# PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE
À RENVOYER AU PLUS TARD LE 28 JANVIER 2026

Les consignes suivantes sont à lire attentivement :

- Le groupe senior est constitué des élèves nés en 2010 ou avant, ou étant en terminale. Les autres élèves sont dans le groupe junior.
- 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.* Existe-t-il des entiers $a, b$ tels que $a^2 + b^2 = 103^3$ ?

*Exercice 2.* Trouver le plus grand entier naturel $k$ tel que $7^n + 5$ soit divisible par $k$ pour tout $n \geqslant 1$.

*Exercice 3.* Trouver tous les entiers positifs $x, y$ tels que $x^2 + y! = 2026$.

*Exercice 4.* Soient $a$ et $b$ des entiers strictement positifs tels que $a + b + 1$ soit premier et

$$a + b + 1 \mid 4ab - 1.$$

Montrer que $a = b$.

*Exercice 5.* Trouver toutes les paires d'entiers strictement positifs $(n, d)$ telles que $d \mid n^2$ et $(n - d)^2 < 2d$.

*Exercice 6.* Soit $p$ un nombre premier, et $n$ le plus petit entier strictement supérieur à $1$ tel que $n^6 - 1$ soit divisible par $p$. Montrer que $p$ divise au moins l'un des deux nombres suivants :

$$(n + 1)^6 - 1, \quad (n + 2)^6 - 1.$$

*Exercice 7.* Trouver toutes les paires d'entiers strictement positifs $(n, k)$ tels que $n! + n = n^k$.

*Exercice 8.* Déterminer tous les entiers $n \geqslant 2$ tels que les nombres $2^k \cdot n - 1$ soient premiers pour tout $k \in \{2, 3, \ldots, n\}$.

*Exercice 9.* Trouver tous les entiers $k \geqslant 0$ tels qu'il existe des entiers $m, n \geqslant 2$ tels que

$$3^k + 5^k = n^m.$$

# Exercices Seniors

*Exercice 10.* Soit $(a_n)_{n\geqslant 0}$ une suite arithmétique d'entiers telle que $a_0 = 1$, et telle que la suite est non constante. Montrer que la suite contient une infinité de cubes parfaits.
Note : Une suite $(a_n)_{n\geqslant 0}$ d'entiers est dite *arithmétique* s'il existe un entier $r \in \mathbb{Z}$ tel que pour tout $n \geqslant 0$, $a_{n+1} - a_n = r$. Un entier $z \in \mathbb{Z}$ est appelé un *cube parfait* s'il existe un entier $s \in \mathbb{Z}$ tel que $z = s^3$.

*Exercice 11.* Trouver toutes les paires d'entiers strictement positifs $(n, d)$ telles que $d \mid n^2$ et $(n-d)^2 < 2d$.

*Exercice 12.* Un entier $n \geqslant 2$ est dit discontinu si en notant $d_1 < d_2 < \ldots < d_k$ ses diviseurs strictement positifs, il existe $i$ tel que $d_i > d_{i-1} + \cdots + d_1 + 1$.
Montrer qu'il existe une infinité d'entiers $n$ tels que $n, n+1, \ldots, n+2025$ sont discontinus.

*Exercice 13.* Déterminer tous les entiers $n \geqslant 2$ tels que pour tout $p$ premier divisant $n$, $p + n$ est un carré parfait.

*Exercice 14.* Déterminer tous les entiers $n \geqslant 2$ tels que les nombres $2^k \cdot n - 1$ soient premiers pour tout $k \in \{2, 3, \ldots, n\}$.

*Exercice 15.* Trouver toutes les fonctions $f$ de $\mathbb{N}^*$ dans $\mathbb{Z}$ telles que $f(a) \leqslant f(b)$ si $a \mid b$ et

$$f(ab) + f(a^2 + b^2) = f(a) + f(b)$$

pour tous $a, b \in \mathbb{N}^*$.

*Exercice 16.* Soit $P$ un polynôme non constant à coefficients entiers tel que $P(0) = 0$ et $\text{pgcd}\{P(i), i \in \mathbb{N}\} = 1$. Montrer qu'il existe une infinité d'entiers $n$ tels que $\text{pgcd}\{P(i+n) - P(i), i \in \mathbb{N}\} = n$.

*Exercice 17.* Montrer qu'il n'existe pas d'entier $n > 1$ tel que $2^n - 1 \mid 3^n - 1$.

*Exercice 18.* Soient $m_1, \ldots, m_{2025}$ des entiers premiers entre eux deux-à-deux, et pour tout $1 \leqslant i \leqslant 2025$, $A_i$ un sous ensemble de $\{1, \ldots m_i - 1\}$. Montrer qu'il existe un entier $N > 0$ satisfaisant

$$N \leqslant \prod_i (2|A_i| + 1)$$

et tel que pour tout $i$ et pour tout $a \in A_i$, $m_i \nmid N - a$.

# Solutions junior

*Solution de l'exercice 1*

On a des carrés, on regarde donc modulo $4$. Des potentielles solutions $(a, b)$ doivent vérifier $a^2 + b^2 \equiv 103^3 \equiv 3^3 \equiv 3 \pmod 4$. Or, le carré d'un nombre pair est congru à $0$ modulo $4$ : $0^2 \equiv 2^2 \equiv 0 \pmod 4$, et le carré d'un nombre impair est congru à $1$ modulo $4$ : $1^2 \equiv 3^2 \equiv 1 \pmod 4$.

On obtient donc que si $a$ et $b$ sont tous les deux pairs, $a^2 + b^2 \equiv 0 + 0 \equiv 0 \pmod 4$, si l'un des deux est pair et l'autre impair, $a^2 + b^2 \equiv 1 + 0 \equiv 1 \pmod 4$, et si les deux sont impairs, $a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$.

Dans tous les cas, on voit qu'il est impossible de trouver de tels entiers solutions. La réponse est donc non.

Commentaire des correcteurs : Le modulo bashing est une des premières méthodes à tester lorsque l'on a une équation diophantienne. Ici il peut être utile de rappeler de passer au modulo avant de faire des calculs (et encore mieux si on remarque que $3 \equiv -1 \mod 4$).

*Solution de l'exercice 2*

Notons $k$ la solution du problème. On commence par regarder les petits cas pour se faire une idée de ce que $k$ peut être. On voit qu'un tel naturel $k$ doit diviser $7^1 + 5 = 12$ et $7^2 + 5 = 54$. Par le théorème de Bézout, il existe des entiers $x$ et $y$ tels que $x \cdot 12 + y \cdot 54 = (12, 54) = 6$, où $(12, 54)$ désigne le plus grand commun diviseur de $12$ et $54$. Ainsi, $k$ doit également diviser $6$.

Par ailleurs, si $n \geqslant 1$ est un naturel, $7^n$ et $5$ sont tous deux impairs donc $7^n + 5$ est pair, et

$$7^n + 5 \equiv 1^n + 5 \equiv 6 \equiv 0 \pmod 3,$$

donc on a toujours $2 \mid 7^n + 5$ et $3 \mid 7^n + 5$. Comme $2$ et $3$ sont premiers entre eux, $6 \mid 7^n + 5$.

On a montré que $6$ est un diviseur de tous les $7^n + 5$, d'où $6 \leqslant k$. Mais on a également montré que $k$ doit diviser $6$. On trouve donc $k = 6$.

Commentaire des correcteurs : Le problème a été très bien résolu !

*Solution de l'exercice 3*

L'idée est que si $y$ est grand, $y!$ va être nul modulo tout ce que l'on regarde, ce qui nous permettra de trouver une contradiction grâce au fait que les carrés ne peuvent pas prendre tous les restes modulo ce que l'on regarde. Il ne nous restera alors qu'un nombre fini de cas à traiter.

Remarquons que $2026 \equiv 2 \pmod 4$, donc si on avait une solution avec $y \geqslant 4$, on aurait

$$x^2 \equiv 2026 \equiv 2 \pmod 4,$$

ce qui n'est pas possible puisque les seuls résidus quadratiques (valeurs prises par des carrés) sont $0$ et $1$ modulo $4$. Toute solution vérifie donc $y \leqslant 3$, et on teste ces petits cas à la main : $y = 0$, $y = 1$, $y = 2$ et $y = 3$ nous donnent respectivement $x^2 + 1 = 2026$, $x^2 + 1 = 2026$, $x^2 + 2 = 2026$ et $x^2 + 6 = 2026$. Parmi $2025$, $2024$ et $2020$, seul $2025 = 45^2$ est un carré, donc on a deux solutions, correspondant à $y = 0$ et $y = 1$ : $(45, 0)$ et $(45, 1)$.

Commentaire des correcteurs : Le problème est très bien résolu, cependant de trop nombreux élèves oublient de traiter le cas $y = 0$, et donc manquent une des deux solutions. Il faut aussi rappeler (ou apprendre) que $0! = 1$ par convention, et non $0$.

*Solution de l'exercice 4*
Pour utiliser la condition $a + b + 1$ premier, on va essayer de factoriser le terme de droite. Tel quel, ce n'est pas possible, donc on va essayer de l'exprimer différemment. Modulo $a + b + 1$, $b$ est congru à $-a - 1$, donc

$$0 \equiv 4ab - 1 \equiv -4a(a + 1) - 1 = -4a^2 - 4a - 1 = -(2a + 1)^2 \pmod{a + b + 1}.$$

Ainsi, $a+b+1 \mid (2a+1)^2$. Seulement $a+b+1$ est un nombre premier, donc on a même $a+b+1 \mid 2a+1$ d'après le lemme d'Euclide. En particulier, $a + b + 1 \leqslant 2a + 1$, ou encore $b \leqslant a$. De même, on obtient $a \leqslant b$ (car le problème est symétrique en $a$ et $b$), donc on a bien $a = b$.

*Solution alternative à l'exercice 4 :*
Une fois que l'on a montré que $a + b + 1 \mid 2a + 1$, il est également possible de conclure par un autre argument de taille : en effet, $0 < 2a + 1 < 2(a + b + 1)$, donc $2a + 1 = a + b + 1$, soit $a = b$.

*Deuxième solution alternative à l'exercice 4 :*
On peut similairement remarquer que

$$a + b + 1 \mid (a + b + 1) \cdot (a + b - 1) = a^2 + b^2 + 2ab - 1,$$

donc

$$a + b + 1 \mid a^2 + b^2 + 2ab - 1 - (4ab - 1) = (a - b)^2.$$

Par le lemme d'Euclide, $a + b + 1$ divise $|a - b|$, mais $|a + b + 1| > |a - b|$ car $a, b > 0$, donc $a + b + 1 > \max(a, b) > |a - b|$. Cela montre que $a - b = 0$ puisque $|a - b| \geqslant 0$, ce qui conclut.
Une autre façon de conclure à partir du fait que $a \equiv b \pmod{a + b + 1}$ serait de dire que

$$0 \leqslant a, b < a + b + 1,$$

donc $a \equiv b$ implique que $a = b$.

Remarque : On peut passer d'une méthode à l'autre en utilisant le fait que

$$2a + 1 \equiv a + (a + 1) \equiv a - b \pmod{a + b + 1}.$$

Commentaire des correcteurs : Le probléme a été bien résolu, avec de nombreux raisonnements différents, dont la plupart sont présentés ci-dessus. Beaucoup d'élèves ont perdu des points pour avoir affirmé quelque chose comme : "$p \mid a - b$ et $p > a - b$, donc $a - b = 0$". Cet énoncé est erroné tel quel ; il faut en effet avoir l'hypothèse supplémentaire $a - b \leqslant 0$. Pour ce faire, il est possible de supposer sans perte de généralité que $a \geqslant b$, ou alors de rajouter des valeurs absolues : $p \mid |a - b|$ et $p > |a - b|$ et $|a - b| \geqslant 0$, donc $a = b$.

*Solution de l'exercice 5*
Les hypothèses de l'énoncé nous incitent à étudier ce qui se passe modulo $d$. On a :

$$(n-d)^2 \equiv n^2 - d(2n-d) \equiv 0 \pmod{d}.$$

Or, $(n-d)^2 < 2d$. Ainsi, puisque $(n-d)^2$ est un multiple positif de $d$, on en déduit que $(n-d)^2 = 0$ ou que $(n-d)^2 = d$.
Dans le premier cas, on obtient directement que $n = d$.
Dans le second cas, $d$ s'écrit sous la forme $a^2$, avec $a > 0$, donc $(n-a^2)^2 = a^2$. Ainsi, $n - a^2 = \pm a$, ce qui donne $n = a^2 \pm a$ (avec $a > 1$ si $n = a^2 - a$ car $n > 0$).
Réciproquement, toutes les paires d'entier de la forme $(a, a)$ ou $(a^2+a, a^2)$ pour $a > 0$ et $(a^2-a, a^2)$ pour $a > 1$ sont solutions, ce sont donc les seules.

*Solution alternative de l'exercice 5 :* Commençons par noter que $n = d$ marche toujours, supposons à présent $d \neq n$. On traite les cas $d < n$ et $d > n$ ; cela va changer quelques petites choses dans les calculs, même si les idées restent les mêmes.

Supposons dans un premier temps que $d < n$ et posons $a = n - d > 0$. On doit avoir $n - a \mid n^2$ et $a^2 < 2(n-a)$. Remarquons que $n - a \mid n^2 - a^2$, et comme $n - a \mid n^2$, on en déduit que $n - a \mid a^2$. Comme de plus $a^2 < 2(n-a)$, $a^2$ est un multiple de $n - a$ qui est strictement positif et strictement inférieur à $2(n-a)$, donc $a^2 = n - a$, ou encore $n = a(a+1)$. Réciproquement, si $d = a^2$ et $n = a(a+1)$ pour un entier $a$, les deux conditions de l'énoncé sont bien vérifiées.

Supposons à présent que $d > n$, et posons $a = d - n > 0$. On doit avoir $a + n \mid n^2$ et $a^2 < 2(a+n)$. On a également $a + n \mid a^2 - n^2$, d'où $a + n \mid a^2$ et $a^2 = a + n$ comme précédemment. Puisque l'on doit avoir $n > 0$, il faut que $a > 1$. Réciproquement, si $d = a^2$ et $n = a(a-1)$ pour un entier $a > 1$, les deux conditions de l'énoncé sont bien vérifiées.

Finalement, les solutions sont exactement les couples de la forme $(a, a)$, $(a(a+1), a^2)$ ou $(a(a-1), a^2)$ avec $a$ un entier strictement positif (et $a > 1$ dans le dernier cas).

Commentaire des correcteurs : Le problème a été correctement traité par la plupart des copies. Cependant, de nombreux.ses élèves ont oublié qu'une équation de degré 2 a deux solutions, et ont donc seulement trouvé la moitié des solutions. Un bon moyen d'éviter ce genre d'erreurs est de dresser la liste des solutions pour des petites valeurs de $n$ et de $d$, pour vérifier ensuite que les solutions trouvées coïncident avec cette liste de solutions. De plus, on rappelle qu'il est important de vérifier que les solutions trouvées vérifient bien l'énoncé. En effet, même lorsque ce n'est pas nécessaire si on a raisonné par équivalences, cela permet de s'assurer qu'il n'y a pas eu d'erreur de calcul et d'éviter de perdre un point bêtement.

*Solution de l'exercice 6*

On commence par traiter le cas $n = 2$ à part. Dans ce cas, on a $p \mid 2^6 - 1 = 63$, donc $p = 3$ ou $p = 7$. Dans les deux cas, le petit théorème de Fermat nous permet d'affirmer que $4^6 \equiv 1 \pmod{p}$, d'où le résultat dans ce cas. On suppose donc à présent que $n \geqslant 3$.

Remarquons que l'on dispose de la factorisation suivante :

$$n^6 - 1 = (n^3 - 1)(n^3 + 1) = (n - 1)(n^2 + n + 1)(n + 1)(n^2 - n + 1).$$

Si $p$ divise $n^6 - 1$ il doit donc diviser l'un de ces facteurs par le lemme d'Euclide.

- Si $p \mid n - 1$, alors $p \mid (n - 2) + 1$, et donc $p \mid (n - 2)^6 - 1$, ce qui contredit la minimalité de $n$, à l'exception peut-être du cas $n = 3$ où l'on n'aurait pas $n - 2 > 1$. Seulement si $n = 3$, $p \mid 2$ et on a bien $2 \mid (3 + 2)^6 - 1$.
- Si $p \mid n^2 + n + 1$, alors $p \mid (n + 1)^2 - (n + 1) + 1$, et donc $p \mid (n + 1)^6 - 1$ comme voulu.
- Si $p \mid n + 1$, alors $p \mid (n + 2) - 1$, et donc $p \mid (n + 2)^6 - 1$ comme voulu.
- Si $p \mid n^2 - n + 1$, alors $p \mid (n - 1)^2 + (n - 1) + 1$, donc $p \mid (n - 1)^6 - 1$, ce qui contredit la minimalité de $n$ puisque $n - 1 > 1$.

Ainsi, dans tous les cas où $n$ est minimal, $p$ divise bien au moins l'un des deux nombres $(n + 1)^6 - 1$ et $(n + 2)^6 - 1$.

Commentaire des correcteurs : Le problème a été bien résolu. La grande majorité des élèves ont trouvé la solution du corrigé, d'autres ont trouvé une solution utilisant des ordres. Cependant, beaucoup d'élèves ont perdu un point pour avoir omis les conditions de l'énoncé qui demandent de considérer $n > 1$ pour $n^6 - 1$, et donc quand on manipulait $n - 1$ et $n - 2$, il fallait s'assurer qu'il soit défini dans ce contexte, et donc traiter à part $n = 2$ et $n = 3$. Enfin, un élément important qui facilitait la compréhension de l'exercice était de remarquer que si $\nu_n = n^2 + n + 1$ alors $\nu_{n-1} = n^2 - n + 1$ et $\nu_{n+1} = n^2 + 3n + 3$.

*Solution de l'exercice 7*

Il ne peut y avoir de solution lorsque $k = 1$ puisque $n! > 0$. Ainsi, $k \geqslant 2$.

On commence par diviser par $n$ puis regarder modulo $n$, ce qui donne $(n-1)! \equiv -1 \pmod{n}$. On reconnaît ici le théorème de Wilson : $n$ doit être premier (car $n = 1$ ne marche clairement pas). En effet, dans le cas contraire, $n$ posséderait un facteur premier $p \leqslant n-1$, donc $n$ et $(n-1)!$ ne pourraient pas être premiers entre eux.

On cherche à résoudre $(n-1)! + 1 = n^{k-1}$, soit $(n-1)! = n^{k-1} - 1 = (n-1)(n^{k-2} + \ldots + 1)$, ou encore (car $n > 1$) : $(n-2)! = 1 + \ldots + n^{k-2}$. On remarque que si $n > 5$, $(n-1) \mid (n-2)!$.

En effet, $n$ est un nombre premier supérieur à $5$ donc $n-1$ est pair. Or, $n > 5$, donc $\frac{n-1}{2} > 2$. On a donc $2 < \frac{n-1}{2} \leqslant n-2$, donc on a un facteur $2$ et un facteur $\frac{n-1}{2}$ dans $(n-2)!$. Donc $n-1 = 2 \cdot \frac{n-1}{2} \mid (n-2)!$.

Ainsi, $n-1 \mid 1 + \ldots + n^{k-2}$ mais l'on sait que $n$ est congru à $1$ modulo $n-1$.

Par suite, $n-1 \mid k-1$ donc $n-1 \leqslant k-1$. Donc $(n-1)! + 1 = n^k \geqslant n^n$, ce qui est absurde car

$$(n-1)! \leqslant (n-1)^{n-2} < n^{n-1} \leqslant n^n - 1,$$

puisque chaque facteur $> 1$ du produit $(n-1)!$ est $\leqslant n-1$.

Il reste donc à tester $n = 2, 3, 5$ et on trouve comme solutions $(2, 2)$, $(3, 2)$ et $(5, 3)$.

Commentaire des correcteurs : Il s'agissait d'un problème difficile. Comme il y avait une factorielle, Wilson est un outil à garder en tête. Par ailleurs il faut comme d'habitude tester les petits cas. Nous nous réjouissons que les élèves ayant rendu une copie à ce problème aient trouvé ces deux points. Le fait que $n-1 \mid (n-2)!$ est assez naturel mais la difficulté du reste de la preuve réside surtout dans le fait de penser à considérer l'exercice modulo $n-1$. En fait il faut se dire qu'une équation faisant intervenir une expression $A$ pourra souvent être intéressante modulo les nombres proches de $A$. La conclusion par un argument de taille n'a pas posé souci, ce que nous tenons à féliciter.

*Solution de l'exercice 8*

Supposons que $n \geqslant 3$, et que $n-1$ possède un diviseur premier impair $p$. Par le petit théorème de Fermat,

$$2^{p-1} \cdot n - 1 \equiv 1 \cdot 1 - 1 \equiv 0 \pmod{p},$$

et donc $2^{p-1} \cdot n - 1$ est divisible par $p$, ce qui est impossible car $2^{p-1} \cdot n - 1 \geqslant n > p$ (on a bien $2 \leqslant p - 1 \leqslant n$). Donc $n-1$ est une puissance de 2.

Supposons désormais disposer d'un diviseur premier impair $p$ de $n-2$. Par le petit théorème de Fermat,

$$2^{p-2} \cdot n - 1 \equiv 2^{p-2} \cdot 2 - 1 \equiv 0 \pmod{p},$$

d'où $2^{p-2} \cdot n - 1$ est divisible par $p$.

Si $p > 3$, on a bien $2 \leqslant p - 2 \leqslant n$, et si $p = 3$, $3 \mid 2^3 \cdot n - 1$, avec $2 \leqslant 3 \leqslant n$. On obtient une absurdité dans tous les cas, car $2^{p-2} \cdot n - 1 \geqslant n - 1 > p$ et $2^3 \cdot n - 1 \geqslant n > 3$.

Ainsi $n-2$ est aussi une puissance de 2, ce qui force $n = 3$ (car au moins un des deux nombres parmi $n-1$ et $n-2$ est impair et vaut donc 1, qui est la seule puissance de 2 impaire). Les seules solutions possibles sont donc $n = 2$ et $n = 3$, et réciproquement on vérifie que les deux sont bien solutions.

Commentaire des correcteurs :

L'exercice est plutôt bien réussi. Attention à bien vérifier toutes les solutions. La plupart des élèves n'ont pas montré que $n-2$ était une puissance de 2, mais ont montré que $n$ valait 0 modulo 3 et 5, ce qui est incompatible avec le fait d'être de la forme $2^k + 1$.

*Solution de l'exercice 9*

Soit $k$ solution, et $m, n \geqslant 2$ tels que $3^k + 5^k = n^m$. On va s'intéresser aux facteurs premiers de $3^k + 5^k$. Ce dont on peut être sûr, c'est que $3^k + 5^k$ est toujours pair. On s'intéresse donc à sa valuation 2-adique. Pour cela, on va regarder la valeur de $3^k + 5^k$ modulo des puissances de 2.

Si $k$ est pair, $3^k \equiv 5^k \equiv 1 \pmod 4$, donc $3^k + 5^k \equiv 2 \pmod 4$ et $v_2(3^k + 5^k) = 1$. Mais $v_2(3^k + 5^k) = v_2(n^m) = m v_2(n)$, ce qui est absurde car $m \geqslant 2$.

Donc $k$ est impair. Si $k \equiv 1 \pmod 4$, alors $3^k + 5^k \equiv 3 + 5 \equiv 8 \pmod{16}$, et si $k \equiv 3 \pmod 4$, alors $3^k + 5^k \equiv 27 + 125 \equiv 152 \equiv 8 \pmod{16}$. Dans tous les cas, on $v_2(3^k + 5^k) = 3$. On a donc toujours $m v_2(n) = v_2(3^k + 5^k) = 3$, donc $m \mid 3$ et puis $m = 3$ car $m > 1$.

On a donc $3^k + 5^k = n^3$. On commence à voir apparaître beaucoup de facteurs 3, on va donc regarder modulo 3. Ça ne donne rien de bien intéressant, donc on essaye modulo 9.

Si $k \geqslant 2$, on obtient $5^k \equiv n^3 \pmod 9$. Les cubes valent $-1$, 0 ou 1 modulo 9, tandis que les puissances de 5 valent successivement 1, 5, $-2$, $-1$, 4, 2, 1,... modulo 9. On en déduit que les deux termes de l'égalité valent $-1$ ou 1 modulo 9, et en particulier que $3 \mid k$. En notant $k = 3l$, on obtient

$$(3^l)^3 + (5^l)^3 = n^3 \quad (\star).$$

Or, en réduisant cette égalité modulo 7, on obtient :

$$(-1)^l + (-1)^l \equiv n^3 \pmod 7,$$

ce qui constitue une contradiction car les cubes ne prennent que les valeurs $0, 1, 6$ modulo 7.

On a donc $k = 1$, qui réciproquement est bien solution : $3^1 + 5^1 = 8 = 2^3$. La seule solution est donc $k = 1$.

Remarque : On peut également noter que l'égalité $(\star)$ est impossible à cause de résultats comme le théorème de Zsigmondy ou le grand théorème de Fermat.

Commentaire des correcteurs :

Ce problème, plutôt facile pour sa position, a été abordé et résolu par de nombreux élèves. Toutes les solutions montraient que $m = 3$ en utilisant un argument de valuation 2-adique et puis regardaient modulo 9, mais à partir de là il était possible de conclure en regardant modulo 7, en utilisant le théorème de Wiles-Fermat ou celui de Zsigmondy,... Plusieurs copies n'ont pas vérifié que $k = 0$ ne fonctionnait pas, ce qui n'a pas été pénalisé ici puisque ce n'était ni très dur, ni très intéressant.

# Solutions senior

*Solution de l'exercice 10* Notons $r \in \mathbb{Z}^*$ la raison de cette suite arithmétique. On a alors $a_n = nr + 1$ pour tout $n \in \mathbb{N}$. On veut trouver beaucoup de cubes congrus à $1$ modulo $r$. Or, le cube d'un nombre congru à $1$ modulo $r$ est lui-même congru à $1$ modulo $r$, plus précisément : $(nr+1)^3 = n^3r^3 + 3n^2r^2 + 3nr+1 = (n^3r^2+3n^2r+3n)r+1$. Donc pour tout $n$ assez grand, puisque $r^2 > 0$, on a $n^3r^2+3n^2r+3n \geqslant 0$ et $a_{n^3r^2+3n^2r+3n}$ est donc un cube, ce qui conclut. De plus, lorsque l'on se restreint à des $n$ assez grands, la quantité précédente est strictement croissante donc on obtient bien une infinité de cubes distincts.

Commentaire des correcteurs : Le problème a été traité par un grand nombre d'élèves. La plupart ont soit trouvé la solution du corrigé, soit une solution en passant par les classes de congruences. La grande majorité des erreurs étaient de ne pas vérifier que la construction des cubes soit bien définie, car la suite $a_n$ est définie uniquement pour $n > 0$.

*Solution de l'exercice 11*
Les hypothèses de l'énoncé nous incitent à étudier ce qui se passe modulo $d$. On a :

$$(n-d)^2 \equiv n^2 - d(2n-d) \equiv 0 \pmod{d}.$$

Or, $(n-d)^2 < 2d$. Ainsi, puisque $(n-d)^2$ est un multiple positif de $d$, on en déduit que $(n-d)^2 = 0$ ou que $(n-d)^2 = d$.
Dans le premier cas, on obtient directement que $n = d$.
Dans le second cas, $d$ s'écrit sous la forme $a^2$, avec $a > 0$, donc $(n-a^2)^2 = a^2$. Ainsi, $n - a^2 = \pm a$, ce qui donne $n = a^2 \pm a$ (avec $a > 1$ si $n = a^2 - a$ car $n > 0$).
Réciproquement, toutes les paires d'entier de la forme $(a, a)$ ou $(a^2 + a, a^2)$ pour $a > 0$ et $(a^2 - a, a^2)$ pour $a > 1$ sont solutions, ce sont donc les seules.

*Solution alternative de l'exercice 5 :* Commençons par noter que $n = d$ marche toujours, supposons à présent $d \neq n$. On traite les cas $d < n$ et $d > n$ ; cela va changer quelques petites choses dans les calculs, même si les idées restent les mêmes.

Supposons dans un premier temps que $d < n$ et posons $a = n - d > 0$. On doit avoir $n - a \mid n^2$ et $a^2 < 2(n-a)$. Remarquons que $n - a \mid n^2 - a^2$, et comme $n - a \mid n^2$, on en déduit que $n - a \mid a^2$. Comme de plus $a^2 < 2(n-a)$, $a^2$ est un multiple de $n - a$ qui est strictement positif et strictement inférieur à $2(n-a)$, donc $a^2 = n - a$, ou encore $n = a(a+1)$. Réciproquement, si $d = a^2$ et $n = a(a+1)$ pour un entier $a$, les deux conditions de l'énoncé sont bien vérifiées.

Supposons à présent que $d > n$, et posons $a = d - n > 0$. On doit avoir $a + n \mid n^2$ et $a^2 < 2(a+n)$. On a également $a + n \mid a^2 - n^2$, d'où $a + n \mid a^2$ et $a^2 = a + n$ comme précédemment. Puisque l'on doit avoir $n > 0$, il faut que $a > 1$. Réciproquement, si $d = a^2$ et $n = a(a-1)$ pour un entier $a > 1$, les deux conditions de l'énoncé sont bien vérifiées.

Finalement, les solutions sont exactement les couples de la forme $(a, a)$, $(a(a+1), a^2)$ ou $(a(a-1), a^2)$ avec $a$ un entier strictement positif (et $a > 1$ dans le dernier cas).

Commentaire des correcteurs :
Exercice très bien traité dans l'ensemble. Attention cependant, l'équation $(n-d)^2 = d$ a deux solutions : $n - d = \sqrt{d}$ mais aussi $n - d = -\sqrt{d}$.

*Solution de l'exercice 12*

On aimerait bien utiliser le lemme chinois pour que $n, \dots, n+2025$ aient peu de petits facteurs premiers et un facteur premier gigantesque. Une manière de faire ça est d'imposer que $n$ soit congru à $1$ modulo beaucoup de choses, ce qui revient simplement à prendre $n = K!+1$, pour $K$ un gros nombre à déterminer.
Remarquons que si $d \mid n+i$, on a $d \mid K! + i + 1$, donc $d > K$ ou $d \mid i+1$.
Ainsi, la somme des diviseurs plus petits que $K$ de $n+i$ vaut au plus $\sigma(i+1)$, la somme des diviseurs (positifs) de $i+1$. Donc si $K > \max(\sigma(i+1), i \in \{0, \dots, 2025\})+1$, alors pour tout $i$ le plus petit diviseur strictement supérieur à $K$ de $n+i$ (qui existe car $n+i > K! > K$) est strictement supérieur à la somme des diviseurs inférieurs à $K$ à laquelle on ajoute $1$, donc $n+i$ a bien un diviseur strictement supérieur à la somme des diviseurs précédents à laquelle on ajoute $1$, ce qui montre que le $n$ choisi convient bien.

Commentaire des correcteurs :

Une des principales difficultés de cet exercice était de bien dénombrer sans en oublier les diviseurs des nombres $x! + i$, et elle a été très bien gérée par les élèves.

*Solution de l'exercice 13*
Soit $n \geqslant 2$ une potentielle solution.
Pour tout diviseur premier $p$ de $n$, on a que $p \mid n+p$, donc $p^2 \mid n+p$. Ainsi, $p^2 \nmid n$ car sinon $n+p \equiv p \pmod{p^2}$. Cela montre que $n$ est squarefree (il n'est divisible par aucun carré de nombre premier).
Si $n$ admet deux diviseurs premiers $p < q < \sqrt{n}$, alors

$$\sqrt{n+p}^2 = n+p < n+q = n+p+q-p \leqslant n+p+\sqrt{n} \leqslant n+p+\sqrt{n+p} < (\sqrt{n+p}+1)^2,$$

et donc $n+q$ est un carré strictement compris entre les carrés de deux entiers consécutifs, absurde.
Si $n$ admet au moins trois facteurs premiers, les deux plus petits sont strictement plus petits que $\sqrt{n}$ : en effet, si $q > p$ sont deux facteurs premiers de $n$, alors $pq \mid n$, donc $p < \sqrt{n}$ car $n \geqslant pq > p^2$. D'après le paragraphe précédent, ce cas-là est donc impossible.
Si $n$ est premier, alors $n+n = 2n$ est un carré et donc $n = 2$, qui est réciproquement un entier solution.
Si $n = pq$ avec $p < q$ des nombres premiers, alors $p(q+1)$ et $q(p+1)$ sont des carrés, donc $p \mid q+1$ et $q \mid p+1$, donc comme $q > p$ on doit avoir $q = p+1$. L'un des deux parmi $p$ et $q$ est donc pair et vaut donc $2$, seul premier pair. Le cas $q = 2$ donne $p = 1$, impossible, donc $p = 2$ puis $q = 3$, et finalement $n = 6$. $6+2 = 8$ n'est pas un carré, donc $n = 6$ ne convient pas.
En conclusion, $2$ est la seule solution.

*Solution alternative*
De même que précédemment, on remarque que $n$ est squarefree.
Si $n \equiv 0 \pmod{4}$, $4 \mid n$ et $n$ n'est pas squarefree.
Si $n \equiv 3 \pmod{4}$, $n$ a nécessairement un facteur premier $p \equiv 3 \pmod{4}$ (car $n$ ne peut pas être un produit de facteurs premiers tous congrus à $1$ modulo $4$), et alors $n+p \equiv 2 \pmod{4}$ ne peut pas être un carré.
Si $n \equiv 1 \pmod{4}$, si on note $p$ un facteur premier de $n$, $p$ est impair et si $p \equiv 1 \pmod{4}$, $n+p \equiv 2 \pmod{4}$ ne peut pas être un carré. Donc tous les facteurs premiers de $n$ sont congrus à $3$ modulo $4$.
Si $n \equiv 2 \pmod{4}$ possède un facteur premier impair $p$, on voit que $p \equiv 1 \pmod{4}$ donne $p+n \equiv 3 \pmod{4}$, qui ne peut pas être un carré. Donc tous les facteurs premiers impairs de $n$ sont congrus à $3$ modulo $4$.
Dans tous les cas, tous les facteurs premiers impairs de $n$ sont congrus à $3$ modulo $4$. Supposons que $n$ ait deux facteurs premiers impairs distincts $p, q$. Puisque $n+p$ et $n+q$ sont des carrés, on sait que $p$ est un résidu quadratique modulo $q$ et inversement. Donc d'après la loi de réciprocité quadratique

$$1 = 1 \cdot 1 = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1,$$

absurde.
Donc $n$ a au plus un facteur premier impair, et comme il est squarefree, il s'écrit sous la forme $2$, $q$ ou $2q$, avec $q$ un nombre premier impair. Cependant, $q+q = 2q$ n'est pas un carré, et $2q+q = 3q$ n'est un carré que si $q = 3$, ce qui donne $n = 2 \cdot 3 = 6$ qui ne convient pas. On a donc bien $n = 2$, qui convient réciproquement.

Commentaire des correcteurs : Cet exercice a été bien abordé, les élèves ont proposé des solutions assez diverses et variées. Les principales sources d'erreurs sont : l'oubli de vérifier que $2$ est effectivement solution, l'oubli de certains cas parmi ceux traités, et quelques imprécisions dans les inégalités utilisées.

*Solution de l'exercice 14*

Supposons que $n \geqslant 3$, et que $n-1$ possède un diviseur premier impair $p$. Par le petit théorème de Fermat,

$$2^{p-1} \cdot n - 1 \equiv 1 \cdot 1 - 1 \equiv 0 \pmod{p},$$

et donc $2^{p-1} \cdot n - 1$ est divisible par $p$, ce qui est impossible car $2^{p-1} \cdot n - 1 \geqslant n > p$ (on a bien $2 \leqslant p - 1 \leqslant n$). Donc $n-1$ est une puissance de 2.

Supposons désormais disposer d'un diviseur premier impair $p$ de $n-2$. Par le petit théorème de Fermat,

$$2^{p-2} \cdot n - 1 \equiv 2^{p-2} \cdot 2 - 1 \equiv 0 \pmod{p},$$

donc $2^{p-2} \cdot n - 1$ est divisible par $p$.

Si $p > 3$, on a bien $2 \leqslant p - 2 \leqslant n$, et si $p = 3$, on a $3 \mid 2^3 \cdot n - 1$, avec $2 \leqslant 3 \leqslant n$. On obtient une absurdité dans tous les cas, car $2^{p-2} \cdot n - 1 \geqslant n - 1 > p$ et $2^3 \cdot n - 1 \geqslant n > 3$.

Ainsi $n-2$ est aussi une puissance de 2, ce qui force $n = 3$ (car au moins un des deux nombres parmi $n-1$ et $n-2$ est impair et vaut donc 1, qui est la seule puissance de 2 impaire). Les seules solutions possibles sont donc $n = 2$ et $n = 3$, et réciproquement on vérifie que les deux sont bien solutions.

Commentaire des correcteurs :

L'exercice a été bien traité par les éléves ayant rendu une copie. De nombreux élèves ont procédé comme dans le corrigé, d'autres ont regardé modulo 3 et 5 une fois avoir prouvé que $n-1$ était une puissance de 2. Attention cependant aux justifications : lorsque l'on a une divisibilité du type $p \mid 2^k \cdot n - 1$ avec $p > 1$, il faut encore vérifier $2^k \cdot n - 1 \neq p$ pour affirmer que $2^k \cdot n - 1$ est premier !

*Solution de l'exercice 15*

Notons tout d'abord que pour tout $n$, $f(1) \leqslant f(n)$, et que si $f$ est solution, alors $f - f(1)$ l'est aussi. Supposons donc que $f(1) = 0$, ce qui implique $f \geqslant 0$.

*Lemme :* Si $-1$ est un résidu quadratique modulo $n$, alors $f(n) = 0$. En particulier, si $p = 2$ ou si $p$ est un nombre premier congru à $1 \pmod 4$, alors $f(p) = 0$.
*Preuve :* Si $-1$ est un résidu quadratique modulo $n$, il existe un entier strictement positif $a$ tel que $n \mid a^2 + 1$. En posant $b = 1$, on obtient alors $f(a^2 + 1) = f(1) = 0$.

Soit $p$ un nombre premier divisant $a$. En posant $b = p$ on obtient $f(ap) + f(a^2 + p^2) = f(a) + f(p)$, et comme $f(ap) \geqslant f(a)$ et $f(a^2 + p^2) \geqslant f(p)$ on doit avoir égalité dans chacune des inégalités, et en particulier $f(ap) = f(a)$. Cela implique assez clairement que $f(n) = f(\mathrm{rad}(n))$ pour tout $n$, où $\mathrm{rad}(n)$ est le produit de tous les diviseurs premiers (distincts) de $n$ (il suffit "d'enlever" les facteurs premiers de $n$ présents en plusieurs exemplaires au fur et à mesure).

Soit à présent $p$ ne divisant pas $a$, étudions $f(a^2 + p^2)$.
Notons que si $q$ est un nombre premier congru à $3 \pmod 4$ et si $q \mid a^2 + p^2$, alors $q \mid a$ et $q \mid p$ (car $-1$ n'est pas un résidu quadratique modulo $q$), donc $p = q \mid a$, ce qui est impossible. Ainsi, $a^2+p^2$ a tous ses facteurs premiers congrus à 1 ou $2 \pmod 4$, donc $-1$ est un carré modulo $q$ pour tout diviseur premier $q$ de $a^2+p^2$. Le théorème des restes chinois nous informe alors que $-1$ est également un résidu quadratique modulo leur produit $\mathrm{rad}(a^2 + p^2)$. En effet, si $q_i \mid a^2 + p^2$, il existe $x_i$ tel que $x_i^2 \equiv -1 \pmod{q_i}$. Donc si on prend $x \equiv x_i \pmod{q_i}$ pour tout $i$, on a $q_i \mid x^2 + 1$ pour tout $i$, donc $\prod_{q \mid a^2+p^2} q \mid x^2 + 1$, soit $\mathrm{rad}(a^2 + p^2) \mid x^2 + 1$. On a donc

$$f(a^2 + p^2) = f(\mathrm{rad}(a^2 + p^2)) = 0$$

par le lemme.
Mais alors, $f(a) + f(p) = f(ap) + f(a^2 + p^2) = f(ap)$. Ainsi,

$$f(n) = f(\mathrm{rad}(n)) = f\Big(\prod_{p \mid n} p\Big) = \sum_{p \mid n} f(p) = \sum_{p \in \mathcal{P}(n)} f(p),$$

où $\mathcal{P}(n)$ est l'ensemble des nombres premiers congrus à $3 \pmod 4$ qui divisent $n$.
Il s'avère qu'en essayant un peu plus, on ne peut pas vraiment dire plus de choses sur les valeurs de $f$ en $p \equiv 3 \pmod 4$, et il y a en fait une bonne raison : tout choix de valeurs va donner une solution.

Faisons donc la synthèse : supposons fixées les valeurs $f(p) \geqslant 0$ pour tout $p$ premier congru à $3 \pmod 4$, et montrons que la fonction

$$f(n) = \sum_{\mathcal{P}(n)} f(p)$$

est bien solution.
Tout d'abord, la condition $f(a) \leqslant f(b)$ si $a \mid b$ est bien vérifiée par le fait que $f(p) \geqslant 0$. De plus, pour $a, b \in \mathbb{N}^*$, on a $\mathcal{P}(ab) = \mathcal{P}(a) \cup \mathcal{P}(b)$. Soit $p$ un nombre premier congru à $3 \pmod 4$ qui divise $a^2 + b^2$. Alors $p \mid a$ et $p \mid b$, donc $\mathcal{P}(a^2 + b^2) = \mathcal{P}(a) \cap \mathcal{P}(b)$. Enfin, on a

$$f(ab) + f(a^2 + b^2) = \sum_{p \in \mathcal{P}(a) \cup \mathcal{P}(b)} f(p) + \sum_{p \in \mathcal{P}(a) \cap \mathcal{P}(b)} f(p) = \sum_{p \in \mathcal{P}(a)} f(p) + \sum_{p \in \mathcal{P}(b)} f(p) = f(a) + f(b),$$

comme voulu.

Ainsi, les solutions sont exactement celles de la forme

$$f(n) = c + \sum_{p \in \mathcal{P}(n)} c_p,$$

où $c \in \mathbb{Z}$ et $c_p \in \mathbb{N}$ sont fixées.

Commentaire des correcteurs :
L'exercice a été résolu par une majorité des personnes qui l'ont rendu. On peut souligner qu'aucune solution qui résout l'analyse n'a oublié l'étape de vérification ! Cet exercice utilisait fortement les résultats sur les facteurs premiers de nombres de la forme $a^2 + b^2$, et il était dur d'aller loin dans le problème sans une connaissance des lemmes clés dans cette direction. Il arrivera que ce genre de test de culture générale apparaisse également en compétition, les élèves avec cette ambition devraient donc chercher à connaître ce genre de résultat. Enfin, remarquer que si $f$ vérifie l'équation alors $f - f(1)$ la vérifie également simplifiait beaucoup de calculs en supprimant de nombreux $f(1)$ de beaucoup d'équations. En général, c'est une bonne idée de se poser une ou deux minutes pour voir si on ne peut pas supposer des propriétés intéressantes pour une solution éventuelle.

*Solution de l'exercice 16*

Rappelons que comme $P$ est à coefficients entiers, $a-b \mid P(a)-P(b)$ pour tous entiers $a$ et $b$. Ce qu'on peut déjà remarquer, c'est donc que pour tout $n>0$ et pour tout $i \in \mathbb{N}$, $n \mid i+n-i \mid P(i+n)-P(i)$. Donc $n \mid \operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\}$.

On aimerait qu'il y ait une infinité d'entiers $n$ tels que $\operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\} \mid n$. Fixons un $n>0$, et considérons un facteur premier $p$ de $\operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\}$. On a par hypothèse que $p \mid P(n)-P(0)=P(n)$, puis que $p \mid P(2n)-P(n)$ donc $p \mid P(2n)$, et ainsi de suite : pour tout $i \in \mathbb{Z}$, $p \mid P(in)$. Si $p$ ne divise pas $n$, $n$ est alors inversible modulo $p$, d'inverse noté $n^{-1}$. Donc pour tout $i \in \mathbb{N}$, $i \equiv in^{-1}n \pmod{p} \Longrightarrow P(i) \equiv P(in^{-1}n) \equiv 0 \pmod{p}$. Donc $p \mid \operatorname{pgcd}\{P(i), i \in \mathbb{N}\}=1$, ce qui est absurde. Donc on a $p \mid n$.

Pour contrôler les facteurs premiers de $\operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\}$, on veut que $n$ ait peu de facteurs premiers, ce qui nous incite à prendre $n$ une puissance de nombre premier : $n=p^{\alpha}$, $\alpha>0$. On sait donc que $\operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\}$ est divisible par $p^{\alpha}$, son seul facteur premier est $p$, donc pour montrer que ça vaut $p^{\alpha}$, il suffit de montrer que ce n'est pas divisible par $p^{\alpha+1}$.

Supposons par l'absurde que $p^{\alpha+1} \mid \operatorname{pgcd}\{P(i+n)-P(i), i \in \mathbb{N}\}$. Pour tout $i \in \mathbb{N}$, on a

$$P(i+n)=P(i+p^{\alpha}) \equiv P(i)+p^{\alpha}P'(i) \pmod{p^{\alpha+1}}$$

d'après la formule de Taylor (on peut aussi le voir en développant tout en utilisant le binôme de Newton). Donc $p^{\alpha+1} \mid p^{\alpha}P'(i)$ pour tout $i$, soit $p \mid P'(i)$ pour tout $i$.

Or, $P$ est non-constant, donc $P'$ est non-nul. Il existe ainsi $i \in \mathbb{N}$ tel que $P'(i) \neq 0$, et en prenant $p>|P'(i)|$, $p \mid P'(i)$ est alors impossible. Donc toutes les puissances de ce nombre premier $p$ conviennent, ce qui conclut.

Commentaire des correcteurs :

Il s'agissait d'un problème en deux parties sur lequel on pouvait développer de nombreuses idées d'ordre purement arithmétique. La première partie, plus accessible, consistait à s'intéresser à l'existence d'un éventuel diviseur premier différent de $p$ de l'expression $\gcd(P(n+p)-P(n))_{n \in \mathbb{N}}$, et a été très bien résolue. La seconde était nettement plus technique et se trouvait grandement facilitée par la connaissance de propriétés des polynômes sur $\mathbb{Z}/p\mathbb{Z}$ (formule de Taylor, ...). Bien que les copies ayant abordé le problème s'en soit rendu compte, il est souvent moins habituel de manipuler des polynômes dans $\mathbb{Z}/p\mathbb{Z}$, donc il est important de vérifier (surtout aux débuts), que toutes les hypothèses des théorèmes utilisés sont vraiment vérifiées (ou bien que les théorèmes existent vraiment). A ce sujet, le cours de Théo en 2022 au groupe D est très intéressant !

*Solution de l'exercice 17*

Tout d'abord, si $n$ est pair, alors $3 \mid 2^n - 1 \mid 3^n - 1$, ce qui est impossible car $n \geqslant 1$. On en déduit qu'une potentielle solution $n$ doit être impair.

On déduit alors de $2^n - 1 \mid 3^{n+1} - 3$ que pour tout facteur premier $p$ de $2^n - 1$ (qui est donc $\neq 3$),

$$3 \equiv (3^{\frac{n+1}{2}})^2 \pmod{p},$$

donc $3$ est un résidu quadratique (non-nul) modulo $p$. Donc si $p$ est un diviseur premier (forcément impair) de $2^n - 1$, on a en utilisant le symbole de Legendre et la réciprocité quadratique :

$$1 = \left(\frac{3}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{3-1}{2})} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right),$$

donc $p \equiv 1 \pmod 3$ et $p \equiv 1 \pmod 4$, ou $p \equiv -1 \pmod 3$ et $p \equiv -1 \pmod 4$. Le théorème des restes chinois nous informe donc que $3$ est un résidu quadratique modulo $p$ exactement quand $p \equiv \pm 1 \pmod{12}$. On doit donc avoir $2^n - 1 \equiv \pm 1 \pmod{12}$, puisque $2^n - 1$ est un produit de premiers congrus à $\pm 1$ modulo $12$. Si $2^n - 1 \equiv 1 \pmod{12}$, $2^n$ n'est pas divisible par $4$, donc $n \leqslant 1$ ce qui est exclu. Si $2^n - 1 \equiv -1 \pmod{12}$, on a $3 \mid 2^n$, ce qui est impossible. Il n'y a donc aucune solution.

Commentaire des correcteurs : L'exercice a été résolu par la plupart des élèves qui l'ont rendu. Toutes les solutions utilisaient la réciprocité quadratique ou des outils équivalents. Ce serait bien, avant d'utiliser la réciprocité quadratique, de vérifier que $p$ ne vaut ni $2$ ni $3$.

*Solution de l'exercice 18*

On se rappelle qu'une solution à $x \equiv a_i \pmod{m_i}$ pour tout $i$ est $x = \sum a_i t_i$, où pour tout $i$, $t_i$ est une solution modulo $m_1 \dots m_{2025}$ de $t_i \equiv 1 \pmod{m_i}$ et $t_i \equiv 0 \pmod{m_j}$ pour tout $j \neq i$. On veut donc qu'il existe $0 < N = \sum_i b_i t_i$, avec pour tout $i$, $b_i \notin A_i$ et $N \leqslant (2|A_1|+1) \dots (2|A_{2025}|+1)$. Plutôt que de chercher un tel $N$ directement, on va chercher à l'exprimer comme une différence de deux termes pas trop éloignés. On va donc considérer des nombres de la forme $\sum_i c_i t_i$, où $c_i \in C_i$, avec $C_i$ un ensemble de valeurs à déterminer tel que $\forall x, y \in C_i$, $x - y$ n'est congru à aucun élément de $A_i$ modulo $m_i$.

On va montrer que l'on peut les construire avec au moins $\frac{m_i}{2|A_i|+1}$ éléments. On suppose donc disposer d'un $C_i$ qui vérifie cette propriété, mais qui a strictement moins de $\frac{m_i}{2|A_i|+1}$ éléments. Si l'on veut rajouter un élément à $C_i$, les seuls valeurs interdites (modulo $m_i$) sont : un élément de $C_i$, un élément de $C_i$ moins un élément de $A_i$, un élément de $C_i$ plus un élément de $A_i$. Donc le nombre de valeurs interdites est au plus $|C_i| + |A_i||C_i| + |A_i||C_i| = (2|A_i| + 1)|C_i| < m_i$, et on peut donc bien mettre une nouvelle valeur dans $C_i$.

Considérons désormais tous les nombres de la forme $\sum_i c_i t_i$ (pris modulo $m_1 \dots m_{2025}$), où pour tout $i$, $c_i \in C_i$. Il y a au moins $|C_1| \dots |C_{2025}|$ tels nombres différents (car deux 2025-uplets de $c_i$ conduisent à deux nombres différents modulo $m_1 \dots m_{2025}$, puisque $\sum_i c_i t_i \equiv c_i \pmod{m_i}$ pour tout $i$), donc il y en a au moins $\frac{m_1 \dots m_{2025}}{(2|A_1|+1)\dots(2|A_{2025}|+1)}$. Par principe des tiroirs, comme tous ces nombres sont compris entre $0$ et $m_1 \dots m_{2025} - 1$ (quitte à choisir les bons représentants modulo $m_1 \dots m_{2025}$), on a un nombre $N$ inférieur à $(2|A_1| + 1) \dots (2|A_{2025}| + 1)$ qui est congru à $\sum_i (c_i - c_i')t_i$ modulo $m_1 \dots m_{2025}$, avec $c_i, c_i' \in C_i$ pour tout $i$. Donc pour tout $i$, $N \equiv c_i - c_i' \pmod{m_i}$, et n'est donc congru à aucun des $a \in A_i$ modulo $m_i$ par définition de $C_i$. Ainsi, ce $N$ convient bien.

Commentaire des correcteurs :

Ce problème, extrêmement difficile, a été abordé par trois élèves et résolu par un élève seulement. Cet élève, à l'aide de techiques complètement différentes de celles du corrigé, a prouvé la meilleure borne $N \leqslant \prod_{i=1}^{2025} (|A_i| + 1)$.