

Une équation fonctionnelle arithmétique (IMO25 Pb3)

Marc SAGE

7 août 2025

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

$$\forall \begin{array}{c} \blacksquare \\ \square \end{array} \in \mathbf{N}^*, \quad f(\square)^{f(\blacksquare)} = \square^{\blacksquare} \bmod f(\blacksquare). \quad \text{Déterminer } \max_{n \in \mathbf{N}^*} \max_{F \in \mathcal{F}} \frac{F(n)}{n}.$$

Après une résolution en trois cas, nous allons explicitement *résoudre* l'équation fonctionnelle « appartenir à $\mathcal{F}$ », ce qui rendra limpide l'exemple parachuté réalisant le maximum trouvé.

Notations, terminologie, rappels

1. Soit $f \in \mathcal{F}$, soient $a, b, i, n, p \in \mathbf{N}^*$ tels que i impair et p premier.
Nous pourrions être amenés à quantifier universellement sur l'un de ces symboles.
2. Les images par f seront notées avec des primes, *e. g.* $n' := f(n)$. Quand cette dernière image vaut 1, nous dirons que f **tué** n ou que n est **tué** (sous-entendu : par f).
Par exemple, remplacer dans l'hypothèse $\blacksquare$ par un tué ne nous apprend rien (1 divise chaque entier !), tandis que remplacer $\square$ par un tué (et $\blacksquare \leftarrow a$) montre que $\frac{a'}{a}$ divise le p. g. c. d. $\bigwedge_{\substack{t \text{ tué}}} (t^a - 1)$.
3. L'application *valuation dyadique* sera noté $v : \boxed{v(n) := \max \{e \in \mathbf{N} ; 2^e \mid n\}}$.
4. Les modules des (non-)égalités modulaires seront précisés au-dessus d'un signe d'égalité (éventuellement barré), *e. g.* (tout ce qui suit est affirmé)

$$a^p \stackrel{p}{=} a \text{ (énoncé du petit théorème de FERMAT)} \quad \text{ou} \quad i \stackrel{2}{\neq} 0$$

$$\text{ou encore} \quad i^2 \stackrel{8}{=} 1 \quad \text{ou plus généralement} \quad i^{2^n} \stackrel{2^{n+2}}{=} 1,$$

cette dernière égalité s'établissant aisément par récurrence *via* à la factorisation¹

$$i^{2^{n+1}} - 1 = (i^{2^n} - 1)(i^{2^n} + 1).$$

Résolution

Remplacer dans l'hypothèse $\begin{pmatrix} \blacksquare \\ \square \end{pmatrix} \leftarrow \begin{pmatrix} a \\ a \end{pmatrix}$ donne la divisibilité $a' \mid a^a$. En particulier² quand $a = p$, l'image p' doit être une puissance de p , donc ou bien vaut $p^0 = 1$ (cas où p est tué) ou bien est multiple de p .

Dans ce dernier cas, chaque égalité $\stackrel{p'}{=}$ pourra devenir une égalité $\stackrel{p}{=}$, ce qui permettra d'itérer le petit théorème de FERMAT et d'utiliser l'égalité $n^{p'} \stackrel{p}{=} n$. En particulier, l'égalité $a^p \stackrel{p'}{=} a'^{p'}$ obtenue en remplaçant $\begin{pmatrix} \blacksquare \\ \square \end{pmatrix} \leftarrow \begin{pmatrix} p \\ a \end{pmatrix}$ devient $a^p \stackrel{p}{=} a'^{p'}$, çàd $a \stackrel{p}{=} a'$, d'où le

lemme clef : $p' \neq 1 \implies p \mid a' - a$.

Ce lemme va irriguer notre preuve et structurer les distinctions de cas à venir.

¹réécrire $\frac{i^{2^{n+1}} - 1}{i^{2^n} - 1} = 2 + \frac{i^{2^n} - 1}{i^{2^n} - 1}$ montrerait plus précisément que la suite $\left(v(i^{2^N} - 1)\right)_{N \geq 1}$ est affine de raison 1

²on peut également récolter l'égalité $1' = 1$ (ce qui permet par exemple de minorer le maximum cherché par $\max_{F \in \mathcal{F}} \frac{F(1)}{1} = 1$) mais elle nous sera inutile et découlera d'autres considérations : selon les cas, l'argument 1 jouera le même rôle que n'importe quel point fixe (cas 1), n'importe quel entier ≥ 1 (cas 2) ou n'importe quel impair (cas 3) – aucun rapport donc avec les premiers !

1. Supposons que f ne tue aucun premier. D'après le **lemme clef**, la différence $a' - a$ est alors divisible par chaque premier, *i. e.* est nulle, d'où l'égalité $\boxed{f = \text{Id}}$.

Alternative. Si l'on avait remplacé $\square$ également par un *premier*, nous aurions alors seulement montré la fixité de chaque *premier*. Il suffirait pour conclure d'établir la multiplicativité (totale) de f , *e. g.* en partant des égalités

$$\text{mod } p' : (ab)^{p'} = (ab)^p = a^p b^p = a^{p'} b^{p'} \quad \text{et en les passant modulo } p \\ \text{puis en faisant "varier" } p.$$

2. L'idée (plus générale) derrière les égalités ci-dessus est d'utiliser l'hypothèse en gardant le même $\square$; dans cet esprit, on obtiendrait pour chaque famille $\mathcal{D}$ finie de $\mathbf{N}^*$ l'égalité $(\prod_{d \in \mathcal{D}} d)^a \stackrel{a'}{=} (\prod_{d \in \mathcal{D}} d')^{a'}$. En particulier, quand a vaut le produit $\prod_{\mathcal{D}}$ de gauche, le membre de gauche a^a s'annule, d'où le

$$(\text{bonus utile}) \quad a = \prod d \implies a' \mid \left(\prod d' \right)^{a'}.$$

Supposons à présent que 2 est tué. Si p n'est pas tué, le **lemme clef** donne l'absurde divisibilité $p \mid 2' - 2 = -1$, laquelle impose la tuerie de chaque premier. Le **bonus utile** permet alors, avec l'existence des décompositions en facteurs premiers, de conclure à la constance $\boxed{f = 1}$.

3. Supposons enfin que f tue au moins un premier autre que 2 et soit N l'un d'eux. Observer alors grâce aux conditions $\begin{cases} N > 2 \\ N' = 1 \end{cases}$ la non-nullité de $N' - N$. Quand $p \neq 1$ nous obtenons (**lemme clef**) la divisibilité $p \mid N' - N \neq 0$ et, partant, la majoration $p \leq N - 1$, d'où par contraposée l'implication

$$p \geq N \implies p \text{ tué.}$$

L'image a' divise donc le p. g. c. d. $\bigwedge_{\pi \text{ premier} > N} (\pi^a - 1)$, ce qui a l'air fort contraignant. Que dire

déjà *sans* l'exposant a ? Imposer $\begin{cases} p \stackrel{a'}{=} -1 \\ p > N \end{cases}$ (possible par DIRICHLET³) montre que ce dernier p. g. c. d.

divise $p - 1 \stackrel{a'}{=} -2$, d'où $a' \mid 2$, ce qui est en effet contraignant. Avec l'exposant a , on s'en sort en imposant $a = i$ impair, auquel cas l'égalité $(-1)^i = -1$ livre la même conclusion $i' \mid 2$; combinée à la divisibilité $i' \mid i^i$ par un impair, on obtient la tuerie

$$\boxed{i' = 1} \quad (\text{sanity check : chaque premier} > N \text{ est impair}).$$

Notre stock d'entiers tués s'étant agrandi, nous pouvons affirmer la divisibilité (plus contraignante)

$$\underline{\underline{a' \mid D}} := \bigwedge_{\iota \in \mathbf{N} \text{ impair}} (\iota^a - 1).$$

Le p. g. c. d. de droite n'ayant aucun diviseur impair autre que 1 (chaque tel diviseur ι divise d'une part ι^a d'autre part $D \mid \iota^a - 1$), il est une puissance de 2, à savoir $\underline{\underline{D = 2^{\min_{\iota \text{ impair}} v(\iota^a - 1)}}}$. Ensuite, les valuations $v(\iota^a - 1)$ sont données par les égalité⁴ et minoration suivantes quand l'argument a est pair⁵ :

$$v(i^a - 1) - v(a) \stackrel{\text{"lifting the exponent"}}{=} \underbrace{v(i^2 - 1) - 1}_{\geq 3 \text{ car } i^2 \not\equiv 1} \geq \underline{\underline{2}} \quad \text{avec égalité ssi} \quad \begin{cases} i^2 \stackrel{2^3}{=} 1 \\ i^2 \neq 1 \end{cases},$$

i. e. ssi $i \stackrel{16}{=} \pm 3$ ou ± 5 , ce qui est réalisé *e. g.* quand $i = 3$. Il en résulte les implications

$$a \text{ pair} \implies \underline{\underline{D = 2^{2+v(a)}}} = 4 \cdot \underline{\underline{2^{v(a)}}} \mid \underline{\underline{4a}}.$$

³le théorème utilisé est souvent dit *de la progression arithmétique*

⁴cas particulier du théorème dit *LTE* (pour *Lifting The Exponent*) ; en guise de preuve expresse, l'impairité quand b est impair de $\frac{i^{2^n b} - 1}{i^{2^n} - 1} = \sum_{0 \leq \star < b} i^{2^n \star}$ permet de se ramener au cas $a = 2^n$, lequel est traité dans les rappels

⁵lorsque a est impair, son image 1 divise n'importe quoi et l'information $a' \mid D$ est vide ; plus essentiellement, le *LTE* ne s'applique **pas** et le calcul de $\underline{\underline{D = 2}}$ (laissé à la curiosité de la lectrice) ne tombe pas dans le cadre obtenu quand a est pair

La divisibilité $a' \mid 4a$ restant valide pour a impair, on peut majorer $\max_{\mathbf{N}^*} \frac{f}{\text{Id}} \leq 4$. Or l'application χ tuant chaque impair, quadruplant 4 et valant 2 sur chaque autre pair va réaliser ce maximum, d'où⁶

$$\begin{array}{l} \text{la conclusion} \\ \text{de notre énoncé} \end{array} : \quad \boxed{\boxed{\max_{n \in \mathbf{N}^*} \frac{F(n)}{n} = 4}} \quad \text{avec } F \in \mathcal{F}$$

(oui, l'application χ est parachutée et, oui, les vérifications suivantes sont complètement *ad hoc* : toute surprise devrait néanmoins être dissipée par les lumières de nos parties finales “à rebours”).

Ultime bureaucratie. Continuons à noter avec des primes les images par l'application χ . L'égalité $b'^a \stackrel{a'}{=} b^a$ est alors triviale pour a impair. Quand $a = 2$, cette égalité $b'^{\text{pair}} \stackrel{2}{=} b^2$ se reformule $b' \stackrel{2}{=} b$ et traduit l'identité de parité entre un argument et son image – identité vérifiée. Supposons enfin $a = 4$: quand b est pair, les deux membres de l'égalité $b'^{16} \stackrel{16}{=} b^4$ sont multiples de 2^4 , donc nuls, ce qui la valide ; finalement, quand b est impair, le rappel $b'^{2^n} \stackrel{2^{n+2}}{=} 1$ s'applique pour $n = 2$ et donne $b^4 \stackrel{16}{=} b'^{16}$, ce qui conclut.

Complément sur les résidus modulaires (autre preuve de $D \mid 4a$). Une alternative pour obtenir la divisibilité $D \mid 4a$ sans expliciter le p. g. c. d. D (et donc sans *LTE*) est d'invoquer des connaissances au sujet des racines n -ièmes *modulo* des puissances de 2. En effet, si DIRICHLET ne peut plus nous aider pour exploiter la divisibilité $a' \mid \bigwedge_{\iota \text{ impair}} \iota^a - 1$ (on avait extrait quand a était impair une racine a -ième de -1 modulo a'), on peut tâcher d'en garder l'idée et de regarder à quelle condition -1 admet quand a est pair une racine a -ième *modulo* une puissance de 2 (à savoir a'). Or un article de 2022 traite précisément de ces questions⁷.

Nous imposerons a pair pour la suite de ce paragraphe. Nous avons alors le

Théorème : *Supposons $n \geq 3$. L'équation $r^a \stackrel{2^n}{=} i$ admet alors une solution (en $r \in \mathbf{N}$) ssi $i \stackrel{2^n \wedge 4a}{=} 1$.*

Appliquons. Nous avons déjà vu que le p. g. c. d. D est une puissance de 2 et l'on peut donc imposer $D = 2^n$, l'égalité $i^a \stackrel{8}{=} 1$ permettant de minorer $n \geq 3$. Imposons alors $i = 1 + D \wedge 4a$ (qui est bien impair par parité de D) et soit $r \in \mathbf{N}$ tel que $r^a \stackrel{2^n}{=} i$. Cette dernière égalité passe *modulo* 2 et donne $r^a \stackrel{2}{=} i$, çàd $r \stackrel{2}{=} 1$, imparité qui montre que D divise $r^a - 1 \stackrel{D}{=} i - 1 = D \wedge 4a$, d'où la conclusion $D \mid 4a$.

Remonter le courant. Prenons le temps de bien voir en quoi la condition $\underline{a' \mid D}$ de notre cas 3 captait l'information restant de l'appartenance $f \in \mathcal{F}$: devons-nous chercher ailleurs ? le *pouvions-nous* seulement ? Cela nous permettra *in fine* d'explicitier l'ensemble $\mathcal{F}$ et d'éclairer les vérifications bureaucratiques ci-dessus⁸.

Soit $F : \mathbf{N}^* \rightarrow \mathbf{N}^*$ dont on continue à noter les images avec des primes. Supposons $F \neq \text{Id}$ et $F \neq 1$.

Soit $P \geq 2$ pair. Montrons alors l'équivalence $F \in \mathcal{F} \iff \left\{ \begin{array}{l} i' = 1 \\ 2 \mid P' \mid 2^P \\ P' \mid \bigwedge_{\iota \text{ impair}} \iota^P - 1 \end{array} \right.$

$\implies$ Reprenons notre cas 3 à l'affirmation $\underline{a' \mid D}$: il nous reste à établir les divisibilités $2 \stackrel{?}{\mid} P' \stackrel{?}{\mid} 2^P$.

Tout d'abord, puisque 2 n'est pas tué⁹, le **lemme clef** fournit la divisibilité $2 \mid a' - a$, donc l'image a' a même parité que a , d'où $\boxed{2 \mid P'}$.

Ensuite, l'image $\boxed{a' \text{ est une puissance de } 2}$ car divise une telle puissance – le p. g. c. d. D . Autre preuve (plus directe) en footnote¹⁰. *Sanity check*¹¹ : quand $a = i$, on a bien $i' = 2^0$.

⁶ conjointement à l'égalité $\max_{\mathbf{N}^*} \frac{f}{\text{Id}} = 1$ des deux premiers cas (*i. e.* quand $f = \text{Id}$ ou $f = 1$)

⁷ Ferucio Laurențiu ȚIPLEA, *Efficient Generation of Roots of Power Residues Modulo Powers of Two*, pdf disponible sur <https://www.mdpi.com/2227-7390/10/6/908>

⁸ la lectrice est invitée à repérer dans ce qui suit où – et sous quelle forme – chacune de ces vérifications apparaît

⁹ l'hypothèse est lointaine... mais structure génériquement la disjonction des cas 2 et 3

¹⁰ Supposons $a = 2^n i$ et appliquons le **bonus utile** (cf. cas 2) : l'image a' divise le produit $(2^n i')^{a'}$. Or chaque facteur $2'$ est une puissance de 2 (en tant qu'image du premier 2) et le dernier facteur i est tué (en tant qu'impair), donc a' divise une puissance de 2, *a fortiori* EST une puissance de 2.

¹¹ ce sanity check est en fait *nécessaire* au sens de la réciproque suivante : *si chaque image est une puissance de 2*, l'image i' en est alors une, qui plus est impaire (vu l'égalité $i' \stackrel{2}{=} i$), çàd vaut $2^0 = 1$, donc *chaque impair est tué*

Soient enfin $\begin{smallmatrix} \ell \in \mathbf{N} \\ m \in \mathbf{N}^* \end{smallmatrix}$ tels que $\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} 2^\ell \\ 2^m \end{pmatrix}$, la condition $m \geq 1$ équivariant à la parité de b . Nous allons majorer $\ell \stackrel{?}{\leq} a$, ce qui conclura à $\boxed{P' \mid 2^P}$ (remplacer $a \leftarrow P$).

Nous voulons la divisibilité $2^\ell \mid 2^a$, *i. e.* la nullité mod a' de $2^a \stackrel{a'}{=} 2^{a'}$: montrons plus généralement celle de $b^{a'} = 2^{ma'}$ (il suffira d'y remplacer $b \leftarrow 2$). Vu les minoration $\begin{cases} m \geq 1 \\ a' = 2^\ell > \ell \end{cases}$, l'exposant ma' majore 1ℓ , d'où $2^\ell \mid 2^{ma'}$, ce qu'il fallait démontrer.

$\boxed{\Leftarrow}$ Supposons réciproquement $\left\{ \begin{array}{l} i' = 1 \\ 2 \mid P' \mid 2^P \\ P' \mid \bigwedge_{\iota \text{ impair}} \iota^P - 1 \end{array} \right.$. L'égalité $b^{a'} \stackrel{a'}{=} b^a$ est alors triviale pour a impair

(1 divise chaque entier !) et vérifiée quand b est pair grâce au travail du paragraphe précédent (la tuerie des impairs permet bien de mettre a' et b' sous forme de puissances de 2, la parité de b entraîne la nullité $b'^{a'} \stackrel{a'}{=} 0$ et, avec la condition $a' \mid 2^a$, la nullité $b^a = (\frac{b}{2}2)^a \stackrel{a'}{=} 0$). L'affirmer pour chaque $a, b \in \mathbf{N}^*$ revient donc à l'affirmer pour chaque a pair et chaque b impair, affirmation équivalant précisément à l'hypothèse $P' \mid \bigwedge_{\iota \text{ impair}} \iota^P - 1$, d'où la conclusion $F \in \mathcal{F}$.

À la source. Incorporons enfin l'explicitation $\bigwedge_{\iota \text{ impair}} \iota^P - 1 = 2^{2+v(P)}$ dans l'équivalence sus-établie.

Imposons $P = 2^n i$ pour alléger. La conjonction $\left\{ \begin{array}{l} P' \mid 2^{2+n} \\ P' \mid 2^P \end{array} \right.$ se traduit alors par $P' \mid 2^{\min\{P, 2+n\}}$, le minimum en exposant¹² valant $\left\{ \begin{array}{ll} 2 & \text{si } P = 2 \\ 2+n & \text{sinon} \end{array} \right.$. Par conséquent, les divisibilités $2 \mid P' \mid 2^{\min\{P, 2+n\}}$ équivalent resp. $\left\{ \begin{array}{ll} \text{quand } P = 2 & \text{à } 2 \mid P' \mid 2^P, \quad i. e. \text{ à } 2' \in \{2, 4\} \\ \text{quand } P > 2 & \text{à } \exists e \in [1, 2+n], \quad P' = 2^e \end{array} \right.$.

Conclusion. Nous pouvons conclure enfin à la description de $\mathcal{F} \setminus \{\text{Id}, 1\}$:

$$F \in \mathcal{F} \iff \begin{cases} 2' \in \{4, 8\} \\ \forall A \text{ impair}, A' = 1 \\ \forall B \text{ pair} \neq 2, \exists e \in \mathbf{N}, \begin{cases} B' = 2^e \\ 1 \leq e \leq 2 + v(B) \end{cases} \end{cases} \quad (\text{ou } F = \text{Id} \text{ ou } F = 1).$$

Construire un élément de $\mathcal{F}$, vu comme la suite de ses images $(1', 2', 3' \dots)$, revient donc – outre la suite constante $(1, 1, 1, \dots)$ et la suite identité $(1, 2, 3, \dots)$ – à choisir une image dans chacune des colonnes suivantes¹³ :

[illegible]

Le maximum 4 annoncé sera alors atteint ss'il y a au moins une puissance de 2 (autre que 2^0 ou 2^1) pour laquelle l'exposant e choisi ci-dessus est maximal (cas d'égalité dans les divisibilités $a' \mid 4 \cdot 2^{v(a)} \mid 4a$), *i. e.* si l'on choisit au moins une image encadrée : $\boxed{16}, \boxed{32}, \boxed{64} \dots$

pour la route : comment reconstruire ainsi l'application χ parachutée ?

$$^{12}\text{d\'erouler par exemple les implications} \quad \begin{cases} P = 2 \implies n + 2 = 1 + 2 = 3 > P \\ \text{et } i > 1 \implies 2^n i > 2^n 2 = 2^{n+1} \geq (n + 1) + 1 = n + 2 \\ \text{et } n \geq 2 \implies 2^n = 2 \cdot 2^{n-1} \geq 2((n - 1) + 1) = n + n \geq n + 2 \end{cases}$$

¹³Voici 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 $(2^E)_{1 \leq E \leq n+2}$, 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, 8).