PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE
À RENVOYER AU PLUS TARD LE 11 FÉVRIER 2024

Les consignes suivantes sont à lire attentivement :

- Le groupe junior est constitué des élèves nés en 2009 ou après. Les autres élèves sont dans le groupe senior.
- Les exercices classés “Juniors” ne sont à chercher que par les élèves du groupe junior.
- Les exercices classés “Seniors” ne sont à chercher que par les élèves du groupe senior.
- Les exercices doivent être cherchés de manière individuelle.
- Utiliser des feuilles différentes pour des exercices différents.
- Respecter la numérotation des exercices.
- Bien préciser votre nom en lettres capitales, et votre prénom en minuscules sur chaque copie.

Exercices Juniors

Exercice 1. Soient a, b deux entiers relatifs. Montrer que, si ni a, ni b n'est multiple de 3, alors $a^4 - b^2$ est multiple de 3.

Solution de l'exercice 1 Rappelons que si k n'est pas un multiple de 3, alors k vaut 1 ou 2 modulo 3. Ainsi k^2 vaut $1^2 = 1$ ou $2^2 \equiv 4 \equiv 1 \pmod 3$: tout carré d'un nombre non divisible par 4 vaut 1 modulo 3.
Ainsi $a^4 - b^2 \equiv (a^2)^2 - b^2 \equiv 1^2 - 1 \equiv 0 \pmod 3$, donc $a^4 - b^2$ est un multiple de 3.

Commentaire des correcteurs : L'exercice a été très bien réussi dans l'ensemble, cependant pas mal d'élèves pourraient aller plus vite en utilisant des modulos plutôt que les écritures explicites des divisions euclidiennes, les calculs seraient de fait allégés.

Exercice 2. Soit n un entier vérifiant $n \geqslant 2$. On note d le plus grand diviseur de n différent de n. On suppose que $d > 1$. Démontrer que $n + d$ n'est pas une puissance de 2.

Solution de l'exercice 2 Supposons par l'absurde que $n + d$ est une puissance de 2. Notons que d divise n, donc d divise $n + d$, donc d divise une puissance de 2. Ainsi d est une puissance de 2 : on pose $d = 2^k$ pour un certain $k \in \mathbb{N}$. On a $k \geqslant 1$ car $d \neq 1$. Posons $n = da = 2^k a$ avec $a \in \mathbb{N}^*$. Comme d est différent de n, on a $a \geqslant 2$. Ainsi $2^{k-1}a$ est un diviseur de n, supérieur ou égal à $2^k = d$, et différent de n. Par hypothèse $d = 2^{k-1}a$, donc $a = 2$. Ainsi $n = 2^{k+1}$.
On trouve alors $n + d = 2^k(2+1) = 3 \times 2^k$ qui n'est pas une puissance de 2, ce qui est une contradiction. Ainsi $n + d$ n'est pas une puissance de 2.

Commentaire des correcteurs : L'exercice a été très bien réussi, mais plusieurs copies ont oublié que 1 est un diviseur impair d'une puissance de 2.

Exercice 3. Déterminer tous les entiers $n \geqslant 0$ tels que $2023 + n!$ est un carré parfait.

Solution de l'exercice 3 Soit $n \geqslant 0$ tel que $2023 + n!$ est un carré parfait. Si $n \geqslant 4$, alors 4 divise $n!$, donc $2023 + n! \equiv 2023 \equiv 3 \pmod 4$. Or 3 n'est pas un carré modulo 4 (les carrés modulo 4 sont 0 et 1), donc on a une contradiction. Ainsi $n \leqslant 3$.
Notons que $44^2 = 1936 < 2023+0! = 2023+1! = 2024 < 2023+2! = 2025 = 45^2 < 2023+3!+2029 < 2116 = 46^2$. Ainsi pour $n = 0, 1, 3$, $2023 + n!$ n'est pas un carré, mais pour $n = 2$ c'est un carré.
Ainsi $2023 + n!$ est un carré si et seulement si $n = 2$.

Commentaire des correcteurs : L'exercice a été très bien réussi. Quelques copies ont oublié le cas $n = 0$.

Exercice 4. Déterminer tous les triplets (p, q, r) de nombres premiers tels que $p + q^2 = r^4$.

Solution de l'exercice 4 Notons que l'équation se réécrit $p = (r^2)^2 - q^2 = (r^2 - q)(r^2 + q)$. Come $r^2 + q$ est strictement positif, et p aussi, $r^2 - q$ aussi. En particulier, d'après l'équation précédente, on a que $r^2 - q = 1$ et $r^2 + q = p$. Si r et q sont impairs, alors $r^2 - q$ est pair, ce qui est contradictoire. Ainsi parmi r et q, un est pair, donc vaut 2 car q et r sont premiers.
Si $r = 2$, alors $r^2 - q = 1$, donc $q = 4 - 1 = 3$. De plus $p = q + r^2 = 7$, donc $(p, q, r) = (7, 3, 2)$ est une éventuelle solution.
Si $q = 2$, alors $r^2 = q + 1 = 3$ ce qui est impossible.
Réciproquement, pour $(p, q, r) = (7, 3, 2)$, $p + q^2 = 7 + 9 = 16 = 2^4$.

Commentaire des correcteurs : L'exercice est très bien résolu. Beaucoup d'approches différentes de celle proposée dans le corrigé étaient envisageables, et les élèves les ont toujours bien mises en oeuvre.

Exercice 5. Déterminer tous les quadruplets (a, b, c, d) d'entiers positifs avec a, b, c strictement positifs tels que

$$\begin{aligned} \text{PPCM}(b, c) &= a + d \\ \text{PPCM}(c, a) &= b + d \\ \text{PPCM}(a, b) &= c + d \end{aligned}$$

Solution de l'exercice 5 Le système étant symétrique, on suppose que c est le maximum de a, b et c. Comme c divise $\text{PPCM}(b, c)$, c divise $a + d$. Comme c divise $\text{PPCM}(c, a)$, c divise $b + d$, donc c divise $a + d - (b + d) = a - b$. Or $-c < a - b < c$ donc $a = b$. La dernière ligne donne alors $a = \text{PPCM}(a, b) = c + d \geqslant c$. Pour avoir égalité, on a donc $d = 0$ et $a = c$.
Réciproquement, si $a = b = c$ et $d = 0$, chaque équation équivaut à $a = a + 0$, qui est vrai. Les quadruplets solution sont donc les $(a, a, a, 0)$ pour $a \in \mathbb{N}^*$.

Commentaire des correcteurs : L'exercice a été bien réussi dans l'ensemble. Cependant beaucoup d'élèves oublient que A divise B n'implique pas $A \leqslant B$: cela ne marche que si A est positif et B strictement positif. Si B est uniquement positif, il peut être nul. Et beaucoup d'élèves raisonnent par implication, mais oublient de vérifier les solutions à la fin : en compétition cela coûte systématiquement un point.

Exercice 6. Un entier $n \geqslant 2$ est écrit au tableau. Chaque jour, quelqu'un choisit p un diviseur premier de l'entier écrit n au tableau, efface celui-ci et écrit $n + \frac{n}{p}$ à la place. Montrer que $p = 3$ est choisi une infinité de fois.

Solution de l'exercice 6 Fixons $N \in \mathbb{N}$. Notons $2^{a_k}3^{b_k}c_k$ l'entier écrit au tableau le jour k, avec c_k produit de nombres premiers distincts de 2 et 3. Supposons par l'absurde qu'on peut ne jamais choisir $p = 3$ à partir du jour N.
Si le k-ième jour on choisit $p \neq 2, 3$, alors le nombre écrit au tableau devient $2^{a_k}3^{b_k}\frac{c_k}{p}(p+1)$. Posons $p+1 = 2^b3^c d$ avec b, c, d des entiers positifs et d premier avec 2 et 3. Comme p est premier et différent de 2, il est pair, donc $a \geqslant 1$, donc $d \leqslant \frac{p+1}{2}$. Ainsi comme le nombre écrit au tableau est $2^{a_k+a}3^{b_k+b}\frac{c_k}{p}d$, donc $a_{k+1} = a_k + a$, $b_{k+1} = b_k + b$ et $c_{k+1} = \frac{c_k}{p}d \leqslant c_k\frac{p+1}{2p} < c_k$.
Si le k-ième jour on choisit $p = 2$, le nombre écrit au tableau devient $\frac{3}{2}2^{a_k}3^{b_k}c_k = 2^{a_k-1}3^{b_k+1}c_k$.
En particulier, la suite $(c_k)_{k\geqslant N}$ décroît et est strictement positive. Elle ne peut donc décroître strictement infiniment souvent, sinon elle deviendrait négative. Donc à partir d'un certain jour $k > N$, on ne choisit plus $p \neq 2, 3$, donc $p = 2$ est choisit chaque jour à partir du k-ième jour.
Or si à partir du jour $k > N$ on ne choisit que $p = 2$, alors $a_{j+1} = a_j - 1$ pour tout $j \geqslant k$. Donc la suite d'entiers $(a_j)_{j\geqslant k}$ décroît strictement, elle doit donc devenir strictement négative ce qui est absurde.
Ainsi, on est obligé de choisir au moins une fois $p = 3$ après le N-ième jour.
Supposons que $p = 3$ n'est pas choisi une infinité de fois. A partir d'un certain jour, noté N, $p = 3$ n'est plus jamais choisi. Cela contredit ce qu'on vient de prouver : $p = 3$ est donc choisi une infinité de fois.

Commentaire des correcteurs : L'idée du raisonnement derrière l'exercice a généralement été comprise, mais les solutions ont été assez mal rédigées dans leur ensemble, préférant des descriptions informelles à des énoncés précis et soigneusement démontrés. Rédiger de telles démonstrations au collège n'est certainement pas chose facile, mais est tout de même nécessaire pour éviter quelques écueils. Si ceux-ci étaient mineurs et relativement faciles à contourner dans ce problème (pour peu qu'on les vît, ce qui était rare), ce n'est pas toujours le cas et des conclusions "intuitivement vraies" peuvent s'avérer complètement fausses parce que des étapes cruciales de raisonnement n'auraient pas été envisagées. Quelques élèves n'ont pas compris la question : il ne s'agissait pas ici de montrer que l'on pouvait choisir $p = 3$ une infinité de fois avec un choix judicieux d'opérations. Il fallait montrer que quelle que soit la suite d'opérations choisie à partir de n'importe quel entier (et même si on essayait d'éviter de le faire), on doit choisir $p = 3$ une infinité de fois. Les autres élèves ont, pour la plupart, compris que les facteurs premiers de n devenaient de plus en plus petits, puisqu'un facteur $p > 2$ était remplacé par le nombre pair $p + 1$, dont tous les facteurs premiers étaient strictement inférieurs à p. Cette intuition est correcte, mais ne doit pas figurer telle quelle dans une copie, parce que cet énoncé n'est pas clair : en quel sens les facteurs premiers devenaient-ils de plus en plus petits ? Leur maximum ? Leur nombre ? Une espèce de combinaison des deux, dirait-on intuitivement, mais encore faut-il la décrire ! Tout le problème d'employer cette intuition informelle comme une étape de raisonnement est qu'il semble naturel d'en déduire qu'au bout d'un certain moment, l'entier écrit au tableau n'a plus que des 2 et des 3 comme facteurs premiers. Ceci n'est pas vrai, puisqu'on peut par exemple multiplier une suite valide par 5. Cela peut paraître un contre-exemple trivial, mais *cela montre qu'il existe des contre-exemples*, et donc qu'il peut exister des contre-exemples plus subtils que celui-ci. Le corrigé permet de trouver une des façons de formaliser cette intuition, en explicitant une quantité entière qui ne peut que décroître (un "mono-variant") et qui doit donc être constante à partir d'un certain moment. Quelques élèves ont pris une autre approche, consistant essentiellement à raisonner par récurrence (forte) en se reposant sur l'observation suivante : si $n = ab$, alors on peut aussi considérer qu'on a chaque jour deux nombres a et b écrits sur deux tableaux différents, et qu'on effectue chaque jour l'opération sur l'un des deux tableaux. Partant, l'un ou l'autre des entiers est modifié selon l'opération une infinité de fois et on a donc par hypothèse de récurrence

utilisé $\mathrm{p} = 3$ une infinité de fois.

Exercice 7. Soit k un entier premier avec n vérifiant $1 \leqslant k < n$. Augustin colorie les entiers de $\{1, 2, \ldots, n-1\}$ avec autant de couleur qu'il le souhaite. Cependant, si j est un entier vérifiant $1 \leqslant j \leqslant n-1$, les entiers j et $n-j$ sont de la même couleur. De plus, si i est un entier vérifiant $1 \leqslant i \leqslant n$ et $i \neq k$, les entiers i et $|i-k|$ sont de la même couleur.
Démontrer que Augustin a colorié tous les entiers de la même couleur.

Solution de l'exercice 7 Pour $k = 1$, on voit que n a la même couleur que $n-1$, puis que $n-2$ à la même couleur que $n-1$, etc et tous les entiers ont la même couleur.
Pour $k = 2$, n est impair et on voit que $n, n-2, \ldots, 1$ ont la même couleur, puis que $n-1$ a la même couleur que 1, et que $n-1, n-3, \ldots, 2$ ont la même couleur.
En faisant la même chose pour des petites valeurs de k, on se rend compte qu'on arrive à chaque fois à montrer successivement que $n-k, \ldots, n-(n-1)k$ pris modulo n sont tous de la même couleur. Essayons de formaliser cela.
Notons c la couleur de n. On montre par récurrence la propriété suivante pour tout $j \in \{1, \ldots, n-1\}$:
$\mathcal{P}(j)$: "Le reste de la division euclidienne de $n-jk$ n'est pas congru à 0 modulo n, et est colorié avec la couleur c.
Initialisation : pour $j = 1$, comme $1 \leqslant n-k \leqslant n-1$, le reste de la division euclidienne de $n-k$ vaut $n-k$, n'est pas congru à 0 modulo n, et est colorié avec la couleur c.
Hérédité : Soit $j \in \{0, \ldots, n-2\}$, supposons que $P(j)$ est vraie et montrons $P(j+1)$. Notons r le reste de la division euclidienne de $n-jk$ par n.
Premier cas : si $r > k$, alors $n > r \geqslant r-k > 0$. Or $r-k \equiv n-jk-k \equiv n-(j+1)k \pmod{n}$. Donc le reste de la division euclidienne de $n-jk$ par n vaut $r-k$, est non nul et est de la même couleur que r, donc de la couleur c ce qui conclut.
Second cas, si $r = k$, alors $n-jk \equiv k \pmod{n}$, i.e. $(j+1)k \equiv 0 \pmod{n}$. Comme n est premier avec k, et divise $(j+1)k$, n divise $j+1$, mais comme $j+1 \in \{1 \ldots, , n-1\}$, ce cas est impossible.
Troisième cas : si $k > r$, alors $k-r$ est de la couleur de de r, donc de la couleur c. De plus on a $1 \leqslant k-r \leqslant k \leqslant n-1$, donc $n-(k-r)$ vérifie $1 \leqslant n-(k-r) \leqslant n-1$ et est de la couleur c. Or $n-(k-r) \equiv r-k \equiv n-(j+1)k \pmod{n}$, donc $n-(k-r)$ est le reste de la division euclidienne de $n-(j+1)k$ par n, est non nul et de couleur c, ce qui conclut.
Ceci conclut l'hérédité.
Maintenant donnons nous $j \in \{1, \ldots, n-1\}$. Il existe $\ell \in \{0 \ldots, n-1\}$ tel que $j \equiv n-\ell k \pmod{n}$: en effet, ceci est équivalent à $\ell k \equiv n-j \pmod{n}$, soit à $\ell \equiv (n-j)k^{-1} \pmod{n}$ (où k^{-1} est l'inverse de k modulo n, qui existe car k est premier avec n), et admet une solution dans $\{0 \ldots, n-1\}$. En particulier, j est le reste de la divison euclidienne de $n-\ell j$ par n, donc de couleur c. Ainsi tous les entiers de 1 à $n-1$ ont la même couleur que n, donc tous les entiers sont coloriés de la même couleur.

Commentaire des correcteurs : L'exercice est relativement mal résolu : beaucoup de preuves fournies s'avèrent incomplètes, car elles oublient certaines contraintes ($i \neq k$ pour dire que $|i-k|$ et i ont la même couleur, oubli que i et $i+k$ n'ont pas la même couleur si $i > n-k$, etc).

Exercice 8. Déterminer tous les couples (a, p) d'entiers strictement positifs, avec p premier, tels que pour tout couple (m, n) d'entiers strictement positifs, le reste de la division euclidienne de a^{2^n} par p^n est non nul, et est le même que celui de a^{2^m} par p^m.

Solution de l'exercice 8 En prenant $n = 1$ dans l'énoncé, on obtient que pour tout entier m strictement positif, le reste de a^{2^m} modulo p^m vaut celui de a^2 modulo p, donc est constant. Notons r ce reste : on a donc $r \neq 0$ ainsi $r \in \{1, \dots, p-1\}$. On a $a^2 \equiv r \pmod{p}$ et $a^4 \equiv r \pmod{p^2}$, donc $a^4 \equiv r \pmod{p}$, donc $r^2 \equiv r \pmod{p}$. Ainsi comme r est premier avec p, r est inversible mod p, donc $r \equiv 1 \pmod{p}$. On a donc $a^{2^m} \equiv 1 \pmod{p^m}$ pour tout m. En particulier $a^2 \equiv 1 \pmod{p}$
Or

$$a^{2^m} - 1 = (a^{2^{m-1}} - 1)(a^{2^{m-1}} + 1) = \cdots = (a^2 - 1)(a^2 + 1)(a^4 + 1) \dots (a^{2^{m-1}} + 1)$$

Si $p \geqslant 3$, pour tout $k \geqslant 1$, $a^{2^k} + 1 \equiv 1^{2^{k-1}} + 1 \equiv 2 \not\equiv 0 \pmod{p}$, donc si $a \neq 1$ $V_p(a^{2^m} - 1) = V_p(a^2 - 1)$. Or pour tout m, p^m divise $a^{2^m} - 1$, donc $m \leqslant V_p(a^{2^m} - 1) = V_p(a^2 - 1)$ ce qui est absurde car $V_p(a^2 - 1)$ est fini. Ainsi $a = 1$. Réciproquement pour tout p premier, $a = 1$ est solution car le reste de 1^{2^m} modulo p^m vaut toujours 1 et est non nul.
Si $p = 2$ et $a \neq 1$, $a^2 \equiv 1 \pmod{2}$, donc a est impair. Réciproquement si a est impair, rappelons que

$$a^{2^m} - 1 = (a^{2^{m-1}} - 1)(a^{2^{m-1}} + 1) = \cdots = (a^2 - 1)(a^2 + 1)(a^4 + 1) \dots (a^{2^{m-1}} + 1)$$

Le produit de droite contient m termes tous pairs, donc est divisible par 2^m. Ainsi pour tout n, le reste de a^{2^n} modulo 2^n vaut 1 et est non nul, donc tous les couples de la forme $(a, 2)$ avec a impair sont solutions.
Ainsi les couples solutions sont ceux de la forme $(1, p)$ pour $p \geqslant 3$ et $(a, 2)$ pour a impair.

Solution alternative A partir du fait que $a^{2^m} \equiv 1 \pmod{p^m}$ pour tout m, on a comme p divise $a^2 - 1$, par LTE si $p \geqslant 3$ que si $a > 1$, $V_p(a^{2^m} - 1) = V_p(a^2 - 1) + V_p(2^{m-1}) = V_p(a^2 - 1)$. En particulier, comme $V_p(a^{2^m} - 1) \geqslant m$ pour tout $m \geqslant 1$, $V_p(a^2 - 1) \geqslant m$ pour tout m ce qui est absurde donc $a = 1$. Réciproquement, $a = 1$ et $p \geqslant 3$ convient comme dans la solution précédente.
Pour le cas $p = 2$, de même que précédemment on a p impair, donc 4 divise $p^2 - 1 = (p-1)(p+1)$, donc par LTE, comme 4 divise $a^4 - 1$, si $a > 1$ $V_2(a^{2^m} - 1) = V_2(a^2 - 1) + V_2(2^{m-1}) \geqslant 2 + m - 1 = m + 1$, ainsi $a^{2^m} - 1$ est divisible par 2^m pour tout m, et on conclut de la même façon que précédemment.

Commentaire des correcteurs : L'exercice est résolu de manière inégale par ceux qui s'y sont essayés. En effet, certains loupent certaines solutions (soit le cas $p = 2$ soit le cas $a = 1$: les petites valeurs devraient pourtant permettre de repérer ces solutions. Attention aussi aux utilisations du LTE : le théorème LTE a des hypothèses, il faut les vérifier sous peine d'écrire des choses fausses.

Exercice 9. Déterminer tous les quadruplets (x, y, z, t) d'entiers strictement positifs tels que $2^x 3^y + 5^z = 7^t$.

Solution de l'exercice 9 Supposons $x \geqslant 2$, en regardant modulo 4, $1 \equiv 2^x 3^y + 5^z \equiv 7^t \equiv (-1)^t \pmod 4$, donc t est pair.
L'équation prise modulo 3 devient $0 + (-1)^z \equiv 1 \pmod 3$ donc z est pair. En particulier, posons $z = 2b, t = 2c$, on a alors $2^x 3^y = (7^b - 5^c)(7^b + 5^c)$. Le pgcd de $7^b + 5^c$ et $7^b - 5^c$ divise leur somme et leur produit, donc il divise $2^x 3^y$ et 2×7^b, ainsi il divise 2. Or $7^b + 5^c$ et $7^b - 5^c$ sont égaux mod 2 donc ils ont la même parité, et leur produit est pair, donc chacune est pair, leur pgcd vaut 2. Comme $7^b - 5^c < 7^b + 5^c$, on a $(7^b - 5^c, 7^b + 5^c) = (2, 2^{x-1}3^y), (2^{x-1}, 2 \times 3^y), (2 \times 3^y, 2^{x-1})$.

- Dans le premier cas, si $c \geqslant 2$, modulo 25, $7^b \equiv 2 \pmod{25}$. Or les puissances de 7 valent $1, 7, -1, -7$ modulo 25, mais jamais 2. Comme $c \neq 0$ car $z \neq 0$, on a donc $c = 1$, donc $7^b = 5+2 = 7$, donc $b = 1$. On a donc $12 = 2^{x-1}3^y$ donc $(x, y, z, t) = (3, 1, 2, 2)$, qui réciproquement est solution car $2^3 \times 3 + 5^2 = 24 + 25 = 49 = 7^2$.
- Dans le second cas $(7^b - 5^c, 7^b + 5^c) = (2^{x-1}, 2 \times 3^y)$. Par parité, on a $x \geqslant 2$, et comme le cas où $x = 2$ est déjà couvert par le cas précédent, on peut supposer $x \geqslant 3$. On pose $x' = x - 1$, on a alors $7^b = 5^c + 2^{x'}$ avec $x' \geqslant 2$. En regardant modulo 4, $(-1)^b \equiv 1 \pmod 4$, donc b est pair. En regardant modulo 5, $2^b \equiv 2^{x'} \pmod 5$. Or les puissances de 2 alternent entre $1, 2, 4, 3$ mod 5, donc deux puissances de 2 ont même valeur modulo 5 si et seulement si leur exposant sont égaux modulo 4, donc b et x' ont même parité. En regardant modulo 3, $1 \equiv (-1)^c + (-1)^{x'} \pmod 3$ donc c et x' sont impairs. Ceci contredit le fait que b et x' ont même parité.

Avant de traiter le dernier cas, résolvons l'équation dans le cas $x = 1$: on a $2 \times 3^y + 5^z = 7^t$. Modulo 3, on obtient comme avant que z est pair, donc $5^z \equiv 25^{z/2} \equiv 1 \pmod 8$. En particulier modulo 8, $(-1)^t \equiv 1 + 2 \times 3^y$. Le terme de droite vaut 3 si y est pair, -1 sinon, donc t est impair et y est impair (car $3^2 \equiv 1 \pmod 8$). On a alors en regardant modulo 5, comme les puissances de 7 valent $1, 2, 4, 3, 1$ et les puissances de 3 valent $1, 3, 4, 2, 1$, on a $7^t \equiv 2$ ou 3 car t est impair, et 7 d'ordre 4 (qui est pair) modulo 5. Comme y est impair, on a $2 \times 3^y \equiv 1$ ou 4 modulo 5 car l'ordre de 3 modulo 5 est pair. Or l'équation modulo 5 donne $2 \times 3^y \equiv 7^t$ ce qui est impossible. Il n'y a donc pas de solution avec $x = 1$.
Pour le troisième cas $(7^b - 5^c, 7^b + 5^c) = (2 \times 3^y, 2^{x-1})$, on a $7^b - 5^c = 2 \times 3^y$. Comme $c > 0$, on est ramené au cas précédent il n'y a pas de solution.
Ainsi la seule solution est $(x, y, z, t) = (3, 1, 2, 2)$.

Commentaire des correcteurs : L'exercice était très difficile et a été très peu abordé. Il est tout de même regrettable que les quelques copies qui réussissent à trouver la factorisation ne pensent que rarement à considérer le pgcd de $7^z + 5^t$ et $7^z - 5^t$ (ou même simplement la parité de ces deux nombres !) et se lancent tête baissée dans de grandes disjonctions de cas ou dans des utilisations abusives du théorème de Zsigmondy, que beaucoup auraient pu s'épargner (un seul élève a su utiliser ce théorème vraiment efficacement).

Exercices Seniors

Exercice 10. Soient a, b deux entiers relatifs. Montrer que, si ni a, ni b n'est multiple de 3, alors $a^4 - b^2$ est multiple de 3.

Solution de l'exercice 10 Rappelons que si k n'est pas un multiple de 3, alors k vaut 1 ou 2 modulo 3. Ainsi k^2 vaut $1^2 = 1$ ou $2^2 \equiv 4 \equiv 1 \pmod 3$: tout carré d'un nombre non divisible par 4 vaut 1 modulo 3.
Ainsi $a^4 - b^2 \equiv (a^2)^2 - b^2 \equiv 1^2 - 1 \equiv 0 \pmod 3$, donc $a^4 - b^2$ est un multiple de 3.

Commentaire des correcteurs : Exercice très bien réussi.

Exercice 11. Soit n un entier vérifiant $n \geqslant 2$. On note d le plus grand diviseur de n différent de n. On suppose que $d > 1$. Démontrer que $n + d$ n'est pas une puissance de 2.

Solution de l'exercice 11 Supposons par l'absurde que $n+d$ est une puissance de 2. Notons que d divise n, donc d divise $n+d$, donc d divise une puissance de 2. Ainsi d est une puissance de 2 : on pose $d = 2^k$ pour un certain $k \in \mathbb{N}$. On a $k \geqslant 1$ car $d \neq 1$. Posons $n = da = 2^k a$ avec $a \in \mathbb{N}^*$. Comme d est différent de n, on a $a \geqslant 2$. Ainsi $2^{k-1}a$ est un diviseur de n, supérieur ou égal à $2^k = d$, et différent de n. Par hypothèse $d = 2^{k-1}a$, donc $a = 2$. Ainsi $n = 2^{k+1}$.
On trouve alors $n+d = 2^k(2+1) = 3\times 2^k$ qui n'est pas une puissance de 2, ce qui est une contradiction. Ainsi $n + d$ n'est pas une puissance de 2.

Commentaire des correcteurs : Exercice bien réussi, cependant quelques élèves vont un peu trop vite et oublient des étapes, essentielles pour aboutir à des contradictions, alors injustifiées.

Exercice 12. Déterminer tous les quadruplets (a, b, c, d) d'entiers positifs avec a, b, c strictement positifs tels que

$$\begin{aligned} \text{PPCM}(b, c) &= a + d \\ \text{PPCM}(c, a) &= b + d \\ \text{PPCM}(a, b) &= c + d \end{aligned}$$

Solution de l'exercice 12 Le système étant symétrique, on suppose que c est le maximum de a, b et c. Comme c divise $\text{PPCM}(b, c)$, c divise $a + d$. Comme c divise $\text{PPCM}(c, a)$, c divise $b + d$, donc c divise $a + d - (b + d) = a - b$. Or $-c < a - b < c$ donc $a = b$. La dernière ligne donne alors $a = \text{PPCM}(a, b) = c + d \geqslant c$. Pour avoir égalité, on a donc $d = 0$ et $a = c$.
Réciproquement, si $a = b = c$ et $d = 0$, chaque équation équivaut à $a = a + 0$, qui est vrai. Les quadruplets solution sont donc les $(a, a, a, 0)$ pour $a \in \mathbb{N}^*$.

Commentaire des correcteurs : L´exercice est très bien réussi, cependant quelques élèves ont oublié de vérifier que les solutions trouvées étaient solutions du système ce qui les a pénalisés.

Exercice 13. Un entier $n \geqslant 2$ est écrit au tableau. Chaque jour, quelqu'un choisit p un diviseur premier de l'entier écrit n au tableau, efface celui-ci et écrit $n + \frac{n}{p}$ à la place. Montrer que $p = 3$ est choisi une infinité de fois.

Solution de l'exercice 13 Fixons $N \in \mathbb{N}$. Notons $2^{a_k}3^{b_k}c_k$ l'entier écrit au tableau le jour k, avec c_k produit de nombres premiers distincts de 2 et 3. Supposons par l'absurde qu'on peut ne jamais choisir $p = 3$ à partir du jour N.
Si le k-ième jour on choisit $p \neq 2, 3$, alors le nombre écrit au tableau devient $2^{a_k}3^{b_k}\frac{c_k}{p}(p+1)$. Posons $p+1 = 2^b3^c d$ avec b, c, d des entiers positifs et d premier avec 2 et 3. Comme p est premier et différent de 2, il est pair, donc $a \geqslant 1$, donc $d \leqslant \frac{p+1}{2}$. Ainsi comme le nombre écrit au tableau est $2^{a_k+a}3^{b_k+b}\frac{c_k}{p}d$, donc $a_{k+1} = a_k + a$, $b_{k+1} = b_k + b$ et $c_{k+1} = \frac{c_k}{p}d \leqslant c_k\frac{p+1}{2p} < c_k$.
Si le k-ième jour on choisit $p = 2$, le nombre écrit au tableau devient $\frac{3}{2}2^{a_k}3^{b_k}c_k = 2^{a_k-1}3^{b_k+1}c_k$.
En particulier, la suite $(c_k)_{k\geqslant N}$ décroît et est strictement positive. Elle ne peut donc décroître strictement infiniment souvent, sinon elle deviendrait négative. Donc à partir d'un certain jour $k > N$, on ne choisit plus $p \neq 2, 3$, donc $p = 2$ est choisit chaque jour à partir du k-ième jour.
Or si à partir du jour $k > N$ on ne choisit que $p = 2$, alors $a_{j+1} = a_j - 1$ pour tout $j \geqslant k$. Donc la suite d'entiers $(a_j)_{j\geqslant k}$ décroît strictement, elle doit donc devenir strictement négative ce qui est absurde.
Ainsi, on est obligé de choisir au moins une fois $p = 3$ après le N-ième jour.
Supposons que $p = 3$ n'est pas choisi une infinité de fois. A partir d'un certain jour, noté N, $p = 3$ n'est plus jamais choisi. Cela contredit ce qu'on vient de prouver : $p = 3$ est donc choisi une infinité de fois.

Commentaire des correcteurs : Certains élèves ont mal compris l'énoncé : il s'agissait de prouver que l'on était obligé de choisir $p = 3$ une infinité de fois quels que soient les choix effectués, pas que l'on pouvait s'arranger pour que ce soit le cas. L'exercice est généralement bien abordé par ceux qui l'ont correctement interprété, mais de trop nombreux élèves manquent de rigueur. L'enjeu était de trouver un argument rigoureux (donc a priori un monovariant, que ce soit celui proposé par le corrigé, l'ordre lexicographique inversé des exposants ou beaucoup d'autres possibilités) pour clarifier la phrase lue dans de trop nombreuses copies : "les facteurs premiers décroissent". Cette phrase dénuée de sens mathématique ne constitue en aucun cas un argument recevable, il faut clarifier l'intuition qui se cache derrière. C'est un écueil que l'on croise souvent en combinatoire : il est parfois délicat de passer de l'intuition à l'argument rigoureux, et souvent une partie de la difficulté de l'exercice réside justement dans cette étape.

Exercice 14. Soit k un entier premier avec n vérifiant $1 \leqslant k < n$. Augustin colorie les entiers de $\{1, 2, \ldots, n-1\}$ avec autant de couleur qu'il le souhaite. Cependant, si j est un entier vérifiant $1 \leqslant j \leqslant n-1$, les entiers j et $n-j$ sont de la même couleur. De plus, si i est un entier vérifiant $1 \leqslant i \leqslant n$ et $i \neq k$, les entiers i et $|i-k|$ sont de la même couleur.
Démontrer que Augustin a colorié tous les entiers de la même couleur.

Solution de l'exercice 14 Pour $k = 1$, on voit que n a la même couleur que $n-1$, puis que $n-2$ à la même couleur que $n-1$, etc et tous les entiers ont la même couleur.
Pour $k = 2$, n est impair et on voit que $n, n-2, \ldots, 1$ ont la même couleur, puis que $n-1$ a la même couleur que 1, et que $n-1, n-3, \ldots, 2$ ont la même couleur.
En faisant la même chose pour des petites valeurs de k, on se rend compte qu'on arrive à chaque fois à montrer successivement que $n-k, \ldots, n-(n-1)k$ pris modulo n sont tous de la même couleur. Essayons de formaliser cela.
Notons c la couleur de n. On montre par récurrence la propriété suivante pour tout $j \in \{1, \ldots, n-1\}$:
$\mathcal{P}(j)$: "Le reste de la division euclidienne de $n-jk$ n'est pas congru à 0 modulo n, et est colorié avec la couleur c.
Initialisation : pour $j = 1$, comme $1 \leqslant n-k \leqslant n-1$, le reste de la division euclidienne de $n-k$ vaut $n-k$, n'est pas congru à 0 modulo n, et est colorié avec la couleur c.
Hérédité : Soit $j \in \{0, \ldots, n-2\}$, supposons que $P(j)$ est vraie et montrons $P(j+1)$. Notons r le reste de la division euclidienne de $n-jk$ par n.
Premier cas : si $r > k$, alors $n > r \geqslant r-k > 0$. Or $r-k \equiv n-jk-k \equiv n-(j+1)k \pmod{n}$. Donc le reste de la division euclidienne de $n-jk$ par n vaut $r-k$, est non nul et est de la même couleur que r, donc de la couleur c ce qui conclut.
Second cas, si $r = k$, alors $n-jk \equiv k \pmod{n}$, i.e. $(j+1)k \equiv 0 \pmod{n}$. Comme n est premier avec k, et divise $(j+1)k$, n divise $j+1$, mais comme $j+1 \in \{1 \ldots, , n-1\}$, ce cas est impossible.
Troisième cas : si $k > r$, alors $k-r$ est de la couleur de de r, donc de la couleur c. De plus on a $1 \leqslant k-r \leqslant k \leqslant n-1$, donc $n-(k-r)$ vérifie $1 \leqslant n-(k-r) \leqslant n-1$ et est de la couleur c. Or $n-(k-r) \equiv r-k \equiv n-(j+1)k \pmod{n}$, donc $n-(k-r)$ est le reste de la division euclidienne de $n-(j+1)k$ par n, est non nul et de couleur c, ce qui conclut.
Ceci conclut l'hérédité.
Maintenant donnons nous $j \in \{1, \ldots, n-1\}$. Il existe $\ell \in \{0 \ldots, n-1\}$ tel que $j \equiv n-\ell k \pmod{n}$: en effet, ceci est équivalent à $\ell k \equiv n-j \pmod{n}$, soit à $\ell \equiv (n-j)k^{-1} \pmod{n}$ (où k^{-1} est l'inverse de k modulo n, qui existe car k est premier avec n), et admet une solution dans $\{0 \ldots, n-1\}$. En particulier, j est le reste de la divison euclidienne de $n-\ell j$ par n, donc de couleur c. Ainsi tous les entiers de 1 à $n-1$ ont la même couleur que n, donc tous les entiers sont coloriés de la même couleur.

Commentaire des correcteurs : L'exercice est relativement mal résolu : beaucoup de preuves fournies s'avèrent incomplètes, car elles oublient certaines contraintes ($i \neq k$ pour dire que $|i-k|$ et i ont la même couleur, oubli que i et $i+k$ n'ont pas la même couleur si $i > n-k$, etc). Il est crucial que les élèves se relisent à froid : certaines copies n'ont vraiment pas de sens en les relisant à froid, et plusieurs élèves auraient évité une déconvenue en relisant leur production à tête reposée.

Exercice 15. Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes à coefficients entiers. On suppose qu'il existe un polynôme Q unitaire à coefficient entier tel que $P_{n+1} - P_n = Q$ pour tout $n \geqslant 0$. On suppose de plus que pour tout $n \geqslant 0$, P_n a une racine entière. Montrer qu'on est dans un des deux cas suivants :

— P_0 et Q ont une racine entière en commun

— Il existe un polynôme à coefficients entiers R tel que $P_0 = RQ$ et le degré de R est 1.

Solution de l'exercice 15 Supposons que P_0 et Q n'ont pas de racines entière en commun. Notons que par récurrence immédiate $P_n = P_0 + nQ$ pour tout $n \geqslant 0$. Notons x_n une racine entière de P_n pour tout $n \geqslant 0$, on a que $nQ(x_n) = -P_0(x_n)$, donc $Q(x_n)$ divise $P_0(x_n)$.
Notons que si $x_k = x_j$ avec $k \neq j$, alors $P_0(x_k) + kQ(x_k) = 0 = P_0(x_j) + jQ(x_j)$, donc $(k-j)Q(x_k) = 0$, donc $Q(x_k) = 0$. Ainsi $P_0(x_k) = 0$, donc P_0 et Q ont une racine entière en commun, ce qui est contradictoire. Ainsi la suite $(x_k)_{k\geqslant 0}$ est injective donc prend des valeurs arbitrairement grandes.
Faisons la division euclidienne de P_0 par Q. Comme Q est unitaire à coefficient entier (et P_0 à coefficients entiers), il existe des polynômes R et S à coefficients entiers tels que $P_0 = QR+S$ avec S de degré inférieur ou égal à Q.
En évaluant en x_n, $P_0(x_n) = Q(x_n)R(x_n) + S(x_n)$, donc comme $Q(x_n)$ divise $P_0(x_n)$, $Q(x_n)$ divise $S(x_n) = P_0(x_n) - Q(x_n)R(x_n)$. Or pour tout entier k avec $|k|$ assez grand, comme le degré de S est strictement inférieur à celui de Q, $|S(k)| < |Q(k)|$. Comme la suite (x_n) prend des valeurs arbitrairement grande, il existe une infinité de n tels que $|S(x_n)| < |Q(x_n)|$. Comme $Q(x_n)$ divise $S(x_n)$, on en déduit qu'il existe une infinité de n tels que $S(x_n) = 0$. Comme la suite est injective, S a une infinité de racine, donc $S = 0$. Ainsi $P_0 = QR$.
De plus, en évaluant en x_n, on a $-nQ(x_n) = P_0(x_n) = Q(x_n)R(x_n)$. Si $Q(x_n) = 0$, alors $P_0(x_n) = 0$ et P_0 et Q ont une racine en commun, contradiction. Ainsi $Q(x_n) \neq 0$, donc $R(x_n) = -n$. Ainsi pour tout entier $N \geqslant 0$, il existe au moins N entiers y tels que $R(y) \in [-N, N]$.
Or si le degré de R noté d vaut au moins 2, pour un M assez grand et pour un $C > 0$, on a pour tout x vérifiant $|x| \geqslant M$, $|R(x)| \geqslant C|x|^d$. Ainsi pour N assez grand, le nombre d'entier tel que $|R(x)| \leqslant N$ est plus petit que $2M + 1$ (le nombre d'entiers dans $[-M, M]$), auquel on ajoute le nombre d'entiers $|x| \geqslant M$ tel que $|P(x)| \leqslant N$. Pour ces x, on a $C|x|^d \leqslant N$ donc $|x| \leqslant (N/C)^{1/d}$. Ainsi on a au plus $2M + 1 + 2(N/c)^{1/d} + 1$ entiers tels que $P(y) \in [-n, n]$, ce qui est strictement inférieurs à N pour N assez grand, ce qui est contradictoire.
Ainsi le degré de R est au plus 1. Comme on a $R(x_n) = -n$ pour tout n, le degré de R vaut 1.

Alternativement, pour prouver que le degré de R valait n, on pouvait remarquer que pour tout n, $x_{n+1}-x_n$ divise $R(x_{n+1}) - R(x_n) = -1$. En particulier $x_{n+1} - x_n = \pm 1$ pour tout n. Comme la suite (x_n) est injective, on ne peut avoir $x_{n+1} - x_n = 1$ et $x_{n+2} - x_{n+1} = -1$, ou avoir $x_{n+1} - x_n = -1$ et $x_{n+2} - x_{n+1} = 1$ sinon $x_n = x_{n+2}$. Ainsi on a facilement par récurrence que soit pour tout n, $x_{n+1} - x_n = 1$, et donc $x_n = x_0 + n(x_1 - x_0)$, soit $x_{n+1} - x_n = -1$, et donc $x_n = x_0 - n(x_1 - x_0)$.
Dans le premier cas, en posant $S(X) = R(x_0 + X(x_1 - x_0)) - X$, on voit que $Q(n) = 0$ pour tout n. Comme S est un polynôme, c'est le polynôme nul, donc pour tout x réel, $R(x_0 + x(x_1 - x_0)) = x$. Ainsi en posant $x = \frac{y-x_0}{x_1-x_0}$ (qui est bien défini car $x_1 \neq x_0$), on a que $R(y) = \frac{y-x_0}{x_1-x_0}$ pour tout y, donc par identification $R(X) = \frac{X-x_0}{x_1-x_0}$: R est de degré 1.
Dans le second cas, en posant $S(X) = R(x_0 - X(x_1 - x_0)) - X$, on voit que $Q(n) = 0$ pour tout n. Comme S est un polynôme, c'est le polynôme nul, donc pour tout x réel, $R(x_0 - x(x_1 - x_0)) = x$. Ainsi en posant $x = \frac{x_0-y}{x_1-x_0}$ (qui est bien défini car $x_1 \neq x_0$), on a que $R(y) = \frac{x_0-y}{x_1-x_0}$ pour tout y, donc par identification $R(X) = \frac{X-x_0}{x_1-x_0}$: R est de degré 1.

Commentaire des correcteurs : L'exercice a été très bien traité par les élèves qui l'ont abordé. Presque tous ont bien vu qu'un R de degré au moins 2 " croirait et décroirait trop vite" pour attendre tous les entiers négatifs, mais certains n'ont pas rendu cette idée, certes vraie, rigoureuse. De plus, il faut garder

en tête qu'on peut considérer la divison euclidienne de P_0 par Q dans $\mathbb{Z}[X]$ seulement parce que Q est unitaire. Enfin, ne jamais oublier les cas triviaux : il est dommage de voir des élèves perdre un point pour ne pas avoir préciser que R ne pouvait être constant.

Exercice 16. Soit p un nombre premier et n un entier vérifiant $n \geqslant 2$.

— A quelle condition existe-t-il $n+1$ entiers (pas forcément distincts) tels que, pour tout choix de n entiers parmi les $n+1$, leur somme est une puissance de p ?

— A quelle condition existe-t-il $n+1$ entiers strictement positifs (pas forcément distincts) tels que, pour tout choix de n entiers parmi les $n+1$, leur somme est une puissance de p ?

Solution de l'exercice 16 Essayons d'analyser l'énoncé. Posons $x_1, \dots, x_{n+1}$ les entiers tels que pour tout choix de n entiers parmi les $n+1$ entiers, alors leur somme est une puissance de p. Il existe donc $\alpha_1, \dots, \alpha_{n+1}$ des entiers positifs tels que $x_2 + \cdots + x_{n+1} = p^{\alpha_1}$, $x_1 + x_3 + \cdots + x_{n+1} = p^{\alpha_2}, \dots, x_1 + \cdots + x_n = p^{\alpha_{n+1}}$.
En particulier, notons déjà que $p^{\alpha_i} = x_1 + \cdots + x_{n+1} - x_i$ pour tout $i \in \{1, \dots, n+1\}$ et que $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} = n(x_1 + \cdots + x_{n+1})$, donc pour tout $i \in \{1, \dots, n+1\}$, $x_i = \frac{p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}}{n} - p^{\alpha_i}$.
Réciproquement, si on se donne $\alpha_1, \dots, \alpha_{n+1}$ des entiers positifs tels que $x_i = \frac{p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}}{n} - p^{\alpha_i}$ pour tout $i \in \{1, \dots, n+1\}$, alors on voit que $x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_{n+1} = p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} - p^{\alpha_1} - \cdots - p^{\alpha_{i-1}} - p^{\alpha_{i+1}} - \cdots - p^{\alpha_{n+1}} = p^{\alpha_i}$.
La question revient donc à la suivant : existe-t-il des entiers positifs $\alpha_1, \dots, \alpha_{n+1}$ tels que n divise $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}$ pour la première question, et pour la seconde question tels que $\frac{p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}}{n} - p^{\alpha_i} > 0$, i.e. $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} > np^{\alpha_i}$ pour tout i.
Essayons de répondre d'abord à la première partie de la question : à quelle condition sur n existe-t-il $\alpha_1, \dots, \alpha_{n+1}$ tels que n divise $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}$? Déjà, modulo $p-1$, on a $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} \equiv n+1 \pmod{p-1}$. Notons d le pgcd de $p-1$ et n, alors si n divise $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}}$, comme d divise $p-1$, d divise aussi $n+1$. Comme d divise n, on obtient que d divise $n+1-n = 1$, donc $d = 1$. Ainsi il faut que n et $p-1$ sont premiers entre eux.
Réciproquement si n et $p-1$ sont premiers entre eux, soit $x \in \{1, \dots, n+1\}$ on prend $\alpha_1 = \cdots = \alpha_x = 0$ et $\alpha_{x+1} = \cdots = \alpha_{n+1} = 1$. On cherche donc un certain x tel que x tel que n divise $x + (n+1-x)p$, i.e. x tel que $x + p - xp \equiv 0 \pmod{n}$, soit $x \equiv p(p-1)^{-1} \pmod{n}$ (qui existe car $p-1$ et n sont premiers entre eux). On peut prendre un tel x dans $\{1, \dots, n\}$ tel que la précédente congruence est vraie. Ainsi la condition pour la première question est exactement n et $p-1$ sont premiers entre eux.

Pour la seconde question, on cherche de plus à avoir $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} > np^{\alpha_i}$ pour tout i. Quitte à réordonner les α_i, on peut supposer $\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_{n+1}$, la condition est équivalente à $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} > np^{\alpha_{n+1}}$. Si $\alpha_2 < \alpha_{n+1}$, on a :

$$p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} \leqslant 2p^{\alpha_2} + (n-1)p^{\alpha_{n+1}} \leqslant p^{\alpha_2+1} + (n-1)p^{\alpha_{n+1}} \leqslant np^{\alpha_{n+1}}.$$

Ainsi on a $\alpha_2 \geqslant \alpha_{n+1}$, donc $\alpha_2 = \cdots = \alpha_{n+1}$. Dans ce cas, il est clair que $p^{\alpha_1} + \cdots + p^{\alpha_{n+1}} > np^{\alpha_{n+1}}$ est vérifié. Il reste donc à chercher à quelle condition sur n existe-t-il $\alpha_1 \leqslant \alpha_2$ deux entiers positifs tels que n divise $p^{\alpha_1} + np^{\alpha_2}$ donc à quelle condition n divise p^{α_1}. Il est alors clair que les solutions sont les puissances de p. Ainsi la condition pour la seconde question est que n soit une puissance de p.

Commentaire des correcteurs : Chacune des parties de cet exercice a été globalement réussie par les élèves qui l'ont abordée. Néanmoins, plusieurs élèves, après avoir réussi l'une des deux parties, ont cru que l'autre n'en était qu'un simple corollaire, ce qui n'était pas vrai ; ils l'ont donc mal traitée, aboutissant à des résultats incorrects. C'est dommage !

Exercice 17. Soient a, b deux entiers tels que $\text{pgcd}(a, b)$ a au moins deux facteurs premiers distincts. Soit $S = \{x \in \mathbb{N} | x \equiv a[b]\}$. Un élément de S est dit irréductible s'il ne peut pas s'écrire comme un produit d'au moins deux éléments de S (pas forcément distincts).
Montrer qu'il existe $N > 0$ tel que tout élément de S s'écrit comme produit d'au plus N éléments irréductibles de S (pas forcément distincts).

Solution de l'exercice 17 Soit $d = \text{pgcd}(a, b)$, et écrivons $a = da', b = db'$. Commençons par traiter le cas où $\text{pgcd}(d, b') > 1$. Si c'est le cas, alors on a $\text{pgcd}(a^2, b) = d\text{pgcd}(da'^2, b') > d$. Donc, pour tout $k \geqslant 2$, on a $a^k \not\equiv a[b]$. En particulier, tout élément de S est irréductible, et donc $N = 1$ convient.
Supposons à présent que d et b' sont premiers entre eux. On a alors a et b' premiers entre eux ; soit ω l'ordre de a modulo b'. On a alors que $a^{\omega+1} \equiv a[b]$. Donc tout produit de $\omega + 1$ éléments de S est encore un élément de S. Ceci signifie en particulier que tout élément non irréductible de S peut s'écrire comme un produit de k éléments de S pour un certain $k \in [\![2, \omega]\!]$.
Soient p et q deux diviseurs premiers de d, et soit $x \in S$. Si x est irréductible, c'est bon ; sinon, écrivons $x = u_1 u_2 \dots u_k$ avec $u_1, \dots, u_k \in S$, pour un $k \in [\![2, \omega]\!]$. Montrons d'abord qu'on peut supposer $\nu_p(u_j) < \varphi(b') + \nu_p(d)$ pour tout $j < k$. Pour cela, on remarque que, si $\nu_p(u_j) \geqslant \varphi(b') + \nu_p(d)$, alors on peut remplacer u_j par $\frac{u_j}{p^{\varphi(b')}}$ et u_k par $p^{\varphi(b')} u_k$. On a $p^{\varphi(b')} \equiv 1[b']$, donc $p^{\varphi(b')} u_k \equiv u_k \equiv a[b']$. D'autre part, $d \mid u_k$ donc $p^{\varphi(b')} u_k \equiv 0 \equiv a[d]$. Donc, d'après le théorème des restes chinois, on a $p^{\varphi(b')} u_k \equiv a[b]$. D'autre part, on a aussi $\frac{u_j}{p^{\varphi(b')}} \equiv a[b']$, et on a également (puisque $\nu_p(u_j) \geqslant \varphi(b') + \nu_p(d)$) que $d \mid \frac{u_j}{p^{\varphi(b')}}$. Donc $\frac{u_j}{p^{\varphi(b')}} \equiv a[b]$.
On a à présent $\nu_p(u_j) < \varphi(b') + \nu_p(d)$ pour $j < k$. De même, on peut supposer que $\nu_q(u_k) < \varphi(b') + \nu_q(d)$. Toute écriture de u_j ($j < k$) sous forme de produit d'irréductibles fait apparaître seulement des multiples de d, donc de p, et comprend donc au plus $\nu_p(u_j)$ facteurs. De même pour q avec u_k. Finalement, on a réussi à écrire x sous la forme d'un produit d'au plus $(\omega - 1)(\varphi(b') + \nu_p(d) - 1) + \varphi(b') + \nu_q(d) - 1$ facteurs irréductibles, comme souhaité.

Commentaire des correcteurs : L'exercice est réussi par une poignée d'élèves. Il semble que la notion d'irréductibilité a posé des problèmes de compréhension, montrer que tout nombre de S peut s'écrire comme un nombre fini d'éléments irréductibles ne répondait pas à l'énoncé. Enfin, il est regrettable que pour certains, les copies rendues pour ce problème d'envoi soient pratiquement illisibles.

Exercice 18. Pour tout entier $k \geqslant 1$, on note $p(k)$ le plus petit nombre premier ne divisant pas k. Soit $(a_n)_{n\in\mathbb{N}}$ une suite telle que $a_0 \in \mathbb{N}^*$ et pour tout $n \geqslant 0$, a_{n+1} est le plus petit entier strictement positif différent de $a_0, \dots, a_n$ tel que $a_n^{a_{n+1}} - 1$ est divisible par $p(a_n)$. Démontrer que tout entier strictement positif apparaît une unique fois dans la suite $(a_n)_{n\in\mathbb{N}}$.

Solution de l'exercice 18 Déjà notons que la suite est bien définie : si $a_1, \dots, a_n$ sont construits, comme a_n est premier avec $p(a_n)$, il existe une infinité d'entiers k tels que $a_n^k \equiv 1 \pmod{p(a_n)}$ qui sont tous les multiples de l'ordre de a_n modulo $p(a_n)$. En particulier, il existe au moins un de ces entiers n'apparaissant pas parmi $a_1, \dots, a_n$, donc a_{n+1} existe bien.
Notons que chaque entier apparaît au plus une fois dans la suite par construction. Il faut donc montrer que tous apparaissent au moins une fois. Supposons qu'il existe un entier N qui n'apparaît pas dans la suite (x_n), on prend alors N minimal. On note N_0 un entier tel que si $n \geqslant N_0$, $a_n > N$.
Montrons que pour tout premier q, il existe un nombre fini de n tels que $p(a_n) = q$. Supposons que ce n'est pas le cas, et fixons q un nombre premier tel que $p(a_n) = q$ pour une infinité de n. On se donne alors $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $p(a_{\phi(n)}) = q$. Notons alors que tout multiple de $q-1$ apparaît : en effet si on fixe M un multiple de $q-1$, alors comme les $p(a_{\phi(n)+1})$ sont deux à deux distincts, il existe n tel que $a_{\phi(n)+1} > M$. Or comme $q-1$ divise M, $a_{\phi(n)}^M \equiv 1 \pmod{q-1}$ par petit Fermat, ce qui contredit la définition de $a_{\phi(n)+1}$.
Ainsi tous les multiples de $q-1$ apparaissent. on note $p_1 < \cdots < p_k$ les nombres premiers strictement inférieurs à q. On sait que pour tout $j \geqslant 1$, $(p_1 \dots p_k)^{j(q-1)}$ est congru à 1 modulo q, divisible par $q-1$ pour j assez grand (car tous les facteurs de $q-1$ sont parmi $p_1, \dots, p_k$) donc apparaît dans la suite, et vérifie $p\left((p_1 \dots p_k)^{j(q-1)}\right) = q$. Comme il y a une infinité de tels termes, il existe $N_1 > N_0$ tel que $a_{N_1} = (p_1 \dots p_k)^{j(q-1)}$ pour j assez grand. Ainsi $a_{N_1}^N \equiv 1 \pmod{q}$, ce qui contredit le fait que $a_{N_1+1} > N$.
Ainsi on a bien prouvé que pour tout premier q, il existe un nombre fini de n tels que $p(a_n) = q$. En particulier, pour tout $M \in \mathbb{N}$, comme la suite $(p(a_n))$ prend un nombre fini de fois chaque valeurs entre 1 et M, à partir d'un certain rang $p(a_n) > M$, donc $(p(a_n))$ tend vers $+\infty$. En particulier, pour tout k, à partir d'un certain rang, $p_1 \dots, p_k$ divise a_n.
Soit k et m tels que $p_1 \dots p_k$ divise a_m, p_{k+1} ne divise pas a_m, et $p_1 \dots p_{k+1}$ divise a_n pour tout $n \geqslant m+1$. On a alors $p(a_m) = p_{k+1}$, et $a_n^{p_1 \cdots p_k p_{k+1}} \equiv 1 \pmod{p_{k+1}}$. Or par Petit Fermat, $a_n^{p_1 \cdots p_k p_{k+1}} \equiv a^{p_1 \cdots p_k} \pmod{p_{k+1}}$, donc pour tout i vérifiant $1 \leqslant i \leqslant p_k - 1$, $a^{ip_1 \cdots p_k} \equiv 1 \pmod{p_{k+1}}$. Ainsi pour tout i vérifiant $1 \leqslant i \leqslant p_k - 1$, $ip_1 \dots p_k$ apparaît dans la suite (a_n). En prenant i un inverse de $p_1 \dots p_k$ modulo $p_{k+1} - 1$ dans $\{1, \dots, p_{k+1} - 1\}$, on a alors que $(ip_1 \dots p_k)^N \equiv N \pmod{p_{k+1}}$, donc si $a_n = ip_1 \dots p_k$, alors $a_{n+1} < N$, donc $n \leqslant N_0$. Ainsi si de tels k, m existent, alors p_k divise $a_1 \dots a_{n+1}$, donc k est borné.
Or pour tout $K \in \mathbb{N}$, on peut trouver $k \geqslant K$ et m tels que $p_1 \dots p_k$ divise a_m, p_{k+1} ne divise pas a_m, et $p_1 \dots p_{k+1}$ divise a_n pour tout $n \geqslant m+1$. En effet, notons pour tout $k \geqslant 1$ r_k le premier rang à partir duquel $p_1 \dots p_k$ divise a_n. La suite (r_j) est croissante, et ne peut être stationnaire sinon un a_n serait divisible par tous les nombres premiers. Donc elle tend vers $+\infty$, pour tout K, il existe $k \geqslant K$ tel que $r_{k+1} > r_k$. Ainsi $a_{r_{k+1}-1}$ est divisible par $p_1 \dots p_k$ car $r_{k+1} - 1 \geqslant r_k$, et pas par p_{k+1}. Mais tous les termes après r_{k+1} sont divisibles par $p_1 \dots p_{k+1}$, donc $m = r_{k+1} - 1$ convient. On a donc bien obtenu que pour tout $K \in \mathbb{N}$, on peut trouver $k \geqslant K$ et m tels que $p_1 \dots p_k$ divise a_m, p_{k+1} ne divise pas a_m, et $p_1 \dots p_{k+1}$ divise a_n pour tout $n \geqslant m+1$, donc on a abouti à une contradiction.
Ainsi chaque entier apparaît une unique fois dans la suite.

Commentaire des correcteurs : L'exercice est réussi par une poignée d'élèves. Certains ont utilisé des résultats moins élémentaires que le corrigé par exemple le postulat de Bertrand.