PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE

À RENVOYER AU PLUS TARD LE 15 FÉVRIER 2025

Les consignes suivantes sont à lire attentivement :

- Le groupe junior est constitué des élèves nés en 2010 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. Trouver tous les entiers $n \in \mathbb{Z}$ tels que $2n+4$ divise $6n+26$.

Solution de l'exercice 1
Soit $n \in \mathbb{Z}$ tel que $2n+4$ divise $6n+26$. Comme $2n+4$ divise $3(2n+4) = 6n+12$, alors $2n+4$ divise la différence $(6n+26)-(6n+12) = 14$. Celà implique en divisant par 2 de part et d'autre que $n+2$ divise 7. Les seuls diviseurs de 7 sont les 4 éléments de l'ensemble $E = \{\pm 1, \pm 7\}$, donc $n+2 \in E$, d'où $n \in \{-9, -3, -1, 5\}$. Réciproquement, ces 4 valeurs sont bien toutes solution.

Exercice 2. Trouver le plus grand entier strictement positif d tel que pour tout entier positif a, on ait $d \mid a^7 - a$.

<u>*Solution de l'exercice 2*</u>
Puisque $2^7 - 2 = 126 = 2 \times 3^2 \times 7$, il s'ensuit que $d|126$, et que d ne peut être divisible que par les termes intervenant dans la décomposition en facteurs premiers de 1266. Grâce au petit théorème de Fermat, on sait que pour tout entier $a \in \mathbb{Z}$,

$$\begin{aligned}
a &\equiv 0 \pmod 7 \text{ ou } a^7 \equiv 1 \pmod 7; \\
a &\equiv 0 \pmod 3 \text{ ou } a^2 \equiv 1 \pmod 3; \\
a &\equiv 0 \pmod 2 \text{ ou } a^1 \equiv 1 \pmod 2.
\end{aligned}$$

De la première ligne, on déduit que $7|a^7 - a$ pour tout entier a, et donc $7|d$. De la deuxième ligne on déduit pour tout entier a que soit $3|a$, soit $a^2 \equiv 1 \pmod 3$ qui implique à son tour $a^6 \equiv 1 \pmod 3$. Dans ces deux cas, $3|a^7 - a$, d'où $3|d$. De même en partant de la troisième ligne on obtient $2|d$. Comme $2, 3, 7$ sont premiers entre eux, on déduit que $2 \times 3 \times 7 = 42$ divise d.
Il reste à décider si $d = 42$ ou si $d = 126$. Pour cela, on peut remarquer que $9|3^7$ mais que $9 \nmid 3$, ainsi 9 ne divise pas $3^7 - 3$ donc 9 ne divise pas d. Cela permet de conclure que le pgcd recherché vaut $d = 42$.

Exercice 3. Trouver tous les entiers strictement positifs x, y, z tels que :

$$x! + y^2 + 1 = z!.$$

Solution de l'exercice 3

Soit (x, y, z) un triplet solution. Clairement, $x < z$, ainsi tout diviseur de $x!$ divise aussi $z!$. Concentrons nous sur le terme restant. On remarque en regardant l'équation modulo 3 que y^2+1 n'est jamais divisible par 3, ainsi $x!$ ne peut pas l'être, sinon $z!$ le serait aussi et l'on obtiendrait une contradiction. Donc $x < 3$, c'est à dire $x \in \{1, 2\}$. Étudions ces deux cas séparément :

— Si $x = 2$, alors $y^2 + 3 = z!$. Donc $z > 2$ et ainsi 3 divise chacun des membres et donc aussi y. Ainsi 9 divise y^2. Si 9 divisait aussi $z!$ (c'est à dire si $z > 5$), alors 9 devrait a fortiori diviser $z! - y^2 = 3$, ce qui est impossible. Donc $3 \leqslant z \leqslant 5$. On teste facilement ces trois possibilités, dont aucune ne convient.

— Si $x = 1$, alors $y^2 + 2 = z!$, et on peut faire le même raisonnement avec 2 et 4. En effet on remarque que $z > 2$ puisque $y > 0$ (et donc $y^2 + 2 > 2$). Ainsi 2 divise $z! - 2$ et donc y, d'où 4 divise y^2. Comme 4 divise y^2 et 4 ne divise pas 2, alors 4 ne peut diviser $z!$, ce qui force $z < 4$, donc $z = 3$. Ainsi la seule solution possible dans ce cas est $(x, y, z) = (1, 2, 3)$.

Pour conclure, le seul triplet solution est $(1, 2, 3)$. On vérifie aisément qu'il fonctionne.

Exercice 4. Trouver tous les triplets de nombres premiers (p, q, r) tels que $p^q + p^r$ soit un carré parfait.

Solution de l'exercice 4 Soit (p, q, r) un triplet solution.

— Commençons par traiter le cas $q = r$. Dans ce cas, $2p^q$ est un carré parfait, ce qui implique que $2|p$, d'où $p = 2$ puisqu'il est premier. Ainsi, on cherche les premiers q tels que 2^{q+1} est un carré parfait, ce qui est le cas si et seulement q est impair. On a donc démontré que les seules solutions avec $q = r$ sont les triplet $(2, q, q)$ où q est un nombre premier impair.

— Sinon, sans perdre de généralité on suppose $q < r$, et on factorise : il existe un entier naturel n tel que
$$p^q(1 + p^{r-q}) = n^2.$$
La valuation p-adique est égale à q à gauche, et doit être paire à droite, donc q est pair, c'est à dire $q = 2$. Il existe donc un entier naturel m tel que $n = mp$. On passe le 1 de l'autre côté pour obtenir une identité remarquable :
$$p^{r-2} = (m - 1)(m + 1).$$
Cela indique que le seul facteur premier possible pour $m-1$ et $m+1$ est p, donc ces deux nombres sont des puissances de p. En particulier $m - 1$ doit diviser $m + 1$, ce qui implique $m - 1|2$, et en testant tous les cas pour m on trouve $(p, q, r) = (3, 2, 3)$ et $(p, q, r) = (2, 2, 5)$ qui conviennent.

Ainsi, les solutions sont $(2, 2, 5)$, $(2, 5, 2)$, $(3, 2, 3)$, $(3, 3, 2)$ et tous les $(2, q, q)$ pour q premier impair.

Exercice 5. Pour deux entiers strictement positifs quelconques a et b, on définit l'opération

$$a \star b = \frac{a-b}{\operatorname{pgcd}(a,b)}.$$

Trouver tous les entiers strictement positifs n tels que pour tout entier strictement positif $m < n$, $n \star m$ est premier avec n.

Solution de l'exercice 5

Démontrons que les solutions sont les puissances de premiers. En effet, si $n = p^k$ avec p premier et k un entier positif ou nul, alors tout entier $m < n$ se décompose en $m = p^{k'}\ell$ avec $k' < k$ et ℓ entier premier avec p, et

$$n \star m = \frac{p^k - p^{k'}\ell}{p^{k'}} = p^{k-k'} - \ell.$$

Comme ℓ est premier avec p et $k > k'$, alors $n \star m$ est premier avec p et donc avec n, ce qui conclut.
Réciproquement, on suppose que n n'est pas une puissance de premier. Soit p le plus petit diviseur premier de n, alors n se décompose comme $n = p^k\ell$, avec $\ell > p$ premier avec p et $k \geqslant 1$. Dans ce cas on peut choisir $m = n - p^{k+1}$ qui est bien strictement positif et strictement inférieur à n. On a alors

$$n \star m = \frac{n-(n-p^{k+1})}{\operatorname{pgcd}(p^k\ell, p^k(\ell-p))} = \frac{p^{k+1}}{p^k} = p \neq 1,$$

ce qui est en contradiction avec la condition de l'énoncé.

Exercice 6. Soit $n \geqslant 5$ un entier impair, Alice et Bob jouent au jeu suivant : Ils sélectionnent chacun leur tour, en commençant par Alice, un entier entre 1 et $n-1$ qui n'a pas déjà été pris à un tour précédent. On note A l'ensemble des entiers choisis par Alice et B l'ensemble de ceux choisis par Bob. Après cela, Alice donne deux entiers distincts $x_1, x_2 \in A$ à Bob, qui choisit ensuite deux entiers distincts $y_1, y_2 \in B$. Bob gagne si et seulement si :

$$\left(x_1x_2(x_1-y_1)(x_2-y_2)\right)^{\frac{n-1}{2}} \equiv 1 \pmod{n}.$$

Pour quels n Bob a-t-il une stratégie gagnante ?

Solution de l'exercice 6
Bob a une stratégie gagnante si et seulement si n est premier.

En effet, si n n'est pas premier, il existe $1 < d < n$ tel que $d \mid n$, Alice peut donc choisir d au premier tour. Elle peut ensuite donner $x_1 = d$ de sorte que : $d \mid \left(x_1x_2(x_1-y_1)(x_2-y_2)\right)^{\frac{n-1}{2}}$.
Ainsi, si Bob gagnait, on aurait :

$$d \mid n \mid \left(x_1x_2(x_1-y_1)(x_2-y_2)\right)^{\frac{n-1}{2}} - 1.$$

Donc $d \mid 1$, absurde. Ainsi, si n n'est pas premier, Alice dispose d'une stratégie gagnante, donc Bob n'en dispose pas.

Réciproquement, supposons que $n = p$ avec p un nombre premier, Bob peut suivre la stratégie suivante :

- À chaque fois qu'Alice choisit un entier a, Bob prend l'entier $p - a$. En effet, cet entier est disponible car $p - a \neq a$ (sinon $p = 2a$ et $p \geqslant 5$ serait pair.) et car s'il avait été pris à un tour précédent par Alice ou Bob, l'autre aurait pris l'entier a.
- Ensuite, quand Alice donne x_1, x_2, Bob choisit $y_1 = p - x_1$ et $y_2 = p - x_2$ qu'il a préalablement sélectionnés de sorte que :

$$\left(x_1x_2(x_1-y_1)(x_2-y_2)\right)^{\frac{p-1}{2}} \equiv \left((-1)^2x_1^2x_2^2\right)^{\frac{p-1}{2}} \equiv (x_1x_2)^{p-1} \equiv 1\ [p],$$

  d'après le petit-théorème de Fermat car $p \nmid x_1, x_2$ donc $p \nmid x_1x_2$ puisque p est premier.

Bob a donc gagné.

Ainsi, on a bien montré que Bob a une stratégie gagnante si et seulement si n est premier.

Exercice 7. Soient $a_1, a_2, \ldots a_{2025}$ des entiers avec $a_1 = 2^{2024} + 1$ et tels que pour tout $n \leqslant 2024$, a_{n+1} soit le plus grand facteur premier de $a_n^2 - 1$. Combien vaut $a_{2024} + a_{2025}$?

<u>*Solution de l'exercice 7*</u>

Supposons qu'il existe un entier $k \leqslant 2024$ tel que a_k soit pair, alors $a_k \neq a_1$ donc a_k est un nombre premier et $a_k = 2$.

Alors a_{k+1} est le plus grand facteur premier de $4 - 1 = 3$, donc $a_{k+1} = 3$. Ensuite, si $k + 1 \leqslant 2024$, a_{k+2} est le plus grand facteur premier de $9 - 1 = 8$, donc $a_{k+2} = 2$, puis $a_{k+3} = 3$ et etc... Ainsi, (a_n) est 2-périodique à partir du rang k, on en déduit que : $\{a_{2024}, a_{2025}\} = \{2, 3\}$ donc $a_{2024} + a_{2025} = 5$.

Dans le cas contraire, a_k est impair pour tout $k \leqslant 2024$. Nous allons montrer que $a_{2024} \leqslant 3$ en prouvant par récurrence que pour tout $1 \leqslant k \leqslant 2024$, $a_k \leqslant 2^{2025-k} + 1$. On note $\mathcal{P}(k)$ cette propriété.

<u>Initialisation :</u> L'énoncé nous assure que $\mathcal{P}(1)$ est vraie.

<u>Hérédité :</u> Soit $k \leqslant 2023$ tel que $\mathcal{P}(k)$ soit vraie. Alors par hypothèse a_k est impair donc $\frac{a_k-1}{2}$ et $\frac{a_k+1}{2}$ sont entiers, or :

$$a_k^2 - 1 = (a_k - 1)(a_k + 1) = 4\left(\frac{a_k - 1}{2}\right)\left(\frac{a_k + 1}{2}\right).$$

De plus, a_{k+1} est impair et premier, donc $a_{k+1} \nmid 4$ et par le lemme d'Euclide, a_{k+1} divise $\frac{a_k+1}{2}$ ou $\frac{a_k-1}{2}$, il est donc inférieur à un de ces deux nombres et donc d'après $\mathcal{P}(k)$:

$$a_{k+1} \leqslant \frac{a^k + 1}{2} \leqslant \frac{2^{2025-k} + 2}{2} = 2^{2025-(k+1)} + 1.$$

Ceci prouve $\mathcal{P}(k+1)$ et nous permet de conclure par récurrence que $a_{2024} \leqslant 3$.

Or a_{2024} est un nombre premier impair, donc $a_{2024} \geqslant 3$, ainsi $a_{2024} = 3$ et $a_{2025} = 2$.

Par conséquent $\boxed{a_{2024} + a_{2025} = 5}$ dans tous les cas.

Exercice 8. Soit n un entier strictement positif tel que $n^5+n^3+2n^2+2n+2$ soit le cube d'un entier. Montrer que $2n^2+n+2$ n'est pas le cube d'un entier.

<u>*Solution de l'exercice 8*</u>
On étudie chaque quantité modulo 9 :

n	n^2	n^3	n^5	$n^5+n^3+2n^2+2n+2$	$2n^2+n+2$
0	0	0	0	2	2
1	1	1	1	-1	-4
2	4	-1	-4	0	3
3	0	0	0	-1	-4
4	-2	1	-2	-4	2
-4	-2	-1	2	0	3
-3	0	0	0	-4	-1
-2	4	1	4	2	-1
-1	1	-1	-1	0	3

Ce tableau nous permet de remarquer que les seuls cubes modulo 9 sont $0, 1, -1$, or il n'y a aucune ligne sur laquelle les deux quantités considérées appartiennent à cet ensemble : elles ne peuvent être en même temps des cubes parfaits.

Exercice 9. Soient a et b deux entiers strictement positifs. On suppose qu'il existe une infinité de paires (m, n) d'entiers strictement positifs tels que $m^2 + an + b$ et $n^2 + am + b$ sont tous deux des carrés parfaits. Montrer que a divise $2b$.

Solution de l'exercice 9

Sans perte de généralité, on suppose que toutes les paires (m, n) vérifient $m \geqslant n$, pour chacune d'entre elle, il existe $c \in \mathbb{N}^*$ tel que $m^2 + an + b = (m + c)$. Mais alors :

$$(m + c)^2 = m^2 + an + b \leqslant m^2 + am + b \leqslant m^2 + 2bam + a^2b \cdot b = (m + ab)^2$$

Ainsi, $1 < c \leqslant ab$ donc c ne peut prendre qu'un nombre fini de valeurs. Par le principe des tiroirs infinis, il existe un c tel que $m^2 + an + b = (m + c)^2$ pour une infinité de (m, n). On ne considère dans la suite plus que ces paires-ci.

Cela revient à dire que $an + b = 2cm + c^2$ $(*)$, ou encore que $m = \frac{an+b-c^2}{2c}$. Mais alors :

$$n^2 + am + b = n^2 + \frac{a^2}{2c}n + b + \frac{ab}{2c} - \frac{ac}{2} \text{ est un carré pour une infinité de paires } (m, n)$$

On pose $p = \frac{a^2}{2c}$ et $q = b + \frac{ab}{2c} - \frac{ac}{2}$. L'égalité $(*)$ nous dit que pour n fixé, il existe un seul m tel que (m, n) convienne. Ainsi, on trouve qu'il existe une infinité de n tels que $f(n) = n^2 + pn + q$ soit un carré parfait. Montrons alors que $\left(\frac{p}{2}\right)^2 = q$.

Notons $d = q - \left(\frac{p}{2}\right)^2 \neq 0$, de sorte que $f(n) = \left(n + \frac{p}{2}\right)^2 + d$. Il existe alors une infinité de n tels que $(4c)^2 f(n) = (4cn + a^2)^2 + d(4c)^2$ soit un carré parfait, or pour n assez grand (supérieur à $d(4c)^2$) on a :

$$(4cn + a^2 - 1) < (4cn + a^2)^2 + d(4c)^2 < (4cn + a^2 + 1)$$

Ainsi, il est nécessaire que $d = 0$, ce qui est le résultat voulu. Nous avons donc montré que :

$$\left(\frac{a^2}{4c}\right)^2 = \frac{a(b - c^2)}{2c} + b \text{ donc } a^4 = 8ac(b - c^2) + 16bc^2 \ (**)$$

Soit maintenant p un nombre premier impair, on note x, y, z les valuations p-adiques de a, b, c respectivement. On veut montrer que $y \geqslant x$. Si $z \geqslant x$ alors d'après $(*)$ on a $b = an + c(2m + c)$ donc p^x divise a, c donc il divise b et $y \geqslant x$. Sinon, c'est que $z \leqslant x - 1$ mais alors $v_p(16bc^2) = y + 2z$ et $v_p(8ac(b - c^2)) \geqslant x + z + \min(y, 2z)$ et $(**)$ nous donne :

$$16bc^2 = 8ac(b - c^2) - a^4 \text{ donc } y + 2z \geqslant \min\left(4x, x + z + \min(y, 2z)\right)$$

Si $y + 2z \geqslant 4x$ alors on a $4x \leqslant y + 2x - 2$ donc $y \geqslant 2x + 2 \geqslant x$. Sinon, on a $y + 2z \geqslant x + z + \min(y, 2z)$ donc $\max(y, 2z) \geqslant x + z$, mais $z < x$ donc $2z < x + z$ et donc $y \geqslant x + z \geqslant x$.

Ainsi $v_p(a) \leqslant v_p(b)$ dans tous les cas.

Il reste pour conclure à montrer que $v_2(a) \leqslant v_2(b) + 1$, on note à nouveau x, y, z les valuations 2-adiques de a, b, c. Par le même argument que précédemment, si $z \geqslant x - 1$ alors $(*)$ nous donne que $y \geqslant x - 1$. On suppose donc $z \leqslant x - 2$ et en adaptant le cas précédent pour tenir compte des coefficients 8 et 16 on trouve :

$$4 + y + 2z \geqslant \min\left(4x, 3 + x + z + \min(y, 2z)\right)$$

Si $4+y+2z \geqslant 4x$, alors $4x \leqslant 4+y+2x-4$ donc $y \geqslant 2x \geqslant x-1$. Sinon, on a $4+\max(y,2z) \geqslant 3+x+z$ donc $\max(y,2z) \geqslant x-1+z$, mais $z < x-1$ donc $y \geqslant x-1+z \geqslant x-1$.
On a donc bien que $v_2(a) \leqslant v_2(2b)$ et ceci achève de prouver que a divise $2b$.

Exercices Seniors

Exercice 10. Trouver le plus grand entier strictement positif d tel que pour tout entier positif a, on ait $d \mid a^7 - a$.

<u>*Solution de l'exercice 10*</u>
Puisque $2^7 - 2 = 126 = 2 \times 3^2 \times 7$, il s'ensuit que $d|126$, et que d ne peut être divisible que par les termes intervenant dans la décomposition en facteurs premiers de 1266. Grâce au petit théorème de Fermat, on sait que pour tout entier $a \in \mathbb{Z}$,

$$\begin{aligned}
a &\equiv 0 \pmod 7 \text{ ou } a^7 \equiv 1 \pmod 7; \\
a &\equiv 0 \pmod 3 \text{ ou } a^2 \equiv 1 \pmod 3; \\
a &\equiv 0 \pmod 2 \text{ ou } a^1 \equiv 1 \pmod 2.
\end{aligned}$$

De la première ligne, on déduit que $7|a^7 - a$ pour tout entier a, et donc $7|d$. De la deuxième ligne on déduit pour tout entier a que soit $3|a$, soit $a^2 \equiv 1 \pmod 3$ qui implique à son tour $a^6 \equiv 1 \pmod 3$. Dans ces deux cas, $3|a^7 - a$, d'où $3|d$. De même en partant de la troisième ligne on obtient $2|d$. Comme $2, 3, 7$ sont premiers entre eux, on déduit que $2 \times 3 \times 7 = 42$ divise d.
Il reste à décider si $d = 42$ ou si $d = 126$. Pour cela, on peut remarquer que $9|3^7$ mais que $9 \nmid 3$, ainsi 9 ne divise pas $3^7 - 3$ donc 9 ne divise pas d. Cela permet de conclure que le pgcd recherché vaut $d = 42$.

Exercice 11. Trouver tous les entiers strictement positifs x, y, z tels que :

$$x! + y^2 + 1 = z!.$$

Solution de l'exercice 11

Soit (x, y, z) un triplet solution. Clairement, $x < z$, ainsi tout diviseur de $x!$ divise aussi $z!$. Concentrons nous sur le terme restant. On remarque en regardant l'équation modulo 3 que y^2+1 n'est jamais divisible par 3, ainsi $x!$ ne peut pas l'être, sinon $z!$ le serait aussi et l'on obtiendrait une contradiction. Donc $x < 3$, c'est à dire $x \in \{1, 2\}$. Étudions ces deux cas séparément :

— Si $x = 2$, alors $y^2 + 3 = z!$. Donc $z > 2$ et ainsi 3 divise chacun des membres et donc aussi y. Ainsi 9 divise y^2. Si 9 divisait aussi $z!$ (c'est à dire si $z > 5$), alors 9 devrait a fortiori diviser $z! - y^2 = 3$, ce qui est impossible. Donc $3 \leqslant z \leqslant 5$. On teste facilement ces trois possibilités, dont aucune ne convient.

— Si $x = 1$, alors $y^2 + 2 = z!$, et on peut faire le même raisonnement avec 2 et 4. En effet on remarque que $z > 2$ puisque $y > 0$ (et donc $y^2 + 2 > 2$). Ainsi 2 divise $z! - 2$ et donc y, d'où 4 divise y^2. Comme 4 divise y^2 et 4 ne divise pas 2, alors 4 ne peut diviser $z!$, ce qui force $z < 4$, donc $z = 3$. Ainsi la seule solution possible dans ce cas est $(x, y, z) = (1, 2, 3)$.

Pour conclure, le seul triplet solution est $(1, 2, 3)$. On vérifie aisément qu'il fonctionne.

Exercice 12. Soit a, b deux entiers strictement positifs. Martin donne à chacun des $n > 1$ élèves du stage de Valbonne un rectangle de dimension $a \times b$. Chaque élève découpe ensuite son rectangle en plusieurs petits carrés identiques de côté entier (leur taille peut changer selon l'élève). Martin récupère ensuite tous les petits carrés et se rend compte qu'il y en a un nombre premier. Montrer que $a = b$.

Solution de l'exercice 12

Supposons par l'absurde que $a \neq b$, sans perte de généralité, disons que $b > a$. Écrivons la fraction $\frac{b}{a} = \frac{x}{y} > 1$ sous sa forme irréductible, avec donc $\mathrm{PGCD}(x, y) = 1$. Remarquons que $x > 1$ donc il existe un nombre premier p qui divise x, donc p ne divise pas y.

Pour tout $i \in \{1, \dots, n\}$, si l'élève i a découpé des carrés de dimension d_i, on pose $k_i = \frac{a}{d_i} \in \mathbb{N}$ et $l_i = \frac{b}{d_i} \in \mathbb{N}$, de sorte qu'il ait découpé $k_i l_i$ carrés. Mais alors $\frac{l_i}{k_i} = \frac{a}{b} = \frac{x}{y}$ donc $x k_i = y l_i$, donc $p \mid y l_i$ donc $p \mid l_i$ par le lemme d'Euclide.
Ainsi, chaque élève a découpé un nombre de carrés divisible par p, donc p divise le nombre total N de carrés, mais puisqu'il y a $n > 1$ enfants, $N > p$, donc N n'est pas premier, ce qui est absurde.
Ainsi on a bien $a = b$.

Exercice 13. Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite infinie d'entiers telle que :

— Pour tous $m, n \in \mathbb{N}^*$, $a_{mn} = a_m a_n$.

— Il existe une infinité de $n \in \mathbb{N}^*$ tels que $a_1, \ldots, a_n$ soit une permutation de $1, \ldots, n$.

Montrer que $a_n = n$ pour tout $n \in \mathbb{N}^*$

Solution de l'exercice 13

On va prouver la propriété suivante par récurrence forte sur $k \geqslant 2$: pour tout entier $0 < m < k$, $a_m = m$.

Initialisation : On initialise avec $k = 2$, en effet on a bien $a_1^2 = a_1$, d'où $a_1 = 1$. En effet on ne peut avoir $a_1 = 0$ car il existe un $n \geqslant 1$ tel que $\{a_1, \ldots, a_n\}$ est en bijection avec $\{1, \ldots, n\}$ qui ne contient pas 0.

Hérédité : Soit $k > 1$, nous supposons maintenant que $a_m = m$ pour tout entier $0 < m < k$, et démontrons que $a_k = k$. On choisit pour cela un n assez grand qui vérifie la seconde propriété de l'énoncé. On définit alors t comme le plus grand entier tel que $k^t \leqslant n$, en s'assurant que n soit pris suffisamment grand pour que $(k+1)^t > k^{t+1}$ (un t assez grand vérifiera cette inégalité qui se réécrit de façon équivalente comme $(1 + 1/k)^t > k$, où le terme de droite est constant et où le terme de gauche tend vers l'infini). Pour ce choix de n et de t, il s'ensuit que $a_{k^t} \leqslant n < k^{t+1} < (k+1)^t$, où la première inégalité vient du fait que $a_{k^t} \in \{1, \ldots, n\}$ puisque $k^t \leqslant n$ et n vérifie la propriété de permutation. De plus, la propriété de multiplicativité de la suite peut s'utiliser de façon répétée pour obtenir $a_k^t = a_{k^t}$, ce qui mène en prenant les racines dans la chaîne d'inégalités ci-dessus à l'inégalité $a_k < k + 1$. Il reste à démontrer que a_k ne peut être strictement plus petit que k, ce qui est vrai car si ce n'était pas le cas, la suite aurait deux termes égaux, ce qui est rendu impossible par le choix d'un n assez grand vérifiant la propriété de permutation (par exemple le même n que choisi précédemment).

Exercice 14. Trouver tous les entiers strictement positifs n, m tels que nm divise $(2^{2^n}+1)(2^{2^m}+1)$.

Solution de l'exercice 14 Soient n et m des entiers solution. Sans perdre de généralité, on suppose $n \geqslant m$, et on commence par traiter le cas $m > 1$. Dans ce cas, m admet un diviseur premier p. De plus, p est impair car m l'est aussi : il divise $(2^{2^n}+1)(2^{2^m}+1)$ qui est impair. Comme p est premier, p divise l'un des $2^{2^k}+1$, où $k \in \{n, m\}$. En particulier,

$$2^{2^k} \equiv -1 \pmod{p} \text{ et donc } 2^{2^{k+1}} \equiv 1 \pmod{p}.$$

Donc l'ordre modulaire $\omega_p(2)$ de 2 modulo p divise 2^{k+1} mais ne divise pas 2^k, ainsi $\omega_p(2) = 2^{k+1}$. D'après le petit théorème de Fermat, $\omega_p(2)|p-1$, d'où

$$p \equiv 1 \pmod{2^{k+1}}.$$

Comme $p > 1$, on en déduit $p \geqslant 2^{k+1}+1 \geqslant 2^{m+1}+1$, mais on sait que $p \leqslant m$. On obtient donc

$$m \geqslant 2^{m+1}+1,$$

ce qui est faux pour tout entier $m > 1$. On peut donc en déduire que les seules solutions possibles avec $n \geqslant m$ vérifient $m = 1$.
La condition de l'énoncé se réécrit alors

$$n|5(2^{2^n}+1).$$

Supposons que n admette un facteur premier $p \neq 5$. Par le même raisonnement que précédemment, il s'ensuit que $n \geqslant 2^{n+1}+1$, de nouveau absurde. Donc il existe un entier naturel ℓ tel que $n = 5^\ell$. Il nous reste à examiner la valuation 5-adique du terme de droite. On a dès lors que $n > 1$,

$$2^{2^n}+1 \equiv 1+1 \equiv 2 \pmod{5},$$

d'où $\ell < 2$. Il ne nous reste qu'à tester $n = 1$ et $n = 5$ qui sont bien solution. Pour conclure, l'ensemble des solutions est

$$\{(1,1), (1,5), (5,1)\}.$$

Exercice 15. Alice découvre un entier $N > 1$ écrit au tableau, puis chaque jour elle efface l'entier x sur le tableau et le remplace par $\sqrt[3]{x}$ si ce nombre est entier, par $2x+1$ sinon. Montrer que si Alice vit suffisamment longtemps, elle finira par écrire un entier supérieur à 2025^{2025}.

Solution de l'exercice 15

On note a_n le nombre écrit par Alice le n-ème jour de sorte que $a_0 = N$. Remarquons que l'on aura toujours $a_n > 1$ et entier. Ainsi, si a_n est un cube pour un certain $n \in \mathbb{N}$, on aura $1 < a_{n+1} = \sqrt[3]{a_n} < a_n$. Par conséquent, il n'est pas possible qu'Alice réalise une infinité de fois d'affilée l'opération $x \mapsto \sqrt[3]{x}$. On en déduit qu'Alice réalise une infinité de fois l'opération $x \mapsto 2x+1$ (sinon, après la dernière de ces opérations elle ne ferait que prendre la racine cubique).

On s'intéresse maintenant à la suite $u_n = v_2(a_n + 1)$ où $v_2(m)$ désigne le plus grand entier naturel α tel que $2^\alpha \mid m$ pour m entier. Soit $n \in \mathbb{N}$, il y a deux cas :

— Si $a_{n+1} = 2a_n + 1$ alors $u_{n+1} = v_2(2(a_n+1)) = 1 + v_2(a_n+1) = 1 + u_n$. Lorsque c'est l'opération $x \mapsto 2x+1$ qui est faite, u_n augmente de 1.

— Si $a_{n+1} = \sqrt[3]{a_n}$ alors on a :

$$a_n + 1 = a_{n+1}^3 + 1 = (a_{n+1} + 1)(a_{n+1}^2 - a_{n+1} + 1)$$

Or a_{n+1}^2 et a_{n+1} sont de même parité, donc $a_{n+1}^2 - a_{n+1}$ est pair et $(a_{n+1}^2 - a_{n+1} + 1)$ est impair. On en déduit : $u_n = v_2(a_n+1) = v_2(a_{n+1}+1) + v_2(a_{n+1}^2 - a_{n+1} + 1) = u_{n+1}$

Ainsi, la suite (u_n) ne décroît jamais et est augmentée de 1 un nombre infini de fois. Par conséquent, pour tout M arbitrairement grand il existe n tel que $v_2(a_n+1) \geqslant M$, donc $2^M \mid a_n + 1$ donc $a_n \geqslant 2^M - 1$. Il suffit de choisir M tel que $2^M > 2025^{2025}$.

Ainsi, il y aura bien un entier supérieur à 2025^{2025} écrit au tableau.

Exercice 16. Trouver toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que pour tout couple (a, b) d'entiers strictement positifs $f(a)f(a+b) - ab$ soit un carré parfait.

<u>*Solution de l'exercice 16*</u>
Remarquons que la fonction identité est solution, en effet pour tout $(a, b) \in (\mathbb{N}^*)^2$ la condition devient $a(a+b)-ab = a^2$ qui est un carré parfait. Nous allons montrer qu'il s'agit de la seule fonction solution.

Soit f une fonction solution. Pour p premier et $n \in \mathbb{N}^*$, nous noterons $v_p(n)$ la *valuation p-adique* de n, c'est-à-dire la plus grande puissance de p qui divise n.

Nous allons commencer par montrer le résultat suivant :
<u>Lemme 1 :</u> Soit $n \in \mathbb{N}^*$ tel que $v_2(n)$ est impair, alors $f(n) \mid n$
<u>*Preuve :*</u> Supposons par l'absurde que $f(n) \nmid n$, alors il existe p premier tel que $v_p(f(n)) > v_p(n)$. On note $k = v_p(n)$, il y a deux cas :

— Si $p = 2$, alors par hypothèse k est impair. L'énoncé appliqué à $(a, b) = (n, 1)$ nous donne que $f(n)f(n+1) - n$ est un carré parfait.
Pourtant, $2^{k+1} \mid f(n)$ mais $2^{k+1} \nmid n$, donc 2^{k+1} ne divise pas $f(n)f(n+1) - n$; par contre, 2^k divise bien $f(n)f(n+1) - n$. Ainsi $v_2(f(n)f(n+1) - n) = k$ qui est impair, absurde pour un carré parfait.
— Si $p > 2$, il existe $r \in \mathbb{N}^*$ tel que $n = p^k r$ avec $p \nmid r$ et il existe d tel que $f(n) = p^{k+1}d$.
Par le même calcul que pour $p = 2$, on trouve que $v_p(f(n)f(n+1) - n) = k$, donc k est pair. Ainsi, p^k est un carré, mais pour tout $b \in \mathbb{N}^*$ la quantité suivante est un carré parfait :
$$f(n)f(n+b) - n = p^{k+1}d \cdot f(n+b) - p^k rb = p^k(pd \cdot f(n+b) - rb).$$
On en déduit que $pd \cdot f(n+b) - rb$ est un carré parfait pour tout $b \in \mathbb{N}^*$. Or $p > 2$, donc il existe $\frac{p-1}{2} \geqslant 1$ non-résidus quadratiques modulo p, soit x l'un d'entre eux. De plus $p \nmid r$ donc r est inversible modulo p, donc on peut choisir $b \equiv -r^{-1}x$ [p] de sorte que $pd \cdot f(n+b) - rb \equiv x[p]$ qui serait un résidu quadratique modulo p, absurde.

Nous avons donc dans tous les cas une contradiction, ainsi $f(n) \mid n$.

Nous pouvons maintenant prouver un second lemme :
<u>Lemme 2</u> : Soit $m > 4$ tel que $m \equiv 2$ [4], alors $f(m) = m$.
<u>*Preuve :*</u> Nous avons $f(m) \mid m$ car $v_2(m) = 1$ par le lemme précédent, supposons par l'absurde que $f(m) \neq m$, alors $f(m) \leqslant \frac{m}{2}$. Remarquons aussi que $f(2) \mid 2$ donc $f(2) \leqslant 2$.
On applique l'énoncé à $(a, b) = (2, m-2)$, il existe $x \in \mathbb{N}$ tel que :
$$x^2 = f(2)f(m) - 2(m-2) \leqslant 2 \cdot \frac{m}{2} - 2m + 4 = 4 - m < 0,$$
ce qui est absurde, ainsi $f(m) = m$.

Soit $n \in \mathbb{N}^*$, nous pouvons maintenant montrer que $f(n) = n$. Supposons par l'absurde que $f(n) < n$, soit $k \in \mathbb{N}^*$ arbitrairement grand, on pose $m = 4k+2$ et on applique l'énoncé à $(a, b) = (n, m-n)$ (on prend k tel que $m > n$) alors il existe $x \in \mathbb{N}$ tel que : $x^2 = f(n)f(m) - n(m-n) = n^2 + m(f(n) - n)$ par le lemme 2. Or pour m assez grand, cette expression est négative, ce qui est absurde, donc $f(n) \geqslant n$.

On suppose maintenant par l'absurde que $f(n) > n$ et on reprend les mêmes notations. Nous pouvons choisir k suffisamment grand pour que $n^2 + m(f(n) - n) > 4(f(n) - n)^2$ puisque $f(n) - n \neq 0$. On pose $x^2 = n^2 + m(f(n) - n)$ avec $x \in \mathbb{N}$ d'après l'énoncé de sorte que $x > 2(f(n) - n)$. Alors, on aussi

$f(m+4) = m+4$ car $m+4 \equiv m \equiv 2$ [4], ainsi $n^2 + (m+4)(f(n)-n)$ doit aussi être un carré parfait, pourtant :

$$x^2 < n^2 + (m+4)(f(n)-n) = x^2 + 4(f(n)-n) < x^2 + 2x < (x+1)^2,$$

ce qui est une contradiction.

Ainsi on a bien $f(n) = n$ pour tout n et la seule fonction solution est la fonction identité.

Exercice 17. Un entier naturel est dit *descendant* si son écriture en base 10, $\overline{a_k a_{k-1} \cdots a_0}$, vérifie $a_k \geqslant a_{k-1} \geqslant \ldots \geqslant a_0$. Un polynôme à coefficients réels P est dit *entier* si $P(n)$ est entier pour tout entier n, et *descendant-entier* si $P(n)$ est entier pour tout entier *descendant* n. Est-ce que tout polynôme *descendant-entier* est aussi *entier* ?

Solution de l'exercice 17
La réponse est non et nous allons construire un contre-exemple.
Remarquons pour commencer qu'un entier *descendant* peut toujours se mettre sous la forme $a - b_1 - b_2 - \ldots - b_9$ où $a = \overline{99\ldots9}$ et $b_i = \overline{11\ldots1}$ pour tout entier $1 \leqslant i \leqslant 9$. En effet, on part d'une suite de 9, puis on enlève 1 à chaque chiffre à partir du moment où l'un d'eux devient 8, puis 1 à tous ceux à partir du premier 7, etc...

Soit n et $k > n$ deux entiers :

$$\underbrace{\overline{99\ldots9}}_{k \text{ chiffres}} = \underbrace{\overline{99\ldots9}}_{k-n \text{ chiffres}} \times 10^n + \underbrace{\overline{99\ldots9}}_{n \text{ chiffres}} \equiv \underbrace{\overline{99\ldots9}}_{n \text{ chiffres}} \pmod{2^n}$$

Ainsi, les nombres de la forme $\overline{99\ldots9}$ ne peuvent donner que au plus n restes modulo 2^n selon qu'ils comportent 1, 2, 3, ..., n chiffres puisqu'au delà ils sont tous congrus à celui à n chiffres.
Nous avons le même résultat pour les nombres de la forme $\overline{11\ldots1}$. Ainsi, un entier descendant ne peut donner que au plus $n(n+1)^9$ restes modulo 2^n car il y a n choix pour a et à chaque fois au plus $n+1$ choix pour $b_1, \ldots, b_9$ (car ils peuvent valoir 0).

Choisissons donc n assez grand pour que $2^n > n(n+1)^9$ (par exemple $n = 63$ convient car $63 \times 64^9 < 64^{10} = 2^{60} < 2^{63}$). Il existe donc un entier $0 \leqslant r < 2^n$ tel qu'aucun entier *descendant* ne soit congru à r modulo 2^n. On considère alors le polynôme :

$$P(x) = \frac{1}{2 \times (2^n - 1)!} \prod_{i=1}^{2^n-1} (x - r + i)$$

Montrons qu'il est *descendant-entier*. Soit x un entier *descendant*, on peut remarquer que :

$$2P(x) = \frac{1}{(2^n-1)!} \prod_{i=1}^{2^n-1} (x - r + i) = \binom{x - r + 2^n - 1}{2^n - 1} \text{ est entier et que :}$$

$$2(x-r)P(x) = \frac{1}{(2^n-1)!} \prod_{i=0}^{2^n-1} (x - r + i) = 2^n \binom{x - r + 2^n - 1}{2^n} \text{ est multiple de } 2^n$$

Ainsi, puisque 2^n ne divise pas $x - r$, $2P(x)$ est nécessairement pair, donc $P(x)$ est entier.
Ainsi, P est *descendant-entier* mais $P(r) = \frac{1}{2}$, donc P n'est pas *entier*, ce qui nous fournit le contre-exemple recherché.

Exercice 18. Soit p un nombre premier tel que $\frac{p-1}{2}$ soit aussi premier, et soient a, b, c trois entiers non divisibles par p. Démontrer que le nombre d'entiers strictement positifs n tels que $n < p$ et p divise $a^n + b^n + c^n$ est inférieur strictement à $\sqrt{2p} + 1$.

Solution de l'exercice 18

Commençons par écarter le cas particulier où $a \equiv \pm b \pmod p$ et $b \equiv \pm c \pmod p$. Dans ce cas quel que soit n,

$$a^n + b^n + c^n \equiv \pm a^n \text{ ou } \pm 3a^n \pmod p.$$

Comme $p \neq 3$ (car $\frac{3-1}{2}$ n'est pas premier) et $p \nmid a$, alors $p \nmid a^n + b^n + c^n$. L'affirmation de l'énoncé est alors directement vraie, puisqu'aucun n ne convient.

Une fois ce cas particulier exclus, nous pouvons quitte à échanger les noms des variables affirmer $a \not\equiv \pm b \pmod p$, c'est à dire

$$ab^{-1} \not\equiv \pm 1 \pmod p.$$

Posons maintenant $q = \frac{p-1}{2}$. Par le petit théorème de Fermat, l'ordre de ab^{-1} modulo p doit diviser $p - 1 = 2q$. Mais comme $ab^{-1} \not\equiv \pm 1 \pmod p$, l'ordre de ab^{-1} ne divise pas 2, ainsi l'ordre vaut q ou $2q$.

Pour la suite, on définit E l'ensemble des entiers strictement positifs $n < p$ tels que $p | a^n + b^n + c^n$, et pour tout entier t, on note e_t le nombre de couples $(i, j) \in E^2$ tels que $i - j \equiv t \pmod{p-1}$. On aura besoin du lemme ci-dessous.

Lemme : Si t est un entier compris strictement entre 0 et $2q$, et que $t \neq q$, alors $e_t \leqslant 2$.

Preuve : Soit $i, j \in E$ avec $i - j \equiv t \pmod{p-1}$. Alors

$$\begin{aligned}
& a^i + b^i + c^i \equiv 0 \pmod p \\
\Longrightarrow\ & a^i c^{j-i} + b^i c^{j-i} + c^j \equiv 0 \pmod p \\
\Longrightarrow\ & a^i c^t + b^i c^t - a^j - b^j \equiv 0 \pmod p \\
\Longrightarrow\ & a^i (c^t - a^t) \equiv b^i (b^t - c^t) \pmod p.
\end{aligned}$$

Montrons que l'on peut diviser par $(c^t - a^t)$. Si $c^t \equiv a^t \pmod p$, alors on aurait aussi $c^t \equiv b^t \pmod p$, d'où $(ab^{-1})^t \equiv 1 \pmod p$. Mais nous savons déjà que l'ordre de ab^{-1} est q ou $2q$, ainsi comme t est pris tel que $q \nmid t$, on a une contradiction. Donc $(c^t - a^t)$ est inversible modulo p et

$$(ab^{-1})^i \equiv (b^t - c^t) \cdot (c^t - a^t)^{-1} \pmod p.$$

Pour t fixé, le côté droit de l'équation reste fixe, donc $(ab^{-1})^i$ ne peut prendre qu'une seule valeur. Or l'ordre de ab^{-1} est supérieur ou égal à $q = \frac{p-1}{2}$, ce qui limite le nombres de solutions pour i à 2. Cela conclut la preuve du lemme. $\square$

Enfin, pour chaque $i \in E$, il y a au moins $|E| - 2$ éléments de E qui diffèrent de i d'une quantité autre que $q \pmod{p-1}$. Ainsi le lemme implique

$$\begin{aligned}
& |E| \cdot (|E| - 2) \leqslant \sum_{t \neq q} e_t \leqslant 2(p-2) \\
\Longrightarrow\ & (|E| - 1)^2 \leqslant 2p - 3 \\
\Longrightarrow\ & |E| < \sqrt{2p} + 1.
\end{aligned}$$