**Problème n° 300.** (Bulletin de l'APMEP n°450, Janv.–Fév. 2004)

*Soit $a_n$, pour $n \geq 1$, la suite d'entiers tels que*

$$\sum_{d\,|\,n} a_d = 2^n. \tag{1}$$

*Montrer que pour tout $n$*

$$n \text{ divise } a_n. \tag{2}$$

**Solution**[1]. Soit $I_n$ le nombre de polynômes irréductibles unitaires de degré $n$ sur le corps $\mathbb{F}_2$ à deux éléments. L'évaluation classique de $I_n$ donne $\sum_{d\,|\,n} dI_d = 2^n$ et ainsi, par (1), $a_n = nI_n$, ce qui démontre (2). Nous donnons ci-dessous une démonstration élémentaire de (2).

Pour $n = 1$, (1) donne $a_1 = 2$. On calcule aisément $a_2 = 2$, $a_3 = 6$, $a_4 = 12$, $a_5 = 30$, $a_6 = 54$, etc...

Lorsque $n = p$ premier, par (1), $a_p = 2^p - 2$, et (2) est vraie par le petit théorème de Fermat :

$$m \in \mathbb{Z} \quad \Longrightarrow \quad m^p \equiv m \pmod p. \tag{3}$$

Lorsque $n$ est une puissance $p^k$ du nombre premier $p$, les diviseurs de $n$ sont $n = p^k$ et les diviseurs de $p^{k-1}$ ; (1) s'écrit alors

$$a_n = 2^n - \sum_{d\,|\,p^{k-1}} a_d = 2^n - 2^{n/p} = 2^n - 2^{p^{k-1}}$$

et (2) sera une conséquence du lemme suivant, qui est une extension du petit théorème de Fermat :

**Lemme.** *Soit $m \in \mathbb{Z}$, $p$ premier et $k$ un entier naturel non nul. Alors,*

$$m^{(p^k)} \equiv m^{(p^{k-1})} \pmod{p^k}. \tag{4}$$

**Démonstration du lemme.** Raisonnons par récurrence sur $k$. Pour $k = 1$, (2) résulte du théorème de Fermat (3). Supposons que (4) soit vrai pour $k \geq 1$ ; il existe un entier relatif $A_k$ tel que

$$m^{(p^k)} = m^{(p^{k-1})} + A_k p^k. \tag{5}$$

[1]Jean-Louis Nicolas, Mathématiques, Université Claude Bernard (Lyon 1), 69622–Villeurbanne cédex. Mèl : `jlnicola@in2p3.fr`

Elevons l'égalité (5) à la puissance $p$ ; par la formule du binôme de Newton, il vient

$$\begin{aligned} m^{(p^{k+1})} &= m^{(p^k)} + pm^{(p^{k-1})(p-1)}A_k p^k + \sum_{j=2}^{p} \binom{p}{j} m^{(p^{k-1})(p-j)} \left(A_k p^k\right)^j \\ &= m^{(p^k)} + p^{k+1}A_{k+1} \end{aligned}$$

avec

$$A_{k+1} = m^{(p^{k-1})(p-1)}A_k + \sum_{j=2}^{p} \binom{p}{j} m^{(p^{k-1}(p-j))} A_k^j p^{k(j-1)-1}$$

ce qui établit (4) pour $k+1$. □

Démontrons (2) par récurrence. Pour $n = 1$, (2) est vraie. Supposons $n \geq 2$ et

(6) (hypothèse de récurrence) $\qquad m$ divise $a_m$ pour $1 \leq m \leq n-1$.

Ecrivons la décomposition en facteurs premiers de $n$, $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ ; comme $n \geq 2$, on a $r \geq 1$. Un diviseur $d$ de $n$ s'écrit $n = p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}$ avec $0 \leq j_i \leq k_i$, pour $1 \leq i \leq r$. Partageons l'ensemble $\mathcal{D}(n)$ des diviseurs de $n$ en deux sous-ensembles $\mathcal{D}_1(n)$ et $\mathcal{D}_2(n)$ ; $\mathcal{D}_1(n)$ contient les diviseurs $d$ tels que $j_1 < k_1$ ; c'est exactement l'ensemble des diviseurs $\mathcal{D}(n/p_1)$ de $n/p_1$. $\mathcal{D}_2(n)$ contient les diviseurs $d$ de $n$ tels que $j_1 = k_1$ ; ce sont les diviseurs de $n$ qui sont multiples de $p_1^{k_1}$. La formule (1) s'écrit :

$$2^n = a_n + \sum_{d \in \mathcal{D}_1(n)} a_d + \sum_{d \in \mathcal{D}_2(n) \setminus \{n\}} a_d. \tag{7}$$

Or, par (1), la somme $\sum_{d \in \mathcal{D}_1(n)} a_d$ vaut $2^{n/p_1}$ ; et, par (6), chaque terme de la somme $\sum_{d \in \mathcal{D}_2(n) \setminus \{n\}} a_d$ est multiple de $d$, et donc multiple de $p_1^{k_1}$. La formule (7) donne alors avec $b = n/p_1^{k_1}$ :

$$a_n \equiv 2^n - 2^{n/p_1} = 2^{bp_1^{k_1}} - 2^{bp_1^{k_1-1}} \pmod{p_1^{k_1}} \tag{8}$$

et, en appliquant le lemme avec $k = k_1$, $p = p_1$ et $m = 2^b = 2^{n/p_1^{k_1}}$, on obtient

$$p_1^{k_1} \quad \text{divise} \quad a_n.$$

En répétant la même démonstration pour $i = 2, 3, \dots, r$, on obtient que

$$p_i^{k_i} \quad \text{divise} \quad a_n, \qquad 1 \leq i \leq r$$

et, par suite, $n$ divise $a_n$.

ont une droite en commun. C'est en particulier le cas lorsque $n = 3$ : la droite passe alors par l'orthocentre du triangle, et l'on retrouve les relations classiques :

$$\overrightarrow{OH} = 3 \cdot \overrightarrow{OG},$$

$$OH^2 = 9R^2 - (a^2 + b^2 + c^2).$$

Pierre Bornsztein ajoute que la première partie est une généralisation à l'espace d'un résultat dû à M. B. Cantor (1829 - 1920), dont on peut trouver l'énoncé dans le poly du stage olympique de Saint-Malo (été 2003), exercice 11 de la muraille : en appelant $(\Delta_i)$ la perpendiculaire à la tangente au cercle en $A_i$ passant par l'isobarycentre des $(n - 1)$ autres points, les droites $(\Delta_i)$ sont concourantes. Et Michel Hébraud signale une généralisation de la notion d'orthocentre (J. Trignan, *La géométrie des nombres complexes*) : l'orthocentre H d'un polygone inscriptible étant défini par $\overrightarrow{OH} = \sum \overrightarrow{OA_i}$, H est l'intersection de tous les cercles de centres $H_i$ (orthocentre du polygone privé du sommet $A_i$) et de rayon R (car $\overrightarrow{H_iH} = \overrightarrow{OA_i}$). Les droites joignant l'isobarycentre de $p$ points et l'orthocentre des $(n - p)$ restants sont concourantes.

**Énoncé n° 300 (Moubinool OMARJEE, 75-Paris)**

Soit $a_n$, pour $n \geq 1$, une suite d'entiers naturels tels que :

$$\sum_{d|n} a_d = 2^n.$$

Montrer que pour tout $n$, $n$ divise $a_n$.

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 $p^\alpha$, $a_n$ est lui aussi divisible par $p^\alpha$.

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 $\alpha$,

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

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 $\alpha$ : $\dfrac{\alpha+1}{\alpha}\leq 2\leq p$ ). Donc $p^{\alpha-1}\geq\alpha$, et $y^{p^{\alpha-1}}$ est divisible par $p^\alpha$.

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 $p^\alpha$. Ceci prouvé, $a_n$ sera divisible par tout diviseur $p^\alpha$ 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 $p^\alpha$. L'hypothèse peut donc s'écrire :

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

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 $p^\alpha$. 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 $\mu$ de Möbius : $\mu(1)=1$ ; $\mu(p_1p_2\cdots p_m)=(-1)^m$ 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 $n$,

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

alors pour tout entier $n$,

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

En effet, si $n$ possède $m$ diviseurs premiers ($m\geq 1$), il existe $\mathrm{C}_m^r$ produits de $r$ facteurs premiers distincts parmi les diviseurs de $n$, qui vérifient $\mu(d)=(-1)^r$, de sorte que

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

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 :

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

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 $p^\alpha$ 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 $d \cdot O_d$. 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, $2^n=\sum_{d|n}d\cdot O_d$, ce qui entraîne: $a_d = d \cdot O_d$. 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.