Les taureaux, l'internet et les quanta: L'arithmétique des très grands nombres

Henri Darmon

September 9, 2007

La physique et la cosmologie sont le domaine des nombres gigantesques – le diamètre approximatif de notre galaxie (5.6×10^{20} mètres), l'âge de l'univers selon la théorie du big bang (10^{10} années à peu près), ou le nombre d'atomes dans le système solaire (2×10^{57}). A tel point que l'expression "nombre astronomique" est passée dans le langage courant pour désigner ces quantités dont la taille défie l'imagination.

Science pure par excellence, l'arithmétique fait parfois intervenir des nombres auprès desquels les "milliards de milliards" chers au cosmologue Carl Sagan feraient piètre figure. Le problème des *taureaux d'Archimède* [Va], devinette rédigée sous forme d'épigramme, invite le lecteur à calculer le nombre de têtes dans le troupeau du dieu du soleil. Appelons ce nombre x. Avec la notation algébrique dont ne disposaient pas les contemporains d'Archimède – mais qui gagne en efficacité ce qu'elle perd en poésie – le problème se ramène à résoudre l'équation

$$x^2 - 410286423278424 \cdot y^2 = 1$$

pour des valeurs entières positives des inconnues x et y. Cette équation possède une infinité de solutions, mais c'est loin d'être évident: dans la plus petite d'entre elles, x est un nombre de 206545 chiffres! Le cheptel monstrueux d'Archimède dépasse ainsi ce qu'on pourrait rencontrer dans la cosmologie la plus ambitieuse. Dans les mots du mathématicien Américain Amthor, qui publia la solution du problème d'Archimède au début du 20ème siècle, "une sphère du diamètre de la voie lactéee, que la lumière prend dix mille ans à traverser, ne contiendrait qu'une partie infime de ce troupeau, à

supposer même que la taille de chaque animal ne dépassât point celle de la plus minuscule bactérie".

La théorie des nombres se passionne aussi pour l'étude des nombres premiers – nombres qui ne peuvent s'écrire comme produits de nombres plus petits – et pour la factorisation de grands nombres en produit de nombres premiers. Pierre de Fermat, juriste Toulousain du 17ème siècle et mathématicien amateur de grand talent, avança la conjecture – aussi ambitieuse que fausse – que $2^{2^n}+1$ est toujours un nombre premier. C'est le cas quand n est plus petit que 5, puisque $3, 5, 17, 257$ et 65537 sont premiers, mais cela cesse déjà d'être vrai pour $2^{2^5}+1$, comme le démontra Euler en 1732:

$$2^{2^5}+1 = 4294967297 = 641 \times 6700417.$$

Les nombres de Fermat croissent d'ailleurs très rapidement, et ce n'est qu'en 1990 que le neuvième d'entre eux, $2^{2^9}+1$, un nombre de 154 chiffres, fut factorisé au terme d'un calcul auquel contribuèrent plus de 700 ordinateurs à travers le monde travaillant en parallèle et sans arrêt pendant près de quatre mois [LLMP]. Aujourd'hui encore, les algorithmes les plus sophistiqués arrivent difficilement à bout des nombres de plus de 150 ou 200 chiffres, même sur les ordinateurs les plus puissants.

Absorbés dans la contemplation de nombres dont la taille dépasse de loin ce qui peut se rencontrer en physique, les arithméticiens ont-ils perdu tout contact avec le monde pratique? Les considérations esthétiques comptent certes pour beaucoup dans leurs recherches. Mais l'expérience enseigne que les belles mathématiques, d'où naissent des structures à la fois riches et élégantes, ont tôt fait de trouver des applications à des fins plus utilitaires.

Le problème de la factorisation est ainsi à la base d'un procédé d'encryption, employé couramment pour protéger les transactions sur l'internet: le fameux cryptosystème RSA à "clé publique". C'est un entier N de plusieurs centaines de chiffres qui fournit la clé permettant de composer et de transmettre des messages secrets. Mais pour décoder ces messages, il faut détenir la factorisation de N. L'interêt du procédé vient de ce qu'il semble impossible de factoriser N en un temps raisonnable. Le processus de codage fournit donc peu de renseignements sur le processus de décodage, et c'est pourquoi le premier peut être rendu public et accessible à tous, sans compromettre la sécurité du second. (cf. [St], ch. 2.)

Tout comme leurs collègues informaticiens ou cryptologues, les physiciens ont désormais de bonnes raisons pour ne plus confiner leur attention à des

nombres de la taille de la constante d'Avogadro. En effet, la mécanique quantique, théorie fondamentale qui décrit le comportement de la matière et des particules élémentaires, et se trouve donc à mille lieues en apparence du problème de la factorisation, vient de jeter sur ce problème une lumière surprenante. C'est le célèbre physicien Américain Richard Feynman qui a proposé de construire un ordinateur qui exploiterait les propriétés des particules élémentaires, telles que décrites par le modèle quantique, pour effectuer certains calculs avec une rapidité prodigieuse. Réussite la plus spectaculaire de la nouvelle science de l'informatique quantique, l'algorithme de Peter Shor permettrait la factorisation – impossible en pratique par des méthodes classiques – de nombres de plusieurs centaines de chiffres; en admettant qu'un ordinateur quantique puisse un jour être construit, ce qui pour l'instant semble présenter plus de barrières pratiques que théoriques. L'ordinateur quantique ferait le bonheur des disciples de Fermat et d'Euler, et provoquerait une révolution en informatique et en physique théorique, tout en plongeant la cryptologie dans le désarroi en rendant obsolète le cryptosystème RSA. (On peut s'attendre d'ailleurs à ce que ce désarroi ne soit que temporaire, grâce aux cryptosystèmes quantiques dont le mathématicien Québecois Gilles Brassard fut un des pionniers [BBE].) Le développement de l'informatique quantique représente certes un beau défi pour le nouveau millénaire. Gageons que les cryptologues, les informaticiens, les physiciens et les théoriciens des nombres sauront s'unir pour le relever!

References

[BBE] Bennett, C. H., Brassard, G. et Ekert, A. K., *Quantum cryptography*, Scientific American, October 1992, pp. 50 - 57.

[Ko1] Koblitz, Neal. Introduction to elliptic curves and modular forms. Second edition. Graduate Texts in Mathematics, **97**. Springer-Verlag, New York, 1993.

[Ko2] Koblitz, Neal. A course in number theory and cryptography. Second edition. Graduate Texts in Mathematics, **114**. Springer-Verlag, New York, 1994.

[LLMP] Lenstra, A. K.; Lenstra, H. W., Jr.; Manasse, M. S.; Pollard, J. M. *The factorization of the ninth Fermat number*. Math. Comp. **61** (1993), no. 203, 319–349.

[Sh] Shor, Peter W. *Quantum computing*. Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998). Doc. Math. 1998, Extra Vol. I, 467–486 (electronic).

[St] Stewart, Ian. From Here to Infinity: A Guide to Today's Mathematics. Oxford University Press, 1987.

[Va] Ilan Vardi, *Archimedes' Cattle Problem*, American Math. Monthly, vol **105**, No. 4, 1998, 305–319.