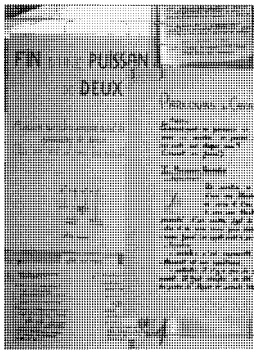
2 puissance n finit par …

par Tatsuhei Iwasaki, Régis Lachaume, Stéphane Fischler,

tous élèves de 1°S du Lycée Jean de la Fontaine 75016 Paris

enseignante : Ghislaine Gaudemet

chercheur : Gilles Godefroy, CNRS



sujet proposé par Monsieur Godefroy :

A quelles conditions il existe une puissance de 2 finissant par un nombre donné ? Par exemple, déterminer s'il existe une (ou plusieurs) puissances de 2 se terminant par 34, 118 ou 492.

I.— Conditions nécessaires pour qu'un nombre soit la fin d'une puissance de 2.

A) Notre notation.

$2^k = d\times10^n + f_n(k)$ où k, d, n et $f_n(k)$ sont des entiers avec $f_n(k) < 10^n$. Dans ces conditions, $f_n(k)$ représente les n derniers chiffres de 2^k. Notre objectif est donc de chercher à quelles conditions un entier donné peut s'écrire $f_n(k)$.

B) $f_n(k)$ ne doit pas être divisible par 5.

En effet, si $f_n(k)$ était divisible par 5, comme 10^n est divisible par 5, $d\times10^n + f_n(k)$, soit 2^k, le serait aussi, ce qui est absurde (une puissance de 2 ne peut pas être divisible par 5).

C) fn(k) doit être divisible par 2^n.

En effet, on a :

$$2^k = d\times10^n + f_n(k)$$
$$2^k = 2^n\times(d\times5^n) + f_n(k)$$
$$f_n(k) = 2^k - 2^n\times(d\times5^n)$$
$$f_n(k) = 2^n\times(2^{k-n} -(d\times5^n)) \text{ avec } n < k \text{ car } 2^k > 10^n$$

En effet, si $2^k < 10^n$, $2^k = f_n(k)$: le problème est trivial : 32, par exemple, est de façon évidente la fin d'une puissance de 2 : 2^5. Comme $2^{k-n} - (d\times5^n)$ est un entier, tout nombre qui s'écrit $f_n(k)$ est divisible par 2^n.

Nous avons démontré que si un nombre est la fin d'une puissance de 2 (c'est-à-dire s'il peut s'écrire $f_n(k)$) alors il est divisible par 2^n et il n'est pas divisible par 5.

Nous sommes donc en présence d'un ensemble d'entiers, que nous noterons E_n, qui remplissent les trois conditions suivantes : ils ont au maximum n chiffres, ils sont divisibles par 2^n et ils ne sont pas divisibles par 5. Ces nombres sont les seuls à pouvoir s'écrire (éventuellement) $f_n(k)$.

II.— Existence d'une périodicité dans les derniers chiffres des puissances de 2.

A) Utilisation du principe de Dirichlet.

La fonction f_n est une application de l'ensemble N des entiers naturels (car k peut être n'importe quel entier) vers l'ensemble E_n (car $f_n(k)$ doit impérativement remplir simultanément les trois conditions ci-dessus). Or le cardinal (c'est-à-dire le nombre d'éléments) de N est infini, alors que celui de E_n est fini (en effet, seul un nombre fini d'entiers ont au plus n chiffres, n étant fixé). Le principe de Dirichlet nous permet alors d'affirmer qu'un élément au moins de E_n, c'est-à-dire une fin $f_n(k)$, a une infinité d'antécédents par f_n, c'est-à-dire qu'il existe au moins un nombre qui est la fin d'une infinité de puissances de deux.

Note : le principe de Dirichlet a une application pratique : si on veut ranger un grand nombre d'objets dans un petit nombre de boîtes, une boîte au moins contiendra deux objets. De même, si on veut ranger une infinité d'objets dans un petit nombre de boîtes, une boîte au moins contiendra une infinité d'objets. Ici, "ranger" signifie appliquer la fonction f_n, les objets sont les entiers k et les boîtes sont les fins $f_n(k)$.

B) Les fins fn(k) sont déterminées par récurrence.

Déterminer $f_n(k)$ par récurrence signifie exprimer $f_n(k+1)$ en fonction de $f_n(k)$. Cela est possible : il suffit de multiplier $f_n(k)$ par 2, puis de ne considérer que les n derniers chiffres (ce qui revient à soustraire 10^n quand $2\times f_n(k) > 10^n$).

C) Conséquence : il existe une période.

Précisons tout d'abord la notion de période appliquée à notre problème : il s'agit de trouver un entier T_n (dépendant de n) tel que 2^{k+T_n} et 2^k aient les mêmes n derniers chiffres, c'est-à-dire qu'on ait :

$$f_n(k + T_n) = f_n(k) \text{ pour tout entier k.}$$

La démonstration qui suit n'est pas rigoureuse, car sinon elle serait trop "lourde".

Travaillons pour n fixé. Notons A un nombre qui est la fin d'une infinité de puissances de 2 (nous savons qu'il en existe au moins un d'après le principe de Dirichlet, mais il y en a peut-être plusieurs).

On a : $A \in E_n$, et il existe un nombre k_1 tel que : $A = f_n(k_1)$. Les fins des puissances de 2 suivantes, $f_n(k_1+1)$, $f_n(k_1+2)$, … , seront déterminées en fonction de A. Or, au bout d'un nombre fini T_n d'itérations, on aura : $f_n(k_1+T_n) = A$, car A est l'image par f_n d'une infinité d'entiers k. Les fins suivantes $f_n(k_1+T_n+1)$, $f_n(k_1+T_n+2)$, … , seront définies en fonction de $f_n(k_1+T_n) = A$: ces nombres seront donc les mêmes que $f_n(k_1+1)$, $f_n(k_1+2)$, … La fonction f_n est donc périodique de plus petite période T_n.

D) Majoration de la période.

Comme les fins $f_n(k)$ sont définies par récurrence, il n'existe pas deux nombres différents a et b compris entre k_1 exclu et k_1+T_n tels que $f_n(a) = f_n(b)$. Les nombres $f_n(k_1+1)$, $f_n(k_1+2)$, … , $f_n(k_1+T_n)$ sont donc tous différents. Or tous ces nombres sont des éléments de l'ensemble E_n des fins possibles. Ces nombres doivent donc être moins nombreux (ou aussi nombreux) que les éléments de E_n. On a donc : $T_n \leq \text{Card}(E_n)$, où $\text{Card}(E_n)$ désigne le nombre d'éléments de E_n.

Calculons donc $\text{Card}(E_n)$. E_n est une partie de l'ensemble F_n des entiers naturels inférieurs à 10^n et divisibles par 2^n. Le nombre d'éléments de F_n est $10^n/2^n$, soit 5^n. Mais E_n ne contient que les éléments de F_n qui ne sont pas divisibles par 5, soit 4 sur 5 (car les éléments de F_n ont pour seule spécificité d'être divisibles par 2^n, ce qui n'influe en rien sur le fait d'être divisible par 5).

On a donc : $\text{Card}(E_n) = 4\times 5^{n-1}$.

La période T_n est donc inférieure ou égale à $4\times 5^{n-1}$.

III.— Détermination de la valeur de la période.

A) Recherche d'un test pour identifier la période.

D'après la définition de T_n, 2^n et 2^{n+T_n} ont les mêmes n derniers chiffres. Il existe donc un entier d tel que : $2^{n+T_n} = d \times 10^n + 2^n$. En divisant chaque membre de cette égalité par 2^n, il vient : $2^{T_n} = d \times 5^n + 1$. Nous noterons ceci : $2^{T_n} \equiv 1 \pmod{5^n}$.

N.B. : la notation "$a \equiv b \pmod c$" signifie que (a - b) est divisible par c, avec $c > 0$.

Les lignes écrites ci-dessus étant équivalentes (car aucune condition n'est imposée à d), un nombre donné T_n est une période si, et seulement si, on a : $2^{T_n} \equiv 1 \pmod{5^n}$. (1)

B) Application du test aux valeurs envisageables pour la période.

En réalisant des expériences sur calculatrice, nous nous sommes aperçus que la période vaut en réalité $4 \times 5^{n-1}$, c'est-à-dire la valeur maximale envisageable. Nous allons donc démontrer que ce nombre vérifie la relation (1) pour tout n, et qu'aucun de ses diviseurs ne la vérifie, quel que soit n : nous aurons ainsi prouvé que $4 \times 5^{n-1}$ est la plus petite période. Ces diviseurs à tester sont $2 \times 5^{n-1}$ et $4 \times 5^{n-2}$, soit la moitié et le cinquième de $4 \times 5^{n-1}$, puisque la décomposition de ce dernier nombre en facteurs premiers ne fait intervenir que des 2 et des 5. Nous pouvons donc écrire ces trois nombres sous la forme : $h \times 5^{n-2}$, h étant un entier pouvant valoir 4, 10 ou 20. La formule (1) peut maintenant s'écrire :

$$2^{h*5^{n-2}} \equiv 1 \pmod{5^n}. \quad (2)$$

Nous ne pouvons pas tester la relation (2) avec toutes les valeurs de n ; c'est pourquoi nous avons démontré d'abord que sa véracité (ou sa non-véracité) ne dépend pas de n. Nous avons placé cette démonstration en annexe car c'est celle que nous avons eu le plus de mal à trouver, et que c'est aussi, à notre avis, la plus difficile à comprendre.

Admettons donc (pour l'instant) que la véracité de la relation (2) ne dépend pas de n. Il ne reste alors qu'à prendre des exemples avec n petit pour démontrer la relation quel que soit n. Avec n = 2, cette relation s'écrit : $2^h \equiv 1 \pmod{25}$. Les nombres 2^4, 2^{10} et 2^{20} valent respectivement 16, 1024 et 1048576. On remarque que seul 2^{20}, soit 1048576, quand il est diminué de 1, devient divisible par 25. On a donc : h = 20 et $T_n = 4 \times 5^{n-1}$, et ce quel que soit n. La période dans les n derniers chiffres des puissances successives de 2 est donc $4 \times 5^{n-1}$.

On remarque que cette période est exactement égale au cardinal de E_n : chaque élément de E_n peut s'écrire, d'une manière et d'une seule, $f_n(k)$ avec k pris dans un intervalle semi-ouvert d'amplitude T_n. Si on laisse k décrire N, chaque élément de E_n peut s'écrire $f_n(k)$ d'une infinité de manières.

Ainsi, si on considère les 3 derniers chiffres des puissances de 2, seuls les nombres de 1, 2 ou 3 chiffres, divisibles par $2^3 = 8$, et non divisibles par 5 sont la fin d'une, et même d'une infinité de puissances de 2. Ainsi, 320 (divisible par 5) et 444 (non divisible par 8) ne sont la fin d'aucune puissance de 2. En revanche, 472, qui est divisible par 8 et non par 5, est la fin d'une infinité de puissances de 2. On trouve par un programme sur calculatrice que 2^{37} se termine par 472 ; la période T_3 valant $4 \times 5^{3-1} = 4 \times 25 = 100$, les nombres 2^{137}, 2^{237} et 2^{65437} se terminent aussi par 472.

ANNEXE :

Nous allons démontrer que la véracité de l'expression (2) : $2^{h*5^{n-2}} \equiv 1 \pmod{5^n}$ ne dépend pas de n. On remarque que pour passer de n à n+1, il suffit d'élever le membre de gauche à la puissance 5 et de remplacer "mod 5^n" par "mod 5^{n+1}". Il nous faut donc démontrer que : $a \equiv 1 \pmod{5^n}$ équivaut à : $a^5 \equiv 1 \pmod{5^{n+1}}$.

Nous allons donc chercher les conditions nécessaires et suffisantes pour qu'on ait $a^5 \equiv 1 \pmod{5^{n+1}}$; nous allons montrer que ces conditions se résument à : $a \equiv 1 \pmod{5^n}$.

1) Condition préliminaire nécessaire : $a \equiv 1 \pmod 5$.

Raisonnons par l'absurde. Partons de l'hypothèse (dont nous allons montrer qu'elle est fausse) : $a \equiv s \pmod 5$ où s vaut 0, 2, 3 ou 4. On peut écrire aussi : $a = 5 \times p + s$, avec p entier. En élevant chaque membre à la puissance 5 (grâce au triangle de Pascal), on obtient : $a^5 = 5 \times p' + s^5$, avec p' entier. En effet, dans le membre de droite une fois développé, tous les termes, sauf s^5, sont divisibles par 5. On a donc : $a^5 - 1 = 5 \times p' + (s^5 - 1)$. (3)

Or on remarque que, quelle que soit la valeur de s (0, 2, 3, ou 4), on a : $s^5 \equiv s \pmod 5$. En effet :
Si s = 0, $s^5 = 0$ et on a bien : $0^5 \equiv 0 \pmod 5$.
Si s = 2, $s^5 = 32$ et on a bien : $2^5 \equiv 2 \pmod 5$.
Si s = 3, $s^5 = 243$ et on a bien : $3^5 \equiv 3 \pmod 5$.
Si s = 4, $s^5 = 1024$ et on a bien $4^5 \equiv 4 \pmod 5$.

L'égalité (3) devient alors :

$a^5 - 1 = 5 \times p'' + (s - 1)$ avec p'' entier.

Comme (s - 1) n'est pas nul (car, par hypothèse, s ne peut valoir que 0, 2, 3 ou 4), $a^5 - 1$ n'est pas divisible par 5, donc a fortiori par 5^{n+1}. On n'a donc pas : $a^5 \equiv 1 \pmod{5^{n+1}}$. Une condition nécessaire pour que cette dernière relation soit vraie est donc : $a \equiv 1 \pmod 5$. On peut donc écrire :

$$a = 5k + 1, \text{ avec k entier.}$$

2) Condition nécessaire et suffisante : $a \equiv 1 \pmod{5^n}$.

Développons pour commencer $a^5 - 1$, en remplaçant a par $5 \times k + 1$. En utilisant les coefficients de la cinquième ligne du triangle de Pascal (1, 5, 10, 10, 5, 1), on obtient :

$$(5k+1)^5 - 1 = (5k)^5 + 5 \times (5k)^4 + 10 \times (5k)^3 + 10 \times (5k)^2 + 5 \times (5k) + 1^5 - 1.$$

$$(5k+1)^5 - 1 = 5^2k \times (5^3k^4 + 5^3k^3 + 2 \times 5^2k^2 + 2 \times 5k + 1).$$

$$a^5 - 1 = 5^2 k \times (5 \times q + 1) \quad \text{avec q entier.}$$

Pour que $a^5 - 1$ soit divisible par 5^{n+1} (c'est le second membre de l'équivalence que nous voulons obtenir), il faut et il suffit que 5^2k le soit (car $5 \times q + 1$ n'est pas divisible par 5). Il faut et il suffit donc que k soit divisible par 5^{n-1}, donc que $a - 1 = 5 \times k$ soit divisible par 5^n, ce qui peut s'écrire : $a \equiv 1 \pmod{5^n}$.

L'équivalence cherchée est donc démontrée.