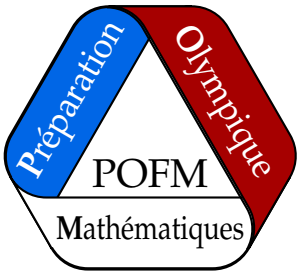

ENVOI 3 : ARITHMÉTIQUE
CORRIGÉ

Exercices Juniors

Exercice 1. Trouver tous les entiers p tels que p, $p+2$ et $p+4$ soient tous les 3 premiers ?

Un nombre premier est un entier $\geqslant 2$ qui n'est divisible que par 1 et lui-même.

Solution de l'exercice 1 Tout d'abord, on peut s'attendre à ce qu'il n'y en ait que très peu. On souhaite obtenir des informations sur ces nombres premiers.
Notons qu'un nombre premier divisible par 3 est a fortiori égal à 3. On considère 3 cas en fonction du reste de la division de p par 3 (modulo 3) :

- $p = 3k$: p est divisible par 3 donc $p = 3$. $\{3, 5, 7\}$ est bien un triplet de nombres premiers.
- $p = 3k+1$: $p+2$ est divisible par 3 et premier donc $p = 1$ (impossible).
- $p = 3k+2$: $p+4$ est divisible par 3 et premier donc $p = -1$ (impossible).

D'où $p = 3$.
Commentaire des correcteurs L'exercice est globalement très bien traité, à part quelques tentatives modulo 10, l'argument modulo 3 a bien été compris. Attention à ne pas oublier le cas $p = 2$.

Exercice 2. Déterminer tous les couples d'entiers (n, p) strictement positifs où p est un nombre premier et tels que $n + p$ soit une puissance de n.

Une puissance de n est de la forme n^k pour k entier naturel.

Solution de l'exercice 2 Soit (p, n) un éventuel couple solution. On dispose d'un entier naturel k tel que

$$n + p = n^k$$

Tout d'abord, si $k = 0$, alors $n+p = 1$. Or p étant premier, $p > 1$ et $n \geqslant 0$ donc $n+p = 1 < p \leqslant p+n$ ce qui est absurde. On a donc $k \geqslant 1$.
On peut alors réécrire l'équation comme ceci :

$$p = n(n^{k-1} - 1)$$

On obtient que n divise p. Comme p est premier, il faut donc que $n = 1$ ou $n = p$.
Si $n = 1$, alors $1 + p = 1$ ce qui est absurde puisque $p \neq 0$.
On a donc $n = p$. Alors $2p = p^k$ donc 2 divise p. Ainsi, $p = 2$ et l'équation devient $2 + 2 = 2^k$ donc $k = 2$. Réciproquement, le couple $(2, 2)$ vérifie bien que $2 + 2 = 2^2$ et donc que $2 + 2$ est une puissance de 2.

Le seul couple solution est donc $(2, 2)$.
Commentaire des correcteurs L'exercice est bien réussi. Plusieurs approches pouvaient fonctionner. Il était cependant assez facile d'oublier des cas particuliers.

Exercice 3. On pose 23 allumettes sur une table et 2 joueurs jouent à un jeu : chacun, à son tour, retire entre 1 et 4 allumettes (inclus). Celui qui prend la dernière gagne. Existe-t-il une stratégie gagnante pour l'un des deux ?

Une stratégie gagnante est une manière de jouer qui permet à l'un des deux de gagner peu importe comment son adversaire joue.

Solution de l'exercice 3 Le 1^{er} joueur possède une stratégie gagnante. La voici :

1. J1 prend 3 allumettes : il en reste un multiple de 5
2. J2 en retire $\mathtt{r} \in \{1, 2, 3, 4\}$
3. J1 en enlève $5 - \mathtt{r}$: il en reste un multiple de 5

Et ainsi de suite. Donc à chaque fois que J2 joue, il y a un nombre d'allumettes divisible par 5. A chaque fois que J1 joue, en revanche, il y en a un nombre non-divisible par 5 et donc en particulier non nul ! Ce qui assure à J1 de gagner.
Commentaire des correcteurs L'exercice est très bien réussi, il faut cependant penser à bien détailler la rédaction parfois un peu trop succincte.

Exercice 4. Déterminer tous les triplets d'entiers (a, b, n) strictement positifs vérifiant :

$$a! + b! = 2^n$$

Solution de l'exercice 4 Les factorielles ayant beaucoup de facteurs impairs en commun, on se dit directement qu'obtenir une puissance de 2 va être très contraignant.
Supposons que $a, b \geqslant 3$, 3 divise donc la somme des factorielles et donc 2^n : c'est absurde.
C'est à dire que l'un des deux est dans $\{1, 2\}$. Par symétrie, on ne traite que deux cas :

1. $a = 1$: encore deux petits cas de figure :
   — $b = 1$: $n = 1$
   — $b \geqslant 2$: les deux membres n'ont pas la même parité, c'est impossible
2. $a = 2$: $b \geqslant 2$ (comme vu au-dessus), quelques cas :
   — $b = 2,\ 3$: $n = 2,\ 3$
   — $b \geqslant 4$: il y a un problème modulo 4, impossible

D'où : les seules solutions sont dans $\{(1, 1, 1),\ (2, 2, 2),\ (2, 3, 3),\ (3, 2, 3)\}$.
Commentaire des correcteurs
L'exercice plutôt bien réussi. Il ne faut pas oublier de bien préciser que l'on peut supposer $a \geqslant b$ avant d'utiliser cette inégalité dans son raisonnement.

Exercice 5. Trouver tous les couples de nombres premiers (p, q) tels que :

$$p^2(p^3 - 1) = q(q + 1)$$

Solution de l'exercice 5 Si $p = q$, alors $p^4 - p = p + 1$. Or $p^4 = p \cdot p^3 \geqslant 8p > 2p + 1$ pour tout nombre premier p car $p \geqslant 2$. On a donc $p \neq q$ et donc p et q sont premiers entre eux.
p^2 est premier avec q donc d'après le lemme de Gauss, $p^2 \mid q + 1$. On dispose donc de $k \in \mathbb{N}^*$ tel que $q + 1 = kp^2$.
Comme q est premier avec p^2, $q \mid p^3 - 1 = (p - 1)(p^2 + p + 1)$. Donc $q \mid p - 1$ ou $q \mid p^2 + p + 1$.
Si $q \mid p - 1$, alors

$$p < kp^2 - 1 = q \leqslant p - 1$$

ce qui est absurde.
On a donc $q \mid p^2 + p + 1$ donc $kp^2 - 1 = q \leqslant p^2 + p + 1$ soit $(k - 1)p^2 \leqslant p + 2$. Si $k = 1$, alors $q = p^2 - 1 = (p - 1)(p + 1)$ qui n'est premier que si $p = 2$.
On a alors $q = 3$ mais $2^2(2^3 - 1) = 28 \neq 12 = 3(3 + 1)$.
On en déduit que $k \geqslant 2$ et $p > 2$, donc $p + 2 < p^2 \leqslant (k - 1)p^2 \leqslant p + 2$ ce qui est également absurde.

Finalement il n'y a pas de solution.
Commentaire des correcteurs
Peu d'élèves ont entièrement réussi le problème. On a pu voir beaucoup d'erreurs de divisibilité et bien souvent, le cas $p = q$ n'a pas été considéré.

Exercice 6. Trouver tous les couples d'entiers strictement positifs (m, n) pour lesquels :

$$1 + 2^n + 3^n + 4^n = 10^m$$

Solution de l'exercice 6 Cette équation est valable pour tous n, m, elle est donc valable en la passant modulo un entier k, c'est-à-dire en ne considérant que les restes de la division par rapport à k.
On commence par la regarder modulo 3 :

$$1 + (-1)^n + 0 + 1^n \equiv 1^m \pmod 3 \text{ donc } (-1)^n \equiv -1$$

Donc n est impair : soit $k \in \mathbb{N}$ tel que $n = 2k + 1$.

On suppose à présent que $n, m \geqslant 3$ et on regarde modulo 8 :

$$1 + 0 + 3 \cdot 3^{2k} + 0 \equiv 0 \pmod 8 \text{ ie } 1 + 3 \cdot 1 \equiv 0$$

Ce qui est absurde.
On en déduit que l'un des deux est dans $\{1, 2\}$.

Il suffit alors de traiter les cas $n = 1$, $n = 2$, $m = 1$ et $m = 2$.
Pour $n = 1$ on trouve $1 + 2 + 3 + 4 = 10$, $(1, 1)$ est solution. Pour $n = 2$, $1 + 4 + 9 + 16 = 30$ n'est pas une puissance de 10 (car 30 est divisible par 3). Comme l'application qui à n associe $1 + 2^n + 3^n + 4^n$ est strictement croissante à m fixé on a au plus une solution. Comme $(1, 1)$ et $(3, 2)$ sont solutions (car $1 + 2^3 + 3^3 + 4^3 = 1 + +27 + 64 = 100 = 10^2$), ce sont donc les seules solutions avec $m = 1$ ou 2. L'ensemble des solutions est donc $\{(1, 1),\ (2, 3)\}$.
Commentaire des correcteurs
Même si beaucoup d'élèves ont quasiment réussi l'exercice, peu se retrouvent avec la note maximale : en effet, plusieurs n'ont pas justifié pourquoi, pour $m = 2$, seul $n = 3$ était solution (ce qui pouvait se faire par encadrement ou en utilisant un argument de croissance). La rédaction n'est pas une course, il vaut mieux écrire une page et avoir tous les arguments bien expliqués que de compacter tout en 9 lignes et se retrouver avec une copie peu claire pour le correcteur et souvent incomplète (de plus, souvent les copies compactes sont bien plus compliquées à lire que des copies un peu longues mais bien détaillées). Il ne faut pas oublier de vérifier que les couples obtenus vérifient bien l'équation.

Exercice 7. Soit $p \geqslant 3$ un nombre premier. Pour $k \in \mathbb{N}$ vérifiant $1 \leqslant k \leqslant p-1$, le nombre de diviseurs de $kp+1$ qui sont compris strictement entre k et p est noté a_k.
Que vaut $a_1 + a_2 + \ldots + a_{p-1}$?

Solution de l'exercice 7 La réponse est $p-2$.
Nous allons montrer que chacun de $\{2, \ldots, p-1\}$ contribue exactement une fois au comptage représenté par $a_1 + a_2 + \ldots + a_{p-1}$.
Soit $2 \leqslant m \leqslant p-1$ un entier, on se propose de montrer deux choses :

1. m est compté au plus une fois
2. m est bien compté

m est compté au plus une fois :
Par l'absurde, on suppose qu'il existe $1 \leqslant i < j \leqslant p-1$ deux entiers vérifiant :
— $m \mid ip+1$ et $m > i$
— $m \mid jp+1$ et $m > j$
On a donc $m \mid p(j-i)$ or $\mathrm{pgcd}(m,p) = 1$ donc $m \mid j-i$. Cependant, c'est impossible car $0 < j-i < j < m$: m est compté au plus une fois

m est bien compté :
On considère les $m-1$ entiers $\{p+1, 2p+1, \ldots, (m-1)p+1\}$.
Exactement comme précédemment, on voit qu'ils sont 2 à 2 distincts modulo m. De plus, aucun d'entre eux n'est $\equiv 1 \pmod{m}$ car si on retire les $+1$ aucun entier n'est divisible par m.
D'où m est compté une et une fois et cela conclut.
Commentaire des correcteurs
Le chemin à suivre a été globalement compris, mais la formalisation de ce raisonnement n'était pas toujours rigoureuse.

Exercice 8. Déterminer tous les entiers $n \geqslant 1$ tels qu'il existe une permutation $(a_1, a_2, \ldots, a_n)$ de $(1, 2, \ldots, n)$ vérifiant la condition suivante :

$$k \mid a_1 + a_2 + \ldots + a_k$$

pour tout $k \in \{1, 2, \ldots, n\}$.

Solution de l'exercice 8 On commence par regarder ce qu'il se passe pour $n = 1,\ 2,\ 3$: $n = 1,\ 3$ sont solutions mais $n = 2$ ne l'est pas. Soit $n > 3$ vérifiant la propriété de l'énoncé.

On a $n \mid a_1 + a_2 + \ldots + a_n = 1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$ et donc $\dfrac{n+1}{2} \in \mathbb{Z}$: n est impair.

Ensuite $n - 1 \mid a_1 + a_2 + \ldots + a_{n-1} = \dfrac{n(n+1)}{2} - a_n$.

Et $n - 1 \mid \dfrac{(n-1)(n+1)}{2}$ donc $n - 1 \mid \dfrac{n+1}{2} - a_n$.

Cependant, il y a un "problème de taille" : $-(n-1) < \dfrac{n+1}{2} - a_n < n - 1$

ce qui n'est pas absurde, mais implique que $a_n = \dfrac{n+1}{2}$.

On poursuit (pas de souci, $n > 3$) :

$n - 2 \mid \dfrac{n(n+1)}{2} - \dfrac{n+1}{2} - a_{n-1} = \dfrac{(n-1)(n+1)}{2} - a_{n-1}$.

Et $n - 2 \mid \dfrac{(n-2)(n+1)}{2}$ donc $n - 2 \mid \dfrac{n+1}{2} - a_{n-1}$.

Comme précédemment, $-(n-2) < \dfrac{n+1}{2} - a_{n-1} < n-2$ et donc $a_n = a_{n-1} = \dfrac{n+1}{2}$: c'est absurde.

Les seules solutions sont donc bien 1 et 3.

Commentaire des correcteurs

Peu d'élèves ont entièrement réussi le problème. Les solutions sont assez diverses dans l'ensemble même si elles tournent autour de la même idée.

Exercice 9. Existe-t-il des entiers a et b pour lesquels : a^5b+3 et ab^5+3 sont tous deux des cubes parfaits ?

Un cube parfait est un entier n pour lequel il existe $m \in \mathbb{Z}$ tel que : $n = m^3$.

Solution de l'exercice 9 Nous allons montrer qu'il n'y a pas d'entiers a et b satisfaisant les conditions du problème.
Soient a et b des entiers tels que a^5b+3 et ab^5+3 sont des cubes parfaits. Soit m et n des entiers tels que $a^5b+3 = m^3$ et $ab^5+3 = n^3$. Supposons que $3 \mid n$. Alors $27 \mid n$. De plus $3 \mid ab^5$ donc $3 \mid a$ ou $3 \mid b^5$. Si $3 \mid a$, alors $3^5 \mid a^5$ donc $3 \mid a^5b+3 = m^3$. Mais alors $27 \mid m^3$ et $27 \mid a^5$ donc $27 \mid m^3 - a^5b = 3$ ce qui est absurde. Si $3 \mid b$, alors $3^5 \mid b^5$ et en particulier $27 \mid n^3 - ab^5 = 3$ ce qui est aussi absurde. On déduit que 3 ne divise pas n et de même 3 ne divise pas m. Si $3 \mid a$, alors $3 \mid m, n$ ce qui est exclut. On déduit donc que 3 ne divise pas non plus a et b. Notons que

$$m^3 - n^3 = a^5b - ab^5 = ab(a-b)(a+b)(a^2+b^2)$$

Comme a et b ne sont pas divisibles par 3, $a^2 \equiv b^2 \equiv 1 \mod 3$ donc $3 \mid a^2 - b^2 = (a-b)(a+b)$ et donc $3 \mid m^3 - n^3$. D'après le théorème de Fermat, $m^3 \equiv m \mod 3$ et $n^3 \equiv n \mod 3$. On déduit que $m \equiv m^3 \equiv n^3 \equiv n \mod 3$. Il vient que

$$m^2 + mn + n^2 \equiv 3m^2 = 0 \mod 3$$

On déduit que 3 divise $m-n$ et 3 divise m^2+mn+n^2 donc $9 \mid (m-n)(m^2+mn+n^2) = m^3 - n^3$. Il vient que $9 \mid ab(a-b)(a+b)(a^2+b^2)$. Mais 3 ne divise pas a, b et $a^2+b^2 \equiv 2 \mod 3$ donc 3 ne divise pas non plus a^2+b^2 et donc 9 non plus. On déduit que $9 \mid a^2 - b^2$, soit $a^2 \equiv b^2 \mod 9$. Ainsi

$$m^3 = a^5b + 3 \equiv a^3 \cdot a^2 \cdot b + 3 \equiv a^3b^2 \cdot b + 3 \equiv (ab)^3 + 3 \mod 9$$

Or les cubes modulo 9 prennent uniquement les valeurs $-1, 0$ et 1. On ne peut donc avoir $m^3 - (ab)^3 \equiv 3 \mod 9$. La condition de l'énoncé ne peut donc pas être satisfaite, comme annoncé.
Commentaire des correcteurs
Plusieurs élèves se sont contentés de tester tous les cas, d'autres ont fourni de bons raisonnements par l'absurde. Globalement le problème est bien réussi par ceux qui l'ont abordé.

Exercices Seniors

Exercice 10. Trouver tous les triplets (p, q, r) de nombres premiers tels que les 3 différences

$$|p - q|,\ |q - r|,\ |r - p|$$

soient également des nombres premiers.

Solution de l'exercice 10 Notons que les trois nombres doivent être deux à deux distincts puisque 0 n'est pas un nombre premier. On peut donc supposer, quitte à échanger l'ordre des variables, que $p > q > r$. Un nombre premier est impair ou égal à 2.
On suppose que p, q et r sont tous impairs. Alors $p - q$, $q - r$ et $r - p$ sont pairs. Comme leur valeur absolue est première, ces nombres valent tous 2. Ainsi les entiers $p, p + 2$ et $p + 4$ sont premiers. Si p est divisible par 3, alors $p = 3$ et $q = 5$ et $r = 7$.
Cependant, le triplet $(3, 5, 7)$ n'est pas solution du problème : $7 - 3 = 4$ n'est pas premier.
Si p n'est pas divisible par 3, alors p est de la forme $3k + 1$ ou $3k + 2$. Le premier cas implique que $p + 2$ soit divisible par 3 donc $p + 2 = 3$ mais $p = 1$ n'est pas un nombre premier. Le deuxième cas implique que $p + 4$ soit divisible par 3, mais $p + 4 = 3$ ne donne pas de solution strictement positive.
On suppose que $r = 2$. Alors p et q sont impaires et $p - q$ est pair et premier donc égal à 2. Il vient que $q + 2, q$ et $q - 2$ sont tous les trois des nombres premiers. D'après le cas précédent, cela implique que $q - 2 = 3$ donc $p = 7$. Réciproquement, le triplet $(p, q, r) = (2, 5, 7)$ et ses permutations sont donc bien solutions au problème.

Les seuls triplets solutions sont donc $(2, 5, 7)$ ainsi que ses permutations.
Commentaire des correcteurs
Beaucoup d'élèves ont les idées majeures, mais perdent bêtement des points pour la rédaction. Il faut toujours vérifier que les solutions obtenues satisfont bien l'énoncé. Certains ont affirmé sans aucune justification que si p, $p + 2$ et $p + 4$ sont premiers alors $p = 3$. De même certains ont dit qu'on ne peut pas avoir $|p - q| = |q - r| = |r - p| = 2$ sans le justifier, ce qui était assez clair (on peut supposer $p > q > r$ par exemple). Il vaut mieux un peu plus détailler les points importants pour ne pas perdre de points.

Exercice 11. Trouver tous les nombres entiers $z \in \mathbb{Z}$ tels que

$$2^z + 2 = r^2$$

où $r \in \mathbb{Q}$ est un nombre rationnel.
Un nombre rationnel est un nombre qui s'écrit sous la forme $\frac{a}{b}$ avec a, b des entiers et $b \neq 0$.

Solution de l'exercice 11 Notons que si (z, r) est un couple solution, $(z, -r)$ est également un couple solution. On peut donc supposer pour la suite que $r \geqslant 0$. Etant donné que $2^z + z > 0$, on a même $r > 0$. On pose $r = \frac{a}{b}$, avec a et b des entiers strictement positifs et premiers entre eux.
Si $z \geqslant 0$, alors $2^z + 2$ est entier donc r est entier et $b = 1$. On doit désormais résoudre l'équation $2^z + 2 = a^2$ dans les entiers positifs. Si $z \geqslant 2$, alors l'équation vue modulo 4 donne $a^2 \equiv 2 \mod 4$ ce qui n'a pas de solution puisqu'un carré est toujours congru à 0 ou à 1 modulo 4. On déduit que $z = 0$ ou $z = 1$. Dans le premier cas, on obtient $3 = a^2$ qui n'admet pas de solution entière. Dans le deuxième cas on trouve $4 = a^2$ soit $a = 2$. Réciproquement, les couples $(1, -2)$ et $(1, 2)$ satisfont bien l'équation.
Si $z < 0$, alors on pose $z' = -z$, avec $z' > 0$. L'équation dévient $\frac{1}{2^{z'}} + 2 = \frac{a^2}{b^2}$. En supprimant les dénominateurs on obtient

$$b^2(1 + 2^{z'+1}) = a^2 \cdot 2^{z'}$$

Puisque $1 + 2^{z'+1}$ est premier avec $2^{z'}$, par le lemme de Gauss on obtient que $2^{z'+1} + 1$ divise a^2. Comme a et b sont premiers entre eux, par le lemme de Gauss on obtient aussi que a^2 divise $1 + 2^{z'+1}$. On déduit que $a^2 = 2^{z'+1} + 1$, que l'on réécrit $2^{z'+1} = (a - 1)(a + 1)$. On déduit que $a + 1$ et $a - 1$ sont tous les deux des puissances de 2 dont la différence vaut 2. On déduit donc que $a + 1 = 4$ et $a - 1 = 2$ soit $a = 3$ et $z' = 2$. Ainsi $b = 2$. Réciproquement, les couples $(-2, -\frac{3}{2})$ et $(-2, \frac{3}{2})$ sont bien solutions de l'équation. Les solutions sont donc $\{(-2, -\frac{3}{2}), (-2, \frac{3}{2}), (1, -2), (1, 2)\}$.
Commentaire des correcteurs
Un tiers des élèves a écrit que $x^2 = 4$ implique que $x = 2$ et oublie donc la solution $x = -2$. Quelques élèves n'ont pas vu que l'on se plaçait dans $\mathbb{Z}$ et $\mathbb{Q}$ et ont juste regardé l'équation sur les entiers positifs. Mis à part cela, l'exercice est assez bien réussi.

Exercice 12. Déterminer tous les triplets d'entiers (a, b, n) strictement positifs vérifiant :

$$a! + b! = 2^n$$

Solution de l'exercice 12 Les factorielles ayant beaucoup de facteurs impairs en commun, on se dit directement qu'obtenir une puissance de 2 va être très contraignant.
Supposons que $a, b \geqslant 3$, 3 divise donc la somme des factorielles et donc 2^n : c'est absurde.
C'est à dire que l'un des deux est dans $\{1, 2\}$. Par symétrie, on ne traite que deux cas :

1. $a = 1$: encore deux petits cas de figure :
   — $b = 1 : n = 1$
   — $b \geqslant 2$: les deux membres n'ont pas la même parité, c'est impossible
2. $a = 2 : b \geqslant 2$ (comme vu au-dessus), quelques cas :
   — $b = 2,\ 3 : n = 2,\ 3$
   — $b \geqslant 4$: il y a un problème modulo 4, impossible

D'où : les seules solutions sont dans $\{(1, 1, 1),\ (2, 2, 2),\ (2, 3, 3),\ (3, 2, 3)\}$.
Commentaire des correcteurs
Il y a eu pas mal d'erreurs de logique. Ce n'est pas parce que l'on ne peut pas avoir $a \geqslant 3$ et $b \geqslant 3$ en même temps qu'on a forcément $a < 3$ et $b < 3$ (on a plutôt $a < 3$ ou $b < 3$). 1 est une puissance de 2 qu'il ne faut pas oublier et 0 n'est pas dans $\mathbb{N}^*$ et 1 est un diviseur impair de 2 qu'il ne faut pas oublier non plus. Ne pas oublier de rappeller les solutions symétriques si on suppose $a \geqslant b$.

Exercice 13. Déterminer tous les triplets d'entiers (x, y, z) vérifiant la propriété suivante :

$$\mathrm{pgcd}(x,\ y,\ z) < \mathrm{pgcd}(x+y,\ y+z,\ z+x)$$

Solution de l'exercice 13 Notons que puisque $\mathrm{pgcd}(x, y, z)$ divise chacun des x, y, z, il divise également $\mathrm{pgcd}(x+y, y+z, z+x)$.
On remarque que si le triplet (x, y, z) est solution, alors les triplets (kx, ky, kz) sont solutions pour tout $k \in \mathbb{N}^*$. On peut donc supposer, quitte à diviser chaque variable par $\mathrm{pgcd}(x, y, z)$, que les entiers x, y, z sont premiers entre eux dans leur ensemble. En particulier ils ne sont pas tous pairs.
Soit $d = \mathrm{pgcd}(x+y, y+z, z+x)$. Alors d divise $(x+y)+(x+z)-(y+z) = 2x$ et de même d divise $2y$ et $2z$. Donc d divise $\mathrm{pgcd}(2x, 2y, 2z) = 2\mathrm{pgcd}(x, y, z) = 2$. On déduit que $d = 1$ ou $d = 2$. Mais comme $d > 1$, $d = 2$ donc les entiers x, y, z sont tous de même parité. Comme ils ne sont pas tous paires, ils sont tous impaires.
Réciproquement, si x, y et z sont tous les trois impaires, étant donné que $\mathrm{pgcd}(x, y, z)$ et 2 sont premiers entre eux et divisent $\mathrm{pgcd}(x+y, y+z, z+x)$, on a bien

$$\mathrm{pgcd}(x, y, z) < 2\mathrm{pgcd}(x, y, z) \leqslant \mathrm{pgcd}(x+y, y+z, z+x)$$

Les triplets solutions sont donc les triplets $\{(kx, ky, kz), k \in \mathbb{N}^*, x, y, z \text{ impaires}\}$.
Commentaire des correcteurs
Les correcteurs étaient très satisfait des différentes approches des élèves. Quelques erreurs sont à noter : ce n'est pas parce que $2n \equiv k \mod a$ que k est pair et ce n'est pas parce que $\mathrm{pgcd}(x, y, z) = \mathrm{pgcd}(x+y, y+z, z+x)$ que $(x, y, z) = (x+y, y+z, z+x)$.

Exercice 14. Existe-t-il des entiers a et b pour lesquels : a^5b+3 et ab^5+3 sont tous deux des cubes parfaits ?

Un cube parfait est un entier n pour lequel il existe $m \in \mathbb{Z}$ tel que : $n = m^3$.

Solution de l'exercice 14 Nous allons montrer qu'il n'y a pas d'entiers a et b satisfaisant les conditions du problème.
Soient a et b des entiers tels que a^5b+3 et ab^5+3 sont des cubes parfaits. Soit m et n des entiers tels que $a^5b+3 = m^3$ et $ab^5+3 = n^3$. Supposons que $3 \mid n$. Alors $27 \mid n$. De plus $3 \mid ab^5$ donc $3 \mid a$ ou $3 \mid b^5$. Si $3 \mid a$, alors $3^5 \mid a^5$ donc $3 \mid a^5b+3 = m^3$. Mais alors $27 \mid m^3$ et $27 \mid a^5$ donc $27 \mid m^3 - a^5b = 3$ ce qui est absurde. Si $3 \mid b$, alors $3^5 \mid b^5$ et en particulier $27 \mid n^3 - ab^5 = 3$ ce qui est aussi absurde. On déduit que 3 ne divise pas n et de même 3 ne divise pas m. Si $3 \mid a$, alors $3 \mid m, n$ ce qui est exclut. On déduit donc que 3 ne divise pas non plus a et b. Notons que

$$m^3 - n^3 = a^5b - ab^5 = ab(a-b)(a+b)(a^2+b^2)$$

Comme a et b ne sont pas divisibles par 3, $a^2 \equiv b^2 \equiv 1 \mod 3$ donc $3 \mid a^2 - b^2 = (a-b)(a+b)$ et donc $3 \mid m^3 - n^3$. D'après le théorème de Fermat, $m^3 \equiv m \mod 3$ et $n^3 \equiv n \mod 3$. On déduit que $m \equiv m^3 \equiv n^3 \equiv n \mod 3$. Il vient que

$$m^2 + mn + n^2 \equiv 3m^2 = 0 \mod 3$$

On déduit que 3 divise $m-n$ et 3 divise m^2+mn+n^2 donc $9 \mid (m-n)(m^2+mn+n^2) = m^3 - n^3$. Il vient que $9 \mid ab(a-b)(a+b)(a^2+b^2)$. Mais 3 ne divise pas a, b et $a^2+b^2 \equiv 2 \mod 3$ donc 3 ne divise pas non plus a^2+b^2 et donc 9 non plus. On déduit que $9 \mid a^2 - b^2$, soit $a^2 \equiv b^2 \mod 9$. Ainsi

$$m^3 = a^5b + 3 \equiv a^3 \cdot a^2 \cdot b + 3 \equiv a^3b^2 \cdot b + 3 \equiv (ab)^3 + 3 \mod 9$$

Or les cubes modulo 9 prennent uniquement les valeurs $-1, 0$ et 1. On ne peut donc avoir $m^3 - (ab)^3 \equiv 3 \mod 9$. La condition de l'énoncé ne peut donc pas être satisfaite, comme annoncé.
Commentaire des correcteurs
Beaucoup d'élèves ont une solution brutale qui consiste à regarder les paires (ab^5, ba^5) modulo 9 d'une façon ou d'une autre, ce n'est pas forcément une mauvaise chose mais il est plus subtil d'utiliser le petit théorème de Fermat en compétition pour ne pas perdre de temps (et parce que souvent les études ne sont pas exhaustives). La plupart des élèves ont une solution légèrement différente du corrigé qui consiste à remarquer que a^5b+3 et b^5a+3 ne peuvent pas être congrus à des cubes en même temps $\mod 9$.

Exercice 15. Soit p un nombre premier impair, $h < p$ un entier, $e \in \{1, 2\}$.
On pose $n = h \cdot p^e + 1$ et on suppose que :

$$\begin{cases} n \mid 2^{n-1} - 1 \\ n \nmid 2^h - 1 \end{cases}$$

Montrer que n est premier.

Solution de l'exercice 15 Soit ω l'ordre de 2 modulo n. Par hypothèse, ω divise $n-1$ mais ω ne divise pas $h = \frac{n-1}{p^e}$, donc p divise ω.
ω divise $\phi(n)$ par le théorème d'Euler donc p divise $\phi(n)$. Evidemment, p ne divise pas n donc il existe q premier qui divise n avec $q = 1 \pmod p$ (d'après la formule donnant ϕ)
On écrit $n = q^a N$ où N est premier avec q. Modulo p on a $1 = 1^a * N$ donc $N = 1 \pmod p$. On va montrer que $n = q$.
Dès lors, si $n \neq q$, soit $a \geqslant 2$ soit $N \geqslant p+1$ et donc $n \geqslant (p+1)^2 > p^2 + 1 > ph + 1$ donc $e = 2$ et le raisonnement montre que soit $a = 1$, soit $N = 1$ et dans tous les cas $a \leqslant 2$ et $N < p^2$.

Traitons deux cas :
• Si $a = 2$, $n \equiv q^2 \equiv (1+pk)^2 \equiv 1 + 2kp \pmod p$ où $q = 1 + kp$. Or $n \equiv 1 \pmod{p^2}$ donc p divise $2k$; p divise k et donc $q \geqslant p^2 + 1$ et $n = q^2 > p^3 + 1 > p^2 h + 1 = n$, contradiction
• Si $a = 1$, $q = 1 + kp$, $N = 1 + lp$ avec $k, l > 0$ (car $q \equiv N \equiv 1 \pmod p$). On a obligatoirement $k, l < p$ car sinon $n = qN \geqslant (1+p^2)(1+p) > p^3 + 1 > p^2 h + 1 = n$. De plus $1 + (k+l)p \equiv n \equiv 1 \pmod{p^2}$ donc $k + l = p$. Un parmi k et l est donc impair, ce qui oblige q ou N pair, donc dans tous les cas n est pair, ce qui contredit $n \mid 2^{n-1} - 1$.

Dans tous les cas $n = q$ est premier.
Commentaire des correcteurs
Les correcteurs ont noté beaucoup d'erreurs d'inattention et de mauvaises utilisations de l'ordre d'un élément modulo n. Certains élèves ont été surpris en train d'essayer d'arnaquer les correcteurs, ce qui est inutile et ne permettra sûrement pas de gagner des points en compétition.

Exercice 16. Soit $m, n \geqslant 2$ des entiers vérifiant la propriété suivante :

$$a^n \equiv 1 \pmod{m} \quad a = 1, ..., n$$

Prouver que m est un nombre premier et que $n = m - 1$.

Solution de l'exercice 16 Commençons par supposer que $m = p$ est un nombre premier. On doit donc montrer $n = p - 1$. Si $n \geqslant p$, on a $p^n \equiv 1 \pmod{p}$, une évidente contradiction. Donc $n < p$.
Considérons $T = X^n - 1$ le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$. Il a pour racines par hypothèse $1, \ldots, n$, qui sont au nombre de n et distinctes, et, puisque $\mathbb{Z}/p\mathbb{Z}$ est intègre, et que T est de degré n, ce sont les seules. Donc $T = (X-1)\cdot\ldots\cdot(X-n)$. En regardant le coefficient en X^{n-1} de T, on voit que $0 \equiv 1+\ldots+n \pmod{p}$ par les formules de Viète. Ainsi, $p \mid \frac{n(n+1)}{2}$, donc (puisque $n < p$) on a nécessairement $n = p - 1$.

Revenons au cas général. Soit p un diviseur premier de m. On a $n = p - 1$ puisque l'hypothèse de l'énoncé reste vraie pour $m = p$. Dès lors, si q est un autre diviseur premier de m, $q - 1 = n = p - 1$ et $q = p$. Il reste à voir que m ne peut pas être une puissance de p autre que p. Il suffit clairement de le voir pour $m = p^2$. Or $(p-1)^{p-1} \equiv (-1)^{p-1} + p \times (-1)^{p-2}\binom{p}{p-1} \pmod{p^2}$ par le binôme de Newton. Puisque $p - 1$ est pair, et que $p^2 \nmid -p(p-1)$, on a bien $(p-1)^{p-1} \not\equiv 1 \pmod{p^2}$. Ceci achève la démonstration.
Commentaire des correcteurs
Il y avait pas mal de bonnes copies mais plein de petites erreurs donc les notes se trouvent majoritairement entre 4 et 7.

Exercice 17. Soit S un ensemble non vide d'entiers strictement positifs vérifiant la propriété suivante : Pour tous entiers $a, b \in S$, l'entier $ab + 1$ appartient aussi à S.
Montrer que l'ensemble des nombres premiers ne divisant aucun des éléments de S est fini.

Solution de l'exercice 17 Soit p un nombre premier et soit $a_1, a_2, \dots a_k$ les restes possibles des éléments de S modulo p. On suppose que 0 n'appartient pas à $R = \{a_1, \dots, a_k\}$, c'est-à-dire que p ne divise aucun élément de S.
On sait que pour tout i, j, $a_i a_j + 1 \in R$. Notons que si j et l sont distincts, alors $a_i a_j + 1$ et $a_i a_l + 1$ sont distincts. En effet

$$a_i a_j + 1 - (a_i a_l + 1 - \equiv a_i(a_j - a_l) \neq 0 \mod p$$

Ainsi pour i fixé, $R = \{a_1, \dots, a_k\} = \{a_i a_1 + 1, \dots, a_i a_k + 1\}$. Il vient que

$$a_1 + \dots + a_k \equiv a_i a_1 + 1 + \dots + a_i a_k + 1 \equiv a_i(a_1 + \dots + a_k) + k \mod p$$

Si $a_1 + \dots + a_k \equiv 0 \mod p$, alors $k \equiv 0 \mod p$ donc $k = p$ et $0 \in R$ ce qui est contraire à l'hypothèse.
On déduit que $a_1 + \dots + a_k$ est inversible modulo p et

$$a_i \equiv \frac{k}{a_1 + \dots + a_k} \mod p$$

Ce terme ne dépend pas de i. Donc les a_i sont égaux et R est un singleton noté $\{a\}$. Ainsi $a^2 + 1 \equiv a \mod p$ donc $p \mid a^2 + 1 - a$ et $p \leqslant n^2 - n + 1$ pour tout n dans S. Si n_0 est le plus petit élément de S, alors en particulier $p \leqslant n_0^2 - n_0 + 1$.
En conclusion, si p ne divise aucun élément de S, p est borné par $n_0^2 - n_0 + 1$. Ainsi l'ensemble des nombres premiers ne divisant aucun élément de S est fini.
Commentaire des correcteurs
L'exercice a été bien résolu par les quelques élèves qui l'ont traité.

Exercice 18. Trouver tous les entiers $n \geqslant 1$ pour lesquels la fonction :

$$x \longmapsto x^x$$

prenne toutes les valeurs possibles modulo n lorsque x parcourt $[\![0, n-1]\!]$.

On dit que c'est une surjection dans $\mathbb{Z}/n\mathbb{Z}$.

Solution de l'exercice 18 Notons déjà que si n vérifie la propriété, alors tout diviseur d de n la vérifie également. Posons f l'application qui à x dans $\mathbb{N}^*$ dans $\mathbb{Z}/n\mathbb{Z}$.
Pour $n = p^2$ avec p premier, notons que p n'est pas dans l'image de f. En effet, si $f(x) \equiv p \pmod{p^2}$, p divise x^x donc p divise x. En particulier, comme $x \geqslant p \geqslant 2$, p^2 divise $x^x = f(x)$ contradiction. En particulier, si n vérifie la propriété, dans sa décomposition en facteurs premiers toutes les valuations p adiques valent au plus 1.
Pour $n = p$ premier, donnons nous $y \in \mathbb{N}$. On cherche x entier positif tel que $x^x \equiv y \pmod{p}$. Pour cela, on utilise le petit théorème de Fermat : si $p-1$ divise $x-1$, $x^x \equiv x^{x-1} \times x \equiv x \pmod{p}$. En particulier, il suffit de prendre x strictement positif tel que $x \equiv 1 \pmod{p-1}$ et $x \equiv y \pmod{p}$. Ceci est possible par le théorème des restes chinois, car p et $p-1$ sont premiers entre eux, donc f est surjective.

Il reste à traiter le cas où n est un produit de facteurs premiers deux à deux distincts : supposons $n = p_1 \dots p_k$ avec les (p_i) premiers et deux à deux distincts. On peut réessayer d'utiliser l'argument précédent : soit $y \in \mathbb{N}$, on cherche x entier strictement positif tel que $x^x = y \pmod{n}$, ceci est équivalent par théorème des restes chinois à $x^x = y \pmod{p_i}$ pour tout i entre 1 et k. Il suffit de prendre x tel que $x \equiv 1 \pmod{p_i - 1}$ et $x \equiv y \pmod{p_i}$ pour tout i, c'est à dire $x \equiv 1 \pmod{\prod_{i=1}^{k}(p_i - 1)}$ et $x \equiv y \pmod{p_i}$ pour tout i. Notons que les (p_i) sont deux à deux premiers entre eux, mais à priori on ne peut pas affirmer que p_i est premier $\prod_{i=1}^{k}(p_i - 1)$ pour tout i.

Si pour tout (i, j) entre 1 et k, p_i ne divise pas $p_j - 1$, dans ce cas p_i est premier $\prod_{i=1}^{k}(p_i - 1)$ pour tout i, donc par théorème des restes chinois on peut trouver x tel que $x \equiv 1 \pmod{\prod_{i=1}^{k}(p_i - 1)}$ et $x \equiv y \pmod{p_i}$ pour tout i, ainsi $x^x \equiv y \pmod{n}$.

Supposons qu'il existe (i, j) tel que p_i divise $p_j - 1$. Comme $i \neq j$, il suffit dans ce cas de vérifier que f n'est pas surjective modulo m avec $m = p_i p_j$, supposons que f est surjective modulo m. Soit $a \in \mathbb{N}$, y tel que $y \equiv 0 \pmod{p_i}$ et $y \equiv a \pmod{p_j}$ par théorème des restes chinois. Supposons qu'il existe x tel que $x^x \equiv y \pmod{p_i p_j}$. Dans ce cas $x^x \equiv 0 \pmod{p_i}$ donc p_i divise x, posons alors $x = kp_i$. Dans ce cas, $x^x \equiv (x^k)^{p_i} \equiv a \pmod{p_j}$. On obtient, en élevant à la puissance $\frac{p_j - 1}{p_i}$, $a^{\frac{p_j-1}{p_i}} = (x^k)^{p_j - 1} = 1 \pmod{p_j}$. En particulier, si a est une racine primitive modulo p_j, comme a est d'ordre exactement $p_j - 1$, on obtient une contradiction, l'application f n'est pas surjective.

Ainsi l'application est surjective si et seulement si $n = p_1 \dots p_k$ avec les (p_i) premiers et deux à deux distincts et pour tout (i, j) entre 1 et k, p_i ne divise pas $p_j - 1$.
Commentaire des correcteurs
Les copies reçues sur ce problème sont de très bon niveau. Le problème était relativement difficile, mais nombreux sont ceux qui ont trouvé de bonnes avancées. Certaines copies ont voulu utiliser le lemme chinois, certes il pouvait être utile, mais il pouvait causer beaucoup d'erreurs : notamment ce n'est pas

parce que l'application est surjective modulo p pour tout nombre p premier qu'elle l'est pour tout nombre "squarefree" c'est-à-dire sans facteur premier avec multiplicité supérieure ou égale à 2. Attention aussi à l'utilisation du théorème d'Euler ($a^{\Phi(n)} = 1 \pmod{n}$) : pour pouvoir l'utiliser, il faut que le nombre soit premier avec n.