

Problème 553-5 (Au fil des maths)

François Hublet

Il est demandé s'il existe une fonction $f : \mathbb{N} \rightarrow \mathbb{N}$ telle que, pour tout $n \in \mathbb{N}$, $f \circ f(n) = n^2$.

1 Préliminaires

Commençons par définir l'ensemble suivant, que nous appellerons ensemble des *bases* :

$$\mathcal{B} = \{b \in \mathbb{N} \setminus \{0, 1\} \mid \nexists n < b, k \in \mathbb{N}. b = n^{2^k}\}.$$

On a clairement le

Lemme 1. *L'ensemble $\mathcal{B}$ contient l'ensemble $\mathbb{P}$ des nombres premiers.*

d'où on déduit le

Lemme 2. *L'ensemble $\mathcal{B}$ est infini.*

Tout nombre entier se décompose de manière unique comme puissance 2^{k_e} d'une base :

Lemme 3. *Soit $n \in \mathbb{N}$. Il existe une unique paire $(b, k) \in \mathcal{B} \times \mathbb{N}$ telle que $n = b^{2^k}$.*

Démonstration. Soit $n \in \mathbb{N}$. Soit $\mathcal{E}(n) = \{(b, k) \in \mathbb{N}^2 \mid n = b^{2^k}\}$. L'ensemble $\mathcal{E}(n)$ est non-vidé, contenant $(n, 0)$. Soit $(b, k) \in \mathcal{E}(n)$ telle que b est minimal. Montrons que $b \in \mathcal{B}$. Si $b \notin \mathcal{B}$, on obtient $n' < b$ et $k' \in \mathbb{N}$ tels que $b = n'^{2^{k'}}$. Mais alors $n = b^{2^k} = \left(n'^{2^{k'}}\right)^{2^k} = n'^{2^{k'} \cdot 2^k} = n'^{2^{k'+k}}$ avec $n' < b$, contredisant la minimalité de b . S'il existe deux paires $(b_1, k_1), (b_2, k_2) \in \mathcal{B} \times \mathbb{N}$ telles que $(b_1, k_1) \neq (b_2, k_2)$, supposons sans perte de généralité que $b_1 < b_2$. Alors $b_1^{2^{k_1}} = n = b_2^{2^{k_2}}$ avec $k_1 > k_2$. Par conséquent, $b_1 = b_2^{2^{k_2}/2^{k_1}} = b_2^{2^{k_2-k_1}}$, contredisant $b_1 \in \mathcal{B}$. $\square$

En vertu du lemme précédent, on définit à bon droit :

Définition 4. Soit $\beta : \mathbb{N} \rightarrow \mathbb{N}$ et $\kappa : \mathbb{N} \rightarrow \mathbb{N}$ telles que pour tout $n \in \mathbb{N}$,

$$\beta(n) = \min\{b \in \mathcal{B} \mid \exists k \in \mathbb{N}. n = b^{2^k}\} \quad \kappa(n) = \log_2(\log_{\beta(n)}(n)).$$

On obtient :

Lemme 5. *Pour tout $n \in \mathbb{N}$, on a*

$$(1) \ n = \beta(n)^{2^{\kappa(n)}}$$

$$(2) \ \beta\left(\beta(n)^{2^{\kappa(n)}}\right) = \beta(n)$$

$$(3) \ \kappa\left(\beta(n)^{2^k}\right) = k$$

Démonstration. Soit $n \in \mathbb{N}$.

(1) L'ensemble $\{b \in \mathcal{B} \mid \exists k \in \mathbb{N}. n = b^{2^k}\}$ est non-vidé par le Lemme 3. Par conséquent, $\beta(n)$ est bien défini et il existe $k \in \mathbb{N}$ tel que $n = \beta(n)^{2^k}$. Clairement, $k = \kappa(n)$.

(2) Par définition de β , il existe $k \in \mathbb{N}$ tel que $\beta(n)^{2^{\kappa(n)}} = \beta(n)^{2^k}$. De même, $k = \kappa(n)$.

(3) Par le point (2),

$$\kappa\left(\beta(n)^{2^k}\right) = \log_2\left(\log_{\beta(n)^{2^k}}\left(\beta(n)^{2^k}\right)\right) \stackrel{(2)}{=} \log_2(\log_{\beta(n)}(\beta(n)^{2^k})) = k.$$

$\square$

2 Démonstration

Nous prouvons :

Théorème 6. Soit $f : \mathbb{N} \rightarrow \mathbb{N}$. Les deux conditions suivantes sont équivalentes :

1. Pour tout $n \in \mathbb{N}$, $f \circ f(n) = n^2$.
2. Il existe une partition $\mathcal{B} = \mathcal{B}_1 \sqcup \mathcal{B}_2$ et deux bijections $g : \mathcal{B}_1 \xrightarrow{\sim} \mathcal{B}_2$ et $h : \{0, 1\} \xrightarrow{\sim} \{0, 1\}$ telles que

$$\forall n \in \mathbb{N}. f(n) = \begin{cases} h(n) & n \in \{0, 1\} \\ g(\beta(n))^{2^{\kappa(n)}} & \beta(n) \in \mathcal{B}_1 \\ g^{-1}(\beta(n))^{2^{\kappa(n)+1}} & \beta(n) \in \mathcal{B}_2. \end{cases}$$

Démonstration. $\boxed{\Leftarrow}$ Si h est l'identité, alors $f \circ f(0) = f(0) = 0$ et $f \circ f(1) = f(1) = 1$. Si h n'est pas l'identité, alors $h(0) = 1$ et $h(1) = 0$, d'où $f \circ f(0) = f(1) = 0$ et $f \circ f(1) = f(0) = 1$.

Pour $n \in \mathbb{N}$ tel que $\beta(n) \in \mathcal{B}_1$, il vient

$$\begin{aligned} f \circ f(n) &= g^{-1} \left(\beta \left(g(\beta(n))^{2^{\kappa(n)}} \right) \right)^{2^{\kappa \left(g(\beta(n))^{2^{\kappa(n)}} \right) + 1}} && \text{(définition de } f) \\ &= g^{-1} \left(g(\beta(n)) \right)^{2^{\kappa(n)+1}} && \text{(Lemmes 5(2), 5(3))} \\ &= \beta(n)^{2^{\kappa(n)+1}} && \text{(définition de } g) \\ &= \left(\beta(n)^{2^{\kappa(n)}} \right)^2 \\ &= n^2 && \text{(Lemme 5(1)).} \end{aligned}$$

De même, pour $n \in \mathbb{N}$ tel que $\beta(n) \in \mathcal{B}_2$,

$$\begin{aligned} f \circ f(n) &= g \left(\beta \left(g^{-1}(\beta(n))^{2^{\kappa(n)+1}} \right) \right)^{2^{\kappa \left(g^{-1}(\beta(n))^{2^{\kappa(n)+1}} \right)}} && \text{(définition de } f) \\ &= g \left(g^{-1}(\beta(n)) \right)^{2^{\kappa(n)+1}} && \text{(Lemmes 5(2), 5(3))} \\ &= \beta(n)^{2^{\kappa(n)+1}} && \text{(définition de } g) \\ &= \left(\beta(n)^{2^{\kappa(n)}} \right)^2 \\ &= n^2 && \text{(Lemme 5(1)).} \end{aligned}$$

$\boxed{\Rightarrow}$ Montrons d'abord que pour tout $b \in \mathcal{B}$, $\kappa(f(b)) \in \{0, 1\}$. Par l'absurde, supposons $\kappa(f(b)) \geq 2$. Par le Lemme 5(1), on obtient $f(b) = \beta(f(b))^{2^{\kappa(f(b))}}$. Comme $\kappa(f(b)) \geq 2$, on récrit $f(b) = \beta(f(b))^{4 \cdot 2^k} = \left(\beta(f(b))^{2^k} \right)^4 = r^4$ où $k = \kappa(f(b)) - 2$, $r = \beta(f(b))^{2^k}$. Soit maintenant $r' = f(r)$. Puisque $f \circ f(n) = n^2$ pour tout n , on a $f \circ f(r) = r^2$, $f^{(3)}(r) = r'^2$, $f^{(4)}(r) = r^4 = f(b)$, $f^{(5)}(r) = r'^4$. Comme $f^{(4)}(r) = f(b)$, on a par ailleurs $f^{(5)}(r) = f \circ f^{(4)}(r) = f \circ f(b) = b^2$, d'où $b^2 = r'^4$ et donc $b = r'^2$. Cela contredit $b \in \mathcal{B}$ et prouve donc $\kappa(f(b)) \in \{0, 1\}$.

Posons maintenant $\mathcal{B}_1 = \{b \in \mathcal{B} \mid \kappa(f(b)) = 0\} = \mathcal{B} \cap f^{-1}(\mathcal{B})$, $\mathcal{B}_2 = \{b \in \mathcal{B} \mid \kappa(f(b)) = 1\}$, $g = f|_{\mathcal{B}_1}$ et $h = f|_{\{0,1\}}$. Clairement, $\mathcal{B}_1$ et $\mathcal{B}_2$ partitionnent $\mathcal{B}$. Pour tout $b \in \mathcal{B}_1$, on a $\kappa(f(f(b))) = \kappa(b^2) \geq 1$, puisque b^2 est un carré. Mais $f(b) \in \mathcal{B}$ puisque $b \in \mathcal{B}_1$ et donc $\kappa(f(f(b))) \in \{0, 1\}$. Par conséquent, $\kappa(f(f(b))) = 1$, d'où $f(b) \in \mathcal{B}_2$. Cela prouve $g : \mathcal{B}_1 \rightarrow \mathcal{B}_2$.

Montrons que g est une injection. Soit $b_1, b_2 \in \mathcal{B}_1$ telles que $g(b_1) = g(b_2)$. Alors $g \circ g(b_1) = g \circ g(b_2)$, d'où $b_1^2 = b_2^2$ puis $b_1 = b_2$.

Montrons que g est une surjection. Soit $b_2 \in \mathcal{B}_2$. Par définition de $\mathcal{B}_2$, $\kappa(f(b_2))$ est un carré, et on obtient donc $r \in \mathbb{N}$ tel que $f(b_2) = r^2$. Montrons que $f(r) = b_2$. On a d'une part

$f^{(3)}(r) = f^{(2)} \circ f(r) = (f(r))^2$ et d'autre part $f^{(3)}(r) = f \circ f^{(2)}(r) = f(r^2) = f \circ f(b_2) = b_2^2$, d'où $(f(r))^2 = b_2^2$ et finalement $f(r) = b_2$.

Il s'ensuit que g est une bijection entre $\mathcal{B}_1$ et $\mathcal{B}_2$. Si $n \in \{0, 1\}$, alors $n^2 = n$. On récrit d'une part $f^{(3)}(n) = f^{(2)} \circ f(n) = (f(n))^2$ et d'autre part $f^{(3)}(n) = f \circ f^{(2)}(n) = f(n^2) = f(n)$ pour obtenir $f(n) = (f(n))^2$ et donc $f(n) \in \{0, 1\}$. Si $f(0) = 1$, alors on a nécessairement $f(f(0)) = f(1) = 0$. Si $f(0) = 0$, alors $f(1) = 0$ impliquerait $f \circ f(1) = 0 \neq 1$, et par conséquent $f(1) = 1$. Dans les deux cas, h est bien une bijection et $f(n) = h(n)$ pour tout $n \in \{0, 1\}$.

Montrons enfin que pour tout $n \geq 2$, on a

$$f(n) = \begin{cases} g(\beta(n))^{2^{\kappa(n)}} & \beta(n) \in \mathcal{B}_1 \\ g^{-1}(\beta(n))^{2^{\kappa(n)+1}} & \beta(n) \in \mathcal{B}_2 \end{cases}$$

par récurrence sur $\kappa(n)$. Si $\kappa(n) = 0$, alors $n = \beta(n) \in \mathcal{B}$. Si $\beta(n) \in \mathcal{B}_1$, on a prouvé précédemment que $g(\beta(n)) \in \mathcal{B}_2$, et donc $f(n) = g(n) = g(\beta(n)) = g(\beta(n))^{2^0} = g(\beta(n))^{2^{\kappa(n)}}$. Si $\beta(n) \in \mathcal{B}_2$, on a prouvé précédemment que $\kappa(n) = 1$, et donc $f(n) = b^2 = b^{2^{\kappa(n)+1}}$ où $b \in \mathcal{B}$. Il reste à prouver que $b = g^{-1}(\beta(n))$. Pour ce faire, on observe d'abord que, puisque $g^{-1}(\beta(n)) \in \mathcal{B}_1$, le point précédent prouve $f(g^{-1}(\beta(n))) = g(g^{-1}(\beta(n)))^{2^{\kappa(g^{-1}(\beta(n)))}} = \beta(n) = n$, où on a utilisé le Lemme 5(2). Par suite, $b^2 = f(n) = f \circ f \circ g^{-1}(\beta(n)) = g^{-1}(\beta(n))^2$ et finalement $b = g^{-1}(\beta(n))$.

Soit $k \in \mathbb{N}$. Supposons la proposition vraie jusqu'au rang k . Soit $n \in \mathbb{N}$ tel que $\kappa(n) = k + 1$. Supposons $\beta(n) \in \mathcal{B}_1$. Soit $n' = g(\beta(n))^{2^{\kappa(n)-1}}$. On a $\beta(n') \in \mathcal{B}_2$ par le Lemme 5(2), d'où, par hypothèse de récurrence, $f(n') = g^{-1}(g(\beta(n)))^{2^{(\kappa(n)-1)+1}} = \beta(n)^{2^{\kappa(n)}} = n$, où on a utilisé le Lemme 5(1) dans la troisième équation. Par propriété de f , on obtient finalement $f(n) = f \circ f(n') = n'^2$, soit $f(n) = g(\beta(n))^{2^{\kappa(n)}}$. De manière similaire, si $\beta(n) \in \mathcal{B}_2$, on pose $n' = g^{-1}(\beta(n))^{2^{\kappa(n)}}$ et on montre $f(n') = n$, d'où $f(n) = n'^2 = g^{-1}(\beta(n))^{2^{\kappa(n)+1}}$ et la conclusion. $\square$

De ce théorème, on tire aisément le corollaire suivant qui répond à la question posée :

Théorème 7. *Il existe une infinité dénombrable de fonctions f satisfaisant $f \circ f(n) = n^2$.*

Démonstration. D'après le Lemme 1, $\mathcal{B}$ est un ensemble infini. Étant un sous-ensemble de $\mathbb{N}$, il est également dénombrable. D'après le Théorème 6, la fonction f est définie de manière unique par le choix d'une partition de $\mathcal{B}$ en deux sous-ensembles et d'une bijection entre ces deux ensembles, ou, de manière équivalente, par le choix d'une partition de $\mathcal{B}$ en sous-ensembles ordonnés de cardinal 2. Il existe clairement une infinité de tels choix. Par ailleurs, toute telle partition peut être vue comme un cas particulier d'application de $\mathbb{N}$ dans $\mathbb{N} \times \{0, 1\}$, et comme l'ensemble de ces applications est dénombrable, l'ensemble des fonctions f satisfaisant l'équation ci-dessus est également dénombrable. $\square$

Remerciements. L'auteur remercie Pierre-Alain Sallard pour avoir suggéré cette question ainsi que pour sa relecture attentive de ce document.