis au point, le plus fiable est sans conteste le RSA, dit "à clé révélée" : on prend deux nombres premiers d'une centaine de chiffres et on les multiplie l'un par l'autre pour obtenir un nombre de deux cents chiffres qui devient la base du cryptage. Pour "ouvrir la porte", le destinataire doit, dans l'état actuel des connaissances, disposer obligatoirement des deux diviseurs. Or la

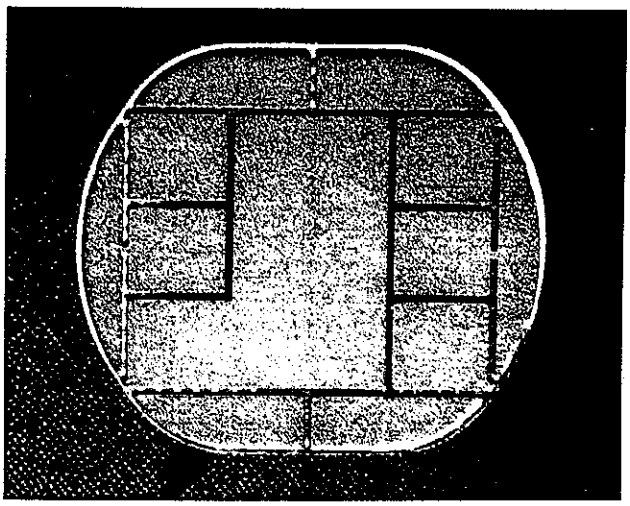
recherche de ces diviseurs reste encore un problème quasi insoluble ; malgré leur obstination, malgré les puissants ordinateurs dont ils disposent, les chercheurs parviennent à peine à factoriser des nombres de plus de cent chiffres. Il y a quelques années, les mathématiciens de Bell ont déverrouillé un nombre de 155 chiffres ; mais ils avaient dû mobiliser pendant plusieurs heures un bon millier d'ordinateurs ! Difficile à répéter tous les jours, même pour des espions d'envergure internationale...



Reste une question : comment fabriquer les nombres premiers de cent chiffres indispensables au codage ?

Les chercheurs travaillent en fait à l'envers : ils proposent à l'ordinateur des nombres de cent chiffres en abondance, et celui-ci effectue en moins d'une minute la vérification de primalité de chacun d'entre eux.

La méthode ne s'appuie pas sur la recherche de diviseurs - on a vu plus haut que la tâche était impossible - mais sur des moyens parallèles qui fournissent en fin de calcul des



coefficients, ou "certificats de primalité" qui indiquent si le nombre est premier ou non.

L'opération est devenue routinière pour les nombres de cent chiffres, mais elle tient encore de l'exploit au-delà des 1000 chiffres. François Morain, autre chercheur du LMDI, détient un prestigieux record du monde dans ce domaine : il a établi en 1992 la primalité d'un nombre de 1505 chiffres.

Pourtant, mathématiciens et cryptographes doutent encore de la sécurité de leurs systèmes.

La sécurité des codes reste à la merci d'une nouvelle formule

Comment affirmer avec certitude qu'on ne peut factoriser des nombres de deux cents chiffres ? Ne peut-on pas "ouvrir la porte" sans trouver les diviseurs, de la même façon qu'on démontre une non-primalité sans trouver les diviseurs ? Des questions nouvelles pour les spécialistes des nombres premiers, passés en deux décennies du statut de chercheurs de l'ombre à celui de gardiens de la confidentialité des armes, des finances et des ordinateurs de ce monde... Pour Jean-Louis Nicolas, directeur du LMDI, la réponse ne se trouve pas nécessairement du côté des mathématiques : *"les secrets les mieux gardés sont toujours à la merci d'une photocopie oubliée dans une corbeille ou d'une confidence sur l'oreiller"*. Il faudra toutefois bien de la mémoire et de la patience aux Mata-Hari de demain pour soutirer à leur conquête les 127 chiffres d'une clé de cryptage !

BENOIT PLAYOUST

(1) Laboratoire de Logique, Mathématiques Discrètes, Informatique LMDI - UCB La Doua - 43, boulevard du 11 novembre 1918 69622 Villeurbanne Cedex