Une belle équation diophantienne (IMO22 Pb5)

Marc SAGE

10 août 2022

Énoncé. *Trouver les entiers positifs a, b, p avec p premier tels que*

$$a^p = b! + p.$$

Soient de tels entiers.

Idée 1 : des facteurs communs ! EG si p minore b, il divisera $b!$, donc divisera la somme $b! + p = a^p$, çàd divisera a. De même, si un diviseur de a minore b, il divisera alors la différence $a^p - b! = p$, donc vaudra 1 ou p.
Idée 2 : des ordres de grandeur ! EG $b! < b^b$. On utilisera en particulier la minoration[1]

$$p^{p-1} - 1 > (p-1)!$$

ainsi que l'implication[2]

$$2 \leq b < p \Longrightarrow b^p - p > b^b.$$

Idée 3 : regarder les valuations dyadiques. Seul nous suffira le résultat suivant[3], en apparence parachuté mais qui apparaîtra en temps voulu : pour chaques entiers $r \equiv s \equiv 1$ *modulo* 4, on a l'égalité[4]

$$v\left(r^n - s^n\right) = v\left(r - s\right) + v\left(n\right).$$

Mise en oeuvre.

Préparation
Minorons $\boxed{a, b \geq 2}$: on majore

$$a^p = b! + p \geq 0! + p > 1, \text{ d'où } a > 1, \text{ çàd } a \geq 2, \text{ puis}$$
$$b! - 1 = a^p - p - 1 \geq 2^p - (p+1) \overset{p>1}{>} 0, \text{ d'où } b! > 1, \text{ çàd } b \geq 2.$$

Traitons le cas $p = 2$. Si $b! \equiv 0 \ [4]$ alors $a^2 \equiv 2 \ [4]$ *absurde*[5], d'où $b \leq 3$ çàd $b \in \{2, 3\}$. On obtient alors

$$a^2 = \begin{array}{l} 2! + 2 = 4 = 2^2, \\ 3! + 2 = 8 \ \textit{absurde} \end{array}, \text{ d'où } \begin{pmatrix} a & b \\ & p \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ & 2 \end{pmatrix}, \text{ qui est bien solution.}$$

---

[1] développer le binôme $\left(\underline{p-1} + 1\right)^{p-1}$ et ne garder que les 2 termes extrêmes, ou bien établir par récurrence $(n+1)^n > n! + 1$

[2] s'établit par croissance stricte de la suite $(n^p - n)$ ou par récurrence sur p, l'initialisation découlant dans les deux cas des minorations

$$b^{b+1} - b^b = \underbrace{b^b}_{\geq b^2 \geq 2b > b+1} \underbrace{(b-1)}_{\geq 1} > b + 1$$

[3] cas particulier du théorème dit *LTE* (*lifting the exponant*) qui étudie les valuations $v_p\left(\alpha^N - \beta^N\right)$ des différences de puissances de même exposant

[4] À établir par récurrence sur $v\left(n\right)$. Si n impair, alors

$$\frac{r^n - s^n}{r - s} = \sum_{i+j=n-1} r^i s^j \overset{mod.}{\underset{4}{\equiv}} \sum_0^{n-1} 1 = n \in \{1, 3\}.$$

Ensuite, évaluer $\frac{r^{2n} - s^{2n}}{r^n - s^n} = r^n + s^n \overset{mod.}{\underset{4}{\equiv}} 1^n + 1^n = 2$.

[5] rappelons que, *modulo* 4, les carrés sont 0 et 1

On imposera donc $p \geq 3$, çàd $\boxed{p \text{ impair}}$.

(on aurait également pu traiter le cas $p = 3$ à l'aide des cubes *modulo* 9, ce qui aurait forcé $b \leq 5$ et fourni une deuxième solution $\binom{a\ b}{p} = \binom{3\ 4}{3}$ via l'égalité $3^3 - 3 = 24 = 4!$)

La suite procède en deux morceaux **indépendants** :

1. montrer l'égalité $a = p$;
2. prouver l'équivalence $p^p - p = b! \iff \binom{p}{b} = \binom{3}{4}$.

En conséquence, les solutions mises au jour en aval seront les deux seules de notre équation :

$$2^2 = 2! + 2 \qquad \text{et} \qquad 3^3 = 4! + 3.$$

Gros œuvre. Établissons l'égalité $a = p$.

Supposons $p > b$. On peut alors majorer (intro *idée 2*) $a^p = b! + p \leq b^b + p < b^p$, d'où $a < b$. Cette majoration conduit d'une part (avec l'hypothèse) à $a < p$, d'autre part (*idée 1*) à $a \mid p$, le tout contredisant $a \geq 2$.

Il en résulte $\boxed{p \leq b}$, d'où (*idée 1*) la divisibilité $p \mid a$. Notons $\begin{cases} d := \frac{a}{p} \\ m := b - p \end{cases}$ et montrons $d = 1$.

Simplifier par p l'équation de départ $a^p - p = b!$ donne

$$d^p p^{p-1} - 1 = (p-1)! \prod_{i=1}^{m} (p+i)\,.$$

Filtrer *modulo* p livre $0 - 1 \equiv ?m!$, d'où $m! \not\equiv 0\ [p]$, çàd $m < p$, ce qui permet de majorer le produit de droite et ainsi (en calquant $(p-1)! = \prod_{i=1}^{p-1} (p-i)$) de majorer

$$d^p p^{p-1} - 1 \leq \prod_{i=1}^{p-1} \underbrace{(p-i)\,(p+i)}_{=p^2-i^2<p^2} < \prod_{i=1}^{p-1} p^2 = p^{2p-2} \underset{\text{(ok avec } \square, p>2)}{\overset{\square \leq p\square - 1}{<}} p^{2p-1} - 1,$$

d'où $d^p < p^p$, çàd $\boxed{d < p}$.

Combiner les deux majorations encadrées fournit $d \leq b$, donc (*idée 1*) le diviseur $d \mid a$ vaut 1 ou p et la majoration $d < p$ permet[6] de conclure.

Finition. Une fois établie l'égalité $a = p$, notre équation devient

$$p^p - p = b! \qquad \text{ou encore} \qquad p^{p-1} - 1 = \frac{b!}{p}.$$

D'après le LTE (*idée 3* avec les hypothèses $p^2 \equiv 1\ [4]$ bien vérifiées), la valuation dyadique de la différence $p^{p-1} - 1 = \left(p^2\right)^{\frac{p-1}{2}} - 1^{\frac{p-1}{2}}$ vaut $v\left(p^2-1\right) + v\left(\frac{p-1}{2}\right)$, çàd celle du produit des

$$\text{trois facteurs } p+1 > p-1 > \frac{p-1}{2}.$$

Or ces facteurs apparaissent DÉJÀ dans le produit $\frac{b!}{p}$ sous l'hypothèse $b > p$, hypothèse découlant de fait *(idée 2)* de la minoration $p^{p-1} - 1 > (p-1)!$. Ceci montre que les AUTRES facteurs de $\frac{b!}{p}$ ne contribuent pas à sa valuation dyadique, çàd sont impairs.

En particulier, le pair $2 \leq b$ doit valoir l'un de ces trois facteurs, d'où $p \in \{1, 3, 5\}$. Or la différence $5^5 - 5 = (625-1) \cdot 5 \begin{matrix} < 5000 < 7! \\ > 1000 > 6! \end{matrix}$ n'est pas une factorielle, ce qui nous laisse avec le seul cas $p = 3$ où $b! = 3^3 - 3 = 4!$, d'où la conclusion.

[6] une alternative (nettement plus longue que ces deux courtes lignes) serait de regarder l'équation *modulo* $\frac{p\pm1}{2}$ et de montrer que les ordres de d valent 1, d'où $d \equiv 1\ \left[\frac{p^2-1}{4}\right]$, puis d'utiliser la majoration obtenue $d < p$ en minorant $p \leq \frac{p^2-1}{4}$ afin de situer l'unique reste $d = 1$