Une équation fonctionnelle arithmétique (IMO25 Pb3) – résolution compacte

Marc SAGE

31 août 2025

Énoncé. *On note $\mathcal{F}$ l'ensemble des applications $f : \mathbf{N}^* \longrightarrow \mathbf{N}^*$ telles que*

$$\forall \begin{matrix}\blacksquare\\ \square\end{matrix} \in \mathbf{N}^*, \quad f(\square)^{f(\blacksquare)} = \square^{\blacksquare} \bmod f(\blacksquare). \qquad \textit{Déterminer } \max_{\bigstar \in \mathbf{N}^*}{}^{F \in \mathcal{F}} \frac{F(\bigstar)}{\bigstar}.$$

Les application constante 1 et identité Id sont clairement dans $\mathcal{F}$: mises à part ces dernières, nous allons explicitement *résoudre* l'équation fonctionnelle « appartenir à $\mathcal{F}$ », ce qui livrera le maximum cherché.

Résultat central. *Construire un élément de $\mathcal{F}$, vu comme la suite de ses images $(1', 2', 3'...)$, revient – outre la suite constante $(1, 1, 1, ...)$ et la suite identité $(1, 2, 3, ...)$ – à choisir une image dans chacune des colonnes suivantes*[1] *:*

1	2 4 (pas 8 !)	1	2 4 8 $\boxed{16}$	1	2 4 8	1	2 4 8 16 $\boxed{32}$	1	2 4 8	1	2 4 8 16	1	2 4 8	1	2 4 8 16 32 $\boxed{64}$	1...				

Corollaire. *Le maximum cherché vaut 4 et est atteint ssi l'on choisit (dans la description ci-dessus) au moins une image encadrée :* $\boxed{16}$, $\boxed{32}$, $\boxed{64}$...

Mise en œuvre. Soient $a, b, i, n, p \in \mathbf{N}^*$ tels que i impair et p premier.

Soit $f : \mathbf{N}^* \longrightarrow \mathbf{N}^*$ dont on note les images avec des primes, *e. g.* $\boxed{n' := f(n)}$. Quand cette dernière image vaut 1, nous dirons que $\boxed{f \textbf{ \textit{tue} } n}$ ou que $\boxed{n \text{ est } \textbf{\textit{tué}}}$ (sous-entendu : par f).

On note enfin $\boxed{v}$ l'application *valuation dyadique* et $\boxed{\Lambda}$ la suite des p. g. c. d. $\left(\bigwedge_{\iota \text{ impair}} \iota^N - 1\right)_{N \geq 1}$.

Lemme 1. *Supposons $f \in \mathcal{F}$ et $p' \neq 1$. On a alors la divisibilité $p \mid a' - a$.*

Lemme 2. *Soit (d) une famille finie de naturels dont a est le produit. Si $f \in \mathcal{F}$, alors a' divise $(\prod d')^{a'}$.*

Lemme 3. *Le p. g. c. d. Λ_a est une puissance de 2.*

Lemme 4. *Supposons a pair. On a alors*[2] *l'égalité $v(i^a - 1) - v(a) = v\left(i^2 - 1\right) - 1$.*

Lemme 5. *Supposons a pair. Le p. g. c. d. Λ_a vaut alors $2^{2+v(a)}$.*

Preuve des lemmes. Remplacer dans l'hypothèse $\binom{\blacksquare}{\square} \leftarrow \binom{a}{a}$ montre que l'image a' divise a^a.

$\boxed{\text{L1}}$ L'image p' divise p^p, donc est une puissance de p, autre que 1, donc est multiple de p. En particulier, l'égalité $a^p = a'^{p'} \bmod p'$ obtenue en remplaçant $\binom{\blacksquare}{\square} \leftarrow \binom{p}{a}$ passe *modulo* p. Le petit théorème de Fermat s'applique alors à gauche et (au besoin plusieurs fois) à droite, d'où la conclusion $a = a' \bmod p$.

[1] Voici un algorithme engendrant ces colonnes et mettant au jour ses symétries. *Étape 1* : écrire 1. Soit ensuite $n \geq 1$ tel que l'étape n a été effectuée. *Étape $n+1$* : rajouter à droite la colonne $\left(2^E\right)_{1 \leq E \leq n+2}$, puis recopier à droite de cette dernière ce qui était à sa gauche (on peut aussi le réfléchir par rapport à cette colonne). *Étape finale* : élaguer le 8 de la première colonne $(2, 4, \not{8})$.

[2] cas particulier du théorème dit *LTE* (pour *Lifting The Exponent*), voir par exemple le pdf https ://pregatirematematicaolimpiadejuniori.wordpress.com/wp-content/uploads/2016/07/lte.pdf

L2 Multiplier les égalités $d'^{a'} = d^a \bmod a'$ obtenues en remplaçant $\binom{\blacksquare}{\square} \leftarrow \binom{a}{d}$ donne $\left(\prod d'\right)^{a'} = \left(\prod d\right)^a \bmod a'$. Or le membre de droite a^a est divisible par l'image a'.

L3 Si i divise Λ_a, alors i divise d'une part i^a d'autre part $\Lambda_a \mid i^a - 1$, donc la différence $i^a - (i^a - 1)$.

L4 L'imparité quand b est impair de $\frac{i^{2^n b}-1}{i^{2^n}-1} = \sum_{0 \le \bigstar < b} i^{2^n \bigstar}$ permet de se ramener au cas $a = 2^n$, puis réécrire $\frac{i^{2^{n+1}}-1}{\boxed{i^{2^n}-1}} = 2 + \boxed{i^{2^n}-1}$ montre que la suite $\left(v\left(i^{2^N}-1\right)\right)_{N \ge 1}$ est affine de raison 1.

L5 D'après le lemme 3, le p. g. c. d. Λ_a est une puissance de 2, à savoir $\underline{\underline{\Lambda_a = 2^{\min_{\iota \text{ impair}} v(\iota^a - 1)}}}$. Or le lemme 4 permet de minorer l'exposant par $v(a)$ plus $v\left(i^2-1\right) - 1 \ge 2$ avec égalité obtenue pour $i = 3$.

Le résultat central découle alors du théorème suivant.

Théorème. *Supposons $f \neq \mathrm{Id}$ et $f \neq 1$. On a alors les équivalences*

$$f \in \mathcal{F} \Longleftrightarrow \begin{cases} \forall I \text{ impair}, I' = 1 \\ \forall P \text{ pair}, \begin{cases} 2 \mid P' \mid 2^P \\ P' \mid \Lambda_P \end{cases} \end{cases} \Longleftrightarrow \begin{cases} 2' \in \{2, 4\} \\ \forall I \text{ impair}, I' = 1 \\ \forall P \text{ pair} \neq 2, \exists e \in \mathbf{N}, \begin{cases} P' = 2^e \\ 1 \le e \le 2 + v(P) \end{cases} \end{cases}.$$

Preuve de la 2de équivalence. (Il n'y a rien à faire pour les impairs.)

Soit P pair et imposons $P = 2^n i$. Le lemme 5 explicite alors $\Lambda_P = 2^{2+n}$ et la conjonction $\begin{cases} P' \mid 2^P \\ P' \mid 2^{2+n} \end{cases}$ se traduit par $P' \mid 2^{\min\{P, 2+n\}}$, le minimum en exposant[3] valant $\begin{cases} 2 & \text{si } P = 2 \\ 2+n & \text{sinon} \end{cases}$. Par conséquent, les divisibilités $2 \mid P' \mid 2^{\min\{P,2+n\}}$ équivalent resp. $\begin{cases} \text{quand } P = 2 & \text{à} \quad 2 \mid P' \mid 2^P, \quad i.\,e. \text{ à } 2' \in \{2, 4\} \\ \text{quand } P > 2 & \text{à} \quad \exists e \in [1, 2+n], \ P' = 2^e \end{cases}$.

Preuve de la 1re équivalence.

$\boxed{\Longleftarrow}$ L'égalité $b'^{a'} \stackrel{?}{=} b^a \bmod a'$ découle, lorsque a est impair, de l'hypothèse $a' = 1$ et, lorsque b est impair, de l'hypothèse $a' \mid \Lambda_a$. Supposons donc a et b pairs et soient $\ell, m \in \mathbf{N}$ tels que $\binom{a'}{b'} = \binom{2^\ell}{2^m}$ (permis par les hypothèses $P' \mid 2^P$), l'hypothèse $2 \mid b'$ permettant de minorer $m \ge 1$: la puissance b^a est alors multiple de 2^a, donc de a' (par hypothèse $P' \mid 2^P$), d'où sa nullité *modulo* a' ; par ailleurs, la puissance $b'^{a'} = 2^{ma'}$ a un exposant $ma' \ge 1a' > \ell$, donc est elle aussi nulle $\bmod 2^\ell$.

$\boxed{\Longrightarrow}$ Si f ne tue aucun premier, la différence $a' - a$ est alors (lemme 1) divisible par chaque premier, *i. e.* est nulle, d'où l'égalité $f = \mathrm{Id}$ exclue. Si 2 est tué, alors le lemme 1 ne peut jamais s'appliquer (sa conclusion s'écrit $p \mid 2' - 2 = -1$), donc f tue chaque premier, *a fortiori* (lemme 2 et existence de décomposition en facteurs premiers) chaque entier, d'où l'égalité $f = 1$ à nouveau exclue. (Au passage, le premier 2 n'étant pas tué, le lemme 1 fournit la divisibilité $2 \mid a' - a$, d'où la parité $\boxed{2 \mid P'}$ de l'image de chaque pair P.)

On peut à présent supposer que f tue un certain premier $N > 2$: la conclusion $p \mid N - 1$ du lemme 1 implique alors la majoration $p < N$, d'où (par contraposée) la tuerie de chaque premier assez grand. Imposer en particulier $p = -1 \bmod i'$ (permis par DIRICHLET) livre la nullité $\bmod i'$ de $p^i - 1 \equiv -2$, d'où (avec la divisibilité de i' par l'impair i^i) la tuerie $\boxed{i' = 1}$. Remplacer $\binom{\blacksquare}{\square} \leftarrow \binom{a}{i}$ livre alors la divisibilité $\boxed{a' \mid \Lambda_a}$, ce qui montre (lemme 3) que a' est une puissance de 2. Il suffit pour conclure d'établir la nullité $(\bmod a')\boxed{0 \stackrel{?}{\equiv} 2^a}^{f \in \mathcal{F}} \stackrel{?}{\equiv} 2'^{a'}$. Or nous avons déjà prouvé (sens $\boxed{\Longleftarrow}$) celle de $b'^{a'}$ quand b' était une puissance de 2 autre que 2^0 : nous n'avons donc qu'à utiliser la parité $2 \mid P'$ sus-démontrée pour P pair et à remplacer $b, P \leftarrow 2$.

[3] dérouler par exemple les implications $\begin{cases} P = 2 \Longrightarrow n + 2 = 1 + 2 = 3 > P \\ \text{et } i > 1 \Longrightarrow 2^n i > 2^n 2 = 2^{n+1} \ge (n+1) + 1 = n + 2 \\ \text{et } n \ge 2 \Longrightarrow 2^n = 2 \cdot 2^{n-1} \ge 2\left((n-1)+1\right) = n + n \ge n + 2 \end{cases}$