PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE
À RENVOYER AU PLUS TARD LE 17 FÉVRIER 2022

Les consignes suivantes sont à lire attentivement :

- Le groupe junior est constitué des élèves nés en 2007 ou après. Les autres élèves sont dans le groupe senior.
- Les exercices classés “Juniors” ne sont à chercher que par les élèves du groupe junior.
- Les exercices classés “Seniors” ne sont à chercher que par les élèves du groupe senior.
- Les exercices doivent être cherchés de manière individuelle.
- Utiliser des feuilles différentes pour des exercices différents.
- Respecter la numérotation des exercices.
- Bien préciser votre nom en lettres capitales, et votre prénom en minuscules sur chaque copie.

Exercices Juniors

Exercice 1. Montrer que pour tout entier n, le nombre $n^3 - 7n$ est divisible par 6.

Solution de l'exercice 1 Une première approche est de regarder l'expression modulo 6 :

$$n^3 - 7n \equiv n^3 - n \equiv (n-1)n(n+1) \mod 6$$

donc il suffit de montrer que 6 divise $(n-1)n(n+1)$. Or parmi trois nombres consécutifs, au moins un est divisible par 2 et au moins un est divisible par 3. Ainsi comme 2 et 3 sont premiers entre eux, $6 \mid n^3 - n$ et donc 6 divise $n^3 - 7n$.

Une deuxième approche qui fonctionne aussi ici consiste aussi à regarder l'expression $n^3 - 7n$ et de montrer à la main que celle-ci est toujours nulle en faisant une disjonction de cas sur les valeurs que peut prendre n modulo 6.

n	$n^3 - 7n$
0	$0^3 - 7 \cdot 0 \equiv 0 + 0 \equiv 0$
1	$1^3 - 7 \cdot 1 \equiv 1 - 1 \equiv 0$
2	$2^3 - 7 \cdot 2 \equiv 8 - 2 \equiv 0$
3	$3^3 - 7 \cdot 3 \equiv 3 - 3 \equiv 0$
$4 \equiv -2$	$(-2)^3 - 7 \cdot (-2) \equiv -2 + 2 \equiv 0$
$5 \equiv -1$	$(-1)^3 - 7 \cdot (-1) \equiv -1 + 1 \equiv 0$

Ainsi, quelle que soit la valeur de n modulo 6, $n^3 - 7n \equiv 0$.

Commentaire des correcteurs : L'exercice est très bien résolu.

Exercice 2. Soient a, b, c trois entier tels que 7 divise $a^2 + b^2 + c^2$. Montrer que 7 divise $a^4 + b^4 + c^4$.

Solution de l'exercice 2

Les carrés modulo 7 valent $0, 1, 2, 4$. On cherche donc toutes les sommes de trois de ces nombres étant divisible par 7. Après avoir testé toutes les possibilités, on s'aperçoit que les seuls ensembles de trois carrés modulo 7 dont la somme est divisible par 7 sont $\{0, 0, 0\}$ et $\{1, 2, 4\}$.

On alors $a^4+b^4+c^4 \equiv 0^2+0^2+0^2 \equiv 0 \mod 7$ ou $a^4+b^4+c^4 \equiv 1^2+2^2+4^2 \equiv 1+4+16 \equiv 0 \mod 7$

Dans les deux cas, $a^4 + b^4 + c^4 \equiv 0 \mod 7$, comme désiré.

Commentaire des correcteurs : L'exercice est très bien résolu.

Exercice 3. Soit $a, b, c \geqslant 1$ des entiers tels que $a^b \mid b^c$ et $a^c \mid c^b$. Montrer que $a^2 \mid bc$.

Solution de l'exercice 3

Nous allons regarder les valuations p-adiques de chacun des nombres premiers a, b et c. En effet, il suffit de montrer que pour tout nombre premier p, on a $2v_p(a) = v_p(a^2) \leqslant v_p(bc) = v_p(b) + v_p(c)$.
Soit p un nombre premier. L'hypothèse que $a^b \mid b^c$ se traduit en terme de valuation $p-$adique par $bv_p(a) \leqslant cv_p(b)$, ou encore $v_p(a) \leqslant \frac{c}{b} v_p(b)$. De même, on obtient que $v_p(a) \leqslant \frac{b}{c} v_p(c)$.

En multipliant les deux relations, on trouve que $v_p(a)^2 \leqslant v_p(b)v_p(c)$. On a donc, d'après l'inégalité des moyennes :

$$v_p(a) \leqslant \sqrt{v_p(b)v_p(c)} \leqslant \frac{v_p(b) + v_p(c)}{2}$$

ce qui donne bien $2v_p(a) \leqslant v_p(b) + v_p(c)$ comme voulu. Ceci étant vrai pour tout premier p, on a bien $a^2 \mid bc$.

Commentaire des correcteurs : L'exercice est très bien résolu.

Exercice 4. Trouver tous les couples d'entiers naturels non nuls (x, n) tels que

$$3 \cdot 2^x + 4 = n^2.$$

Solution de l'exercice 4 Pour $x = 0$, l'équation devient $n^2 = 7$ qui n'a pas de solution. Supposons $x > 0$, on factorise : $3 \cdot 2^x = (n-2)(n+2)$. Le membre de gauche est pair donc le membre de droite est paire. Les deux facteurs du membre de droite sont de même parité donc ils sont tous les deux pairs et on a deux cas :

— Cas 1 : $3 \cdot 2^a = n - 2$ et $2^b = n + 2$, avec $a + b = x$. On peut combiner ces deux équations pour trouver $2^b = 3 \cdot 2^a + 4$. Notons que $n+2$ et $n-2$ ont pour différence 4 donc ils ne peuvent pas être tous les deux divisibles par 8. On a donc $a \leqslant 2$ ou $b \leqslant 2$. Or $2^b > 4$, donc $b > 2$ et on déduit que $a \leqslant 2$. Si $a = 0$, $2^b = 3 + 4 = 7$ ce qui n'est pas possible. Si $a = 1$, $2^b = 6 + 4 = 10$ ce qui n'est pas possible non plus. Si $a = 2$, alors $2^b = 12 + 4 = 16$ donc $b = 4$. On obtient $x = 6$ et $n = 14$. réciproquement, on vérifie que $3 \cdot 2^6 + 4 = 196 = 14^2$ et le couple $(6, 14)$ est bien solution.

— Cas 2 : $3 \cdot 2^a = n + 2$ et $2^b = n - 2$, avec $a + b = x$. Les deux équations combinées donnent $2^b + 4 = 3 \cdot 2^a$. De même que précédemment, on a $a \leqslant 2$ ou $b \leqslant 2$.

1. Si $b \leqslant 2$, alors $b = 0, 1$ ou 2. Si $b = 0$, alors $5 = 3 \cdot 2^a$ ce qui n'est pas possible. Si $b = 1$, $6 = 3 \cdot 2^a$ et $a = 1$, soit $x = 2$ et $n = 4$ et on vérifie que $3 \cdot 2^2 + 4 = 16 = 4^2$ et $(2, 4)$ est bien solution. Si $b = 2$, alors $8 = 3 \cdot 2^a$ ce qui n'est pas possible.
2. Si $a \leqslant 2$, alors $a = 0, 1$ ou 2. Si $a = 0$, $2^b + 4 = 3 < 4$ ce qui n'est pas possible. Si $a = 1$, on retombe sur le cas où $b = 1$ et sur le couple $(2, 4)$. Si $a = 2$, $2^b + 4 = 12$ donc $b = 3$. Ceci donne $x = 5$ et $n = 10$. Réciproquement, on vérifie que $3 \cdot 2^5 + 4 = 100 = 10^2$ et $(5, 10)$ est bien solution.

Ainsi l'ensemble des couples (x, n) solutions est $\{(2, 4), (5, 10), (6, 14)\}$

Commentaire des correcteurs : L'exercice est globalement bien résolu, mais de nombreux élèves oublient des cas, ou oublient tout simplement de vérifier les solutions trouvées, chose pourtant cruciale dans une équation diophantienne.

Exercice 5. Un ensemble E d'entiers strictement positifs est dit *intéressant* si pour tout $n \geqslant 1$ et pour tous $x_1, \ldots, x_n$ des éléments de E deux à deux distincts, leur moyenne arithmétique $\frac{1}{n}(x_1 + \ldots + x_n)$ et leur moyenne géométrique $(x_1 \cdot \ldots \cdot x_n)^{\frac{1}{n}}$ sont des entiers.

1. Existe-t-il un ensemble E intéressant contenant exactement 2022 éléments ?
2. Existe-t-il un ensemble E intéressant infini ?

Solution de l'exercice 5

1) Pour commencer, on peut remarquer que si $n \geqslant 1$, alors dès que $x_1, \ldots, x_n \geqslant 1$ sont des entiers tous multiples de n, chacun des nombres $\dfrac{x_k}{n}$ est un entier, de sorte que leur somme $\dfrac{1}{n}(x_1 + \ldots + x_n)$ est un entier. De même, si $n \geqslant 1$, alors dès que $x_1, \ldots, x_n \geqslant 1$ sont des entiers tous puissances n-ièmes parfaites, chacun des nombres $x_k^{1/n}$ est entier, de sorte que leur produit $(x_1 \times \ldots \times x_n)^{\frac{1}{n}}$ est un entier. Pour trouver un ensemble E intéressant contenant exactement 2022 éléments, il suffit donc que pour tout $1 \leqslant n \leqslant 2022$, tous les éléments de E soient à la fois des multiples de n et des puissances n-ièmes parfaites. Pour cela, il suffit que tous les éléments de E soient à la fois des multiples de $2022!$, et des puissances $2022!$-ièmes parfaites. Ainsi, $E = \{(2022!)^{k2022!}, 1 \leqslant k \leqslant 2022\}$ convient.

2) Nous allons montrer qu'il n'existe pas d'ensemble intéressant infini. En fait, on va montrer qu'il n'existe même pas d'ensemble infini d'entiers strictement positifs vérifiant l'hypothèse sur les moyennes arithmétiques. En effet, supposons par l'absurde qu'un tel ensemble infini E existe, c'est-à-dire que pour tout $n \geqslant 1$ et $x_1, \ldots, x_n \in E$ deux à deux distincts, la moyenne arithmétique $\frac{1}{n}(x_1 + \ldots + x_n)$ est un entier. Soit $a < b$ deux éléments quelconques de E et $n \geqslant 2$. Choisissons $x_1 < \ldots < x_{n-1}$ des éléments deux à deux distincts de E, et distincts de plus de a et b. L'hypothèse appliquée successivement aux n-uplets $(x_1, \ldots, x_{n-1}, a)$ et $(x_1, \ldots, x_{n-1}, b)$ assure que n divise à la fois $x_1 + \ldots + x_{n-1} + a$ et $x_1 + \ldots + x_{n-1} + b$. Ainsi, n divise la différence de ces deux nombres qui vaut $a - b$. Ceci étant vrai pour tout $n \geqslant 2$, l'entier $a - b$ admet un nombre infini de diviseurs. Il est donc nul, c'est-à-dire que $a = b$. Ceci est en contradiction avec notre hypothèse de départ, un tel ensemble E n'existe donc pas.

Commentaire des correcteurs : La première question de l'exercice est plus souvent traitée que la deuxième. Attention, plusieurs élèves y construisent un ensemble dont les moyennes arithmétique et géométrique de tous les éléments de l'ensemble sont entièress, mais pas les moyennes des éléments de n'importe quel sous-ensemble.

Exercice 6. Soit p un nombre premier. Montrer qu'il existe une permutation $(a_1, \ldots, a_p)$ de $(1, \ldots, p)$ telle que les entiers $a_1, a_1 \cdot a_2, \ldots, a_1 \cdot a_2 \cdot \ldots \cdot a_p$ donnent p restes deux à deux distincts lorsque qu'on réalise leur divison euclidienne par p.

Solution de l'exercice 6 On peut être très optimiste sur cet exercice et vouloir que $a_1 a_2 \cdots a_k \equiv k \mod p$ pour tout k compris entre 1 et p. Il faut donc que $a_1 = 1$ et pour tout $k \neq 1$:

$$a_k \equiv \frac{a_1 \cdots a_k}{a_1 \cdots a_{k-1}} \equiv \frac{k}{k-1} \mod p$$

où l'on note $\frac{a}{b}$ tout nombre entier dont le reste c par la division euclidienne par p vérifie $cb \equiv a \mod p$, qui existe toujours dès que b est non nul. Ainsi, pour $k \neq 1$, on peut poser a_k l'élément de $\{1, \ldots, p\}$ vérifiant $(k-1)a_k \equiv k \mod p$.
Il reste juste à vérifier que tous les nombres a_k que l'on a formés sont bien deux à deux distincts, et ainsi que $\{a_1, \ldots, a_p\}$ est bien une permutation de $\{1, \ldots, p\}$. Supposons qu'il existe $i < j$ tels que $a_i \equiv a_j$. Si $i = 1$, pour tout $j \geqslant 2$, $\frac{j}{j-1} \neq 1 \mod p$. Sinon $\frac{i}{i-1} \equiv \frac{j}{j-1}$ implique que $ij - j \equiv ij - i$, soit $i \equiv j \mod p$, ce qui est en contradiction avec notre hypothèse de départ.
Ainsi tous les a_k sont différents modulo p. Etant donné qu'il y a p termes dans la suite et p éléments dans $\{1, 2, \cdots, p\}$, $(a_1, a_2, \cdots, a_p)$ est une permutation de $(1, 2, \cdots p)$.

Commentaire des correcteurs : L'exercice a été peu traité. Avoir l'idée de créer une permutation telle que $a_1 a_2 \ldots a_i \equiv i \mod p$ était l'idée principale du problème. Pour la mettre en oeuvre, il fallait une bonne compréhension de la notion d'inverse modulo p, et c'était le cas de la plupart des élèves qui ont rendu une solution.

Exercice 7. Soit $n \geqslant 1$ un entier. Trouver tous les diviseurs $d \geqslant 1$ de $3n^2$ tels que $n^2 + d$ soit un carré parfait.

Solution de l'exercice 7 Soit $d \geqslant 1$ un diviseur de $3n^2$ tel que $n^2 + d$ soit un carré parfait. Puisque $n^2 < n^2 + d <= n^2 + 3n^2 = (2n)^2$, il existe $k \in [\![1, n]\!]$ tel que $n^2 + d = (n + k)^2$. En simplifiant, on obtient $d = 2kn + k^2$, de sorte que $k(k + 2n) \mid 3n^2$.
Notons $\alpha = \gcd(k, n) \geqslant 1$. On dispose d'entiers $\ell, m \geqslant 1$ premiers entre eux tels que avec $k = \alpha l$, $n = \alpha m$. La relation de divisibilité précédente s'écrit alors, après simplification, $\ell(\ell + 2m) \mid 3m^2$. Or on a $\gcd(\ell + 2m, m) = \gcd(\ell + 2m - 2m, m) = \gcd(\ell, m) = 1$, c'est-à-dire $\ell + 2m$ premier avec m, donc avec m^2. Comme $\ell + 2m \mid 3m^2$, on a par le lemme de Gauss $\ell + 2m \mid 3$, c'est-à-dire $\ell + 2m \in \{1, 3\}$. Mais $\ell, m \geqslant 1$ donc $\ell + 2m \geqslant 3$. Autrement dit, $\ell + 2m = 3$ et donc nécessairement, $\ell = m = 1$. Alors $k = n = \alpha$, et $d = k(k + 2n) = 3n^2$.
Réciproquement, $d = 3n^2$ convient puisque c'est un diviseur de $3n^2$ et que $n^2 + 3n^2 = (2n)^2$.

Commentaire des correcteurs : L'exercice est peu traité. Toutes les copies ont la bonne intuition de l'unique solution. D'autres démonstrations que celle du corrigé ont été proposées par des élèves (elles passent notamment par la parité des valuations p-adiques pour p premier et en trouvant les m tels que $\frac{m+3}{m}$ est un carré de rationnel).

Exercice 8. Un ensemble A d'entiers est dit *admissible* s'il vérifie la propriété suivante : pour tous $x, y \in A$ (non nécessairement distincts), et pour tout $k \in \mathbb{Z}$, on a $x^2 + kxy + y^2 \in A$.
Déterminer tous les couples d'entiers non nuls (m, n) tels que le seul ensemble *admissible* contenant à la fois m et n soit $\mathbb{Z}$.

Solution de l'exercice 8 Remarquons que si $d = \gcd(m, n) > 1$ alors l'ensemble A des multiples de d est un ensemble admissible contenant n et m mais n'étant pas égal à $\mathbb{Z}$. En effet, si x et y sont multiples de d, alors pour tout entier k, $x^2 + kxy + y^2$ est bien divisible par d et est dans A. On déduit que les couples (m, n) recherchés doivent vérifier $\gcd(m, n) = 1$.

Réciproquement, soient m et n des entiers tels que $\gcd(m, n) = 1$. Montrons que tout ensemble admissible contenant m et n est $\mathbb{Z}$. Soit A un ensemble admissible contenant m et n. Remarquons que si $x \in A$, alors l'hypothèse nous donne que pour tout entier k, l'entier $x^2 + kx \cdot x + x^2 = (k+2)x^2$ est dans A. On déduit que tout multiple de x^2 est dans A si x est dans A.
Notons que si $\gcd(m, n) = 1$, alors on a aussi $\gcd(m^2, n^2) = 1$. D'après le théorème de Bezout, on dispose donc d'entiers $u, v \in \mathbb{Z}$ tels que $um^2 + vn^2 = 1$. Comme um^2 et vn^2 sont dans A, en appliquant l'hypothèse à $x = um^2$, $y = vn^2$ et $k = 2$, on a

$$\left(um^2\right)^2 + 2um^2vn^2 + \left(vn^2\right)^2 = (um^2 + vn^2)^2 = 1^2 = 1 \in A$$

Par conséquent, $\forall k \in \mathbb{Z}, k \cdot 1^2 \in A$. Ainsi $A = \mathbb{Z}$ et le seul ensemble admissible contenant m et n est $\mathbb{Z}$.

Les couples recherchés sont donc les couples d'entiers (m, n) premiers entre eux.

Commentaire des correcteurs : Parmi les élèves ayant rendu une tentatives, on trouve beaucoup de solutions complètes. Parmi les solutions non complètes, la plupart des élèves ont deviné la nature des couples solutions et ont réussi à montrer que si 1 est dans A, alors $A = \mathbb{Z}$. Avoir été si loin dans ce problème difficile est déjà très bien !

Exercice 9. Déterminer tous les triplets d'entiers naturels (a, b, c) tels que

$$a! + 5^b = 7^c.$$

Solution de l'exercice 9 Un premier réflexe à avoir est de regarder les petites valeurs de a, b et c que l'on peut trouver dans une solution (a, b, c).
Tout d'abord, si $a = 0$ ou $a = 1$, alors $a! = 1$, donc $0 \equiv a! + 5^b \equiv 7^c \equiv 1 \pmod 2$, ce qui est impossible. On en déduit que $a \geqslant 2$.
Puis, si $a \geqslant 7$, alors $5^b \equiv a! + 5^b \equiv 7^c \pmod 5$ et $5^b \equiv a! + 5^b \equiv 7^c \pmod 7$, donc $b = c = 0$. Mais alors $a! + 5^b = a! + 1 \neq 1 = 7^c$, ce qui est impossible. On en déduit que $2 \leqslant a \leqslant 6$.
Supposons maintenant que $b \leqslant 1$. Alors

$$7^c = a! + 5^b \in \{2, 6, 24, 120, 720\} + \{1, 5\} = \{3, 7, 11, 25, 29, 121, 125, 721, 725\}.$$

Dans ce dernier ensemble, seul 7 lui-même est une puissance de 7. On en déduit les deux triplets solutions $(a, b, c) = (2, 1, 1)$ et $(3, 0, 1)$, qui sont les deux seules solutions pour $b \leqslant 1$.
On s'intéresse enfin aux cas où $b \geqslant 2$. Alors $a! \equiv a! + 5^b \equiv 7^c \pmod{25}$. Or, comme $7^2 \equiv -1 \pmod{25}$, on sait que $7^c \equiv 1, 7, -1$ ou $-7 \pmod{25}$ (selon que $c \equiv 0, 1, 2$ ou $3 \pmod 4$) et que $a! \equiv 2, 6, -1, -5$ ou $-5 \pmod{25}$ (selon que a vaut $2, 3, 4, 5$ ou 6). Cela signifie donc que $a = 4$ et $c \equiv 2 \pmod 4$.
Mais alors $(-3)^b \equiv a! + 5^b \equiv (-1)^c \equiv 1 \pmod 8$, ce qui signifie que b est pair. On pose alors $\beta = b/2$ et $\gamma = c/2$, de sorte que

$$24 = a! = 7^c - 5^b = (7^\gamma + 5^\beta)(7^\gamma - 5^\beta).$$

On en déduit notamment que $7^\gamma + 5^\beta \leqslant 24$, donc que $\gamma \leqslant 1$ et $c \leqslant 2$. Comme $c \equiv 2 \pmod 4$, cela signifie que $c = 2$, donc que $5^b = 7^c - a! = 49 - 24 = 25 = 5^2$.
Les solutions recherchées sont donc les triplets $(a, b, c) = (2, 1, 1)$, $(3, 0, 1)$ et $(4, 2, 2)$.

Commentaire des correcteurs : Globalement bien traité pour ceux qui l'ont rédigé, le principal souci de cet exercice consistait à bien se ramener à $a < 7$, et à travailler modulo la bonne puissance de nombre premier, ici 25, ce qui a été plutôt bien trouvé. Il faut bien faire attention aux cas limites ($b = 0, c = 0$).

Exercices Seniors

Exercice 10. Soit $a, b, c \geqslant 1$ des entiers tels que $a^b \mid b^c$ et $a^c \mid c^b$. Montrer que $a^2 \mid bc$.

Solution de l'exercice 10 Nous allons regarder les valuations p-adiques de chacun des nombres premiers a, b et c. En effet, il suffit de montrer que pour tout nombre premier p, on a $2v_p(a) = v_p(a^2) \leqslant v_p(bc) = v_p(b) + v_p(c)$.
Soit p un nombre premier. L'hypothèse que $a^b \mid b^c$ se traduit en terme de valuation $p-$adique par $bv_p(a) \leqslant cv_p(b)$, ou encore $v_p(a) \leqslant \frac{c}{b} v_p(b)$. De même, on obtient que $v_p(a) \leqslant \frac{b}{c} v_p(c)$.

En multipliant les deux relations, on trouve que $v_p(a)^2 \leqslant v_p(b)v_p(c)$. On a donc, d'après l'inégalité des moyennes :

$$v_p(a) \leqslant \sqrt{v_p(b)v_p(c)} \leqslant \frac{v_p(b) + v_p(c)}{2}$$

ce qui donne bien $2v_p(a) \leqslant v_p(b) + v_p(c)$ comme voulu. Ceci étant vrai pour tout premier p, on a bien $a^2 \mid bc$.

Commentaire des correcteurs : Le problème est globalement bien réussi. Une poignée d'élèves s'est trompée en affirmant que si a divise b^c, alors a divise b. Cette affirmation peut être réfutée en regardant $a = 25, b = 10$ et $c = 2$.

Exercice 11. Trouver tous les entiers $n \geqslant 1$ tels que

$$6^n - 1 \mid 7^n - 1.$$

Solution de l'exercice 11 Soit n un éventuel entier vérifiant $6^n - 1 \mid 7^n - 1$.
On a $5 = 6 - 1 \mid 6^n - 1^n$, donc $5 \mid 7^n - 1$. On calcule donc les puissances de 7 modulo 5 :

n	0	1	2	3	4
$7^n \pmod 5$	1	2	4	3	1

Ainsi, si on note $n = 4q + r$ la division euclidienne de n par 4, on a $7^n \equiv (7^4)^q \times 7^r \equiv 1^q 7^r \equiv 7^r \pmod 5$. Donc pour que $5 \mid 7^n - 1$, il faut que $r = 0$, autrement dit n est multiple de 4.
En regardant alors modulo 7, on obtient $6^n \equiv (-1)^{4q} \equiv 1 \pmod 7$, donc $7 \mid 6^n - 1 \mid 7^n - 1$, ce qui n'est pas possible.
Il n'y a donc aucun n vérifiant $6^n - 1 \mid 7^n - 1$.

Commentaire des correcteurs : L'exercice est très bien résolu et a été traité par de nombreux élèves.

Exercice 12. Déterminer tous les couples d'entiers strictement positifs (m, n) tels que

$$mn - 1 \mid n^3 - 1.$$

Solution de l'exercice 12 Remarquons que les couples $(1, n)$ et $(m, 1)$ sont solutions pour tous les entiers strictement positifs m et n. On suppose dans la suite que $m, n \geqslant 2$.
Notons que les nombres $mn - 1, n^3 - 1$ sont strictement positifs. La condition de divisibilité implique donc que $mn - 1 \leqslant n^3 - 1$, donc $m \leqslant n^2$.
On commence par ramener un peu de symétrie au problème en remarquant que $mn-1$ divise $(mn)^3-1^3$, de sorte que $mn - 1$ divise $(mn)^3 - 1 - m^3(n^3 - 1) = m^3 - 1$.
Maintenant que le problème est complètement symétrique en m et n , on peut supposer sans perte de généralité que $m \geqslant n$. $m \geqslant n$. Puisque $mn - 1$ divise $n^3 - 1$ et $mn - 1$, il divise également $n^3 - 1 - (mn - 1) = n(n^2 - m)$. Comme $mn - 1$ et n sont premiers entre eux, on a par le lemme de Gauss que $mn - 1$ divise $n^2 - m$. Mais alors, si $n^2 - m$ est non nul, puisque $m \geqslant n$ et $m \geqslant 1$,

$$0 < n^2 - m < mn - 1 \leqslant n^2 - m$$

ce qui est impossible. On a donc $n^2 = m$. Réciproquement, le couple (n^2, n) est bien solution (n^2, n).

Ainsi, les couples solutions sont $\{(1, n), (n, 1), (n^2, n), (n, n^2)\}$.

Solution alternative :
De même que précédemment, on se ramène au cas où $n \geqslant 2$.
Soit (m, n) une solution. On a donc un entier a tel que $n^3 - 1 = a(mn - 1)$. En passant modulo n, on obtient $-1 \equiv -a \pmod{n}$, soit $a \equiv 1 \pmod{n}$. Écrivons donc $a = kn + 1$.
En réinjectant, on obtient $n^3 - 1 = (kn + 1)(mn - 1) = kmn^2 + (m - k)n - 1$, ce qui se simplifie en $n^2 = kmn + m - k$.
Repasser modulo n nous donne $m \equiv k \pmod{n}$, donc si $m = np + r$ et $k = nq + r'$ sont les divisions euclidiennes de m et k par n, on a $r = r'$. On réécrit donc l'égalité sous la forme $n^2 = (np + r)(nq + r)n + np + r - (nq + r)$, qu'on peut encore une fois simplifier :

$$n = p - q + n^2pq + nr(p + q) + r^2$$

Si $p \geqslant 1$, alors $n = p - q + n^2pq + nr(p + q) + r^2 \geqslant n^2q - q = q(n^2 - 1)$. Ainsi si $q \geqslant 1$, il faut $n \geqslant n^2 - 1$, impossible car $n \geqslant 2$.
On vient de montrer qu'au moins un nombre parmi p et q doit être nul.
Si $p = 0$ et $q \geqslant 1$, on a $n = q(nr - 1) + r^2$. Comme $r = m \geqslant 1$, $nr - 1 \geqslant 1$ donc $q(nr - 1) \geqslant nr - 1$ donc $n = q(nr - 1) + r^2 \geqslant (nr - 1) + 1 = nr \geqslant n$. Toutes ces inégalités sont donc des égalités, ce qui impose $q = r = 1$. On obtient donc $m = 1$.
Si $q = 0$ et $p \geqslant 1$, on a $n = p(nr + 1) + r^2$. Ainsi, si $r \geqslant 1$, on a $n \geqslant n + 2$, donc $r = 0$, puis $n = r$ et finalement $m = n^2$.
Si $p = q = 0$, on a $n = r^2$ et $m = r$.

Ainsi les solutions sont les couples $(1, n)$ et (n^2, n) pour tout $n \geqslant 1$, ainsi que les couples (r, r^2) avec $r \geqslant 1$. On vérifie réciproquement que tous ces couples sont solutions, et que $n = 1$ donne bien les mêmes solutions (puisqu'a priori ce ne sont que les solutions avec $n \geqslant 2$).

Commentaire des correcteurs : L'exercice est globalement bien réussi. Pas mal d'élèves oublient de traiter les cas particuliers de leur raisonnement, alors que dans un tel problème c'est justement les cas particuliers/dégénérés qui donnent les solutions.

Exercice 13. Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction telle que pour tout entier $n \geqslant 1$, $f(f(n))$ soit égal au nombre de diviseurs positifs de n. Montrer que si p est un nombre premier, alors $f(p)$ est aussi un nombre premier.

Solution de l'exercice 13
Dans la suite, on note $d(n)$ le nombre de diviseurs positifs de n. Si p est premier, on a $f(f(p)) = 2$ par définition. En appliquant f des deux côtés de l'égalité, on voit que $f(2) = d(f(p))$. On veut donc montrer que $f(2) = 2$, ce qui prouvera que $f(p)$ a exactement deux diviseurs et est donc premier. Or, on a aussi $f(2) = d(f(2))$. Or, pour qu'un entier $n \geqslant 2$ soit égal à son nombre de diviseurs, tous les nombres inférieurs à n doivent diviser n, y compris $n - 1$ qui est toujours premier avec n, donc $n - 1 = 1$ et $n = 2$. On déduit que $f(2) \in \{1, 2\}$. Si $f(2) = 1$, alors $d(f(p)) = 1$ pour tout p premier, donc $f(p) = 1$ pour p premier, puisque 1 est le seul entier à admettre un seul diviseur. Mais alors

$$1 = f(3) = f(d(2^2)) = f(f(f(2^2))) = d(f(2^2))$$

et l'on déduit que $f(4) = 1$. Mais alors

$$f(f(4)) = f(1) = f(f(2)) = d(2) = 2 \neq d(4)$$

ce qui fournit la contradiction désirée. On a donc bien $f(2) = 2$, ce qui conclut.

Commentaire des correcteurs : Une bonne partie des élèves ont résolu le problème, mais beaucoup d'autres sont allés bien trop vite. En effet, à partir de l'égalité $f(f(f(p))) = f(p)$, il est tentant de conclure immédiatemment que $f(p) = 2$. Mais un autre cas possible est le cas où $f(2) = 1$, puisque 1 vérifie aussi que $d(n) = n$. C'est traiter ce cas qui constituait la principale difficulté du problème. Il est donc dommage d'être passé à côté.

Exercice 14. On dit que deux entiers $a, b \in \mathbb{N}^\star$ sont *reliés* s'il existe un nombre premier p tel que $a = pb$ ou $b = pa$.
Trouver tous les entiers $n \geqslant 1$ ayant la propriété suivante : on peut écrire tous les diviseurs positifs de n (1 et n compris) exactement une fois sur un cercle de sorte que tout diviseur soit relié avec chacun de ses deux voisins ?

Solution de l'exercice 14 Traitons d'abord le cas où n n'a qu'un seul facteur premier, donc $n = p^\alpha$. Si $\alpha \leqslant 1$, n'importe quelle configuration marche. En revanche, si $\alpha \geqslant 2$, 1 doit être placé à côté de deux nombres différents, et n'est relié qu'à un seul autre diviseur de p^α (celui-ci étant p), ce n'est donc pas possible.
Remarquons que la parité du nombre de diviseurs premiers comptés avec multiplicité change forcément entre un nombre et un nombre qui lui est relié. Ainsi, si n a un nombre impair de diviseurs, l'existence d'une telle configuration impliquerait que 1 a à la fois un nombre pair et un nombre impair de diviseurs premiers, ce qui n'est pas possible. Les nombres ayant un nombre impair de diviseurs étant les carrés parfaits, ceux-ci ne vérifient pas non plus la propriété de l'énoncé.
Maintenant, essayons de résoudre le cas où on a deux facteurs premiers, mettons $n = p^a q^b$ avec l'un des nombres a ou b étant impair, et l'on suppose sans perte de généralité qu'il s'agit de a.
L'arrangement suivant fonctionne :

$$1, q, q^2, \ldots, q^b, pq^b, pq^{b-1}, \ldots, pq, p^2q, \ldots, p^{a-1}q^b, p^aq^b, p^aq^{b-1}, \ldots, p^aq, p^a, p^{a-1}, \ldots, p, 1$$

On utilise le fait que a est impair pour dire qu'on a effectivement écrit $p^{a-1}q^b$ juste avant p^aq^b.

On procède maintenant par récurrence sur le nombre de diviseurs premiers : supposons avoir montré pour un $k \geqslant 2$ que tous les nombres de la forme $\prod_{i=1}^{k} p_i^{\alpha_i}$ avec au moins l'un des α_i impair vérifient la propriété de l'énoncé, et soit $n = \prod_{i=1}^{k+1} p_i^{\alpha_i}$ avec au moins l'un des α_i impairs, disons α_1. Alors l'hypothèse de récurrence nous dit qu'on peut ordonner les diviseurs de $n' = \prod_{i=1}^{k} p_i^{\alpha_i}$ de la forme $d_1, \ldots d_m$ de sorte que d_i et d_{i+1} soient tous reliés, de même que d_m et d_1. Alors l'arrangement suivant fonctionne pour m (car m est pair) :

$$d_1, p_{k+1}d_1, \ldots, p_{k+1}^{\alpha_{k+1}}d_1, p_{k+1}^{\alpha_{k+1}}d_2, \ldots p_{k+1}d_2, d_2, d_3, \ldots, p_{k+1}^{\alpha_{k+1}}d_m, \ldots p_{k+1}d_m, d_m, d_1$$

Ainsi les nombres qui ne vérifient pas cette propriété sont les carrés (différents de 1) et le puissances (plus grandes que 2) de nombres premiers.

Commentaire des correcteurs : L'exercice, un peu combinatoire, est relativement peu traité mais globalement bien réussi par les élèves qui l'ont abordé. La plupart des élèves qui ont l'intuition de la construction à réaliser pour des nombres composés ont des difficultés à la formuler rigoureusement (par une récurrence).

Exercice 15. Soit $m, n \geqslant 2$ des entiers tels que $\text{PGCD}(m, n) = \text{PGCD}(m, n-1) = 1$. On définit la suite $(n_k)_{k\in\mathbb{N}}$ par $n_0 = m$ et $n_{k+1} = n \cdot n_k + 1$ pour $k \in \mathbb{N}$. Montrer que les entiers $n_1, \ldots, n_{m-1}$ ne peuvent pas tous être des nombres premiers.

Solution de l'exercice 15 Tout d'abord, la suite (n_k) est une suite arithmético-géométrique. On peut donc établir une formule close pour son terme général, à savoir $n_k = n^k m + \frac{n^{k+1}-1}{n-1}$, que l'on peut aussi obtenir par récurrence à partir du calcul des premiers termes. De cette expression on déduit en particulier que $n_k > m$ pour tout $k > 0$. On va désormais montrer que l'un des nombres $n_1, \ldots, n_{m-1}$ est divisible par m, ce qui fera de ce nombre un nombre composé.

En passant modulo m, on déduit $n_k \equiv \frac{n^{k+1}-1}{n-1} \mod m$ par récurrence, où l'on a utilisé que $n-1$ est inversible modulo m car $n-1$ est premier avec m.
Soit ω l'ordre de n mod m (celui-ci existe car m et n premiers entre eux). On a $\omega \leqslant \varphi(m) \leqslant m-1$ d'après le théorème d'Euler. On déduit que $m \mid n^\omega - 1$, ce qui implique que m divise $n_{\omega-1} - 1$ comme voulu. Ainsi, les n_k ne sont pas tous premiers.

Commentaire des correcteurs : L'exercice est très bien résolu. Les élèves ont pratiquement tous pensé à justifier le fait que $m < n_k$, ce qui est nécessaire pour conclure que n_k est composé s'il est divisible par m.

Exercice 16. Soient p un nombre premier impair et $x_1, \dots, x_p$ des entiers relatifs.
On suppose que pour tout $k \geqslant 1$ entier, on a

$$p \mid x_1^k + \cdots + x_p^k.$$

Montrer que les entiers $x_1, \dots, x_p$ sont tous congrus modulo p.

Solution de l'exercice 16 Notons que la relation est également vrai pour $k = 0$ car $\underbrace{1 + \ldots + 1}_{p \text{ fois}} \equiv 0 \mod p$
Soit $Q(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers. On a

$$Q(x_1) + \ldots + Q(x_p) = \sum_{\ell=1}^{p} \sum_{k=0}^{n} a_k x_\ell^k = \sum_{k=0}^{n} a_k \underbrace{\sum_{\ell=1}^{p} x_\ell^k}_{\equiv 0 \mod p} \equiv 0 \mod p$$

On suppose par l'absurde que les x_i ne donnent pas tous le même reste modulo p. Soit $\{y_1, \dots, y_r\}$ l'ensemble des restes modulo p généré par l'ensemble $\{x_1, \dots, x_p\}$, avec $y_1 \equiv x_1$. On note a_1 le nombre d'éléments de l'ensemble $\{x_1, \dots, x_p\}$ qui ont pour reste y_1. Soit $P(X) = (X - y_2) \dots (X - y_r)$. P est nul en chacun des y_i pour $i \neq 0$. Notons que comme $y_1 \neq y_i \mod p$, $P(y_1) \neq 0 \mod p$. La relation établie plus haut nous donne alors $a_1 P(y_1) \equiv 0 \mod p$, ce qui implique que $a_1 = 0 \bmod p$, c'est-à-dire que $a_1 = p$. Cela est en contradiction avec notre supposition de départ, donc les x_i sont tous égaux.

Solution alternative : On présente une solution un peu plus conceptuelle qui s'appuie sur la structure de corps de $\mathbb{Z}/p\mathbb{Z}$ et sur le fait que les sommes de Newton des racines d'un polynôme déterminent ses coefficients.

Soit $P(X) = (X - x_1) \dots (X - x_p)$ le polynôme unitaire à coefficients entiers dont les racines sont les x_ℓ. L'hypothèse de l'énoncé nous indique que les sommes de Newton des x_ℓ sont nulles modulo p.
Or il est possible de relier les coefficients du polynômes P aux sommes de Newton du polynôme P, via les formules suivantes : si a_k est le coefficient devant X^k dans l'écriture de P, alors pour tout $0 \leqslant k \leqslant p$:

$$k a_{p-k} = (-1)^{k-1} \sum_{\ell=1}^{k-1} a_{p-\ell}(x_1^\ell + \ldots + x_p^\ell)$$

On peut retrouver ces formules par récurrence à l'aide des relations de Viète.
On remarque alors que si $k \neq 0, p$, $k a_{p-k} \equiv 0 \mod p$ car chacune des $x_1^\ell + \ldots + x_p^\ell$ est divisible par p. Ainsi, dans $\mathbb{Z}/p\mathbb{Z}[X]$, le polynôme P est de la forme $P(X) = X^p - a = X^p - a^p = (X - a)^p$, où l'on a utilisé que $a^p \equiv a \pmod p$ par le petit théorème de Fermat et que dans la formule $(X - a)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} X^k$, seuls les coefficients $\binom{p}{0}$ et $\binom{p}{p}$ sont non nuls modulo p. Cela implique que les x_i sont tous égaux (à a) modulo p comme voulu.

Commentaire des correcteurs : L'exercice est très bien réussi. Cet exercice demandait de la culture sur les polynômes modulo p, et les élèves ont présenté diverses preuves pour s'en sortir.

Exercice 17. Soit n un entier strictement positif et soient $a, a_1, \ldots, a_n$ des entiers strictement positifs. On suppose que pour tout entier k pour lequel l'entier $ak+1$ est un carré parfait, au moins l'un des entiers $a_1k+1, \ldots, a_nk+1$ est également un carré parfait.
Montrer qu'il existe un indice $1 \leqslant i \leqslant n$ tel que $a = a_i$.

Solution de l'exercice 17 Commençons par deux lemmes sur les résidus quadratiques.
Lemme 1 : Si x est résidu quadratique modulo p avec p premier impair, il l'est aussi modulo p^2 (et même p^m, mais on n'en a pas besoin ici).

Démonstration : En effet, soit a tel que $a^2 \equiv x \pmod{p}$, ce qu'on réécrit sous la forme $a^2 - x = kp$. Mais alors on obtient $(a - 2^{-1}kp)^2 \equiv a^2 - kp \equiv x \pmod{p^2}$, et 2 est inversible modulo p^2 car p est impair. Ainsi, x est bien un résidu quadratique modulo p^2. □

Lemme 2 : Sii t est un entier non nul et p est un nombre premier tel que $p \equiv 1 \pmod{8t}$, alors $\left(\frac{t}{p}\right) = 1$.

Démonstration : En effet, soit q un diviseur premier de t et $\alpha = v_q(t)$. Si $q = 2$, $\left(\frac{2}{p}\right) = 1$ car $p \equiv 1 \pmod{8}$. donc q est résidu quadratique modulo p. Notons maintenant que α est pair, alors q^α est automatiquement un carré modulo p, et si α est impair, q^α est le produit de q (qui est un carré) avec $q^{\alpha-1}$ qui est un carré, donc q^α est un carré modulo p. Si $q \geqslant 3$, comme $p \equiv 1 \pmod{4}$, la loi de réciprocité quadratique nous donne $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$,. De même que précédemment, on déduit que $\left(\frac{q^\alpha}{p}\right) = 1$. La multiplicativité des symboles de Legendre permet de conclure que $\left(\frac{t}{p}\right) = 1$. □

On rappelle également un cas particulier du théorème de la progression arithmétique de Dirichlet : pour tout t entier, il existe une infinité de nombres premiers p tels que $p \equiv 1 \mod 8t$.

Revenons à l'exercice. Supposons par l'absurde que tous les a_i sont différents de a.
Posons $M = \max\{a, a_1, \ldots, a_n\} \geqslant 2$. On construit alors une suite de nombres premiers $p_1, \ldots p_n$ par récurrence comme suit : par le théorème de la progression arithmétique de Dirichlet, il existe au moins un nombre premier $p_1 \equiv 1 \pmod{8a_1(a_1 - a)}$ avec $p_1 > M$. (On utilise ici le fait que $a_1 - a \neq 0$).
Pour $2 \leqslant i \leqslant n$, on prend ensuite p_i tel que $p_i \equiv 1 \pmod{8a_i(a_i - a)}$ avec $p_i > p_{i-1}$ (qui existe pour les mêmes raisons que p_1).
En particulier les p_i sont deux-à-deux distincts, et $p_i \equiv 1 \mod 8a_i$ et $p_i \equiv 1 \mod 8(a_i - a)$, de sorte que d'après le deuxième lemme, pour tout i, $\left(\frac{a_i}{p_i}\right) = \left(\frac{a_i - a}{p_i}\right) = 1$.
Par définition, pour tout i il existe n_i tel que $n_i^2 \equiv a_i - a \pmod{p_i}$, et quitte à remplacer n_i par $n_i + p_i$, on peut supposer $p_i^2 \nmid n_i^2 - (a_i - a)$ ($p_i \neq 2$). Ainsi, on peut écrire $n_i^2 \equiv ac_ip_i + (a_i - a) \pmod{p_i^2}$ avec $p_i \nmid c_i$ puisque a et p_i sont premiers entre eux ($a < p_i$).
Ensuite, comme a_i est inversible modulo p_i pour tout i, le théorème des restes chinois indique que l'on peut trouver un entier k vérifiant que pour tout i, $k \equiv (c_ip_i - 1)a_i^{-1} \mod p_i^2$, ou encore $a_ik + 1 \equiv c_ip_i \pmod{p_i^2}$.
Remarquons que, par construction,

$$ak + 1 \equiv a\frac{c_ip_i - 1}{a_i} + 1 \equiv \frac{ac_ip_i - a + a_i}{a_i} \equiv \frac{n_i^2}{a_i} \equiv a_i\left(\frac{n_i}{a_i}\right)^2 \pmod{p_i^2}$$

Or $\left(\frac{a_i}{p_i}\right) = 1$, donc a_i est également un résidu quadratique modulo p_i^2 par le premier lemme, donc on a un entier, mettons N_i, tel que $ak + 1 \equiv N_i^2 \pmod{p_i^2}$.

Alors le théorème des restes chinois nous donne un entier x tel que $x \equiv N_i \pmod{p_i^2}$ pour tout i et $x \equiv 1 \pmod{a}$ (car a est premier avec les p_i). Mais alors $x^2 \equiv N_i^2 \equiv ak+1 \pmod{p_i^2}$ pour tout i, et $x^2 \equiv 1^2 \equiv ak+1 \pmod{a}$, donc $x^2 \equiv ak+1 \pmod{aP^2}$, où on a posé $P = \prod_{i=1}^{n} p_i$.

On réécrit maintenant la congruence sous la forme $x^2 = ak+1+maP^2 = a(P^2m+k)+1$. On utilise enfin l'hypothèse de l'énoncé : il existe un indice j tel que $a_j(P^2m+k)+1$ soit un carré parfait. Mais alors $a_j(P^2m+k)+1 \equiv a_jk+1 \equiv c_jp_j \pmod{p_j^2}$, et comme $p_j \nmid c_j$, $v_{p_j}(a_j(P^2m+k)+1) = 1$, ce qui est en contradiction avec le fait que c'est un carré parfait. Notre affirmation de départ était donc fausse, et l'un des $a_i - a$ est non nul.

Commentaire des correcteurs : L'exercice est globalement bien réussi par les quelques élèves qui l'ont traité, et qui présentent des solutions très différentes de celle du corrigé.

Exercice 18. Déterminer tous les polynômes $P \in \mathbb{Z}[X]$ tels que :
(i) $P(n) \geqslant 1$ pour tout $n \geqslant 1$
(ii) $P(mn)$ et $P(m)P(n)$ ont le même nombre de diviseurs premiers pour tous $m, n \geqslant 1$.

Solution de l'exercice 18 Dans la suite, pour tout entier $n \in \mathbb{N}^*$, on note $\mathcal{D}(n)$ l'ensemble des diviseurs premiers de n, et $\delta(n) = |\mathcal{D}(n)|$. Soit $P \in \mathbb{Z}[X]$ un polynôme vérifiant les deux conditions.
On commence par montrer le résultat suivant :
Lemme : Soit $n \geqslant 1$. Pour tout $k \in \mathbb{N}^*$, $\mathcal{D}(P(n^k)) = \mathcal{D}(P(n))$.

Démonstration : On montre d'abord le résultat pour des petites valeurs de k.
Tout d'abord, par hypothèse, $\delta(P(n^2)) = \delta(P(n)^2) = \delta(P(n))$. De même, $\delta(P(n^4)) = \delta(P(n^2)) = \delta(P(n))$. Mais $\delta(P(n^4)) = \delta(P(n^3)P(n))$. $P(n^4)$ ayant le même nombre de diviseurs premiers que $P(n)$, cette dernière égalité assure que $\mathcal{D}(P(n^3)) \subset \mathcal{D}(P(n))$. Par ailleurs $\delta(P(n^3)) = \delta(P(n^2)P(n)) \geqslant \delta(P(n))$. Par conséquent, l'inclusion précédente est saturée par cardinalité, et $\mathcal{D}(P(n^3)) = \mathcal{D}(P(n))$. Alors $\delta(P(n)) = \delta(P(n^3)) = \delta(P(n^2)P(n))$, donc nécessairement $\mathcal{D}(P(n^2)) \subset \mathcal{D}(P(n))$. Par égalité des cardinaux, $\mathcal{D}(P(n)) = \mathcal{D}(P(n^2)) = \mathcal{D}(P(n^3))$.

Soit maintenant $k \geqslant 3$. On montre l'égalité $\mathcal{D}(P(n^k)) = \mathcal{D}(P(n))$ par récurrence. Supposons que $\mathcal{D}(P(n)) = \mathcal{D}(P(n^2)) = \ldots = \mathcal{D}(P(n^k))$. Alors $\delta(P(n^{k+1})) = \delta(P(n^k)P(n))$, où par hypothèse de récurrence, $P(n^k)$ et $P(n)$ ont exactement les mêmes diviseurs premiers, donc $\delta(P(n^k)P(n)) = \delta(P(n))$, et $\delta(P(n^{k+1})) = \delta(P(n))$. Alors d'une part, $\delta(P(n^{k+2})) = \delta(P(n^k)P(n^2)) = \delta(P(n^2))$ puisque $\mathcal{D}(P(n^k)) = \mathcal{D}(P(n))$ (vu que $k \geqslant 3$) d'où $\delta(P(n^{k+2})) = \delta(P(n))$. Mais d'autre part, avec l'égalité $\delta(P(n^{k+2})) = \delta(P(n^{k+1})P(n))$, on voit que nécessairement, $\mathcal{D}(P(n^{k+1})) \subset \mathcal{D}(P(n))$. Par égalité des cardinaux, on a bien $\mathcal{D}(P(n^{k+1})) = \mathcal{D}(P(n))$, ce qui achève l'hérédité. □

On utilise désormais l'égalité $\mathcal{D}(P(n^k)) = \mathcal{D}(P(n))$ pour conclure l'exercice. On écrit $P = X^d Q$, où $d \in \mathbb{N}$ et $Q \in \mathbb{Z}[X]$ vérifie $Q(0) \neq 0$. Clairement $Q(n) \geqslant 1$ si $n \geqslant 1$. Fixons p premier ne divisant pas $Q(0)$. Pour $k \geqslant 1$, $p \nmid Q(p^k)$ donc $\mathcal{D}(Q(p^k)) = \mathcal{D}(Q(p))$ d'après le point précédent. En effet, si $d = 0$ cela correspond à l'égalité démontrée plus haut, et si $d \geqslant 1$, $\{p\} \cup \mathcal{D}(Q(p^k)) = \mathcal{D}(P(p^k)) = \mathcal{D}(P(p)) = \{p\} \cup \mathcal{D}(Q(p))$ où $p \nmid Q(p^k)$ et $p \nmid Q(p)$.

Supposons par l'absurde que Q est non constant. Q tend donc vers $+\infty$ à l'infini. Alors $\delta(Q(p)) \geqslant 1$ car dans le cas contraire $Q(p^k)$ serait égal à 1 pour tout $k \geqslant 1$, donc $Q(X) - 1$ admettrait une infinité de racines et serait donc constant. Notons $\mathcal{D}(Q(p)) = \{q_1, \ldots, q_s\}$ où $s \geqslant 1$ et $q_1 < \ldots < q_s$ des nombres premiers. Soit $\alpha = \max_{r \text{ premier}} \nu_r(Q(1)) \geqslant 0$. Il existe $k_0 \geqslant 1$ tel que pour tout $k \geqslant k_0$, il existe $i(k) \in [\![1, s]\!]$ avec $\nu_{q_{i(k)}}(Q(p^k)) \geqslant \alpha + 1$ En effet, comme Q tend vers $+\infty$ en ∞, pour k assez grand, $Q(p^k)$ est strictement supérieur à $(q_1 \ldots q_s)^\alpha)$. Soit $\beta = \varphi((q_1 \ldots q_s)^{\alpha+1}) \geqslant 1$, et $N \geqslant 1$ tel que $N\beta \geqslant k_0$. Alors $q_{i(N\beta)}^{\alpha+1} \mid Q(p^{N\beta})$, mais $p^{N\beta} \equiv 1 \pmod{(q_1 \ldots q_s)^{\alpha+1}}$ puisque $p \notin \{q_1, \ldots, q_s\}$. En particulier, $Q(p^{N\beta}) \equiv Q(1) \pmod{q_{i(N\beta)}^{\alpha+1}}$, et donc $q_{i(N\beta)}^{\alpha+1} \mid Q(1)$. Cela est en contradiction avec la maximalité de α. Ainsi, Q est constant égal à $a \in \mathbb{N}^*$, et $P = aX^d$ avec $d \in \mathbb{N}$.

On vérifie réciproquement que les polynômes de la forme aX^d avec $d \in \mathbb{N}$ et $a \in \mathbb{N}^*$ sont solutions.

Commentaire des correcteurs : Seuls cinq élèves ont rendu une tentative sur cet exercice. Il était très agréable de lire les différentes (excellentes) idées des élèves, qu'elles aient mené à une solution complète ou pas. Les élèves ont pratiquement tous invoqué un résultat (attribué à Schür) sur le fait que l'ensemble des nombres premiers divisant l'un des $P(n)$ est infini si P est non constant à coefficients entiers. Ce résultat, assez puissant et dont la preuve constituerait un exercice en soi, était d'une grande aide ici.