NOMBRES RIMANT AVEC LEUR CARRE (COMPLEMENTS)

Julien Moreau

Ce texte fait suite à l'article « nombres rimant avec leur carré » paru dans le BV n° 484. Rappelons-en les points essentiels :

On étudie le problème (P_n) : *un entier strictement positif* n *étant donné, trouver les entiers naturels dont l'écriture décimale a mêmes* n *derniers chiffres que celle de leur carré.*

Cela revient à résoudre l'équation (P'_n) : $x^2 \equiv x \pmod{10^n}$. *Elle admet, modulo* 10^n, *quatre solutions. Ce sont 0, 1 et deux nombres* u_n *et* v_n *que l'on détermine comme suit :*

▪ *ils appartiennent à* $[\,0\,, 10^n\,[$ *;*

▪ $u_0 = 5$ *et, pour tout* n, $u_{n+1} \equiv {u_n}^2 \pmod{10^{n+1}}$ *;*

▪ *pour tout n,* $u_n + v_n = 10^n + 1$.

Ce problème est susceptible d'être prolongé dans différentes directions. Nous en donnons trois ci-après.

1. Nombres rimant avec leur puissance q-ième

Tout nombre vérifiant $x^2 \equiv x \pmod{10^n}$ vérifie pour tout entier $q \geq 2$, $x^q \equiv x^{q-1}$ et finalement $x^q \equiv x$. Il en résulte que, pour toute solution x de (P_n), c'est-à-dire pour tout entier naturel ayant mêmes n derniers chiffres que son carré, toutes les puissances de x ont mêmes n derniers chiffres que x.

On peut alors se poser la question suivante : q étant donné, *y a-t-il, en dehors des solutions de* (P_n), *d'autres nombres* x ($x \in \boldsymbol{N}$) *tels que les n derniers chiffres de l'écriture décimale de* x^q *soient les mêmes que ceux de x ?*

Nous n'allons pas étudier le cas général, mais seulement les deux cas $q = 3$ et $q = 4$. Voyons d'abord le second, qui peut être rapidement expédié.

Nombres rimant avec leur puissance quatrième

Le problème se ramène à la résolution dans **Z** de $x^4 - x \equiv 0 \pmod{10^n}$,
autrement dit $x\,(x-1)\,(x^2 + x + 1) \equiv 0 \pmod{10^n}$.

Mais, quelle que soit la parité de x, le nombre $x^2 + x + 1$ est impair ; il n'est de plus jamais divisible par 5 (regarder ce qui se passe selon que x vaut 0, ± 1 ou ± 2 modulo 5). Étant premier avec 2 et 5, il est premier avec 10, donc avec 10^n. La congruence ci-dessus se ramène donc à $x(x-1) \equiv 0 \pmod{10^n}$, autrement dit $x^2 \equiv x \pmod{10^n}$. Nous pouvons conclure :

Un nombre rime avec sa puissance quatrième si et seulement si il rime avec son carré.

N.B. : Des raisonnements analogues montrent aisément que $x^7 \equiv x \pmod{10^n}$ équivaut à $x^3 \equiv x \pmod{10^n}$ et que $x^8 \equiv x \pmod{10^n}$ équivaut à $x^2 \equiv x \pmod{10^n}$.

Nombres rimant avec leur cube

Quels sont les nombres x ($x \in \mathbb{N}$) *tels que les n derniers chiffres de l'écriture décimale de* x^3 *soient les mêmes que ceux de x ?*

Ce problème (Q_n) se ramène à la résolution de l'équation

$x^3 \equiv x \pmod{10^n}$, c'est-à-dire

$$(E_n) \qquad x(x-1)(x+1) \equiv 0 \pmod{10^n}.$$

Solutions immédiates

Si l'un des trois facteurs du premier membre de (E_n) est nul modulo 10^n, on obtient aussitôt les solutions : nombres finissant par 000…00, 000…01, 999…99.

Si l'un des deux produits $x(x-1)$ ou $x(x+1)$ est nul modulo 10^n, le problème est vite résolu. En effet $x(x-1) \equiv 0 \pmod{10^n}$ n'est autre que l'équation (P'_n), dont nous connaissons les solutions non triviales u_n et v_n.

Quant à $x(x+1) \equiv 0 \pmod{10^n}$, si l'on pose $x+1 = y$, cette équation devient $y(y-1) \equiv 0 \pmod{10^n}$. On retombe sur le cas que nous venons de traiter. Les solutions non triviales sont donc $u_n - 1$ et $v_n - 1$.

Solutions non immédiates

Nous restons en présence de deux types de situations :

▪ (S_1) : $(x-1)(x+1) \equiv 0 \pmod{10^n}$ sans qu'aucun des facteurs soit nul modulo 10^n.

▪ (S_2) : $x(x-1)(x+1) \equiv 0 \pmod{10^n}$ sans qu'aucun des produits deux à deux soit nul modulo 10^n.

Étude de (S_1) : $(x-1)(x+1) \equiv 0 \pmod{10^n}$

Deux remarques préalables :

▪ si x est solution, $-x$ l'est aussi.

▪ toute solution x est impaire, ce qui entraîne que $x-1$ et $x+1$ ne sont pas premiers entre deux, leur pgcd étant 2.

Le fait que 2^n divise $(x-1)(x+1)$ implique donc que l'un des deux facteurs soit divisible par 2, mais non par 4, et l'autre par 2^{n-1}.

On peut supposer que c'est $x+1$ qui est divisible par 2, mais non par 4, l'autre cas s'en déduisant par changement de x en $-x$. Posons $x = 2z-1$; z est donc impair. L'équation de départ devient :

$$4z(z-1) \equiv 0 \pmod{10^n}$$

2^{n-2} divise $z(z-1)$ et est premier avec z, donc il divise $z-1$. Il nous faut donc chercher z tel que 2^{n-2} divise $z-1$ et 5^n divise z ou $z-1$.

Dire que 2^{n-2} et 5^n divisent tous deux $z-1$ revient à dire que z est de la forme $25k.10^{n-2}+1$, donc que $x = 5k.10^{n-1}+1$, ce qui nous amène pour solutions les nombres finissant par 000… 01, déjà connus, et ceux finissant par 500… 01.

Reste à voir la situation où 2^{n-2} divise $z-1$ et 5^n divise z. Nous connaissons déjà un nombre satisfaisant ces conditions, à savoir u_n. Cherchons les autres : z répond à la question si et seulement si 2^{n-2} et 5^n divisent $z-u_n$, autrement dit si 25.10^{n-2} divise $z-u_n$, c'est-à-dire encore si z est de la forme $u_n+\gamma 25.10^{n-2}$ avec $\gamma \in$ **Z**. Finalement il est nécessaire et suffisant que

$$x = 2u_n - 1 + 5\gamma.10^{n-1},$$

ce qui donne deux valeurs possibles de x modulo 10^n, à savoir $2u_n-1$ et $2u_n-1+5.10^{n-1}$, qu'il faut éventuellement ramener dans [0, 10^n [en leur retranchant si nécessaire 10^n.

Il nous faut ajouter à ces solutions celles qui en sont déduites par changement de x en $-x$, modulo 10^n bien sûr. De la solution 500… 01 on déduit la solution 499…99. De la solution $x = 2u_n-1+5\gamma.10^{n-1}$ on déduit, compte tenu de la relation entre u_n et v_n, la solution $x = 2v_n-1+5\lambda.10^{n-1}$, ce qui donne deux valeurs modulo 10^n : $2v_n-1$ et $2v_n-1+5.10^{n-1}$, qu'il faut éventuellement ramener dans [0, 10^n [en leur retranchant si besoin est 10^n.

Étude de (S_2) :

Nous voulons ici trouver les x tels que $x(x-1)(x+1) \equiv 0 \pmod{10^n}$ sans qu'aucun des produits deux à deux ne soit nul modulo 10^n.

Observons d'abord qu'un seul des trois facteurs est divisible par 5 ; il est alors divisible par 5^n.

Si x est pair, $x-1$ et $x+1$ sont impairs, donc 2^n divise x. Ainsi ou bien x est nul modulo 10^n, ou bien son produit par $x-1$ ou $x+1$ est nul modulo 10^n, deux cas déjà étudiés, que nous avons ici exclus par hypothèse.

Reste à étudier le cas où x est impair. Alors $x-1$ et $x+1$ sont pairs (leur pgcd est alors évidemment 2) et 2^n divise $(x-1)(x+1)$. Le cas où 5^n divise aussi ce produit est exclu, car alors $(x-1)(x+1)$ serait nul modulo 10^n, cas que nous avons écarté.

Finalement, donc, 5^n divise x et 2^n divise $(x-1)(x+1)$ sans diviser l'un des deux facteurs. La seconde proposition signifie que l'un des deux nombres $x-1$ et $x+1$ est divisible par 2, mais non par 4, et l'autre par 2^{n-1}, mais pas par 2^n. En changeant éventuellement x en $-x$, on peut toujours se ramener au cas suivant :

$$5^n \text{ divise } x,\ 2^{n-1} \text{ divise } x-1.$$

Le raisonnement est du même type que celui fait pour (S_1) **.** Le nombre u_n satisfait ces conditions. Un nombre x les satisfera si et seulement si 5^n et 2^{n-1} (mais pas 2^n) divisent $x-u_n$, donc si x est du type $u_n+5\,\mu.10^{n-1}$ avec μ impair. Finalement l'unique solution correspondante de (Q_n) est celui des nombres $u_n+5.10^{n-1}$ et $u_n-5.10^{n-1}$ qui est dans]0, 10^n [.

Il faut évidemment y adjoindre ce qu'on obtient en changeant x en $-x$, c'est-à-dire, selon les cas, $5.10^{n-1}-u_n$ ou $15.10^{n-1}-u_n$ (c'est-à-dire $v_n+5.10^{n-1}-1$).

Récapitulation

Nous avons donc trouvé :

▪ des solutions triviales, les nombres finissant par

000…0, 000… 01, 999… 99, 500… 01 , 499… 99.

▪ les nombres ayant mêmes n derniers chiffres que :

u_n, u_n-1, $2\,u_n-1$, $2\,u_n-1+5.10^{n-1}$, $u_n+5.10^{n-1}$.

▪ les nombres (modulo 10^n, ce sont les opposés des précédents) ayant mêmes n derniers chiffres que :

v_n-1, v_n, $2\,v_n-1$, $2\,v_n-1+5.10^{n-1}$, $v_n+5.10^{n-1}-1$.

Exemples

Nous donnons ici les solutions pour n allant de 2 à 4.

▪ 00 ; 01 ; 24 ; 25 ; 49 ; 51 ; 75 ; 76 ; 99

▪ 000 ; 001 ; 125 ; 249 ; 251 ; 375 ; 376 ; 499 ; 501 ; 624 ; 625 ; 749 ; 751 ; 875 ; 999.

▪ 0000 ; 0001 ; 0624 ; 0625 ; 1249 ; 3751 ; 4375 ; 4999 ; 5001 ; 6249 ; 5625 ; 8751 ; 9375 ; 9376 ; 9999.

Puisque, pour $n = 3$, les quinze solutions sont distinctes, on peur affirmer qu'il en est ainsi pour tout $n \geq 3$.

N.B. : On voit immédiatement par récurrence que, si $x^3 \equiv x \pmod{10^n}$, alors, pour tout q entier naturel, $x^{2q+1} \equiv x \pmod{10^n}$. Si x rime avec son cube, il rime avec toutes ses puissances impaires.

2. Nombres rimant dans une base donnée avec leur carré

Une base B étant choisie, il s'agit de trouver les nombres x tels que $x^2 \equiv x \pmod{B^n}$.

Si B est une puissance d'un nombre premier, soit $B = b^h$, le problème est trivial. Puisque x et $x-1$ sont premiers entre eux, la congruence $x(x-1) \equiv 0 \pmod{b^{nh}}$ se ramène en effet à :

$$x \equiv 0 \pmod{b^{nh}} \quad \text{ou} \quad x-1 \equiv 0 \pmod{b^{nh}}.$$

Il n'y a d'autre solution que les nombres dont l'écriture en base B finit par 0…000 ou 0…001. Notons que c'est le cas de deux bases d'usage courant, 2 et 16.

Cas général

Pour simplifier les écritures, nous nous placerons dans le cas où $B = a^h b^k c^l$, où a, b, c sont premiers distincts (mais les résultats ont une portée générale). Dire que B^n divise $x(x-1)$ revient à dire que chacun des facteurs a^{nh}, b^{nk}, c^{nl} divise $x(x-1)$. Puisque x et $x-1$ sont premiers entre eux, cela revient aussi à dire que chacun des facteurs a^{nh}, b^{nk}, c^{nl} divise un des deux nombres x et $x-1$ (il est alors premier avec l'autre).

La congruence $x(x-1) \equiv 0 \pmod{a^{nh} b^{nk} c^{nl}}$ équivaut donc au système :

$$(\Sigma) \qquad \begin{cases} x \equiv \varepsilon \pmod{a^{nh}} \\ x \equiv \varepsilon' \pmod{b^{nk}} \\ x \equiv \varepsilon'' \pmod{c^{nl}} \end{cases}$$

avec ε, ε', ε'' valant 0 ou 1 indépendamment les uns des autres.

On est donc ramené à résoudre huit systèmes de trois congruences linéaires modulo trois nombres premiers entre eux deux à deux. On sait (d'après le « théorème chinois[1] ») qu'un tel système a une solution, unique modulo le produit des trois nombres (ici : modulo $a^{nh} b^{nk} c^{nl}$, autrement dit modulo B^n).

Il y a donc, dans le cas envisagé, huit solutions au problème posé, donc six autres que les solutions triviales 0…000 et 0…001.

[1] La démonstration de ce théorème est faisable sans sortir du programme de Terminale S.

Lorsque B a r facteurs premiers distincts, le problème a, en incluant les deux solutions triviales, 2^r solutions.

3. Entiers décadiques

(L'idée de ce paragraphe est de Jean-Pierre Friedelmeyer)

Nous avons été amenés, dans la recherche des nombres dont l'écriture décimale a mêmes n derniers chiffres que celle de son carré, à envisager les deux suites illimitées de chiffres …… 59918212890625 (pour avoir u_n, on prend les n chiffres de droite) et …… 40081787109376 (pour avoir v_n, on prend les n chiffres de droite).

Il s'agit de donner un sens à ces suites de chiffres écrites à rebours. Appelons $\mathbf{Z}_{10}$ l'ensemble des suites $\alpha_0, \alpha_1, \dots, \alpha_n, \dots$ d'entiers appartenant à [0 , 9], que nous écrirons $\dots\alpha_n\ \alpha_{n-1}\dots\alpha_1\ \alpha_0$. Une telle suite sera appelée un entier *décadique* ou *10-adique*.

Lorsque tous les α_n sont nuls à partir d'un certain rang, cet entier $\dots 000\,\alpha_m\dots\alpha_1\ \alpha_0$ sera identifié à l'entier naturel $\overline{\alpha_m\dots\alpha_1\ \alpha_0}$, la barre indiquant qu'il s'agit d'une écriture décimale et non d'un produit. Ainsi, par exemple, …00001 est identifié à 1.

On peut de façon naturelle mettre dans $\mathbf{Z}_{10}$ une addition et une multiplication prolongeant celle des entiers usuels : il suffit de poser l'opération comme d'habitude et de continuer indéfiniment.

Précisons les choses dans le cas le plus délicat, celui de la multiplication. Soit $X = \dots\alpha_n\dots\alpha_1\ \alpha_0$ et $Y = \dots\beta_n\dots\beta_1\ \beta_0$. Posons, pour tout n, $x_n = \overline{\alpha_n\dots\alpha_1\ \alpha_0}$ et $y_n = \overline{\beta_n\dots\beta_1\ \beta_0}$, qui seront dits troncatures[2] au rang n de X et Y. On a évidemment $x_n \equiv x_{n-1} \pmod{10^n}$ et $y_n \equiv y_{n-1} \pmod{10^n}$, d'où $x_n\ y_n \equiv x_{n-1}\ y_{n-1} \pmod{10^n}$. Appelons, pour tout n, z_n le reste de la division de $x_n\ y_n$ par 10^{n+1}. La différence $z_n - z_{n-1}$ est un multiple de 10^n inférieur à 10^{n+1} ; elle est donc du type $\gamma_n.10^n$, où γ_n est un entier appartenant à [0 , 9]. Par définition, le produit $X\ Y$ est l'entier décadique $Z = \dots\gamma_n\dots\gamma_1\gamma_0$ associé à la suite des γ_n.

Autrement dit : on fait le produit des troncatures au rang n de X et Y. Alors le reste de la division par 10^n de ce produit est la troncature au rang n de $X\ Y$.

Il est alors aussi facile que fastidieux de vérifier que ces deux opérations donnent à $\mathbf{Z}_{10}$ une structure d'anneau commutatif unitaire. Les nombres u_n et v_n rencontrés dans l'étude du problème (P_n) posé initialement sont alors les troncatures au rang $n-1$ de deux entiers décadiques U et V.

---

[2] Terme non canonique.

Les résultats obtenus précédemment peuvent alors être interprétés comme suit : le fait que, pour tout n, $u_n^2 \equiv u_n \pmod{10^n}$ et $v_n^2 \equiv v_n \pmod{10^n}$ équivaut à $U^2 = U$ et $V^2 = V$. On voit aussitôt[3] que l'équation $X^2 = X$ a dans Z_{10} exactement quatre solutions : 0, 1, U et V.

La relation « pour tout n, 10^n divise $u_n + v_n - 1$ » montre que $U + V = 1$. En rapprochant cette relation de $U(1-U) = 0$, il vient $U\,V = 0$. L'anneau $\mathbf{Z}_{10}$ n'est donc pas intègre.

On peut aisément introduire dans $\mathbf{Z}_{10}$ une valeur absolue comme suit. On pose $abs(0) = 0$ et, pour $X = \ldots\alpha_n \ldots \alpha_1\,\alpha_0$, $abs(X) = 10^{-\lambda}$, où λ est le premier indice tel que $\alpha_\lambda \neq 0$; par exemple $abs(\ldots 111100) = 10^{-3}$. Cette fonction a pour l'addition et la multiplication les mêmes propriétés que la valeur absolue classique. Elle permet donc de définir une distance, $dist(X, Y) = abs(X - Y)$, et par suite une notion de limite.

Il en résulte aussitôt que $dist(U, u_n) \leq 10^{-n}$ et donc que $U = \lim_{n \to +\infty} u_n$; de même $V = \lim_{n \to +\infty} v_n$.

[3] Le lecteur pourra de même aisément vérifier que l'équation $X^4 = X$ n'a que ces quatre solutions et que l'équation $X^3 = X$ a huit solutions : les quatre nombres précédents et $-U$, $-V$, $2U - 1$, $2V - 1$.