Découverte des nombres premiers longs

1 Introduction

Depuis toujours j'ai été étonné par le résultat de la division par 7. Lorsqu'on divise les premiers nombres entiers entre eux, la division tombe souvent juste, et sinon, il y a un chiffre qui se répète jusqu'à l'infini.

1÷1=2÷2=3÷3=4÷4=5÷5=6÷6=7÷7=8÷8=9÷9=1
1÷2=2÷4=3÷6=4÷8=0,5
1÷4=2÷8=0,25
3÷4=6÷8=0,75
1÷5=0,2
2÷5=0,4
3÷5=0,6
4÷5=0,8
1÷8=0,25
3÷8=0,375
5÷8=0,625
7÷8=0,875

1÷3=2÷6=3÷9=0,333333....
2÷3=4÷6=6÷9=0,666666....
1÷6=0,166666....
5÷6=0,833333....
1÷9=0,111111....
2÷9=0,222222....
4÷9=0,444444....
5÷9=0,555555....
7÷9=0,777777....
8÷9=0,888888....

Voici pour les divisions entre nombres inférieurs à 10 avec un diviseur supérieur au dividende, mais voici celles qui ont longtemps suscité mon étonnement:

1÷7=0,142857142857142857....
2÷7=0,285714285714285714....
3÷7=0,428571428571428571....
4÷7=0,571428571428571428....
5÷7=0,714285714285714285....
6÷7=0,857142857142857142....

Non seulement il n'y a pas un mais 6 chiffres différents - 142857 - qui se répètent, mais aussi il y a exactement les mêmes chiffres qui se répètent dans toutes ces divisions! Je savais qu'au bout d'un moment les chiffres devaient se répéter car, dans la division, dès qu'un reste a déjà été obtenu, on est sûr que les chiffres du quotient vont se répéter. Et des restes différents, il y en avait forcément moins que le nombre, par définition du reste. Mais si 2÷7 donne la même séquence de chiffres que 1÷7 alors que c'est son double, c'est que 142857×2 vaut 285714, ou autrement dit, que les 6 chiffres subissent une permutation circulaire lors de la multiplication par 2. Et c'est la même chose pour la multiplication par 3, 4, 5 et 6 (et aussi 8, 9, 10, etc.), car en effet on a :

142857×2=285714
142857×3=428571
142857×4=571428
142857×5=714285
142857×6=857142
142857×7=999999

Ce dernier résultat surprend un peu car cela conduit au résultat étrange 7÷7=0,9999999.... alors qu'on s'attendrait plutôt à 7÷7=1. Mais cela s'explique assez simplement. Ce fut mon professeur de sixième qui me fit comprendre cela : il nous affirma que 1=0,99999... et pour nous en convaincre il nous écrivit toute une suite de soustractions qu'il nous fallait effectuer:

1–0,9= 1–0,99= 1–0,999= 1–0,999999= 1–0,9999999...=

Bien sûr, il nous bien fallu admettre que la dernière soustraction ne pouvait pas donner autre chose que 0,000000.... (le 1 final étant repoussé si loin - à l'infini - qu'il ne comptait vraiment pas pour grand-chose) et donc que tout nombre décimal pouvait s'écrire avec une suite infinie de 9 :

1=0,99999... 2,5=2,499999... 0,3=0,299999...

Pour en revenir à ce nombre 142857, il devait avoir bien d'autres propriétés cachées, comme par exemple celle-ci : 142857×14 devait valoir 1 999 998 puisque 14÷7=2=1,999999.... et que 14÷7=14×(1÷7)=14×(0,142857 142857 142857....) et donc, on pouvait écrire 1,99999... comme une addition de séquences de 1 999 998 mises bout à bout comme ça :

```
  1     9  9  9     9  9  8
+                   1     9  9  9     9  9  8
```

```
+                                                   1     9  9  9     9  9  8 ....
-----------------------------------------------------------------------------
  1     9  9  9     9  9  9     9  9  9     9  9  9     9  9  9     9  9  8 ....
```

Il fallait aussi que l'on obtienne 1 999 998 en additionnant 142857×10 et 142857×4, soit 1428570 et 571428. Et tous ces résultats "forcés" sont liés à notre exemple 14÷7=2, mais nous avons tout autant de sommes étonnantes avec 21÷7=3=2,9999999... (car alors c'est 2857140+142857 qui devrait valoir 2999997 et aussi 142857×21) ou avec toute une infinité d'autres résultats, tous parfaitement organisés :
2857140+1142857=3999996=142857×28 - 4285710+714285=4999995=142857×35 - etc.

2 Exploration

Je ne savais pas du tout si ce nombre 142857 était le seul à avoir toutes ces propriétés ou s'il en existait d'autres, obtenus en utilisant des diviseurs plus grands que 10. Je me mis donc à explorer l'ensemble des nombres entiers pour ce qui est de la division de 1 par ces nombres entiers, pensant trouver ensuite les permutations circulaires pour les autres dividendes que 1. Je calculais donc, chiffre par chiffre et à la main, car la calculatrice est vite limitée par son affichage d'une douzaine de chiffres seulement, les développements décimaux des inverses des entiers supérieurs à 9.

1÷10=0,1
1÷11=0,09090909....
1÷12=0,08333333....
1÷13=0,076923076923....
1÷14=0,07142857142857....
1÷15=0,06666666....
1÷16=0,0625
1÷17=0,0588235294117647 0588235294117647 ....
1÷18=0,0555555 ....
1÷19=0,0526315789473684 0526315789473684 ....
1÷20=0,05

Je n'avais pas fait un gros travail et déjà je voyais que la division par deux autres nombres premiers, 17 et 19 semblait posséder les mêmes propriétés que celle par 7. Diviser par 17 conduit à une séquence de 16 chiffres différents qui se répète jusqu'à l'infini et diviser par 19 en donne une de 18 chiffres. Ces séquences sont d'une longueur maximale si l'on considère la remarque précédente sur les restes qui doivent tous être différents. On trouve d'autres séquences relativement longues mais elles n'ont pas toujours cette longueur maximale (égale au nombre moins 1). Par exemple, la division par 13 donne 6 chiffres alors que la longueur maximale est 12, la division par 14 donne aussi 6 chiffres (les mêmes que la division par 7) pour une longueur maximale théorique de 13. Les nombres 7, 17 et 19 sont donc les représentants d'une famille de nombres, incluse semblait-il dans les nombres premiers, qui possèdent cette propriété remarquable de conduire à des séquences d'une longueur maximum. Je pensais que ces séquences ont toutes les propriétés étonnantes qui ont été détaillées plus haut pour 142857. Mais il me fallait tout de même tester s'il en allait bien de même pour les nouvelles que je venais d'obtenir : 0588235294117647 et 052631578947368421.
Tout d'abord, vérifions que les chiffres des multiples sont bien obtenus par permutation circulaire.

0588235294117647×2=1176470588235294	052631578947368421×2=105263157894736842
0588235294117647×3=1764705882352941	052631578947368421×3=157894736842105263
0588235294117647×4=2352941176470588	052631578947368421×4=210526315789473684
0588235294117647×5=2941176470588235	052631578947368421×5=263157894736842105
0588235294117647×6=3529411764705882	052631578947368421×6=315789473684210526
0588235294117647×7=4117647058823529	052631578947368421×7=368421052631578947
...	...
0588235294117647×16=9411764705882352	052631578947368421×18=947368421052631578
0588235294117647×17=9999999999999999	052631578947368421×19=999999999999999999

C'est fantastique! Mais les autres nombres premiers, même s'ils ne conduisent pas à des séquences

de longueur maximale, conduisent à des séquences qui ont des propriétés voisines. Par exemple la division par 13 conduit à deux séquences différentes de 6 chiffres 076923 et 153846, la première étant obtenue dans la division par 13 de 1, 3, 4, 9, 10 et 12 alors que la seconde est obtenue dans la division par 13 de 2, 5, 6, 7, 8 et 11. Les permutations circulaires s'effectuent en sautant d'une de ces séquences à l'autre:

076923×2=153846
076923×3=230769
076923×4=307692
076923×5=384615
076923×6=461538
076923×7=538461
076923×8=615384
076923×9=692307
076923×10=769230
076923×11=846153
076923×12=923076
076923×13=999999

Ces sauts d'une séquence à l'autre obéissent à une loi interne que j'ignore encore mais dont j'ai découvert un aspect en observant ces séquences de nombres 1, 3, 4, 9, 10 et 12 et 13 de 2, 5, 6, 7, 8 et 11 : elles ont en commun...leur somme, 39 dans les 2 cas! Et ce n'est pas un hasard comme j'ai pu m'en convaincre en prenant un autre nombre premier. En effet, dans la division par 11 on trouve 5 séquences de chiffres qui sont 09 (pour 1 et 10), 18 (pour 2 et 9), 27 (pour 3 et 8), 36 (pour 4 et 7) et 45 (pour 5 et 6), et la somme des dividendes vaut à chaque fois 11! Un autre nombre premier, le nombre 3, conduit à 2 séquences qui alternent : 3 et 6. Les autres nombres premiers rencontrés jusqu'ici sont 2 et 5, mais ceux-ci sont des exceptions car ils conduisent à des nombres décimaux, donc à des séquences de 0 ou de 9, ce qui est identique comme on l'a vu.

1÷2=0,5=0,4999999 1÷5=0,2=0,1999999 2÷5=0,4=0,3999999 etc.

Pousser plus loin l'investigation pour ce genre de nombres premiers me paraît prometteur, mais je m'écarte de mon sujet. Revenons donc à cette partie des nombre premiers qui conduit à des séquences maximales, dont 7, 17 et 19 sont les premiers représentants, et que j'appellerai désormais les nombre premiers longs (c'est le nom que la communauté mathématique leur donne). A leur propos, je voulais déjà disposer d'une liste plus longue et, pour cela, il me faudrait un petit programme qui effectue les divisions chiffre par chiffre et repère le moment où un reste a déjà été obtenu. Ce programme écrit, je trouvais alors la suite des nombres premiers longs 7, 17, 19, 23, 29, 47, 59, 61 et 97 pour ceux qui sont inférieurs à 100, ce qui représente environ le tiers des 26 nombres premiers de cet intervalle. Voici le début de la liste des nombres premierd, les longs étant en rouge :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 59, 61, 67, 71, 73, 79, 83, 89 et 97

Pour affiner la fréquence trouvée (9/25, soit 36%) je poussais mon programme un peu plus loin et trouvais 60 nombres premiers longs inférieurs à 1000 sur les 168 nombre premiers de cet intervalle, soit avec un ratio de 60/1608 une fréquence d'environ 35,7% qui semble indiquer une stabilité de cette valeur.

3 Changements de base

Lorsque je devins prof de maths, quelques années plus tard donc, je racontais un jour cette trouvaille à un collègue qui réfléchit d'abord puis me répondit que cette caractéristique devait vraisemblablement être liée à la base de numération employée (nous comptons en base 10 mais nous aurions pu tout aussi bien employer une autre base, par exemple la base 8 qui n'utilise que 8 chiffres, ou la base 2 qui n'en utilise que 2). Il me donna cet argument : en base 7 le nombre 7 s'écrit 10 et le nombre 7^2 s'écrit 100, les puissances de 7 remplaçant les puissances de 10 pour déterminer les valeurs des différentes positions de chiffres. De même pour les chiffres après la virgule, 7^{-1} c'est à dire 1÷7 s'écrit 0,1 ce qui fait de ce nombre l'équivalent d'un nombre décimal. Plus de séquence de 6 chiffres en base 7! En tout cas plus pour le quotient de 1 par 7. Je m'imaginais qu'il devait bien y avoir des nombres premiers longs en base 7 mais était-ce les mêmes qu'en base 10, excepté le nombre 7 qui visiblement ne l'était pas? Pour répondre à cette question, je me mis à effectuer à la main des divisions en base 7 (colonne de gauche) et, comme je n'étais pas habitué, je m'aidais des tables de multiplication en base 7 (colonne de droite).

```
1          | 5
1  0       | 0,12541...
   2  0
      4    0
           3  0
              1  0
                 2
                 ...
```

Table de 5 en base 7

5×0=0
5×1=5
5×2=13
5×3=21
5×4=26
5×5=34
5×6=42
5×10=50

1÷5=0,12541254...

Il y a une séquence de 4 chiffres qui se répète quand on divise par 5 en base 7 et donc 5 est un nombre premier long en base 7 (il ne l'est pas en base 10)

```
1          | 10
1  0       | 0,1
   0
```

1÷10=0,1

Quand on divise par 7 (qui s'écrit 10) en base 7 on obtient un nombre décimal et donc 7 n'est pas un nombre premier long en base 7 (il l'est en base 10)

```
1          | 3
1  0       | 0,22...
   1  0
      ...
2          | 3
2  0       | 0,44...
   2  0
      ...
```

Table de 3 en base 7

3×0=0
3×1=3
3×2=6
3×3=12
3×4=15
3×5=21
3×6=24
3×10=30

1÷3=0,22...

Il y a un seul chiffre qui se répète quand on divise par 3 en base 7 et donc 3 n'est pas un nombre premier long en base 7 (il ne l'est pas non plus en base 10)

En base 7 les nombres premiers 3 et 7 ne sont pas longs, par contre les nombres premiers 2, 5 et 11 sont longs. 2 est long car 1÷2=0,333... il y a 1 chiffre qui se répète et 11, qui s'écrit 14 en base 7, est long car 1÷14=0,043116235504... il y a 10 chiffres qui se répètent. Je fis aussi quelques multiplications en base 7 pour me persuader que les propriétés de permutation de chiffres pour les séquence longues se retrouvaient dans toutes les bases.

1254×2=2541
1254×3=4125
1254×4=5412
1254×5=6666 Ah oui! Le 6 en base 7 joue le rôle du 9 en base 10...

Pour aller plus loin dans mon exploration des nombres premiers il faut donc que je modifie mon programme afin qu'il convertisse les nombres dans la base de mon choix et qu'il effectue les divisions chiffre par chiffre dans cette base. J'obtins alors le tableau suivant qui se prolonge à volonté dans les deux directions.

	Bases														
Nombre	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2		L		L		L		L		L		L		L	
3	L			L			L			L			L		
5	L	L				L	L				L	L			
7		L		L					L		L				
11	L				L	L	L					L			

13	L				L	L				L			L	
17		L		L	L	L			L	L	L		L		
19	L	L							L			L	L	L	
23				L		L			L	L			L	L	
29	L	L					L		L	L			L	L	
31		L								L	L	L			
37	L			L								L		L	
41					L	L				L	L	L		L	
43		L		L							L				
47				L					L	L		L		L	
53	L	L		L			L				L		L		
59	L				L		L		L	L		L	L		
61	L				L	L			L						
67	L					L				L	L	L			
71						L				L		L			
73				L	L					L		L	L	L	
79		L			L	L									
83	L			L	L		L					L	L	L	
89		L				L						L	L	L	
97				L		L			L			L	L	L	

Aussitôt ce tableau rempli, de nouvelles propriétés m'apparaissent.

1. Propriété des colonnes: certaines bases n'ont pas de nombres premiers longs. La base 4 et la base 16 sont les premières bases dans ce cas. D'autres bases n'ont que le nombre 2 comme premier long. C'est le cas de la base 9 dans le tableau, mais on peut supposer qu'il s'agit des bases qui sont des carrés d'entier ($4=2^2$, $9=3^2$, $16=4^2$), et donc on peut supposer qu'il n'y a pas de premier long en base 4, 16, 36, 64, etc. et qu'il n'y en a qu'un en base 9, 25, 49, etc.

La répartition des nombres premiers longs dans les bases qui en contiennent est relativement homogène. Cela va de 7 à 15 sur 25 longs pour les 12 premières bases qui en contiennent, selon le récapitulatif suivant:

Bases	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
longs/25	12	11	0	12	9	13	7	1	9	13	8	15	11	12	0

Pour affiner ces valeurs nous avons poussé les calculs pour les 2 bases extrêmes : la base 8 qui contient le moins de longs et la base 13 qui en contient le plus.

	sur 25 prem.inf.à 100	sur 168 prem.inf.à 1000	sur 303 prem.inf.à 2000
base 8	7 soit 28%	39 soit 23,2%	70 soit 23,1%
base 13	15 soit 60%	69 soit 41,1%	115 soit 38%

S'il y a une atténuation avec le nombre, la variabilité semble se confirmer. Si l'on considère l'ensemble des bases possibles, il y a donc une grande variabilité du nombre de premiers longs (de 0 à une petite moitié), certaines bases sont donc plus "favorables" aux longs que d'autres.

2. Propriétés des lignes : Tous les nombres premiers sont longs dans une base ou dans une

autre, et ce, de façon assez homogène. Ainsi, pour les 15 premières bases de numération, les 25 premiers nombres premiers sont longs dans 3 à 7 bases selon le récapitulatif suivant:

Nombre	longs/15				
2	7	23	6	59	7
3	5	29	7	61	4
5	6	31	4	67	5
7	4	37	4	71	3
11	5	41	6	73	6
13	5	43	3	79	3
17	8	47	5	83	7
19	6	53	6	89	5
				97	6

Concernant la variabilité qui semble assez faible sur les lignes, j'observais que la 1ère ligne était une alternance de longs et de pas longs, que je note L-x. Pour la 2ème ligne c'était une succession de la séquence L-x-x, sur la 3ème ligne une succession de L-L-x-x-x. En fait chaque ligne possède une séquence qui se répète sur l'ensemble des bases, cette séquence ayant la longueur du nombre premier en jeu. Je pouvais alors facilement déterminer la fréquence exacte des bases pour lesquelles un nombre premier est long: il suffisait de disposer de la séquence dans son intégralité, ce que mon tableau me donne jusqu'au nombre premier 13, mais que je peux pousser facilement pour obtenir les séquences intrinsèques des 10 premiers nombres premiers. Ainsi j'obtiens le tableau suivant qui donne une moyenne de 38,2% de l'ensemble des bases:

2	L-x	1/2 soit 50%
3	L-x-x	1/3 soit 33%
5	L-L-x-x-x	2/5 soit 40%
7	x-L-x-L-x-x-x	2/7 soit 29%
11	L-x-x-x-L-L-L-x-x-x-x	4/11 soit 36%
13	L-x-x-x-L-L-x-x-x-L-x-x-x	4/13 soit 31%
17	x-L-x-L-L-L-x-x-L-L-L-x-L-x-x-x-x	8/17 soit 47%
19	L-L-x-x-x-x-x-x-L-x-x-L-L-L-x-x-x-x-x	6/19 soit 32%
23	x-x-x-L-x-L-x-x-L-L-x-x-L-L-x-L-x-L-L-L-x-x-x	10/23 soit 43%
29	L-L-x-x-x-x-L-x-L-L-x-x-L-L-x-x-L-L-x-L-L-x-x-x-x-x-L-L-x-x-x	12/29 soit 41%

4 Référence à la théorie

Si je voulais comprendre davantage le phénomène, il me faut l'aide de la communauté des mathématiciens qui a certainement déjà bien étudié la question et construit un ensemble cohérent de concepts et de théorèmes. Je fais un tour dans les bibliothèques de mon quartier et finis par tomber sur un livre de Jean-Paul Delahaye intitulé "Ces merveilleux nombres premiers" qui est un ouvrage de vulgarisation comportant un chapitre assez clair et facile d'accès sur la théorie qui m'intéresse et qui constitue un des développement de l'arithmétique modulaire[1]. J'y trouve la raison pour laquelle un nombre premier p est long dans une base b : il faut et il suffit que b^{p-1} soit la première puissance de b à être congrue à 1 modulo p, c'est-à-dire à être égal à un multiple de p plus 1. Par exemple, 7 est un nombre premier long en base 10 car 10^6 est la première puissance de 10 à être congrue à 1 modulo 7. Vérifions cela:

$10^1=10=3 \pmod 7$

$10^2=100=7\times14+2=2 \pmod 7$

$10^3=1000=7\times142+6=6 \pmod 7$ Pour simplifier les calculs, selon les propriétés de l'arithmétique modulaire, on peut directement calculer dans le modulo, par exemple ici, $10^3=10\times10^2=3\times2=6 \pmod$

1 Arithmétique inventée par Carl Friedrich Gauss (1777-1855) à 24 ans qui utilise les restes de la division euclidienne.

7), $10^4=10\times10^3=3\times6=4 \pmod 7$, $10^5=10\times10^4=3\times4=5 \pmod 7$ et $10^6=10\times10^5=3\times5=1 \pmod 7$

Je trouve donc bien ce qu'il faut, mais je reste un peu sur ma faim pour ce qui est de l'explication du phénomène. La condition nécessaire et suffisante fournie par la théorie me permit cependant de comprendre le phénomène de périodicité observée dans mon tableau et aussi l'absence de longs dans les bases 4, 9 ou 16. Commençons par cela, et plus particulièrement cherchons pourquoi, en base 4, il n'y a pas de premiers longs.

$4^1=0 \pmod 2$ or, il aurait fallu que $4^1=1 \pmod 2$ pour que 2 soit long en base 4

$4^1=1$ et $4^2=1 \pmod 3$ or, il aurait fallu que $4^1\neq1 \pmod 3$ pour que 3 soit long en base 4

$4^1=4$, $4^2=1$, $4^3=4$ et $4^4=1 \pmod 5$ or, il aurait fallu que $4^2\neq1 \pmod 5$ pour que 5 soit long en base 4

De même, il aurait fallu que $4^3\neq1 \pmod 7$ pour que 7 soit long en base 4 et que $4^5\neq1 \pmod{11}$ pour que 11 soit long en base 4, etc. Hormis donc pour 2, la cause de l'absence de longs en base 4 est due à une puissance de 4 congrue à 1, et comme $4=2^2$, cela revient à une puissance de 2 congrue à 1, voyons laquelle:

$4^1=2^2=1 \pmod 3$ $4^2=2^4=1 \pmod 5$ $4^3=2^6=1 \pmod 7$ $4^5=2^{10}=1 \pmod{11}$

$4^6=2^{12}=1 \pmod{13}$ $4^8=2^{16}=1 \pmod{17}$ $4^{11}=2^{22}=1 \pmod{23}$ etc.

Il s'agit donc toujours de 2^{p-1}, modulo p ce nombre est toujours congru à 1, et cela empêche l'existence de nombres premiers longs dans la base 4. Je me replonge un instant dans la théorie car cela n'est pas la condition nécessaire et suffisante, mais cela vient d'un autre résultat, intitulé "petit théorème de Fermat[2]" qui est une propriété des nombres premiers : si un nombre p est premier, alors, pour tout entier n non multiple de p, on a $n^{p-1}=1 \pmod p$. Ce théorème explique donc pourquoi, pour toute base b, on trouvait $b^{p-1}=1 \pmod p$ pour tous les nombres premiers p. C'est uniquement quand il y a une puissance de b inférieure à p-1 congrue à 1 modulo p que le nombre premier p n'est pas long en base b.

Comme tous les nombres premiers supérieurs à 2 sont impairs, p-1 sera toujours pair et donc pourra s'écrire $2\times p'$. Ainsi la condition $2^{p-1}=1 \pmod p$ qui caractérise les nombres premiers peut s'écrire $2^{2p'}=4^{p'}=1 \pmod p$ et comme $p'=(p-1)/2$ on a bien $p'<p$ pour tous les nombres premiers p supérieurs à 2, et donc p ne peut jamais être long en base 4. Ce raisonnement peut être étendu à toutes les bases qui sont des carrés d'entier. Mais pour le nombre premier 2, il en va autrement car $4^1=0 \pmod 2$ alors que $9^1=1 \pmod 2$, les nombres pairs sont congrus à 0 et les nombres impairs à 1. Or comme tous les carrés de nombres pairs sont pairs et tous les carrés de nombres impairs sont impairs, les bases comme 4, ou 16 n auront aucun premiers longs alors que celles comme 9 ou 25 en auront juste un.

Il doit se passer le même genre de phénomène avec les bases qui sont des cubes de nombres entiers, comme 8 par exemple qui est le cube de 2. Ceci expliquant sans doute la fréquence relativement faible des premiers longs dans cette base.

Comment la condition nécessaire et suffisante de la théorie explique le phénomène de périodicité du tableau? C'est très simple, car la condition est vraie modulo p. Regardons ce qui se passe pour le nombre premier 3, pour lequel on a observé la séquence L-x-x dans le tableau :

$2^1=1$ et $2^2=1 \pmod 3$ donc 3 est long en base 2

$3^1=0$ et $3^2=0 \pmod 3$ donc 3 n'est pas long en base 3

$4^1=1$ et $4^2=1 \pmod 3$ donc 3 n'est pas long en base 4

$5^1=2^1=1$ et $5^2=2^2=1 \pmod 3$ donc 3 est long en base 5

$6^1=3^1=0$ et $6^2=3^2=0 \pmod 3$ donc 3 n'est pas long en base 6

$7^1=4^1=1$ et $7^2=4^2=1 \pmod 3$ donc 3 n'est pas long en base 7

2 Pierre de Fermat (1601-1665) énonce ce théorème en 1640 mais il ne s'agit alors que d'une conjecture indémontrée.

etc.

La périodicité du tableau est donc une conséquence de la périodicité de la condition nécessaire et suffisante : ce qui est vrai pour une base b modulo p sera vrai pour les bases b+p, b+2p, etc. Finalement, pour savoir si un nombre premier p est long dans une base b, il suffit d'examiner la table des puissances du modulo p. Par exemple, dressons la table des puissances du modulo 5 qui nous renseignera sur la longueur des développements décimaux de 1÷5 dans les différentes bases :

a	a^1	a^2	a^3	a^4
1	**1**	**1**	**1**	**1**
2	2	4	3	**1**
3	3	4	2	**1**
4	4	**1**	4	**1**
5	0	0	0	0

En voyant cette table, on comprend que 5 sera un premier long en base 2 et 3, mais aussi, du fait de la périodicité de la table, en base 7 et 8 ou encore 12 et 13, etc. Par contre 5 ne sera pas long dans les bases 4, 5 et 6 et aussi dans les bases, 9, 10 et 11 ou encore 14, 15 et 16, etc.

Pour résumer, il y a deux causes pour qu'un nombre premier ne soit pas long en base b:

1. qu'on ait $b^1=b^2=....=b^{p-1}=0$ (mod p). Cette condition est vérifiée lorsque b=p, par exemple $5^1=5^2=....=5^4=0$ (mod 5), ce qui explique que 5 n'est pas premier long en base 5, ou lorsque b est un multiple de p comme par exemple $10^1=10^2=....=10^4=0$ (mod 5), ce qui explique que 5 n'est pas premier long en base 10 .
2. qu'il existe une puissance p', inférieure à p-1, telle que $b^{p'}=1$ (mod p), par exemple $4^2=1$ (mod 5), ce qui s'explique, on l'a vu, par le petit théorème de Fermat car $4^2=2^4=1$ (mod 5) du fait que 5 est premier. Mais on trouve aussi d'autres exemples qui ne s'expliquent pas directement par ce théorème. Voyons par exemple la table des puissances du modulo 7 :

a	a^1	a^2	a^3	a^4	a^5	a^6
1	**1**	**1**	**1**	**1**	**1**	**1**
2	2	4	1	2	4	**1**
3	3	2	6	4	5	**1**
4	4	2	**1**	4	2	**1**
5	5	4	6	2	3	**1**
6	6	**1**	6	**1**	6	**1**
7	0	0	0	0	0	0

Ici, l'explication du $2^3=1$ (mod 7) n'est pas directement le petit théorème de Fermat sauf si l'on considère que $4^2=2$ (mod 7) et donc $2^3=(4^2)^3=4^6$ (mod 7), ce qui est expliqué par le petit théorème de Fermat car 7 étant un nombre premier $4^6=1$ (mod 7). De même $6^2=1$ (mod 7) s'explique indirectement par le petit théorème de Fermat en utilisant le fait que $6=3^3=5^3$ (mod 7) car alors $6^2=(3^3)^2=3^6=1$ (mod 7) puisque 7 est premier, et de même $6^2=(5^3)^2=5^6=1$ (mod 7).

5 Première conclusion

Je voudrais comprendre le lien qu'il y a entre la périodicité des restes dans la division et la périodicité des puissances dans le modulo. Je voudrais expliciter en particulier le rôle du 1 dans la table des puissances du modulo. Dans cette table, je lis $2^3=1$ (mod 7), puis-je en déduire qu'il y aura 3 chiffres dans le développement décimal de 1÷7 en base 2? Effectuons cette division : 1÷7 s'écrit

1÷111 en base 2. On a 1÷111=0,001001001... en base 2. Il y a bien une séquence de 3 chiffres. Je lis encore dans la table que $4^3=1$ (mod 7). Cela signifie t-il qu'il va y avoir une séquence de 3 chiffres qui se répète dans la division de 1 par 7 en base 4? Effectuons cette division : 1÷7 s'écrit 1÷13 en base 4. On a 1÷13=0,021021021... en base 4. Il y a bien une séquence de 3 chiffres. Pour achever de me convaincre j'effectue la division de 1 par 7 en base 6 et constate, comme l'indique $6^2=1$ (mod 7), qu'il y a bien une séquence de 2 chiffres qui se répète. Effectivement, 1÷11=0,05050505... en base 6.

Si je résume cela, il y a autant de chiffres dans la séquence qui se répète que l'exposant de la première puissance modulo mon nombre premier, congrue à 1. Il doit y avoir 1 seul chiffre qui se répète quand je divise 1 par 7 en base 8 (=1 modulo 7), 3 chiffres dans la base 9, 6 chiffres dans la base 10 (c'était le point de départ de ma réflexion), etc.

Une autre idée me vient pour avancer dans ma compréhension du mécanisme en jeu : revenir dans la base 10 qui m'est plus familière. Quand je divise 1 par 3 en base 10, je n'ai qu'un seul chiffre qui se répète car $10^1=1$ (mod 3). De quelle façon l'égalité 10=1 (mod 3) me permet-elle de comprendre qu'il n'y a qu'un chiffre dans la séquence? Si je compare 10÷3 et 1÷3, je m'aperçois que ces quotients ont les mêmes parties décimales, ce que je comprends encore mieux en écrivant que comme 10=9+1, alors 10÷3= (9+1)÷3= 9÷3+ 1÷3=3+ 1÷3, la différence entre 10÷3 et 1÷3 est un entier, et ceci est bien une conséquence directe de 10=1 (mod 3).

Prenons un autre exemple, dans la division par 11 il va y avoir une séquence de 2 chiffres en base 10, car $10^1=10$ (mod 11) et $10^2=1$ (mod 11). le quotient de 1 par 11 est 0,090909... tandis que celui de 100 par 11 est 9,090909... Ces deux quotients diffèrent d'un entier comme le laisse prévoir l'égalité 100=1(mod 11), car elle signifie seulement que 100=99+1=11×9+1 et donc, en divisant par 11, que 100÷11= 9+ 1÷11. Or le quotient 100÷11 n'est que 100 fois le quotient 1÷11, selon l'égalité 100÷11=100×1÷11, c'est-à-dire qu'on passe de l'un à l'autre en déplaçant la virgule de 2 rangs. La période du développement décimal est égale à 2 pour cette simple raison. Pour 10÷3 et 1÷3, c'est pareil : ils ont la même partie décimale et on passe de l'un à l'autre en déplaçant la virgule de 1 rang, le développement décimal aura donc fatalement une période égale à 1.

Ainsi s'éclairait pour moi, d'une lumière limpide et triomphante, ce mystère qui m'avait longtemps intrigué. D'un coup je comprenais tout et tout me paraissait facile. Comment avais-je pu ne pas comprendre avant ce qui est finalement si simple? Dans la division par 7 en base 10, du fait que 10^6 est la première puissance de la base à être congrue à 1 modulo 7, je pouvais en déduire que les quotients 10^6÷7 et 1÷7 avaient la même partie décimale, or, comme on passe de l'un à l'autre en déplaçant la virgule de 6 rangs, cela signifiait que leur développement décimal devait avoir une période égale à 6! Et cette explication se transpose dans toutes les bases aussi aisément car, par définition de l'écriture décimale des nombres en base *b*, multiplier par b^a revient à déplacer la virgule de *a* rangs. Si la virgule est déplacée de *a* rangs et que les parties décimales sont égales, *a* étant la plus petite valeur pour laquelle cette égalité se produit, c'est que le développement décimal dans cette base a une périodicité égale à *a*. Or, pour que cela se produise, p étant le diviseur employé, pour que les quotients b^a÷p et 1÷p aient la même partie décimale, il faut et il suffit que b^a *soit la première puissance de b congrue à 1 modulo p*. Cette expression un peu hermétique, car peu familière, m'avait un temps écarté de la lumière tout en préparant le terrain à une compréhension réelle.

Je n'avais pas de peine non plus à concevoir les autres particularités entrevues pendant cette étude, sauf encore le petit théorème de Fermat qui gardait encore une sorte d'auréole mystérieuse. Quant aux permutations circulaires obtenues avec les séquences périodiques des quotients, elles restaient comme des cadeaux que cette étude avait mis en exergue et qui m'intriguaient encore. Ce qui paraissait étonnant était la présence de ces nombres 9, 999999, 9999999999999999 obtenus en multipliant 3, 7 (ou 13) et 17 par la séquence périodique qui leur correspondait. J'ai obtenu un pseudo-éclairage sur cette question en déchiffrant le tableau suivant, découvert dans un des ouvrages sur le sujet, et qui se prolonge jusqu'à l'infini donnant tous les nombres premiers:

Entier précédent une puissance de la base (10)	Décomposition de cet entier	Nombre premier dont on obtient la 1ère apparition
$10^1-1=9$	3^2	3
$10^2-1=99$	$3^2\times11$	11
$10^3-1=999$	$3^3\times37$	37
$10^4-1=9\,999$	$3^2\times11\times101$	101
$10^5-1=99\,999$	$3^2\times41\times271$	41, 271
$10^6-1=999\,999$	$3^3\times7\times11\times13\times37$	7,13
$10^7-1=9\,999\,999$	$3^2\times239\times4\,649$	239, 4 649
$10^8-1=99\,999\,999$	$3^2\times11\times73\times101\times137$	73, 137
$10^9-1=999\,999\,999$	$3^4\times37\times333\,667$	333 667
$10^{10}-1=9\,999\,999\,999$	$3^2\times11\times41\times271\times9\,091$	9 091
$10^{11}-1=99\,999\,999\,999$	$3^2\times513\,239\times21\,649$	513 239, 21 649
$10^{12}-1=999\,999\,999\,999$	$3^3\times7\times11\times13\times37\times101\times9\,901$	9 901

La légende de ce tableau signalait que 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 apparait dès la 2ème ligne. La longueur de la période de 1÷7 ou de 1÷13 est 6 car 7 et 13 n'apparaissent qu'à la 6ème ligne. Cette caractéristique se transpose dans les autres bases. Par exemple en base 7, on avait déjà rencontré 6666 (en multipliant par 5 la séquence de l'inverse de 5). Le tableau précédent transposé en base 7 donne:

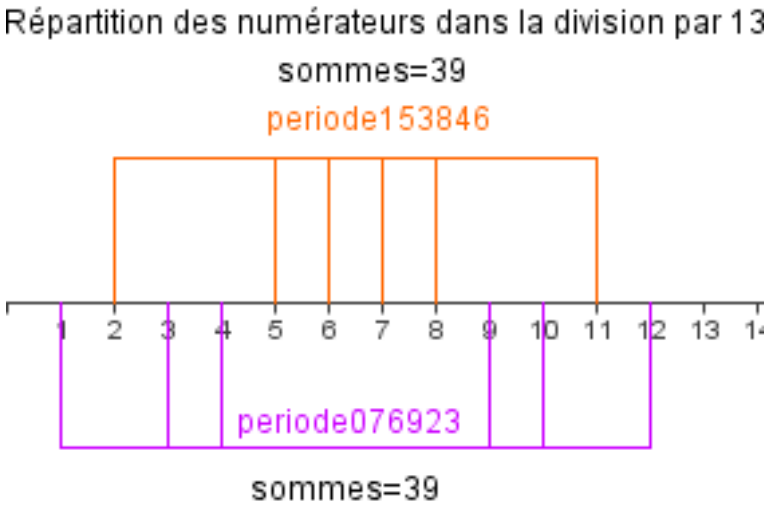
Entier précédent une puissance de la base (7)	Entier précédent converti en base 10	Décomposition (base 10)	Nombre premier dont on a la 1ère apparition
$10^1-1=6$	6	2×3	2,3
$10^2-1=66$	48	$2^4\times3$	
$10^3-1=666$	342	$2\times3^2\times19$	19
$10^4-1=6\,666$	2 400	$2^5\times3\times5^2$	5
$10^5-1=66\,666$	16 806	$2\times3\times2\,801$	2 801
$10^6-1=666\,666$	117 648	$2^4\times3^2\times19\times43$	43
$10^7-1=6\,666\,666$	823 542	$2\times3\times29\times4\,733$	29, 4 733
$10^8-1=66\,666\,666$	5 764 800	$2^6\times3\times5^2\times1\,201$	1 201
$10^9-1=666\,666\,666$	40 353 606	$2\times3^3\times19\times37\times1\,063$	37, 1 063
$10^{10}-1=6\,666\,666\,666$	282 475 248	$2^4\times3\times11\times191\times2\,801$	191
$10^{11}-1=66\,666\,666\,666$	1 977 326 742	$2\times3\times1\,123\times293\,459$	1 123, 293 459
$10^{12}-1=666\,666\,666\,666$	13 841 287 200	$2^5\times3^2\times5^2\times13\times19\times43\times181$	13, 181

Nous constatons bien que 5 est sur la 4ème ligne, son inverse doit donc avoir une période de 4 chiffres. Nous constatons aussi qu'il n'y a aucun nombre en base 7 dont l'inverse a une période de 2 chiffres. Nous retrouvons le nombre premier 13, long en base 7, dans la 12ème ligne...
Je ne comprends pas vraiment le lien entre la décomposition de 10^n-1 en facteurs premiers et le nombre de chiffres dans la période de l'inverse d'un des facteurs premiers, mais il y a beaucoup

d'autres choses que je ne comprends pas, comme cette particularité évoquée à la fin de la partie 2, concernant l'égalité des sommes des numérateurs qui conduisent à une même période, lorsqu'il y a plusieurs périodes pour un même dénominateur. En somme, il y a beaucoup plus de questions non résolues qu'au début de cette étude. Avoir répondu à une question en a suscité plus d'une. Ce doit être un des modes de fonctionnement de la nature, comme la graine qui germant, donne naissances a plein de graines nouvelles...

6 symétries

Je reviens vers cette question non élucidée de la répartition des numérateurs ayant des périodes identiques lors de la division par un nombre premier qui n'est pas long et qui conduit donc à plusieurs périodes différentes. Notre premier exemple était avec 13 (début de la page 3) qui conduit à 2 périodes différentes en base 10 : 076923 et 153846. Les numérateurs conduisant à une quelconque de ces périodes ont une somme égale à 39 dans les 2 cas. C'est assez remarquable mais, si l'on considère que le total des numérateurs doit valoir 78 (1+2+...+12=13×6) et que l'on doit partager ce nombre en 2, il est assez logique qu'on tombe sur 39, la moitié de 78 mais quelle loi interdit que le partage soit inégal (qu'on aie par exemple 21 et 57, selon le partage 1+2+...+6=21 et 7+8+...+12=57)? Ce qui est aussi très remarquable est la répartition symétrique des numérateurs comme le montre la figure ci-dessous.



Notre idée est d'examiner maintenant comment ça se passe pour les autres nombres premiers *p* qui ne sont pas longs. Pour commencer dressons le début du tableau donnant pour la base 10, la longueur *l* de la période, le nombre c de périodes différentes, le total t des numérateurs et le rapport t/c qui nous donne la somme théorique revenant pour chaque période (dans le cas de p=13 on avait un rapport t/c=39).

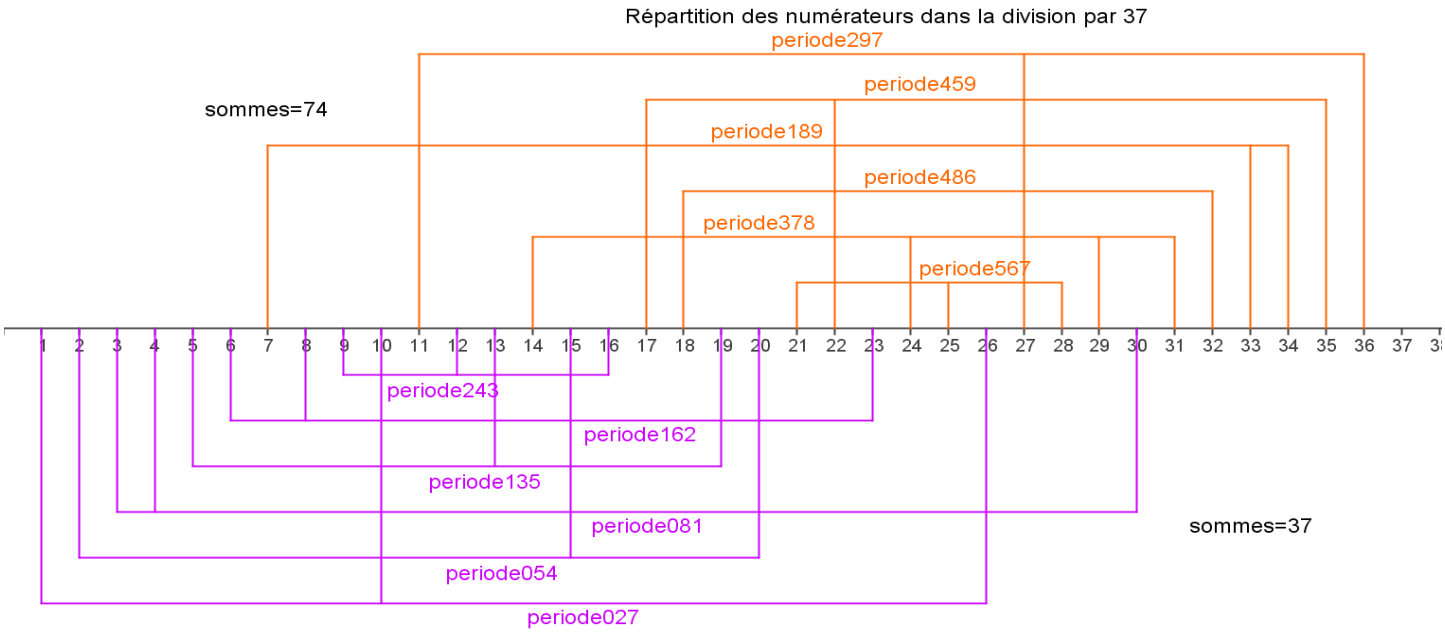
p	11	13	31	37	41	43	53	67	71	73
c	5	2	2	12	8	2	4	2	2	9
l	2	6	15	3	5	21	13	33	35	8
t	55	78	465	666	820	903	1378	2211	2485	2628
t/c	11	39	?	?	?	?	?	?	?	292

Nous constatons que la plupart des rapports théoriques ne sont pas entiers. Nous avons mis un point d'interrogation pour signaler cela car le partage des numérateurs ne peut conduire qu'à des nombres entiers. Ils sont en fait égaux à p×*l*÷2 et donc ne sont entiers que lorsque *l* est pair (cela arrive 27 fois sur les 60 premiers nombres premiers non longs, inférieurs à 550). Le grand organisateur de la nature (et des nombres) a dû prévoir un moyen de répartir ces entiers d'une façon inégale et c'est ce

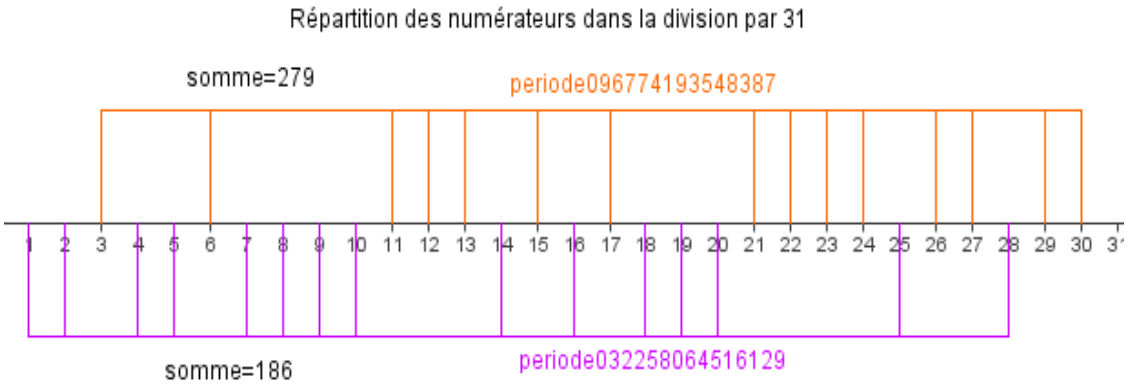
qu'on souhaite découvrir. Nous avons donc observé comment cette répartition est faite, ce qui nous a permis de compléter le tableau précédent.

p	11	13	31	37	41	43	53	67	71	73
c	5	2	2	12	8	2	4	2	2	9
l	2	6	15	3	5	21	13	33	35	8
somme (s)	11	39	186 279	37 74	82 123	430 473	371 318	1072 1139	994 1491	292

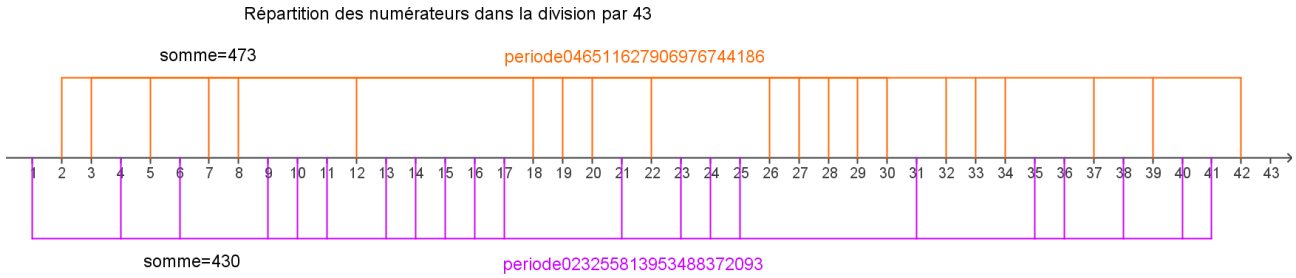
La répartition suit la somme théorique lorsque celle-ci égale un entier (pour 11, 13 et 73) et sinon, lorsque la somme théorique n'est pas divisible en 2 parties égales, le partage se fait en 2 parties inégales mais contenant exactement le même nombre de numérateurs par période, ce nombre étant exactement la longueur *l* de la période. De plus, il y a toujours autant de périodes pour les 2 parties. Par exemple, pour 37 qui est partagé en 2 parties, il y a 6 périodes de longueur 3 dans chaque partie, chaque période étant amenée par 3 numérateurs différents. Voyez plutôt la figure ci-dessous qui montre à quel point le partage est sophistiqué tout en restant symétrique. Chaque période d'une des partie trouvant son symétrique exact dans l'autre partie. On remarque en outre que la symétrie dans le cas de 37 est de type symétrie centrale, alors qu'elle était une symétrie axiale dans le cas de 13.



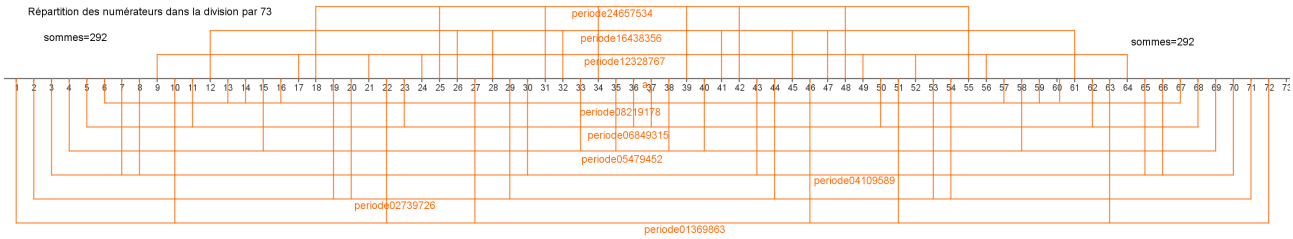
Il semble que la symétrie centrale se rencontre lorsque les 2 parties sont inégales, c'est-à-dire lorsque les longueurs *l* des séquences sont impaires, comme par exemple pour 31 ou pour 43. Ces nombres conduisent à 2 périodes seulement, comme 13, mais voient leurs numérateurs partagés en 2 parties ayant un centre de symétrie, contrairement à 13 où il y a un axe de symétrie. La raison est simple, la longueur *l* de la séquence est égale au nombre de numérateurs amenant cette séquence (les différents restes que l'on obtient en effectuant la division). Or les numérateurs se regroupent par



paires dont la somme vaut le dénominateur premier. Par exemple, avec le dénominateur 31, les 30 numérateurs se regroupent en 15 paires de somme 31: 1+30, 2+29, 3+28, ... , 15+16. Ces paires étant symétriques par rapport à la moitié du dénominateur (31÷2=15,5), il faut prendre des paires entières pour conserver la symétrie dans une partie. Or, la longueur de la séquence étant ici un nombre impaire (15), il faut choisir 15 numérateurs et donc il n'est pas possible de conserver la symétrie qui nécessite un nombre pair de numérateurs. Le découpage se fait alors en mettant dans une partie 15 numérateurs n'ayant pas leur complément à 31, et dans l'autre partie les compléments, d'où la symétrie centrale observée.



Regardons comment cela se répartit dans le cas de 73, avec ses 9 périodes distinctes. Le calcul prévoit une somme de 292 par période et le partage ne peut pas se faire avec 2 parties, même inégales, car il n'y a pas un nombre pair de périodes différentes à partager.



Nous constatons que le partage est symétrique par rapport à un axe perpendiculaire à l'axe gradué, comme dans le cas de 11 ou 13, ce qui semble appuyer cette hypothèse que le partage a un axe de symétrie lorsque le rapport t/c est un nombre entier et un centre de symétrie dans le cas contraire. Dans le cas de 173, qui doit se répartir de façon inégale car le rapport t/c n'est pas entier, la répartition se fait en 4 parties associées 2 par 2 par symétrie centrale. Nous avons vérifié ainsi tous les nombres premiers inférieurs à 200, mais il est évident que nous ne pouvons rien prouver simplement en examinant une ou deux dizaines d'exemples. Un millier ne suffirait pas non plus. Ce qu'on peut à la rigueur rechercher est un contre-exemple qui nous forcerait à abandonner ou modifier notre hypothèse. Pour ce qui est de notre modeste observation, nous reconnaissons que ces partages des numérateurs obéissent à des lois très strictes, où aucune place ne semble laissée au hasard.

Nous pouvons approfondir notre exploration afin de dégager d'autres propriétés de ce partage. En effet, les sommes obtenues dans le partage des numérateurs de 31, 37, 41, 43, etc. ne sont pas quelconques :

>Pour 31, les 2 sommes sont 186 et 279, c'est-à-dire 6×31 et 9×31. Ces sommes sont des sommes de 15 nombres car la période est 15.
>Pour 37, les 2 sommes sont 37 et 74, donc 1×37 et 2×37. Ces sommes sont des sommes de 3 nombres car la période est 3.
>Pour 43, les 2 sommes sont 430 et 473, c'est-à-dire 10×31 et 11×31. Ces sommes sont des sommes de 21 nombres car la période est 21.
>Pour 173, les 4 sommes sont 3460, 3633, 3806 et 3979, c'est-à-dire 20, 21, 22 et 23×173. Ces sommes sont des sommes de 43 nombres car la période est 43.

Nous avons vu que dans une partie, il ne pouvait y avoir que des nombres non-appariés (pour le dénominateur 37, il n'y a dans une partie que des nombres privés de leur complément à 37). Il

s'ajoute maintenant une autre contrainte sur le partage : la somme des numérateurs doit être un multiple du dénominateur premier. Remarquons que cette dernière contrainte est également satisfaite lorsque le partage ne conduit qu'à une seule partie (lorsque la période est paire), car alors il n'y a que des nombres appariés et donc naturellement, la somme des numérateurs dans une partie est un multiple du dénominateur. Une nouvelle question surgit donc : comment s'effectue le partage de la période entre les différentes parties? Par exemple, pour 31, pourquoi partage-t-on 15 en 6 et 9? Pourquoi pas 7 et 8, ou 5 et 10? Ne peut-on pas faire 7×31 et 8×31 en répartissant par groupe de 15 nombres les 30 premiers entiers? J'avoue ne pas savoir comment répondre à cette question. Toujours est-il que le partage réalise des groupes de 15 nombres totalisant 6 et 9 fois 31 et non pas 7 et fois 31.

Une deuxième remarque vient compléter cette observation : si j'additionne les chiffres de la séquence qui se répète, j'obtiens des multiples de 9:

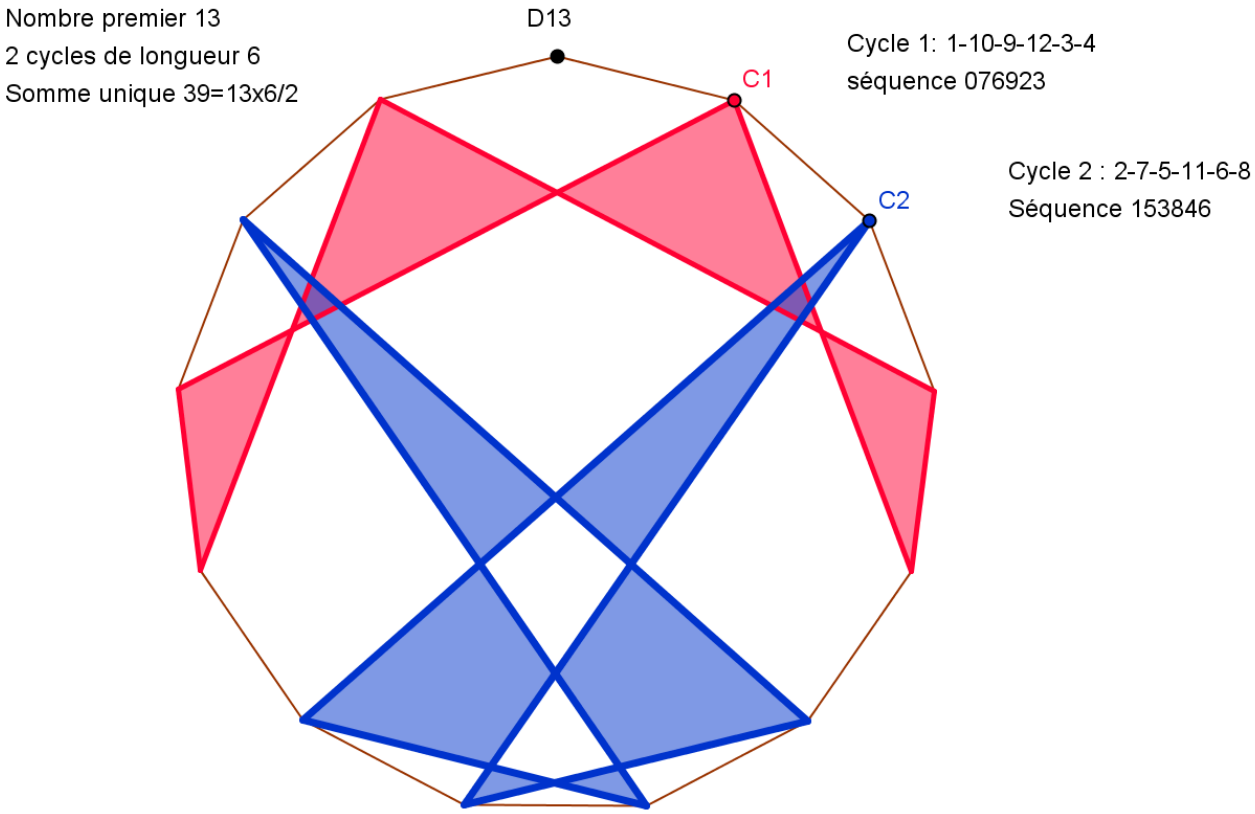
>Pour 31, les séquences étant 032258064516129 et 096774193548387, les sommes sont 54 et 91, donc 6×9 et 9×9.
>Pour 37, les séquences étant 027, 054, 081, 135, 162, 189, 243, 297, 378, 459, 486 et 567, les sommes sont 9=1×9 pour la 1ère partie (nombres non soulignés) et 18=2×9 pour l'autre partie, symétrique de la 1ère.
>Pour 43, les séquences étant 023255813953488372093 et 046511627906976744186, les sommes sont 90 et 99, donc 10×9 et 11×9.
>Pour 173, les 4 séquences contiennent 43 chiffres, ce qui est un peu long à écrire, mais les sommes de ces chiffres sont 20, 21, 22 et 23×9.

Bien sûr, ces sommes de chiffres sont à rapprocher des "entiers précédents une puissance de la base (10)" que nous avons vu au chapitre précédent, qui, par leur décomposition en facteurs premiers, nous donnaient la longueur de la période pour l'inverse des facteurs premiers. Par exemple, 37 apparaissant pour la 1ère fois dans la décomposition de 999, l'inverse de 37 aura une période de 3 chiffres. De même, 41 apparaissant pour la 1ère fois dans la décomposition de 99 999, l'inverse de 41 aura une période de 5 chiffres. Nous n'avions pas continué notre tableau jusque là, mais 31 n'apparaît pas avant la décomposition de 10^{15}-1, 43 n'apparaît qu'avec 10^{21}-1 et 173 n'apparaît qu'avec 10^{43}-1. Nous avons déjà remarqué que ces nombres sont obtenus en multipliant la période de l'inverse par le nombre premier. Par exemple 032258064516129×31=999999999999999, ou 027×37=999, ou encore 023255813953488372093×43=999999999999999999999. Par le jeu de la symétrie des parties et des permutations circulaires au sein d'une partie, on comprend que la somme des chiffres des deux parties (s'il n'y en a que deux) doit égaler ces nombres constuits exclusivement avec des 9. Par exemple 31, si on le décompose en 1+30, on va additionner 032258064516129×1 et 032258064516129×30, mais ce dernier nombre est la plus grande permutation de la séquence symétrique, c'est donc 967741935483870, et la somme 032258064516129+ 967741935483870, on le vérifie aisément, est 999999999999999. Pour 37, les différentes séquences sont appariées entre les deux parties, par exemple la séquence 027 de la 1ère partie (celle dont la somme des chiffres est 9) est appariée avec la séquence 297 de la 2ème partie (297 est obtenu en divisant 36, le symétrique de 1, par 37). Ces appariements se voient bien sur les schémas donnés plus haut. Les sommes des chiffres pour chaque paire de séquences vaut donc ici 3×9, comme pour le nombre 999.

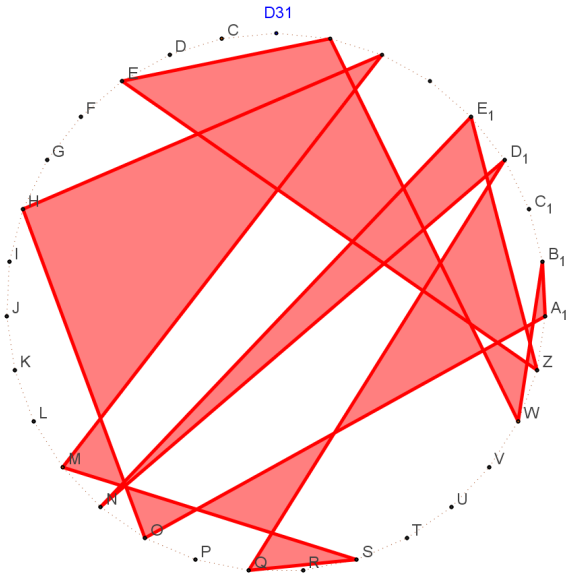
A ce niveau, ce qui est remarquable, c'est que le partage des 9 se calque sur celui des numérateurs. Pour 31 le partage est 6 et 9 pour les 2 partages (6×9 pour les chiffres de la 1ère séquence et 6×31 pour ses numérateurs et 9×9 pour les chiffres de la 2ème séquence et 9×31 pour ses numérateurs), pour 37 le partage est 1 et 2 (cela ne pouvait pas être autrement), pour 43 c'est 10 et 11... Nous avons noté encore un autre partage qui s'effectue de la même façon : dans un ensemble de numérateurs correspondant à une séquence donnée, il y a n nombres inférieurs à la moitié du dénominateur premier et n' nombres supérieurs. La somme $n+n'$ vaut le nombre de numérateurs par séquence qui est aussi la longueur de la séquence. Regardons comment s'effectue le partage entre n et n' dans le cas de 31 par exemple : n=9 et n'=6 pour la 1ère séquence, celle de l'inverse, celle qui totalise 6×9 et 6×31 ; pour l'autre séquence, qui totalise 9×9 et 9×31, la répartition entre les petits

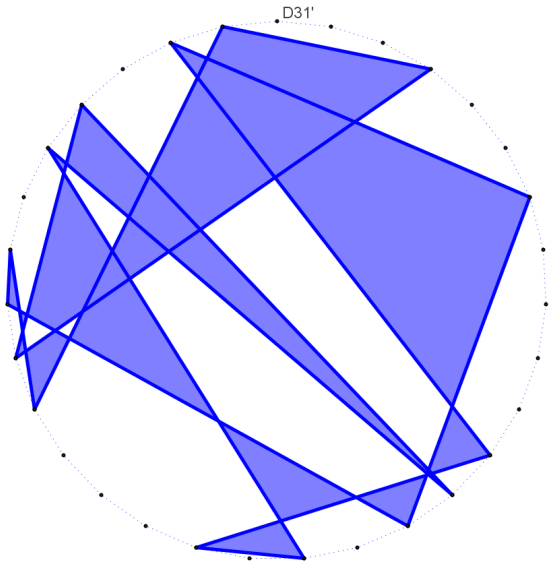
et les grands numérateurs est n=6 et n'=9. Il semble que n', le nombre de numérateurs supérieurs à la moitié du dénominateur premier, soit égal à la part des 9 ou la part des numérateurs. Cela se vérifie pour 37 où il y a 6 séquences qui prennent 1 part et les 6 autres séquences qui prennent 2 parts. Mais dès le nombre 41, il y a une répartition qui se complique : il y a 8 séquences de 5 chiffres réparties en 4 paires. Pour 2 paires, le partage des chiffres suit les 2 autres partages (2×9 et 2×41 d'une part et 3×9 et 3×41 d'autre part) et l'on a n=3 et n'=2 d'une part et n=2 et n'=3 d'autre part. Par contre, pour les 2 autres paires, le partage des chiffres ne suit pas les 2 autres partages et l'on a n=4 et n'=1 d'une part (celle des 3) et n=1 et n'=4 d'autre part (celle des 2). Ainsi, nous voyons que cette 3ème remarque n'est pas une propriété générale : la répartition des chiffres entre les petits et les grands ne suit généralement pas la même règle que pour les 2 autres partages. Rappelons tout de même que ces règles de partage sont énoncées à titre d'hypothèse de travail. Nous n'avons rien prouvé. Par ailleurs, nos lectures sur le sujet ne nous ont pas donné d'indication sur ces propriétés. Cela ne veut pas dire que le sujet a été ignoré par les mathématiciens (qui étudient la question depuis des siècles, 2 au moins si l'on fait commencer la théorie rigoureuse sur cette questions aux travaux de Gauss) mais plutôt que nos lectures n'ont pas été assez approfondies.

Ce que nous étudions, la division par un nombre premier p, avec la succession des restes qui sont par nature inférieurs à p, serait peut-être mieux représenté graphiquement par un cercle, plutôt que par une droite. En guise de récréation, reprenons la répartition des numérateurs lorsqu'on divise par 13, 37 ou 43.

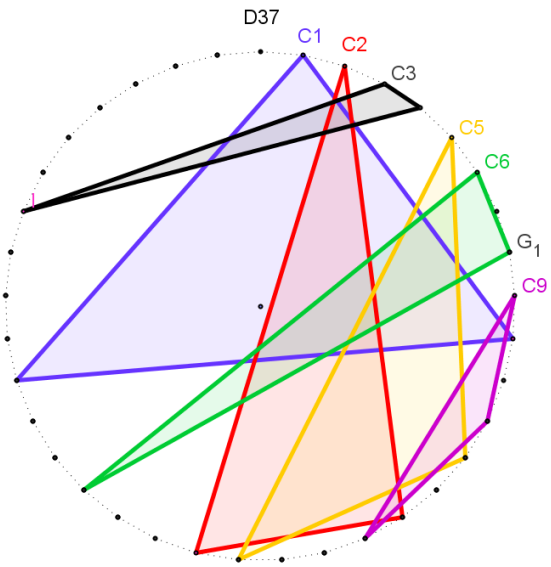


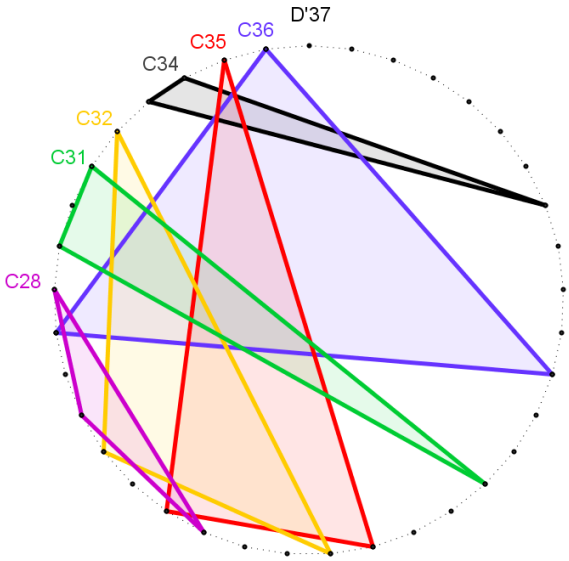
Nous voyons, avec la division par 13, comment se visualise cette symétrie qui est ici aussi une symétrie axiale : chaque nombre d'une séquence étant apparié avec son complémentaire, ici complémentaire à 13, les polygones obtenus admettent le diamètre passant par 0 comme axe de symétrie. Voyons maintenant ce que sont les 2 polygones qu'on obtient dans les divisions par 31. Nous savons qu'ils ont 15 sommets qui ne sont pas appariés avec leur complémentaire à 31. Ce qui apparaissait comme une symétrie centrale dans la représentation sur une droite, apparaît maintenant comme une symétrie axiale sur le cercle : les 2 polygones sont symétriques l'un de l'autre par rapport au diamètre qui passe par 0 (nous avons séparé les 2 polygones afin de ne pas surcharger la figure obtenue).





Pour 37 qui possède 12 groupes de numérateurs répartis en 2 familles symétriques, nous obtenons cette représentation qui montre bien les 6 paires de triangles symétriques.





... à suivre ...

Philippe Moutou, août 2009