Certains travaux du mathématicien Holey dans les années 1960, liant la conjecture de Artin à une autre conjecture célèbre (la conjecture généralisée de Riemann), rendent très probable qu'il y a une infinité de nombres premiers longs dans toute base fixée.

En base 2, la proportion d'entiers premiers longs semble être exactement la même qu'en base 10. En revanche, pour d'autres bases, les choses sont plus compliquées, et d'autres conjectures ont été formulées. Par exemple, en base 8, on pense que la proportion de nombres premiers longs est $3C/5$ (où C est la constante de Artin).

6. FACTORISATION DES $10^1 - 1$

$10^1 - 1 = 9 = 3^2$
$10^2 - 1 = 99 = 3^2\ 11$
$10^3 - 1 = 999 = 3^3\ 37$
$10^4 - 1 = 9999 = 3^2\ 11\ 101$
$10^5 - 1 = 99999 = 3^2\ 41\ 271$
$10^6 - 1 = 999999 = 3^3\ 7\ 11\ 13\ 37$
$10^7 - 1 = 9999999 = 3^2\ 239\ 4649$
$10^8 - 1 = 99999999 = 3^2\ 11\ 73\ 101\ 137$
$10^9 - 1 = 999999999 = 3^4\ 37\ 333667$
$10^{10} - 1 = 9999999999 = 3^2\ 11\ 41\ 271\ 9091$
$10^{11} - 1 = 99999999999 = 3^2\ 513239\ 21649$
$10^{12} - 1 = 999999999999 = 3^3\ 7\ 11\ 13\ 37\ 101\ 9901$
$10^{13} - 1 = 9999999999999 = 3^2\ 53\ 79\ 265371653$
$10^{14} - 1 = 99999999999999 = 3^2\ 11\ 239\ 4649\ 909091$
$10^{15} - 1 = 999999999999999 = 3^3\ 31\ 37\ 41\ 271\ 2906161$
$10^{16} - 1 = 9999999999999999 = 3^2\ 11\ 17\ 73\ 101\ 137\ 5882353$
$10^{17} - 1 = 99999999999999999 = 3^2\ 5363222357\ 2071723$
$10^{18} - 1 = 999999999999999999 = 3^4\ 7\ 11\ 13\ 19\ 37\ 333667\ 52579$
$10^{19} - 1 = 9999999999999999999 = 3^2\ 1111111111111111111$
$10^{20} - 1 = 99999999999999999999 = 3^2\ 11\ 41\ 101\ 271\ 27961\ 9091\ 3541$

Lorsque p est un nombre premier, la longueur de la période de $1/p$ est donnée par la ligne où il apparaît la première fois dans ce tableau. La longueur de la période de 1/11 est 2, car 11 apparaît dès la deuxième ligne. La longueur de la période de 1/13 est 6, car 13 n'apparaît qu'à la ligne 6.

7. NOMBRES PREMIERS LONGS ET CONSTANTE DE ARTIN

Les nombres premiers longs sont, par définition, les nombres premiers p tels que l'écriture de $1/p$ est de période maximale possible $p - 1$.
Le nombre 7 est le plus petit nombre premier long.
Parmi les 303 nombres premiers inférieurs à 2 000, il y en a 116 qui sont des nombres premiers longs en base 10. Ce sont :

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593, 619, 647, 659, 701, 709, 727, 743, 811, 821, 823, 857, 863, 887, 937, 941, 953, 971, 977, 983, 1019, 1021, 1033, 1051, 1063, 1069, 1087, 1091, 1097, 1103, 1109, 1153, 1171, 1181, 1193, 1217, 1223, 1229, 1259, 1291, 1297, 1301, 1303, 1327, 1367, 1381, 1429, 1433, 1447, 1487, 1531, 1543, 1549, 1553, 1567, 1571, 1579, 1583, 1607, 1619, 1621, 1663, 1697, 1709, 1741, 1777, 1783, 1789, 1811, 1823, 1847, 1861, 1873, 1913, 1949, 1979

La constante de Artin est le rapport limite de la proportion de nombres premiers longs sur le nombre de nombres premiers. On la note C, et elle vaut pour 303 nombres premiers : 116/303 = 0,38283828
Une conjecture de Artin stipule que :
$C = (1/2)\ (5/6)\ (19/20)\ (41/42)\ (109/110)\ \ldots = 0{,}3739558136\ldots$
(on prend le produit infini de toutes les fractions $(p^2 - p - 1)/(p^2 - p)$ pour p nombre premier 2, 3, 5, 7, 11, 13, etc.)
En fait, aujourd'hui on ne sait même pas démontrer qu'il y a une infinité de nombres premiers longs !

LES GÉNÉRATEURS EN $1/N$

Les propriétés des suites de chiffres qu'on trouve dans le développement de l'inverse d'un nombre premier long sont assez bien connues. Ces suites présentent des qualités de bon mélange et d'uniformité qui ont conduit à les utiliser comme suites de nombres pseudo-aléatoires. Regardez les chiffres du développement de 1/383 (383 est un nombre premier long en base 10). Ne semblent il pas quelconques?
1/383=0,[00261096605744125326370757180156657963446475195822454308093994778067885117493472584856396866840731070496083550913833812010443864229765013054830287206266318537859007832898172323759791122715404699738903394255874673629242819843420365535248041775456919060052219321148825065274151436031331592689295039164490861618798955613577023498694516971279373368146214099216710182767624020887728459 53].

Ces suites peuvent être utilisées en simulation, où l'on a besoin de suites pseudo-aléatoires. En revanche, les propriétés de ces suites étudiées par les mathématiciens L. Blum, M. Blum et M. Shub montrent que de telles suites sont *repérables* et ne doivent pas être utilisées en cryptographie : l'arithmétique ici nous donne à moindre coup du *hasard faible*, mais pas du *hasard moyen* (dont a besoin la cryptographie), ni bien sûr le véritable *hasard fort*, que seuls des mécanismes physiques peuvent engendrer.

N'est-il pas étonnant et merveilleux que, dans les fractions de l'école primaire, se cache un monde complexe et organisé où l'on découvre des séquences répétées, le théorème de Bézout, les nombres premiers longs, puis les suites pseudo-aléatoires et enfin des conjectures mystérieuses.

Jean-Paul DELAHAYE est directeur adjoint du Laboratoire d'informatique fondamentale de Lille du CNRS.

e-mail : delahaye @lifl.fr

J. H. CONWAY et R. GUY, *The Book of Numbers*, Copernicus, Springer, 1996.

E. KRANAKIS, *Primality and Cryptography*, John Wiley and Sons, 1986.

M. E. LINES, *A Number for Your Thoughts : Facts and Speculations about Numbers From Euclid to The Latest Computers*, Institute of Physics Publishing, Bristol, 1986, 1993.

Eric W. WEISSTEIN, *Decimal Expansion Maximal Period*, Treasure Troves 1997 http://www.astro.virginia.edu/~eww6n/math