Les fractions et leurs mystères

JEAN-PAUL DELAHAYE

Divisez, divisez, il en restera toujours quelque chose.

Les fractions nous sont familières? Erreur : nous les connaissons mal. Nous savons les simplifier 100/500 = 10/50 = 1/5, 12/18 = 6/9 = 2/3 (si le numérateur et le dénominateur sont divisibles par un même nombre entier, il faut effectuer la division, et cela jusqu'à ce qu'il n'y ait plus de facteurs communs, excepté 1).

Nous savons faire des divisions 1/5 = 0,2 et 2/3 = 0,666666… Là commencent les ennuis : la division ne tombe pas toujours juste, ce qui conduit à des suites infinies de décimales qu'on ne peut pas écrire toutes!

Cela est fort intéressant et peut nous entraîner très loin, y compris dans des problèmes encore non résolus. Commençons par les fractions au développement décimal fini. Quelles sont-elles?

Votre expérience vous l'a peut-être déjà fait deviner : les fractions ayant un développement décimal fini sont celles dont (une fois simplifiées) le dénominateur est un produit de 2 et/ou de 5, autrement dit de la forme $2^i 5^j$. Les fractions 9/16 = 0,5625, 17/250 = 0,068, 230/1250 = 0,184 ont une écriture décimale finie, car $16 = 2 \times 2 \times 2 \times 2$ $250 = 2\times5\times5\times5$, $1250 = 2\times5\times5\times5\times5$.

Les nombres qui ont une écriture décimale finie sont bien sûr ceux qui, lorsqu'on les multiplie par une puissance de 10 assez grande, donnent des entiers : 0,23432 multiplié par 10^5 donne 23 432.

Pour cela, il faut que le dénominateur soit composé uniquement de diviseurs de 10, c'est-à-dire un produit de 2 et de 5. Une fraction s'écrit de manière finie en base 10 si, après simplification, le dénominateur est de la forme $2^i 5^j$. Le nombre exact de décimales est le plus grand des deux entiers i et j. Si le dénominateur contient un autre facteur, alors l'écriture décimale est infinie : 5/12 = 0,41666666..., 3/11 = 0,272727… 2/9 = 0,222222… etc.

Et dans une autre base de numération? Une fraction simplifiée s'écrit de manière finie en base B si et seulement si tout facteur premier du dénominateur est aussi un facteur premier de la base B. Par exemple, 2/5 en base 3, s'écrit : 0,101210210210210… Le développement est infini, car 5 n'est pas un facteur premier de 3. En base 9, 16/27 s'écrit : 0,53. C'est fini, car 27 n'a qu'un facteur premier : 3, qui est aussi un facteur premier de 9.

Des rappels d'arithmétique sont proposés dans la figure 1, et la méthode pour écrire un nombre entier ou réel en base B est expliquée à la figure 2.

Les développements infinis que nous avons écrits nous ont montré que l'écriture des fractions, lorsqu'elle n'était pas finie, était répétitive. Quelle est la période de cette répétition?

1. SOUVENIRS D'ARITHMÉTIQUE

L'arithmétique n'est plus guère enseignée et peut-être avez-vous oublié ses merveilles (qui sont utiles dans le texte).

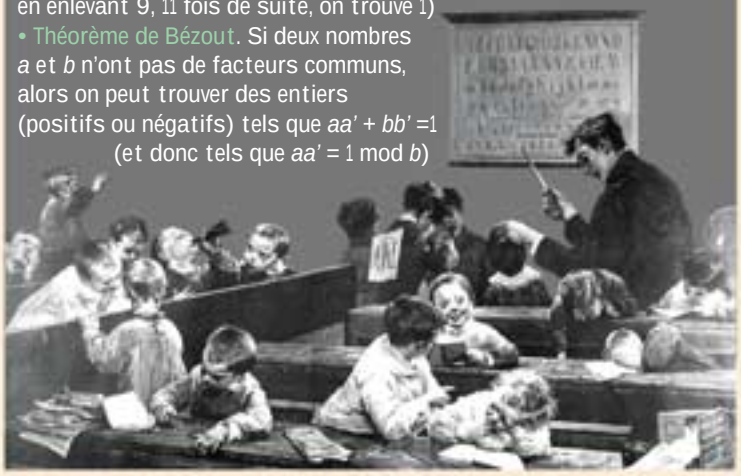
• Nombre premier : nombre divisible seulement par 1 et lui-même. Exemples 2, 3, 5, 7, 11, 13.
Le nombre 9 n'est pas premier, car divisible par 3.

• Facteurs premiers : tout nombre entier s'écrit comme produit de facteurs premiers d'une seule façon : sa décomposition en facteurs premiers. Exemples : 100 = 2 x 2 x 5 x 5, 122 = 2 x 61, 99 = 3 x 3 x 11.

• Un nombre est un carré si et seulement si sa décomposition en facteurs premiers ne comporte que des exposants pairs.
Exemple : $400 = 20^2 = 2^4 5^2$

• Arithmétique modulaire ou arithmétique modulo n. On compte comme avec les entiers, mais on soustrait ou on ajoute n autant de fois que nécessaire pour toujours se ramener à des nombres entre 0 et n - 1. Exemple : 12 = 3 mod 9 100 = 1 mod 9 (car 100 = 11 x 9 + 1 ; donc, en enlevant 9, 11 fois de suite, on trouve 1)

• Théorème de Bézout. Si deux nombres a et b n'ont pas de facteurs communs, alors on peut trouver des entiers (positifs ou négatifs) tels que $aa' + bb' = 1$ (et donc tels que $aa' = 1$ mod b)



Musée d'Histoire de l'Éducation

Faisons quelques tests :

7/33 = 0,21212121212121212121…

7/13 = 0,538461538461538461… (538461 se répète toujours)

Le phénomène n'est pas propre à la base 10. En base 3 : 1/2 = 0,111111…, 1/5 = 0,012012012012012… : toutes les fractions ont un développement en base 10 (ou autres) qui finit par se répéter, et réciproquement, si un nombre est périodique dans une base, c'est un rapport de deux entiers (et il est donc périodique dans toute base).

LES NOMBRES PÉRIODIQUES

Les nombres ayant un développement fini peuvent être vus comme des nombres ayant un développement périodique de période de longueur nulle. Nous adopterons ce point de vue quand nous parlerons de nombres périodiques. Nous adopterons aussi la notation 12,35[47] pour représenter le nombre périodique 12,3547474747… dont la séquence 47 se répète après le début 12,35.

Quelle est la fraction qui correspond au développement décimal périodique général :$a_1a_2…a_n$, $b_1b_2…b_m$ $[c_1c_2…c_p]$, n chiffres devant la virgule, puis m chiffres, puis une partie de p chiffres qui se répètent sans cesse ? Le calcul montre que c'est la fraction :

$a_1…a_n\, b_1…b_m/10^m + c_1… c_p/10^m\,(10^p – 1)$.

Par exemple : 12,3547474747… = 12,35[47] = 1235 /100 + 47/9900 = 30578/2475

463,124558642642642642… = 463,124558[642] = 463124558/1000000 + 642/999000000 = 38555119507/83250000

Dans le cas d'une base B quelconque, le résultat est bien sûr obtenu en remplaçant 10 par la base B dans la formule ci-dessus.

Le fait est évident : lorsqu'on effectue une division, on finit toujours par retomber sur un reste obtenu précédemment (ce qui signifie que le quotient est périodique). Cela démontre que les fractions s'écrivent avec un développement périodique et que ce sont les seuls nombres ainsi : «être une fraction» est parfaitement équivalent à «avoir des chiffres périodiques».

On en déduit un résultat amusant d'algèbre infinie : si vous faites la somme, la multiplication ou la division de deux nombres périodiques (ce qui en théorie prendrait un temps infini, mais les mathématiciens ne s'arrêtent pas à de tels détails), le résultat est un développement périodique. Par exemple, si vous divisez l'un par l'autre deux nombres dont le développement est périodique, vous calculez le développement d'une fraction de fractions $(a/b) / (c/d)$ qui est une fraction ad/bc et qui possède donc un développement périodique.

La caractérisation des nombres rationnels (les fractions) comme nombres ayant un développement périodique est indépendante de la base. Cela signifie que l'algorithme de changement de base décrit à la figure 2 préserve la périodicité (et la non-périodicité).

Aussi la périodicité est-elle une propriété qui se conserve bien : elle persiste quand on multiplie, quand on divise, quand on change de base de numération.

2. ÉCRITURE EN BASE B D'UN NOMBRE ENTIER

Six est entier vous le divisez par B, le reste vous indique son chiffre des unités en base B ; en recommençant avec le quotient, vous obtenez le chiffre suivant, etc.

Exemple : 123 en base 3

123 = 41 x 3 + 0 ..... donc 0
41 = 13 x 3 + 2 ..... donc 2
13 = 4 x 3 + 1 ..... donc 1
4 = 1 x 3 + 1 ..... donc 1
1 = 1 ..... donc 1

donc 123 s'écrit 1 1 1 2 0 en base 3.

Si x n'est pas entier. Convertissez d'abord la partie devant la virgule en base B. Pour le reste, voici le procédé : multipliez par B ; ce qui se trouve alors devant la virgule est le premier chiffre après la virgule. Multipliez ce qui reste par B ; ce qui se trouve alors devant la virgule est le second chiffre, etc.

Exemple : 123,541 en base 3

par conversion en base 3 de ce qui est devant la virgule 1 1 1 2 0 ;

il reste 0,541

0,541 multiplié par 3 cela donne 1,623 donc 1 ; il reste 0,623
0,623 multiplié par 3 cela donne 1,869 donc 1 ; il reste 0,869
0,869 multiplié par 3 cela donne 2,607 donc 2 ; il reste 0,669

donc le début est 11120,112

Si l'on poursuit on obtient :

11120,112121101111120200112211012222002221110110001212022010102120 2...

RACINES CARRÉES PÉRIODIQUES?

Pour la racine carrée, est-ce aussi simple ? Non. La racine carrée d'un nombre dont le développement est périodique peut ne pas être périodique et ne l'est même qu'exceptionnellement. La racine carrée N/D d'un nombre périodique n/d est périodique si et seulement si son numérateur et son dénominateur sont tous deux des carrés parfaits (comme 4, 9, 16, 25, etc.)

La démonstration de ce résultat tient en quelques mots. Supposons que n/d est simplifié, ainsi que N/D ; $n/d = N^2/D^2$, ce qui équivaut à $n D^2 = d N^2$ .Tout facteur premier p de n divise N^2 (car il ne peut pas diviser d puisque n/d a été simplifiée), donc il divise N^2 un nombre pair de fois, disons $2i$ fois (car, dans la décomposition en facteur premier d'un carré, chaque exposant est pair). Mais puisque les deux nombres $n D^2$ et $d N^2$ sont égaux, ils ont la même décomposition en facteurs premiers, et comme p ne peut pas apparaître dans celle de D (car p divise N et N/D a été supposée simplifiée), c'est que p^{2i} est présent dans la décomposition de n. Cela étant vrai pour tout facteur premier de n, n est un carré parfait. De même, d est un carré parfait. Il est donc nécessaire, pour qu'une racine carrée de fraction n/d soit périodique, que n et d soient des carrés parfaits. C'est bien sûr aussi suffisant.

Ni 2 ni 3 n'étant des carrés parfaits, le développement de leur racine carrée n'est pas périodique.

LES IRRATIONNELS ARTIFICIELS ET NATURELS

Si les nombres rationnels sont les nombres dont le développement est périodique, cela signifie deux choses intéressantes et, à nouveau, non triviales.

À chaque fois que l'on écrit un nombre dont les chiffres ne sont pas périodiques, comme 0,12112111211112111112 … (des séquences de 1 de plus en plus longues séparées par des 2), alors ce n'est pas une fraction : ne cherchez pas, aucun quotient de deux nombres entiers n'aura ce développement décimal !

Aussi, il existe des nombres qui ne sont pas des fractions (ce qui n'est pas si évident que cela). Ces nombres, qui ne sont pas quotients de deux entiers, s'appellent les irrationnels ; lorsque les Grecs découvrirent leur existence (à propos de racine de 2), ils en furent très éton-

3. PETITS CALCULS

1/3 = 0,3333333… = 0,[3]
2/3 = 0,6666666… = 0,[6]

1/6 = 0,166666… = 0,1[6]
2/6 = 0,333333… = 0,[3]
3/6 = 0,5
4/6 = 0,66666… = 0,[6]
5/6 = 0,83333… = 0,8[3]

1/7 = 0,142857142857… = 0,[142857]
2/7 = 0,285714285714… = 0,[285714]
3/7 = 0,428571428571… = 0,[428571]
4/7 = 0,571428571428… = 0,[571428]
5/7 = 0,714285714285… = 0,[714285]
6/7 = 0,857142857142… = 0,[857142]

1/9 = 0,111… = 0,[1]
2/9 = 0,222… = 0,[2]
3/9 = 0,333… = 0,[3]
4/9 = 0,444… = 0,[4]
5/9 = 0,555… = 0,[5]
6/9 = 0,666… = 0,[6]
7/9 = 0,777… = 0,[7]
8/9 = 0,888… = 0,[8]

1/11 = 0,090909… = 0,[09]
2/11 = 0,181818… = 0,[18]
3/11 = 0,272727… = 0,[27]
4/11 = 0,363636…= 0,[36]
5/11 = 0,454545… = 0,[45]
6/11 = 0,545454… = 0,[54]
7/11 = 0,636363… = 0,[63
8/11 = 0,727272… = 0,[72]
9/11 = 0,818181… = 0,[81]
10/11 = 0,909090… = 0,[90]

1/12 = 0,08333… = 0,08[3]
2/12 = 0,16666… = 0,1[6]
3/12 = 0,25
4/12 = 0,33333… = 0,[3]
5/12 = 0,41666… = 0,41[6]
6/12 = 0,5
7/12 = 0,58333… = 0,58[3]
8/12 = 0,66666…= 0,[6]
9/12 = 0,75
10/12 = 0,83333…= 0,8[3]
11/12 = 0,916666… = 0,91[6]

1/13 = 0,[076923]
2/13 = 0,[153846]
3/13 = 0,[230769]
4/1 3 = 0,[307692]
5/13 = 0,[384615]
6/13 = 0,[461538]
7/13 = 0,[538461]
8/13 = 0,[615384]
9/13 = 0,[692307]
10/13 = 0,[769230]
11/13 = 0,[846153]
12/13 = 0,[923076]

En base 2
1/9 = 0,000111000111… = 0,[000111]
3/9 = 0,01010101… = 0,[10]

nés. Tous les nombres suivants sont donc des irrationnels :
0,055000555500000555555000000000… (un 0, deux 5, trois 0, quatre 5, etc.)
0,488488884888888884… (un 4, deux 8, un 4, quatre 8, un 4, huit 8, etc.)
0,1234567891011121314… (nombre de Champernowne, constitué par la chaîne des entiers)
0,235791113… (les nombres premiers les uns derrière les autres).

Le second résultat un peu étonnant qui résulte de la caractérisation des rationnels est que, si l'on découvre qu'un nombre n'est pas rationnel, alors on sait aussitôt, sans rien avoir à calculer, que ses chiffres en base 10 (ou autre) ne sont pas périodiques. Puisque racine de deux n'est pas rationnel (2 n'est pas un quotient de deux carrés parfaits), ses décimales ne sont pas périodiques, de même que ses chiffres en binaire. Même si vous ne savez pas les calculer, même si vous n'en avez jamais calculé aucun, vous savez que, quelle que soit la base de numération utilisée, les chiffres de racine de deux ne sont pas périodiques. Le mathématicien est un magicien qui fait connaître l'infini.

PÉRIODES ÉGALES ET INÉGALES

Étudions maintenant les choses plus systématiquement. Le tableau de la figure 3 indique ce que donnent les divisions des nombres entre 0 et 1, avec un dénominateur inférieur ou égal à 13. Nous avons éliminé les dénominateurs 2, 4, 5, 8 et 10, car nous savons que toutes les fractions avec ces dénominateurs ont des développements finis en base 10.

Surprise : il semble que, pour un dénominateur donné, toutes les fractions qui ne se simplifient pas ont la même longueur de période. Pourrait-on le démontrer ? Oui, et cela va nous entraîner dans des raisonnements un peu plus compliqués que précédemment, mais tel est le prix à payer pour passer d'une constatation empirique à une certitude mathématique.

Pour une fraction n/d non simplifiable et de développement infini, nous supposerons n plus petit que d, ce qui revient à ne garder que la partie non entière des fractions. Pensons, pour notre démonstration, à l'opération de division comme nous la posons à l'école

– le premier reste est le reste de la division de $10n$ par d (car on a ajouté un zéro à n pour que d y soit au moins une fois),

– le second est celui de la division de $100n$ par d, etc.

Les restes ne peuvent pas être tous différents, car ils sont inférieurs à d, donc à un certain moment, on retombera sur un reste déjà obtenu à une étape antérieure i. Soit i et $i + j$ les plus petits des numéros d'étapes où se produit l'égalité de deux restes. Les nombres i et j sont ceux qui donnent l'endroit où commence la période et sa longueur. Dans le langage de l'arithmétique modulaire, n/d est périodique de période j à partir du chiffre i, si et seulement si i et j sont les plus petits entiers tels que : $n10^i = n10^{i+j} \bmod d$ (rappelons que «mod n» signifie qu'on ne garde d'un nombre que son reste après la division par n, ou, exprimé autrement, qu'on revient à zéro quand on arrive à n : 0 = 0 mod 3 ; 1 = 1 mod 3 ; 2 = 2 mod 3 ; 3 = 0 mod 3 ; 4 = 1 mod 3 ; 5 = 2 mod 3 ; 6 = 0 mod 3 ; etc.)

Exemple. Prenons 1/84. Si on pose la division, on trouve 1/84 = 0,01[190476], on constate que $i = 2$ et $j = 6$.

Vérifions cela par un calcul en arithmétique modulaire :

$10^0 = 1 \bmod 84$
$10^1 = 10 \bmod 84$
$10^2 = 100 = 16 \bmod 84$
$10^3 = 160 = 76 \bmod 84$
$10^4 = 760 = 4 \bmod 84$
$10^5 = 40 \bmod 84$
$10^6 = 400 = 64 \bmod 84$
$10^7 = 640 = 52 \bmod 84$
$10^8 = 520 = 16 \bmod 84$

On retombe sur 16 pour $i = 2$ (le début de la période) après $j = 6$ multiplications supplémentaires par 10.

Lorsque n et d n'ont pas de facteurs communs, l'égalité modulaire ci-dessus ne dépend pas de n, car il existe un nombre n' tel que $n\,n' = 1 \bmod d$ *(voir sur la figure 1 le théorème de Bézout)*, et on multiplie chaque côté de l'égalité modulaire par ce n', ce qui la simplifie en : $10^i = 10^{i+j} \bmod d$.

Cela est remarquable : toutes les fractions simplifiées ayant le même dénominateur ont un développement ayant la même période et cette période commence au même endroit après la virgule. Toutes les fractions ayant 12 comme dénominateur *(voir la figure 3)* et ne se simplifiant pas ont un développement dont la période est de longueur 1 qui commence au troisième chiffre après la virgule. De même, la période commune aux fractions de dénominateur 7 est constante (c'est 6).

Si on suppose maintenant que d n'est divisible ni par 2 ni par 5, alors on peut simplifier par 10^i, (car cela signifie que d et 10 sont premiers entre eux et donc, grâce au théorème de Bézout, qu'il existe un nombre k tel que $10k = 1$ modulo d). De $10^i = 10^{i+j} \bmod d$, on passe donc à $1 = 10^j \bmod d$, qui signifie que la période commence juste après la virgule et que la longueur de la période est le plus petit entier j tel que : $1 = 10^j \bmod d$ (c'est-à-dire tel que $10^j - 1$, soit un multiple de d).

À nouveau, cela explique pourquoi à la figure 4, pour 6, 12, 14, on n'a pas de

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… en base 10 période maximale 6

1/7 = 0,001001001001001… 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 : [0232558139534883720093] [0465116279069767441860]
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	1	6	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 multiplierez 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 x 1 = 142857 142857 x 2 = 285714
142857 x 3 = 428571 142857 x 4 = 571428
142857 x 5 = 714285 142857 x 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 x 2 = 153846 153846 x 2 = 307692
076923 x 3 = 230769 153846 x 3 = 461538
076923 x 4 = 307692 153846 x 4 = 615384
076923 x 5 = 384615 153846 x 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).

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,[00261096605744125326370757180156657963446475195822454308093994778067885117493472584856396866840731070496083550913833812010443864229765013054830287206266318537859007832898172323759791122715404699738903394255874673629242819843342036553524804177545691906005221932114882506527415143603133159268929503916449086161879895561357702349869451697127937336814621409921671018276762402088772845953].

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