

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).

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 ? $1/383=0, [002610966057441253263707571801566579634464751958224543080939947780678851174934725848563968668407310704960835091383812010443864229765013054830287206266318537859007832898172323759791122715404699738903394255874673629242819843342036553524804177545691906005221932114882506527415143603133159268929503916449086161879895561357702349869451697127937336814621409921671018276762402088772845953]$.

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 @lilf.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>

6. FACTORISATION DES $10^i - 1$

$10^1 - 1 = 9 = 3^2$
 $10^2 - 1 = 99 = 3^2 \cdot 11$
 $10^3 - 1 = 999 = 3^3 \cdot 37$
 $10^4 - 1 = 9999 = 3^2 \cdot 11 \cdot 101$
 $10^5 - 1 = 99999 = 3^2 \cdot 41 \cdot 271$
 $10^6 - 1 = 999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$
 $10^7 - 1 = 9999999 = 3^2 \cdot 239 \cdot 4649$
 $10^8 - 1 = 99999999 = 3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137$
 $10^9 - 1 = 999999999 = 3^4 \cdot 37 \cdot 333667$
 $10^{10} - 1 = 9999999999 = 3^2 \cdot 11 \cdot 41 \cdot 271 \cdot 9091$
 $10^{11} - 1 = 99999999999 = 3^2 \cdot 513239 \cdot 21649$
 $10^{12} - 1 = 999999999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$
 $10^{13} - 1 = 9999999999999 = 3^2 \cdot 53 \cdot 79 \cdot 265371653$
 $10^{14} - 1 = 99999999999999 = 3^2 \cdot 11 \cdot 239 \cdot 4649 \cdot 909091$
 $10^{15} - 1 = 999999999999999 = 3^3 \cdot 31 \cdot 37 \cdot 41 \cdot 271 \cdot 2906161$
 $10^{16} - 1 = 9999999999999999 = 3^2 \cdot 11 \cdot 17 \cdot 73 \cdot 101 \cdot 137 \cdot 5882353$
 $10^{17} - 1 = 99999999999999999 = 3^2 \cdot 5363222357 \cdot 2071723$
 $10^{18} - 1 = 999999999999999999 = 3^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 333667 \cdot 52579$
 $10^{19} - 1 = 9999999999999999999 = 3^2 \cdot 1111111111111111$
 $10^{20} - 1 = 99999999999999999999 = 3^2 \cdot 11 \cdot 41 \cdot 101 \cdot 271 \cdot 27961 \cdot 9091 \cdot 3541$

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 CONSTATE 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 :

$C = (1/2) (5/6) (19/20) (41/42) (109/110) \dots = 0,3739558136\dots$

(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.)

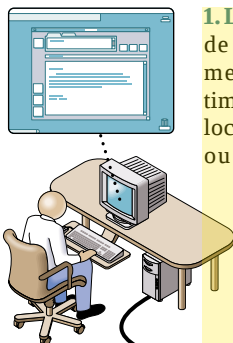
En fait, aujourd'hui on ne sait même pas démontrer qu'il y a une infinité de nombres premiers longs !

Le courrier électronique sur l'Internet

Des milliards de courriers électroniques (courriel ou mël, selon l'Académie) transitent sur le réseau Internet chaque année. L'envoi de lettres électroniques, soit d'un bureau à un bureau voisin ou d'un endroit du Globe à l'autre, est devenu si fréquent que ces envois remplacent le courrier postal ou le téléphone. Ce moyen de transmission universel n'est plus restreint aux seuls échanges de fichiers de texte, mais transporte de plus en plus souvent la voix, des télécopies, des images, des sons ou de la vidéo.

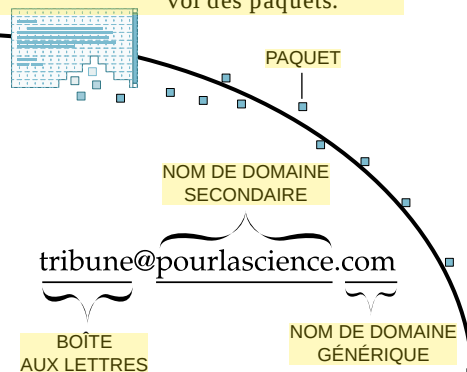
Un message arrive chez son destinataire quelques secondes après son envoi. Pour cette raison, le courrier électronique sur l'Internet a transformé notre façon de communiquer.

Paul HOFFMAN
Consortium du mail sur l'Internet.



1. LA PERSONNE QUI ENVOIE LE MESSAGE utilise un programme de courrier électronique baptisé *client*, pour construire un document qui peut inclure des annexes, comme des documents multimédias. Le programme *client* s'adresse à un serveur de messagerie local, un ordinateur qui est sur le réseau interne d'une société ou chez un fournisseur d'accès à l'Internet, lequel gère l'envoi. Sur cet ordinateur, un programme utilise un protocole de transmission (le plus souvent TCP, l'acronyme de *Transmission Control Protocol*, soit «protocole de contrôle de transmission») pour séparer le message en paquets et adjoindre à chaque paquet l'information qui concerne son envoi, par exemple, l'ordre d'envoi des paquets.

2. LES ADRESSES INTERNET attachées à chaque message sont de la forme «boîte_aux_lettres@nom_de_domaine», par exemple «tribune@pouurlascience.com». Le nom de domaine comprend un nom de domaine générique («.com») qui suit le nom de domaine secondaire («pouurlascience»). Un message est distribué à un groupe ou à un individu grâce à une boîte aux lettres («tribune»).



3. LE SERVEUR DE MESSAGERIE LOCAL convertit le nom de domaine du récipiendaire du message («pouurlascience.com») en une adresse numérique du protocole Internet (IP). Pour cela, il interroge les serveurs de nom de domaine (DNS) répartis sur le réseau. Par exemple, le serveur de messagerie peut demander d'abord à un serveur où se trouvent les serveurs qui contiennent des informations sur les noms de domaine «.com» (a). Ensuite, il interroge l'un de ses serveurs sur la localisation du serveur «pouurlascience.com» (b). Une requête finale au serveur de nom «pouurlascience.com» fournit l'adresse IP de l'ordinateur qui reçoit le courrier de pouurlascience.com, adresse qui est alors jointe à chaque paquet (c). Le serveur de messagerie envoie ensuite les paquets à des routeurs répartis sur l'Internet.

a OÙ EST LE SERVEUR .COM?

b OÙ EST LE SERVEUR DE NOM POURLASCIENCE.COM?

c OÙ EST LE SERVEUR DE MESSAGERIE POURLASCIENCE.COM?

SERVEUR DE NOM

ROUTEUR

SERVEUR DE MESSAGERIE POURLASCIENCE.COM

SERVEUR DE MESSAGERIE LOCAL

Jared Schneidman Design

4. LES ROUTEURS lisent l'adresse IP de chaque paquet et les relayent jusqu'à destination, par le chemin le plus efficace. En raison de l'encombrement des lignes de données, il n'est pas toujours plus rapide d'envoyer le paquet directement à son destinataire. Les différents paquets peuvent transiter par des chemins différents, relayés par une dizaine de routeurs, avant d'arriver à destination.

5. LE SERVEUR DE MESSAGERIE FINAL remplace les paquets reçus dans leur ordre initial, grâce aux instructions contenues dans chaque paquet, et stocke le message dans la boîte aux lettres du récipiendaire. Le programme de courrier électronique peut alors afficher le message.

