SOLUTION

Cet énoncé a suscité 13 solutions, de Richard BECZKOWSKI (71-Chalon-sur-Saône), Pierre BORNSZTEIN (78-Maisons-Laffitte), Marie-Laure CHAILLOUT (95-Sarcelles), Christian DUFIS (87-Limoges), Christine FENOGLIO (69-Lyon), Michel HÉBRAUD (31-Toulouse), Michel LAFOND (21-Dijon), Gérard LAVAU (21-Fontaine-lès-Dijon), René MANZONI (76-Le Havre), Jean-Louis NICOLAS (69-Villeurbanne), Gérard PRIGENT (93-Dugny), Pierre RENFER (67-Ostwald) et Pierre SAMUEL (92-Bourg-la-Reine).

La méthode généralement adoptée consiste à prouver par récurrence que, pour tout nombre premier p, si n est divisible par p^α, a_n est lui aussi divisible par p^α.

Et pour cela, on fait appel à deux petits lemmes : tout d'abord, si $x \equiv 1 \pmod{p^\alpha}$, $x^p \equiv 1 \pmod{p^{\alpha+1}}$. Cela se démontre classiquement :
– soit avec la formule du binôme, en développant $x^p = (1 + q \cdot p^\alpha)^p$,
– soit en factorisant : $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$; les p termes de la deuxième parenthèse étant tous congrus à 1 modulo p, leur somme est multiple de p.

Il en résulte un second lemme : pour tout entier y, tout nombre premier p et tout entier α,

$$y^{p^\alpha} \equiv y^{p^{\alpha-1}} \pmod{p^\alpha}.$$

En effet,

$$y^{p^{\alpha}} - y^{p^{\alpha-1}} = \left(y^{(p-1)p^{\alpha-1}} - 1\right) y^{p^{\alpha-1}}.$$

Si y n'est pas multiple de p, $y^{p-1} \equiv 1 \pmod{p}$, donc $y^{(p-1)p} \equiv 1 \pmod{p^2}$ et, par récurrence,

$$y^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^{\alpha}}.$$

C'est une généralisation classique du petit théorème de Fermat. Si y est multiple de p, $y^{p^{\alpha-1}}$ est multiple de $p^{p^{\alpha-1}}$. Or, pour tout $p \geq 2$ et tout $\alpha \geq 1$, $p\alpha \leq p^{\alpha}$ (à nouveau par récurrence sur α : $\dfrac{\alpha+1}{\alpha} \leq 2 \leq p$). Donc $p^{\alpha-1} \geq \alpha$, et $y^{p^{\alpha-1}}$ est divisible par p^{α}.

Dès lors, revenons à notre problème. Supposons la conclusion vraie pour tout entier strictement inférieur à n. Si p est un facteur premier de n, posons: $n = k \cdot p^{\alpha}$ (k premier avec p), et montrons que a_n est divisible par p^{α}. Ceci prouvé, a_n sera divisible par tout diviseur p^{α} de n, donc par leur PPCM, à savoir n.

Les diviseurs de n qui ne divisent pas $k \cdot p^{\alpha-1}$ sont nécessairement multiples de p^{α}. L'hypothèse peut donc s'écrire :

$$2^n = 2^{k \cdot p^{\alpha}} = \sum_{d \mid k \cdot p^{\alpha-1}} a_d + \sum_{d \mid k, d < k} a_{d \cdot p^{\alpha}} + a_n.$$

La première somme vaut, par hypothèse, $2^{k \cdot p^{\alpha-1}}$. Dans la seconde somme, $d \cdot p^{\alpha}$ étant strictement inférieur à n, d'après l'hypothèse de récurrence, $a_{d \cdot p^{\alpha}}$ est divisible par $d \cdot p^{\alpha}$, donc cette seconde somme est divisible par p^{α}. On en déduit que

$$a_n \equiv 2^{k \cdot p^{\alpha}} - 2^{k \cdot p^{\alpha-1}} \pmod{p^{\alpha}},$$

soit, en utilisant le second lemme ci-dessus avec $y = 2^k$, que

$$a_n \equiv 0 \pmod{p^{\alpha}}.$$

Plusieurs lecteurs signalent que l'on peut remplacer 2^n par c^n pour n'importe quel entier c : la démonstration ci-dessus est inchangée, on a juste $y = c^k$. Certains font appel à la fonction μ de Möbius : $\mu(1) = 1$; $\mu(p_1 p_2 \ldots p_m) = (-1)^m$ si tous les p_i, pour $1 \leq i \leq m$, sont premiers distincts ; et si n est divisible par le carré d'un nombre premier, $\mu(n) = 0$.

Cette fonction vérifie entre autres : si pour tout entier n,

$$\sum_{d \mid n} a_d = \mathrm{A}_n,$$

alors pour tout entier n,

$$a_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \mathrm{A}_d.$$

En effet, si n possède m diviseurs premiers ($m \geq 1$), il existe C_m^r produits de r facteurs premiers distincts parmi les diviseurs de n, qui vérifient $\mu(d) = (-1)^r$, de

sorte que

$$\sum_{q|n}\mu\left(\frac{n}{q}\right)=\sum_{r=0}^{m}\mathrm{C}_m^r(-1)^r=(1-1)^m=0.$$

Alors que si $n = 1$,

$$\sum_{q|n}\mu\left(\frac{n}{q}\right)=\mu(1)=1.$$

Il en résulte :

$$a_n=\sum_{b|n}a_b\sum_{q|\frac{n}{b}}\mu\left(\frac{n}{bq}\right),$$

la seconde somme étant nulle sauf pour $b = n$. En permutant les sommations, et en posant $d = bq$, on obtient :

$$a_n=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{b|d}a_b=\sum_{d|n}\mu\left(\frac{n}{d}\right)\mathrm{A}_d.$$

Or si $n = k \cdot p^\alpha$ (k premier avec p), les seuls diviseurs de n vérifiant $\mu\left(\frac{n}{d}\right)\neq 0$ sont les $q \cdot p^\alpha$ et les $q \cdot p^{\alpha-1}$, pour $q \mid k$ tels que $\mu\left(\frac{k}{q}\right)\neq 0$ et l'on a: $\mu\left(\frac{k}{q}p\right)=-\mu\left(\frac{k}{q}\right)$, si bien que

$$a_n=\sum_{q|k}\mu\left(\frac{k}{q}\right)\left(2^{q\cdot p^\alpha}-2^{q\cdot p^{\alpha-1}}\right)$$

est divisible par p^α d'après nos lemmes du début.

Richard Beczkowski donne les 32 premières valeurs de la suite (2, 2, 6, 12, 30, 54, 126, 240, 504, 990, 2 046, 4 020, 8 190, 16 254, 32 730, 65 280, 131 070, etc.) et Gérard Prigent signale que cette suite est répertoriée sous la référence A027375 dans « the On-Line Encyclopedia of Integer Sequences » (www.research.att.com). a_n y est présenté comme le nombre de suites binaires non périodiques de longueur n :

$a_3 = 6 = \text{Card}\ \{001, 010, 100, 011, 110, 101)$.

Gérard Lavau en donne une variante : si l'on colorie en deux couleurs les n sommets d'un polygone régulier, et qu'on fait opérer sur ces coloriages le groupe des rotations du polygone, chaque coloriage décrit une orbite dont la longueur divise n. Si O_d est le nombre d'orbites de longueur d, le nombre de coloriages de ces orbites est $d \cdot \mathrm{O}_d$. Et ce nombre dépend de d et non de n : un tel coloriage équivaut à une suite binaire non périodique de d couleurs, qui se répète $\frac{n}{d}$ fois tout autour du polygone. Comme il existe 2^n coloriages au total, $2^n=\sum_{d|n}d\cdot\mathrm{O}_d$, ce qui entraîne: $a_d = d \cdot \mathrm{O}_d$. Enfin Jean-Louis Nicolas ajoute que O_d est aussi le nombre de polynômes irréductibles unitaires de degré d sur le corps à deux éléments.