PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE
À RENVOYER AU PLUS TARD LE 25 JANVIER 2021

Les consignes suivantes sont à lire attentivement :

- Le groupe junior est constitué des élèves nés en 2006 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.

Animath,
Préparation Olympique Française de Mathématiques,
11-13 rue Pierre et Marie Curie,
75005 Paris.
contact-pofm@animath.fr

Exercices Juniors

Exercice 1. Soit n un entier naturel tel que n divise 2^n. Montrer que $\dfrac{2^n}{n}$ est une puissance de 2.

Solution de l'exercice 1
Comme 2^n est une puissance de 2, tous ses diviseurs sont des puissances de 2. On a supposé que n divisait 2^n, donc on sait que $\dfrac{2^n}{n}$ est un entier. Or $\dfrac{2^n}{n} \cdot n = 2^n$, donc $\dfrac{2^n}{n}$ est un diviseur de 2^n. Cela montre que $\dfrac{2^n}{n}$ est une puissance de 2.

Commentaire des correcteurs : L'exercice est très bien réussi. Néanmoins quand on parle de puissances de 2 en arithmétique, on sous-entend les nombres de la forme 2^ℓ avec $\ell \in \mathbb{N}$, pas $\ell \in \mathbb{Z}$. Certains ont dit que comme n divisait une puissance de 2, n était de la forme 2^k, donc $\frac{2^n}{n} = 2^{n-k}$ est une puissance de 2, il aurait été bien de dire que forcément $k \leqslant n$, pour avoir que $n - k \geqslant 0$.

Exercice 2. Trouver tous les couples (x, y) d'entiers naturels tels que :

$$x^2 - 4y^2 = 3$$

.

Solution de l'exercice 2
En réduisant l'équation modulo 4, on constate que $x^2 \equiv 3[4]$. Un tableau de congruence montre alors que les carrés ne peuvent prendre que les valeurs 0 ou 1 modulo 4. Cette équation n'a donc pas de solutions entières.

Solution alternative n°1
On peut factoriser l'équation sous la forme $(x - 2y)(x + 2y) = 3$. Comme $x + 2y \geqslant 0$, on sait que $x - 2y \geqslant 0$ sinon leur produit serait négatif. Or la seule manière d'écrire 3 comme produit de deux entiers naturels est $1 \cdot 3$, donc comme $x + 2y \geqslant x - 2y$, on a $x + 2y = 3$ et $x - 2y = 1$. En soustrayant la deuxième équation à la première, on trouve $4y = 2$, donc il n'y a pas de solutions entières.

Commentaire des correcteurs : L'exercice est très bien réussi. Néanmoins, une fois écrit $(x + 2y)(x - 2y) = 3$, certains oublient de mentionner que $x + 2y \geqslant 0$, alors que sinon on pourrait envisager que $x + 2y = -1$ ou -3.

Exercice 3. Alice met 100 billes dans un sac. Sur chaque bille elle a écrit le carré d'un entier. Bob souhaite trouver deux billes dont la différence des numéros est un multiple de 7. Combien de billes doit-il piocher au minimum pour être sûr de remplir son objectif, quels que soient les numéros choisis par Alice au départ ?

Solution de l'exercice 3

Un tableau de congruence modulo 7 montre que le carré d'un entier ne peut prendre que les valeurs 0, 1, 2 ou 4 modulo 7. Ainsi, si Bob pioche 5 billes, il en aura deux qui ont le même reste modulo 7, d'après le principe des tiroirs. La différence des numéros de ces deux billes sera donc bien un multiple de 7. A l'inverse, s'il ne pioche que 4 billes, il pourrait avoir une bille portant un numéro congru à 0 modulo 7, une portant un numéro congru à 1, une portant un numéro congru à 2 et une portant un numéro congru à 4, si bien qu'il ne remplirait pas son objectif. Ainsi, Bob doit piocher 5 billes.

Commentaire des correcteurs : L'exercice est très bien réussi. Néanmoins, il y a pas mal de confusions sur le principe des tiroirs. Comme il y a 4 carrés modulo 7, le principe des tiroirs assure que si on prend 5 boules, alors deux auront la même congruence modulo 7. Par contre, il faudrait expliquer pourquoi prendre 4 boules n'assure pas de pouvoir avoir deux fois la même congruence modulo 7 (en donnant un contre-exemple).

Exercice 4. Trouver tous les couples (a, b) d'entiers naturels tels que :

$$ab + 85 = 12 \cdot \text{ppcm}(a, b) + 20 \cdot \text{pgcd}(a, b)$$

Solution de l'exercice 4

On utilise la relation $\text{ppcm}(a, b) \cdot \text{pgcd}(a, b) = ab$. Soient $p = \text{ppcm}(a, b)$ et $q = \text{pgcd}(a, b)$. En substituant dans l'équation initiale, on se ramène à :

$$pq + 85 = 12p + 20q$$

On peut factoriser cette équation sous la forme :

$$(p - 20)(q - 12) = 155 = 5 \cdot 31$$

Puisque 5 et 31 sont des nombres premiers, on a mis en évidence que les seuls diviseurs de 155 sont $1, 5, 31$ et 155. Ainsi, les nombres $p - 20$ et $q - 12$ appartiennent à l'ensemble $\{\pm 1, \pm 5, \pm 31, \pm 155\}$. On a alors 8 cas à traiter :

$$\underline{\text{Cas 1}} : \begin{cases} p - 20 = 1 \\ q - 12 = 155 \end{cases} \iff \begin{cases} p = 21 \\ q = 167 \end{cases}$$

$$\underline{\text{Cas 2}} : \begin{cases} p - 20 = 5 \\ q - 12 = 31 \end{cases} \iff \begin{cases} p = 25 \\ q = 43 \end{cases}$$

$$\underline{\text{Cas 3}} : \begin{cases} p - 20 = 31 \\ q - 12 = 5 \end{cases} \iff \begin{cases} p = 51 \\ q = 17 \end{cases}$$

$$\underline{\text{Cas 4}} : \begin{cases} p - 20 = 155 \\ q - 12 = 1 \end{cases} \iff \begin{cases} p = 175 \\ q = 13 \end{cases}$$

$$\underline{\text{Cas 5}} : \begin{cases} p - 20 = -1 \\ q - 12 = -155 \end{cases} \iff \begin{cases} p = 19 \\ q = -143 \end{cases}$$

$$\underline{\text{Cas 6}} : \begin{cases} p - 20 = -5 \\ q - 12 = -31 \end{cases} \iff \begin{cases} p = 15 \\ q = -19 \end{cases}$$

$$\underline{\text{Cas 7}} : \begin{cases} p - 20 = -31 \\ q - 12 = -5 \end{cases} \iff \begin{cases} p = -11 \\ q = 7 \end{cases}$$

$$\underline{\text{Cas 8}} : \begin{cases} p - 20 = -155 \\ q - 12 = -1 \end{cases} \iff \begin{cases} p = -135 \\ q = 11 \end{cases}$$

Ici il faut faire attention à ne pas aller trop vite en besogne et à bien vérifier lesquelles de ces solutions fonctionnent. Les 4 derniers cas ne peuvent pas fonctionner puisqu'ils fournissent des entiers négatifs comme solution. Pour les 4 premiers cas, on se rappelle que $p = \text{ppcm}(a, b)$ et $q = \text{pgcd}(a, b)$, ce qui implique que q doit diviser p. Cela n'est vérifié que dans le Cas 3. On a donc $p = 51 = 3 \cdot 17$ et $q = 17$.

On peut écrire a et b sous la forme $a = xq$ et $b = yq$ avec x et y des entiers naturels premiers entre eux par définition du pgcd. On sait de plus que $ab = pq$, soit $xyq^2 = pq$ donc $xyq = p$. En réinjectant les valeurs de p et q dans cette équation, on obtient $xy = 3$, donc $x = 1$ et $y = 3$ ou $x = 3$ et $y = 1$. Comme $a = 17x$ et $b = 17y$, on a donc deux solutions possibles : $(a, b) = (17, 51)$ ou $(a, b) = (51, 17)$. On vérifie alors réciproquement que ces deux solutions conviennent bien, puisque $17 \cdot 51 + 85 = 952 = 12 \cdot 51 + 20 \cdot 17$.

Commentaire des correcteurs : L'exercice est plutôt bien compris, néanmoins peu d'élèves ont la totalité des points. En effet, certains oublient de vérifier que les couples trouvés sont solutions. D'autres obtiennent que $(\mathtt{ppcm}(a,b)-20)(\mathtt{pgcd}(a,b)-12)=155$, mais ne pensent pas à prendre en compte le fait que $\mathtt{ppcm}(a,b)-20$ et $\mathtt{pgcd}(a,b)-12$ peuvent être tous deux négatifs.

Exercice 5. Soit $n \in \mathbb{Z}$. Montrer qu'il n'existe qu'un nombre fini de couples (a, b) d'entiers tels que :

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

.

Solution de l'exercice 5
Pour montrer qu'il y a un nombre fini de solutions, on peut essayer de montrer que tous les a et b solutions sont plus petit qu'un certain nombre dépendant de n. En effet, supposons que l'on a trouvé un entier $C > 0$ tel que pour tout couple d'entiers (a, b) solution de l'équation, $|a|, |b| \leqslant C$. Alors on a au plus $2C + 1$ choix de a et $2C + 1$ choix de b pour former une solution, ce qui fait au plus $(2C + 1)^2$ couples solutions de l'équation et on aura donc montré que le nombre de solutions est fini.

On se met donc en quête d'un tel entier C.

Soient a et b des entiers solutions. Remarquons que $a^2 + ab + b^2 = (a - b)^2 + 3ab = (a + b)^2 - ab$.
Ainsi, comme $(a - b)^2 \geqslant 0$ et $(a + b)^2 \geqslant 0$, on a $a^2 + ab + b^2 \geqslant |ab|$.
Si $n < 0$, il n'y a donc pas de couple $(a, b) \in \mathbb{Z}^2$ tel que $a^2 + ab + b^2 = n$.
Si $n \geqslant 0$, les couples $(a, b) \in \mathbb{Z}^2$ avec $a^2 + ab + b^2 = n$ vérifient $|ab| \leqslant n$, donc $|a| \leqslant n$ et $|b| \leqslant n$.
On a donc montré que $C = n$ vérifiait la condition voulue.

Il y a donc toujours un nombre fini de solutions.

Solution alternative n°1
Dans la même veine que la solution précédente, on remarque que :

$$a^2 + b^2 + ab = \frac{a^2 + b^2 + a^2 + 2ab + b^2}{2} = \frac{a^2 + b^2 + (a + b)^2}{2}$$

On a donc que $2n = a^2 + b^2 + (a + b)^2 \geqslant a^2$ et de même $2n \geqslant b^2$. En particulier si $n < 0$, l'équation n'a pas de solutions.
Si $n \geqslant 0$, on a donc $|a| \leqslant \sqrt{2n}$ et $|b| \leqslant \sqrt{2n}$, donc a, b sont entre $-\sqrt{2n}$ et $+\sqrt{2n}$. Il y a donc un nombre fini de valeurs possibles pour a et b, donc un nombre fini de solutions de l'équation.

Commentaire des correcteurs : L'exercice est globalement réussi, mais certains utilisent que si k est un entier fixé, $k = ab$ a un nombre fini de couples d'entiers (a, b) solution. Ce résultat est vrai, sauf si $k = 0$: il fallait donc bien séparer le cas $ab = 0$ des autres cas.

Exercice 6. Trouver tous les triplets (x, y, z) d'entiers strictement positifs tels que :

$$1005^x + 2011^y = 1006^z$$

Solution de l'exercice 6

On peut commencer par étudier l'équation modulo un entier bien choisi. Un bon candidat serait l'un des entiers présent dans l'équation, afin d'obtenir une équation simplifiée.
Considérons par exemple cette équation modulo 1006 : on a $2011 \equiv 1005 \equiv -1[1006]$, donc $(-1)^x + (-1)^y \equiv 0[1006]$. Cela montre que x et y sont de parités opposées.

Une fois que l'on a regardé l'équation modulo les entiers présents dans l'équations, on peut chercher des modulos plus subtils. Pour simplifier l'équation, on peut utiliser un diviseur simple de l'un des entiers comme modulo. Un diviseur simple de 1006 est 2 par exemple, mais l'équation n'est pas très intéressante modulo 2. L'astuce est a lors de se placer dans le cas où $z \geqslant k$ pour un certain k, car alors 2^k divise 1006^z, et on peut espérer que l'équation modulo 2^k pour un entier k bien choisi soit intéressante.
Supposons ainsi que $z \geqslant 3$. On a alors $1006^z \equiv 0[8]$, donc $0 \equiv 1005^x + 2011^y \equiv (-3)^x + 3^y[8]$. Cela n'est le cas que lorsque x et y sont de même parité, ce qui est une contradiction. Ainsi, $z \leqslant 2$. On remarque alors que $2011^3 > 1006^2$ et $1005^3 > 1006^2$, donc $x \leqslant 2$ et $y \leqslant 2$.

On s'est ramené à traiter un nombre fini de cas particuliers. On se rappelle que les trois inconnues sont strictement positives. Si $z = 1$, $1005^x + 2011^y > 1005 + 2011 > 1006$, donc il n'y a pas de solutions. Si $z = 2$, on a nécessairement $y = 1$ car $2011^2 > 1006^2$, auquel cas $1005^x + 2011 = 1006^2$. On constate alors que $x = 2$ convient, puisque $1006^2 - 1005^2 = (1006 + 1005)(1006 - 1005) = 2011$. Finalement, la seule solution est $(x, y, z) = (2, 1, 2)$.

Commentaire des correcteurs : L'exercice est globalement bien réussi par ceux qui l'ont rendu.

Exercice 7. Soit $n \geqslant 3$ un entier naturel et soient $a_1, a_2, \ldots, a_n$, n entiers naturels premiers entre eux dans leur ensemble tels que $\mathrm{ppcm}(a_1, a_2, \ldots, a_n)$ divise $a_1 + a_2 + \ldots + a_n$. Montrer que le produit $a_1 \cdot a_2 \cdots a_n$ divise $(a_1 + a_2 + \ldots + a_n)^{n-2}$.

Solution de l'exercice 7

Nous allons démontrer que pour chaque nombre premier p divisant le produit $a_1 \cdot \ldots \cdot a_n$, la valuation $p-$adique de $a_1 \cdot \ldots \cdot a_n$ est inférieure ou égale à la valuation $p-$adique de l'entier $(a_1 + \ldots + a_n)^{n-2}$.

Dans la suite, on fixe p un nombre premier divisant $a_1 \cdot \ldots \cdot a_n$ et on note $\nu_p(a)$ la valuation $p-$adique de l'entier a.

Etant donné que pour tous entiers a, b, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, on trouve que $\nu_p((a_1 + \ldots + a_n)^{n-2}) = (n-2)\nu_p(a_1 + \ldots + a_n)$. D'autre part, on trouve aussi que $\nu_p(a_1 \cdot \ldots \cdot a_n) = \nu_p(a_1) + \ldots + \nu_p(a_n)$.

On exploite désormais l'hypothèse donnée par l'énoncé. Celle-ci se traduit par

$$\max_{1,\ldots,n}(\nu_p(a_i)) = \nu_p(\mathrm{ppcm}(a_1, \ldots a_n)) \leqslant \nu_p(a_1 + \ldots + a_n)$$

Le fait que les entiers a_i soient premiers entre eux dans leur ensemble signifie qu'il y a au plus $n-1$ entiers a_i divisibles par p. Supposons cependant qu'il y ait exactement $n-1$ entiers a_i qui soient divisibles par p et supposons, quitte à renuméroter les entiers, que p divise tous les a_i sauf a_n. Alors p ne peut diviser la somme $a_1 + \ldots + a_n$ car p divise $a_1 + \ldots + a_{n-1}$. Pourtant p divise $\mathrm{ppcm}(a_1, \ldots, a_n)$ qui lui-même divise $a_1 + \ldots + a_n$. On obtient donc une contradiction.

On déduit que p divise au plus $n-2$ entiers parmi $a_1, \ldots, a_n$ et on suppose, quitte à renuméroter les entiers, que p ne divise pas a_{n-1} et a_n. Alors

$$\begin{aligned}
\nu_p(a_1 \cdot \ldots \cdot a_n) &= \nu_p(a_1) + \ldots + \underbrace{\nu_p(a_{n-1})}_{=0} + \underbrace{\nu_p(a_n)}_{=0} \\
&\leqslant (n-2)\max_{1,\ldots,n}(\nu_p(a_i)) \\
&= (n-2)\nu_p(\mathrm{ppcm}(a_1, \ldots a_n)) \\
&\leqslant (n-2)\nu_p(a_1 + \ldots + a_n) \\
&= \nu_p((a_1 + \ldots + a_n)^{n-2})
\end{aligned}$$

ce qui est exactement l'inégalité voulue. Puisqu'elle est vraie pour tout nombre premier p, on a bien le résultat demandé.

Commentaire des correcteurs : L'exercice a été peu compris, et nombreux sont ceux qui ont fourni une solution fausse. Deux erreurs étaient possibles. La première est de croire que les a_i étaient deux à deux premiers entre eux et en déduire que $\mathrm{PPCM}(a_1, \ldots, a_n) = a_1 \times \ldots a_n$, ce qui est faux par exemple pour $n = 3$ et $a_1 = 2, a_2 = 3, a_3 = 6$. La deuxième erreur récurrente était d'invoquer que $\mathrm{PPCM}(a_1, \ldots, a_n) \times \mathrm{PGCD}(a_1, \ldots, a_n) = a_1 \times \cdots \times a_n$ ce qui implique que $\mathrm{PPCM}(a_1, \ldots, a_n) = a_1 \times \ldots a_n$: l'exemple précédent montre bien que ce n'est pas le cas. En fait l'égalité $\mathrm{PPCM}(a_1, \ldots, a_n) \times \mathrm{PGCD}(a_1, \ldots, a_n) = a_1 \times \cdots \times a_n$ est vraie pour $n = 2$, mais s'avère fausse si $n \geqslant 3$. Il existe une généralisation de cette identité qui est

$$\mathrm{PPCM}(a_1, \ldots, a_n) = \prod_{I \subset \{1,\ldots,n\}} \mathrm{PGCD}(a_i, i \in I)^{(-1)^{|I|}}$$

Mais cette formule, analogue à la formule du crible, est rarement, voire quasiment jamais, exploitable (et ne l'était pas ici). Attention à bien essayer de vérifier ses formules sur des cas particuliers : regarder quelques cas pour $n = 3$ aurait permis de se rendre compte de l'erreur commise. De plus, l'exercice devenait vraiment simple si on avait automatiquement $\mathrm{PPCM}(a_1, \ldots, a_n) = a_1 \times \cdots \times a_n$, trop simple pour le niveau d'un exercice 7 : revérifier sa preuve ou demander une explication éventuelle à son tuteur est alors une bonne idée pour s'assurer de ne pas avoir loupé quelque chose.

Exercice 8. Déterminer tous les couples (m, n) d'entiers strictement positifs tels que :

$$125 \times 2^n - 3^m = 271$$

Solution de l'exercice 8
125 étant un cube, il serait bien de prouver que n et m sont des multiples de 3 pour pouvoir factoriser le côté gauche de l'équation. Dans ce but, on regarde l'équation modulo un nombre premier congru à 1 modulo 3.
Regardons par exemple modulo 7. Les puissances de 3 modulo 7 valent $1, 3, 2, 6, 4, 5, 1$ et celles de 2 valent $1, 2, 4, 1$. Or $271 \equiv 5$ modulo 7 et $125 \equiv -1$. Les seules possibilités sont donc d'avoir la puissance de 2 valant 1 et celle de 3 valant 1 ou la puissance de 2 valant 4 et celle de 3 valant 5. Ainsi, on a $n \equiv 0 \pmod 3$ et $m \equiv 0 \pmod 6$ ou $n \equiv 2 \pmod 3$ et $m \equiv 5 \pmod 6$. Si on arrive à exclure la deuxième possibilité, on a bien m, n divisibles par 3. Notons qu'on a forcément $n \geqslant 2$ car $250 < 271$. En regardant modulo 4, on a $3^m \equiv 1$ donc m est pair, on ne peut donc pas avoir $m \equiv 5 \pmod 6$. La deuxième possibilité est donc exclue et les entiers m et n sont divisibles par 3.

On pose $m = 3k$, $n = 3\ell$. L'équation devient

$$271 = (5 \times 2^k)^3 - (3^\ell)^3 = (5 \times 2^k - 3^\ell)(25 \times 2^{2k} + 5 \times 2^{k+1} \times 3^l + 3^{2\ell})$$

Or 271 est premier et comme $(25 \times 2^{2k} + 5 \times 2^{k+1} \times 3^\ell + 3^{2\ell})$ est positif et strictement supérieur à $(5 \times 2^k - 3^\ell)$, on a $5 \times 2^k - 3^\ell = 1$. Si $k \geqslant 3$, on a $3^\ell \equiv -1 \pmod 8$ ce qui n'est pas possible car 3^ℓ vaut 1 ou 3 modulo 8. On obtient donc $k = 0, 1, 2$. Pour $k = 0$, on obtient $3^\ell = 4$ ce qui est bien sûr impossible. Pour $k = 2$, on obtient $3^\ell = 19$ qui est également impossible. Pour $k = 1$, on obtient $3^\ell = 9$ donc $\ell = 2$ donc $(n, m) = (3, 6)$.
Réciproquement $125 \times 2^3 - 3^6 = 1000 - 729 = 271$ donc $(3, 6)$ est bien solution.

La seule solution de l'équation est donc le couple $(3, 6)$.

Solution alternative n°1
En regardant l'équation modulo 5, on trouve que $-3^m \equiv 1 \pmod 5$ donc que $3^m \equiv -1 \pmod 5$. Or l'ordre de 3 modulo 5 est 4 et les puissances alternent entre $1, 3, -1, -2$. On en déduit que $m \equiv 2 \pmod 4$.
Supposons que $n \geqslant 4$. Alors en regardant l'équation modulo 16, on a $-3^m \equiv 271 \equiv -1 \pmod{16}$ donc $3^m \equiv 1 \pmod{16}$. Or l'ordre de 3 modulo 16 vaut 4, puisque $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 11$ et $3^4 \equiv 1 \pmod{16}$. On a donc forcément $m \equiv 0 \pmod 4$ ce qui contredit l'hypothèse précédente.
On a donc $n < 4$.

- Si $n = 3$, l'équation est équivalente à $729 = 3^m$. Or $729 = 3^6$, donc l'équation donne $m = 6$. On trouve que le couple $(6, 3)$ est solution.
- Si $n = 2$, on obtient $3^m = 229$ qui n'est pas divisible par 3, contradiction.
- Si $n = 1$, $3^m = 250 - 271 < 0$ ce qui est impossible.

Ainsi l'unique solution est $(m, n) = (6, 3)$.

Commentaire des correcteurs : L'exercice a été peu traité, mais les copies rendues sont majoritairement excellentes. Attention néanmoins à être rigoureux sur les justifications. Certains élèves obtiennent qu'un produit de deux facteurs vaut 271, qui est premier, et déduisent directement que le premier facteur vaut 271 et le second facteur vaut 1 : pour obtenir cela, il faut justifier que les deux termes sont positifs, et que le premier est plus grand que le second.

Exercice 9. Trouver tous les triplets (m, n, p) d'entiers strictement positifs, avec p premier, tels que :

$$(m^3 + n)(n^3 + m) = p^3$$

Solution de l'exercice 9

Commençons par remarquer que si $m = n$, $p^3 = (m^3 + m)^2$ est un carré parfait, ce qui est impossible. On peut donc supposer sans perte de généralité que $m > n$. On sait alors que $m^3 + n > n^3 + m > 1$. Comme les deux seules manières de décomposer p^3 comme produit de deux entiers positifs sont $p^2 \cdot p$ et $p^3 \cdot 1$, on a ici $m^3 + n = p^2$ et $n^3 + m = p$. Dès lors, on peut remplacer m par $p - n^3$ dans la première équation, pour obtenir :

$$(p - n^3)^3 + n = p^2$$

En regardant cette équation modulo p, on obtient $-n^9 + n \equiv 0[p]$, donc p divise

$$n^9 - n = n(n - 1)(n + 1)(n^2 + 1)(n^4 + 1)$$

Or $p = n^3 + m > n^3$, donc p ne peut pas diviser n, $n + 1$ ou $n^2 + 1$. On distingue donc deux cas.

Cas 1 : p divise $n - 1$

L'inégalité $p > n^3 > n - 1$ implique alors que $n = 1$. Dans ce cas, $m^3 + 1 = p^2 = (m + 1)^2$, donc $m^3 - m^2 - 2m = 0$, ce qui se factorise en $m(m + 1)(m - 2) = 0$. La seule solution est donc pour $m = 2$, ce qui donne le triplet $(2, 1, 3)$.

Cas 2 : p divise $n^4 + 1$

Dans ce cas, comme $p = n^3 + m$, p divise également la combinaison linéaire $n(n^3 + m) - (n^4 + 1) = mn - 1$. Mais alors on remarque que

$$p^3 = (m^3 + n)(n^3 + m) > m^3 n^3$$

Ainsi $p > mn > mn - 1$, donc $mn - 1 = 0$. Cela donne $m = n = 1$, donc $p^3 = 4$ ce qui est absurde. Finalement, la seule solution est celle trouvée au Cas 1, à savoir $(2, 1, 3)$, et on vérifie qu'elle convient bien.

Commentaire des correcteurs : Peu d'élèves ont rendu le problème mais les quelques copies qui l'ont trouvé proposent des solutions très diverses. Certains ont réussi, sans conclure, à apporter de nombreux éléments utiles à la résolution : c'est une bonne idée de s'entraîner à rédiger des éléments de solutions partiels, puisqu'un jour de test c'est ce qu'il faudra faire sur tous les exercices non résolus.

Exercices Seniors

Exercice 10. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ tels que n divise $a - b$. Montrer que n^2 divise $a^n - b^n$.

Solution de l'exercice 10
On factorise l'entier $a^n - b^n$ sous la forme

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$$

Puisque n divise $a - b$, on a $a \equiv b \pmod{n}$. Aisni

$$a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1} \equiv b^{n-1} + \ldots + b^{n-1} \equiv nb^{n-1} \equiv 0[n]$$

Si bien que n divise les deux facteurs du produit, et donc $n^2 \mid a^n - b^n$.

Commentaire des correcteurs : Beaucoup de très bonnes solutions. Nous notons quelques cas d'utilisations du lemme LTE, mais quasi-toutes incomplètes ou frauduleuses (appliquer le lemme LTE demande de vérifier des hypothèses !). Il est également bon de se demander s'il est pertinent d'invoquer un résultat aussi technique sur un exercice élémentaire. Quitte à connaître un tel résultat et à y voir un lien avec l'exercice, autant se demander si les éléments de la preuve du lemme LTE ne sont pas plus instructifs pour étudier l'exercice que le résultat donné par le lemme.

Exercice 11. Soit x un réel positif ou nul tel que x^2 et x^3 sont tous les deux des entiers. Montrer que x est entier.

Solution de l'exercice 11

Si $x = 0$, il est entier. Supposons donc $x > 0$. Alors $x = \dfrac{x^3}{x^2}$ est rationnel comme quotient de deux entiers. Ainsi, x est rationnel et x^2 est entier. Posons $x = \dfrac{a}{b}$, où a et b sont des entiers strictement positifs. Alors $a^2 = x^2 b^2$, donc $b^2 \mid a^2$. Il reste à en déduire que $b \mid a$.

Soit p un nombre premier. Si $k \geqslant 1$, on note $v_p(k)$ la valuation p-adique de k. Alors $2v_p(b) = v_p(b^2) \leqslant v_p(a^2) = 2v_p(a)$. Ainsi $v_p(b) \leqslant v_p(a)$. Cette inégalité étant vraie pour tout nombre premier p, on a bien $b \mid a$. Par conséquent, x est entier.

Commentaire des correcteurs : Quasiment que des preuves correctes. Attention seulement à ne pas considérer $v_p(x)$ avant d'avoir montré que x est rationnel.

Exercice 12. Soit $n \geqslant 3$ un entier naturel et soient $a_1, a_2, \ldots, a_n$, n entiers naturels premiers entre eux dans leur ensemble tels que $\mathrm{ppcm}(a_1, a_2, \ldots, a_n)$ divise $a_1 + a_2 + \ldots + a_n$. Montrer que le produit $a_1 \cdot a_2 \cdots a_n$ divise $(a_1 + a_2 + \ldots + a_n)^{n-2}$.

Solution de l'exercice 12

Nous allons démontrer que pour chaque nombre premier p divisant le produit $a_1 \cdot \ldots \cdot a_n$, la valuation $p-$adique de $a_1 \cdot \ldots \cdot a_n$ est inférieure ou égale à la valuation $p-$adique de l'entier $(a_1 + \ldots + a_n)^{n-2}$.

Dans la suite, on fixe p un nombre premier divisant $a_1 \cdot \ldots \cdot a_n$ et on note $\nu_p(a)$ la valuation $p-$adique de l'entier a.

Etant donné que pour tous entiers a, b, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, on trouve que $\nu_p((a_1 + \ldots + a_n)^{n-2}) = (n-2)\nu_p(a_1 + \ldots + a_n)$. D'autre part, on trouve aussi que $\nu_p(a_1 \cdot \ldots \cdot a_n) = \nu_p(a_1) + \ldots + \nu_p(a_n)$.

On exploite désormais l'hypothèse donnée par l'énoncé. Celle-ci se traduit par

$$\max_{1,\ldots,n}(\nu_p(a_i)) = \nu_p(\mathrm{ppcm}(a_1, \ldots a_n)) \leqslant \nu_p(a_1 + \ldots + a_n)$$

Le fait que les entiers a_i soient premiers entre eux dans leur ensemble signifie qu'il y a au plus $n-1$ entiers a_i divisibles par p. Supposons cependant qu'il y ait exactement $n-1$ entiers a_i qui soient divisibles par p et supposons, quitte à renuméroter les entiers, que p divise tous les a_i sauf a_n. Alors p ne peut diviser la somme $a_1 + \ldots + a_n$ car p divise $a_1 + \ldots + a_{n-1}$. Pourtant p divise $\mathrm{ppcm}(a_1, \ldots, a_n)$ qui lui-même divise $a_1 + \ldots + a_n$. On obtient donc une contradiction.

On déduit que p divise au plus $n-2$ entiers parmi $a_1, \ldots, a_n$ et on suppose, quitte à renuméroter les entiers, que p ne divise pas a_{n-1} et a_n. Alors

$$\begin{aligned}
\nu_p(a_1 \cdot \ldots \cdot a_n) &= \nu_p(a_1) + \ldots + \underbrace{\nu_p(a_{n-1})}_{=0} + \underbrace{\nu_p(a_n)}_{=0} \\
&\leqslant (n-2)\max_{1,\ldots,n}(\nu_p(a_i)) \\
&= (n-2)\nu_p(\mathrm{ppcm}(a_1, \ldots a_n)) \\
&\leqslant (n-2)\nu_p(a_1 + \ldots + a_n) \\
&= \nu_p((a_1 + \ldots + a_n)^{n-2})
\end{aligned}$$

ce qui est exactement l'inégalité voulue. Puisqu'elle est vraie pour tout nombre premier p, on a bien le résultat demandé.

Commentaire des correcteurs : L'exercice est bien résolu dans l'ensemble et une grande partie des élèves a montré une bonne maitrise de la notion de valuation $p-$adique. Une partie non négligeable des élèves a confondu les notions de "nombres premiers entre eux deux à deux" et "nombres premiers entre eux dans leur ensemble". La première définition implique, comme beaucoup l'ont pensé, que $\mathrm{PPCM}(a_1, \ldots, a_n) = a_1 \ldots a_n$. En revanche, cette égalité n'est pas vraie dans le seoncd cas. De même, la relation $\mathrm{PPCM}(a_1, \ldots, a_n) \cdot \mathrm{PGCD}(a_1, \ldots, a_n) = a_1 \ldots a_n$ n'est vraie dans le cas général que si $n = 2$.

Exercice 13. Alice et Bob jouent avec un jeu de 2020 cartes. Sur chaque carte est écrit un des entiers de 1 à 2020 (chaque entier apparaît sur exactement une carte). Alice commence en retirant du paquet une carte de son choix, portant le numéro a. Bob voit la carte qu'Alice a choisie, et décide de retirer la carte portant le numéro b. Puis Bob écrit sur un tableau un des deux polynômes $x^2 - ax + b$ ou $x^2 - bx + a$ au choix. La partie continue ainsi jusqu'à ce qu'il n'y ait plus de cartes. A la fin de la partie, Bob gagne si tous les polynômes qu'il a écrits possèdent une racine entière, sinon Alice gagne. Montrer que Bob possède une stratégie gagnante.

Solution de l'exercice 13

Il s'agit, pour Bob, de s'assurer que pour chaque entier a choisi par Alice, il existe un entier b écrit sur l'une des cartes encore dans le paquet tel que l'un des deux polynômes $x^2 - ax + b$ ou $x^2 - bx + a$ possède une racine. La façon la plus simple de procéder est donc pour Bob de créer des paires disjointes d'entiers (a, b) avec les entiers de 1 à 2010, telles que pour chaque paire, l'un des polynômes autorisés possède une racine.

Bob va par exemple regrouper les entiers de 1 à 2020 en 1010 paires de la forme $(2n - 1, 2n)$, pour n allant de 1 à 1010. Chaque fois qu'Alice retire une carte appartenant à une paire, Bob retire l'autre carte de la paire. Les deux nombres a et b seront alors toujours de la forme $2n - 1, 2n$. Bob peut donc écrire le polynôme $x^2 - (2n)x + (2n - 1)$ qui se factorise en $(x - 1)(x - (2n - 1))$. Bob s'assure ainsi que tous ses polynômes aient bien une racine entière.

Commentaire des correcteurs : L'exercice est très bien résolu. Attention toutefois à la façon de raconter une stratégie gagnante. Il ne suffit pas de montrer que Bob peut jouer un nombre souhaitable à chaque tour, il faut également démontrer que l'entier que Bob doit jouer n'a pas déjà été utilisé ! Cet oubli a été retrouvé chez plusieurs élèves qui avaient pourtant la bonne stratégie. Même si la justification peut paraître évidente, il est nécessaire de la mentionner ! D'autres élèves voient leur stratégie s'effondrer justement parce qu'ils ne peuvent pas s'assurer que Bob pourra toujours jouer l'entier prévu par la stratégie.

Exercice 14. Trouver tous les triplets d'entiers strictement positifs (m, n, p), avec p premier, tels que :

$$(m^3 + n)(n^3 + m) = p^3$$

Solution de l'exercice 14

Commençons par remarquer que si $m = n$, $p^3 = (m^3 + m)^2$ est un carré parfait, ce qui est impossible. On peut donc supposer sans perte de généralité que $m > n$. On sait alors que $m^3 + n > n^3 + m > 1$. Comme les deux seules manières de décomposer p^3 comme produit de deux entiers positifs sont $p^2 \cdot p$ et $p^3 \cdot 1$, on a ici $m^3 + n = p^2$ et $n^3 + m = p$. Dès lors, on peut remplacer m par $p - n^3$ dans la première équation, pour obtenir :

$$(p - n^3)^3 + n = p^2$$

En regardant cette équation modulo p, on obtient $-n^9 + n \equiv 0[p]$, donc p divise

$$n^9 - n = n(n - 1)(n + 1)(n^2 + 1)(n^4 + 1)$$

Or $p = n^3 + m > n^3$, donc p ne peut pas diviser n, $n + 1$ ou $n^2 + 1$. On distingue donc deux cas.

Cas 1 : p divise $n - 1$

L'inégalité $p > n^3 > n - 1$ implique alors que $n = 1$. Dans ce cas, $m^3 + 1 = p^2 = (m + 1)^2$, donc $m^3 - m^2 - 2m = 0$, ce qui se factorise en $m(m + 1)(m - 2) = 0$. La seule solution est donc pour $m = 2$, ce qui donne le triplet $(2, 1, 3)$.

Cas 2 : p divise $n^4 + 1$

Dans ce cas, comme $p = n^3 + m$, p divise également la combinaison linéaire $n(n^3 + m) - (n^4 + 1) = mn - 1$. Mais alors on remarque que

$$p^3 = (m^3 + n)(n^3 + m) > m^3 n^3$$

Ainsi $p > mn > mn - 1$, donc $mn - 1 = 0$. Cela donne $m = n = 1$, donc $p^3 = 4$ ce qui est absurde. Finalement, la seule solution est celle trouvée au Cas 1, à savoir $(2, 1, 3)$, et on vérifie qu'elle convient bien.

Commentaire des correcteurs : L'exercice a été abordé par beaucoup d'élèves mais finalement assez peu en viennent à bout. Il nécessitait de combiner des raisonnements de nature purement arithmétique et des raisonnements par comparaison d'entiers. La plupart des élèves ayant rendu une tentative fournissent des éléments allant dans l'un de ces deux sens et se rapprochent significativement de la solution.

Plusieurs élèves éliminent dès le départ le cas où l'un des facteurs peut valoir 1. Si ce cas est effectivement impossible et la justification très courte, il faut tout de même l'envisager et justifier un minimum pourquoi il est impossible. Il est dommage de perdre des points à cause d'une rédaction trop économique. Le même problème se pose lorsque les élèves obtiennent l'équation $(m - n)(m^2 + mn + n^2 - 1) = 0 \pmod p$ et déduisent immédiatement que $m^2 + mn + n^2 - 1 \pmod p$ sans justifier que l'on ne pas avoir $m = n \pmod p$.

Exercice 15. Déterminer s'il existe une suite infinie $(a_n)_{n\in\mathbb{N}}$ d'entiers strictement positifs vérifiant les deux propriétés suivantes :

1. Tout entier strictement positif apparaît exactement une fois dans la suite ;
2. Pour tout entier $n \geqslant 1$, $\prod_{i=1}^{n} a_i$ s'écrit comme puissance $n-$ième d'un entier.

Solution de l'exercice 15

Pour deviner la réponse à une question ouverte de cette façon, il est essentiel d'essayer de construire les premiers termes d'une telle suite. Après quelques essais, on peut ici se convaincre que la réponse est oui. Pour le montrer, nous allons construire une suite respectant les conditions de l'énoncé. Le plus simple est de construire successivement les termes de la suite par récurrence.

On peut choisir comme premiers termes $a_1 = 1$, $a_2 = 4$, $a_3 = 2$, qui satisfont bien la deuxième condition. On procède ensuite par récurrence en supposant que tous les entiers de 1 à $n-1$ apparaissent une unique fois dans la suite avant le rang $\ell - 1$, pour lequel $a_{\ell-1} = n-1$, et que les entiers $a_1, \dots a_{\ell-1}$ satisfont bien sûr la deuxième hypothèse de l'énoncé. On veut alors faire apparaître à son tour l'entier n dans la suite. Si l'entier n apparaît avant le rang ℓ, il n'y a rien à faire. On suppose désormais que l'entier n n'apparaît pas avant le rang ℓ.
L'idée consiste à choisir astucieusement le terme a_ℓ afin de pouvoir prendre $a_{\ell+1} = n$ tout en satisfaisant la deuxième hypothèse de l'énoncé.

On note $(p_i)_{i\geqslant 1}$ la liste ordonnée des nombres premiers ($p_1 = 2, p_2 = 3,$ etc.). On pose $n = \prod_{i\geqslant 1} p_i^{\alpha_i}$ (avec $\alpha_i = 0$ si p_i ne divise pas n). On appelle $N = a_1 \cdot a_2 \cdots a_{\ell-1}$, et on rappelle qu'il s'agit d'une puissance $(\ell-1)-$ème. On peut donc écrire $N = \prod_{i\geqslant 1} p_i^{(\ell-1)\beta_i}$. Le théorème des restes chinois nous permet d'affirmer, pour tout i, l'existence d'un γ_i tel que ;

$$\gamma_i + (\ell-1)\beta_i \equiv 0[\ell]$$
$$\gamma_i + (\ell-1)\beta_i + \alpha_i \equiv 0[\ell+1]$$

On peut alors avoir $a_{\ell+1} = n$ comme on le voulait en posant $a_l = \prod_{i\geqslant 1} p_i^{\gamma_i}$ et en choisissant les γ_i de sorte que ce nombre ne soit pas déjà apparu dans la suite, ce qui est bien possible puisqu'il y a une infinité de choix possibles. On s'est alors assurer que $a_1 \cdot a_2 \cdots a_\ell$ est bien une puissance $\ell-$ième et que $a_1 \cdot a_2 \cdots a_{\ell+1}$ est une puissance $(\ell+1)-$ième, puisque tous les exposants dans la décomposition en facteurs premiers sont respectivement multiples de ℓ et de $\ell+1$. Ceci achève la récurrence et conclut l'exercice.

Commentaire des correcteurs : L'exercice est bien résolu ! Les élèves ont bien établi le cahier des charges pour pouvoir placer l'entier N dans la suite.

Exercice 16. Montrer qu'il existe un entier $n < 10^6$ tel que l'écriture décimale de 5^n comporte au moins 6 zéros consécutifs.

Solution de l'exercice 16 La difficulté de cet exercice réside dans la construction de l'entier n. On peut se demander d'abord où apparaîtront les zéros dans l'écriture de 5^n. Si l'on veut éviter d'avoir à trouver de bonnes estimations de $\log_{10} 5$ par des rationnels de petit dénominateur, ce qui ne s'avère pas très élégant, il faut éviter de chercher des zéros en début d'écriture décimale. Par ailleurs, il est clair que 5^n ne se terminera jamais par un zéro. A partir de là, on pourrait espérer avoir des zéros parmi les derniers chiffres.

L'idée est de remarquer que si $k \geqslant 1$ est fixé, alors pour tout $n > k$, on a $5^n \equiv 5^k \pmod{5^k}$. Donc pour que $5^n - 5^k$ se termine par k zéros, il suffit que $5^n \equiv 5^k \pmod{2^k}$. Comme $\varphi(2^k) = 2^{k-1}$, c'est le cas dès que $n \equiv k \pmod{2^{k-1}}$. Et dans ce cas, pourvu que 5^k s'écrive avec strictement moins de k chiffres, il restera des zéros consécutifs parmi les k derniers chiffres de 5^n.

Plus précisément, considérons l'entier $n = 20 + 2^{19} = 524308 < 10^6$. Clairement $5^n \equiv 5^{20} \pmod{5^{20}}$, et $5^n \equiv 5^{20} \pmod{2^{20}}$ puisque $\varphi(2^{20}) = 2^{19}$. Ainsi, l'entier $5^n - 5^{20}$ est divisible par 10^{20} et donc termine par au moins 20 zéros. Puisque

$$5^{10} = \frac{10^{10}}{2^{10}} < \frac{10^{10}}{10^3} = 10^7$$

on a $5^{20} < 10^{14}$. Ainsi, 5^{20} a au plus 14 chiffres, donc les 20 derniers chiffres de $5^n = (5^n - 5^{20}) + 5^{20}$ commencent par une série de 6 zéros consécutifs.

Commentaire des correcteurs : Ce problème était assez difficile et astucieux, et très peu d'élèves ont rendu une tentative de solution. Cependant, parmi ceux qui ont rendu une solution, un très grand nombre a fourni une solution (quasi-)complète. En complément de la solution $n = 2^{19} + 20$ donnée dans le corrigé, certains élèves ont prouvé que $n = 2^{19} + 21$ et $n = 2^{18} + 20$ convenaient aussi, avec le même type de raisonnement. Voici quelques remarques générales :

- Il se trouve qu'un programme informatique (en Python par exemple) permet de voir facilement que $n = 3375$ est aussi solution. Cependant, il n'y a très vraisemblablement pas de preuve mathématique simple de ce fait. Les quelques copies qui mentionnaient cette solution sans justification n'ont donc pas obtenu de point.
- D'autres élèves ont imaginé qu'il était possible de prendre n négatif assez petit pour que 5^n soit strictement inférieur à 10^{-6}, et donc commence en écriture décimale par 6 zéros consécutifs. L'énoncé était effectivement imprécis à ce sujet, mais dans un exercice de théorie des nombres à cette position dans l'envoi, les élèves auraient pu déduire qu'il s'agissait uniquement des entiers naturels...
- Plusieurs élèves ont utilisé le lemme LTE dans le cas particulier $p = 2$ pour estimer $v_2(5^n - 1)$ où $n \geqslant 1$. Soulignons qu'ici, on a bien $v_2(5^n - 1) = 2 + v_2(n)$, mais rappelons que pour ce cas $p = 2$, en général, si x et y sont deux entiers impairs, on a $v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1$.
- Enfin, nous attendions que les élèves justifient précisément les inégalités invoquées concernant les puissances de 2, 5 ou 10 utilisées. En particulier, tous les élèves qui ont visiblement fait usage de leur calculatrice pour voir par exemple que 5^20 a au plus 14 chiffres ont perdu un point.

Exercice 17. Montrez qu'il existe un entier naturel N, tel que pour tout entier $n \geqslant N$, il existe $a_1, a_2, \ldots, a_{2020}$ des entiers satisfaisant les conditions :

— $n = a_1 + a_2 + \ldots + a_{2020}$;
— $a_{2020} > a_{2019} > \ldots > a_1 \geqslant 1$;
— Pour tout $1 \leqslant i \leqslant 2019$, a_i divise a_{i+1}.

Solution de l'exercice 17

On se doute que l'énoncé n'est pas seulement vrai pour le nombre 2020 et on peut donc essayer de montrer le résultat pour tous les entiers k. Le caractère héréditaire de l'énoncé nous encourage même à montrer le résultat par récurrence sur k. Il s'agit donc de montrer que pour tout entier k, il existe un entier naturel N_k tel que pour tout entier $n \geqslant N_k$, il existe $a_1, \ldots, a_k$ des entiers satisfaisant les conditions :

— $n = a_1 + \ldots + a_k$;
— $a_k > a_{k-1} > \ldots > a_1$;
— Pour tout $1 \leqslant i \leqslant k-1$, $a_i \mid a_{i+1}$

Si $k = 1$, pour un entier $n \geqslant 1$, l'entier $a_1 = n$ satisfait les trois conditions.

Dans la suite, on appellera rang associé à ℓ un entier N_ℓ vérifiant que si $n \geqslant N_\ell$, il existe ℓ entiers vérifiant les trois propriétés.
On suppose donc que l'énoncé est vrai pour un certain entier k.
Il s'agit désormais de trouver un rang N_{k+1} associé à $k+1$ en fonction du rang N_k associé à a_k.
Soit donc n un entier assez grand dans un sens que l'on cherchera à préciser par la suite. On l'écrit sous la forme $n = (2m+1)2^{2t+r} = 2^r(2m+1)2^{2t}$, avec $r \in \{0, 1\}$, m et t des entiers naturels, et on distingue deux cas :

Cas 1 : $m \geqslant N_k$
Par hypothèse, on peut écrire $m = a_1 + a_2 + \ldots + a_k$ où les a_i vérifient les conditions attendues. On a alors :

$$n = 2^{2t+r}(1 + 2m) = 2^{2t+r} + 2^{2t+r+1}a_1 + 2^{2t+r+1}a_2 + \ldots + 2^{2t+r+1}a_k$$

On a obtenu une décomposition de n comme somme de $k+1$ entiers, et on montre qu'elle vérifie bien les hypothèses. On a bien $2^{2t+r} \geqslant 1$, et 2^{2t+r} divise $2^{2t+r+1}a_1$. Les autres conditions sont satisfaites par hypothèse de récurrence. Ainsi, on a bien une décomposition sous la forme voulue dans ce cas.

Cas 2 : $2^t \geqslant N_k$
Cette fois, on écrit $2^t + 1 = a_1 + a_2 + \ldots + a_k$, où les a_i vérifient à nouveau les conditions voulues. On trouve d'abord une décomposition de 2^{2t} comme suit :

$$2^{2t} = 1+(2^t-1)(2^t+1) = 1+(2^t-1)(a_1+a_2+\ldots+a_k) = 1+(2^t-1)a_1+(2^t-1)a_2+\ldots+(2^t-1)a_k$$

On vérifie que cette décomposition en $k+1$ éléments de 2^{2t} vérifie les trois hypothèses. On en déduit alors une décomposition de n, en multipliant l'équation ci-dessus par $2^r(2m+1)$, ce qui ne viole aucune des trois conditions, puisque $2^r(2m+1) \geqslant 1$ et que la multiplication par un même nombre positif ne change pas l'ordre ni les divisibilités.

Il reste donc à montrer qu'on peut trouver N_{k+1} suffisamment grand pour que tous les entiers supérieurs à N_{k+1} entrent dans l'un des deux cas précédents. On peut s'assurer de cela en posant $n_{k+1} = 4n_k^3$. En effet, si aucun des deux cas n'est vérifié pour un certain $\overline{n} = 2^{2t+r}(2m+1)$, alors $2^t < n_k$ et $m \leqslant n_k - 1$, donc :

$$\overline{n} = 2^{2t+r}(2m+1) \leqslant 2^r \cdot \left(2^t\right)^2 \cdot (2n_k - 1) < 2 \cdot n_k^2 \cdot 2n_k = 4n_k^3$$

Donc pour tout $n \geqslant 4n_k^3$, la propriété est vraie au rang $k+1$, ce qui achève la récurrence. Il ne reste plus qu'à choisir $N = n_{2019}$ pour conclure.

Commentaire des correcteurs : L'exercice a été bien résolu par les quelques élèves qui l'ont traité. Les élèves ont présenté des solutions diverses et variées au problème.

Exercice 18. Soit $a \geqslant 1$ un entier fixé. Montrer que l'ensemble des diviseurs premiers des nombres de la forme $2^{2^n} + a$ pour $n \in \mathbb{N}$ est infini.

Solution de l'exercice 18 Signalons pour commencer que cet exercice est en fait un cas particulier du théorème de Kobayashi, stipulant que si S est un ensemble d'entiers naturels non nuls, et si l'ensemble des nombres premiers divisant au moins l'un des éléments de S est fini, alors l'ensemble des nombres premiers divisant au moins l'un des éléments de $S + a$ est infini, dès que $a \neq 0$. On trouvera l'article original de 1981 de Hiroshi KOBAYASHI au lien suivant :
`https://projecteuclid.org/download/pdf_1/euclid.tjm/1270215162`.

Dans la suite de l'exercice, on adoptera les notations suivantes :

- si $b, n \geqslant 1$ sont deux entiers premiers entre eux, $\mathrm{ord}_n(b)$ désigne l'ordre de b modulo n
- si $n \geqslant 1$ et p est premier, $\nu_p(n)$ désigne la valuation p-adique de n

Commençons par prouver deux lemmes qui nous seront utiles.

Lemme 1. Soit $p \geqslant 3$ un nombre premier, et c, α des entiers strictement positifs avec c impair non divisible par p. Notons $\omega = \mathrm{ord}_p(2)$, et $b = \nu_p(2^\omega - 1) \geqslant 1$. Alors $\mathrm{ord}_{cp^\alpha}(2) = \mathrm{ppcm}(\mathrm{ord}_c(2), \omega p^{(\alpha-b)^+})$, où si $n \in \mathbb{Z}$, $n^+ = \max(n, 0)$ est la partie positive de n.

Preuve. Si $k \in \mathbb{N}$, on remarque que comme $p \nmid c$, $cp^\alpha \mid 2^k - 1$ si et seulement si $c \mid 2^k - 1$ et $p^\alpha \mid 2^k - 1$, c'est-à-dire si et seulement si $\mathrm{ord}_c(2) \mid k$ et $\mathrm{ord}_{p^\alpha}(2) \mid k$. Ainsi, on a déjà $\mathrm{ord}_{cp^\alpha}(2) = \mathrm{ppcm}(\mathrm{ord}_c(2), \mathrm{ord}_{p^\alpha}(2))$. Il suffit donc d'expliciter $\mathrm{ord}_{p^\alpha}(2)$.
Comme $\alpha \geqslant 1$, on a déjà $\omega = \mathrm{ord}_p(2) \mid \mathrm{ord}_{p^\alpha}(2)$. On cherche donc $k \geqslant 1$ minimum tel que $\nu_p(2^{k\omega} - 1) \geqslant \alpha$. Or, d'après le lemme LTE, on a pour tout $k \geqslant 1$, $\nu_p(2^{k\omega} - 1) = \nu_p(2^\omega - 1) + \nu_p(k) = b + \nu_p(k)$. Ainsi :

- si $\alpha \leqslant b$, le plus petit $k \geqslant 1$ tel que $\nu_p(2^{k\omega} - 1) \geqslant \alpha$ est $k = 1$ et $\mathrm{ord}_{p^\alpha}(2) = \omega$
- si $\alpha > b$, le plus petit $k \geqslant 1$ tel que $\nu_p(2^{k\omega} - 1) \geqslant \alpha$ est égal au plus petit $k \geqslant 1$ tel que $\nu_p(k) \geqslant \alpha - b$, c'est-à-dire $k = p^{\alpha-b}$. Et ainsi $\mathrm{ord}_{p^\alpha}(2) = \omega p^{\alpha-b}$, ce qui conclut la preuve de ce premier lemme.

Lemme 2. Soit $p \geqslant 3$ un nombre premier. Notons $\omega = \mathrm{ord}_p(2) = 2^\delta \gamma$, où $\delta \in \mathbb{N}$, et $\gamma \geqslant 1$ impair. Notons comme précédemment $b = \nu_p(2^\omega - 1)$.Soit n un entier supérieur à δ. Soit $\alpha \in \mathbb{N}$ tel que $p^\alpha \mid 2^{2^n} + a$. On suppose que $\alpha \geqslant 2b$. Alors le plus petit entier $k \geqslant 1$ tel que $p^\alpha \mid 2^{2^{n+k}} + a$ est $k_0 = \mathrm{ppcm}(\mathrm{ord}_\gamma(2), \omega p^{\alpha-2b})$.

Preuve. Soit $k \geqslant 1$ fixé. Alors $p^\alpha \mid 2^{2^{n+k}} + a$ si et seulement si $2^{2^n} \equiv 2^{2^{n+k}} \pmod{p^\alpha}$, c'est-à-dire si et seulement si $2^n \equiv 2^{n+k} \pmod{\mathrm{ord}_{p^\alpha}(2)}$. Comme $\alpha \geqslant b$ en particulier, on a par le lemme précédent, $\mathrm{ord}_{p^\alpha}(2) = \omega p^{\alpha-b} = 2^\delta \gamma p^{\alpha-b}$. Et comme $n \geqslant \delta$, la dernière congruence se produit si et seulement si $2^n \equiv 2^{n+k} \pmod{\gamma p^{\alpha-b}}$, c'est-à-dire si et seulement si $\mathrm{ord}_{\gamma p^{\alpha-b}}(2) \mid k$. On en déduit que le $k \geqslant 1$ minimum est $k_0 = \mathrm{ord}_{\gamma p^{\alpha-b}}(2)$.
Avant de réappliquer le lemme précédent, il faut vérifier que $p \nmid \gamma$, mais c'est vrai puisque $\gamma \leqslant \omega = \mathrm{ord}_p(2) \leqslant p - 1$ d'après le petit théorème de Fermat.
On a encore $\alpha - b \geqslant b$, de sorte que $k_0 = \mathrm{ord}_{\gamma p^{\alpha-b}}(2) = \mathrm{ppcm}(\mathrm{ord}_\gamma(2), \omega p^{\alpha-2b})$, ce qui conclut la preuve de ce second lemme.

On va résoudre l'exercice grâce au lemme 2. Pour $n \in \mathbb{N}$, on note $u_n = 2^{2^n} + a$. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers divisant l'un des u_n pour $n \in \mathbb{N}$, et notons-les $3 \leqslant p_1 < \ldots < p_r$ ($r \in \mathbb{N}$). Notons $d = \nu_2(a)$, et $n_0 \in \mathbb{N}$ minimum tel que $2^{n_0} > d$. Alors pour $n \geqslant n_0$, on a $\nu_2(u_n) = d$ et $u_n > 2^d$ donc u_n a au moins un diviseur premier impair et $r \geqslant 1$.

Pour $i \in [\![1, r]\!]$, notons comme dans le lemme 2, $\omega_i = \mathrm{ord}_{p_i}(2) = 2^{\delta_i}\gamma_i$, avec $\delta_i \in \mathbb{N}$ et γ_i impair. On note encore $b_i = \nu_{p_i}(2^{\omega_i} - 1) \geqslant 1$.
Soit $\alpha \geqslant 2\max(b_1, \ldots, b_r)$ à bien choisir, $n_1 = \max(n_0, \delta_1, \ldots, \delta_r)$, et $N(\alpha)$ le plus petit entier supérieur ou égal à n_1 tel que $u_{N(\alpha)} > 2^d(p_1 \ldots p_r)^{\alpha-1}$.
Soit $n \geqslant N(\alpha)$. Comme $n \geqslant n_0$, on a $\nu_2(n) = d$. Et comme $u_n > 2^d(p_1 \ldots p_r)^{\alpha-1}$, on sait qu'il existe $i \in [\![1, r]\!]$ tel que $p_i^\alpha \mid u_n$ (puisque u_n ne peut avoir par hypothèse comme diviseur premier impair que $p_1, \ldots, p_r$). Comme $n \geqslant \delta_i$ et $\alpha \geqslant 2b_i$, on a d'après le lemme 2 que le plus petit $k \geqslant 1$ tel que $p_i^\alpha \mid u_{n+k}$ est $\mathrm{ppcm}(\mathrm{ord}_{\gamma_i}(2), \omega_i p_i^{\alpha-2b_i})$. Et il se trouve qu'on a aussi :

$$\mathrm{ppcm}(\mathrm{ord}_{\gamma_i}(2), \omega_i p_i^{\alpha-2b_i}) \;\geqslant\; \omega_i p_i^{\alpha-2b_i} \;\geqslant\; p_i^{\alpha-2b_i} \;\geqslant\; 2^{\alpha-2b} \quad (*)$$

où $b = \max(b_1, \ldots, b_r)$. C'est une minoration uniforme qui ne dépend plus que de α.
On a presque fini ! Il ne reste plus qu'à choisir le bon α. On prend $\alpha_0 \geqslant 2b$ tel qu'on ait de plus

$$2^{\alpha_0-2b} \;>\; r \quad (**)$$

et on note $N = N(\alpha_0)$.
Rassemblons les morceaux. Il existe un entier $i_0 \in [\![1, r]\!]$ tel que $p_{i_0}^\alpha \mid u_N$, un entier $i_1 \in [\![1, r]\!]$ tel que $p_{i_1}^\alpha \mid u_{N+1}$, …, et il existe enfin un entier $i_r \in [\![1, r]\!]$ tel que $p_{i_r}^\alpha \mid u_{N+r}$. L'inégalité (*) et la condition (**) assurent que les $r+1$ entiers $i_0, \ldots i_r$ doivent être deux à deux distincts dans $[\![1, r]\!]$. On a ainsi obtenu une contradiction, ce qui achève la preuve.
Solution alternative n°1 On présente ici une solution plutôt astucieuse.
On suppose par l'absurde que l'ensemble des nombres premiers p divisant l'un au moins des $u_n = 2^{2^n} + a$ pour $n \in \mathbb{N}$ est fini. Notons les $2 \leqslant p_1 < \ldots < p_N$ où $N \geqslant 1$. Soit $r \geqslant 1$ un entier suffisamment grand pour qu'on ait :

$$\forall i \in [\![1, N]\!], \forall s \in [\![1, N]\!], p_i^r \nmid a^{2^s} + a$$

Posons $m = (p_1 \ldots p_N)^{r-1}$, et $n_0 \in \mathbb{N}$ tel que si $n \geqslant n_0$, on ait $u_n > m$. Un argument similaire à celui de la première solution montre que si $n \geqslant n_0$, on a $i(n) \in [\![1, N]\!]$ tel que $p_{i(n)}^r \mid u_n$. Par le principe des tiroirs, il existe $n \geqslant n_0$ et $s \in [\![1, N]\!]$ tels que $i(n) = i(n+s) = i \in [\![1, N]\!]$. Alors $p_i^r \mid u_n$ et $p_i^r \mid u_{n+s}$. Autrement dit, $2^{2^n} \equiv -a \pmod{p_i^r}$ et $2^{2^{n+s}} \equiv -a \pmod{p_i^r}$ aussi. Or $2^{2^{n+s}} = \left(2^{2^n}\right)^{2^s}$, de sorte que $(-a)^{2^s} \equiv -a \pmod{p_i^r}$. D'où, comme $s \geqslant 1$, $p_i^r \mid a^{2^s} + a$. Ceci fournit la contradiction et conclut.

Commentaire des correcteurs : Ce problème relativement difficile a été très bien réussi par les quelques élèves qui s'y sont penchés. Il y avait essentiellement deux types de solution : celle du corrigé (assez pédestre et simplifiable, utilisant des considérations sur l'ordre multiplicatif de 2 modulo des puissances de nombres premiers impairs) et une autre plus astucieuse, trouvée par quelques élèves. De manière générale, signalons quelques remarques :

- le nombre premier 2 jouant ici un rôle particulier, il est primordial de bien faire attention à le distinguer des nombres premiers impairs. Cela a plutôt bien été fait.
- il faut faire attention lorsqu'on veut manipuler et comparer des logarithmes dans des bases différentes. Typiquement, si $1 < a < b$ et $x > 1$ alors $\log_a(x) > \log_b(x)$
- s'il peut être intéressant de voir ce qu'impliqueraient certaines conjectures (typiquement ici celle des nombres premiers de Mersenne) dans le cadre d'un exercice, il ne faut jamais considérer avoir résolu le problème si l'argument principal n'est pas prouvé...