Cet article est rédigé par des élèves. Il peut comporter des oublis ou des imperfections, autant que possible signalés par nos relecteurs dans les notes d'édition.

Les chiffres des puissances de 2

Année 2021-2022

Lucas Hermier–Gastineau, Jean-Bastien Ricot, Alix Saugier, Saada Mamouni (Terminale), Karina Albu, Anaïs Girard (1ère)

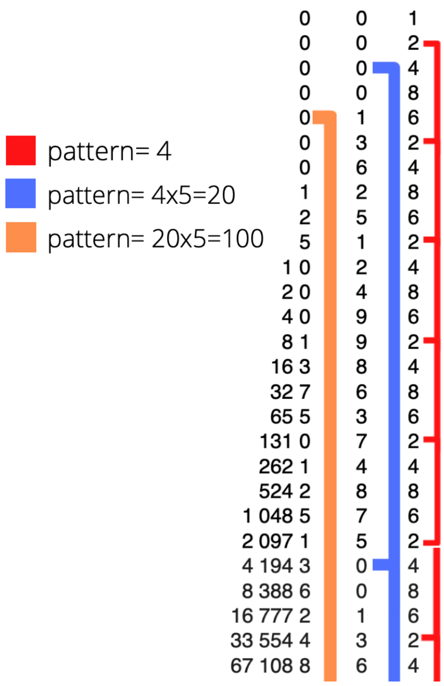
Établissement : Lycée Frédéric Mistral, Fresnes (94)

Enseignantes : Sophie Volatier et Marie-Claude Moussaïd

Chercheur : Joël Cohen, Université de Paris-Saclay

1 Présentation du sujet

Le sujet que nous avons choisi est l'étude des chiffres qui apparaissent dans les puissances de 2.



On peut observer que pour toute colonne, un motif de chiffres qui se répète à l'infini existe.

On appelle la taille de ce motif une période.

On observe que la période est multipliée par 5 lorsque qu'on se décale d'une colonne vers la gauche. Le motif ne commence néanmoins pas directement : pour la colonne 1 (la colonne des unités), le chiffre au rang 0 n'est pas inclus dans la motif. De manière plus générale, pour une colonne k, le motif ne commence qu'au rang k.

On peut mesurer la fréquence d'apparition de chaque chiffre dans le motif d'une colonne donnée. À l'aide d'un programme écrit en langage Python, on trouve que pour toutes les colonnes à partir de la deuxième, chaque chiffre apparaît le même nombre de fois dans un motif. Ainsi, dans le motif de ces colonnes, il y a autant de fois les chiffres 0, 1, 2, etc.

2 Résultats

Les colonnes sont numérotées à partir de 1 de la droite vers la gauche, dans le tableau précédent. On appelle colonne k la $k^{\text{ième}}$ colonne du tableau , k étant un entier supérieur ou égal à 1.

On a démontré par récurrence sur les colonnes les trois théorèmes suivants :

Théoreme 1. *En base 10, il existe un motif de répétition des* <u>*k derniers chiffres*</u> *qui est de taille* $4 \times 5^{k-1}$. *Le motif ne commence qu'à partir du rang k.*

Théoreme 2. *: En base 10, il existe un motif de répétition* <u>*des chiffres de la colonne k*</u> *qui est de taille* $4 \times 5^{k-1}$. *Le motif ne commence qu'à partir du rang k.*

Théoreme 3. *En base 10, pour toutes les colonnes sauf la première, chaque chiffre (de 0 à 9) apparaît le même nombre de fois dans un motif. On exclut la première colonne, car 6 chiffres n'y apparaissent pas.*

3 Motif de répétition des k derniers chiffres

Lemme 1. *Deux nombres ont les mêmes k derniers chiffres en base 10 si et seulement si ils ont les mêmes k derniers chiffres en base 2 et en base 5.*

Démonstration.

Soient n_1 et n_2 avec $(n_1, n_2) \in \mathbb{N}^2$.

Si $n_1 \equiv n_2\ [2^k]$ et $n_1 \equiv n_2\ [5^k]$, alors $2^k \mid (n_1 - n_2)$ et $5^k \mid (n_1 - n_2)$ (1).

Or, pour tout $k \in \mathbb{N}$, 2^k et 5^k sont premiers entre eux, donc d'après le théorème de Gauss alors $10^k = 2^k \times 5^k \mid (n_1 - n_2)$, soit $n_1 \equiv n_2\ [10^k]$.

Réciproquement, si $n_1 \equiv n_2\ [10^k]$, alors $10^k \mid (n_1 - n_2)$ d'où $2^k \mid (n_1 - n_2)$, soit $n_1 \equiv n_2\ [2^k]$.

De la même manière, $n_1 \equiv n_2\ [10^k] \implies n_1 \equiv n_2\ [5^k]$.

On conclut que $n_1 \equiv n_2 [2^k]$ et $n_1 \equiv n_2 [5^k] \iff n_1 \equiv n_2 [10^k]$.

Or en base 2 les k derniers chiffres du nombre n_1 correspondent au reste de la division euclidienne de n_1 par 2^k. De la même manière en base 5 et en base 10 les derniers chiffres correspondent au reste de la division euclidienne respectivement par 5^k et 10^k.

On note $R_{2,1}$ les k derniers chiffres de n_1 en base 2, $R_{5,1}$ en base 5, $R_{10,1}$ en base 10. De la même manière, on utilise $R_{2,2}$, $R_{5,2}$ et $R_{10,2}$ pour n_2.

On a alors

$$R_{10,1} = R_{10,2} \iff (R_{2,1}, R_{5,1}) = (R_{2,2}, R_{5,2}).$$

Or il y a 10^k $R_{10,1}$ possibles. On sait également qu'il y a 2^k $R_{2,1}$ possibles et 5^k $R_{5,1}$ possibles. Il existe donc 10^k couples ($R_{2,1}$, $R_{5,1}$) possibles.

On sait donc que pour chaque $R_{10,1}$ différent, on aura un couple ($R_{2,1}$, $R_{5,1}$) différent et qu'il y a le même nombre de $R_{10,1}$ possibles que de couples ($R_{2,1}$, $R_{5,1}$) possibles. On en conclut que pour chaque $R_{10,1}$ possible, il existe un unique couple ($R_{2,1}$, $R_{5,1}$) correspondant. □

Dans le cadre de notre recherche, cela signifie que pour prouver une répétition des k derniers chiffres en base 10, on peut se contenter de prouver une répétition en base 5 et en base 2. Une répétition des k derniers chiffres existe en base 10 si et seulement si elle existe en base 2 et en base 5.

L'analyse des puissances de 2 en base 2 se révèle très simple :

Puissances de 2 en base 2	
0001	2^0
0010	2^1
0100	2^2
1000	2^3
...	

On ne fait que gagner un zéro à chaque multiplication par 2, de la même manière que si on analysait les puissances de 10 en base 10.

La réelle difficulté est l'analyse des puissances de 2 en base 5. Nous allons commencer par démontrer le lemme suivant.

Lemme 2. *S'il existe $n \in \mathbb{N}^*$, tel que $2^n \equiv 1\ [5^k]$, alors le motif de répétition des k derniers chiffres en base 5 commence dès le rang 0.*

Exemple :

Puissances de 2 en base 5	
00**01**	2^0
0002	2^1
0004	2^2
0013	2^3
0031	2^4
0112	2^5

0224	2^6
...	
..33**01**	2^{20}
..2102	2^{21}
..4204	2^{22}

2^{20} est la première puissance qui finit une nouvelle fois par 01, c'est-à-dire $2^{20} \equiv 1 \equiv 2^0\ [5^2]$.

Ainsi, pour tout $n \in \mathbb{N}$, $2^n \equiv 2^{20+n}\ [5^2]$.

Cest pour cela que les 2 derniers chiffres en base 5 vont se répéter avec une période de 20. On remarque également que le motif de répétition des 2 derniers chiffres commence au rang 0.

Démonstration. Si le motif des k derniers chiffres ne commence pas au rang 0, alors les k derniers chiffres du rang 0 ne se retrouvent à aucun autre rang.

On peut le voir en base 10 pour le motif du dernier chiffre :

01	2^0
0**2**	2^1
04	2^2
08	2^3
16	2^4
3**2**	2^5
64	2^6

Le premier chiffre qui se répète n'est pas le chiffre au rang 0 mais au rang 1. Ainsi le motif de répétition du dernier chiffre n'inclut pas le dernier chiffre au rang 0. Le dernier chiffre au rang 0 ne réapparaît donc à aucun autre rang.

De manière plus générale, si le motif de répétitions des k derniers chiffres ne commence pas au rang 0, alors les k derniers chiffres au rang 0 ne sont jamais répétés.

Par contraposée, si l'on retrouve les k derniers chiffres du rang 0 à un autre rang, cela signifie que le motif de répétition des k derniers chiffres commence au rang 0 (2).

Or, $2^0 = ...001$, donc s'il existe $n \in \mathbb{N}^*$, tel que $2^n \equiv 1[5^k]$, alors le motif de répétition des k derniers chiffres commence au rang 0 en base 5. □

Dans ce cas, *la période des k derniers chiffres a pour valeur le plus petit n non nul tel que* $2^n \equiv 1[5^k]$ (3).

Lemme 3. *Soit* $n = ...ab0...01$ *en base* β*, avec* $b \neq 0$*, c'est-à-dire que n finit par un nombre fini de 0 puis 1. Alors,* $n^\beta = ...b0...01$ *avec un 0 en plus.*

Exemple :

On prend n un entier naturel qui se termine par 4301 en base 10, donc n = ...4301,

$$n \equiv 4 \times 10^3 + 3 \times 10^2 + 1\ [10^4].$$

Ici, $\beta = 10$, $a = 4$, $b = 3$.

Ce qui est démontré par la suite, c'est que

$$\ldots 4301^{10} \equiv 3001\ [10^4].$$

De même, si $n = \ldots 65001$ et que $\beta = 7$, alors la fin de $(65001)^7$ sera "5<u>0</u>001".

On rajoute ici un 6 pour montrer que le chiffre qui vient avant le 5 n'a pas d'importance. Étant donné que nous nous servons des congruences dans notre démonstration, si nous n'avions pas pris en compte ce chiffre, notre démonstration aurait uniquement fonctionné pour n = ...05001.

Démonstration.

Soit $\beta \in \mathbb{N}$ tel que $\beta \geq 2$. Soient $n \in \mathbb{N}$ tel que $n = \ldots ab \underbrace{0\ldots0}_{p-1 \text{ zéros}} 1$ en base β où $(a\,;\,b) \in \mathbb{N}^2$, avec $a,\ b < \beta$ et $b \neq 0$, et $p \in \mathbb{N}$ tel que $p \geq 2$ (p correspond au nombre de 0 plus un).

On a donc $n \equiv a\beta^{p+1} + b\beta^p + 1\ [\beta^{p+2}]$

Soit $c \in \mathbb{N}$. On note $P(c)$ la propriété suivante :

$$n^c \equiv ac\beta^{p+1} + bc\beta^p + 1\ [\beta^{p+2}.]$$

Initialisation :

$$n^0 = 1 \text{ et } a \times 0 \times \beta^{p+1} + b \times 0 \times \beta^p + 1 = 1.$$

Or $1 \equiv 1\ [\beta^{p+1}]$, donc $P(0)$ est vraie.

Hérédité :

Soit $k \in \mathbb{N}$. On suppose que $P(k)$ est vraie.

$$\begin{aligned}
n^k &\equiv ak\beta^{p+1} + bk\beta^p + 1\ [\beta^{p+2}] \\
n^{k+1} &\equiv (a\beta^{p+1} + b\beta^p + 1)(ak\beta^{p+1} + bk\beta^p + 1)[\beta^{p+2}] \rightarrow \text{ on a multiplié par } n \text{ des deux côtés de la relation} \\
&\equiv a^2k\beta^{2p+2} + abk\beta^{2p+1} + a\beta^{p+1} + abk\beta^{2p+1} + b^2k\beta^{2p} + b\beta^p + ak\beta^{p+1} + bk\beta + 1\ [\beta^{p+2}] \\
&\equiv a\beta^{p+1} + b\beta^p + ak\beta^{p+1} + bk\beta^p + 1\ [\beta^{p+2}] \text{ car } p \geq 2 \Leftrightarrow 2p \geq p+2 \\
&\equiv a\beta^{p+1}(k+1) + b\beta^p(k+1) + 1\ [\beta^{p+2}].
\end{aligned}$$

La propriété est vraie au rang $k+1$.

Conclusion : $P(c)$ est vraie pour tout $c \in \mathbb{N}$.

En particulier, pour $c = \beta$, on a

$$n^\beta \equiv a\beta^{p+2} + b\beta^{p+1} + 1\ [\beta^{p+2}] \equiv b\beta^{p+1} + 1\ [\beta^{p+2}].$$

Par conséquent, si $n \equiv a\beta^{p+1} + b\beta^p + 1\ [\beta^{p+2}]$, alors $n^\beta \equiv b\beta^{p+1} + 1\ [\beta^{p+2}]$.

Ainsi , si $n \equiv b\beta^p + 1\ [\beta^{p+1}]$, alors $n^\beta \equiv b\beta^{p+1} + 1\ [\beta^{p+2}]$.

On a donc démontré qu'un 0 s'intercalait à la fin d'un nombre élevé à la puissance de sa base. Néanmoins il faut qu'un 0 au moins soit déjà présent à la fin de ce nombre. En effet notre démonstration ne fonctionne que pour $p \geq 2$. □

Lemme 4. *Pour tout $k \in \mathbb{N}^*$, le motif de répétition des k derniers chiffres des puissances de 2 en base 5 commence au rang 0.*

Démonstration.

On sait que $2^{20} = \ldots 301$. D'après le lemme 3, $(2^{20})^5 = \ldots 3001$, donc $2^{100} = \ldots 3001$.

De la même manière, $2^{500} = \ldots 30001$, $2^{2500} = \ldots 300001$, etc.

Étant donné qu'on peut répéter ce processus à l'infini, on en déduit qu'en base 5, pour tout $k \in \mathbb{N}^*$, il existe $n \in \mathbb{N}^*$ tel que $2^n \equiv 1 [5^k]$.

Avec le lemme 2, on en déduit que pour tout $k \in \mathbb{N}^*$, le motif de répétition des k derniers chiffres commence dès 2^0. □

Ainsi, *pour tout $k \in \mathbb{N}^*$, la période des k derniers chiffres de 2^n en base 5 a pour valeur le plus petit n non nul tel que $2^n \equiv 1 [5^k]$.*

Lemme 5. *Pour tout $k \in \mathbb{N}^*$, la période minimale des k derniers chiffres en base 5 est de $4 \times 5^{k-1}$.*

Définitions :

Motif minimal : Si l'on prend les chiffres des unités des puissances de 2 en base 10, on a 1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6, etc.. "2, 4, 8, 6, 2, 4, 8, 6" est donc un motif qui se répète dans les chiffres des unités. Néanmoins, on peut le subdiviser en deux fois le motif "2, 4, 8, 6". Le motif minimal est donc le motif le plus petit possible, un motif qu'on ne peut pas subdiviser : "2, 4, 8, 6".

Période minimale : Taille du motif minimal.

Exemple :

On sait que $2^{20} = \ldots 301$, et que la période minimale des 2 derniers chiffres en base 5 est de 20. On en déduit, d'après la démonstration précédente que $2^{100} = \ldots 3001$. Cela nous indique qu'une période pour les 3 derniers chiffres est de 100.

Néanmoins, on ne sait pas si la période minimale est de 100. On pourrait avoir $2^{50} = \ldots 001$ par exemple. Le fait que 100 soit une période nous indique tout de même que la période minimale doit être un diviseur de 100.

On sait également que $2^{20} = \ldots 301$, la période minimale des 2 derniers chiffres en base 5 est de 20. De ce fait, les seules puissances qui finissent par 01 sont 2^{20t} avec $t \in \mathbb{N}$. Or, pour qu'une puissance de 2 finisse par 001, il faut qu'elle finisse par 01.

On en déduit que la période minimale pour les 3 derniers chiffres doit être un multiple de celle pour les 2 derniers chiffres.

Ainsi, la période minimale pour les 3 derniers chiffres doit être un multiple de 20, et un diviseur 100. Les seules possibilités que l'on a sont 20 et 100. Or, on sait que cela ne peut être 20, car $2^{20} = ...301$. Le 3 nous indique que cela ne peut pas être le motif minimal pour les 3 derniers chiffres : 2^{20} ne finit par par 001.

On en conclut, que la période minimale pour les 3 derniers chiffres est de 100.

Ce raisonnement est généralisable pour toutes les colonnes à l'aide d'une récurrence. On va ainsi démontrer que la période minimale de répétitions des k derniers chiffres est de $4 \times 5^{k-1}$.

Démonstration.

Soit $k \in \mathbb{N}$ avec $k \geq 2$. Soit $P(k)$, la propriété :

"le plus petit n non nul tel que $2^n \equiv 1\ [5^k]$ *est* $n = 4 \times 5^{k-1}$. *Dans ce cas* $2^n = 30...1$ *avec* $k-1$ *fois le chiffre 0."*

Initialisation :

$2^{20} = ...301$. C'est la première puissance à finir par 01 en base 5, si on exclut 2^0. Donc $P(2)$ est vraie.

Hérédité :

Soit $k \in \mathbb{N}$ avec $k \geq 2$. On suppose que $P(k)$ est vraie.

Par hypothèse de récurrence, pour $n = 4 \times 5^{k-1}$, $2^n = ...30...01$, avec $k-1$ fois le chiffre 0. Toujours par hypothèse de récurrence, la période minimale pour les k derniers chiffres est de $4 \times 5^{k-1}$.

D'après le lemme 3, $(2^n)^5 = 2^{5n} = ...300...01$ avec k fois le chiffre 0.

$5n = 4 \times 5^k$, par conséquent la période minimale de répétition pour les $k+1$ derniers chiffres est un diviseur de 4×5^k.

On sait aussi que pour qu'une puissance de 2 finisse par k fois le chiffre 0 puis 1, il faut qu'elle finisse par $k-1$ fois le chiffre 0 puis 1. On en déduit que que la période minimale de répétition des $k+1$ derniers chiffres doit être un multiple de $4 \times 5^{k-1}$. Les seuls nombres qui sont des multiples de $4 \times 5^{k-1}$ et des diviseurs de 4×5^k, sont $4 \times 5^{k-1}$ et 4×5^k.

Or, on sait que $4 \times 5^{k-1}$ ne peut être la période minimale puisque la présence du chiffre 3 montre qu'il n'y a que $k-1$ fois le chiffre 0. On en déduit que la période minimale de répétition pour les $k+1$ derniers chiffres est 4×5^k.

Ainsi $2^{4 \times 5^k} = ...300...01$ avec k fois le chiffre 0 et c'est la première puissance de 2 avec ce nombre de 0, puis 1. Notre propriété est donc héréditaire.

Conclusion : $P(k)$ est vraie pour tout $k \in \mathbb{N}$ avec $k \geq 2$.

Notre lemme s'applique également lorsque $k = 1$ même si ce cas ne fait pas partie de notre récurrence, en effet $2^4 = 301$. □

Théoreme 1. *En base 10 le motif minimal de répétition des k derniers chiffres est de taille* $4 \times 5^{k-1}$. *Ce motif ne commence qu'à partir du rang k.*

Démonstration.

En base 2, la période minimale des k derniers chiffres est toujours de 1, mais contrairement à la base 5, elle ne se met pas en place directement :

Puissances de 2 en base 2	
0001	2^0
0010	2^1
0100	2^2
1000	2^3
...	

D'après le lemme 1, on sait qu'il faut attendre que les k derniers chiffres forment un motif en base 2 ET en base 5 pour qu'ils forment un motif en base 10.

À l'aide du lemme 5, on en déduit qu'en base 10 la période minimale pour le dernier chiffre est de taille 4, mais le motif n'inclut pas le rang 0.

La période minimale pour les 2 derniers chiffres est de taille 20 mais le motif n'inclut ni le rang 0, ni le rang 1.

De manière générale, le motif minimal de répétition des k derniers chiffres en base 10 est de taille $4 \times 5^{k-1}$, mais ne commence qu'à partir du rang k. □

4 Motif de répétition des chiffres de la colonne k

Maintenant que l'on a fini l'analyse du motif minimal de répétition des k derniers chiffres, il faut que l'on voie en quoi cela s'applique lorsqu'on regarde uniquement le chiffre de la colonne numéro k.

En effet, le fait qu'il y ait une répétition des k derniers chiffres implique que les chiffres de la colonne k se répètent.

Néanmoins la réciproque n'est pas vraie. On pourrait s'imaginer une situation où uniquement les chiffres de la colonne k se répètent sans que les chiffres qui suivent le fassent également.

Lemme 6. *Le motif de répétition de toute colonne k ne commence qu'au rang k.*

Démonstration.

Pour simplifier l'explication de la démonstration, on va prendre l'exemple de la colonne des dizaines.

Puissances de 2 en base 10

01	2^0
02	2^1
04	2^2
08	2^3
16	2^4
32	2^5
...	
..576	2^{20}
..152	2^{21}
..3**04**	2^{22}
..608	2^{23}
..216	2^{24}

On a démontré précédemment que le motif des 2 derniers chiffres ne commence à se répéter qu'à partir de 2^2 et est de période 20.

Par conséquent, $2^{21} \not\equiv 2^1 \equiv 02\ [100]$ mais $2^{22} \equiv 2^2 \equiv 04\ [100]$. La seule possibilité est alors $2^{21} \equiv 52\ [100]$.

En effet, $2^{21} \equiv b + 2\ [100]$ avec $b \not\equiv 0\ [100] \implies 2^{22} \equiv 2b + 04\ [100]$.

Or, comme dit précédemment $2^{22} \equiv 04\ [100]$. Donc $04 \equiv 2b + 04\ [100] \iff 2b \equiv 0\ [100] \iff 50 \mid b$. La seule possibilité était donc $2^{21} \equiv 50 + 2\ [100]$.

Si l'on prend un autre exemple, on sait que le motif des 3 derniers chiffres ne commence qu'à partir de 2^3 et est de taille 100. Par conséquent, $2^{103} \equiv 008\ [1000]$, mais $2^{102} \not\equiv 004\ [1000]$. En suivant la même logique, cela veut dire que $2^{102} \equiv 504\ [1000]$.

Ainsi, le motif de la colonne 3 ne commence bien qu'à partir de 2^3, puisque $2^{102} \equiv 500 + 2^2 [1000]$. Ce raisonnement fonctionne pour toutes les colonnes, donc le motif des chiffres d'une colonne k ne commence bien qu'à partir du rang k (4). □

On va ici changer notre manière d'analyser un motif. Pour ce faire, il nous faut introduire quelques notations :

Notations :
Le $k^{\text{ième}}$ chiffre en partant de la droite, de 2^n en base 10 se note $C_{k,n}$.
La retenue générée par $C_{k,n-1}$ se note $r_{k,n}$.

Prenons les premières puissances de 2.

Puissances de 2 en base 10

01	2^0
02	2^1
04	2^2
08	2^3
16	2^4
32	2^5
64	2^6

À chaque fois, on multiplie le chiffre de la colonne des dizaines par 2. Mais on peut en plus avoir ou non une retenue de 1 qui vient de la colonne des unités.

On a donc, $C_{2,n+1} \equiv 2C_{2,n}$ [10] s'il n'y a pas de retenue, ou $C_{2,n+1} \equiv 2C_{2,n} + 1$ [10] s'il y a une retenue.

On a une retenue dans la colonne des dizaines à 2^4 car le chiffre des unités de 2^3 est 8, et $8 \times 2 \geq 10$. De la même manière, on a une retenue à 2^5 car le chiffre des unités de 2^4 est 6 et $6 \times 2 \geq 10$.

Or, si $0 \leq n < 5$, alors $2n < 10$ et $2n+1 < 10$, et si $5 \leq n < 10$, alors $2n \geq 10$ et $2n+1 \geq 10$.

Autrement dit, si le chiffre de la colonne des unités est 0, 1, 2, 3, ou 4 alors on n'aura pas de retenue à la puissance suivante. Si c'est 5, 6, 7, 8, ou 9, alors on en aura une. Or, les chiffres des unités se répètent, donc les retenues se répètent également.

On peut étendre ce concept et voir chaque colonne comme "générant" le motif de retenues qui sert à construire la colonne suivante. Pour des raisons d'optimisation d'espace, on va représenter les puissances de 2 à l'horizontale.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$C_{1,n}$	1	2	4	8	6	2	4	8	6	2	4	8	6	2	4	8	6	2	4	8	6
$r_{1,n}$	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
$C_{2,n}$	0	0	0	0	1	3	6	2	5	1	2	4	9	9	8	6	3	7	4	8	7
$r_{2,n}$	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1	1	1	0	1	0	1

Comme défini au-dessus, la ligne $C_{1,n}$ correspond aux chiffres des unités, la ligne $C_{2,n}$ au chiffre des dizaines, etc.

Ainsi,

$$\begin{cases} C_{k,n+1} = 2C_{k,n} + r_{k-1,n+1}. \\ r_{k,n} = 1 \text{ si } C_{k,n-1} \geq 5, \quad r_{k,n} = 0 \text{ sinon.} \end{cases}$$

On voit que le motif des retenues ne se met pas directement en place. Dans la suite des lemmes, on parle de motif des retenues et de motifs de chiffres une fois qu'ils ont commencé à se répéter.

Lemme 7. *La période minimale d'une colonne doit être un multiple de la période minimale des retenues générées par la colonne d'avant.*

Démonstration.

Soit t la période minimale d'une colonne k. Cela signifie qu'il existe $n_0 \in \mathbb{N}$ tel que pour tout $n > n_0$, $C_{k,n+t} = C_{k,n}$. Donc pour tout $n > n_0$, $C_{k,n+1+t} = C_{k,n+1}$.

D'après la relation de récurrence,

$$\begin{aligned} C_{k,n+1+t} &= 2C_{k,n+t} + r_{k-1,n+1+t} = 2C_{k,n} + r_{k-1,n+1+t} \\ &= C_{k,n+1} = 2C_{k,n} + r_{k-1,n+1} \\ &\Leftrightarrow r_{k-1,n+1+t} = r_{k-1,n+1}. \end{aligned}$$

On en conclut que t est une période des retenues issues de la colonne $k-1$. Ainsi, la période minimale des retenues issue de la colonne $k-1$ est un diviseur de la période minimale de la colonne k. □

Lemme 8. *Tout motif périodique des retenues de taille strictement supérieure à 4 est générée par une unique séquence de chiffres.*

Démonstration.

On va prendre un exemple de motif de retenues et voir comment trouver le motif de chiffres qui l'a généré. Si le motif des retenues est (0, 1, 1, 0, 1, 0, 1), on va commencer par prendre un chiffre de fin au hasard. Supposons que ce soit 9. Pour mieux visualiser quel chiffre pourrait précéder, on va faire un tableau de tous les chiffres qui pourraient être avant dans notre suite.

$n \equiv$ [10]	0	1	2	3	4	5	6	7	8	9
$2n \equiv$ [10]	0	2	4	6	8	0	2	4	6	8
$2n+1 \equiv$ [10]	1	3	5	7	9	1	3	5	7	9
Retenues	0	0	0	0	0	1	1	1	1	1

Il y a deux chiffres qui pourraient précéder 9 : 4 et 9. En effet, ce sont les seules valeurs de n, telles que $2n \equiv 9$ [10] ou $2n+1 \equiv 9$ [10]. Néanmoins, seule l'une d'entre elles donnera le 1 que l'on cherche dans le motif des retenues. Ainsi, on sait que le chiffre d'avant est 9. Le chiffre encore avant peut être soit 9 soit 4, mais cette fois-ci on ne veut pas qu'il génère de retenue. C'est donc 4. Le chiffre avant 4 peut être soit 2 soit 7. On veut qu'une retenue soit générée, donc il s'agit de 7, etc... On peut répéter le processus pour reconstituer le motif des chiffres qui a donné ce motif des retenues :

Chiffres	8	6	3	7	4	9	9
Retenues	0	1	1	0	1	0	1

Ainsi, si on fixe le chiffre de fin, il n'existe qu'une seule suite qui donne le motif des retenues voulu. En effet, à chaque fois il n'existe qu'une seule possibilité pour le chiffre qui précède. On a choisi 9 comme chiffre de départ mais cela aurait pu être n'importe quel chiffre :

Chiffres	8	6	3	7	4	9	9
Chiffres	8	6	3	7	4	9	8
Chiffres	8	6	3	7	4	8	7
Chiffres	8	6	3	7	4	8	6
Chiffres	8	6	3	6	3	7	5
Chiffres	8	6	3	6	3	7	4
Chiffres	8	6	3	6	3	6	3
Chiffres	8	6	3	6	3	6	2
Chiffres	8	6	3	6	2	5	1
Chiffres	8	6	3	6	2	5	0
Retenues	0	1	1	0	1	0	1

Toutes ces suites sont valides. On est à chaque fois parti d'un chiffre final différent. On remarque qu'à chaque fois, seuls les derniers termes changent.

En effet peu importe le chiffre de fin, il faut que l'on ait une retenue. L'avant dernier chiffre doit donc être 5, 6, 7, 8 ou 9. L'avant-avant dernier chiffre ne doit pas donner de retenues et donner 5, 6, 7, 8, 9.

Ainsi, les seules possibilités pour l'avant-dernier chiffre sont 2, 3 ou 4, etc... À chaque fois, on diminue le nombre de possibilités.

De ce fait, seuls les 4 derniers termes de ces différentes suites changent.

Pour choisir le chiffre tout à la fin, il faut prendre en compte que l'on veut que le motif des retenues soit périodique. Il faut donc que depuis le chiffre final, on revienne au 8 du début de la suite sans retenue (car la première retenue est 0).

Ainsi, le dernier chiffre doit être 4. Le seul motif possible est donc (8, 6, 3, 6, 3, 7, 4) pour ce motif des retenues.

Si un motif de retenues a une taille strictement supérieure à 4, alors les différents motifs de chiffres possibles commenceront tous par le même chiffre. Il n'y a donc qu'un chiffre final possible pour que le motif soit périodique. Par conséquent, un motif périodique de retenues de taille strictement supérieure à 4 ne peut être généré que par un unique motif de chiffres. □

Lemme 9. *La période minimale d'une colonne k doit être un diviseur de la période minimale de la colonne k+1.*

Démonstration.

D'après le lemme 8, il n'existe qu'un seul motif de chiffres qui puisse générer un certain motif de retenues qui se répète.

De ce fait, on ne peut avoir un motif de retenues qui se répète si le motif des chiffres qui le génère ne se répète pas. Par conséquent, la période minimale pour le motif des retenues issue d'une colonne est la même que la période minimale de cette colonne.

Or, d'après le lemme 7, la période minimale d'un motif doit être un multiple de la période minimale du motif des retenues générée par la colonne d'avant. Donc, chaque colonne doit avoir comme période minimale un multiple de la période minimale de la colonne précédente. □

Lemme 10. *Pour tout $k \in \mathbb{N}^*$, la période minimale de la colonne k est $4 \times 5^{k-1}$.*

Démonstration.

On sait, d'après le théorème 1, que $4 \times 5^{k-1}$ est la période minimale des k derniers chiffres. Ainsi, c'est un motif de répétition des chiffres de la colonne k, mais pas forcément le motif minimal pour la colonne k. Cependant, la taille de ce motif est un multiple de celle du motif minimal.

Par conséquent, la période minimale de la colonne k est un diviseur $4 \times 5^{k-1}$. Cependant, cela ne peut pas être n'importe quel diviseur. En effet, la période minimale de répétition pour les $k-1$ derniers chiffres est de $4 \times 5^{k-2}$.

Si la période minimale pour les chiffres de la colonne k était également de $4 \times 5^{k-2}$, cela voudrait dire que la période minimale pour les k derniers chiffres est de $4 \times 5^{k-2}$. Cela n'est pas possible puisque la période minimale pour les k derniers chiffres est de $4 \times 5^{k-1}$.

Si l'on généralise, cela veut dire que la période minimale de la colonne k ne peut pas être un diviseur de $4 \times 5^{k-2}$.

La période minimale de la colonne k doit être un diviseur $4 \times 5^{k-1}$, mais ne peut être un diviseur de $4 \times 5^{k-2}$. Les seuls nombres qui remplissent ces deux conditions sont 5^{k-1}, $2 \times 5^{k-1}$, et $4 \times 5^{k-1}$.

D'après le lemme 9, la période minimale d'une colonne doit être un multiple de celle de la colonne précédente. Étant donné que la colonne des unités a une période de taille 4, cela signifie que la période minimale de la colonne k doit être un multiple de 4.

On en conclut que $4 \times 5^{k-1}$ est la période minimale de la colonne k. □

Théoreme 2. *En base 10, la période minimale des chiffres de la colonne k est de taille* $4 \times 5^{k-1}$. *Ce motif ne commence qu'à partir du rang k.*

Démonstration.

Le lemme 10 et le lemme 6 prouvent les deux parties de notre théorème.

□

5 Statistiques

On va désormais analyser la fréquence d'apparition de chaque chiffre dans le motif d'une colonne.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$r_{1,n}$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
$C_{2,n}$	0	0	1	3	6	2	5	1	2	4	9	9	8	6	3	7	4	8	7	5

Grâce au motif des retenues, on sait que $C_{2,3} \equiv 2C_{2,2}$ [10], $C_{2,4} \equiv 2(2C_{2,2}) + 1$ [10] et donc

$$C_{2,6} \equiv 2(2(2(2C_{2,2}) + 1) + 1) \ [10].$$

Par conséquent, $C_{2,6} \equiv 16\, C_{2,2} + 6$ [10]. On peut ajouter à cela que le motif des retenues se répète avec une période de 4. Ainsi, on passe par les mêmes retenues au même moment pour aller de $C_{2,6}$ à $C_{2,10}$ que pour aller de $C_{2,2}$ à $C_{2,6}$. On en déduit que $C_{2,10} \equiv 2(2(2(2C_{2,6}) + 1) + 1)$ [10] $\equiv 16\, C_{2,6} + 6$ [10].

De manière plus générale, si $n = 4l + 2$, on a $C_{2,n+4} \equiv 2(2(2(2C_{2,n}) + 1) + 1)[10]$.

Donc, pour $n = 4l + 2$, $C_{2,n+4} \equiv 16\, C_{2,n} + 6[10]$. Étant donné qu'on est modulo 10, cela veut dire que $C_{2,n+4} \equiv 6\, C_{2,n} + 6$ [10].

Cependant, cette suite ne couvre que le quart des chiffres de la colonne des dizaines. On va donc utiliser la même méthode pour avoir les suites correspondant aux autres chiffres. Pour tout entier l strictement positif,

$$
\begin{aligned}
C_{2,4l+2} &\equiv 6C_{2,4(l-1)+2} + 6\ [10] \\
C_{2,4l+3} &\equiv 2(2(2(2C_{2,4(l-1)+3} + 1) + 1))\ [10] \\
&\equiv 16\, C_{2,4(l-1)+3} + 12\ [10] \equiv 6\, C_{2,4(l-1)+3} + 2\ [10] \\
C_{2,4l} &\equiv 6\, C_{2,4(l-1)} + 9\ [10] \\
C_{2,4l+1} &\equiv 6\, C_{2,4(l-1)+1} + 3\ [10].
\end{aligned}
$$

Définition :

Sous-suite : On appelle sous-suite chacune de ces suites arithmético-géométriques modulo 10, qui à 4 nous permettent de retrouver la suite principale.

On peut analyser indépendamment chacune de ces suites. Pour que notre démarche soit bien claire, on va colorer dans notre suite d'origine chaque nombre en fonction de la sous-suite à laquelle elle appartient :

n	0	1	2	3	4	5
$U_{n+1} \equiv 6U_n + 6[10]$	0	6	2	8	4	0
$V_{n+1} \equiv 6V_n + 2[10]$	0	2	4	6	8	0
$W_{n+1} \equiv 6W_n + 9[10]$	1	5	9	3	7	1
$X_{n+1} \equiv 6X_n + 3[10]$	3	1	9	7	5	3

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$r_{1,n}$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
$C_{2,n}$	0	0	1	3	6	2	5	1	2	4	9	9	8	6	3	7	4	8	7	5	0

On retrouve bien que la période pour les dizaines est de 20. En effet, la première sous-suite (bleue) est périodique avec une période de 5. Étant donné que cette sous-suite correspond à 1 chiffre sur 4, cela signifie que $C_{2,2} = C_{2,22}$.

Or, la période des retenues issue de la colonne précédente est de taille 4.

Ainsi, si $C_{2,2} = C_{2,22}$, alors $C_{2,3} = C_{2,23}$ puisque l'on a une retenue de 0 dans les 2 cas.

De manière générale, pour tout $t \in \mathbb{N}$, $C_{2,2+t} = C_{2,22+t}$ car on aura les mêmes retenues au même moments pour les deux nombres.

On a donc bien un motif de taille 20.

Si l'on généralise cette idée, on a un motif de répétition dès qu'un nombre se répète dans une sous-suite. En effet, nos sous-suites correspondent à 1 chiffre sur 4, et il suffit qu'on ait 2 fois le même nombre, espacés d'un multiple de 4 pour que tous les nombres qui suivent soient également les mêmes.

Ici, on voit qu'on a $X_0 = 3$ (5). En pratique, pour l'étude de la sous-suite (X_n), X_0 n'a pas d'importance. En effet, la sous-suite est périodique : on part de 3 pour revenir à 3. On aurait donc pu commencer à n'importe quel nombre impair, et l'on aurait eu la même suite décalée.

Néanmoins, il n'aurait pas été sensé de partir d'un nombre pair. En effet, étant donné que le motif des retenues a une période de 4 et que notre sous-suite couvre 1 chiffre sur 4, elle est toujours au même endroit dans le motif des retenues.

Ici, chacun des nombres de notre sous-suite correspond à un endroit où l'on a une retenue, tous les nombres sont donc impairs. On peut d'ailleurs le voir du fait que "+**3**" est impair.

N'importe quel chiffre au rang 0 qui est impair aurait donc fonctionné. Ainsi, pour des raisons pratiques, lorsqu'on étudiera les sous-suites on choisira 1 comme chiffre au rang 0 si la sous-suite correspond à des chiffres où l'on a des retenues, et 0 sinon :

n	0	1	2	3	4	5
$U_{n+1} \equiv 6U_n + 2[10]$	0	2	4	6	8	0
$V_{n+1} \equiv 6U_n + 3[10]$	1	9	7	5	3	1
$W_{n+1} \equiv 6U_n + 6[10]$	0	6	2	8	4	0
$X_{n+1} \equiv 6U_n + 9[10]$	1	5	9	3	7	1

À l'aide de tous ces éléments, on peut expliquer pourquoi la colonne des dizaines contient chaque chiffre à la même fréquence. Chaque sous-suite contient soit tous les chiffres pairs, soit tous les chiffres impairs possibles en base 10, et l'on a autant de sous-suites avec des nombres pairs que de sous-suites avec des nombres impairs.

Ici, le motif des retenues est de taille 4, donc on a créé 4 sous-suites qui avaient toutes la forme : $C_{2,n+4} \equiv 2^4 C_{2,n} + b$ [10] avec $0 \leq b < 10$.

On peut généraliser cela aux autres colonnes.

Si l'on prenait la colonne des centaines, on aurait un motif des retenues de 20 étant donné que le motif des chiffres pour les dizaines est de 20. On devrait donc faire 20 sous-suites de la forme $C_{3,n+20} = 2^{20} C_{3,n} + b$ [10] avec $0 \leq b < 10$. Chaque sous-suite correspondrait à 1 chiffre sur 20 de la colonne des centaines.

Or, $2^{20} \equiv 6$ [10], donc pour la colonne des centaines, on aurait les mêmes sous-suites de la forme $U_{n+1} \equiv 6\, U_n + b$ [10] avec $0 \leq b < 10$.

En réalité, toutes les colonnes sauf la première ont un motif des retenues qui est un multiple de 4. Or $2^{4k} = 16^k$. Mais $6 \times 6 \equiv 36 \equiv 6$ [10], donc 16 à n'importe quelle puissance finira par 6 en base 10. Ainsi $2^{4k} \equiv 6[10]$.

Par conséquent, pour toute colonne k avec $k \neq 1$, on a des sous-suites de la forme $C_{k,n+4\times 5^{k-2}} \equiv 6C_{k,n} + b[10]$ avec $0 \leq b < 10$.

On peut donc faire un tableau avec tous les b possibles :

n	0	1	2	3	4	5
$U_{n+1} \equiv 6U_n[10]$	0	0	0	0	0	0
$U_{n+1} \equiv 6U_n + 1[10]$	1	7	3	9	5	1
$U_{n+1} \equiv 6U_n + 2[10]$	0	2	4	6	8	0
$U_{n+1} \equiv 6U_n + 3[10]$	1	9	7	5	3	1
$U_{n+1} \equiv 6U_n + 4[10]$	0	4	8	2	6	0
$U_{n+1} \equiv 6U_n + 5[10]$	1	1	1	1	1	1
$U_{n+1} \equiv 6U_n + 6[10]$	0	6	2	8	4	0
$U_{n+1} \equiv 6U_n + 7[10]$	1	3	5	7	9	1
$U_{n+1} \equiv 6U_n + 8[10]$	0	8	6	4	2	0
$U_{n+1} \equiv 6U_n + 9[10]$	1	5	9	3	7	1

Pour toutes les sous-suites possibles, on passe soit par tous les nombres pairs/impairs possibles, soit on reste sur le nombre de départ. Le deuxième comportement n'est pas spécifique au fait qu'on parte de 1 ou 0.

Pour $U_{n+1} \equiv 6\ U_n\ [10]$:

Si U_0 est n'importe quel nombre pair $n = 2k$, alors $U_1 \equiv 6\ U_0 \equiv 6 \times 2k \equiv 12k \equiv 2k\ [10]$, donc $U_0 \equiv U_1\ [10]$

Pour $U_{n+1} \equiv 6U_n + 5[10]$:

Si U_0 est n'importe quel nombre impair $n = 2k+1$, alors $U_1 \equiv 6\ U_0 + 5 \equiv 6(2k+1)+5 \equiv 12k+11 \equiv 2k+1\ [10]$, donc $U_0 \equiv U_1\ [10]$

Si l'on reprend l'exemple de la colonne des centaines cela veut dire qu'on a deux possibilités. Si une sous-suite a une période de 1, cela veut dire que deux chiffres espacés de 20 seront les mêmes.

Or, la période des retenues issue de la colonne d'avant est de 20. Dans ce cas, la période minimale de la colonne des centaines serait donc de 20. Cela n'est pas possible puisqu'on a prouvé que la taille du motif était multipliée par 5 à chaque fois qu'on se décalait d'une colonne. Autrement dit la taille du motif de la colonne des centaines est de 100.

On doit donc avoir uniquement des sous-suites de période 5. Dans ces dernières, il y a la même fréquence d'apparition pour tous les nombres pairs/impairs.

Il ne nous reste plus qu'à prouver qu'il y a autant de sous-suites avec des nombres pairs que de sous-suites avec des nombres impairs.

Comme dit précédemment, une sous-suite contient des nombres impairs si elle est à un endroit du motif des retenues où il y a 1, sinon elle contient des nombres pairs. Pour prouver qu'il y a autant de sous-suites avec des nombres pairs que de sous-suites avec des nombres impairs, il suffit donc de prouver que le motif des retenues que l'on reçoit contient autant de 1 que de 0.

On a montré précédemment que lorsque le chiffre de la colonne précédente est 5, 6, 7, 8, ou 9, l'on a une retenue. Si le chiffre est 0, 1, 2, 3 ou 4, on n'en a pas. Étant donné que dans la colonne des dizaines chaque chiffre apparaît le même nombre fois, le motif des retenues que reçoit la colonne des centaines contient bien autant de 1 que 0.

Ainsi, chaque chiffre apparaît le même nombre de fois dans la colonne des centaines. On peut généraliser ce raisonnement à toutes les colonnes à l'aide d'une récurrence.

Initialisation : La colonne des dizaines contient chaque chiffre le même nombre de fois

Hérédité :

Prenons la colonne n, avec $n \geq 2$ (6). D'après ce qu'on a démontré dans la partie "Taille des motifs", la taille du motif de la colonne n est un multiple de 4. Donc, la taille du motif des retenues que reçoit la colonne $n+1$ est un multiple de 4.

Ainsi, notre colonne $n+1$ peut être décomposée en sous-suites de la forme $U_{n+1} \equiv 6U_n + b[10]$ avec $0 \leq b < 10$. Étant donné qu'on a démontré que la taille du motif de la colonne n est 5 fois celle de la colonne n, on n'aura que des sous-suites de période 5. Par conséquent, chaque sous-suite passera par tous les nombres pairs ou impairs possibles.

Par hypothèse de récurrence, dans la colonne n, chaque chiffre apparaît le même nombre de fois. Ainsi, le motif des retenues que reçoit la colonne $n+1$ contient autant de 1 que de 0. On a donc autant de sous-suite avec des nombres pairs que de sous-suites avec des nombres impairs dans la colonne $n+1$. Chaque chiffre apparaît donc le même nombre de fois dans le motif de la colonne n+1.

En conclusion, on a démontré le théorème 3.

6 Vers une généralisation

Nous avons démontré nos trois théorèmes pour les puissances de 2 en base 10. L'on peut pour finir se demander à quel point nos méthodes pourraient être utilisées pour d'autres puissances et d'autres bases. La première étape de notre raisonnement a été de prouver que pour analyser les motifs en base 10, on pouvait les analyser en base 2 et en base 5. Notre démonstration est généralisable à toute base tant qu'on la décompose en facteurs qui sont 2 à 2 des nombres premiers entre-eux.

Dans notre cas l'intérêt était qu'en base 5 les puissances de 2 commencent dès le rang 2^0 (7). On le sait car on a démontré que peu importe k, on peut trouver un entier naturel n, tel que $2^n \equiv 1[5^k]$. On a pu prouver cela car en base 5, $2^{20} = ...301$. À partir de là, on savait que $(2^{20})^5 = ...3001$, etc... À l'inverse, en base 10, on ne retrouve jamais de 1 au chiffre des unités sauf pour 2^0.

En réalité, si la base et la puissance (8) sont premières entre elles, on aura de nouveau un 1 au chiffre des unités.

Soit $a \in \mathbb{N}^*$, la puissance que l'on analyse et $b \in \mathbb{N}^* \setminus \{1\}$, la base. On suppose que a et b sont premiers entre eux.

Il n'y a qu'un nombre fini de possibilités pour ce à quoi a^n peut être congru modulo b. Par conséquent il existe n_1 et n_2 tels que $n_1 < n_2$, et $a^{n_1} \equiv a^{n_2}\ [b]$, c'est-à-dire $b \mid (a^{n_1} - a^{n_2}) = a^{n_1}(1 - a^{n_2-n_1})$.

a^{n_1} et b sont premiers entre eux, donc d'après le théorème de Gauss, $b \mid (1 - a^{n_2-n_1})$, d'où $a^{n_2-n_1} \equiv 1\ [b]$.

Maintenant que l'on sait que si la base et la puissance sont premières entre elles, on va de nouveau avoir une puissance qui finit par 1, il faut qu'on en ait une qui finisse par 01. En effet, la démonstration qui montre que l'on gagne un 0 lorsque l'on met un nombre qui finit par "...01" à puissance de la base ne s'applique que si l'on a déjà un 0. Ainsi, on a la preuve que $2^{20} = ...301 \implies 2^{100} = ...3001$, mais l'on n'a pas la preuve que $2^5 = ...31 \implies 2^{20} = ...301$. Pour ce cas précis, il va falloir modifier légèrement notre démonstration.

En reprenant les mêmes notations que pour notre première démonstration :
si $n \equiv a\beta^2 + b\beta + 1\ [\beta^3]$ alors, notre propriété $P(k)$ devient

$$n^k \equiv ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\ [\beta^3]\ \textit{pour tout}\ \ k \in \mathbb{N}\ (9).$$

Initialisation :
$n^0 = 1$ et $a \times 0 \times \beta^{p+1} + \frac{-0\times 1}{2}b^2\beta^2 + b \times 0 \times \beta^p + 1 = 1$.
Donc $P(0)$ est vraie.

Hérédité :
Soit $k \in \mathbb{N}$. On suppose que $P(k)$ est vraie.
On a par hypothèse de récurrence

$$\begin{aligned}
n^k &\equiv ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\ [\beta^3] \\
n^{k+1} &\equiv (a\beta^2 + b\beta + 1)\left(ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\right)\ [\beta^3] \\
&\equiv ka^2\beta^4 + \frac{k(k-1)}{2}ab^2\beta^4 + akb\beta^3 + a\beta^2 \\
&\quad + kab\beta^3 + \frac{k(k-1)}{2}b^3\beta^3 + kb^2\beta^2 + b\beta \\
&\quad + ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\ [\beta^3] \\
&\equiv a\beta^2 + kb^2\beta^2 + b\beta + ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\ [\beta^3] \\
&\equiv a\beta^2(k+1) + b\beta(k+1) + b^2\beta^2\left(k + \frac{k(k-1)}{2}\right) + 1\ [\beta^3] \\
&\equiv a\beta^2(k+1) + b\beta(k+1) + b^2\beta^2\ \frac{((k+1)-1)(k+1)}{2} + 1\ [\beta^3].
\end{aligned}$$

On en déduit que $P(k)$ est héréditaire.

Conclusion :
Si $n \equiv a\beta^2 + b\beta + 1\ [\beta^3]$, alors pour tout $k \in \mathbb{N}$, $n^k \equiv ka\beta^2 + \frac{k(k-1)}{2}b^2\beta^2 + kb\beta + 1\ [\beta^3]$

Donc, pour $k = \beta$,

$$\begin{aligned}
n^\beta &\equiv a\beta^3 + \frac{\beta(\beta-1)}{2}b^2\beta^2 + b\beta^2 + 1\ [\beta^3] \\
&\equiv \frac{\beta(\beta-1)}{2}b^2\beta^2 + b\beta^2 + 1\ [\beta^3].
\end{aligned}$$

Ainsi, si la base est impaire, $\beta = 2k_2 + 1$, avec $k_2 \in \mathbb{N}$, donc

$$\begin{aligned} n^\beta &\equiv \frac{\beta(2k_2+1-1)}{2} b^2\beta^2 + b\beta^2 + 1 \; [\beta^3] \\ &\equiv \frac{\beta \times 2k_2}{2} b^2\beta^2 + b\beta^2 + 1 \; [\beta^3] \\ &\equiv k_2 b^2 \beta^3 + b\beta^2 + 1 \; [\beta^3] \\ &\equiv b\beta^2 + 1 \; [\beta^3]. \end{aligned}$$

Ainsi, $2^5 = ...31 \implies 2^{20} = ...301$ puisque la base est impaire.

Néanmoins si la base est paire on n'est pas sûr de pouvoir retirer le terme $\frac{\beta(\beta-1)}{2} b^2\beta^2$ (10).

Ainsi, si la base est paire, on sait que l'on va gagner un 0, mais l'on n'a pas de garantie que le chiffre d'avant reste le même. Par exemple en base 4, $31^4 = ...101$. On gagne un 0 mais le 3 se transforme en 1. On peut même gagner plusieurs 0s d'un coup. Par exemple, en base 2, $11^2 = 1001$.

Si l'on résume, si la puissance et la base sont premières entre elles, on aura une autre puissance que a^0 où le chiffre des unités est 1. Si l'on prend ce nombre puissance la base, on aura un nombre qui finit par "01", mais on pourra avoir gagné plus d'un 0 si la base est paire.

Néanmoins, après cela on ne gagnera plus qu'un 0 à chaque fois que l'on fait notre nombre puissance la base (11).

Ainsi, on conjecture que les motifs des premières colonnes seront parfois quelque peu chaotiques, mais après cela, la période sera multipliée par un nombre constant lorsqu'on se décale d'une colonne vers la gauche.

Une simple analyse avec un programme python des puissances de 3 en 10 suggère que la fréquence d'apparition de chaque chiffre ne semble pas être la même dans le motif de chaque colonne. On conjecture que c'est une propriété qui ne s'applique qu'à certaines puissances et certaines bases.

Néanmoins, nous pensons que la méthode de décomposer le motif d'une colonne en sous-suites devrait être applicable à d'autres puissances et d'autres bases.

Notes d'édition

(1) Pour les lecteurs qui ne la connaissent pas, si a, b et c sont trois entiers, c étant non nul, la notation $a \equiv b\ [c]$ se lit "a est congru à b modulo c" et signifie que $a - b$ est un multiple de c. En particulier, $a \equiv 0\ [c]$ si et seulement si a est multiple de c, que l'on note aussi $c \mid a$.
La suite de l'article utilise le fait que la relation de congruence modulo c est compatible avec l'addition et la multiplication : si $a_1 \equiv b_1\ [c]$ et $a_2 \equiv b_2\ [c]$, alors $a_1 + a_2 \equiv b_1 + b_2\ [c]$ et $a_1 a_2 \equiv b_1 b_2\ [c]$.

(2) Il semble à l'éditeur que c'est plutôt cette contraposée qui peut se montrer directement : si lon retrouve les k derniers chiffres du rang 0 a un autre rang n, c'est-à-dire $2^n \equiv 1\ [5^k]$, alors on a aussi $2^{n+l} = 2^n \times 2^l \equiv 2^l\ [5^k]$ pour tout entier $l \geq 0$ et donc la suite est périodique à partir du rang 0.

(3) Il sagit ici de la plus petite période (la période minimale définie plus loin). Tous ses multiples sont également des périodes.

(4) Pour préciser, la période $4 \times 5^{k-1}$ des k derniers chiffres est aussi *une* période des chiffres de la colonne k; a priori ce n'est pas nécessairement leur période minimale, mais c'est un multiple de celle-ci. Si le motif des chiffres de la colonne k se répétait à partir d'un rang antérieur à k, on devrait retrouver le chiffre du rang $k-1$ au rang $4 \times 5^{k-1} + k - 1$ dans cette colonne.

(5) Rappelons que (X_n) est la quatrième sous-suite.

(6) On suppose que cette colonne contient chaque chiffre le même nombre de fois.

(7) C'est-à-dire qu'en base 5 les premiers chiffres des puissances de 2 sont périodiques dès le rang 1.

(8) La "puissance" désigne ici le nombre dont on regarde les puissances.

(9) Remarquons que $k(k-1)/2$ est bien toujours un entier car soit k, soit $k-1$ est pair.

(10) En effet, si β est impair $\beta(\beta-1)/2$ est multiple de β et donc $\beta^3(\beta-1)/2$ est multiple de β^3, mais ce n'est plus le cas si β est pair.

(11) Cela a été prouvé dans le lemme 3.