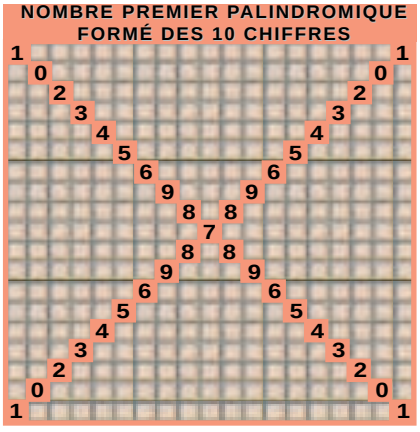

Les chasseurs de nombres premiers

JEAN-PAUL DELAHAYE

Nuit et jour, des centaines d'ordinateurs recherchent éperdument des nombres premiers.

Dans le zoo des nombres, les mathématiciens ont identifié, il y a plus de deux mille ans, une espèce remarquable, les nombres premiers (comme 2, 3, 5, 7, 11, ...) qui ne sont multiples exacts que de 1 et d'eux-mêmes. Ces nombres sont aux entiers ce que les éléments sont aux composés chimiques, car tout nombre entier se décompose de façon unique en produit de facteurs premiers. Exemple : $440 = 2 \times 2 \times 2 \times 5 \times 11$.

L'esprit de sérieux s'est emparé du sujet, et des milliers de pages de mathématiques difficiles, voire très difficiles, ont été écrites sur cette espèce numérique qui ne sera jamais en voie d'extinction puisqu'elle est infinie et que, de toute façon, lorsqu'un nombre est premier, rien ne peut changer sa nature !

Les universitaires sont obsessionnellement attachés à la répartition des nombres premiers (quelle est la proportion moyenne des nombres premiers parmi les nombres inférieurs à *n*?) ; ils s'y cassent le nez depuis plus de cent ans (la conjecture de Riemann, qui donnerait des informations précises de répartition échappe obstinément à toutes les tentatives de preuve). Parallèlement, une secte d'amateurs est restée fidèle à la tradition des pythagoriciens qui furent sans doute les premiers à définir et à prêter attention aux nombres premiers, et à y chercher émerveillements et amusements.

Les membres pacifiques et tranquilles de cette secte examinent les sous-espèces de nombres premiers, mènent toutes sortes de calculs, lancent des défis sans cesse renouvelés qui résistent ou tombent, mais sont alors reformulés en défis plus forts ou plus absurdes. Le tout constitue un jeu à l'échelle planétaire qui s'épanouit sur Internet. Ces zoologues mathématiciens se sont particulièrement intéressés aux nombres premiers *repunits* et aux nombres premiers palindromes.

Les repunits

Les *repunits* sont des nombres constitués d'une chaîne de 1. Le nombre 11 est premier. En revanche, le nombre 111 ne l'est pas, car $111 = 3 \times 37$. De même, quatre "1" consécutifs ou cinq "1" ne constituent pas des nombres premiers : $1111 = 11 \times 101$ et $11111 = 41 \times 271$. Plus loin, 11...1 (19 fois le "1") est premier comme l'est 11...1 (23 fois le "1"). D'où la question : quels sont les *repunits* premiers ?

Cette question est loin d'être simple, et personne aujourd'hui ne connaît de règles simples permettant de savoir systématiquement et rapidement quels sont les *repunits* premiers et quels sont les *repunits* composés. Notre ignorance n'est cependant pas complète, car on a découvert quelques propriétés des *repunits*.

– Pour être premier, un *repunit* doit nécessairement comporter un nombre premier de "1". En effet, si *m* divise *n* alors 11...1 (*m* fois) divise 11...1 (*n* fois). On le démontre en généralisant l'égalité $111111111111 = 1111 \times 100010001$ (ce qui est facile).

– Un nombre *repunit* ne peut être ni un carré (comme $25 = 5 \times 5$), ni un cube (comme $27 = 3 \times 3 \times 3$), ni une puissance cinquième (comme $32 = 2 \times 2 \times 2 \times 2 \times 2$). Les deux derniers résultats sont récents, et nul ne sait ce qui se passe pour les puissances autres que les multiples de 2, 3 et 5.

Les *repunits* de petites tailles (moins de 30 000 chiffres) susceptibles d'être premiers ont été étudiés soigneusement. On peut résumer ce qu'on sait en quelques mots :

– 11...1 (*n* fois le "1") est un nombre premier pour $n = 2, 19, 23, 317$ (découvert par Hugh Williams en 1978), 1031 (découvert par Hugh Williams et Harvey Dubner en 1986).

– Aucune autre valeur de *n* inférieure à 30 000 ne donne de *repunits* premiers. Au-delà de 30 000, les calculs deviennent trop longs, et l'on ignore donc ce qui s'y passe, comme d'ailleurs on ignore si l'espèce des *repunits* premiers est infinie.

1. REPUNITS EN BASE 2 ET NOMBRES DE MERSENNE

En base 2, les *repunits* sont de la forme $2^n - 1$. Ces nombres premiers sont dénommés les nombres premiers de Mersenne, en l'honneur du père Mersenne, qui les étudia en 1644.

Ces nombres sont particulièrement intéressants, car on connaît une méthode très efficace pour en tester la primalité. Le test de Lucas-Lehmer est basé sur le résultat suivant : $2^p - 1$ est premier si et seulement si $2^p - 1$ divise $S(p - 1)$, où $S(1) = 4$ et $S(n + 1) = S(n)^2 - 2$.

Grâce à ce test, le plus grand nombre premier connu est un nombre de Mersenne. Il s'agit de $2^{3021377} - 1$ (découvert en 1998 par Clarkson, Woltman et Kurowki), qui comporte 909 526 chiffres. On espère trouver un nombre premier de un million de chiffres avant l'an 2000.

On connaît aujourd'hui 37 nombres premiers de Mersenne, qui sont ceux correspondant aux exposants: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377. On ne sait prouver que les nombres de Mersenne premiers sont en nombre infini, ni que les nombres de Mersenne composés ayant un exposant premier sont en nombre infini.