

convenaient plus pour des diamètres supérieurs. Après avoir échoué cinq fois dans ses tentatives de fabriquer un miroir de 42 centimètres de diamètre, Foucault conçut trois techniques pour le contrôle des surfaces optiques, ce que l'on nomme aujourd'hui le «foucaultage des miroirs». La plus efficace était le test du «tranchant de couteau» : une lame mince élimine partiellement l'image réfléchie d'une source ponctuelle, de sorte que l'on perçoive les défauts de polissage comme des reliefs exagérés, ce qui permet leur élimination.

Le plus grand des télescopes qu'il réalisa comprenait un miroir de 80 centimètres de diamètre. Il fut installé à l'Observatoire de Marseille. La voie des télescopes géants était ouverte.

La mesure de la distance du Soleil

Pour Le Verrier, la découverte de Neptune n'était que le début de l'œuvre de sa vie : l'analyse des mouvements des corps dans le Système solaire. Par des calculs extrêmement fastidieux, Le Verrier affina les estimations des masses des planètes. Il découvrit également que la distance du Soleil était inférieure de trois pour cent à ce que l'on croyait alors. À cette époque, la vitesse de la lumière était évaluée seulement à partir de mesures astronomiques, dont l'une était celle de la distance du Soleil. Aussi Le Verrier estima que la vraie valeur de la vitesse de la lumière dans le vide était inférieure d'environ trois pour cent à la meilleure estimation astronomique de l'époque, qui était de 308 000 kilomètres par seconde.

Le Verrier demanda à Foucault de l'aider à confirmer cette prévision : pouvait-il modifier son expérience de 1850 afin d'obtenir une mesure absolue de la vitesse de la lumière ? Foucault allongea le trajet lumineux à 20 mètres en utilisant un relais de cinq miroirs concaves à face avant argentée. Une roue dentée, entraînée en rotation par un mouvement d'horlogerie, permettait de régler le miroir tournant, par effet stroboscopique, à une vitesse précise de 400 tours par seconde. Ainsi, en 1862, Foucault annonça à l'Académie des sciences que la vitesse de la lumière dans l'air était égale à 298 000 kilomètres par seconde, conformément à la prédiction de Le Verrier (cette valeur est à moins de un pour cent de la valeur moderne).



William Toin

Les manuels de physique contemporains présentent parfois la mesure de Foucault en indiquant que la méthode était celle qu'adoptait plus tard Albert Michelson aux États-Unis, mais ils montrent mal l'objectif réel de Foucault qui ignorait, comme ses contemporains, que la vitesse de la lumière est une constante physique d'importance primordiale (James Clerk Maxwell ne publia la théorie électromagnétique de la lumière qu'en 1865, et Einstein n'était pas encore né). L'unique question, en 1862, était la distance du Soleil, considérée par Le Verrier comme la question «la plus délicate de l'astronomie moderne».

La mesure de la vitesse de la lumière fut la dernière contribution d'importance de Foucault en phy-

sique. Il consacra le reste de sa vie à des travaux de comité et à des études de régulateurs mécaniques : il cherchait un régulateur de vitesse universel, qui aurait fait sa fortune. Il obtint des systèmes remarquables, supérieurs même à ceux de James Watt, mais les impératifs industriels étaient trop nombreux, et les prototypes qu'il expérimenta étaient dynamiquement instables.

Une vie de chat

Quel était le statut scientifique de Foucault ? Donné écrivait : «Tout le monde ne considérait pas Foucault comme un vrai physicien, [...] et cela, parce qu'il n'avait pas étudié toutes les parties de la science, qu'il aurait peut-



4. CE TÉLESCOPE ÉQUIPÉ D'UN MIROIR DE 20 centimètres de diamètre (à gauche) fut réalisé par Foucault, qui appliqua une mince couche d'argent sur la face avant d'un bloc de verre poli, concave. Il mit au point des techniques pour fabriquer des miroirs bien plus grands, ouvrant ainsi la voie aux télescopes à réflexion géants. Le plus grand des télescopes de Foucault (ci-dessus), qui possède un miroir en verre argenté de 80 centimètres de diamètre, fut réalisé à Paris au début de 1862. Il fut ensuite installé à l'Observatoire de Marseille, où il fut utilisé pendant une centaine d'années. Ce télescope fait aujourd'hui partie du patrimoine historique français.

être été incapable de faire un cours complet de physique élémentaire. [...] Pour beaucoup, c'était un amateur. Lui-même, au reste, se donnait ce titre et s'en glorifiait. "Nous sommes des amateurs [...], mais dans le bon sens ; [...] nous cultivons les points de la science vers lesquels nous porte notre instinct".»

La force de Foucault résidait dans sa précision expérimentale : même aujourd'hui, la mise en place d'un pendule de Foucault n'est pas aisée. Pour un pendule tel que celui du Panthéon, la fréquence de rotation du plan d'oscillation est environ 10 000 fois inférieure à celle de l'oscillation. En fait, le mouvement du plan d'oscillation de bien des prétendus pendules de Foucault ne résulte pas du mouvement de rotation de la Terre, mais des imprécisions de construction et d'expérimentation, qui engendrent une trajectoire composée de boucles.

La Société royale de Londres, qui accorda à Foucault sa distinction la plus prestigieuse, la médaille Copley, en 1855, n'est qu'une des nombreuses sociétés savantes qui reconnurent ses mérites. En France, en revanche, l'expérimentateur n'eut pas droit aux honneurs qu'il méritait : la tradition scientifique française prise plus l'analytique et le formel que l'expérimental et l'intuitif. Or, Foucault avait des connaissances mathématiques limitées.

Sa thèse de doctorat relative aux expériences dans l'air et dans l'eau menées en 1850 contenait des erreurs de calcul qu'il avait été incapable de corriger pendant la soutenance.

Enfin Foucault n'était pas passé par les Grandes Écoles qui formaient l'élite scientifique. C'est peut-être pour ces raisons, et aussi à cause des articles dans le *Journal des débats*, qu'il ne fut élu à l'Académie des sciences qu'en 1865, à la sixième tentative, alors que sa renommée internationale était établie depuis longtemps.

Deux ans plus tard, en juillet 1867, Foucault commença à ressentir des

symptômes de paralysie. Il mourut en moins de sept mois, à l'âge de 48 ans, moins de surmenage et de soucis, comme on le supposa à l'époque, que de ce qui devait être une sclérose en plaques foudroyante.

Dans la notice nécrologique qu'il rédigea, Donné fit découvrir quelques-unes des nombreuses facettes de Foucault : «Lorsque je l'eus introduit dans l'intimité de ma famille, on le trouva souvent désagréable, agaçant, surtout parce qu'il ne se fâchait pas, mais qu'il soutenait son dire du même ton froid et calme. Ce calme était une grande force dans certaines occasions, et je l'ai vu, lui, d'une apparence faible et chétive, faire reculer les plus redoutables adversaires. [...] et sans avoir moins de complaisance à expliquer aux ignorants, et surtout aux ignorantes, les lois les plus abstraites de la physique.»

Foucault ne se maria jamais. Comme l'écrivait Donné : «Il menait, pour ainsi dire, la vie de ces chats de bonne maison qui s'établissent à la meilleure place de la chambre ou du salon... Quand il venait une visite qui ne lui convenait pas, il se retirait dans un coin, avec son carnet et son crayon qui ne l'abandonnait pas.» Donné ajoute : «S'il n'était pas souple, sa fidélité en amitié était à toute épreuve.» De fait, de très nombreuses personnes se réunirent lors de l'enterrement de Foucault.

Son nom fut ultérieurement coulé dans la charpente métallique de la Tour Eiffel. Il n'était pas un génie de l'envergure de Newton ou d'Einstein, mais c'est à bon droit qu'est entré dans la postérité ce fils remarquable de la Ville lumière.

William TOBIN enseigne l'astronomie et la physique à l'Université de Canterbury, en Nouvelle-Zélande. Il prépare une biographie de Foucault.

C.M. GARIEL, *Recueil des travaux scientifiques de Léon Foucault*, éditions Gauthier-Villars, 1878.

William TOBIN, *Foucault's Invention of the Silvered-Glass Reflecting Telescope and the History of His 80-cm Reflector at the Observatoire de Marseille*, in *Vistas in Astronomy*, vol. 30, n° 2, pp. 153-184, 1987.

William TOBIN, *Perfecting the Modern Reflector*, in *Sky & Telescope*, vol. 74, n° 4, pp. 358-359, octobre 1987.

Janet E. BUERGER, *French Daguerreotypes*, University of Chicago Press, 1989.

Le pendule de Foucault au Musée des Arts et Métiers, CNAM, 1990.

William TOBIN, *Tothed Wheels and Rotating Mirrors: Parisian Astronomy and Mid-Nineteenth Century Experimental Measurements of the Speed of Light*, in *Vistas in Astronomy*, vol. 36, n° 3, pp. 253-294, 1993.

W. TOBIN et B. PIPPARD, *Foucault, His Pendulum and the Rotation of the Earth*, in *Interdisciplinary Science Reviews*, vol. 19, n° 4, pp. 326-337, 1994.

Stéphane DELIGEORGES, *Foucault et ses pendules*, Éditions Carré, 1995.

William TOBIN, *Foucault, son pendule et la rotation de la Terre*, in *L'astronomie*, vol. 110, pp. 50-62, février 1996.

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'igno-

rance 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