

développement périodique dès le départ, alors que, pour chaque dénominateur 3, 7, 9, 11 ou 13, non seulement la longueur de la période est constante, mais la période commence dès la virgule.

Effectuons une petite vérification sur $7/13 = 0,538461$

$$10^0 = 1 \bmod 13$$

$$10^1 = 10 \bmod 13$$

$$10^2 = 9 \bmod 13$$

$$10^3 = 12 \bmod 13$$

$$10^4 = 3 \bmod 13$$

$$10^5 = 4 \bmod 13$$

$$10^6 = 1 \bmod 13$$

Dans le cas de dénominateurs qui sont des nombres premiers autres que 2 et 5 (ce qui assure qu'ils n'ont de facteur commun ni avec leur numérateur ni avec 10), les choses sont particulièrement simples et nettes : si p est un nombre premier autre que 2 et 5, alors toutes les fractions non nulles simplifiées de dénominateur p ont un développement décimal qui est périodique dès la virgule, et dont la longueur de la période est le plus petit nombre j tel que $10^j - 1$ est divisible par p .

LES LONGUES PÉRIODES

Le raisonnement sur les restes successifs, quand on pose l'opération de division, montre que, pour un dénominateur d , la période est au plus $d - 1$ (les restes qui peuvent intervenir sont tous les nombres non nuls inférieurs à d). Si un nombre n'est pas premier, la période est inférieure à $d - 1$. En effet, deux cas sont possibles :
(i) un des restes successifs est un diviseur de d , on est ramené à une fraction simplifiée avec un dénominateur plus petit que d , et donc sa période est inférieure à d ;
(ii) aucun des restes successifs n'est un diviseur de d , alors il y en a moins que $d - 1$, et donc la période est inférieure à $d - 1$.

Pour les dénominateurs premiers, on constate avec 7, 17 ou 19 que la période peut-être $p - 1$ (voir la figure 4). D'autres considérations d'arithmétique montrent que, lorsque p est un nombre premier, la longueur des cycles est toujours un diviseur de $p - 1$. On le vérifie en regardant le tableau de la figure 5.

Reste un mystère. Pourquoi la période est-elle maximale, et égale à $(p - 1)$, pour certains nombres premiers appelés *nombres premiers longs* en base 10, et pas pour les autres ? Notons bien que la notion de *nombre premier long* dépend de la base de numération : un nombre peut être un premier long en base 10 et pas en base 2. C'est le cas, par exemple, pour 7 :

$1/7 = 0,142857142857142857\dots$ en base 10 période maximale 6

$1/7 = 0,001001001001\dots$ en base 2 période 3

On montre que, pour tout nombre premier, il existe une base B inférieure à p dans laquelle p est un nombre premier long.

Y a-t-il beaucoup de nombres premiers longs en base 10 (ou autres) ? La question est réellement difficile, et les mathématiciens n'ont pas même réussi à établir qu'il existe une infinité de nombres premiers longs en base 10. Or, ceux-ci ne sont pas très rares, puisqu'on en trouve

116 sur les 303 nombres premiers inférieurs à 2 000, ce qui fait une proportion de 38,28 pour cent.

On conjecture d'ailleurs que leur proportion est 37 pour cent. La conjecture a été formulée par le mathématicien allemand Emil Artin (1898-1962) et suggère que la proportion de nombres premiers longs soit C , la constante de Artin (voir la figure 7).

4. CYCLES DES FRACTIONS

Tableau des cycles pour les nombres premiers inférieurs à 50

3 : [3] [6]
7 : [142857]
11 : [09] [18] [26] [37] [45]
13 : [076923] [153846]
17 : [0588235294117647]
19 : [052631578947368421]
23 : [0434782608695652173913]
29 : [0344827586206896551724137931]
31 : [032258064516129] [096774193548387]
37 : [027] [054] [081] [135] [162] [189] [243] [297] [378] [459] [486] [567]
41 : [02439] [04878] [07317] [09756] [12195] [14634] [26829] [36585]
43 : [023255813953488372093] [046511627906976744186]
47 : [0425531914893617021276595744680851063829787234]

Tableau des longueurs des périodes pour les nombres premiers

Nombre premier (sauf 2 et 5) : n . Nombre de cycles : c . Longueur des cycles : l .

n	3	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137
c	2	1	5	2	1	1	1	1	2	12	8	2	1	4	1	1	2	2	9	6	2	2	1	25	3	2	1	1	3	1	17
l	16	2	6	16	18	22	28	15	3	5	21	46	13	58	60	33	35	8	13	41	44	96	4	34	53	108	112	42	130	8	

5. TROIS CURIOSITÉS NUMÉRIQUES

1) Lorsque p est un nombre premier et que la période de $1/p$ est paire, alors, en additionnant les deux moitiés de la période, on ne trouve que des 9. Ainsi pour 13, on a les périodes 076923 et 153846, et l'on vérifie que :
 $076 + 923 = 999$ $153 + 846 = 999$. Pour 19 on a une unique période :
052631578947368421, et l'on constate que :
 $052631579 + 947368421 = 999999999$

2) À partir de tout nombre premier long p , en prenant sa période, vous créez un entier qui, lorsque vous le multipliez par 2, 3, ..., $p - 1$, se redonne lui-même, à une permutation près de ses chiffres (un tel nombre est parfois appelé entier cyclique). Le cycle 142857 du nombre premier long 7 est le plus petit de ces entiers :
 $142857 \times 1 = 142857$ $142857 \times 2 = 285714$
 $142857 \times 3 = 428571$ $142857 \times 4 = 571428$
 $142857 \times 5 = 714285$ $142857 \times 6 = 857142$
De plus, en le multipliant par 7, on obtient 999999
Pour 17, vous trouverez l'entier cyclique 0588235294117647.

3) En prenant un nombre premier p dont la période est de longueur $(p - 1)/2$ (par exemple $p = 13$), vous obtenez une paire de nombres associés : en multipliant l'un ou l'autre par 1, 2, ..., $p - 1$, vous trouvez l'un ou l'autre à une permutation de chiffres près. Les deux cycles donnés par 13 fournissent les nombres associés 076923 et 153846
 $076923 \times 2 = 153846$ $153846 \times 2 = 307692$
 $076923 \times 3 = 230769$ $153846 \times 3 = 461538$
 $076923 \times 4 = 307692$ $153846 \times 4 = 615384$
 $076923 \times 5 = 384615$ $153846 \times 5 = 769230$, etc...

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 !