NOTE D'ECOUTE

Les nombres premiers

par François Jaboeuf (Séminaire de l'U.P.S.)

La conférence de François Jaboeuf fut si dense et riche d'informations que je ne peux n'en donner qu'un compte-rendu partiel. En particulier je ne reprendrai pas les exemples numériques qui éclairaient agréablement les questions ou les résultats énoncés. L'importance de l'étude des nombres premiers tient à leur utilité dans divers domaines des mathématiques, et en particulier dans un usage récent en cryptographie ou théorie du codage qui développe depuis une vingtaine d'années la recherche de très grands nombres premiers ou de décomposition en facteurs premiers de très grands nombres. Les nombres premiers sont importants pour la théorie des nombres elle-même, car ils servent à construire tous les autres nombres, sans être eux-mêmes constructibles à partir d'autres. Le résultat a été énoncé par Gauss en 1801: "Tout nombre entier (différent de 0 et de 1) se décompose de façon unique en un produit de nombres premiers". Il est quasiment déjà acquis par Euclide au IIIème siècle avant J.C., comme en témoignent les propositions 30, 31 et 32 du 7ème livre des *Eléments*.

La première question posée dans la conférence fut celle de **la reconnaissance des nombres premiers**. Eratosthène, contemporain d'Euclide, a proposé son célèbre crible qui permet de séparer les nombres premiers de ceux qui ne le sont pas. Son procédé nous a été transmis par un néo-pythagoricien du IIème siècle après J.C., Nicomaque de Gérase. L'usage du crible d'Erathostène n'est pas commode pour les tester de grands nombres. Tester tous les diviseurs potentiels inférieurs au nombre n étudié serait inutilement long, il suffit de chercher si n admet un diviseur premier inférieur ou égal à $\sqrt{n}$, procédé encore simplifié si on remarque que les nombres premiers supérieurs à 4 sont tous de la forme $6k \pm 1$.

Un autre procédé, qui a l'avantage de ne pas nécessiter de division, utile pour reconnaître un nombre ayant deux diviseurs proches (donc proches de $\sqrt{n}$), est l'algorithme de Fermat. Il est fondé sur la propriété que tout nombre impair n est différence de deux carrés ($n = x^2 - y^2$), et il y a unicité du couple (x,y) si et seulement si n est premier. L'algorithme consiste à tester si $x^2 - n$ est un carré, pour tous les entiers x consécutifs supérieurs à $\sqrt{n}$; si l'algorithme ne s'arrête que pour $x = \frac{n+1}{2}$, n est premier.

Ces méthodes sont malheureusement inopérantes pour les très grands nombres. Pour établir par exemple que $2^{216091} - 1$ (le plus grand nombre premier actuellement connu et qui s'écrit avec 65050 chiffres) est premier, il faudrait 10 000 millions d'années de calcul d'un ordinateur parmi les plus puissants à l'heure actuelle. A la fin de sa conférence, F. Jaboeuf a signalé d'autres tests. L'un d'eux est basé sur le petit théorème de Fermat (tout nombre premier p ne divisant pas a divise $a^{p-1} - 1$), dont la réciproque n'est malheureusement pas vraie. On a pu améliorer le résultat de Fermat sous la forme: n est premier si et seulement si il existe un entier a , compris entre 2 et $n-1$, tel que $a^{n-1} \equiv 1 \mod (n)$ et si , pour tout diviseur premier p de $n-1$, $a^{(n-1)/p} \equiv 1 \mod(n)$, ce qui a permis à Robien de proposer en 1980 un test probabiliste pour reconnaître si un nombre n est premier. En testant aléatoirement k nombres a compris entre 2 et $n-1$, on peut , si tous les nombres vérifient la condition, affirmer avec un risque d'erreur inférieur à 4^{-k}, que n est premier. Pour de grands nombres la fiabilité du résultat est meilleure que celle des ordinateurs.

La deuxième question abordée fut celle-ci: **La suite des nombres premiers est-elle illimitée?** Cette question a déjà été résolue par Euclide, à la proposition 20 du 9ème livre des *Eléments* . Il montre, dans une démonstration exemplaire, qu'on peut toujours toujours construire un nombre premier plus grand que tous les nombres premiers d'une famille (finie) de nombres premiers: le produit des nombres de la famille augmenté de l'unité est premier ou bien admet un diviseur premier qui n'est pas dans la famille initiale. Une autre démonstration de ce résultat est donnée par Euler en 1768, qui fait intervenir de façon téméraire l'infini en acte, et qui mêle analyse et théorie des nombres, puisqu'elle utilise le développement en série de $ln \frac{1}{1-x}$ pour $x = 1$.

La troisième question fut celle de **la répartition des nombres premiers dans l'ensemble des entiers.** Sont-ils régulièrement répartis, dispersés, concentrés sur de petits intervalles? A propos des nombres premiers jumeaux (dont la différence est 2, comme 5 et 7), F. Jaboeuf a signalé que la conjecture de Goldbach, qui fit l'objet du 8ème problème de Hilbert reste ouverte: y a-t-il ou non une infinité de nombres premiers jumeaux? Legendre affirma en 1785 qu'une progression arithmétique dont le premier terme et la raison sont premiers entre eux contient une infinité de nombres premiers. On peut aussi trouver un intervalle d'entiers arbitrairement grand ne contenant aucun nombre premier, par exemple l'intervalle $[n!+2 ; n!+n]$ ne contient aucun nombre premier.

Legendre, puis Gauss, au 19ème siècle, ont proposé des formules empiriques donnant une approximation du nombre $\pi(x)$ des nombres premiers inférieurs à x .

Pour Legendre , $\pi(x) \simeq \frac{x}{\ln x - 1,08366}$. Pour Gauss, $\pi(x) \simeq \int_2^x \frac{du}{\ln u}$.

En 1896, Hadamard et La Vallée-Poussin démontrent que $\pi(n)$ est équivalent à $\frac{n}{\ln n}$ et on peut en déduire la loi de raréfaction des nombres premiers lorsque n tend vers l'infini.

Une quatrième question est celle d'**une formule qui donnerait tous les nombres premiers**, quête longtemps déçue. Aucun polynôme P(x) ne donne que des nombres premiers pour x décrivant l'ensemble des entiers. Des formules génératrices des nombres premiers ont cependant été récemment découvertes, dont l'intérêt est plus théorique que pratique.

F. Jaboeuf nous a également parlé des nombres de Fermat (de la forme $2^{2^n} + 1$) , que Fermat pensait premiers. On conjecture actuellement que ne sont premiers que les nombres de Fermat obtenus pour n inférieur ou égal à 4. Il nous a parlé des nombres de Mersenne (de la forme $2^n - 1$), qui ne sont pas tous premiers mais qui permettent de construire de grands nombres premiers. Le test de Lucas-Lehmer, spécifique aux nombres de Mersenne, a été mis au point par Lehmer en 1930. C'est lui qui a permis de découvrir le plus grand nombre premier actuellement connu.

Signalons que François Jaboeuf a écrit un chapitre consacré aux nombres premiers dans un ouvrage collectif de la commission inter-IREM d'épistémologie et d'histoire des mathématiques à paraître aux éditions Ellipses, intitulé "Histoires de Problèmes, Histoire des Mathématiques".

Michèle Grégoire