La factorisation des grands nombres

JOHANNES BUCHMANN

Les systèmes modernes de cryptage de données seront sûrs tant que la décomposition des nombres de plus de 100 chiffres en facteurs premiers restera difficile. Toutefois les techniques de factorisation progressent rapidement.

Le nombre 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 est le produit de deux nombres premiers ; lesquels? Martin Gardner posa cette question aux lecteurs de *Pour la Science* en octobre 1977, dans sa rubrique de «Jeux mathématiques», mais une réponse ne fut donnée que 16 ans plus tard : en avril 1994, Paul Leyland, de l'Université d'Oxford, Michael Graff, de l'Université de l'Iowa, et Derek Atkins, de l'Institut de technologie du Massachusetts, identifièrent les deux facteurs, après avoir distribué des parties de la tâche, grâce au réseau *Internet*, à quelque 600 volontaires, qui laissèrent fonctionner sur leurs ordinateurs, pendant de nombreuses nuits, le programme écrit par Arjen Lenstra, du Centre de recherches de la Société *Bell Communications*.

La multiplication de deux nombres, même très grands, n'est pas compliquée : avec du papier et un crayon, on calcule le produit de deux nombres de 65 chiffres en une heure environ ; par ordinateur, le calcul est immédiat. En revanche, l'opération inverse, c'est-à-dire l'identification des facteurs d'un produit, est très difficile, même avec les calculateurs les plus rapides.

Les opérations mathématiques telles que la multiplication et la factorisation sont à la base des systèmes cryptographiques modernes : le cryptage est rapide, mais le décryptage est quasi impossible en pratique.

En 1978, Ronald Rivest, de l'Institut de technologie du Massachusetts, Adi Shamir, de l'Institut Weizmann à Rehovot (Israël), et Leonard Adleman, de l'Université de Californie du Sud, ont mis au point un protocole de cryptage, nommé RSA d'après leurs initiales, qui est fondé sur la factorisation : une personne voulant recevoir des messages cryptés choisit deux nombres premiers p et q, c'est-à-dire deux nombres entiers naturels qui ne sont divisibles que par 1 et par eux-mêmes ; il calcule leur produit $p \times q$ et le rend public, tout en conservant secrets les facteurs *(voir l'encadré de la page 90)*. Pour crypter un message, il suffit de connaître ce produit, nommé la clé publique, tandis que, pour décrypter un message, il faut connaître les facteurs premiers p et q : si ceux-ci ont plus de 150 chiffres, même les meilleures méthodes connues et les ordinateurs les plus puissants mettront 2 000 ans pour les trouver. Ainsi, on fabrique facilement des problèmes de factorisation, mais on ne sait pas, aujourd'hui, les résoudre en un temps raisonnable, si les facteurs premiers sont trop grands.

Trouvera-t-on un jour une méthode de factorisation rapide? Les Laboratoires RSA ont organisé un concours mondial de factorisation. Ils publient des produits de grands nombres premiers et récompensent leur factorisation *(on peut consulter leur site sur le réseau Internet : voir la bibliographie)*.

L'idée de mettre le public à contribution est judicieuse : on ignore si la factorisation est difficile par essence ou si les mathématiciens n'ont pas encore trouvé la méthode la plus habile. Aussi la seule garantie de la sécurité des procédés de cryptage est l'ignorance d'une méthode rapide de factorisation des nombres entiers.

L'étude de la factorisation date de l'Antiquité : les mathématiciens d'alors savaient déjà que chaque nombre naturel est un produit de nombres premiers, et que la décomposition en facteurs premiers est unique, à l'ordre près. Par exemple, 12 se décompose seulement en $2 \times 2 \times 3$. L'étude des propriétés des nombres entiers naturels impose souvent la décomposition en facteurs premiers.

Les ordinateurs ont beaucoup apporté à la théorie des nombres. Dans cet article, nous verrons comment fonctionnent les algorithmes modernes de factorisation. Souvent les indications seront suffisamment précises pour qu'une programmation soit possible sur un ordinateur personnel ; en outre, une bibliothèque de programmes nommée LiDIA est proposée sur le réseau *Internet (voir la bibliographie)*.

Les nombres de Fermat

Le juriste français Pierre de Fermat (1601-1665), notamment célèbre pour sa conjecture démontrée en 1997, pensait avoir trouvé une méthode pour fabriquer des nombres premiers aussi grands que l'on voulait : à partir des nombres entiers naturels i, il construisait les nombres $F_i = 2^{2^i} + 1$, nommés aujourd'hui nombres de Fermat. Les quatre premiers nombres de Fermat sont premiers : $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$ et $F_4 = 2^{2^4} + 1 = 65\,537$.

Cependant, dès 1732, le mathématicien suisse Leonhard Euler trouva que