Progresser en arithmétique

Martin Rakovsky & al

2026

2 Un peu de théorie

2.1 Divisibilité et taille, épisode1 - les fondamentaux

Exercice 2.1. Soient a, b, n des entiers tels que pour tout $k > b$, on a $k - b \mid k^n - a$. Montrer que $a = b^n$.

Solution 2.1. Soit $k > b$. Alors par hypothèse, puisque $k \equiv b \mod k - b$,

$$0 \equiv k^n - a \equiv b^n - a \mod k - b.$$

On déduit que $k - b \mid a - b^n$ pour tout entier k. Le nombre $a - b^n$ admet un infinité de diviseurs, il est donc nul et $\boxed{a = b^n}$.

Exercice 2.2. Soit p un nombre premier et m et n des entiers. On suppose que $p^2 + m^2 = n^2$. Montrer que $n = m + 1$.

Solution 2.2. Notons que $n^2 > m^2$ donc $n > m$. L'équation se factorise sous la forme $p^2 = n^2 - m^2 = (n - m)(n + m)$. Donc $n - m$ est un diviseur de p^2, de sorte que $n - m = 1, p$ ou p^2. Si $n - m \geqslant p$, alors $n + m = \dfrac{p^2}{n - m} \leqslant n - m$, ce qui est absurde. On déduit que $n - m = 1$, comme voulu.

Exercice 2.3. Soient $k, m, n \geqslant 1$ des entiers tels que $m^2 + n = k^2 + k$. Montrer que $m \leqslant n$.

Solution 2.3. Supposons par l'absurde que $m > n$. On a donc $k^2 + k < n + n^2$, ce qui implique que $k < n$, ou encore que $k \leqslant n - 1$. Mais alors $k^2 + k \leqslant (n - 1)^2 + n - 1 = n^2 - n < m^2 + n$, ce qui est absurde. On a donc bien $m \leqslant n$.

Solution alternative
Une autre solution est d'utiliser un encadrement par des carrés. En multipliant les deux côtés de l'équation et en ajoutant 1, on trouve

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4m^2 + 4n + 1.$$

Puisque $(2k + 1)^2 > 4m^2$, on a $(2k + 1)^2 \geqslant (2m + 1)^2$. Après développement, cette inégalité implique

$$4m^2 + 4n + 1 = (2k + 1)^2 \geqslant (2m + 1)^2 = 4m^2 + 4m + 1,$$

ce qui implique que $m \leqslant n$.

Exercice 2.4. Soient Montrer que $2^a + 1$ divise $2^b + 1$ si et seulement si $a \mid b$ et b/a est impair.

Solution 2.4. $\boxed{\Leftarrow :}$ Supposons que $b \mid a$ et introduisons k l'entier (supposé impair) tel que $a = bk$. Le fait que $2^b + 1 \mid 2^a + 1$ vient de la factorisation suivante :

$$2^a + 1 = 2^{bk} + 1 = (2^b + 1)(2^{b(k-1)} - 2^{b(k-2)} + \ldots - 2 + 1).$$

On aurait également pu utiliser les congruences, puisque $2^a \equiv -1 \mod 2^a + 1$ et que k est impair :

$$2^b + 1 = (2^a)^k + 1 \equiv (-1)^k + 1 \equiv 0 \mod 2^a + 1.$$

$\boxed{\Rightarrow :}$ On suppose que $2^b + 1 \mid 2^a + 1$. On effectue la division euclidienne de a par b, et on écrit $a = kb + r$ avec $0 \leqslant r < b$. On regarde alors $2^b + 1$ modulo $2^a + 1$, qui vaut 0 par hypothèse :

$$0 \equiv 2^b + 1 = (2^a)^k 2^r + 1 \equiv (-1)^k 2^r + 1 \mod 2^a + 1.$$

Or, $-(2^a + 1) < (-1)^k 2^r + 1 < 2^a + 1$, donc $(-1)^k 2^r + 1 = 0$, soit $2^r = (-1)^k$, ce qui conduit à la fois à $r = 0$ et à k impair, ce qui donne que $b = ak$ avec k impair, comme voulu.

Exercice 2.5. (APMO 2011 P1) Soient a, b et c des entiers strictement positifs. Montrer que les trois nombres $a^2 + b + c, b^2 + c + a$ et $c^2 + a + b$ ne peuvent pas être tous les deux des carrés parfaits.

Solution 2.5. Supposons, quitte à renommer les variables, que $a \leqslant b \leqslant c$. On a alors l'encadrement

$$c^2 < c^2 + a + b \leqslant c^2 + 2c < (c + 1)^2.$$

Le nombre $c^2 + a + b$ ne peut donc pas être un carré parfait. Il n'y a donc pas de solutions.

Exercice 2.6. Soient a et b des entiers tels que $a > b$. On suppose que $a - b \mid a^2 + b$. Montrer que $\dfrac{a+1}{b+1} \leqslant \mathrm{PGCD}(a, b) + 1$.

Solution 2.6. Puisqu'il est plus pratique de travailler avec des entiers premiers entre eux, introduisons $d = \mathrm{PGCD}(a, b)$ et notons x et y les entiers tels que $a = dx$ et $b = dy$. On a alors $x > y$ et $\mathrm{PGCD}(x, y) = 1$.

La condition de l'énoncé devient $d(x - y) \mid d(dx^2 + y)$, ce qui implique que $x - y \mid dx^2 + y$. Comme $x \equiv y \mod y - x$, on trouve

$$0 \equiv dx^2 + y \equiv dy^2 + x = y(dy + 1) \mod x - y.$$

Puisque x et y sont premiers entre eux, $x - y$ est premier avec x. D'après le lemme de Gauss, on déduit que $\boxed{x - y \mid dy + 1}$.

Comme $dy + 1 > 0$ et $x - y > 0$, on en déduit que $x - y \leqslant dy + 1$. On a alors

$$\frac{a+1}{b+1} = \frac{dx+1}{dy+1} = \frac{dy + 1 + dx - dy}{dy+1} = 1 + d\frac{x-y}{dy+1} \leqslant 1 + d = \mathrm{PGCD}(a, b) + 1.$$

Exercice 2.7. (Baltic Way 2024) Soit (a_n) une suite d'entiers supérieurs ou égaux à 2 telle que, pour tout $n \geqslant 1$, $a_{n+2} \mid a_n + a_{n+1}$. Montrer qu'il existe un nombre premier qui divise une infinité de termes de la suite.

Solution 2.7. Ici, une simple disjonction de cas suffit :

- Si une infinité de termes est pair, alors $p = 2$ convient.
- Sinon, il existe un rang N à partir duquel, pour tout $n \geqslant N$, le nombre a_n est impair. Il vient que, pour tout $n \geqslant N$, $a_n + a_{n+1}$ est pair. Comme a_{n+2} est également pair, on a $a_{n+2} \mid (a_n + a_{n+1})/2$, ce qui implique que $a_{n+2} \leqslant \dfrac{a_n + a_{n+1}}{2}$.

  Une récurrence immédiate assure alors que $a_n \leqslant \max(a_1, \ldots, a_N, a_{N+1})$. La suite (a_n) est donc bornée par une constante C. D'après le principe des tiroirs, il existe une infinité de termes égaux au même nombre $a \geqslant 2$. Tout diviseur premier de a convient alors.

Exercice 2.8. (Nordic MO 2016) Déterminer toutes les suites d'entiers $(a_1, \ldots, a_{2016})$ telles que les entiers sont tous bornés par 2016 et $i + j \mid ia_i + ja_j$ pour tout $i, j \in \{1, \ldots, 2016\}$.

Solution 2.8. **Réponse :** Les suites constantes égales à un entier de $[\![1, 2016]\!]$ sont les seules solutions.

On s'empresse de constater que la relation de divisibilité implique, pour tout indice $i \neq j$,

$$i + j \mid ia_i + ja_j - (i + j)a_j = i(a_i - a_j).$$

Dans le but de montrer que $a_i = a_j$ pour tout i, j, on procède en plusieurs temps, en choisissant plusieurs valeurs du couple (i, j) pour lesquelles $i + j$ est premier avec i.

D'une part, en prenant $(i, j) = (2016, 2015)$, on trouve que $2016+2015 \mid 2016(a_{2016} - a_{2015})$. Comme $2016+2015$ est premier avec 2016, on trouve que $4031 \mid a_{2016} - a_{2015}$. Comme les deux entiers sont dans $[\![1, 2016]\!]$, ils sont égaux.

Soit j un indice quelconque. Comme 2015 et 2016 sont premiers entre eux, j est premier avec 2015 ou avec 2016 (ou les deux). Notons $i \in \{2015, 2016\}$ tel que j est premier avec i. Alors $i + j$ est premier avec i, donc d'après le lemme de Gauss, $i + j \mid a_i - a_j$. Comme $i + j \geqslant 2016$ et $a_i, a_j \in [\![1, 2016]\!]$, on déduit que $a_j = a_i = a_{2016}$. Ceci conclut que la suite est constante.

Exercice 2.9. Déterminer les couples (m, n) d'entiers tels que $mn - 1$ est non nul et $mn - 1 \mid n^3 - 1$.

Solution 2.9. **Réponse :** L'ensemble des couples solutions est $\{(1, n), (n, 1), (n^2, n), (n, n^2)\}$ pour $n \geqslant 2$.

Remarquons que les couples $(1, n)$ et $(m, 1)$ sont solutions pour tous les entiers strictement positifs m et n supérieurs ou égaux à 2. On suppose dans la suite que $m, n \geqslant 2$. Notons que les nombres $mn - 1, n^3 - 1$ sont strictement positifs.

On commence par ramener un peu de symétrie au problème en remarquant que

$$mn - 1 \mid (mn)^3 - 1^3 \quad \Longrightarrow mn - 1 \mid (mn)^3 - 1 - m^3(n^3 - 1) = m^3 - 1.$$

Maintenant que le problème est complètement symétrique en m et n , on peut supposer sans perte de généralité que $m \geqslant n$. La condition de divisibilité implique donc que $mn - 1 \leqslant n^3 - 1$, donc $\boxed{m \leqslant n^2}$.

Puisque $mn - 1$ divise $n^3 - 1$ et $mn - 1$, il divise également $n^3 - 1 - (mn - 1) = n(n^2 - m)$. Comme $mn - 1$ et n sont premiers entre eux, on a par le lemme de Gauss que $mn - 1$ divise $n^2 - m$. Mais alors, si $n^2 - m$ est non nul, puisque $m \geqslant n$ et $m \geqslant 1$,

$$0 < n^2 - m < mn - 1 \leqslant n^2 - m$$

ce qui est impossible. On a donc $\boxed{n^2 = m}$. Réciproquement, le couple (n^2, n) est bien solution.

Ainsi, les couples solutions sont $\{(1, n), (n, 1), (n^2, n), (n, n^2)\}$.

Exercice 2.10. Déterminer tous les entiers n tels que $2^n + n \mid 8^n + n$.

Solution 2.10. **Réponse :** Les solutions sont $1, 2, 4$ et 6.

En utilisant que $2^n \equiv -n \mod 2^n + n$, on déduit que

$$0 \equiv 8^n + n = (2^n)^3 + n \equiv (-n)^3 + n = n - n^3 \mod 2^n + n.$$

Ceci donne en particulier que, si $n^3 - n \neq 0$, $2^n + n \leqslant n^3 - n$, ce qui sera faut pour n suffisamment grand. La suite du problème, plus technique, consiste à finir ces détails.

On montre par récurrence que pour $n \geqslant 10$, $2^n + n > n^3 - n > 0$, ce qui rend absurde la divisibilité établie.

Initialisation : Si $n = 10$, on a bien $2^{10} + 10 = 1034 > 10^3 - 10 = 990$.

Hérédité : On suppose que $2^n + n > n^3 - n$ pour un $n \geqslant 10$ fixé et on montre que $2^{n+1} + n + 1 > (n+1)^3 - (n+1)$. En effet, on trouve que

$$2^{n+1} + (n + 1) = 2(2^n + n) - n + 1 > 2n^3 - 3n + 1.$$

Il suffit donc de montrer que $2n^3 - 3n + 1 > (n + 1)^3 - (n + 1)$, ou encore que $n^3 > 3n^2 + 5n - 1$. Or, puisque $n \geqslant 10$,

$$n^3 \geqslant 10n^2 > 3n^2 + 5n^2 + 2 > 3n^2 + 5n - 1.$$

Ceci achève la récurrence.

On déduit que $n \leqslant 9$. Il reste à tester les différents cas :

- ➢ Si $n = 9$, $2^n + n = 521$ et $9^3 - 9 = 720$, donc $2^n + n$ ne divise pas $n^3 - n$.
- ➢ Si $n = 8$, $2^8 + 8 = 264$ et $8^3 - 8 = 504$, donc $2^n + n$ ne divise pas $n^3 - n$.

➢ Si $n = 7$, $2^7 + 7 = 135$ et $7^3 - 7 = 336$, donc $2^n + n$ ne divise pas $n^3 - n$.
➢ Si $n = 6$, $2^6 + 6 = 70$ et $6^3 - 6 = 210$. Donc $2^n + n \mid n^3 - n$ et $2^n + n \mid 8^n + n$.
➢ Si $n = 5$, $2^5 + 5 = 37$ et $5^3 - 5 = 120$, donc $2^n + n$ ne divise pas $n^3 - n$.
➢ Si $n = 4$, $2^4 + 4 = 20$ et $4^3 - 4 = 60$. Donc $2^n + n \mid n^3 - n$ et $2^n + n \mid 8^n + n$.
➢ Si $n = 3$, $2^3 + 3 = 11$ et $3^3 - 3 = 24$, donc $2^n + n$ ne divise pas $n^3 - n$.
➢ Si $n = 2$, $2^2 + 2 = 6$ et $2^3 - 2 = 6$. Donc $2^n + n \mid n^3 - n$ et $2^n + n \mid 8^n + n$.
➢ Si $n = 1$, $2^1 + 1 = 3$ et $1^3 - 1 = 0$. Donc $2^n + n \mid n^3 - n$ et $2^n + n \mid 8^n + n$.

En conclusion, les seules solutions sont $1, 2, 4$ et 6.

Exercice 2.11. On définit la suite $a_1, a_2, \ldots$ de la façon suivante : $a_1 = 63$ et, pour tout entier $n \geqslant 2$, a_n est le plus petit entier multiple de n qui soit supérieur ou égal à a_{n-1}. Montrer que les termes de la suite sont deux à deux distincts.

Solution 2.11. La suite (a_n) est croissante par définition. Supposons par l'absurde qu'il existe deux indices $n < m$ tels que $a_n = a_m$ qui sont égaux. Par croissance de la suite, cela implique en particulier que $a_n = a_{n+1} = a$. Par définition, a_n est divisible par n et a_{n+1} est divisible par $n + 1$, donc a est divisible par $n(n + 1)$. En particulier $\boxed{a \geqslant n(n+1)}$.

D'autre part, pour tout indice k, comme l'intervalle $[\![a_{k-1}, a_{k-1} + k - 1]\!]$ contient un multiple de k, on a $a_k \leqslant a_{k-1} + k - 1$, soit $a_k - a_{k-1} \leqslant k - 1$. Par télescopage,

$$a - a_1 = a_n - a_1 = (a_n - a_{n-1}) + \ldots + (a_2 - a_1) \leqslant (n-1) + \ldots + 1 = \frac{n(n-1)}{2}.$$

On déduit l'inégalité suivante sur n :

$$n(n+1) \leqslant \frac{n(n-1)}{2} + 63 \quad \Longrightarrow n(n+3) \leqslant 126 \quad \Longrightarrow n \leqslant 9.$$

Il reste à calculer les dix premières valeurs de la suite. On trouve que $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) = (63, 64, 66, 68, 70, 72, 77, 80, 81, 90)$, donc aucun des indices n de $[\![1, 9]\!]$ ne vérifie $a_n = a_{n+1}$. D'où la contradiction recherchée, et le résultat.

Exercice 2.12. (Iran Round 2 2010) Soient $a > b$ deux entiers strictement positifs. On suppose que $\mathrm{PGCD}(a - b, ab + 1) = 1$ et que $\mathrm{PGCD}(a + b, ab - 1) = 1$. Montrer que $(a - b)^2 + (ab + 1)^2$ n'est pas un carré parfait.

Solution 2.12. Commençons par vérifier que

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

On suppose par l'absurde que ce nombre est un carré parfait. Observons que si a^2+1 et b^2+1 ne peuvent pas tous les deux être des carrés parfaits. En effet, s'il existe x tel que $a^2+1 = x^2$, on déduit que $1 = x^2 - a^2 = (x-a)(x+a)$. Chacun des facteurs $x - a$ et $x + a$ sont donc des diviseurs de 1, et sont strictement positifs, donc ils sont égaux à 1. Ainsi, $x - a = x + a = 1$, donc $a = 0$, ce qui contredit les hypothèses. Ainsi, $a^2 + 1$ et $b^2 + 1$ ne sont pas des carrés parfaits, donc ils ne sont pas premiers entre eux (d'après l'exerice 14).

On note $d = \mathrm{PGCD}(a^2 + 1, b^2 + 1)$ et p un diviseur premier de d (qui existe d'après le paragraphe précédent). Alors p divise également $b^2 + 1 - (a^2 + 1) = b^2 - a^2 = (b - a)(a + b)$. D'après le lemme d'Euclide, p divise $a - b$ ou $a + b$. Si $p \mid a - b$, alors p divise également $ab + 1$ car p divise le nombre $(a - b)^2 + (ab + 1)^2$. Ceci contredit l'hypothèse que $\mathrm{PGCD}(a - b, ab + 1) = 1$. Si $p \mid a + b$, alors p divise également $ab - 1$ car p divise le nombre $(a + b)^2 + (ab - 1)^2$. Ceci contredit l'hypothèse que $\mathrm{PGCD}(a + b, ab - 1) = 1$. On a une contradiction dans tous les cas, ce qui conclut l'exercice.

Exercice 2.13. (Iran MO 2025 Round 2) Déterminer tous les entiers $n \geqslant 2$ tels que, pour tout diviseur premier p de n, $n + p$ est un carré parfait.

Solution 2.13. **Réponse :** La seule solution est $n = 2$.

Soit p un diviseur premier de n et a_p l'entier tel que $n + p = a_p^2$. Alors $p \mid n + p = a_p^2$, donc $p^2 \mid a_p^2$. Si on avait $p^2 \mid n$, alors on aurait $p^2 \mid a_p^2 - n^2 = p$, ce qui est absurde. On déduit que p^2 ne divise pas n, et donc $\boxed{v_p(n) = 1 \text{ pour tout diviseur } p \text{ de } n}$.

Posons donc $n = p_1 \dots p_r$ la décomposition en facteurs premiers de n. On suppose par l'absurde que $r \geqslant 3$. On ordonne les facteurs premiers, quitte à renuméroter, par $p_1 < p_2 < \dots < p_r$. Posons $A = p_3 \dots p_r$, $p = p_1$ et $q = p_2$. On dispose par hypothèse de deux entiers a et b tels que

$$p(1 + qA) = a^2, \quad q(1 + pA) = b^2.$$

Comme $q > p$, on a $b > a$ et $b \geqslant a + 1$. Il vient que

$$q(1 + pA) \geqslant a^2 + 2a + 1 = p(1 + qA) + 2a + 1 \quad \Longrightarrow \quad q - p = 2a + 1.$$

Or, on a $a > \sqrt{pqA}$ tandis que $q - p < q < \sqrt{qA} < \sqrt{pqA}$. On déduit une contradiction. Ainsi, on déduit que $\boxed{n \text{ admet au plus 2 facteurs premiers}}$. Il est de la forme $n = p$ ou $n = pq$.

Si $n = p$, alors $p + p$ est un carré parfait, donc $p = 2$. Réciproquement, $\boxed{n = 2}$ est bien solution.
Si $n = pq$ avec $p < q$, on a que $q(1+p)$ est un parfait. Cela implique que $q \mid p+1$ donc $q \leqslant p+1 < q+1$. Il vient que $q = p + 1$ donc $(p, q) = (2, 3)$ et $n = 6$. Pourtant, $6 + 2$ n'est pas un carré parfait donc 6 n'est pas solution.

Exercice 2.14. (OFM 2024) Déterminer tous les entiers $n \geqslant 2$ pour lesquels il existe n entiers $a_1, \dots, a_n$ supérieurs ou égaux à 2 et tels que $a_i \mid a_j^2 + 1$ lorsque $i \neq j$.

Solution 2.14. **Réponse :** Le seul entier est $n = 2$.

Notons tout d'abord que $n = 2$ est solution puisque $(a_1, a_2) = (2, 5)$ satisfait la condition de l'énoncé.

Soit désormais n un entier solution. Si i et j sont deux indices distincts, alors la divisibilité $a_i \mid a_j^2 + 1$ implique que $\boxed{a_i \text{ et } a_j \text{ sont premiers entre eux}}$. En particulier, puisqu'ils sont supérieurs ou égaux à 2, les entiers sont deux à deux distincts, et quitte à les renuméroter, on peut supposer que $a_1 < \dots < a_n$.
Supposons désormais que $n \geqslant 3$. Puisque a_n et a_{n-1} sont premiers entre eux, on a $a_n a_{n-1} \mid a_1^2 + 1$, ce qui implique

$$a_1^2 + 1 \geqslant a_n a_{n-1} \geqslant (a_{n-1} + 1)a_{n-1} = a_{n-1}^2 + a_{n-1} > a_1^2 + 1.$$

Ceci donne la contradiction désirée. Ainsi $n \leqslant 2$.

Exercice 2.15. (IMO SL 2022 N2) Déterminer tous les entiers $n > 2$ tels que

$$n! \mid \prod_{p<q\leqslant n} (p + q),$$

où le produit est pris sur l'ensemble des paires (p, q) telles que $p < q \leqslant n$ sont des nombres premiers.

Solution 2.15. **Réponse :** Le seul entier est $n = 7$.

Notons $\mathcal{P}(n)$ le produit du terme de droite. Soit n une solution éventuelle, et soit r le plus grand nombre premier tel que $r \leqslant n$.

Puisque r divise $n!$, il divise $\mathcal{P}(n)$, donc il existe deux nombres premiers p et q tels que $p < q \leqslant n$ et r divise $p + q$. Par maximalité de r, on sait que $p + q < 2r$, de sorte que $p + q = r$. Puisque q et r sont impairs, p est donc pair, et $\boxed{p = 2}$.

De même, il existe deux nombres premiers s et t tels que $s < t \leqslant n$ et q divise $s + t$. Nous allons démontrer que $q - 2$ est premier. En effet, si $t \leqslant q$, alors $s + t < 2q$ donc $s + t = q$, donc $s = 2$ et $t = q - 2$. Sinon, $t > q$, donc $t \geqslant q + 2 = r$ et par maximalité de r, $t = r = q + 2$, donc $q < t + s < 2q + 2 < 3q$, de sorte que $t + s = 2q$ et $s = q - 2$. Dans les deux cas, $q - 2$ est un nombre premier.

On a donc trois nombres premiers consécutifs $q-2, q$ et $q+2$. On remarque que 3 divise l'un des trois nombres, et il s'agit nécessairement de $q - 2$, ce qui signifie que $q - 2 = 3$ et que $\boxed{q + 2 = r = 7}$. Ainsi, $7 \leqslant n < 11$, et

$$n! \mid \mathcal{P}(n) = (2 + 3) \times (2 + 5) \times (2 + 7) \times (3 + 5) \times (3 + 7) \times (5 + 7) = 2^6 \times 3^3 \times 5^2 \times 7.$$

Puisque $2 \times 4 \times 6 \times 8 = 2^7 \times 3$ ne divise pas $\mathcal{P}(n)$, on a nécessairement $\boxed{n = 7}$.
Réciproquement, $n = 7$ est bien une solution, car $7! = 2^4 \times 3^2 \times 5 \times 7$.

Exercice 2.16. (EGMO 2023 P5) Soit $s \geqslant 2$ un entier. Pour tout entier k, on définit son *twist* k' de la façon suivante : si $k = as+b$ est la division euclidienne de k par s, alors $k' = bs+a$. Pour un entier strictement positif n, on définit la suite $(d_i)_i$ comme suit : $d_1 = n$, et d_{i+1} est le twist de d_i pour tout $i \geqslant 1$.
Montrer que la suite contient 1 si et seulement si le reste de la division de n par s^2-1 est 1 ou s.

Solution 2.16. La forme de l'énoncé pousse à regarder l'opération du twist modulo s^2-1. Notons que $s^{-1} \equiv s \mod s^2-1$ puisque $s^2 \equiv 1 \mod s^2-1$. En particulier

$$bs + a \equiv s^{-1}(b+as) \equiv s(as+b) \mod s^2-1.$$

Ainsi, on a $d_{i+1} \equiv sd_i \mod s^2-1$. Encore mieux, $d_{i+2} \equiv s^2 d_i \equiv d_i \mod s^2-1$. Ainsi, la suite (d_i) prend uniquement deux valeurs modulo s^2-1, à savoir d_1 et sd_1. En particulier, si il existe un rang d_j tel que $d_j = 1$, alors $1 \equiv d_1$ ou $1 \equiv sd_1$. Ceci impose que $d_1 \equiv 1$ ou $d_1 \equiv s$.
Réciproquement, si $n \equiv 1$ ou $n \equiv s \mod s^2-1$, montrons que 1 appartient à la suite. L'opération *twist* semble faire décroître la suite (puisque $b \leqslant s-1$), essayons de rendre cette intuition rigoureuse.

- **Cas 1 :** Si $d_i \geqslant s^2$, alors $d_{i+1} < d_i$. En effet, posons $d_i = as+b$ avec $b \leqslant s-1$. Puisque $d_i \geqslant s^2$, on a $a \geqslant s$. Mais alors on vérifie que

  $$d_{i+1} = bs + a \leqslant (s-1)s + a \leqslant as \leqslant as + b = d_i.$$

  La première inégalité est une égalité lorsque $b = s-1$, et la dernière lorsque $b = 0$. Ces deux conditions sont incompatibles, on a donc $d_{i+1} < d_i$.
- **Cas 2 :** Si $d_i < s^2$, alors $d_{i+1} < s^2$ et $d_{i+2} = d_i$. En effet, écrivons $d_i = as+b$, avec $b \leqslant s-1$. COmme $d_i < s^2$, $a \leqslant s-1$. Ainsi, $d_{i+1} = bs + a \leqslant (s-1)s + (s-1) < s^2$. On a de même $d_{i+2} \leqslant s^2-1$. Comme $d_{i+2} \equiv d_i \mod s^2-1$ et que $1 \leqslant d_i, d_{i+2} \leqslant s^2-1$, on a $d_i = d_{i+2}$.

De ces deux cas on déduit que la suite (d_i) est périodique de période 2 à partir d'un certain rang N, prenant alternativement les valeurs d_N et sd_N modulo s^2-1. Si $n \equiv 1, s \mod s^2-1$, alors d_N ou sd_N vaut n modulo s^2-1. On déduit que d_N ou d_{N+1} vaut 1 modulo s^2-1. Comme d_N et d_{N+1} sont compris dans $\{1, \dots, s^2-1\}$, d_N ou d_{N+1} vaut 1.

Exercice 2.17. (Balkan MO 2024 P3) Soient a et b des entiers strictement positifs distincts tels que $3^b+2 \mid 3^a+2$. Montrer que $a > b^2$.

Solution 2.17. Posons $a = bq + r$ la division euclidienne de a par b. On peut commencer par montrer que $q \geqslant b$, ce qui est très proche du résultat. La divsiion de l'énoncé implique que $a \geqslant b$ et donc que $q \geqslant 1$. On a ensuite que

$$0 \equiv 3^a + 2 = (3^b)^q \cdot 3^r + 2 \equiv (-2)^q 3^r + 2 \equiv (-2)^q 3^r - 3^b \mod 3^b + 2.$$

Puisque $b > 0$, $3^b + 2$ est premier avec 3^r, on peut donc simplifier la divisibilité :

$$3^b + 2 \mid (-2)^q 3^r - 3^b \implies 3^b + 2 \mid (-2)^q - 3^{b-r}.$$

A partir de là, on distingue deux cas :

- Si $r \neq 0$, alors on montre que $q \geqslant b$, cela conduit bien à $a > b^2$. En effet, si $q \leqslant b-1$, alors, comme $r \geqslant 1$, on déduit de la divisibilité ci-dessus que

  $$3^b + 2 \leqslant |(-2)^q - 3^{b-r}| \leqslant 2^{b-1} + 3^{b-r} \leqslant 3^{b-1} + 3^{b-1},$$

  ce qui est absurde.
- Si $r = 0$, alors on montre que $q > b$. Tout d'abord, $q \neq 1$ car a et b sont distincts. Le nombre $(-2)^q + 2$ est alors non nul. Si $q \leqslant b$, on a dans la congruence ci-dessus $3^b + 2 \mid (-2)^q 3^0 + 2 = (-2)^q + 2$, d'où

  $$3^b + 2 \leqslant |(-2)^q + 2| \leqslant 2^q + 2 < 3^q + 2 \leqslant 3^b + 2,$$

  ce qui est absurde.

Dans les deux cas, on trouve que $a > b^2$.

Exercice 2.18. (IMO SL 2016 N4) Soient n, m, k et ℓ des entiers strictement positifs tels que $n \neq 1$ et $n^k + mn^\ell + 1 \mid n^{k+\ell} - 1$. Montrer que

- soit $m = 1$ et $\ell = 2k$,
- soit $\ell \mid k$ et $m = \dfrac{n^{k-\ell} - 1}{n^\ell - 1}$.

Solution 2.18. On distingue deux cas :

➢ **Si $\ell \leqslant k$:** On a

$$n^k + mn^\ell + 1 \mid n^{k+\ell} - 1 + n^k + mn^\ell + 1 = n^\ell(n^k + n^{k-\ell} + m) \quad \Longrightarrow \quad n^k + mn^\ell + 1 \mid n^k + n^{k-\ell} + m.$$

où on a utilisé le lemme de Gauss puisque n^ℓ est premier avec $n^k + mn^\ell + 1$. Une autre combinaison linéaire donne

$$n^k + mn^\ell + 1 \mid n^k + n^{k-\ell} + m - (n^k + mn^\ell + 1) = n^{k-\ell} + m - mn^\ell - 1.$$

Or $n^{k-\ell} + m < n^k + mn^\ell + 1$ et $mn^\ell + 1 < n^k + mn^\ell + 1$, donc $0 \leqslant |n^{k-\ell} + m - mn^\ell - 1| < n^k + mn^\ell + 1$. Il vient que $\boxed{n^{k-\ell} + m = mn^\ell + 1}$, ce qui se réécrit

$$m = \frac{n^{k-\ell} - 1}{n^\ell - 1}.$$

Cette fraction est entière, donc $n^\ell - 1 \mid n^{k-\ell} - 1$. Or $n^a - 1 \mid n^b - 1$ seulement si $a \mid b$, donc $\ell \mid k - \ell$ et $\boxed{\ell \mid k}$.

➢ **Si $\ell > k$:** On a cette fois-ci

$$n^k + mn^\ell + 1 \mid n^{k+\ell} - 1 + n^k + mn^\ell + 1 = n^k(n^\ell + mn^{\ell-k} + 1) \quad \Longrightarrow \quad n^k + mn^\ell + 1 \mid n^\ell + mn^{\ell-k} + 1.$$

Cette divisibilité implique

$$n^k + mn^\ell + 1 \leqslant n^\ell + mn^{\ell-k} + 1 \quad \Longleftrightarrow \quad (m-1)n^\ell + n^k \leqslant mn^{\ell-k}.$$

Si $m - 1 \geqslant 1$, alors $(m-1)n^\ell > (m-1)n^{\ell-k}$. Le nombre $(m-1)n^\ell$ est de plus un multiple de $n^{\ell-k}$, donc on récupère $(m-1)n^\ell \geqslant mn^{\ell-k}$. Ainsi, $(m-1)n^\ell + n^k > (m-1)n^\ell \geqslant mn^{\ell-k}$, ce qui contredit l'inégalité donnée. On a donc $\boxed{m = 1}$.

Si $m = 1$, la divisibilité ci-dessus devient

$$n^k + n^\ell + 1 \mid n^\ell + n^{\ell-k} + 1 \quad \Longrightarrow \quad n^k + n^\ell + 1 \mid n^{\ell-k} - n^k.$$

Comme $0 < n^{\ell-k}, n^k < n^k + n^\ell + 1$, on déduit que $0 < |n^{\ell-k} - n^k| < n^k + n^\ell + 1$ et $n^{\ell-k} = n^k$, ce qui conduit à $\boxed{\ell = 2k}$.

Ceci réalise les solutions de l'exercice.

Exercice 2.19. (Envoi Pot Pourri 2019-2020 P8) Déterminer le plus petit entier $n \geqslant 2$ tel qu'il existe des entiers strictement positifs $a_1, \ldots, a_n$ tels que

$$a_1^2 + \ldots + a_n^2 \mid (a_1 + \ldots + a_n)^2 - 1.$$

Solution 2.19.
Puisque $a_1 + \ldots + a_n$ et $a_1^2 + \ldots + a_n^2$ sont de même parité, on doit avoir que $a_1 + \ldots + a_n$ est impair. En poussant cette étude de parité en regardant modulo 4 puis 8, on trouve $(a_1 + \ldots + a_n)^2 \equiv 1 \mod 8$ donc $(a_1 + \ldots + a_n)^2 - 1$ est divisible par 8. Or 8 est premier avec $a_1^2 + \ldots + a_n^2$ qui est impair, d'où

$$8(a_1^2 + \ldots + a_n^2) \mid (a_1 + \ldots + a_n)^2 - 1$$

On peut désormais essayer de comparer les quantités $8(a_1^2 + \ldots + a_n^2)$ et $(a_1 + \ldots + a_n)^2 - 1$. D'après l'inégalité de Cauchy-Schwarz,

$$8(a_1^2+\ldots+a_n^2) \leqslant (a_1+\ldots+a_n)^2 - 1 \leqslant n(a_1^2+\ldots+a_n^2) - 1 < n(a_1^2+\ldots+a_n^2)$$

où l'inégalité au milieu correspond à l'inégalité des moyennes arithémtiques et quadratiques. On obtient finalement que $n > 8$ donc $\boxed{n \geqslant 9}$.

Réciproquement, on cherche 9 entiers satisfaisant la propriété. On peut s'attendre à ce que de petits entiers fonctionnent. On peut donc chercher des a_i valant 1 ou 2. Finalement, on trouve qu'en prenant $a_1 = \cdots = a_7 = 1$ et $a_8 = a_9 = 2$, on a bien 15 qui divise $11^2 - 1 = 120 = 15 \times 8$.
La réponse attendue est donc $n = 9$.

Exercice 2.20. (IMO 2015 P2) Déterminer tous les triplets (a, b, c) d'entiers strictement positifs tels que les entiers

$$ab - c, \quad bc - a, \quad ca - b$$

sont des puissances de 2.

Solution 2.20.

➢ Commentaire :

> La solution est une longue disjonction de cas. En introduisant les puissances de 2 correspondant à chaque terme, on souhaite ordonner les nombres en fonction de l'ordre $a \leqslant b \leqslant c$ (le problème étant symétrique en les trois variables). Le raisonnement clé (qui va induire toutes les disjonctions de cas) est le suivant : supposons que $a < b < c$ et posons
>
> $$2^u = ab - c, \quad 2^v = ac - b, \quad 2^w = bc - a.$$
>
> On a au passage que $u < v < w$. De plus, $2^v \mid bc - a - (ac - b) = (c + 1)(b - a)$. Si $c + 1$ n'est pas divisible par 4, alors $2^{v-1} \mid b - a$, donc $b > 2^{v-1}$. D'autre part, si a est grand, $2^v = ac - b > 2c$, donc $c < 2^{v-1}$. Cela implique une contradiction.
>
> Cela fait beaucoup de "si", et donc autant de cas à traiter sur le côté, ce qui va donner les solutions. Néanmoins, les cas restants sont :
> - ➢ le cas où des inconnues sont égales. Moins de variables, moins de difficulté.
> - ➢ le cas où a est petit (c'est-à-dire le cas $a \leqslant 2$). On a à nouveau moins d'inconnues.

Le problème étant symétrique en les trois variables, on suppose que $a \leqslant b \leqslant c$.

Réponse : Les triplets recherchés sont $(2, 2, 2), (2, 2, 3), (2, 6, 11)$ et $(3, 5, 7)$, et leurs permutations.

Notons déjà que si $a = 1$, alors $b - c \leqslant 0$ ne peut pas être une puissance de 2. On a donc $2 \leqslant a \leqslant b \leqslant c$. Dans la suite, on pose

$$2^u = ab - c, \quad 2^v = ac - b, \quad 2^w = bc - a.$$

Puisque $a \leqslant b \leqslant c$, on a $w \geqslant v \geqslant u$.

Cas 1 : $a < b < c$ et $a \geqslant 3$.

Il existe un choix de signe $\varepsilon \in \{-1, 1\}$ tel que $c + \varepsilon$ n'est pas divisible par 4 (il suffit de distinguer selon les valeurs de c modulo 4). On a alors

$$2^w + \varepsilon 2^v = bc - a + \varepsilon(ac - b) = (b + a\varepsilon)(c - \varepsilon).$$

Comme 2^v divise $(b + a\varepsilon)(c - \varepsilon)$ et que $c + \varepsilon$ n'est pas divisible par 4, on déduit que $\boxed{2^{v-1} \mid b + a\varepsilon}$. D'autre part, on a $2^v = ac - b \geqslant 3c - b > 2c$ et par suite $2^{v-1} > c > b > a$. Comme $b + \varepsilon a \neq 0$, l'inégalité précédente et la divisibilité ci-dessus conduisent à $2^{v-1} \leqslant b + \varepsilon a < 2^v$, soit $2^{v-1} = b + \varepsilon a$ puis $\varepsilon = 1$. On déduit que

$$ac - b = 2^v = 2(a + b) \quad \Leftarrow 4b > 3b + a = a(c - 1) \geqslant ab \quad \Leftarrow a \leqslant 3.$$

On déduit que $\boxed{a = 3}$. En simplifiant d'abord l'équation ci-dessus, on obtient $c = b+2$, puis en injectant dans le système de départ, on trouve $2^w = bc - a = b(b+2) - 3 = (b-1)(b+3)$. Comme $b-1$ et $b+3$ ont pour différence 4 et qu'ils sont tous les deux des puissances de 2, on trouve $b - 1 = 4$ et $b + 3 = 8$, soit $\boxed{(a, b, c) = (3, 5, 7)}$. Réciproquement, ce triplet vérifie les conditions avec $(u, v, w) = (3, 4, 5)$.

Cas 2 : $a < b < c$ et $a = 2$.

Supposons que $u \geqslant 1$. Alors $v \geqslant 2$, et on a $2c - b = 2^v \mid 2^w = bc - 2$, d'où

$$0 \equiv bc - 2 \equiv 2c^2 - 2 = 2(c^2 - 1) \mod 2^v.$$

Il vient que $c^2 - 1$ est pair donc c est impair. Mais alors $2^u = 2b - c$ est impair, ce qui contredit que $u > 0$. On déduit que $\boxed{u = 0}$. Il vient que $c = 2b - 1$, puis que $2^v = 3b - 2$. On déduit que $3b - 2 \mid 2^v \mid 2^w = b(2b - 1) - 2$, puis que

$$3b - 2 \mid 2b^2 - b - 2 \quad \Longrightarrow 3b - 2 \mid 9(2b^2 - b - 2) - (6b + 1)(3b - 2) = 16.$$

On déduit que $v \leqslant 4$, soit que $v \in \{1, 2, 3, 4\}$.

- Si $v = 1$, alors $3b - 2 = 2^v = 2$ donc $3b = 4$, ce qui est absurde.
- Si $v = 2$, alors $b = 2$, ce qui contrefit que $a < b$.
- Si $v = 3$, alors $3b = 10$ ce qui est absurde.
- Si $v = 4$, alors $b = 6$ et $c = 11$, et réciproquement le triplet $\boxed{(2, 6, 11)}$ est bien solution avec $(u, v, w) = (1, 4, 6)$.

Cas 3 : Certains des entiers a, b et c sont égaux.

Supposons que $a = b$. Alors le système devient $a^2 - c = 2^u$ et $a(c - 1) = 2^v$. La deuxième égalité implique qu'il existe deux entiers v_1 et v_2 tels que $a = 2^{v_1}$ et $c = 2^{v_2} + 1$. En réinjectant dans la première équation, on trouve que $2^{2v_1} - 2^{v_2} - 1 = 2^u$. Comme $a \geqslant 2$, $v_1 \geqslant 1$. Si $v_2 \geqslant 2$, l'équation précédent est fausse modulo 4. Ainsi, $\boxed{v_2 = 0 \text{ ou } 1}$.

Si $v_2 = 0$, alors $c = 2$ puis $a^2 = 2^u + 2$. Cette équation n'a pas de solution modulo 4 sauf si $u = 1$, conduisant à $a = 2$. Réciproquement, le triplet $\boxed{(2, 2, 2)}$ est solution avec $(u, v, w) = (1, 1, 1)$.

Si $v_2 = 1$, alors $2^{2v_1} = 2^u + 3$, ce qui implique pour des raisons de parité que $u = 0$ et que $v_1 = 1$. On a donc $a = 2$ et $c = 3$. Réciproquement, le triplet $\boxed{(2, 2, 3)}$ est solution avec $(u, v, w) = (0, 2, 2)$.

Comme la preuve précédente s'applique aussi aux cas $b = c$ et $a = c$, on a traité tous les cas.

2.2 Valuation $p-$adique

Exercice 2.21. Soit $a, b, c \geqslant 1$ des entiers tels que $a^b \mid b^c$ et $a^c \mid c^b$. Montrer que $a^2 \mid bc$.

Solution 2.21. Il suffit de montrer que $2v_p(a) \leqslant v_p(bc) = v_p(b) + v_p(c)$ pour tout nombre premier p. On fixe désormais p un nombre premier.
D'après l'énoncé, $bv_p(a) \leqslant cv_p(b)$ et $cv_p(a) \leqslant bv_p(c)$. On déduit, en effectuant le produit de ces deux relations et en simplifiant,

$$v_p(a)^2 \leqslant v_p(b)v_p(c).$$

D'après l'inégalité des moyennes, on obtient alors

$$v_p(a) \leqslant \sqrt{v_p(b)v_p(c)} \leqslant \frac{v_p(b) + v_p(c)}{2},$$

ce qui conclut.

Exercice 2.22. Par combien de zéros termine 2025! ?

Solution 2.22. Le nombre de zéros de 2025! correspond au plus grand entier k tel que $10^k \mid 2025!$. Cet entier k correspond à $\min(v_2(2025!), v_5(2025!))$. Le membre de droite dans la formule de Legendre est décroissant par rapport à p, ce qui signifie que $v_5(2025!) \leqslant v_2(2025!)$, donc il suffit de calculer $v_5(2025!)$. La formule de Legendre donne (avec un peu de calcul)

$$v_5(2025!) = \left\lfloor \frac{2025}{5} \right\rfloor + \left\lfloor \frac{2025}{25} \right\rfloor + \left\lfloor \frac{2025}{125} \right\rfloor + \left\lfloor \frac{2025}{625} \right\rfloor = 405 + 81 + 16 + 3 \boxed{=505}.$$

Exercice 2.23. Montrer que 2^n ne divise jamais $n!$ mais 2^{n-1} divise $n!$ pour une infinité de n.

Solution 2.23. Soit $n \geqslant 1$. D'après le corollaire de la formule de Legendre, $v_2(n!) < n/(2-1) = n$, donc 2^n ne divise jamais $n!$.

Prenons un entier $k \geqslant 1$ et posons $n = 2^k$. Alors

$$v_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2^2} \right\rfloor + \left\lfloor \frac{n}{2^3} \right\rfloor + \ldots = 2^{k-1} + 2^{k-2} + \ldots + 1 = 2^k - 1 = n - 1.$$

Ainsi, pour $n = 2^k$, on a $2^{n-1} \mid n!$, ce qui donne l'infinité annoncée.

Exercice 2.24. (IMO SL 2023 N3) Pour tout entier $k \geqslant 2$ et tout entier $n \geqslant 1$, on note $E_k(n)$ le plus grand entier r tel que $k^r \mid n!$. Montrer qu'il existe une infinité d'entiers n tels que $E_{10}(n) > E_9(n)$ et une infinité d'entiers n tels que $E_{10}(n) < E_9(n)$.

Solution 2.24. Le nombre $E_{10}(n)$ correspond à $\min(v_2(n), v_5(n))$. Le membre de droite dans la formule de Legendre est décroissant par rapport à p, ce qui signifie que $v_5(n) \leqslant v_2(n)$ et $\boxed{E_{10}(n) = v_5(n!)}$. D'autre part, la définition de $E_9(n)$ implique que $E_9(n) = \left\lfloor \frac{v_3(n!)}{2} \right\rfloor$.

➢ **Commentaire :**

> Pour trouver les infinités désirées, il est bon de chercher parmi les entiers n parmi les puissances de 5 et les puissances de 3.
>
> On pose par exemple $n = 5^k$ et on veut établir un cahier des charges sur l'entier k. En bonus (et ce sera en fait nécessaire), on peut choisir la valeur de k pour que $5^k \equiv 2 \mod 3$, afin que $\lfloor n/3 \rfloor = (n-2)/3$, ce qui diminue encore la valeur de $E_9(n)$. Les autres termes peuvent être estimés "à la truelle", c'est-à-dire de façon grossière.

Si $n = 5^{2\ell-1}$, alors $n \equiv (5^2)^\ell \cdot 5^{-1} \equiv 2 \mod 3$. Il vient que, à la manière du corollaire 2.1,

$$v_3(n!) = \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{3^2} \right\rfloor + \ldots = \frac{n-2}{3} + \left\lfloor \frac{n}{3^2} \right\rfloor + \ldots < \frac{n-2}{3} + \frac{n}{3^2} + \frac{n}{3^3} + \ldots = \boxed{\frac{n}{2} - \frac{2}{3}}.$$

$$v_5(n!) = \left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \ldots = 5^{2\ell-2} + 5^{2\ell-3} + \ldots + 5 + 1 = \frac{5^{2\ell-1}-1}{4} = \boxed{\frac{n-1}{4}}.$$

On déduit bien que $E_9(n) \leqslant \dfrac{v_3(n!)}{2} = \dfrac{n}{4} - \dfrac{1}{3} < \dfrac{n-1}{4} = E_{10}(n)$. Donc on a une infinité d'entiers vérifiant $\boxed{E_9(n) < E_{10}(n)}$.

Si $n = 3^{4\ell-2}$ (le choix de l'exposant vise à rendre $v_3(n!)$ pair), alors $n \equiv (3^4)^\ell \cdot 3^{-2} \equiv 4 \mod 5$. Il vient que,

$$v_3(n!) = \left\lfloor \frac{n}{3} \right\rfloor + \left\lfloor \frac{n}{3^2} \right\rfloor + \ldots = 3^{4\ell-3} + 3^{4\ell-4} + \ldots + 3 + 1 = \boxed{\frac{3^{4\ell-1}-1}{2}}.$$

Notons que $3^{4\ell-2} \equiv (-1)^{4\ell-2} \equiv 1 \mod 4$, donc $v_3(n!)$ est pair et $E_9(n) = v_3(n!)/2 = (n-1)/4$. D'autre part,

$$v_5(n!) = \left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \ldots \leqslant \frac{n-4}{5} + \frac{n}{5^2} + \ldots = \boxed{\frac{n}{4} - \frac{4}{5}}.$$

On trouve bien $\boxed{E_{10}(n) < E_9(n)}$.

Exercice 2.25. *(Pologne MO 2023 Round 2)* Déterminer tous les entiers b avec la propriété suivante : il existe un entier a et des entiers k et ℓ distincts tels que $b^{k+\ell}$ divise $a^k + b^\ell$ et $a^\ell + b^k$.

Solution 2.25. **Réponse :** le seul entier solution est $b = 1$.

Notons que $b = 1$ vérifie la propriété. On suppose que $b \geqslant 2$ et on considère les entiers a, k et ℓ fournis par l'énoncé. Soit p un diviseur premier de b. Alors $p^{\ell v_p(b)+1} \mid b^{k+\ell} \mid a^k + b^\ell$ mais $p^{\ell v_p(b)+1} \nmid b^\ell$, donc $p^{\ell v_p(b)+1} \nmid a^k$ mais $p^{\ell v_p(b)} \mid a^k$, de sorte que $\boxed{\ell v_p(b) = k v_p(a)}$.

Mais en exploitant la deuxième divisibilité, on trouve de même que $k v_p(b) = \ell v_p(a)$. Autrement dit $\dfrac{v_p(a)}{v_p(b)} = \dfrac{k}{\ell} = \dfrac{\ell}{k}$, ce qui conduit à $k = \ell$, ce qui est impossible d'après l'énoncé. Cette contradiction implique qu'il n'y a pas d'autre solution que $b = 1$.

Solution alternative

On peut également s'en sortir avec uniquement des arguments de divisibilité. En effet, si on suppose que $k > \ell$, on vérifie que

$$b^{k+\ell} \mid a^{k-\ell}(a^\ell + b^k) - (a^k + b^\ell) = a^{k-\ell}b^k - b^\ell.$$

Ceci implique que $b^k \mid a^{k-\ell}b^{k-\ell} - 1$, et donc que $b \mid 1$, soit $b = 1$.

Exercice 2.26. *(Caucase MO 2024 Junior)* Soient 10 entiers strictement positifs de somme 1000. On suppose que le produit de leurs factorielles est une puissance 10−ème. Montrer que les 10 entiers sont égaux.

Solution 2.26. Notons $n_1, \ldots, n_{10}$ les entiers. Supposons par l'absurde que ces entiers ne sont pas tous égaux. Alors l'un d'eux au moins, disons n_1, vérifie $n_1 > 100$, soit $n_1 \geqslant 101$. Le nombre $n_1!n_2!\ldots n_{10}!$ est donc divisible par 101 qui est premier. Comme il s'agit d'une puissance 10−ème, il est même divisible par 101^{10}.

D'autre part, puisque $n_i \leqslant 1000 < 101^2$ pour tout i, la formule de Legendre indique que $v_{101}(n_i!) = \lfloor n_i/101 \rfloor$. L'inégalité $\lfloor x \rfloor \leqslant x$ permet alors d'établir

$$10 \leqslant v_{101}(n_1!\ldots n_{10}!) = v_{101}(n_1!) + \ldots + v_{101}(n_{10}!) = \left\lfloor \frac{n_1}{101} \right\rfloor + \ldots + \left\lfloor \frac{n_{10}}{101} \right\rfloor \leqslant \frac{n_1}{101} + \ldots + \frac{n_{10}}{101} = \frac{1000}{101}.$$

D'où la contradiction recherchée.

Exercice 2.27. *(Roumanie TST 2007)* Soit $n \geqslant 3$ un entier naturel et soient $a_1, a_2, \ldots, a_n$ des 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 $a_1 \times a_2 \times \ldots \times a_n$ divise $(a_1 + a_2 + \ldots + a_n)^{n-2}$.

Solution 2.27. Il suffit de montrer que, pour tout nombre premier p,

$$v_p(a_1) + \ldots + v_p(a_n) \leqslant (n-2)v_p(a_1 + \ldots + a_n).$$

On fixe désormais un nombre premier p. D'après l'hypothèse de l'énoncé,

$$\max(v_p(a_1), \ldots, v_p(a_n)) \leqslant v_p(a_1 + \ldots + a_n).$$

Montrons que p divise au maximum $n-2$ des entiers $a_1, \ldots, a_n$. Tout d'abord, p ne peux pas diviser tous les entiers, car ils sont premiers entre eux dans leur ensemble. Supposons désormais que p divise exactement $n-1$ des entiers, disons $a_1, \ldots, a_{n-1}$. Remarquons que $p \mid \text{PPCM}(a_1, \ldots, a_n) \mid a_1 + \ldots + a_n$. Il vient que $p \mid (a_1 + \ldots + a_n) - (a_1 + \ldots + a_{n-1}) = a_n$, donc p diviserait tous les entiers, ce qui est exclu.
Comme p divise au plus $n-2$ des entiers $a_1, \ldots, a_n$, on a bien

$$v_p(a_1) + \ldots + v_p(a_n) \leqslant (n-2)\max(v_p(a_1), \ldots, v_p(a_n)) \leqslant (n-2)v_p(a_1 + \ldots + a_n).$$

Exercice 2.28. Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs telle que, pour toute paire (i, j) d'entiers distincts, $\text{PGCD}(a_i, a_j) = \text{PGCD}(i, j)$. Montrer que, pour tout indice i, $a_i = i$.

Solution 2.28. Il suffit de montrer que, pour tout indice i, $v_p(a_i) = v_p(i)$ pour tout nombre premier p. On fixe dans la suite p un nombre premier.
Soit i un entier. Posons $\alpha = v_p(i)$ et prenons $j = p^{\alpha+1}$. On a alors

$$p^\alpha = \text{PGCD}(i, p^{\alpha+1}) = \text{PGCD}(a_i, a_{p^\alpha+1}),$$

ce qui implique en particulier que $p^\alpha \mid a_i$, soit $\boxed{\alpha = v_p(i) \leqslant v_p(a_i)}$.
Comme cette inégalité est vraie pour tout indice i, on a également $p^{\alpha+1} \mid a_{p^{\alpha+1}}$. Comme pourtant $\text{PGCD}(a_i, a_{p^{\alpha+1}}) = p^\alpha$, on déduit que $p^{\alpha+1}$ ne divise pas a_i, ce qui implique bien que $\boxed{v_p(a_i) = \alpha = v_p(i)}$ et conclut.

Exercice 2.29. Rémi écrit n entiers strictement positifs $a_1, \ldots, a_n$ au tableau. Toutes les minutes, Rémi peut remplacer un entier a écrit au tableau par N/a, où N désigne le PPCM des entiers écrits au tableau. Montrer que Rémi peut faire en sorte que tous les nombres écrits au tableau soient des 1 après un nombre fini d'opérations.

Solution 2.29. Notons r le nombre de facteurs premiers distincts dans la décomposition en facteurs premiers de N_0 le PPCM des a_i au premier instant. Montrons que Rémi peut s'arranger pour que le PPCM des a_i au bout d'un nombre fini de mouvements possède au plus $r-1$ facteurs premiers.
On commence par remarquer que lorsque Rémi effectue une opération, le PPCM des entiers écrits au tableau ne gagne pas de facteur premier supplémentaire.
Soit p un diviseur premier de N_0 et $\alpha = v_p(N)$. Par définition, $\alpha = \max(v_p(a_1), \ldots, v_p(a_n))$. Notons S l'ensemble des entiers a_j tels que $v_p(a_j) = \alpha$. Rémi applique alors son opération successivement aux entiers de S. Lors de chaque telle opération, le nouvel entier que Rémi écrit au tableau n'est plus divisible par p, tandis que la valuation $p-$adique du PPCM des entiers écrits n'augmente pas. Ainsi, au bout de ces opérations, aucun des entiers écrits au tableau n'est divisible par p^α. Si N' désigne le PPCM des entiers alors écrits au tableau, on a donc $v_p(N') < v_p(N)$. De proche en proche, Rémi peut donc bien s'arranger pour que, au bout d'un nombre fini d'opération, le PPCM des entiers écrits au tableau ne soit plus divisible par p.
De proche en proche, Rémi peut donc s'arranger pour que, au bout d'un nombre fini d'opérations, le PPCM des entiers écrits au tableau n'ait aucun facteur premier, c'est-à-dire qu'il soit égal à 1, ce qui signifie que tous les entiers écrits valent 1.

Exercice 2.30. (EGMO 2020 P1) Les entiers $a_0, \ldots, a_{3030}$ satisfont la relation

$$2a_{n+2} = a_{n+1} + 4a_n$$

pour tout $n \in \{0, 1, 2, \ldots, 3028\}$. Montrer qu'au moins l'un des a_n est divisible par 2^{2020}.

Solution 2.30. Le travail sur les petits cas suggère que les termes au milieu de la suite auront une v_2 élevée. On souhaite alors procéder par récurrence, en retirant les termes extrémaux lors de l'hérédité. Dans ce genre de problème, la difficulté est d'établir la bonne propriété à démontrer par récurrence, faute de quoi l'hérédité sera très laborieuse. Souvent, la solution dans ce cas est de prouver par récurrence un résultat plus fort que celui de l'énoncé mais dont le passage à l'hérédité sera très simple (c'est ça qui est difficile).

On montre par récurrence sur N que si les entiers $a_0, \dots, a_{3N}$ satisfont la relation de l'énoncé, alors l'entier a_N est divisible par 2^{2N}.

Initialisation : Si $N = 0$, il n'y a rien à démontrer.

Hérédité : On suppose la propriété vraie pour un certain $N \geqslant 0$ fixé. On considère $a_0, \dots, a_{3(N+1)}$ entiers vérifiant la relation voulue. D'après l'hypothèse de récurrence appliquée aux quatre suites d e $3N$ entiers $(a_0, \dots, a_{3N}), (a_1, \dots, a_{3N+1}), (a_2, \dots, a_{3N+2})$ et $(a_3, \dots, a_{3N+3})$, les entiers a_N, a_{N+1}, a_{N+2} et a_{N+3} sont divisibles par 2^{2N}. On considère les relations

$$2a_{N+2} = a_{N+1} + 4a_N, \qquad 2a_{N+3} = a_{N+2} + 4a_{N+1}.$$

Dans la deuxième relation, comme 2^{2N+1} divise $2a_{N+3}$ et $4a_{N+1}$, il divise a_{N+2}. En réinjectant dans la première relation, 2^{2N+2} divise $2a_{N+2}$ et $4a_N$ donc il divise a_{N+1}, ce qui achève la récurrence.

Remarque : D'autres énoncés par récurrence étaient possibles, comme par exemple que $a_n, a_{n+1}, \dots, a_{3030-n+1}$ sont divisibles par 2^{2n} pour tout n.

Exercice 2.31. (JBMO SL 2021 N4) Alice et Bob jouent au jeu suivant : Alice choisit un ensemble infini S de nombres premiers qu'elle communique à Bob. Ensuite, Bob choisit une suite x_1, x_2 infinie d'entiers strictement positifs qu'il communique à Alice. Alice choisit alors un entier M strictement positif et un nombre premier p de S, qu'elle communique à Bob.

Bob gagne si il existe un entier N tel que, pour tout $n \geqslant N$, x_n est divisible par p^M. Sinon, Alice gagne.

Quel joueur dispose d'une stratégie gagnante ?

Solution 2.31. Montrons que Bob possède une stratégie gagnante.

La construction qui suit utilise un argument dit "diagonal" : il s'agit de construire une suite dont les termes x_n doivent avoir deux paramètres arbitrairement grands : le nombre de facteurs premiers distincs de x_n et leurs valuation $p-$adique. Le procédé diagonal permet de garantir ces deux conditions.

Notons $(p_i)_{i\in\mathbb{N}}$ la suite des nombres premiers choisis par Alice. Bob choisit alors la suite définie par $x_n = (p_1 \dots p_n)^n$, que l'on peut voir aussi de cette façon

$$\begin{aligned}
x_1 &= p_1 \\
x_2 &= p_1^2 \times p_2^2 \\
x_3 &= p_1^3 \times p_2^3 \times p_3^3 \\
\vdots \quad &\quad \vdots \quad \ddots \quad \ddots \\
x_n &= p_1^n \times p_2^n \times \ldots \times p_n^n.
\end{aligned}$$

Soit p le nombre premier choisi par Alice et m son indice dans la suite et M l'exposant choisi par Alice. Alors on vérifie que pour tout $\ell \geqslant 0$, p_m^M divise $x_{M+m+\ell}$, ce qui implique que Bob gagne.

Exercice 2.32. (RMM 2019 P1) Alice et Bob jouent au jeu suivant : Alice commence par écrire un entier au tableau. Ensuite, les joueurs jouent chacun à leur tour en commençant par Bob. Pendant son tour, Bob peut remplacer l'entier n écrit au tableau par n'importe quel entier de la forme $n - a^2$, où a est un entier positif. Alice, pendant son tour, peut remplacer l'entier n par n'importe quel entier de la forme n^ℓ, où ℓ est un entier positif. Bob gagne s'il parvient à écrire 0 au tableau.

Alice peut-elle empêcher Bob de gagner ?

Solution 2.32. La réponse est **non**. On donne à présent une stratégie pour Bob.

On montre que Bob peut s'arranger pour faire décroître strictement la partie sans facteur carrée de l'entier écrit au tableau à chacun de ses tours.

On décompose n l'entier écrit au tableau sous la forme $n = bA^2$, où b est la partie "sans carré" de n (i.e le plus grand diviseur de n sans facteur carré). On suppose que c'est à Alice de jouer. Si elle choisit un entier pair $2k$, alors le nouvel entier n^{2k} écrit au tableau est un carré parfait et Bob peut alors choisir $a = n^k$ pour gagner. On suppose donc qu'Alice choisit un entier impair que l'on note $2k+1$. Le nouvel entier écrit au tableau devient

$$n^{2k+1} = b^{2k+1}A^{2(2k+1)} = b(b^kA^{2k+1})^2.$$

La partie sans carré demeure donc inchangée après le coup d'Alice. Posons $Q = b^kA^{2k+1}$. Bob choisit désormais $a = Q$. L'entier écrit au tableau après le tour de Bob est

$$n^{2k+1} - Q^2 = (b-1)Q^2.$$

La partie sans carrée de $n^{2k+1} - Q^2$ est donc un diviseur de $b-1$ et est donc strictement plus petite que b. Ceci conclut que Bob peut faire décroître strictement la partie sans carré de l'entier écrit au tableau pendant son tour.

Ainsi, si Bob poursuit cette stratégie, au bout d'un certain nombre de tours, l'entier écrit au tableau après le tour de Bob sera un carré parfait. Il sera encore un carré parfait m^2 après le tour d'Alice, ce qui permet à Bob de gagner au tour suivant en choisissant $a = m$ pour son tour.

Solution alternative

On propose une autre stratégie pour Bob. Pour cela, on décompose l'entier de départ sous la forme $n = a_1^2 + \ldots + a_m^2$. Une telle décomposition est toujours possible, par exemple en prenant $m = n$ et $a_1 = \ldots = a_n = 1$.

Supposons que cela soit au tour d'Alice, elle ne peut pas choisir un entier k pair, sinon Bob gagne au tour suivant, comme dans la solution précédente. Alice doit donc choisir un entier impair noté $2k+1$. Alors le nouvel entier écrit au tableau devient

$$n^{2k+1} = (a_1^2 + \ldots + a_m^2)^{2k+1} = (a_1^2 + \ldots + a_m^2)(n^k)^2.$$

Après le tour d'Alice, le nombre de carrés parfaits dont la somme vaut n n'a donc pas augmenté. Bob choisit alors pendant son tour $a = a_m n^k$. Le nouvel entier écrit au tableau devient

$$(a_1 n^k)^2 + \ldots + (a_{m-1}n^k)^2$$

et s'écrit donc comme la somme de $m-1$ carrés parfaits. De proche en proche, Bob peut faire décroître le nombre de carrés parfaits nécessaires à l'écriture de l'entier écrit au tableau, si bien qu'au bout de m tours, l'entier écrit au tableau est un carré parfait, ce qui permet à Bob de gagner.

Remarque : Le théorème des quatre carrés assure que n peut toujours s'écrire comme la somme de quatre carré, de sorte que Bob peut toujours gagner en au plus 4 tours.

Exercice 2.33. (USAJMO 2022 P1) Déterminer tous les entiers m pour lesquels il existe une suite arithmétique $a_1, a_2, \ldots$ et une suite géométrique $g_1, g_2, \ldots$ telles que $a_2 - a_1$ n'est pas divisible par m mais $a_n - g_n$ est divisible par m pour tout indice $n \geqslant 1$.

Solution 2.33. **Réponse :** Il s'agit des entiers m divisibles par un carré parfait.

Analyse : Soit m un entier vérifiant les conditions du problème.

Notons d la raison de la suite arithmétique et q la raison de la suite géométrique. On a $(a_1, a_2, a_3) = (a_2 - d, a_2, a_2)$ et $(g_1, g_2, g_3) = (g_2/q, g_2, g_2q)$. D'après la condition de l'énoncé, on a

$$g_2^2 = g_1g_3 \equiv a_1a_3 \equiv (a_2 - d)(a_2 + d) = a_2^2 - d^2 \equiv g_2^2 - d^2 \mod m,$$

ce qui implique que $\boxed{d^2 \equiv 0 \mod m}$. Or, $d = a_2 - a_1$, donc m divise d^2 mais pas d. Cela implique que m admet un facteur premier p tel que $\boxed{v_p(m) \geqslant 2}$ (sinon, on aurait pour tout diviseur premier p que $v_p(m) = 1$, et comme $p \mid m \mid d^2$, alors $p \mid d$ et donc $m \mid d$).

Construction : Soit m un entier divisible par un carré d^2. On construit deux suites (a_n) et (g_n) vérifiant les conditions de l'énoncé.

Posons $m = d^2a$. On choisit $a_k = kda + 1$ et $g_k = (da+1)^k$ pour tout entier $k \geqslant 1$. On vérifie que $a_2 - a_1 = da$ n'est pas divisible par m. En revanche, $a_1 = g_1$ et, on pour tout $k \geqslant 2$, d'après la formule du binôme,

$$g_k - a_k = \sum_{\ell=0}^{k} \binom{k}{\ell} (da)^\ell - (kda+1) \equiv 1 + kda - (kda+1) = 0 \mod m.$$

Les deux suites construites satisfont donc les conditions de l'énoncé.

Exercice 2.34. *(IMO 2026 P1)* On considère 2026 entiers strictement plus grand ue 1 sur un tableau. Chaque minute, tant que cela est possible Alice choisit deux entiers m et n inscrits au tableau et tous les deux strictement plus grands que 1 et les remplace par les deux entiers

$$\mathrm{PGCD}(m,n) \quad \text{et} \quad \frac{\mathrm{PPCM}(m,n)}{\mathrm{PGCD}(m,n)}.$$

1. Montrer que, quels que soient les choix d'Alice, au bout d'un nombre fini de minutes, il y a exactement un entier M strictement plus grand que 1 parmi les entiers du tableau.
2. Montrer que la valeur de M est indépendante des choix d'Alice.

Solution 2.34. 1) Notons m' et n' les entiers remplaçant les entiers m et n. En passant aux valuations $p-$adiques, on trouve que pour tout nombre premier p,

$$v_p(m') = \min(v_p(m), v_p(n)) \quad \text{et} \quad v_p(n') = \max(v_p(m), v_p(n)) - \min(v_p(m), v_p(n))$$

de sorte que

$$v_p(m') + v_p(n') = \max(v_p(m), v_p(n)) = v_p(m) + v_p(n) - \min(v_p(m), v_p(n)).$$

On déduit que

- ➢ Si $\mathrm{PGCD}(m,n) > 1$, alors il existe un nombre premier p pour lequel $\min(v_p(m), v_p(n)) \geqslant 1$ et la somme des valuations $p-$adiques des nombres écrits au tableau diminue strictement après l'opération d'Alice.
- ➢ Si $\mathrm{PGCD}(m,n) = 1$, alors $(m', n') = (1, mn)$ et le nombre d'entiers strictement plus grands que 1 diminue strictement après l'opération d'Alice.

Dans tous les cas, la quantité suivante est une quantité entière, positive, qui diminue strictement à chaque coup d'Alice :

$$\sum_{p \in \mathcal{P}} \left(\sum_{m \text{ au tableau}} v_p(m) \right) + |\{\text{nombres strictement plus grands que 1 au tableau}\}|,$$

où $\mathcal{P}$ est l'ensemble des nombres premiers divisant au moins un des entiers du tableau, dont on vérifie qu'il est stable à chaque opération.

Ceci justifie qu'Alice ne peut jouer qu'un nombre fini de coups.

2) Notons $n_1, \ldots, n_{2026}$ les entiers inscrits au tableau. La clé est de remarquer que, pour un nombre premier p fixé, la quantité

$$\mathrm{PGCD}(v_p(n_1), \ldots, v_p(n_{2026}))$$

est un invariant des opérations d'Alice. En effet, en reprenant les notations de la question 1), on a

$$\begin{aligned}\mathrm{PGCD}(v_p(m'), v_p(n')) &= \mathrm{PGCD}(\min(v_p(m), v_p(n)), \max(v_p(m), v_p(n)) - \min(v_p(m), v_p(n))) \\ &= \mathrm{PGCD}(\min(v_p(m), v_p(n)), \max(v_p(m), v_p(n))) = \mathrm{PGCD}(v_p(m), v_p(n)).\end{aligned}$$

Donc après l'opération d'Alice, le PGCD de l'ensemble des $v_p(n_i)$ n'a pas changé. Notons le D_p.

Comme à au bout d'un nombre fini d'opération, il ne reste que l'entier M qui est strictement supérieur à 1, on a $v_p(M) = D_p$. Ainsi, les $v_p(M)$ sont déterminées par les entiers de départ, donc M aussi et il ne dépend pas des choix d'Alice.

Exercice 2.35. (2017 ELMO P1) Soit n un entier positif impair, soient $a_1, \dots, a_n$ des entiers strictement positifs et soit P leur produit. Montrer que

$$\mathrm{PGCD}(a_1^n + P, a_2^n + P, \dots, a_n^n + P) \leqslant 2\mathrm{PGCD}(a_1, \dots, a_n)^n.$$

Solution 2.35. On commence par simplifier l'inégalité en exploitant l'homogénéité du problème. Notons $d = \mathrm{PGCD}(a_1, \dots, a_n)$ et, pour tout indice i, $a_i = db_i$. Notons qu'alors $\mathrm{PGCD}(b_1, \dots, b_n) = 1$. De plus, pour tout i,

$$a_i^n + P = d^n b_i^n + d^n b_1 b_2 \dots b_n = d^n (b_i^n + b_1 \dots + b_n).$$

Ainsi, en notant $M = b_1 \dots b_n$, le problème se ramène à montrer

$$\mathrm{PGCD}(b_1^n + M, b_2^n + M, \dots, b_n^n + M) \leqslant 2.$$

Notons δ le membre de gauche. Comme δ divise chacun des $b_i^n + M$, on a $b_i^n \equiv -M \mod \delta$ pour tout i. En multipliant ces congruences, on trouve

$$b_1^n \dots b_n^n \equiv (-M)^n = -(b_1 \dots b_n)^n \mod \delta \quad \Longrightarrow \delta \mid 2(b_1 \dots b_n)^n.$$

Il reste donc à montrer que δ est premier avec chacun des b_i. Supposons qu'il existe un nombre premier p divisent δ et un entier b_i. Alors pour tout j, $p \mid M$ et $p \mid \delta \mid b_j^n + M$, donc $p \mid b_j^n$ et $p \mid b_j$. On déduit que p divise tous les b_j, ce qui est absurde car les b_j sont premiers entre eux dans leur ensemble.

On déduit que δ est premier avec tous les b_i, donc $\delta \mid 2$ et $\boxed{\delta \leqslant 2}$ comme voulu.

Exercice 2.36. (IMO SL 2007 N2) Soient $b, n > 1$ des entiers. On suppose que pour tout entier k, il existe un entier a_k tel que $b - a_k^n$ est divisible par k. Montrer qu'il existe un entier A tel que $b = A^n$.

Solution 2.36. Pour montrer que b est une puissance $n-$ème, on montre que pour tout nombre premier p, n divise $v_p(b)$. On fixe désormais un nombre premier p et on pose $a = v_p(b)$.

L'enjeu est de tester l'hypothèse de l'énoncé pour des valeurs particulières et intelligentes de k. Ici, vu le contexte, il est raisonnable de regarder l'énoncé pour k une puissance de b.
Pour $k = p^{a+1}$, il existe donc un entier $B = a_{p^{a+1}}$ tel que p^{a+1} divise $b - B^n$. On a alors les deux implications :

$$p^\alpha \mid b \quad \text{et} \quad p^\alpha \mid b - B^n \quad \Longrightarrow p^\alpha \mid B^n,$$

$$p^{\alpha+1} \nmid b \quad \text{et} \quad p^{\alpha+1} \mid b - B^n \quad \Longrightarrow p^{\alpha+1} \nmid B^n.$$

On déduit que $\alpha = v_p(B^n) = nv_p(B)$. Ainsi, α est divisible par n, ce qui était le résultat voulu.

Exercice 2.37. (BMO SL 2025 N1) Soit k un entier strictement positif et $n_1, \dots, n_k$ des entiers strictement supérieurs à 1 et deux à deux distincts. On suppose qu'il existe un entier strictement positif a tel que

$$n_1! + \dots + n_k! = a^{n_1}.$$

Montrer que l'un au moins des entiers $n_1, \dots, n_k$ est premier.

Solution 2.37. Soit $(n_1, \dots, n_k, a)$ un $(k+1)-$uplet solution de l'équation ci-dessus. Soit n_i le plus petits des k entiers $n_1, \dots, n_k$.

Considérons également j l'indice tel que n_j est le deuxième plus petit entier parmi $n_1, \dots, n_k$.

Supposons qu'il existe un entier m compris entre $n_i + 1$ et n_j tel que m soit divisible par un nombre premier p inférieur ou égal à n_i. Dans le cas contraire, comme $n_i + 1$ ou $n_i + 2$ est pair donc composé, l'un de ces deux entiers admet un facteur premier inférieur ou égal à n_i. On déduit que $n_j \leqslant n_i + 1$ et que $n_j = n_i + 1$ est premier.

Puisque $n_i! \mid n_\ell!$ pour tout indice ℓ, on a que $n_i! \mid a^{n_1}$. Comme $p \leqslant n_1$, on déduit que $p \mid a^{n_1}$ et que $p^{n_1} \mid a^{n_1}$. Ainsi $p^{n_1} \mid n_1! + \dots + n_k!$.
D'après la formule de Legendre,

$$v_p(n_i!) = \left\lfloor \frac{n_i}{p^1} \right\rfloor + \left\lfloor \frac{n_i}{p^2} \right\rfloor + \ldots \leqslant \frac{n_i}{p^1} + \frac{n_i}{p^2} + \ldots < \frac{n_i}{p-1} \leqslant \frac{n_i}{2}.$$

Par définition de p, on a $p \cdot n_i! \mid n_j! \mid n_\ell$ pour tout indice ℓ. Ainsi,

$$v_p(n_1! + \ldots + n_k! - n_i!) \geqslant v_p(n_1!) + 1.$$

D'autre part, comme $p^{v_p(n_i!)+1}$ ne divise pas $n_1!$, on déduit que $p^{v_p(n_i!)+1}$ ne divise pas le membre de droite de l'inégalité, ce qui conduit à l'inégalité

$$\frac{n_i}{2} + 1 > v_p(n_1!) + 1 > v_p(a^{n_1}) \geqslant n_1 \geqslant n_i.$$

On déduit que $n_i < 2$, ce qui est absurde. On a donc le résultat voulu.

2.3 Travailler modulo p, épisode 1 - état d'esprit

2.3.1 Rappel sur la notion d'inversible

Exercice 2.38. Trouver un inverse pour 12 modulo 37.

Solution 2.38. 12 et 37 sont bien premiers entre eux et on a la relation de Bezout suivante $1 \times 37 - 3 \times 12 = 1$, de sorte que $(-3) \times 12 \equiv 1 \mod 37$. Un inverse pour 12 est donc -3, ou encore 34.

Exercice 2.39. Calculer $\varphi(1001)$ et $\varphi(1111)$.

Solution 2.39. D'après la formule, puisque $1001 = 7 \times 11 \times 13$, $\varphi(1001) = 6 \times 10 \times 12 = 720$.
De même, puisque $1111 = 11 \times 101$, $\varphi(1111) = 10 \times 100 = 1000$.

2.3.2 La structure des restes modulo p et le petit théorème de Fermat

Exercice 2.40. (Théorème d'Euler) Soit n un entier et a un entier premier avec n. Montrer que

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Montrer également par un contre-exemple (a, n) **qu'on n'a pas nécessairement** $a^{\varphi(n)+1} \equiv a \mod n$ pour tout entier a.

Solution 2.40. Considérons l'ensemble $[n]^\star$ des entiers de $\{1, \ldots, n-1\}$ qui sont premiers avec n et fixons $a \in [n]^\star$ et notons a^{-1} son inverse. La fonction

$$f_a : \left\{ \begin{array}{ccc} [n]^\star & \longrightarrow & [n]^\star \\ x & \longmapsto & ax \mod n \end{array} \right.$$

est une bijection de $[n]^\star$ dans lui-même, de bijection réciproque $f_{a^{-1}} : x \mapsto a^{-1}x \mod n$. En effet, on vérifie que f_a est bien à valeurs dans $[n]^\star$, puisque si x et a sont premiers avec n, leur produit n'a pas de facteur premier commun avec n. D'autre part, on a bien $f_{a^{-1}} \circ f_a(x) = f_a \circ f_{a^{-1}}(x) = x$, ce qui permet de conclure que f_a et $f_{a^{-1}}$ sont deux bijections réciproques.

Ainsi, si $[n]^\star = \{x_1, \ldots, x_{\varphi(n)}\}$, on peut également écrire $[n]^\star = \{ax_1, \ldots, ax_{\varphi(n)}\}$ (où les nombres sont pris modulo n). On a donc

$$x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \equiv ax_1 \cdot ax_2 \cdot \ldots \cdot ax_{\varphi(n)} = a^{\varphi(n)} x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \mod n,$$

ce qui, après simplification par l'élément inversible $x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)}$ (si tous les nombres sont premiers avec n, leur produit n'a bien aucun facteur premier commun avec n), donne $\boxed{a^{\varphi(n)} \equiv 1 \mod n}$.

Concernant l'exemple, comme la formule est vraie si a est premier avec n, il faut choisir un couple (a, n) avec a qui n'est pas premier avec n. Le plus simple est de choisir a non divisible par n tel que $a^{\varphi(n)+1} \equiv 0$, par exemple en prenant a ayant les mêmes facteurs premiers que n. On pourra prendre $n = 12$ et $a = 6$ et vérifier $a^{\varphi(12)+1} = a^5 \equiv 0 \neq 6 \mod 12$.

Exercice 2.41. Soit n un entier. Montrer que $42 \mid n^7 - n$ et que n^{13} et n ont le même chiffre des unités.

Solution 2.41. D'après le petit théorème de Fermat, $n^7 \equiv n \mod 7$ donc $7 \mid n^7 - n$.
D'autre part, n^7 et n sont de même parité, donc $2 \mid n^7 - n$.
Enfin, on a la factorisation $n^7 - n = n((n^2)^3 - 1) = n(n^2 - 1)(n^4 + n^2 + 1)$. Or $n(n^2 - 1) = (n-1)n(n+1)$ est le produit de trois entiers consécutifs, donc contient toujours un multiple de 3. On déduit que $3 \mid n^7 - n$.
On a bien $\boxed{2 \cdot 3 \cdot 7 \mid n^7 - n}$.

Remarque : On aurait également pu utiliser le petit théorème de Fermat pour dire que $n^7 = n \cdot n^3 \cdot n^3 \equiv n \cdot n \cdot n \equiv n \mod 3$. On a seulement voulu varier les approches.

Pour la deuxième partie, il suffit de montrer que $10 \mid n^{13} - n$.
Comme n^{13} et n ont même parité, $2 \mid n^{13} - n$.

Aussi, par le petit théorème de Fermat, $n^5 \equiv n \mod 5$, donc

$$n^{13} = n \cdot n \cdot n \cdot n^5 \cdot n^5 \equiv n^5 \equiv n \mod 5,$$

si bien que $5 \mid n^{13} - n$. On a donc bien $\boxed{10 \mid n^{13} - n}$.

Exercice 2.42. (Mexico Regional 2021) Soit $n \geqslant 2021$ et $a_1 < \ldots < a_n$ une suite arithmétique telle que, pour tout indice i, le nombre a_i est un nombre premier strictement plus grand que 2021. Montrer que tout nombre premier p tel que $p < 2021$ divise la raison de la suite.

Solution 2.42. Soit $p < 2021$. L'idée est que, comme tous les termes de la suite sont premiers, ils ne sont pas divisibles par p.
Soit r la raison de la suite arithmétique. On a pour tout indice k que $a_k = a_1 + kr$. Si p ne divise pas r, les termes $a_1, \ldots, a_p$ sont deux à deux distincts modulo p : si on a $j \neq k$ et $a_k \equiv a_j \mod p$, alors $kr \equiv jr \mod p$, ce qui, après simplification par r, donne $k \equiv j \mod p$, ce qui est absurde. Comme ils sont au nombre de p, l'un d'eux est nul modulo p et de fait divisible par p, ce qui contredit l'hypothèse de départ. On déduit que $p \mid r$.

Exercice 2.43. Trouver les polynômes P à coefficients entiers tels que, pour tout entier $n \geqslant 1$, n divise $P(2^n)$.

Solution 2.43. **Réponse :** Les seuls polynômes P solutions sont les polynômes nuls.
Pour montrer que P est nul, il suffit de lui trouver une infinité de racines. En l'occurence, on montre que $P(2^k) = 0$ pour tout k, en montrant que $P(2^k)$ est divisible par une infinité de nombres premiers.
Soit k un entier et p un nombre premier impair. D'après le petit théorème de Fermat et l'identité $a - b \mid P(a) - P(b)$,

$$p \mid (2^k)^p - 2^k \mid P(2^{kp}) - P(2^k).$$

Or, $pk \mid P(2^{kp})$ par hypothèse, donc $p \mid P(2^{kp})$. On déduit que $\boxed{p \mid P(2^k)}$. Ainsi, $P(2^k)$ admet une infinité de diviseurs premiers, il est donc nul, ce qui conclut.

Exercice 2.44. Soit $1 \leqslant k \leqslant p-2$. Montrer, sans utiliser de générateur, que p divise $1^k + 2^k + \ldots + (p-1)^k$.

Solution 2.44. Notons $S_k = 1^k + 2^k + \ldots + (p-1)^k$. Fixons a un élément quelconque de $\{1, \ldots, p-1\}$ tel que $a^k \neq 1$ modulo p. Puisque $x \mapsto ax \mod p$ est une bijection de $\{1, \ldots, p-1\}$ dans lui-même, on a

$$S_k = (1 \cdot a)^k + (2a)^k + \ldots + ((p-1)a)^k = a^k S_k.$$

On déduit que $(1 - a^k)S_k \equiv 0 \mod p$, puis que $S_k \equiv 0 \mod p$ par choix de a.

Exercice 2.45. (Balkan MO SL 2013 N4) Soit $p \geqslant 5$ un nombre premier. Montrer que $1^{p+2} + 2^{p+2} + \ldots + (p-1)^{p+2}$ est divisible par p^2.

Solution 2.45. Dans la somme, on rassemble x^{p+2} avec $(p-x)^{p+2}$. Pour tout $x \leqslant \dfrac{p-1}{2}$, on a

$$(p-x)^{p+2} = (-x)^{p+2} + (p+2)(-x)^{p+1}p + \sum_{k=2}^{p+2} \binom{k}{p+2} (-x)^{p+2-k} p^k \equiv -x^{p+2} + 2px^{p+1} \mod p^2.$$

On déduit que

$$1^{p+2} + 2^{p+2} + \ldots + (p-1)^{p+2} \equiv 2p \sum_{x=1}^{\frac{p-1}{2}} x^{p+1} \mod p^2.$$

Il suffit donc de montrer que la somme du membre de droite est divisible par p. D'après le petit théorème de Fermat, on a

$$\sum_{x=1}^{\frac{p-1}{2}} x^{p+1} \equiv \sum_{x=1}^{\frac{p-1}{2}} x^2 = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2} p}{6} \boxed{\equiv 0} \mod p$$

où on a utilisé que $p \geqslant 5$.

Exercice 2.46. (Nordic MO 2022) Soit $n \geq 5$ 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 :

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

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

Solution 2.46. **Réponse :** Bob a une stratégie gagnante si et seulement si n est premier.

Commençons par le cas où n n'est pas premier : On dispose alors d'un diviseur $1 < d < n$ de n, qu'Alice choisit au premier tour. Elle peut ensuite donner $x_1 = d$ de sorte que : $d \mid \big(x_1x_2(x_1-y_1)(x_2-y_2)\big)^{\frac{n-1}{2}}$.
Ainsi, si Bob gagnait, on aurait :

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

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

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 $p \geq 5$ 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 :

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

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 $\boxed{\text{si et seulement si } n \text{ est premier}}$.

Exercice 2.47. Déterminer tous les entiers $n \geqslant 1$ tels qu'il existe un entier k tel que $n! + n = n^k$.

Solution 2.47. **Réponse :** Il s'agit des entiers $2, 3$ et 5.
Soit n un entier solution et k l'entier donné par l'énoncé. Comme $n! > 0$, on a $k \geqslant 2$. En divisant l'équation par n, on trouve que $(n-1)! + 1 = n^{k-1}$. En regardant l'équation modulo n, on trouve que $(n-1)! \equiv -1 \mod n$. On se doute alors que n est premier.
Si p est un diviseur premier de n tel que $1 < p < n$, alors $p \leqslant n-1$ donc $p \mid (n-1)!$, ce qui contredit que $(n-1)!$ est inversible modulo n. Ainsi, n n'est pas composé et $\boxed{n \text{ est premier}}$.

Si $n = 2$, alors l'équation devient $2 = 2^{k-1}$ qui est vraie pour $k = 2$, et $\boxed{2 \text{ est solution}}$. Si $n = 3$, l'équation devient $3 = 3^{k-1}$ qui est vraie pour $k = 2$, et $\boxed{3 \text{ est solution}}$. Enfin, si $n = 5$, l'équation devient $25 = 5^{k-1}$ qui est vraie pour $k = 3$, donc $\boxed{5 \text{ est solution}}$. On suppose donc que $n \geqslant 7$. Après factorisation et simplification par $n-1$, l'équation devient

$$(n-1)! = n^{k-1} - 1 = (n-1)(1 + \ldots + n^{k-2}) \quad \Longleftrightarrow (n-2)! = 1 + \ldots + n^{k-2}.$$

Les nombres 2 et $\dfrac{n-1}{2}$ sont distincts et inférieurs à $n-2$, donc $n - 1 = 2 \cdot \dfrac{n-1}{2} \mid (n-2)!$. En regardant l'équation ci-dessus modulo $n-1$, et puisque $n \equiv 1 \mod n-1$, on a donc

$$0 \equiv 1 + \ldots + n^{k-2}1 + 1 + \ldots + 1 = k - 1 \mod n-1.$$

Comme $k - 1 \geqslant 1$, on déduit que $k - 1 \geqslant n - 1$. Pourtant

$$n^{k-1} - 1 \geqslant n^{n-1} - 1 > (n-1)^{n-1} > (n-1)!,$$

ce qui est absurde. Il n'y a donc pas de solution lorsque $n \geqslant 7$. Notons que, pour établir l'inégalité stricte $n^{n-1} - 1 > (n-1)^{n-1}$, on a utilisé que $n^{n-1} - (n-1)^{n-1} = n^{n-2} + n^{n-3}(n-1) + \ldots + (n-1)^{n-2} > 1$.

Exercice 2.48. (Olympiade Francophone 2020) Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs et soit m un entier. On suppose que, pour tout ensemble S fini et non vide d'indices strictement positifs, le nombre

$$-1 + \prod_{k \in S} a_k$$

est un nombre premier.

Montrer que, parmi les entiers $a_1, a_2, \ldots$, seul un nombre fini de termes possède moins de m facteurs premiers distincts.

Solution 2.48. Nous allons montrer qu'étant donné un nombre premier p, il existe un entier $N \geq 1$ tel que p divise tous les termes a_k pour $k \geq N$, ce qui nous donnera le résultat voulu.
On suppose par l'absurde qu'il existe une infinité d'entiers a_k qui ne sont pas divisibles par p. Alors d'après le principe des tiroirs, il en existe une infinité qui possède le même reste modulo p. On dispose donc de $p-1$ indices $i_1, \ldots i_{p-1}$ tels que $a_{i_1}, \ldots a_{i_{p-1}}$ possède le même reste modulo p, on note a ce reste. Puisqu'on en dispose d'une infinité, on peut choisir $a_{i_{p-1}}$ supérieur strictement à p. En prenant $S = \{i_1, \ldots, i_{p-1}\}$, on obtient que le nombre

$$-1 + \prod_{k \in S} a_k$$

est un nombre premier. Or d'après notre choix de $a_{i_{p-1}}$, ce nombre est strictement supérieur à p et d'après le théorème de Fermat :

$$\prod_{k \in S} a_k \equiv a^{p-1} \equiv 1 \mod p$$

donc le nombre $-1 + \prod_{k \in S} a_k$ est divisible par p. Comme il est strictement plus grand que p, ce n'est pas un nombre premier ce qui donne la contradiction.

Exercice 2.49. (Baltic Way 2025/Peru TST 2023 et all) Déterminer tous les entiers n tels qu'il existe une permutation $(a_1, \ldots, a_n)$ des entiers $(1, \ldots, n)$ telle que les nombres $a_1, 2a_2, \ldots, na_n$ forment des résidus distincts modulo n.

Solution 2.49. **Réponse :** Les seuls entiers sont $n = 1, 2$.

Soit n un entier solution. On considère la permutation $(a_1, \ldots, a_n)$ donnée par l'énoncé. Les entiers sont implicitement mais systématiquement pris modulo n.

Étape 1 : n est sans facteur carré.

Soit d un diviseur de n. L'ensemble $\{1, \ldots, n\}$ contient n/d multiples de d, donc il en est de même des ensembles $\{a_1, \ldots, a_n\}$ et $\{a_1, 2a_2, \ldots, na_n\}$. Comme les nombres $da_d, 2da_{2d}, \ldots, na_n$ sont déjà n/d multiples de d, il s'agit des seuls. On déduit que si $d \mid a_k$, alors $d \mid ka_k$ donc k est un indice multiple de d. Bref, $\boxed{\text{si } d \mid a_k, \text{ alors } d \mid k}$.
En particulier, $n = a_n$.
Si p est un diviseur premier de n tel que $p^2 \mid n$, alors les multiples de p sont exactement $a_p, a_{2p}, \ldots, a_n$, et les seuls multiples de p^2 parmi $\{a_1, 2a_2, \ldots, na_n\}$ sont $p^2 a_{p^2}, \ldots, na_n$. Pourtant, $p^2 \mid pa_p$, ce qui est une contradiction. Donc $\boxed{n \text{ est sans facteur carré}}$.

Étape 2 : $n = 1, 2$.

Supposons que n admet un facteur premier p. On note $n = pm$. L'ensemble des multiples de m de $[\![1, n-1]\!]$ est donc l'ensemble $\{m, 2m, \ldots, (p-1)m\} = \{a_m, a_{2m}, \ldots, a_{(p-1)m}\} = \{ma_m, \ldots, (p-1)ma_{(p-1)m}\}$. Les produits des éléments sont donc égaux, soit

$$a_m \ldots a_{(p-1)m} \equiv ma_m \cdot 2ma_{2m} \cdot \ldots \cdot (p-1)ma_{(p-1)m} = (p-1)! m^{p-1)} a_m \ldots a_{(p-1)m} \mod n.$$

En particulier, la congruence tient modulo p, et comme les a_{km} sont des multiples de m inférieurs à $(p-1)m$, ils sont premiers avec p et on trouve en simplifiant que $(p-1)! m^{p-1} \equiv 1 \mod p$. Pourtant, d'après le petit théorème de Fermat et le théorème de Wilson, on a $m^{p-1}(p-1)! \equiv 1 \cdot -1 \equiv -1 \mod p$. On conclut que $1 \equiv -1 \mod p$ et que $p = 2$. Le seul facteur premier éventuel de n est donc 2, d'où $\boxed{n = 1, 2}$.

Réciproquement, si $n = 1$, le nombre $a_1 = 1$ convient et si $n = 2$, le couple $(1, 2)$ convient également.

Exercice 2.50. (Poland MO 2020 Round 2) Soit p un nombre premier et S un ensemble de $p+1$ entiers. Montrer qu'il existe $a_1, \ldots, a_{p-1} \in S$ des entiers distincts tels que

$$p \mid a_1 + 2a_2 + 3a_3 + \ldots + (p-1)a_{p-1}.$$

Solution 2.50. On transforme plutôt la condition en trouver $a_1, \ldots, a_p$ tels que

$$p \mid a_1 + 2a_2 + \ldots + (p-1)a_{p-1} + pa_p,$$

de sorte qu'il s'agit désormais d'éjecter un seul élément et de faire "tourner" les p autres.

Si tous les éléments de S sont égaux modulo p, alors le choix de p quelconque d'entre eux convient. On suppose donc qu'il existe deux éléments a et b distincts modulo p. En notant s la somme des éléments de s, on a que l'un des deux nombres $s-a$ et $s-b$ est non nul modulo p. On a donc établi qu'il existe $a_1, \ldots, a_p$ dans S dont la somme est non divisible par p. On note cette somme A. On note également $B = a_1 + \ldots + (p-1)a_{p-1} + pa_p$. On va chercher une combinaison de A et B de la forme $B + kA$ qui est divisible par p.

Comme $A \neq 0 \mod p$, on peut choisir $k = -BA^{-1} \mod p$, qui vérifie bien $p \mid A + kB$. On vérifie que

$$\begin{aligned} 0 \equiv B + kA &= a_1 + \ldots + (p-1)a_{p-1} + pa_p + ka_1 + \ldots + ka_p \\ &= (k+1)a_1 + (k+2)a_2 + \ldots + (k+p-1)a_{p-1} + (k+p)a_p \\ &\equiv a_{p+1-k} + 2a_{p+2-k} + \ldots + (p-1)a_{p-1-k} + pa_{p-k} \mod p. \end{aligned}$$

Donc les entiers $(b_1, \ldots, b_p) = (a_{p+1-k}, \ldots a_{p-k})$ conviennent.

Exercice 2.51. (ELMO 2019 P5) Soit S un ensemble non vide d'entiers strictement positifs vérifiant la propriété suivante : pour tous entiers a et b de S, l'entier $ab+1$ est également dans S.

Montrer qu'il n'existe qu'un nombre fini de nombres premiers ne divisant aucun élément de S.

Solution 2.51. Soit p un nombre premier et soit $a_1, a_2, \ldots a_k$ les restes possibles des éléments de S modulo p. On suppose que 0 n'appartient pas à $R = \{a_1, \ldots, a_k\}$, c'est-à-dire que p ne divise aucun élément de S.
On sait que pour tout i, j, $a_i a_j + 1 \in R$. Notons que si j et ℓ sont distincts, alors $a_i a_j + 1$ et $a_i a_\ell + 1$ sont distincts. En effet

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

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

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

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

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

Comme cette expression ne dépend pas de i, les a_i sont tous égaux et R est un singleton noté $\{a\}$. On a alors $a^2 + 1 \equiv a \mod p$ donc $p \mid a^2 + 1 - a$ et $p \leq n^2 - n + 1$ pour tout n dans S. Si n_0 est le plus petit élément de S, alors en particulier $p \leq n_0^2 - n_0 + 1$.

En conclusion, si p ne divise aucun élément de S, p est borné par $n_0^2 - n_0 + 1$. Ainsi l'ensemble des nombres premiers ne divisant aucun élément de S est fini.

Exercice 2.52. (IMO SL 2017 N2) Soit $p \geqslant 2$ un nombre premier. Alice et Bob jouent au jeu suivant. Chacun à leur tour en commençant par Alice, ils choisissent un indice i dans $\{0, 1, \ldots, p-1\}$ qui n'a pas encore été choisi précédemment par l'un des deux joueurs, puis choisissent un nombre a_i de $\{0, \ldots, 9\}$. Lorsque tous les indices sont choisis, on considère le nombre

$$M = a_0 \cdot 10^0 + a_1 \cdot 10^1 + \ldots + a_{p-1} \cdot 10^{p-1}.$$

Alice gagne si M est divisible par p, Bob gagne sinon. Montrer qu'Alice dispose d'une stratégie gagnante.

Solution 2.52. On met de côté les cas $p = 2$ et $p = 5$, pour lesquels il suffit de choisir $a_0 = 0$ pour Alice. Posons $d = \dfrac{p-1}{2}$.

Dans la suite, on cherche à mettre en place une stratégie miroir. Alice commence pour cela par choisir $i = p-1$ et $a_{p-1} = 0$. Puis par la suite, on considère les paires d'indices $(i, d+i)$, qui partitionnent l'ensemble des indices restant. On doit donc aider Alice à bien choisir a_i ou a_{d+i} lorsque Bob a choisi l'un de ces indices. On distingue alors deux cas :

a) $10^d = -1 \mod p$.

b) $10^d = 1 \mod p$.

A noter qu'il n'y a pas d'autre cas car le petit théorème de Fermat indique que $p \mid 10^{2d} - 1 = (10^d - 1)(10^d + 1)$.

Dans le premier cas : si Bob choisit l'indice i et le chiffre a_i, alors Alice choisit l'indice $i+d$ et le chiffre $a_{i+d} = a_i$, de sorte que $a_{i+d}10^{i+d} + a_i 10^i = a_i 10^i(10^d + 1)$ est bien divisible par p (de même, si Bob joue $(i+d)$ et a_{i+d}, Alice joue i et $a_i = a_{i+d}$. A la fin du jeu, M est bien divisible par p comme somme d'entiers divisibles par p.

Dans le second cas, Alice choisit a_i (ou a_{i+d}) de sorte que $a_i + a_{i+d} = 9$. Alors $a_{i+d}10^{i+d} + a_i 10^i \equiv 9 \cdot 10^i \mod p$, de sorte que

$$M \equiv \sum_{i=0}^{d-1} 9 \cdot 10^i = 10^d - 1 = 0 \mod p.$$

Dans tous les cas, Alice gagne.

2.3.3 Imprégnation de la notion d'inverse - Apprendre à écrire $\frac{1}{i}$ plutôt que i^{-1}

Exercice 2.53. Soit p un nombre premier. Soient i et j deux entiers premiers avec p. Avec ces notations, vérifier que $\dfrac{1}{i} + \dfrac{1}{j} \equiv \dfrac{i+j}{ij} \mod p$.

Solution 2.53. Il s'agit de vérifier que $i^{-1} + j^{-1} \equiv (i+j)(ij)^{-1} \mod p$. Or, on a bien

$$(ij)(i^{-1} + j^{-1}) \equiv jii^{-1} + ijj^{-1} \equiv j + i \mod p,$$

la relation voulue s'obtient en multipliant des deux côtés de l'équation par $(ij)^{-1}$.

Exercice 2.54. Soit p un nombre premier et a un entier premier avec p.

- ➢ Montrer que $(p-3)! \equiv -\dfrac{1}{2} \mod p$.
- ➢ Remarquer que $a^{p-2} \equiv \frac{1}{a} \mod p$.

Solution 2.54.

- ➢ D'après le théorème de Wilson, $(p-1)! \equiv -1 \mod p$. En multipliant des deux côtés par $(p-2)^{-1}(p-1)^{-1}$, on trouve

$$(p-3)! \equiv -(p-2)^{-1}(p-1)^{-1} \equiv -(-2)^{-1}(-1)^{-1} \equiv -\frac{1}{2} \mod p.$$

- ➢ D'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \mod p$. En multipliant par a^{-1} des deux côtés, on déduit $a^{p-2} \equiv a^{-1} = \dfrac{1}{a} \mod p$.

Exercice 2.55. Soit $p \geqslant 2$ un entier. Montrer que p et $p+2$ sont des nombres premiers si et seulement si $p(p+2)$ divise $4((p-1)! + 1) + p$.

Solution 2.55. On procède par double implication :

$\boxed{\Rightarrow}$ On suppose que p et $p+2$ sont premiers. D'après le théorème de Wilson appliqué à $(p-1)!$,

$$4((p-1)! + 1) + p \equiv 4(-1+1) + p \equiv 0 \mod p.$$

D'autre part, toujours avec le théorème de Wilson appliqué à $p+2$, $(p+1)! \equiv -1 \mod p+2$, ce qui implique que $(p-1)! \equiv \dfrac{-1}{p(p+1)} \equiv -\dfrac{1}{2} \mod p+2$. On a alors

$$4((p-1)!+1)+p \equiv 4\left(\frac{1}{2}+1\right)-2=0 \mod p+2,$$

ce qui signifie que p et $p+2$, qui sont premiers entre eux, divisent l'expression, comme voulu.

$\boxed{\Leftarrow}$ On suppose que l'on a la division. Si $p=2$, alors $p(p+2)=8$ tandis que $4((p-1)!+1)+p=6$, ce qui est absurde. Ainsi, p est impair et on déduit que p divise $(p-1)!+1$. Supposons que p admette un diviseur strict d. Comme $1<d<p$, d divise $(p-1)!$. On a alors modulo d

$$0 \equiv 4(0+1)+0=4 \mod d,$$

ce qui implique que $d \mid 2$, ce qui est absurde car p est impair. Ainsi, p est premier.

Supposons que $p+2$ admette un diviseur strict d. Si $d=p$, alors $p \mid p+2$, ce qui conduit à $p=2$. Si $d=p+1$, alors $p+1 \mid p+2$, ce qui conduit à 0. Les deux cas étant absurde, $d \leqslant p-1$, donc il divise $(p-1)!$. On déduit modulo d

$$0 \equiv 4(0+1)+(-2)=2 \mod d,$$

ce qui est encore absurde. $p+2$ est donc bien premier.

$\boxed{\text{Remarque :}}$ On aurait aussi pu remonter les calculs du sens $\boxed{\Rightarrow}$ et utiliser la réciproque du théorème de Wilson.

Exercice 2.56. *(Pays-Bas BXMO TST 2018)* Soit p un nombre premier. Montrer qu'il existe une permutation $a_1, \ldots, a_{p-1}$ de $1, \ldots, p-1$ telle que les nombres $a_1, a_1a_2, \ldots, a_1a_2 \ldots a_{p-1}$ donnent $p-1$ restes distincts modulo p.

Solution 2.56. **Réponse :** Oui

On peut être très optimiste sur cet exercice et vouloir que $a_1a_2 \cdots a_k \equiv k \mod p$ pour tout k compris entre 1 et p. On s'inspire alors de la construction de k rationnels dont le produit vaut k. Il faut que $a_1=1$ et pour tout $k \neq 1$:

$$a_k \equiv \frac{a_1 \cdots a_k}{a_1 \cdots a_{k-1}} \equiv \frac{k}{k-1} \mod p$$

Posons donc $\boxed{a_k = \frac{k}{k-1} \mod p}$ pour tout $k \geqslant 2$. Un télescopage donne bien que $a_1 \ldots a_k \equiv k$ pour tout indice $k \geqslant 2$.

Comme l'écriture $a_k = 1 + \dfrac{1}{k-1}$ permet de voir immédiatement que les a_k sont deux à deux disjoints modulo p, $(a_1, a_2, \cdots, a_p)$ est bien une permutation de $(1, 2, \cdots p)$.

Exercice 2.57. *(Thaïlande MO 2022 P7)* Soit p un nombre premier et $a_1, \ldots, a_p, b_1, \ldots, b_p$ des entiers de $\{1, \ldots, p-1\}$. Montrer qu'il existe deux indices $i \neq j$ tels que $a_ib_j - a_jb_i$ est divisible par p.

Solution 2.57. Les expressions "couplent" les indices i et j, on peut donc commencer par réécrire l'expression pour séparer les termes en i et en j afin d'appliquer le principe des tiroirs.

Deux indices $i \neq j$ satisfaisant l'énoncé vérifient, étant donné que b_i et b_j sont inversibles modulo p,

$$0 \equiv a_ib_j - a_jb_i \equiv b_ib_j\left(\frac{a_i}{b_i} - \frac{a_j}{b_j}\right) \mod p$$

et donc

$$\frac{a_i}{b_i} \equiv \frac{a_j}{b_j} \mod p.$$

On peut désormais montrer l'exercice. Les p nombres $\dfrac{a_i}{b_i} \mod p$ sont à valeur dans $\{1, \ldots, p-1\}$. D'après le principe des tiroirs, il existe alors deux indices i et j distincts tels que la congruence ci-dessus est satisfaite, ce qui conclut.

Exercice 2.58. (ELMO SL 2010 N2) Soit p un nombre premier impair. Montrer que

$$\left(1+p\sum_{k=1}^{p-1}k^{-1}\right)^2 \equiv 1-p^2\sum_{k=1}^{p-1}k^{-2} \mod p^4,$$

où les inverses sont pris modulo p^4.

Solution 2.58. Notons $S_{-1}=\sum_{k=1}^{p-1}k^{-1}$ et $S_{-2}=\sum_{k=1}^{p-1}k^{-2}$. D'après l'exemple de la théorie, le numérateur de S_{-1} est divisible par p^2, tandis que le dénominateur n'est pas divisible par p. Il vient en développant que

$$(1+pS_{-1})^2 = 1+p^2S_{-1}^2+2pS_{-1} \equiv 1+2pS_{-1} \mod p.$$

Il s'agit alors de montrer que $2pS_{-1}\equiv -p^2S_{-2} \mod p^4$, ou encore, en simplifiant par p, $2S_{-1}\equiv -pS_{-2} \mod p^3$. De manière analogue à l'exercice 2.53, on a pour tout $k<p-1$ que $\frac{1}{k}+\frac{1}{p-k}\equiv\frac{p}{k(p-k)}$. On a donc

$$2S_{-1}=2\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{1}{k}+\frac{1}{p-k}\right)=2\sum_{k=1}^{\frac{p-1}{2}}\frac{p}{k(p-k)}=p\sum_{k=1}^{p-1}\frac{1}{k(p-k)},$$

où le facteur 2 permet de ramener la somme en une somme de p termes. Il suffit donc de montrer que $\sum_{k=1}^{p-1}\frac{1}{k(p-k)}\equiv -S_{-2} \mod p^2$. Or on a

$$\sum_{k=1}^{p-1}\frac{1}{k(p-k)}+\sum_{k=1}^{p-1}\frac{1}{k^2}=\sum_{k=1}^{p-1}\frac{1}{k}\left(\frac{1}{k}+\frac{1}{p-k}\right)\equiv\sum_{k=1}^{p-1}\frac{1}{k}\frac{p}{k(p-k)} \mod p^2.$$

On peut à nouveau simplifier par p. Enfin, utilisant que $k\mapsto k^{-1}$ est une bijection modulo p,

$$\sum_{k=1}^{p-1}\frac{1}{k^2(p-k)}\equiv-\sum_{k=1}^{p-1}k^{-3}\equiv-\sum_{k=1}^{p-1}k^3=p^2\frac{(p-1)^2}{4}=0 \mod p.$$

Ceci conclut.

Exercice 2.59. (Mexique 2012) Soit p un nombre premier impair. Pour tout $i\in\{1,\dots,p-1\}$, on note r_i le reste de i^p par p^2. Calculer $r_1+\ldots+r_{p-1}$.

Solution 2.59. On couple l'élément i et l'élément $p-i$ dans notre calcul. La formule du binôme donne que

$$(p-i)^p=(-i)^p+\sum_{k=1}^{p-1}\binom{p}{k}p^k(-i)^{p-k}+p^p.$$

Dans chaque terme de la somme, $p\mid\binom{p}{k}$ et $p\mid p^k(-i)^{p-k}$, donc chaque terme de la somme est divisible par p^2. Il en est de même pour p^2. On déduit que $(p-i)^p\equiv -i^p \mod p^2$. Ceci conduit à $\boxed{r_i+r_{p-i}\equiv i^p-i^p=0 \mod p^2}$, donc r_i+r_{p-i} est un multiple de p^2. Comme en plus $0<r_i+r_{p-i}<2p^2$, on trouve que $r_i+r_{p-i}=p^2$. On conclut

$$r_1+\ldots+r_{p-i}=\sum_{k=1}^{\frac{p-1}{2}}(r_i+r_{p-i})=\frac{p-1}{2}p^2.$$

Exercice 2.60. (inspiré de IMAR 2023) Soit p un nombre premier. Montrer qu'il existe une permutation $(a_1,\dots,a_{p-1})$ de $(1,\dots,p-1)$ telle que, pour tout triplet (i,j,k) d'indices distincts,

$$(i-j)a_k+(j-k)a_i+(k-i)a_j\neq 0 \mod p.$$

Solution 2.60. On tente les bijections connues, en remarquant que si $(a_1, \dots, a_{p-1})$ est solution, il en est de même pour $(ba_1 + c, ba_2 + c, \dots, ba_{p-1} + c)$. Il n'y a donc que très peu de familles de permutations que l'on peut chercher.

On essaye $\boxed{a_i \equiv \frac{1}{i} \mod p}$. Il s'agit bien d'une permutation. On a alors

$$\begin{aligned}(i-j)a_k + (j-k)a_i + (k-i)a_j &\equiv \frac{i-j}{k} + \frac{j-k}{i} + \frac{k-i}{j} \mod p \\ &\equiv \frac{ij(i-j) + jk(j-k) + ik(k-i)}{ijk} \mod p\end{aligned}$$

Un effort de factorisation est ici nécessaire. Le numérateur ci-dessus, vu comme un polynôme de degré 2 en i, s'annule lorsque $i = j$ et lorsque $i = k$. On peut donc factoriser ce polynôme, ce qui conduit à

$$(i-j)a_k + (j-k)a_i + (k-i)a_j \equiv \frac{(i-j)(k-i)(j-k)}{ijk} \neq 0 \mod p$$

puisque les indices i, j et k sont distincts. La permutation (a_i) convient donc bien.

Exercice 2.61. (IMC 2022 P6) Soit p un nombre premier impair. Montrer qu'il existe une permutation $(a_1, \dots, a_{p-1})$ de $(1, \dots, p-1)$ telle que

$$a_1a_2 + a_2a_3 + \dots + a_{p-2}a_{p-1} \equiv 2 \mod p.$$

Solution 2.61. Ici, on peut penser à l'identité $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$ pour produire un télescopage. On pose alors $\boxed{a_i = \frac{1}{i} \mod p}$ qui est bien une bijection. On vérifie bien que

$$\begin{aligned}a_1a_2 + a_2a_3 + \dots + a_{p-2}a_{p-1} &\equiv \frac{1}{1\cdot 2} + \dots + \frac{1}{k(k+1)} + \dots + \frac{1}{(p-2)(p-1)} \\ &\equiv \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \dots + \left(\frac{1}{p-2} - \frac{1}{p-1}\right) \\ &= 1 - \frac{1}{p-1} \equiv 2 \mod p.\end{aligned}$$

Exercice 2.62. (Entraînement groupe D 2022) Soit $p \geqslant 5$ un nombre premier et $k \geqslant 2$. Théo et Vincent jouent au jeu suivant : Théo choisit une permutation $a_1, \dots, a_k$ des entiers $1, \dots, k$ et indique à Vincent ce que vaut $a_ia_j \mod p$ pour tous $i \neq j$. Vincent gagne s'il est capable de retrouver les valeurs des a_i. Pour quelles valeurs de k Vincent peut-il gagner à coup sûr quelle que soit la permutation choisie par Théo ?

Solution 2.62. **Réponse :** Les valeurs recherchées sont les entiers $k = 3, 4, \dots, p-2$.

Tout d'abord, si $k \geqslant p+1$, alors la permutation choisie par Théo et la même permutation mais où 1 et $p+1$ sont échangés sont deux permutations qui donneront les mêmes produits a_ia_j modulo p, Vincent ne pourra donc pas retrouver la permutation à coup sur.

Si $k = 2$, les permutations $(1, 2)$ et $(2, 1)$ donnent le même produit a_1a_2 donc on ne peut pas les distinguer.

Si $k = p-1$ ou p, les permutations $(a_1, \dots, a_k)$ et $(p - a_1, \dots, p - a_k)$ vont donner les mêmes produits a_ia_j modulo p, donc Vincent ne pourra pas retrouver les a_i.

On déduit que $\boxed{3 \leqslant k \leqslant p-2}$. Prenons maintenant un tel entier k. Pour tout i, Vincent peut déterminer la valeur de $a_i^2 \equiv \frac{(a_ia_j)(a_ia_\ell)}{(a_ja_\ell)} \mod p$ (où j et ℓ sont deux indices quelconques). Comme 1 figure parmi les a_i mais pas -1, il y a un unique a_i tel que $a_i^2 = 1$, ce qui conduit à $a_i = 1$. Vincent peut alors retrouver a_j pour tout $j \neq i$ via $a_j \equiv a_ia_j$, et il gagne donc dans ce cas.

Exercice 2.63. (IMO SL 2020 N1) Soit $k \geqslant 1$ un entier. Montrer qu'il existe un nombre premier p tel qu'on peut choisir des entiers $a_1, a_2, \dots a_{k+3}$ distincts dans l'ensemble $\{1, 2, \dots, p-1\}$ tels que, pour tout indice $i = 1, 2, \dots, k$, l'entier p divise $a_i a_{i+1} a_{i+2} a_{i+3} - i$.

Solution 2.63. La stratégie est, à l'image des exercices précédents, de d'abord travailler avec des rationnels avant de convertir les calculs modulo p.

Étape 1 : Supposons avoir construit des rationnels distincts $\frac{b_1}{c_1}, \dots, \frac{b_{k+3}}{c_{k+3}}$ (sous forme irréductible) tels que $\frac{b_i}{c_i}\frac{b_{i+1}}{c_{i+1}}\frac{b_{i+2}}{c_{i+2}}\frac{b_{i+3}}{c_{i+3}} = i$ pour $i = 1, \dots, k$. Pour convertir cette égalité modulo p, on choisit p un grand nombre premier. Il faut notamment que les c_i soient non nuls modulo p (pour être inversibles) et que $\frac{b_j}{c_j} \neq \frac{b_i}{c_i} \mod p$, soit $b_j c_i \neq b_i c_j \mod p$ pour toute paire d'indices (i, j). Il suffit pour cela de prendre $p > \max\{b_i, i \in [\![1, k+3]\!]\}, \max\{|b_i c_j - b_j c_i|, i, j \in [\![1, k+3]\!]\}$. Les nombres $b_i c_i^{-1} \mod p$ conviennent alors.

Étape 2 : On construit des rationnels $a_1, \dots, a_{k+3}$ vérifiant l'égalité $a_i a_{i+1} a_{i+2} a_{i+3} = i$ pour tout indice $i \leqslant k$. Pour tout indice i, en regardant l'égalité pour i et $i+1$, on déduit qu'on doit avoir

$$\frac{a_{i+4}}{a_i} = \frac{a_{i+4} a_{i+1} a_{i+2} a_{i+3}}{a_i a_{i+1} a_{i+2} a_{i+3}} = \frac{i+1}{i}.$$

On déduit qu'une fois a_1, a_2, a_3, a_4 choisis de sorte que $a_1 a_2 a_3 a_4 = 1$, on peut construire les autres a_i via la relation de récurrence $a_{i+4} = a_i \frac{i+1}{i}$, et l'égalité $a_i a_{i+1} a_{i+2} a_{i+3} = i$ sera satisfaite pour tout indice.

Étape 3 : On choisit a_1, a_2, a_3, a_4 de sorte que les a_i sont tous distincts. On commence par remarquer que la relation de récurrence sur (a_i) implique que $a_1 < a_5 < \dots < a_{4\ell+1}$, $a_2 < a_6 < \dots < a_{4\ell+2}$, $a_3 < a_7 < \dots < a_{4\ell+3}$ et $a_4 < a_8 < \dots < a_{4\ell+4}$. Il suffit donc de garantir qu'aucune de ces quatre sous-suites strictement croissante n'a de terme en commun. Pour cela, on dispose de deux mathéodes :

- ➢ La méthode arithmétique : on choisit $a_1 = q_1, a_2 = q_2, a_3 = q_3$ et $a_4 = 1/q_1 q_2 q_3$, avec q_1, q_2, q_3 trois nombres premiers strictement plus grand que $k+3$. La construction précédente implique que, pour tout ℓ et tout numéro $i = 1, 2, 3$, le numérateur de $a_{4\ell+i}$ est divisible par q_i mais pas par un autre q_j. Elle implique aussi que le numérateur de $a_{4\ell+4}$ n'est jamais divisible par un q_i. Il vient que les quatre sous-suites définies plus haut n'ont jamais de terme en commun.
- ➢ La méthode de taille : on choisit $a_1 = 1, a_2 = A, a_3 = A^2$ et $a_4 = 1/A^3$, où A est un entier assez grand pour que $a_{4\ell+4} < 1 \leqslant a_{4\ell+1} < A \leqslant a_{4\ell+2} < A^2 \leqslant a_{4\ell+3}$, pour tout indice ℓ. Cela garantit que les quatre sous-suites n'ont aucun terme commun.

Exercice 2.64. (Balkan MO 2016) Déterminer tous les polynômes P à coefficients entiers et de coefficient dominant 1 vérifiant la condition suivante : il existe un entier $N \geqslant 1$ tel que, pour tout nombre premier $p > N$ vérifiant $P(p) > 0$, p divise $2 \cdot P(p)! + 1$.

Solution 2.64. **Réponse :** Le seul polynôme solution est $X - 3$.

Tout d'abord, puisque P est de coefficient dominant 1, il est strictement positif sur un intervalle de la forme $[A, +\infty[$. Ainsi, quitte à remplacer N par $\max(N, A)$, on peut supposer que pour tout $p > N$, on a $P(p) > 0$.

Soit $p > N$ un nombre premier. Comme $p \mid 2 \cdot P(p)! + 1$, p est premier avec $P(p)!$. En particulier, $\boxed{P(p) < p}$ (sinon p diviserait $P(p)!$). On déduit que $\boxed{\deg P \leqslant 1}$. En effet, dans le cas contraire, par croissance comparée, on aurait $P(p) \geqslant \frac{1}{2}p^2 > p$ pour tout p suffisamment grand.

On dispose donc d'un entier a tel que $P(X) = X - a$. De plus, l'inégalité $P(p) < p$ pour tout $p > N$ premier implique que $a > 0$. Pour tout p suffisamment grand, on obtient que $p \mid 2(p-a)! + 1$, soit $2(p-a)! \equiv -1 \mod p$. D'après le théorème de Wilson, on a alors

$$2(p-a)! \equiv -1 \equiv (p-1)! \mod p,$$

ce qui se simplifie en

$$2 \equiv (p-1)\dots(p-a+1) \equiv (-1) \cdot \dots \cdot (-a+1) \equiv (-1)^{a-1}(a-1)! \mod p.$$

Le nombre $2-(-1)^{a-1}(a-1)!$ admet donc une infinité de diviseurs et est nul. On déduit que $a-1$ est pair, puis que $(a-1)!=2$ et $\boxed{a=3}$.

Réciproquement, si $a=3$, on vérifie que pour tout p premier impair,

$$2(p-3)! \equiv 2\frac{(p-1)!}{(p-1)(p-2)} \equiv 2\frac{(-1)}{(-1)(-2)} \equiv -1 \mod p,$$

ce qui implique bien que $p \mid 2(p-3)!+1$. Donc $X-3$ est bien solution.

Exercice 2.65. (IMO 2024 P2) Déterminer tous les couples (a,b) d'entiers strictement positifs pour lesquels il existe des entiers strictement positifs g et N tels que l'égalité

$$\mathrm{PGCD}(a^n+b, b^n+a) = g$$

soit vérifiée pour tout entier $n \geqslant N$.

Solution 2.65. **Réponse :** Le seul couple (a,b) solution est $(1,1)$.

Soit (a,b) un couple solution. Prenons k un entier strictement positif et $n = k\varphi(ab+1)-1$. Notons que les nombres a et $ab+1$ sont premiers entre eux. Ainsi, en notant a^{-1} l'inverse de a modulo $ab+1$ et en utilisant le théorème d'Euler,

$$a^n+b = a^{k\varphi(ab+1)}a^{-1}+b \equiv a^{-1}+b = a^{-1}(1+ab) \equiv 0 \mod ab+1.$$

De la même façon, $ab+1 \mid b^n+a$. Ainsi, il existe une infinité d'entiers n tels que $ab+1 \mid \mathrm{PGCD}(a^n+b, b^n+a)$. En particulier, $ab+1$ divise g. Pour un entier n suffisamment grand, on déduit que $ab+1$ divise a^n+b et $a^{n+1}+b$. On a donc

$$ab+1 \mid a^{n+1}+b-(a^n+b) = a^n(a-1).$$

Puisque $ab+1$ est premier avec a^n, on déduit que $ab+1$ divise $a-1$. Or, $ab+1 > a-1 \geqslant 0$. On déduit que $a=1$. De la même façon, on prouve que $b=1$.

Réciproquement, on vérifie que pour $a=1$ et $b=1$, on a $a^n+b = b^n+a = 2$, de sorte que le couple $(1,1)$ est bien solution du problème.

Exercice 2.66. (RMM 2026 P2) Soit $p \geqslant 11$ un nombre premier. On suppose que, pour tous a,b entiers tels que $1 \leqslant a < b \leqslant p-3$, le nombre $b!-a!$ n'est pas divisible par p. Montrer que 8 divise $p-5$.

Solution 2.66.

➢ **Commentaire :**

> L'énoncé dit que les nombres $1, 2!, 3!, \ldots, (p-3)!$ sont deux à deux distincts modulo p. L'idée principale du problème est de partir du théorème de Wilson pour calculer $(p-k)!$ et $\left(\frac{p-k}{2}\right)!$ pour des k bien choisis :
>
> $$(p-1)! \equiv -1 \mod p \iff (p-k)! \equiv \frac{-1}{(p-1)\ldots(p-k+1)} \equiv (-1)^k\frac{1}{k!} \mod p.$$
>
> Bien que cela soit l'idée principale, elle ne rapporte pas beaucoup de points à elle seule si elle n'est pas appliquée aux bons entiers cas pour en déduire des résultats sensibles.

Soit p un nombre premier vérifiant l'énoncé.

Étape 1 : $p \equiv 1 \mod 4$.

Supposons que $p \equiv 3 \mod 4$. D'après le théorème de Wilson,

$$\begin{aligned} -1 \equiv (p-1)! = \left(\frac{p-1}{2}\right)! \cdot (p-1)\ldots\left(p-\frac{(p-1)}{2}\right) &\equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \\ &\equiv \left(\frac{p-1}{2}\right)! = (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p. \end{aligned}$$

Comme $p \equiv 3 \mod 4$, cela donne que $p \mid \left(\left(\frac{p-1}{2}\right)!\right)^2 - 1$. On déduit que $\left(\frac{p-1}{2}\right)! = \pm 1 \mod p$. Mais il ne peut pas valoir 1, car 1! et $\left(\frac{p-1}{2}\right)!$ donnent des restes distincts modulo p. Donc $\left(\frac{p-1}{2}\right)! = -1 \mod p$. Mais comme $\frac{p-1}{2} \equiv -1/2 \mod p$, on trouve que

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

ce qui est absurde. Ainsi, $p \neq 3 \mod 4$ donc $p \equiv 1 \mod 4$. Notons qu'alors, le calcul ci-dessus donne $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \mod 4$.

Étape 2 : Il n' existe pas de $a \leqslant p-3$ tel que $a! \equiv -1$.

D'après le théorème de Wilson, on a

$$(p-1)! \equiv -1 \mod p \iff (p-k)! \equiv \frac{-1}{(p-1)\dots(p-k+1)} \equiv (-1)^k \frac{1}{(k-1)!} \mod p.$$

En particulier, appliqué à $a+1$, on trouve $(p-a-1)! \equiv (-1)^{a+1}$. Mais $(p-a-1)!$ ne peut valoir $1 = 1!$ ou $-1 = a!$, sauf si $a = \frac{p-1}{2}$. Mais on a vu ci-dessus que si $\left(\frac{p-1}{2}\right)! \equiv -1$, alors $\left(\frac{p-3}{2}\right)! \equiv 2 \mod p$. Ceci conclut cette étape.

Étape 3 : Conclusion.

Les entiers $1!, \dots, (p-3)!$, étant deux à deux distincts, leur produit correspond au produit de $(p-3)$ nombres distincts modulo p. Notons b et -1 les deux entiers n'étant pas dans l'ensemble $\{1!, \dots, (p-3)!\}$. Le produit des nombres $1!, \dots, (p-3)!, -1, b$ correspond donc au produit des nombres $1, \dots, p-1$. On a donc, de nouveau par le théorème de Wilson,

$$-1 \equiv (-1)b \cdot 1! \cdot 2! \cdot \dots (p-1)! \mod p.$$

En s'aidant de la formule établie plus haut donnant que $(p-k-1)!k! \equiv (-1)^{k+1} \mod p$, et en rassemblant $k!$ et $(p-1-k)!$ dans le produit ci-dessus, on trouve

$$-1 \equiv (-b) \cdot \prod_{k=1}^{\frac{p-1}{2}} k!(p-1-k)! \equiv (-b)(-1)^{2+\dots\frac{p-3}{2}} \left(\frac{p-1}{2}\right)! \mod p.$$

Dans le cas où $p \equiv 1 \mod 8$, le nombre $\frac{(p-1)(p-3)}{8}$ est pair. On a donc

$$b \equiv (-1)^{\frac{(p-1)(p-3)}{8}-1}[\left(\frac{p-1}{2}\right)!]^{-1} \equiv \left(\frac{p-1}{2}\right)! \mod p,$$

Cette contradiction avec la définition de b conclut que $p \equiv 5 \mod 8$.

2.4 Théorie de l'ordre

2.4.1 Construction, divisibilité, périodicité

Exercice 2.67. Soit $n \geqslant 1$ un entier impair. Montrer que $n \mid 2^{n!} - 1$.

Solution 2.67. Comme n est impair, il est premier avec 2. 2 admet donc un ordre ω modulo n. D'après le théorème d'Euler, $\omega \leqslant \varphi(n) \leqslant n$. En particulier, ω divise $n!$, si bien que $2^{n!} \equiv 1 \mod n$, comme voulu.

Exercice 2.68. (Albanie TST 2011) Montrer que les facteurs premiers du nombre $11\ldots1$ (avec 2011 chiffres 1) sont tous de la forme $4022k + 1$.

Solution 2.68. Le nombre considéré s'écrit aussi $10^0 + 10^1 + \ldots + 10^{2010} = \dfrac{10^{2011} - 1}{9}$. Soit p un diviseur premier de ce nombre. Notons que p est différent de 3, car le nombre de départ n'est pas divisible par 3 (la somme de ses chiffres n'est pas divisible par 3). Ainsi, p divise $10^{2011} - 1$.

Notons ω l'ordre de 10 modulo p. D'après la congruence, $\omega \mid 2011$. Comme 2011 est premier, on déduit que $\boxed{\omega = 2011}$. D'après le petit théorème de Fermat, $2011 = \omega \mid p-1$. Comme en plus p est impair, $2 \mid p-1$. Ainsi, $4022 = 2 \cdot 2011 \mid p - 1$, ce qui correspond à la condition recherchée.

Exercice 2.69. Soit $n \geqslant 1$ un entier naturel et p un diviseur de $2^{2^n} + 1$. Montrer que $p \equiv 1 \mod 2^{n+1}$.

Solution 2.69. Il suffit de montrer le résultat pour les diviseurs premiers de $2^{2^n} + 1$. On fixe désormais p un tel diviseur premier. p est manifestement impair, de sorte qu'on peut noter ω l'ordre de 2 modulo p. On a alors

$$p \mid 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1.$$

Ainsi, $2^{2^{n+1}} \equiv 1 \mod p$, donc $\omega \mid 2^{n+1}$. ω est donc une puissance de 2, notée 2^a avec $a \leqslant n+1$. Si $a \leqslant n$, on a $2^a \mid 2^n$, de sorte que

$$p \mid 2^{2^a} - 1 \mid 2^{2^n} - 1,$$

de sorte que p divise $2^{2^n} + 1 - (2^{2^n} - 1) = 2$, ce qui vient contredire l'hypothèse que p est impair. On déduit que $a = n+1$ et $\omega = 2^{n+1}$. On combine avec la divisibilité $\omega \mid p-1$ pour déduire que $2^{n+1} \mid p - 1$, comme voulu.

Exercice 2.70. Soient a et b deux éléments inversibles modulo n. On suppose que $\omega_n(a)$ et $\omega_n(b)$ sont premiers entre eux. Montrer que $\omega_n(ab) = \omega_n(a)\omega_n(b)$.

Solution 2.70. Commençons par montrer que $\omega_n(ab) \mid \omega_n(a)\omega_n(b)$. On

$$(ab)^{\omega_n(a)\omega_n(b)} \equiv (a^{\omega_n(a)})^{\omega_n(b)} (b^{\omega_n(b)})^{\omega_n(a)} = 1 \cdot 1 = 1 \mod n,$$

donc, l'ordre de ab divise $\omega_n(a)\omega_n(b)$, ce qui est bien $\boxed{\omega_n(ab) \mid \omega_n(a)\omega_n(b)}$.

On montre la divisibilité réciproque. On a

$$1 = (ab)^{\omega_n(ab)\omega_n(b)} = a^{\omega_n(ab)\omega_n(b)} b^{\omega_n(ab)\omega_n(b)} \equiv a^{\omega_n(ab)\omega_n(b)} \cdot 1 \mod n.$$

On déduit que $a^{\omega_n(ab)\omega_n(b)} \equiv 1 \mod n$, et par propriété de l'ordre, $\omega_n(a) \mid \omega_n(ab)\omega_n(b)$. Comme $\omega_n(a)$ est premier avec $\omega_n(b)$, d'après le lemme de Gauss, on déduit que $\boxed{\omega_n(a) \mid \omega_n(ab)}$. On a la divisibilité similaire pour $\omega_n(b)$, en puisque $\omega_n(a)$ et $\omega_n(b)$ sont premiers entre eux, on déduit que $\boxed{\omega_n(a)\omega_n(b) \mid \omega_n(ab)}$.

La combinaison de ces deux divisibilités conclut.

Exercice 2.71. Soient p et q des nombres premiers distincts et $a \in \mathbb{N}$ tel que $a \equiv 1 \mod (p-1)(q-1)$. Montrer que pour tout $n \in \mathbb{N}$, $n^a \equiv n \mod pq$.

Solution 2.71. Il suffit de montrer que $p \mid n^a - n$ et $q \mid n^a - n$. On se concentre sur la preuve de $p \mid n^a - n$. Si $p \mid n$, alors on a bien le résultat (notons que a est non nul car congru à 1 modulo $(p-1)(q-1)$). Sinon, n est premier avec p et admet un ordre ω modulo n. On a alors

$$\omega \mid p-1 \mid (p-1)(q-1) \mid a-1,$$

de sorte que $n^{a-1} \equiv 1 \mod p$, ce qui implique bien sûr que $n^a \equiv n \mod p$. Il en est de même pour q, ce qui permet de conclure.

Exercice 2.72. Soit $m, n \geqslant 2$ des entiers tels que $\mathrm{PGCD}(m,n) = \mathrm{PGCD}(m, n-1) = 1$. On définit la suite $(n_k)_{k\in\mathbb{N}}$ par $n_0 = m$ et $n_{k+1} = n \cdot n_k + 1$ pour $k \in \mathbb{N}$. Montrer que les entiers $n_1, \ldots, n_{m-1}$ ne peuvent pas tous être des nombres premiers.

Solution 2.72. Tout d'abord, la suite (n_k) est une suite arithmético-géométrique. On peut donc établir une formule close pour son terme général, à savoir $n_k = n^k m + \frac{n^{k+1}-1}{n-1}$, que l'on peut aussi obtenir par récurrence à partir du calcul des premiers termes. De cette expression on déduit en particulier que $n_k > m$ pour tout $k > 0$. On va désormais montrer que l'un des nombres $n_1, \ldots, n_{m-1}$ est divisible par m, ce qui fera de ce nombre un nombre composé.

En passant modulo m, on déduit $n_k \equiv \frac{n^{k+1}-1}{n-1} \mod m$ par récurrence, où l'on a utilisé que $n-1$ est inversible modulo m car $n-1$ est premier avec m.
Soit ω l'ordre de n mod m (celui-ci existe car m et n premiers entre eux). On a $\omega \leqslant \varphi(m) \leqslant m-1$ d'après le théorème d'Euler. On déduit que $m \mid n^\omega - 1$, ce qui implique que m divise $n_{\omega-1} - 1$ comme voulu. Ainsi, les n_k ne sont pas tous premiers.

Exercice 2.73. (Nordic MO 2025) Soit p un nombre premier. On suppose que $2^{2p} \equiv 1 \mod 2p+1$. Montrer que $2p+1$ est un nombre premier.

Solution 2.73. Soit q un diviseur premier de $2p+1$. Notons que q est impair. La congruence de l'énoncé donne $q \mid 2p+1 \mid 2^{2p} - 1$, soit $4^p \equiv 1 \mod q$. Notons ω l'ordre de 4 modulo q. ω est donc un diviseur de p et comme p est premier, $\omega \in \{1, p\}$.

- Si $\omega = p$, d'après le petit théorème de Fermat, on a donc $p = \omega \mid q-1$ donc $q = kp+1$ pour un certain k. Comme $q > 1$ et $q \leqslant 2p+1$, on a $q = p+1$ ou $q = 2p+1$. Or $\mathrm{PGCD}(p+1, 2p+1) = \mathrm{PGCD}(p+1, p) = 1$, donc $p+1$ ne divise pas $2p+1$. On déduit que $q = 2p+1$, ce qui implique que $2p+1$ est premier.
- Si $\omega = 1$, alors $4^1 \equiv 1 \mod q$, soit $q \mid 3$ et $q = 3$. Comme ce résultat est à nouveua vria pour tout autre éventuel diviseur premier de $2p+1$, on déduit que le seul diviseur premier de $2p+1$ est 3 et donc que $2p+1$ est une puissance de 3. Notons k l'entier tel que $\boxed{2p+1 = 3^k}$. Notons qu'alors p doit être différent de 3. En revenant à l'énoncé, on a donc $3^k \mid 4^p - 1$. Or, modulo 3, on a

  $$4^{p-1} + 4^{p-2} + \ldots + 1 \equiv p \neq 0 \mod 3,$$

  donc $v_3(4^p - 1) = v_3(4-1) + v_3(4^{p-1} + 4^{p-2} + \ldots + 1) = v_3(3) = 1$, donc $\boxed{k = 1}$. Mais alors $2p+1 = 3$ et $p = 1$, ce qui est absurde et conclut ce cas.

Remarque : le dernier cas utilise en substance le lemme LTE.

Exercice 2.74. (BMO SL 2016 N1) Déterminer tous les entiers $n \geqslant 1$ tels que $1^{\varphi(n)} + 2^{\varphi(n)} + \ldots + n^{\varphi(n)}$ est premier avec n.

Solution 2.74. **Réponse :** Il s'agit des entiers n n'admettant pas de facteur carré.

Soit p un diviseur premier de n. On écrit $n = p^\alpha k$ avec k premier avec p. On a alors $\varphi(n) = \varphi(p^\alpha)\varphi(k) = (p-1)p^{\alpha-1}\varphi(k)$. On déduit que $p-1 \mid \varphi(n)$, et d'après le petit théorème de Fermat,

$$1^{\varphi(n)} + 2^{\varphi(n)} + \ldots + n^{\varphi(n)} = \sum_{p \nmid n} m^{(p-1)p^{\alpha-1}\varphi(k)} + \sum_{p \mid m} m^{\varphi(n)} \equiv \sum_{p \nmid n} 1 = n - \frac{n}{p} \equiv -\frac{n}{p} \mod p.$$

On déduit que n est premier avec la somme de l'énoncé si et seulement si, pour tout diviseur premier p de n, le nombre $\dfrac{n}{p}$ n'est pas divisible par p, c'est-à-dire si et seulement si $p^2 \nmid n$, ce qui est la condition voulue.

Exercice 2.75. (Pologne MO 2016 Round final) Soient k et n des entiers positifs impairs différents de 1. On suppose qu'il existe un entier $a \geqslant 1$ tel que $k \mid 2^a + 1$ et $n \mid 2^a - 1$. Montrer qu'il n'existe pas d'entier b tel que $k \mid 2^b - 1$ et $n \mid 2^b + 1$.

Solution 2.75. Supposons au contraire qu'il existe un entier b vérifiant l'énoncé.

Notons ω_k l'ordre de 2 modulo k et ω_n l'ordre de 2 modulo n. D'après l'hypothèse de l'énoncé, $k \mid 2^a+1 \mid 2^{2a}-1$, donc $\omega_k \mid 2a$ mais ω_k ne divise pas a car $2^a \equiv -1 \neq 1 \mod k$ (car k est impair différent de 1). On déduit que ω_k divise $2a$ mais ne divise pas a, donc $v_2(\omega_k) = v_2(2a) = v_2(a) + 1$. D'autre part, $2^b \equiv 1 \mod k$ donc $\omega_k \mid b$ et $v_2(\omega_k) \leqslant v_2(b)$. En combinant, on déduit que $v_2(a) + 1 \leqslant v_2(b)$, soit $\boxed{v_2(a) < v_2(b)}$.

En effectuant un raisonnement similaire sur ω_n, on trouve $v_2(b) + 1 \leqslant v_2(\omega_n) \leqslant v_2(a)$, soit $v_2(b) < v_2(a)$. On a donc une contradiction avec l'inégalité précédente, ce qui conclut.

Exercice 2.76. Trouver tous les couples (p, q) de nombres premiers tels que $pq \mid 2^p + 2^q$.

Solution 2.76. **Réponse :** Les seuls couples sont $(2, 2), (2, 3)$ et $(3, 2)$.

Il faut commencer par traiter les cas de bord. Si $p = 2$, alors la divisibilité devient $q \mid 2^2 + 2^q$, or d'après le petit théorème de Fermat, $2^2 + 2^q \equiv 2 + 2^2 = 6$, donc $q = 2$ ou $q = 3$. Réciproquement, on a bien $2\cdot \mid 2^2 + 2^2$ et $2 \cdot 3 \mid 2^2 + 2^3$, donc $\boxed{(2, 3), (2, 2) \text{ et } (3, 2)}$ sont bien solutions.

On suppose désormais que p et q sont impairs. D'après le petit théorème de Fermat,

$$0 \equiv 2^p + 2^q \equiv 2 + 2^q = 2(1 + 2^{q-1}) \mod p.$$

On déduit que $2^{q-1} \equiv -1 \mod p$ puis que $2^{2(q-1)} \equiv 1 \mod p$. Soit ω l'ordre de 2 modulo p. D'après la congruence précédente, $\omega \mid 2(q - 1)$. en revanche, ω ne divise pas $q - 1$ car $2^{q-1} \equiv -1 \neq 1 \mod p$. Comme $\omega \mid 2(q - 1)$ mais pas $q - 1$, on déduit que $v_2(\omega) = v_2(2(q - 1)) = v_2(q - 1) + 1$. D'autre part, d'après le petit théorème de Fermat, $\omega \mid p - 1$, donc $v_2(\omega) \leqslant v_2(p - 1)$.

On conclut que $\boxed{v_2(q - 1) + 1 \leqslant v_2(p - 1)}$, ou encore que $v_2(q-1) < v_2(p-1)$. Un raisonnement complètement symétrique conduit à l'inégalité inverse, ce qui est absurde. On n'a donc pas de solution dans ce cas là.

Exercice 2.77. (JBMO SL 2024 N2) Déterminer tous les couples (p, q) de nombres premiers tels que $p \neq q$ et q^p est un diviseur de $p + p^q + p^{(q^p)}$.

Solution 2.77. Soit (p, q) un couple solution. On calcule chaque terme de $p + p^q + p^{q^p} \mod q$. Pour cela, le petit théorème de Fermat indique que $p^q \equiv p \mod q$. Ainsi,

$$p^{q^p} = (p^q)^{q^{p-1}} \equiv p^{q^{p-1}} = (p^q)^{q^{p-2}} \equiv p^{q^{p-2}} \equiv \ldots \equiv p^q \equiv p \mod q.$$

La relation de divisibilité implique en particulier que $q \mid p + p^q + p^{q^p}$. On déduit que

$$0 \equiv p + p^q + p^{q^p} \equiv p + p + p = 3p \mod q.$$

On déduit que $q \mid 3p$ et donc que $q \mid 3$ ou que $q \mid p$. Mais si $q \mid p$, comme p et q sont premiers, on trouve que $q = p$, ce qui est exclu par l'énoncé. On a donc $q \mid 3$ et $q = 3$. La relation de divisibilité devient

$$3^p \mid p + p^3 + p^{3^p}.$$

Jusqu'ici, on a seulement utilisé que $q \mid p+p^q+p^{q^p}$, mais pas qu'une plus grande puissance de q divise $p+p^q+p^{q^p}$. C'est ce que l'on va faire ici. On va calculer le terme $p^{3^p} \mod 3^p$. Puisque p est premier et distinct de 3, il est premier avec 3. On peut donc appliquer le théorème d'Euler, qui indique que

$$1 \equiv p^{\varphi(3^p)} = p^{3^p - 3^{p-1}} \mod 3^p$$

On déduit que $p^{3^p} \equiv p^{3^{p-1}} \mod 3^p$. Le théorème d'Euler s'écrit également $p^{2\cdot 3^{p-1}} \equiv 1 \mod 3^p$. Cela implique que

$$3^p \mid \left(p^{3^{p-1}}\right)^2 - 1 = \left(p^{3^{p-1}} - 1\right)\left(p^{3^{p-1}} + 1\right).$$

Or, ces deux facteurs ont une différence de 2, donc ils ne peuvent pas être tous les deux divisibles par 3. On a donc $3^p \mid p^{3^{p-1}} - 1$ ou $3^p \mid p^{3^{p-1}} + 1$, ce qui implique que $p^{3^p} \equiv a \mod 3^p$, avec $a = -1$ ou $a = 1$. Finalement, on trouve que

$$0 = p + p^3 + p^{3^p} \equiv p + p^3 + a \mod 3^p.$$

Or, on a pour tout $p \geqslant 5$,

$$0 < p^3 + p - 1 < p^3 + p + 1 < 3^p.$$

La preuve de la dernière inégalité se trouve en annexe. Cet encadrement contredit que 3^p est un diviseur de $p^3 + p + a$. On déduit que $p = 2$. Réciproquement, si $p = 2$ et $q = 3$, on a bien

$$3^2 = 9 \mid 522 = 2 + 2^3 + 2^{3^2}.$$

Le seul couple solution est donc $(2, 3)$.

Annexe : Preuve de l'inégalité $p^3 + p + 1 < 3^p$.

Nous allons montrer par récurrence sur n que $n^3 + n + 1 < 3^n$ pour tout entier $n \geqslant 5$.

Initialisation : Si $n = 5$, on a bien $5^3 + 5 + 1 = 131 < 243 = 3^5$.

Hérédité : On suppose l'inégalité vraie pour un $n \geqslant 5$ fixé et on montre que l'inégalité est vraie pour $n + 1$. L'hypothèse de récurrence donne en effet

$$3^{n+1} = 3 \cdot 3^n > 3(n^3 + n + 1).$$

Pour montrer que $3(n^3 + n + 1) > (n + 1)^3 + (n + 1) + 1$, il suffit, après développement et simplification, de montrer que $2n^3 > 3n^2 + n$. Or on a, puisque $n \geqslant 5$,

$$2n^3 \geqslant 2 \cdot 5n^2 = 3n^2 + 7n^2 > 3n^2 + 4n^2 \geqslant 3n^2 + n.$$

On a donc bien l'inégalité pour $n + 1$, ce qui achève la récurrence et conclut l'exercice.

Remarque : Pour montrer que $p^{3^p} = \pm 1 \mod 3^p$, on peut également avoir recours au lemme "Lifting The Exponent" de la façon suivante. Comme $p \neq 3$, $p = \pm 1 \mod 3$. Supposons par exemple que $p = 1 \mod 3$. D'après le lemme LTE, on a

$$v_3(p^{3^p} - 1) = v_3(p) + v_3(3^p) = p + 1,$$

si bien que $3^p \mid p^{3^p} - 1$. On montre de même que $3^p \mid p^{3^p} + 1$ lorsque $p = -1 \mod 3$.

Exercice 2.78. (IMO SL 2006 N2) Soit x un rationnel de $]0, 1[$. On note y le nombre de $]0, 1[$ dont le n-ème chiffre après la virgule est le 2^n-ème chiffre après la virgule de x. Montrer que y est rationnel.

Solution 2.78. Notons $x = 0, x_1 \dots x_n ldots$ le développement décimal de x, où x_n est le $n-$ème chiffre de x après la virgule. Puisque x est rationnel, son développement décimal est périodique à partir d'un certain rang, et on note p la période et N le rang à partir duquel cette suite est périodique. L'objectif est de montrer que la suite (x_{2^n}) est également périodique à partir d'un certain rang.

Décomposons la période p sous la forme $p = 2^\alpha \beta$ avec β impair. Soit ω l'ordre de 2 modulo β. Alors pour $n \geqslant \alpha$, on vérifie les deux congruences

$$2^{n+\omega} \equiv 2^n \mod \beta, \quad 2^{n+\omega} \equiv 0 \equiv 2^n \mod 2^\alpha.$$

On déduit que $2^{n+\omega} - 2^n$ est un multiple de p, de sorte que $x_{2^{n+\omega}} = x_{2^n}$. La suite (x_{2^n}) est donc périodique à partir du rang $\max(2^\alpha, N)$, ce qui conclut.

Exercice 2.79. Soient $a \geqslant 2$ et n deux entiers strictement positif. On note $a^{\uparrow k} = a^{(a^{\cdot^a})}$, où il y a $k - 1$ termes dans l'exposant. Cette suite est également définie par $a_0 = 1$ et $a_{m+1} = a^{a_m}$ pour tout $m \geqslant 0$. Montrer que la suite $(a^{\uparrow k})_{k \in \mathbb{N}}$ est constante à partir d'un certain rang modulo n.

Solution 2.79. On prouve le résultat par récurrence forte sur n.

Initialisation : Si $n = 1$, la suite est constante égale à 0 modulo 1.

Hérédité : On suppose que l'énoncé est vrai pour tout entier $m < n$ et on entreprend de le démontrer pour n. Supposons d'abord que $\mathrm{PGCD}(a, n) = 1$. Comme $\varphi(n) < n$, on peut appliquer l'hypothèse de récurrence à $\varphi(n)$: il existe un rang k tel que (a_m) soit constante à partir du rang k modulo $\varphi(n)$. Mais alors, pour tout $\ell \geqslant k+1$, on a $a_\ell \equiv a_{\ell-1} \mod \varphi(n)$, donc

$$a_{\ell+1} = a^{a_\ell} \equiv a^{a_{\ell-1}} = a_\ell \mod n,$$

ce qui conclut que la suite est stationnaire/constante à partir du rang $k+1$.

Revenons au cas général. Soit y le plus grand diviseur de n tel que $\mathrm{PGCD}(a, y) = 1$ et posons $n = dy$: y est le produit des facteurs premiers de n ne divisant pas a (avec multiplicité. On pose également $n = dy$. Comme $a \geqslant 2$, la suite $v_p(a_m)$ est strictement croissante pour tout diviseur premier p de a, il existe donc un rang k tel que $d \mid a^{a^{\uparrow k}}$. D'autre part, d'après le raisonnement précédent appliqué à a et y qui sont premiers entre eux, on dispose d'un rang ℓ tel que (a_m) est constante modulo y à partir du rang ℓ.

En posant $N = \max(k, \ell)$, on trouve que la suite $(a_m)_{m \geqslant N}$ est constante modulo d et y, et comme d et y sont premiers entre eux, la suite est également stationnaire modulo $dy = n$, ce qui achève l'hérédité.

2.4.2 L'astuce du plus petit facteur premier

Exercice 2.80. Déterminer tous les entiers n impairs tels que $n \mid 3^n + 1$.

Solution 2.80. Soit p le plus petit diviseur premier de n. p est manifestement premier avec 3, donc on peut considérer ω l'ordre de 3 modulo p. Comme $3^n \equiv -1 \mod p$, on trouve $3^{2n} \equiv 1 \mod p$. Ainsi, $\omega \mid 2n$ et $\omega \mid p-1$. Comme p est le plus petit diviseur de n, $p-1$ est premier avec n, donc ω aussi. Ainsi, ω divise 2 donc $\omega = 1$ ou $\omega = 2$.

- ➢ Si $\omega = 2$: alors $p \mid 3^\omega - 1 = 3^2 - 1 = 8$ et donc $p = 2$, ce qui contredit le fait que n est impair.
- ➢ Si $\omega = 1$: alors $p \mid 3^\omega - 1 = 3^1 - 1 = 2$, ce qui implique à nouveau que $p = 2$ et donne à nouveau une contradiction.

Il n'y a donc pas de solutions.

Exercice 2.81. Déterminer tous les couples d'entiers (n, a) avec $n \geqslant 1$ tels que n divise $(a+1)^n - a^n$.

Solution 2.81. **Réponse :** Les seuls couples solutions sont $(1, a)$ pour tout entier a.

Si $n = 1$, tout entier a convient. On suppose dans la suite que $n \geqslant 2$.

On note p son plus petit facteur premier. On a donc $p \mid (a+1)^n - a^n$. Notons que p ne divise pas a, sinon p diviserait $(a+1)^n$ et donc $a+1$, donc p diviserait $(a+1) - a = 1$, ce qui est absurde. Ainsi, a est inversible modulo p et on a

$$(a+1)^n \equiv a^n \mod p \iff \left(1 + \frac{1}{a}\right)^n \equiv 1 \mod p.$$

Notons ω l'ordre de $1 + a^{-1}$ modulo p. D'après la congruence précédente, $\omega \mid n$. D'après le petit théorème de Fermat, $\omega \mid p-1$. Il vient que $\omega \leqslant p-1$. Par minimalité de p, on déduit que $\omega = 1$ et donc que $1 + a^{-1} \equiv 1 \mod p$, soit $p \mid a^{-1}$, ce qui est absurde car a^{-1} est inversible modulo p. Il n'y a donc pas de solution dans ce cas.

Exercice 2.82. Soient $a_1, \ldots, a_n$ des entiers naturels non nuls tels que $a_1 \ldots a_n$ divise le produit

$$(2^{a_1} - 1) \ldots (2^{a_n} - 1).$$

Montrer que l'un des a_i vaut 1.

Solution 2.82. On suppose au contraire qu'aucun des a_i ne vaut 1. Cela veut dire que tous les termes $2^{a_i-1}+1$ sont impairs, et il en est donc de même des a_i.

Considérons l'entier a_j tel que $v_2(a_j-1)$ est minimal (on peut supposer, quitte à renuméroter les entiers, que $a_j = a_1$). Soit p un diviseur premier de a_1 et i un entier tel que $p \mid 2^{a_i-1}+1$. On a donc

$$2^{a_i-1} \equiv -1 \mod p \iff 2^{2(a_i-1)} \equiv 1 \mod p.$$

En notant ω l'ordre de 2 modulo p, on déduit que $\omega \mid 2(a_i-1)$ mais pas a_i-1. On a donc $v_2(\omega) = v_2(a_i-1)+1$. Mais d'après le petit théorème de Fermat, on a aussi $\omega \mid p-1$, d'où

$$v_2(p-1) \geqslant v_2(\omega) = v_2(a_i-1)+1 \geqslant v_2(a_1-1)+1.$$

Autrement dit, en notant $\alpha = v_2(a_1-1)$, tout facteur premier p de a_1 vérifie $p \equiv 1 \mod 2^{\alpha+1}$. Par multiplication, on déduit que $a_1 \equiv 1 \mod 2^{\alpha+1}$, contredisant la définition de α. Cette contradiction implique l'énoncé.

Exercice 2.83. Déterminer toutes les suites (u_n) telles que, pour tout entier n, $u_n \mid 2^{u_{n+1}}-1$.

Solution 2.83. **Réponse :** Seule la suite constante égale à 1 vérifie l'énoncé.

Commençons par vérifier que s'il existe un indice n_0 (que l'on peut prendre minimal) tel que $u_{n_0} = 1$, alors, pour peu que $n_0 > 1$, on trouve $u_{n_0-1} \mid 2^{u_{n_0}}-1 = 1$, ce qui implique que $u_{n_0-1} = 1$, contredisant la minimalité de n_0. On déduit donc que si la suite (u_n) atteint la valeur 1, elle est en fait constante égale à 1.

On suppose désormais que $u_k > 1$ pour tout indice k, et on note p_k le plus petit facteur premier de u_k.

Fixons désormais un indice n. p_n est manifestement premier avec 2, donc on peut considérer ω l'ordre de 2 modulo p_n. La relation de l'énoncé implique que $\omega \mid u_{n+1}$ et on a toujours $\omega \mid p_n - 1$. Comme $u_n > 1$, $\omega \neq 1$. On déduit que $p_{n+1} \leqslant \omega \leqslant p_n - 1$.

La suite (p_k) est donc une suite strictement décroissante de nombres premiers, ce qui est absurde.

2.4.3 Application à la construction d'entiers

Exercice 2.84. Montrer que, pour toute paire d'entiers strictement positifs (a,b) premiers entre eux, il existe deux entiers $m, n \geqslant 1$ tels que

$$a^m + b^n \equiv 1 \mod ab$$

Solution 2.84. Soit m l'ordre de a modulo b et n l'ordre de b modulo a, les deux étant bien définis car a et b sont premiers entre eux. Quitte à remplacer m par $m+\varphi(b)$, on peut supposer que $m \geqslant 1$. De même on suppose que $n \geqslant 1$. On vérifie alors que

$$a^m + b^n \equiv b^n \equiv 1 \mod a, \qquad a^m + b^n \equiv a^m \equiv 1 \mod b,$$

si bien que a et b divisent tous les deux $a^m + b^n - 1$, donc leur produit aussi.

Exercice 2.85. Montrer qu'il existe un multiple de 2023 qui admet 2023 chiffres 1 dans son écriture décimale (et tous les autres chiffres sont des 0).

Solution 2.85. Puisque 10 est inversible modulo 2023, d'après le théorème d'Euler, il admet un ordre ω. Le nombre $1 + 10^\omega + 10^{2\omega} + \ldots + 10^{2022\omega}$ a donc 2023 chiffres 1 et vérifie

$$1 + 10^\omega + 10^{2\omega} + \ldots + 10^{2022\omega} \equiv 1+1+1+\ldots+1 = 2023 \equiv 0 \mod 2023$$

donc il est bien divisible par 2023.

Exercice 2.86. *(Arabie saoudite 2024)* Montrer qu'il existe une infinité de nombres premiers divisant un terme de la forme $3^{3^n-1}+2$.

Solution 2.86.

➢ **Commentaire :**

> On reprend la preuve classique de l'existence d'une infinité de nombres premiers : on suppose qu'on a trouvé $p_1, \dots, p_r$ des nombres premiers divisant au moins un terme de la suite et on cherche à en construire un autre, en cherchant n tel que $3^{3^n-1}+2$ n'est pas divisible par les p_i (et admet donc un nouveau diviseur premier).
>
> On peut par exemple chercher à ce que $3^{3^n-1} \equiv 1 \mod p_i$, afin que $3^{3^n-1}+2 \equiv 3 \neq 0 \mod p_i$ (on peut supposer que les p_i sont distincts de 3, puisque de toute façon il s'agit d'en construire une infinité). On peut donc chercher un entier n vérifiant $3^n - 1 \equiv 0 \mod p_i - 1$ pour tout i. Cet entier n existe seulement si 3 est premier avec $p_i - 1$, autrement dit seulement si $p_i \equiv 2 \mod 3$.
>
> C'est cette démarche qui guide la solution.

On montre mieux : on montre qu'il existe une infinité de nombres premiers congrus à 2 modulo 3 et divisant un terme de la forme donnée.

On reprend la preuve classique de l'infinité de nombres premiers : on suppose avoir construit $p_1, \dots, p_r$ des nombres premiers congrus à 2 modulo 3 et divisant un terme de la suite. On pose $N = (p_1 - 1)\dots(p_r - 1)$. Comme N est premier avec 3, le nombre 3 admet un ordre n modulo N. En particulier, on a $3^n \equiv 1 \mod N$. D'après le petit théorème de Fermat, et puisque $p_i - 1 \mid 3^n - 1$, on a

$$3^{3^n-1} \equiv 1 \mod p_i \qquad \text{pour tout indice } i.$$

En particulier, $3^{3^n-1}+2 \equiv 1+2 = 3 \mod p_i$, donc les p_i ne divisent pas $3^{3^n-1}+2$. Ce nombre étant congru à 2 modulo 3 (car $n > 0$), il admet pourtant un diviseur premier p congru à 2 modulo 3. On a construit un nouveau diviseur premier, ce qui achève la preuve de l'infinité.

***Exercice 2.87.** (Pologne 2025 round 2)* Déterminer tous les entiers $n \geqslant 2$ vérifiant la propriété suivante : les nombres $2^k \cdot n - 1$ pour $k = 2, 3, \dots, n$ sont des nombres premiers.

Solution 2.87. **Réponse :** les seuls entiers sont $n = 2$ et $n = 3$.

➢ **Commentaire :**

> L'ambition est de trouver, parmi les nombres étudiés, un nombre divisible par un petit nombre connu. Le plus simple est d'étudier les nombres $2^k - 1$, et donc de travailler avec un diviseur d de $n - 1$ pour que $2^k n - 1 \equiv 2^k - 1 \mod d$. Il faut alors que d soit impair pour que 2 ait un ordre (petit).

Posons $n - 1 = 2^\alpha \beta$ avec β impair. Comme $\beta \mid n - 1$, on a $n \equiv 1 \mod \beta$ et donc, pour tout entier k,

$$2^k n - 1 \equiv 2^k - 1 \mod \beta.$$

Si $\beta \geqslant 3$, comme β est impair, 2 est premier avec β et admet donc un ordre ω modulo β. Comme $2 \leqslant \omega \leqslant \beta \leqslant n - 1$, en prenant $k = \omega$, on a bien $d \mid 2^\omega - 1 \mid 2^\omega n - 1$, avec $2^\omega n - 1 > 2^\omega - 1 \geqslant d$ car $n \geqslant 2$. Donc $2^\omega n - 1$ est composé.

Si $\beta = 1$, alors $n - 1 = 2^\alpha$. Si $\alpha \geqslant 2$, le nombre $n - 2$ admet un facteur premier $q \geqslant 3$, qui divise donc $n - 2$, et pour tout k,

$$2^k n - 1 \equiv 2^k \cdot 2 - 1 \equiv 2^{k+1} - 1 \mod q.$$

En prenant $k = q - 2$, la congruence ci-dessus est nulle, donc $q \mid 2^k n - 1$ et $2^k n - 1 > 2^{k+1} - 1 \geqslant q$. Le nombre $2^{q-2} n - 1$ est donc composé.

Il reste donc à vérifier le cas où $\alpha = 0, 1$, soit $n = 2, 3$. Ces deux nombres sont effectivement des solutions, puisque $7, 11$ et 23 sont premiers.

***Exercice 2.88.** (ELMO 2015 P4)* Soit $a \geqslant 2$ un entier. Montrer qu'il existe un entier $n \geqslant 0$ tel que $2^{2^n} + a$ n'est pas un nombre premier.

Solution 2.88.

➢ **Commentaire :**

> L'idée est de montrer qu'il existe k et n tels que $2^{2^k} + a \mid 2^{2^n} + a$, ce qui donne le résultat. Or pour tous k et n on a

$$2^{2^k}+a \mid 2^{2^n}+a \iff 2^{2^k}+a \mid 2^{2^n}+a-(2^{2^k}+a)=2^{2^n}-2^{2^k}.$$

On se ramène à l'étude de la suite (2^n) modulo $\varphi(2^{2^k}+a)$. Il suffit de bien calibrer k et n.

Si a est pair, alors le nombre $2^{2^0}+a$ est pair et supérieur à 4 donc composé. On suppose dans la suite que a est impair.

Posons $a=2^\alpha\beta+1$, où β est impair. Prenons k tel que $2^k>2^\alpha$. Supposons par l'absurde que tous les nombres de la forme $2^{2^n}+a$ sont premiers. On pose $p=2^{2^k}+a$. On a donc $\varphi(p)=2^\alpha(2^{2^k-\alpha}+\beta)$.

Prenons $n=k+\varphi(2^{2^k-\alpha}+\beta)$. Cet entier vérifie les deux congruences

$$2^n\equiv 0\equiv 2^k \mod 2^\alpha,$$

$$2^n=2^k\cdot 2^{\varphi(2^{2^k-\alpha}+\beta)}\equiv 2^k \mod 2^{2^k-\alpha}+\beta.$$

On déduit que $\varphi(p)=2^\alpha(2^{2^k-\alpha}+\beta)\mid 2^n-2^k$. On déduit avec le théorème d'Euler que $p\mid 2^{2^n}-2^{2^k}$. Il vient que

$$p\mid 2^{2^k}+a+2^{2^n}-2^{2^k}=2^{2^n}+a,$$

donc $2^{2^n}+a$ est composé.

Exercice 2.89. *(Canada MO 2018 P5)* Soit $k\geqslant 2$ un entier pair. Sarah choisit un entier $N\geqslant 2$ qu'elle écrit au tableau et le modifie de la façon suivante : à chaque minute, elle choisit un diviseur premier p du nombre n écrit au tableau et remplace l'entier n par $n(p^k-p^{-1})$.

Montrer qu'il existe une infinité d'entiers k pairs pour lesquels, quels que soient les choix de Sarah, au bout d'un certain temps, elle écrira au tableau un nombre divisible par 2018.

Solution 2.89.

➢ Commentaire :

Examinons l'effet d'une action sur $n=pm$, et notamment quels diviseurs premiers sont ajoutés et lesquels sont enlevés. Si $n=pm$ et que Sarah choisit p pour son opération, alors le nouvel entier écrit au tableau est $(p^{k+1}-1)m$. La valuation $p-$adique de l'entier au tableau a diminué, et les diviseurs premiers r de $p^{k+1}-1$ sont des diviseurs du nouvel entier inscrit. Si on choisit $k+1$ premier, la théorie de l'ordre indique que $r\equiv 1 \mod k+1$ pour tout r divisant $p^{k+1}-1$.

Si un tel nombre r est choisit pour l'opération suivante, alors $k+1$ sera un diviseur du nouveau nombre écrit au tableau :

$$pm \longrightarrow \underbrace{(p^{k+1}-1)}_{r\mid} m \longrightarrow \underbrace{(r^{k+1}-1)}_{k+1\mid} m'.$$

Ainsi, en prenant $k+1=1009$, après une telle opération (dont il faut montrer qu'elle arrivera), le nombre inscrit est divisible par 1009.

Posons $k=1008$. On appelle les nombres premiers p tels que $p\equiv 1 \mod 1009$ *bons* et les autres nombres premiers *mauvais*.

Si Sarah choisit un nombre premier p bon pour son opération, et que le nombre écrit au tableau avant l'opération est pm, alors le nouveau nombre écrit est $(p^{k+1}-1)m$, et on a $2\mid p^{k+1}-1$ et $1009\mid p-1\mid p^{k+1}-1$, donc 2018 divise le nouveau nombre écrit au tableau.

On suppose que Sarah n'écrit jamais un nombre divisible par 2018. D'après le paragraphe précédent, cela signifie que Sarah ne choisit jamais un nombre premier bon pour faire son opération. Notons $P(n)$ le produit des diviseurs premiers mauvais de l'entier n (pris avec multiplicité). On montre que la quantité $P(n)$ décroît strictement à chaque opération, si bien qu'au bout d'un certain nombre d'étape, l'entier écrit au tableau n'a que des diviseurs premiers bons.

Soit p un diviseur premier mauvais de n choisit par Sarah et $n=pm$. Le nouveau nombre écrit au tableau est $(p^{k+1}-1)m$. Montrons que $P((p^{k+1}-1)m)\leqslant P(mp)\dfrac{p-1}{p}<P(mp)$, ce qui correspond à l'affirmation voulue.

Un diviseur premier q de $\dfrac{p^{k+1}-1}{p-1}$ vérifie que $p^{k+1} \equiv 1 \mod q$, donc l'ordre de p modulo q divise $k+1 = 1009$, donc cet ordre vaut soit 1 soit 1009. S'il vaut 1, c'est que $q \mid p-1$, mais $\dfrac{p^{k+1}-1}{p-1} \equiv k+1 = 1009 \neq 0 \mod q$ car p est mauvais. Donc cet ordre vaut 1009, et par le petit théorème de Fermat, $q \equiv 1 \mod 1009$. Ainsi, tous les diviseurs premiers mauvais sont des diviseurs de $(p-1)m$. On déduit que $P((p^{k+1}-1)m) = P((p-1)m) = P(p-1)P(m) \leqslant (p-1)P(m) = \dfrac{p-1}{p}P(mp)$. Ceci est la conclusion voulue.

Exercice 2.90. (BXMO 2023) Un entier n strictement positif est dit *amical* si la différence entre deux chiffres voisins de son écriture en base 10 est toujours égale à 1 ou -1. Par exemple, 6787 est amical mais 211 et 901 ne le sont pas.
Déterminer tous les entiers m tels qu'il existe un entier amical divisible par $64m$.

Solution 2.90. **Réponse :** Il s'agit des entiers m impairs et premiers avec 5.

Supposons que m est divisible par 5. Notons N un éventuel multiple amical divisible par $64m$. Alors N est un multiple de $2 \times 5 = 10$. Donc le dernier chiffre de N est 0. Comme N est amical, son chiffre des dizaines est 1. Mais alors $N \equiv 10 \mod 100$ ce qui implique que $N \equiv 2 \mod 4$, ce qui est absurde car N est divisible par $4m$ et donc par 4. Donc $\boxed{\mathrm{PGCD}(m,5) = 1}$.

Réciproquement, prenons un entier m impair vérifiant $\mathrm{PGCD}(m,5) = 1$ et trouvons un multiple amical de $64m$.

➢ **Commentaire :**

> On commence par le cas $m = 1$, où il s'agit d'un calcul à la main. Les deux derniers chiffres d'un multiple de 4 sont bien connus, et parmi eux, les nombres à deux chiffres amicaux sont 12, 32, 56 et 76. Donc un multiple amical de 4 est de la forme $a12$, $a32$, $a56$ ou $a76$.
>
> Parmi ces nombres, on regarde les multiples amicaux de 8 à trois chiffres. en regardant modulo 1000, on trouve qu'un multiple amical de 8 est de la forme $a232, a432, a456, a656$.
>
> Parmi ces nombres, on regarde les multiples amicaux de 16 à quatre chiffres. En regardant modulo 10^4, on trouve qu'un multiple amical de 16 est de la forme $a3232, a3456$.
>
> Parmi ces nombres, on regarde les multiples amicaux de 32 à cinq chiffres. En regardant modulo 10^5, on trouve qu'un multiple amical de 32 est de la forme $a23232, a43232, a23456, a43456$.
>
> Parmi ces nombres, on regarde les multiples amicaux de 64 à cinq chiffres. En regardant modulo 10^6, on trouve qu'un multiple amical de 64 est de la forme $343232, 543232, 123456, 323456$.
>
> Maintenant qu'on a un multiple N amical de 64, on créé le multiple de $64m$ en concaténant des blocs de N, par exemple, on cherche un nombre de la forme
>
> $$343232\,343232, \ldots 343232 = 343232 \cdot (10^{6k} + \ldots + 10^6 + 1) = 343232 \cdot \frac{10^{6(k+1)}-1}{10^6-1}.$$
>
> Il suffit que le deuxième facteur soit divisible par m.

Soit $k+1 = \varphi((10^6-1)m)$. Comme m est impair premier avec 5, d'après le théorème d'Euler, on a $10^{6(k+1)} \equiv 1 \mod m(10^6-1)$ et donc $m \mid \dfrac{10^{6(k+1)}-1}{10^6-1}$. Il vient que

$$64m \mid 343232 \cdot \frac{10^{6(k+1)}-1}{10^6-1} = 343232\,343232, \ldots 343232,$$

qui est bien amical comme voulu.

Exercice 2.91. (IMO SL 2019 N3) Un ensemble S est dit *enraciné* si, pour tout entier $n \geqslant 0$ et tout choix de $a_0, \ldots, a_n$ dans S, les racines entières du polynôme $a_0 + a_1X + \ldots + a_nX^n$ sont également dans S. Déterminer tous les ensembles S enracinés contenant tous les nombres de la forme $2^a - 2^b$ avec $a, b \in S$.

Solution 2.91. **Réponse :** Le seule ensemble solution est l'ensemble des entiers relatifs.

Quelques essais nous permettent de conjecturer que S contient tous les entiers relatifs, et nous allons montrer par récurrence sur N que N appartient à S pour tout N.

Initialisation : On constate que $2^a - 2^a \in S$ pour tout a, donc $0 \in S$. D'autre part, 1 est bien dans S en tant que racine de $(2^2 - 2^1)X - (2^2 - 2^1)$. On montre de même que $-1 \in S$.

Hérédité : On suppose que $0, 1, \ldots, N-1$ sont des éléments de S. On désire montrer que N est également un élément de S.

On cherche alors à travailler avec les polynômes à coefficients dans $\{0, \ldots, N-1\}$, qui sont bien des polynômes admissibles pour l'exercice par hypothèse de récurrence. Si l'on trouve un élément a de S tel que $-a = P(N)$ avec P de coefficient constant nul et dont les autres coefficients sont dans $\{0, \ldots, N-1\}$, alors N sera racine du polynôme $P + a$ qui est à coefficients dans S.

La preuve contient alors deux idées : la première, c'est de trouver un multiple de N qui est dans S. La deuxième, sublime, permet d'exprimer ce multiple comme $P(N)$.

En effet, si l'on écrit $N = 2^\alpha \beta$ avec β impair et si on note ω l'ordre de 2 modulo β, alors N divise $2^{\alpha+1+\omega} - 2^{\alpha+1}$ (qui est bien dans S car chacune des puissances est une puissance non nul de 2). Posons $a = 2^{\alpha+1} - 2^{\alpha+1+\omega}$. Considérons l'écriture de $-a$ en base N :

$$-a = a_d N^d + \ldots + a_1 N + a_0.$$

Notons que $a_0 = 0$ car N divise a, et que chaque terme a_i est dans $\{0, \ldots, N-1\}$. Ainsi, le polynôme $P(X) + a = \sum_{i=1}^{d} a_i X^i$ est à coefficients dans S et a N pour racine, de sorte que N appartient à S.

De même, on prouve que $-N$ est dans S, ce qui achève la récurrence.

Exercice 2.92. (IMO SL 2020 N4) Soit p un nombre premier impair. Pour tout entier n, on note $d_p(n)$ le reste de la division euclidienne de n par p. On appelle *p-suite* une suite $(a_0, a_1, \ldots)$ d'entiers vérifiant que a_0 est premier avec p et $a_{n+1} = a_n + d_p(a_n)$ pour tout indice $n \geqslant 0$.

1) Existe-t-il une infinité d'entiers p tels qu'il existe deux p-suites $(a_0, \ldots)$ et $(b_0, \ldots)$ vérifiant $a_n > b_n$ pour une infinité d'indices n et $a_n < b_n$ pour une infinité d'indices n ?

2) Existe-t-il une infinité d'entiers p tels qu'il existe deux p-suites $(a_0, \ldots)$ et $(b_0, \ldots)$ vérifiant $a_0 < b_0$ et $a_n > b_n$ pour tout $n \geqslant 1$?

Solution 2.92.

➢ **Commentaire :**

> On retire l'indice p de la fonction d dans nos notations.
>
> On constate que $a_{n+1} \equiv 2a_n \mod p$ donc $a_n \equiv 2^n a_0 \mod p$. La suite (a_n) est donc périodique modulo p, de période $\omega = \omega_p(2)$. On déduit notamment que $d(a_{n+\omega}) = d(a_n)$ pour tout entier n. On peut donc calculer la valeur exacte des termes de la suite (a_n) en fonction des ω premiers termes. En notant $S(a_0) = d(a_0) + d(a_1) + \ldots + d(a_{\omega-1})$, on a en effet pour tout r,
>
> $$a_{\omega+r} = a_r + \sum_{k=r+1}^{r+\omega} d(a_k) = a_r + S, \quad \Longrightarrow \quad a_{k\omega+r} = a_r + kS.$$
>
> Une fois qu'on a fait ça, on peut traiter les deux questions.
>
> Pour la question 1), il suffit de trouver un couple (a_0, b_0) tel que $a_0 > b_0$, $a_1 < b_1$ et $S(a_0) = S(b_0)$. Il suffit pour cela de choisir une orbite modulo p donnée par $\{x, \ldots, 2^{\omega-1}x\}$, de prendre un élément b_0 de cette orbite et de choisir $a_0 = x + p$. Il suffit de calibrer x et b_0 pour que $2x + p < b_0 + d(b_0)$.
>
> Pour la question 2), il suffit cette fois-ci au contraire de trouver (a_0, b_0) tel que $a_0 < b_0$ et $S(a_0) > S(b_0)$. En effet, les deux suites auront alors, d'après la forme trouvée ci-dessus, une croissance affine de coefficient directeur différent. Cela implique que, à partir d'un certain rang, $a_n > b_n$ pour tout n. Il reste alors à "tronquer" chaque suite pour les faire démarrer au dernier indice i tel que $a_i < b_i$.
>
> Dans chaque cas, il faut construire les orbites, ce qui revient plus ou moins à construire un nombre premier p admettant deux orbites de même somme pour la 1) et deux orbites différentes pour la 2). L'idée terminale est que l'on peut choisir la taille des orbites en choisissant à l'avance l'ordre de 2.

Étant donné notre nombre premier p de travail, on note ω l'ordre de 2 modulo p. Pour toute $p-$suite, on a $a_{n+1} \equiv 2a_n \equiv 2^{n+1}a_0 \mod p$. On déduit que la suite (a_n) est $\omega-$périodique modulo p, et pour tout entier r, on a

$$d(a_r) + d(a_{r+1}) + \ldots + d(a_{r+\omega-1}) = d(a_0) + \ldots + d(a_{\omega-1}).$$

Autrement dit, la somme de ω restes consécutifs est une constante, que l'on note $S(a_0)$.

1) Soit q un nombre premier impair et p un diviseur de $2^q + 1$ distinct de 3 et 5. Montrons que p vérifie la condition de l'énoncé.

On vérifie que $\omega = 2q$: on a en effet $2^q \equiv -1 \mod p$ donc $2^{2q} \equiv 1 \mod p$. Donc $\omega \mid 2q$ et $\omega \in \{1, 2, q, 2q\}$. Comme $p \neq 3$ et que $2^q \neq 1 \mod p$, on a bien $\omega = 2q$.

Prenons $a_0 = p+1$ et $b_0 = p-1$. On vérifie que $a_1 = p+2$ et $b_1 = 2p-2 > a_1$. Puisque $2^q \equiv -1 \mod p$, l'orbite de 1 est $\{1, 2, \ldots, 2^q, -1, -2, \ldots, 2^{2q}\}$. Ainsi, $d(b_0)$ est dans l'orbite de 1 et on déduit que $S(b_0) = S(1) = S(a_0)$. On a alors pour tout k,

$$a_{k\omega} = a_0 + kS(a_0) > b_0 + kS(a_0) = b_0 + kS(b_0) = b_{k\omega},$$

$$a_{k\omega+1} = a_1 + kS(a_0) < b_1 + kS(b_0) = b_{k\omega+1},$$

donc les suites (a_n) et (b_n) vérifient l'énoncé.

Pour vérifier qu'il existe une infinité de nombres premiers comme définis précédemment, on peut vérifier que $\mathrm{PGCD}(2^q + 1, 2^{q'} + 1) = 2^{\mathrm{PGCD}(q,q')} + 1 = 3$, de sorte que les nombres $\dfrac{2^q + 1}{3}$ sont deux à deux premiers entre eux et donc l'ensemble de leurs diviseurs premiers est infini.

2) Soit q un nombre premier et p un diviseur premier de $2^q - 1$. Cette fois-ci, ω divise q donc $\omega \in \{1, q\}$ et donc $\omega = q$. L'ensemble des résidus non nuls modulo p est partitionné en $(p-1)/q$ ensembles de la forme $O(x) = \{2^k x, 0 \leqslant k \leqslant q-1\}$. Si toutes les orbites avaient la même somme S, on aurait

$$\frac{p-1}{q} S = 1 + 2 + \ldots + (p-1) = \frac{p(p-1)}{2}.$$

En simplifiant, on trouverait $2S = pq$ ce qui est absurde car pq est impair. Donc il existe deux entiers a et b de $\{0, \ldots, p-1\}$ tels que $S(b) > S(a)$. Prenons $a_0 = a + p$ et $b_0 = b$, de sorte que $a_0 > b_0$. Pour tout k et tout $r \leqslant q-1$, on a

$$a_{k\omega+r} = a_r + kS(a), quad b_{k\omega+r} = b_r + kS(b).$$

En prenant k suffisamment grand pour que $k(S(b) - S(a)) > \max_{0 \leqslant r \leqslant q-1}(a_r - b_r)$, on trouve qu'il existe un entier k tel que, pour tout $n \geqslant k\omega$, on ait $a_n < b_n$. En particulier, il existe un indice i maximal tel que $a_i > b_i$. Les suites $(a_i, a_{i+1}, \ldots)$ et $(b_i, b_{i+1}, \ldots)$ vérifient donc le résultat voulu.

Là, justifier l'infinité de nombres premiers est plus simple : si on a construit $p_1, \ldots, p_r$, on choisit $q > \max(p_1, \ldots, p_r)$. Un diviseur premier p de $2^q - 1$ vérifie $q \mid p-1$ donc $p \geqslant q+1 > \max(p_1, \ldots, p_r)$ ce qui justifie que p est distinct des nombres premiers construits précédemment.

Remarque : Dans les deux cas, l'existence d'une infinité de p peut être justifiée rapidement par le théorème de Zsigmondy.

2.5 Le théorème des restes chinois

Exercice 2.93. Un chef militaire possède un régiment avec un certain nombre de soldats compris entre 200 et 270. Il souhaite savoir combien de soldats il possède. Pour cela il fait se ranger les soldats par groupes de 10 et s'aperçoit que 8 soldats restent. Il fait ensuite se ranger les soldats par groupes de 7 et s'aperçoit que 5 soldats restent. Combien y a-t-il de soldats ?

Solution 2.93. Il s'agit de trouver un entier m compris entre 200 et 270 vérifiant le système

$$\begin{cases} m & \equiv 8 & \mod 10 \\ m & \equiv 5 & \mod 7 \end{cases}$$

La résolution explicite du système indique que les entiers m solutions sont de la forme $m = 68 + 70k$, avec k entier. Puisque $200 \leqslant m \leqslant 270$, le seul entier k convenant est $k = 2$, ce qui donne $\boxed{m = 208}$.

Exercice 2.94.

1. Montrer qu'une suite arithmétique de raison 5 et une suite arithmétique de raison 7 contiennent toujours un terme en commun.
2. Que dire d'une suite périodique à la fois de période 5 et de période 7 ?

Solution 2.94.

1. Le terme général de la première suite s'écrit $5n + u_0$, tandis que le terme général de la deuxième suite s'écrit $7n + v_0$. Comme 5 et 7 sont premiers entre eux, le système suivant

$$\begin{cases} m & \equiv u_0 & \mod 5 \\ m & \equiv v_0 & \mod 7 \end{cases}$$

admet une solution m. On a donc un entier k et un entier j tels que $m = 5k + u_0 = 7j + v_0$. Les deux suites ont donc bien un terme en commun.

Remarque : En réalité, comme l'indique la preuve du théorème des restes chinois, dans le cas d'un système à deux équations, le système peut également être résolu élémentairement avec le théorème de Bezout.

2. Montrons que la suite, notée (u_n), est constante. Pour cela, on fixe un indice i et on montre que $u_i = u_{i+1}$. D'après la question précédente, il existe un entier m et deux entiers k et j (que l'on peut choisir positifs en prenant m suffisamment grand) tels que $m = 5k + i = 7j + i + 1$. On a alors par périodicité

$$u_i = u_{5k+i} = u_m = u_{7j+i+1} = u_{i+1}.$$

Ceci conclut.

Exercice 2.95. (Inspiré de Caucase MO 2018) Soit $n \geqslant 1$ un entier.

1. Soient $a_1, \ldots, a_k$ des entiers strictement positifs. Existe-t-il un entier n tel que, pour tout indice $1 \leqslant i \leqslant k$, il existe un entier x_i tel que $a_i n = x_i^{p_i}$, où p_i est le $i-$ème nombre premier ?
2. Soient $a_1, \ldots, a_k$ des entiers strictement positifs. Existe-t-il un entier n tel que, pour tout indice $1 \leqslant i \leqslant k$, il existe un entier x_i tel que $a_i n = x_i^i$?

Solution 2.95.

1. Soit $\mathcal{P}$ l'ensemble des nombres premiers qui divisent l'un des a_i. Il s'agit de trouver un entier n tel que, pour tout nombre premier q dans $\mathcal{P}$, $p_i \mid v_q(a_i n)$ pour tout indice i. Cette congruence se réécrit sous la forme

$$v_q(n) \equiv -v_q(a_i) \mod p_i \quad \forall\, 1 \leqslant i \leqslant k.$$

D'après le théorème des restes chinois, pour tout q, il existe un entier x_q strictement positif solution du système. L'entier n construit comme le produit des q^{x_q} pour q dans $\mathcal{P}$ vérifie alors l'énoncé.

2. La réponse est **non**, et pour le voir on peut revenir à la preuve précédente pour voir où intervient l'hypothèse que les p_i doivent être premiers entre eux. Par exemple, si $a_2 = 2$ et $a_4 = 4$, l'énoncé implique que

$$1 + v_2(n) = v_2(a_2 n) = 0 = v_2(a_4 n) = 2 + v_2(n) \equiv v_2(n) \mod 2,$$

ce qui est impossible.

Exercice 2.96. Prouver que pour tout entier positif n, il existe des entiers a et b tels que $9a^2 + 4b^2 - 1$ soit divisible par n.

Solution 2.96. On commence par le cas où n est une puissance d'un nombre premier puis, pour le cas général, on utilise le théorème des restes chinois pour combiner les solutions modulo les facteurs premiers de n.

Soit p un nombre premier et $\alpha > 0$ un entier.

- ➢ Si $p = 2$, alors en prenant $a = 3^{-1}$ l'inverse de 3 modulo 2^α et $b = 0$, on trouve $9a^2 + 4b^2 \equiv 1 \mod 2^\alpha$.
- ➢ Si $p \neq 2$, alors en prenant $a = 0$ et $b = 2^{-1}$ l'inverse de 2 modulo p^α, on trouve $9a^2 + 4b^2 - 1 \mod p^\alpha$.

On note à présent $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers de n. Pour tout indice i, on note (a_i, b_i) les entiers tels que $9a_i^2 + 4b_i^2 - 1$ soit divisible par $p_i^{\alpha_i}$. D'après le théorème des restes chinois, il existe deux entiers a et b tels que

$$a \equiv a_i \mod p_i^{\alpha_i}, \qquad b \equiv b_i \mod p_i^{\alpha_i} \quad \forall i = 1, \ldots, r.$$

Alors on vérifie que, pour tout indice i,

$$9a^2 + 4b^2 \equiv 9a_i^2 + 4b_i^2 \equiv 1 \mod p_i^{\alpha_i}.$$

Ainsi, $p_i^{\alpha_i}$ divise $9a^2 + 4b^2 - 1$ pour tout i, donc c'est également le cas de n, ce qui conclut.

Exercice 2.97. Soit p un nombre premier. Montrer qu'il existe un entier $n \geqslant 1$ tel que p divise $2025^n - n$.

Solution 2.97. L'idée est que, sauf cas dégénéré, 2025^n définit, modulo p, une suite périodique de période $p-1$ (via la théorie de l'ordre et le petit théorème de Fermat), tandis que le reste de n modulo p est périodique de période p. Ces deux suites ont donc vocation à coïncider. On peut alors trouver un n tel que n et 2025^n ont le même reste modulo p.

Si p est un diviseur de 2025, il suffit de choisir $n = 2025$. Sinon, d'après le théorème des restes chinois, on dispose d'un entier n tel que

$$\begin{cases} n \equiv 0 & \mod p - 1 \\ n \equiv 1 & \mod p \end{cases}$$

On a alors, avec le petit théorème de Fermat,

$$2025^n - n \equiv 2025^0 - 1 = 0 \mod p,$$

comme voulu.

Remarque : Une résolution explicite indique que $n = (p-1)^2$ fonctionne.

Exercice 2.98.

1. Montrer que pour tout entier n, il existe n entiers consécutifs tels qu'aucun d'entre eux n'est un nombre premier.
2. *(IMO 1989)* Montrer que pour tout entier n, il existe n entiers consécutifs tels qu'aucun d'entre eux n'est une puissance d'un nombre premier.

Solution 2.98.

1. La preuve la plus simple est de considérer les entiers $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$, qui admettent respectivement $2, 3, \ldots n+1$ comme diviseurs strictes. La question suivante s'adapte pour donner une preuve de cette question utilisant le théorème des restes chinois.
2. Pour garantir qu'un entier n'est pas une puissance d'un nombre premier p, on peut le forcer à être strictement plus grand que p et divisible par p mais pas par p^2. Cela assure que n n'est pas une puissance de p et que ce n'est pas une puissance d'un autre nombre premier. Un exemple d'entier divisible par p mais pas par p^2 est un entier x tel que $x \equiv p \mod p^2$.

   Pour construire des entiers consécutifs vérifiant cette caractérisation, on peut s'inspirer de l'exemple de la théorie. On fixe $p_1, \ldots, p_n$ des nombres premiers distincts. D'après le théorème des restes chinois, il existe un entier x tel que

$$\begin{cases} x+1 \equiv p_1 \mod p_1^2 \\ x+2 \equiv p_2 \mod p_2^2 \\ \vdots \\ x+n \equiv p_n \mod p_n^2 \end{cases} \iff \begin{cases} x \equiv p_1 - 1 \mod p_1^2 \\ x \equiv p_2 - 2 \mod p_2^2 \\ \vdots \\ x \equiv p_n - n \mod p_n^2. \end{cases}$$

   Les entiers $x+1, \ldots, x+n$ sont donc des entiers consécutifs tels qu'aucun n'est une puissance d'un nombre premier.

Exercice 2.99. (Belarus MO 2018) Déterminer tous les entiers n strictement positifs ayant la propriété suivante : si l'on pose $a_k = \text{PPCM}(k, k+1, \ldots, k+n-1)$ pour tout entier strictement positif k, alors la suite (a_k) est croissante.

Solution 2.99. **Réponse :** le seule entier est $n = 2$.

Si $n = 2$, alors $a_k = k(k+1)$, qui est bien le terme général d'une suite strictement croissante.

On suppose que $n \geqslant 3$ et on exhibe un entier k pour lequel $a_{k+1} < a_k$. Il s'agit de trouver un entier k tel que k est premier avec $N_k = \text{PPCM}(k+1, \ldots, k+n-1)$ (afin que $a_k = kN_k$) mais tel que $k+n$ admette un facteur premier p qui divise N_k, de sorte que $a_{k+1} = N_k \dfrac{k+n}{p}$. Lorsque $\dfrac{k+n}{p} < k$, cela implique $a_{k+1} < a_k$.

Avant de continuer, on examine la première condition de notre cahier des charges : k premier avec N_k. Un éventuel diviseur commun q à k et $k+i$ doit également diviser i. Il suffit donc de choisir k premier avec $2 \times \ldots \times (n-1) = (n-1)!$.

Soit p un diviseur premier de $n-1$ et $\{q_1, \ldots, q_r\}$ l'ensemble des nombres premiers inférieurs ou égaux à $n-1$ et distincts de p. On choisit k une solution strictement positive du système :

$$\begin{cases} k \equiv -1 \mod p \\ k \equiv 1 \mod q_i \text{ pour } i = 1, \ldots, r \end{cases}$$

Alors k est premier avec chacun des q_i et avec p, donc k est premier avec $(n-1)!$. De plus, comme $p \mid n-1$, $k+n \equiv k+1 \equiv 0 \mod p$, donc p divise $k+n$. Pour k choisi suffisamment grand, on a en plus $k+n < kp$. On déduit que

$$a_k = kN_k > \frac{k+n}{p} N_k \geqslant \text{PPCM}(k+1, \ldots, k+n) = a_{k+1}.$$

La suite (a_k) n'est donc pas croissante.

Exercice 2.100. Un point du plan à coordonnées entières (a, b) est dit *invisible* depuis 0 si il existe un point (c, d) du plan, distinct de $(0, 0)$ et (a, b) et qui appartient au segment reliant $(0, 0)$ et (a, b).

Montrer qu'il existe un carré de taille 2026×2026 contenant 2026^2 points invisibles depuis 0.

Solution 2.100. On vérifie qu'un point (a, b) est invisible si et seulement si $\mathrm{PGCD}(a, b) \neq 1$. En effet, si (c, d) est sur le segment reliant $(0, 0)$ et (a, b), cela signifie qu'il existe $k \neq 1$ tel que $a = kc, b = kd$, ce qui implique que $k \mid \mathrm{PGCD}(a, b)$. Réciproquement, si $\mathrm{PGCD}(a, b) = k \neq 1$, on dispose d'entiers c et d tels que $a = kc$ et $b = kd$, et le point (c, d) est donc sur le segment reliant $(0, 0)$ et (a, b).

Il s'agit donc de trouver un entier a et un entier b tels que, pour tout $0 \leqslant k, \ell \leqslant 2025$, $\mathrm{PGCD}(a + k, b + \ell) \neq 1$, signifiant qu'il existe un nombre premier $p_{k,\ell}$ tel que $a \equiv -k \mod p_{k,\ell}$ et $b \equiv -\ell \mod p_{k,\ell}$.

On prend donc le problème par l'autre bout et on choisit $(p_{k,\ell})_{0 \leqslant k,\ell \leqslant 2025}$ une famille de 2026^2 nombres premeirs distincts. D'après le théorème des restes chinois, il existe un entier a tel que

$$a \equiv -k \mod p_{k,\ell}, \quad \text{pour tous } 0 \leqslant k, \ell \leqslant 2025$$

et un entier b tel que

$$b \equiv -\ell \mod p_{k,\ell}, \quad \text{pour tous } 0 \leqslant k, \ell \leqslant 2025.$$

Pour tout $0 \leqslant k, \ell \leqslant 2025$, le nombre $p_{k,\ell}$ divise $a + k$ et $b + \ell$, donc le point $(a + k, b + \ell)$ est invisible. Le carré formé par les points $(a + k, b + \ell)$ pour $0 \leqslant k, \ell \leqslant 2025$ convient donc. Dans le tableau ci-dessous, on a représenté dans la case de coordonnée (i, j) un diviseur commun à $a + i$ et $b + j$.

	b	$b+1$	$\dots$	$b+2025$
a	$p_{0,0}$	$p_{0,1}$	$\cdots$	$p_{0,2025}$
$a+1$	$p_{1,0}$	$p_{1,1}$	$\cdots$	$p_{1,2025}$
$a+2$	$p_{2,0}$	$p_{2,1}$	$\cdots$	$p_{2,2025}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$a+2025$	$p_{2025,0}$	$p_{2025,1}$	$\cdots$	$p_{2025,2025}$

Exercice 2.101.

1. Soit P un polynôme à coefficients entiers et non constant. On suppose qu'il existe n nombres premiers $p_1, \dots, p_n$ divisant chacun au moins un entier de la forme $P(t)$. Montrer qu'il existe un entier t tel que $P(t)$ est divisible par $p_1 \dots p_n$.
2. *(USAMO 2008 P1)* Soit $n \geqslant 2$. Montrer qu'il existe n entiers $k_1, \dots, k_n$ premiers entre eux deux à deux tels que $k_1 \dots k_n - 1$ est le produit de deux entiers consécutifs.

Solution 2.101.

1. On rappelle que si P est à coefficients entiers et si a et b sont deux entiers, alors $a - b \mid P(a) - P(b)$. Notons à présent t_k un entier tel que $p_k \mid P(t_k)$. On a alors que pour tout entier n, $p_k \mid np_k \mid P(t_k + np_k) - P(t_k)$, c'est-à-dire $p_k \mid P(t_k + np_k)$ pour tout entier n. D'après le théorème des restes chinois, on dispose d'un entier t tel que

   $$t \equiv t_k \mod p_k \quad \forall k = 1, \dots, n.$$

   Un tel entier t vérifie donc bien que $P(t) \equiv P(t_k) \equiv 0 \mod p_k$ pour tout indice k, comme attendue.
2. L'énoncé demande l'existence de $k_1, \dots, k_n$ et d'un entier t tels que $k_1 \dots k_n = t(t + 1) + 1$. L'hypothèse "$n$ entiers premiers entre eux" est un peu superflue, et l'énoncé admet la réécriture plus souple qu'il existe un entier t tel que $t^2 + t + 1$ admet au moins n facteurs premiers distincts. Si c'est le cas, en notant $t^2 + t + 1 = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers de $t^2 + t + 1$, avec $r \geqslant n$, il suffit de choisir $k_i = p_i^{\alpha_i}$ pour $i = 1, \dots, n - 1$ et $k_n = \prod_{i=1}^{n-1} p_i^{\alpha_i}$.

   D'après la question précédente appliquée au polynôme $P(X) = X^2 + X + 1$, si l'on trouve n nombres premiers $p_1, \dots, p_n$ divisant chacun un terme de la forme $P(x)$, alors on pourra trouver un t tel que $P(t)$ est divisible par $p_1, \dots, p_n$, comme voulu. Il s'agit désormais de démontrer qu'il existe une infinité de nombres premiers divisant un terme de la forme $P(t)$. Comme bien d'autres preuves d'existences d'infinité

de nombres premiers, on adapte la preuve de l'existence d'une infinité de nombres premiers. Supposons avoir trouvé $p_1, \dots, p_N$ nombres premiers divisant un terme de la forme $P(t)$. On pose $T = p_1 \dots p_N$. Le nombre T^2+T+1 n'est alors divisible par aucun des p_i. Il admet donc un diviseur premier (éventuellement égal à lui-même) qui est distinct des p_i, comme voulu.

Remarque : Le fait que le polynôme X^2+X+1 admette une infinité de diviseurs premiers est un cas particulier du théorème de Schur, qui est présenté dans la section 3.

Exercice 2.102.

1. Montrer qu'il existe un ensemble A d'entiers strictement positifs de cardinal 2022 tel que, pour tout sous-ensemble B non vide de A, la moyenne arithmétique et la moyenne géométrique des éléments de B sont des entiers.
2. Montrer qu'il existe un sous-ensemble A d'entiers strictement positifs de cardinal 2022 tel que pour tout sous-ensemble B de A, la moyenne arithmétique des éléments de B est une puissance parfaite.

Solution 2.102. 1) Pour cela, on prend 2022 entiers $\{a_1, \dots, a_{2022}\}$. Pour tout sous-ensemble B, on note $m(B)$ la moyenne arithmétique des éléments du sous-ensemble B. Alors $|B|m(B)$ est entier pour tout B, avec $|B| \leqslant 2022$, de sorte que l'ensemble $\{2022!a_1, 2022!a_2, \dots, 2022!a_{2022}\}$ a toutes les moyennes arithmétiques de ses éléments entières. En s'inspirant de ce procédé, l'ensemble $\{(2022!a_1)^{2022!}, \dots, (2022!a_{2022})^{2022!}\}$ possède toutes ses moyennes arithmétiques et géométriques entières.

2) Prenons $A' = \{b_1, \dots, b_{2022}\}$ un ensemble dont les moyennes arithmétiques sont toutes entières. Avec les notations de la question 1), pour tout sous-ensemble $B \subset A'$, on note $m(B)$ la moyenne des éléments de B.

On veut multiplier chaque entier par une nouvelle constante de sorte que les $m(B)$ soient des puissances parfaites. Pour cela, on écrit $m(B) = \prod p_i^{\alpha_i(B)}$. On veut multiplier tous les entiers par un nombre $k = \prod p_i^{\beta_i}$, de sorte que la moyenne devienne $km(B) = \prod p_i^{\alpha_i(B)+\beta_i}$ soit une puissance parfaite.

On va utiliser les restes chinois pour cela, et le plus simple est que $km(B)$ soit de la forme $a^{p(B)}$ avec $p(B)$ un nombre premier. On se donne donc $2^{2022}-1$ nombres premiers tous supérieux ou égaux aux $\alpha_i(B)$, et on choisit β_i vérifiant pour tout B

$$\beta_i \equiv -\alpha_i(B) \mod p(B)$$

L'ensemble $\{kb_1, \dots, kb_2\}$ vérifie alors la propriété voulue.

Exercice 2.103. (USA TSTST 2019 P7)

Une fonction f de $\mathbb{Z}$ dans $\{1, \dots, 1000\}$ est dite *intéressante* si, pour tous les entiers x et y, on a

$$\mathrm{PGCD}(f(x), f(y)) = \mathrm{PGCD}(f(x), x-y)$$

Combien existe-t-il de fonctions intéressantes ?

Solution 2.103. **Réponse :** $1+2+\ldots+1000 = \displaystyle\sum_{n=1}^{1000} n = \frac{1000 \times 1001}{2}$.

Soit f une fonction intéressante éventuelle, puis n le PPCM des entiers $f(x)$, et

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

une factorisation de n en produit de facteurs premiers. Pour tout entier $i \leqslant r$, on se donne un entier x_i tel que p^{α_i} divise $f(x_i)$. Le théorème des restes chinois indique qu'il existe un résidu m modulo n tel que $m \equiv x_i \pmod{p_i^{\alpha_i}}$ pour tout i. On vérifie alors que $p_i^{\alpha_i}$ divise $\mathrm{PGCD}(f(x_i), x_i - m) = \mathrm{PGCD}(f(x_i), f(m))$, de sorte que $f(m)$ est divisible par chacun des facteurs $p_i^{\alpha_i}$, donc par n lui-même.
Par conséquent, pour tout entier x, et puisque $f(x)$ divise $n = f(m)$, on sait que

$$f(x) = \mathrm{PGCD}(f(m), f(x)) = \mathrm{PGCD}(f(m), m-x) = \mathrm{PGCD}(n, x-m).$$

Réciproquement, si l'on note $f_{m,n}$ la fonction définie par $f_{m,n} : x \mapsto \mathrm{PGCD}(n, x-m)$, on constate que

$$\mathrm{PGCD}(f_{m,n}(x), f_{m,n}(y)) = \mathrm{PGCD}(n, x-m, y-m) = \mathrm{PGCD}(n, x-m, x-y) = \mathrm{PGCD}(f(x), x-y).$$

Ainsi, chaque fonction $f_{m,n}$ est intéressante.
Enfin, si deux fonctions $f_{m,n}$ et $f_{m',n'}$ coïncident, on sait que n et n' sont tous deux égaux au PPCM des entiers $fm, n(x) = f_{m',n'}(x)$ obtenus lorsque $x \in \mathbb{Z}$, de sorte que $n = n'$. Mais alors $n = f_{m,n}(n) = f_{m',n}(n) = \mathrm{PGCD}(n, m - m')$, donc n divise $m - m'$; réciproquement, si n divise $m - m'$, les fonctions $f_{m,n}$ et $f_{m',n}$ coïncident.
On a donc autant de fonctions intéressantes distinctes que de couples (n, m) avec $n \in \{1, \dots, 1000\}$ et $m \in \{1, \dots, n\}$, ce qui nous fait un total de

$$\sum_{n=1}^{1000} n = \frac{1000 \times 1001}{2} = 500500$$

fonctions intéressantes.

Exercice 2.104. (APMO 2009 P4) Montrer que pour tout entier strictement positif k, il existe des entiers $a_1, \dots, a_k, b_1, \dots, b_k$ deux à deux distincts, tels que a_i et b_i sont premiers entre eux pour tout indice i, et tels que les entiers

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \dots, \quad \frac{a_k}{b_k},$$

forment une progression arithmétique.

Solution 2.104.

➢ Commentaire :

> Comme il y a beaucoup de variables, il faut à tout prix se simplifier la vie et, dès que possible, fixer certaines d'entre elles.
>
> Notons $r = c/d$ la raison de la suite. On a alors pour tout i
>
> $$\frac{a_i}{b_i} = \frac{a_1}{b_1} + k\frac{c}{d}.$$
>
> Il y a fort à parier que d doive posséder des facteurs communs avec les b_i. De plus, si on a une solution avec $c = 1$, on aura une solution pour tout c par homogénéité de l'équation. On peut donc supposer que $c = 1$.
>
> Pour les mêmes raisons, on peut supposer que $b_1, \dots, b_k$ sont premiers entre eux dans leur ensemble mais qu'ils ne sont pas premiers entre eux deux à deux. Pour construire ça, on choisit $p_1, \dots, p_k$ des nombres premiers distincts, on pose $P = p_1 \dots p_k$ et $b_i = P/p_i$. On pose également $d = P$. L'équation devient :
>
> $$\frac{a_i}{P/p_i} = \frac{a_1}{P/p_1} + k\frac{1}{P}, \quad \iff a_i p_i = a_1 p_1 + i.$$
>
> Construire a_1 à partir de cela n'est plus très difficile.

Soient $p_1, \dots, p_k$ des nombres premiers distincts tous supérieurs à $k + 1$, $P = p_1 \dots p_k$ et $b_i = P/p_i$. On pose également $d = P$. D'après le théorème des restes chinois, il existe un entier a_1(que l'on choisir aussi grand qu'on veut) vérifiant

$$a_1 \equiv -ip_1^{-1} \mod p_i, \quad \text{pour tout } i \geqslant 2.$$

Pour tout p_i, il existe donc un entier a_i tel que $p_1 a_i + k = p_i a_i$. Montrons que les b_i et les a_i sont deux à deux distincts. Les b_i sont bien sûr deux à deux distincts. Supposons qu'il existe deux indices i et j tels que $a_i = a_j$. L'égalité devient $a_1 = \dfrac{ip_j - jp_i}{p_i - p_j}$. En prenant a_1 suffisamment grand, on garantit que a_1 ne peut pas prendre cette valeur. Donc les a_i sont deux à deux distincts.

Supposons que $a_i = b_j$ pour certains indices i et j. Cela implique que $a_1 = p_i P/(p_j p_1) - i$. Là encore, on peut choisir a_1 suffisamment grand pour que cette égalité soit fausse pour tous i, j. On a donc bien que les a_i et b_i sont deux à deux distincts.

Ensuite, pour tout i, les nombres b_i et a_i sont premiers entre eux : si p divise b_i et a_i, alors $p = p_j$ pour $j \neq i$. On a donc $p_j \mid p_1 a_1 + i - (p_1 a_1 + j) = i - j$, ce qui est exclut car $p_j > |i - j|$ par construction.

Il reste à vérifier que les fractions $a_1/b_1, \ldots, a_k/b_k$ sont en progression arithmétique. Mais pour tout i, on a

$$\frac{a_i}{b_i} = \frac{(p_1 a_1 + i)/p_i}{P/p_i} = \frac{a_1}{b_1} + \frac{i}{P},$$

ce qui est le résultat voulu.

Exercice 2.105. (IMO 2016 P4) On pose $P(n) = n^2+n+1$. On dit qu'un ensemble est *parfumé* s'il contient au moins deux éléments et si chaque élément possède un facteur premier en commun avec au moins un autre élément. Trouver le plus petit entier positif b tel qu'il existe un entier positif a tel que l'ensemble $\{P(a), \dots, P(a+b-1)\}$ soit parfumé.

Solution 2.105. **Réponse :** $b = 6$.

Commençons par regarder les facteurs premiers communs aux nombres $P(n)$ et $P(n+k)$ pour des petites valeurs de k.

- ➢ Pour $k = 1$: Soit d un diviseur premier de $P(n)$ et de $P(n+1)$. Alors $d \mid P(n+1) - P(n) = 2n+2$ donc d divise $2P(n) - n(2n+2) = 2$. Mais $P(n)$ est impair n car $2 \mid n(n+1)$. Donc $d = 1$ et $P(n)$ et $P(n+1)$ sont premiers entre eux.
- ➢ Pour $k = 2$: De la même façon que précédemment, on trouve que si d est un diviseur de $P(n)$ et de $P(n+2)$, alors $d \mid P(n+2) - P(n) = 4n+6$. Comme $P(n)$ est impair, d divise même $2n+3$. Donc $d \mid n(2n+3) - 2P(n) = n-2$. Donc $d \mid 2n+3-2(n-2) = 7$. Ainsi $\mathrm{PGCD}(P(n), P(n+2)) \in \{1, 7\}$. Notons que si $\mathrm{PGCD}(P(n), P(n+2)) = 7$, alors 7 divise $n-2$ par nos calculs précédents. Réciproquement, si $n \equiv 2 \mod 7$, alors $\mathrm{PGCD}(P(n), P(n+2)) = 7$.
- ➢ Pour $k = 3$: Cette fois-ci, si d divise $P(n)$ et $P(n+3)$, alors $d \mid P(n+3) - P(n) = 6n+12$, de sorte que $d \mid 3n+6$. Ensuite, $d \mid 3P(n) - n(3n+6) = 3-3n$. Ainsi, $d \mid 9$. Donc $\mathrm{PGCD}(P(n), P(n+3)) \in \{1, 3, 9\}$. On vérifie alors que si $n \equiv 0, 2 \mod 3$, alors 3 ne divise pas $P(n)$ donc $\mathrm{PGCD}(P(n), P(n+3)) = 1$ et si $n \equiv 1 \mod 3$, alors $3 \mid \mathrm{PGCD}(P(n), P(n+3))$.

Soit b tel qu'il existe a tel que $\{P(a), \dots, P(a+b-1)\}$, soit parfumé. Notons que $P(a)$ et $P(a+1)$ sont premiers entre eux, de même que $P(a+1)$ et $P(a+2)$, donc $\boxed{b \geqslant 4}$ (si $b = 3$, alors $P(a+1)$ n'a de facteur commun ni avec $P(a)$ si avec $P(a+2)$). Si $b = 4$, $P(a+1)$ ne peut avoir de facteur commun qu'avec $P(a+3)$. On a vu plus haut que ce seul facteur possible est 7, ce qui force $a+1 \equiv 2 \mod 7$. De même, $P(a+2)$ ne peut avoir de facteur commun qu'avec $P(a)$, donc $a \equiv 2 \mod 7$. Les deux congruences ne peuvent être satisfaites en même temps. Donc $\boxed{b \geqslant 5}$.

Si $b = 5$, $P(a+2)$ ne peut avoir de facteur commun qu'avec $P(a)$ et $P(a+4)$, ce qui implique là aussi que $a \equiv 2 \mod 7$ et $a+2 \equiv 2 \mod 7$, ce qui est absurde. Donc $\boxed{b \geqslant 5}$.

Réciproquement, exhibons un a tel que $\{P(a), \dots, P(a+5)\}$ est parfumé. La raisonnement précédent peut nous convaincre qu'il faut chercher un facteur commun à $P(n)$ et $P(n+4)$.

- ➢ Si $k = 4$: Soit d divisant $P(n)$ et $P(n+4)$. Alors $d \mid P(n+4) - P(n) = 8n+20$, soit $d \mid 2n+5$. Donc $d \mid n(2n+5) - 2P(n) = 3n-2$. Donc $d \mid 3(2n+5) - 2(3n-2) = 19$. Ainsi, $PGCD(P(n), P(n+4)) \in \{1, 19\}$. De plus, si $PGCD(P(n), P(n+4)) = 19$, $19 \mid 3n-2$, ce qui a lieu si et seulement si $n \equiv 7 \mod 19$.

Cherchons alors a tel que

$$\mathrm{PGCD}(P(a), P(a+4)) > 1, \quad \mathrm{PGCD}(P(a+1), P(a+3)) > 1, \quad \mathrm{PGCD}(P(a+2), P(a+5)) > 1,$$

de sorte que l'ensemble $\{P(a), \dots, P(a+5)\}$ est parfumé. D'après les calculs ci-dessus, cela exige que

$$a \equiv 7 \mod 19, \quad a+1 \equiv 2 \mod 7, \quad a+2 \equiv 1 \mod 3.$$

Ce système admet une solution d'après le théorème des restes chinois, ce qui garantit l'existence d'un entier a tel que l'ensemble $\{P(a), \dots, P(a+5)\}$ est parfumé et conclut que le plus petit entier est $b = 5$.
Remarque : La résolution explicite du système donne $a = 196$.

Exercice 2.106. (RMM 2021 P2) Alice et Bob jouent au jeu suivant. Alice choisit un entier N tel que $1 \leqslant N \leqslant 5000$, qu'elle ne communique pas à Bob. Elle choisit 20 entiers distincts $a_1, \ldots, a_{20}$ tels que, pour tout $k = 1, \ldots, 20$, $a_k \equiv N \mod k$. Un coup consiste, pour Bob, à choisir un ensemble S d'indices, et Alice lui donne l'ensemble $\{a_k, k \in S\}$ sans lui dire quel nombre correspond à quel indice.

Déterminer le plus petit nombre de coups nécessaires à Bob pour déterminer l'entier N.

Solution 2.106. **Réponse :** le plus petit nombre de coups nécessaires est 2.

Commençons par montrer que Bob peut déterminer N en deux coups. Bob choisit les deux ensembles $\{17, 20\}$ et $\{19, 20\}$, Alice lui communique les paires $\{a_{17}, a_{20}\}$ et $\{a_{19}, a_{20}\}$. En identifiant l'élément commun, Bob peut alors déterminer a_{17}, a_{19} et a_{20}. Il sait alors que N satisifait le système

$$\begin{cases} N & \equiv a_{17} & \mod 17 \\ N & \equiv a_{19} & \mod 19 \\ N & \equiv a_{20} & \mod 20 \end{cases}$$

qui admet une unique solution modulo $17 \times 19 \times 20 = 6420 > 5000$. Ainsi, il y au plus un entier N dans $[\![1, 5000]\!]$ vérifiant le système ci-dessus, donc Bob peut le déterminer.

Montrons à présent que, si Bob n'a qu'un essai, il n'est pas certain de déterminer N. Supposons que Bob a choisi l'ensemble d'indices $S = \{s_1, \ldots, s_k\}$. Il suffit de montrer qu'il existe deux entiers N et N' de $[\![1, 5000]\!]$, des entiers $b_1, \ldots, b_k$ et un bijection f de $\{1, \ldots, k\}$ dans lui même telle que

$$b_i \equiv N \mod s_i, \quad \text{et} \quad b_{f(i)} \equiv N' \mod s_i.$$

Si ces entiers existent, alors si Alice donne l'ensemble $\{b_1, \ldots, b_k\}$, alors Bob ne pourra pas distinguer N et de N' avec les systèmes donnés.

➢ **Commentaire :**

> Avec cette stratégie, dans le système ci-dessus, on a $s_i \mid b_i - N$ et $s_{f^{-1}(i)} \mid b_i - N'$, donc $\mathrm{PGCD}(s_i, s_{f^{-1}(i)}) \mid N - N'$ pour tout i. Comme on veut un construction qui marche pour tout S, il faut que, $\mathrm{PGCD}(a, b) \mid N - N'$ pour tout $a, b \in [\![1, 20]\!]$, soit que
>
> $$\mathrm{PPCM}\{\mathrm{PGCD}(a, b); a, b \in [\![1, 20]\!]\} \mid N - N'.$$
>
> Après calcul, on déduit que $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 \mid N - N'$. On peut donc prendre $N' = N + 2520$ et N tel que $N' \leqslant 5000$.
>
> Ensuite, dans l'objectif de simplifier les choses, on peut choisir la bijection $f(i) = i + 1 \mod k$.

Il reste à construire tous ces entiers. On pose $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$ et $N = 1$ et $N' = M + 1 = 2521$. Prenons la bijection $f(i) = i + 1 \mod k$.

Fisons un indice i. On désire construire un entier b_i tel que

$$\begin{cases} b_i & \equiv 1 & \mod s_i \\ b_i & \equiv M + 1 & \mod s_{i+1} \end{cases}$$

On note $d_i = \mathrm{PGCD}(s_i, s_{i+1})$ et $s_i = d_i x_i$ et $s_{i+1} = d_i y_i$. D'après le théorème de Bezout, il existe deux entiers u et v tels que $ux_i - vy_i = M/d_i$. On déduit que le nombre $b_i = ux_i d_i + 1 + rs_i s_{i+1} = vy_i d_i + M + 1 + rs_i s_{i+1}$ vérifie la congruence voulue. On peut de plus faire varier la valeur de r pour rendre les b_i deux à deux distincts. Ainsi, si Alice donne l'ensemble $\{b_1, \ldots, b_k\}$, Bob ne peut pas distinguer les entiers 1 et $1 + M$ avec les informations données. Ceci conclut que Bob ne peut pas réussir en un essai.

3 Beaucoup de théorie

3.1 LTE, Zsigmondy et autres

3.1.1 LTE et Zsigmondy

Exercice 3.1. (LTE cas $p = 2$) Soient a et b des entiers impairs. Montrer que pour tout entier pair n,

$$v_2(a^n - b^n) = v_2(b - a) + v_2(a + b) + v_2(n) - 1.$$

Solution 3.1. On copie la preuve du cas p impair, et on procède par récurrence sur $v_2(n)$. Seule l'initialisation va être modifiée.

Initialisation : Si $v_2(n) = 1$, on note $n = 2\beta$ où β est impair. On a alors

$$\begin{aligned} a^n - b^n &= (a^\beta - b^\beta)(a^\beta + b^\beta) \\ &= (a-b)\underbrace{(a^{\beta-1} + a^{\beta-2}b + \ldots + ab^{\beta-2} + b^{\beta-1})}_{\equiv 1 \mod 2}(a+b)\underbrace{(a^{\beta-1} - a^{\beta-2}b + \ldots - ab^{\beta-2} + b^{\beta-1})}_{\equiv 1 \mod 2}. \end{aligned}$$

On déduit que

$$v_2(a^n - b^n) = v_2(a-b) + v_2(a+b) = v_2(b-a) + v_2(a+b) + v_2(n) - 1.$$

On a donc bien la formule lorsque $v_2(n) = 1$.

Hérédité : On se ramène à l'énoncé dans le cas $n = 2$. On suppose que $v_2(a^\ell - b^\ell) = v_2(a-b) + v_2(a+b) + v_2(\ell) - 1$ pour tout entier ℓ tel que $v_2(\ell) = k$, avec $k \geqslant 1$ fixé. Soit n un entier tel que $v_p(n) = k+1$. On écrit $n = 2\ell$ avec $v_2(\ell) = k$. Comme $k \geqslant 1$, les nombres a^ℓ et b^ℓ sont des carrés impairs. On a donc $a^\ell + b^\ell \equiv 2 \mod 4$, donc $v_2(a^\ell + b^\ell) = 1$. Il vient

$$v_2(a^{2\ell} - b^{2\ell}) = v_2(a^\ell - b^\ell) + v_2(a^\ell + b^\ell) = v_2(a-b) + v_2(a+b) + v_2(\ell) - 1 + 1,$$

ce qui prouve que $v_2(a^{2\ell} - b^{2\ell}) = v_2(a-b) + v_2(a+b) + v_2(2\ell) - 1$ et achève la récurrence.

Exercice 3.2. Montrer que $3^{1000} \mid 2^{3^{999}} + 1$.

Solution 3.2. D'après le lemme LTE (cas +),

$$v_3(2^{3^{999}} + 1) = v_3(2+1) + v_3(3^{999}) = 1 + 999 = 1000.$$

Exercice 3.3. (IMO SL 1991) Déterminer le plus grand entier k tel que 1991^k divise $1990^{1991^{1992}} + 1992^{1991^{1990}}$.

Solution 3.3. Posons $A = 1990^{1991^{1992}} + 1992^{1991^{1990}}$. L'entier A s'écrit sous la forme

$$A = (1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}.$$

Dans le but d'appliquer le lemme LTE, on observe la décomposition $1991 = 11 \times 181$. On remarque alors que $1990^{1991^2} + 1992 \equiv (-1)^{1991^2} + 1 \equiv 0 \mod 1991$, donc $11 \times 181 \mid 1990^{1991^2} + 1992$. On peut donc appliquer le lemme LTE, qui nous donne

$$v_{11}(A) = v_{11}(1990^{1991^2} + 1992) + v_{11}(1991^{1990}).$$

Or, puisque $1990^2 \equiv (-1)^2 \equiv 1 \mod 11^2$, on a que $1990^{2k} \equiv 1 \mod 11^2$ pour tout k. On déduit que $1990^{1991^2} + 1992 \equiv 1990 + 1992 \equiv 11 \mod 11^2$. On a donc $v_{11}(1990^{1991^2} + 1992)$ et $\boxed{v_{11}(A) = 1 + 1990 = 1991}$.

Par un calcul similaire, on trouve que $v_{181}(1990^{1991^2} + 1992) = 1$ et que $\boxed{v_{181}(A) = 1991}$. On déduit que le plus grand entier k est $\boxed{k = 1991}$

Exercice 3.4. (Korea final round 2023) Déterminer tous les entiers n tels que les facteurs premiers de $2^n - 1$ sont inférieurs ou égaux à 7.

Solution 3.4. Si $n \geqslant 1$, le nombre $2^n - 1$ est impair et ses facteurs premiers seront différents de 2.

D'après le théorème de Zsigmondy, sauf exception, si $n \geqslant 5$, le nombre $2^n - 1$ admet un facteur premier ne divisant pas $2^2 - 1, 2^3 - 1$ et $2^4 - 1$, donc un facteur premier différent de $3, 5$ ou 7. L'entier n ne sera alors pas solution.

Comme $2 + 1$ n'est pas une puissance de 2, la seule exception possible au théorème de Zsigmondy est si $n = 6$. Les seules possibilités sont donc $n = 1, 2, 3, 4$ et 6, dont on vérifie qu'ils sont biens solutions.

Exercice 3.5. Soient p et q des nombres premiers impairs distincts. Montrer que $2^{pq} - 1$ admet au moins trois diviseurs premiers distincts.

Solution 3.5. On suppose que $p < q$. Remarquons que $2^p - 1$ et $2^q - 1$ divisent $2^{pq} - 1$, et que le nombre $2^p - 1$ admet un facteur premier a_1.

D'après le théorème de Zsigmondy, sauf exception, le nombre $2^q - 1$ admet un facteur premier a_2 ne divisant pas $2^p - 1$. Toujours d'après le théorème, sauf exception, le nombre $2^{pq} - 1$ admet un facteur premier a_3 ne divisant ni $2^p - 1$ ni $2^q - 1$. Ainsi, a_1, a_2 et a_3 sont des facteurs premiers distincts de $2^{pq} - 1$.

Il reste à vérifier qu'on est bien dans les conditions d'application du théorème de Zsigmondy. Or, $2+1$ n'est pas un carré parfait, et pq et q sont différents de 6, donc les nombres $2^q - 1$ et $2^{pq} - 1$ ne sont pas des exceptions du théorème, ce qui conclut.

Exercice 3.6. (BXMO 2010) Déterminer tous les quadruplets (a, b, p, n) d'entiers strictement positifs tels que p est un nombre premier et

$$a^3 + b^3 = p^n.$$

Solution 3.6. D'après le théorème de Zsigmondy, sauf exception, le nombre $a^3 + b^3$ admet un facteur premier ne divisant pas $a + b$. Or $a + b$ divise $a^3 + b^3$ et $a + b > 1$ admet au moins un facteur premier, donc le nombre $a^3 + b^3$ admet deux facteurs premiers distincts, il ne peut donc pas être une puissance de p.

Il reste donc à traiter les exceptions du théorème de Zsigmondy. La seule exception est si $(a, b) = (2, 1)$ ou $(a, b) = (1, 2)$, qui fournissent respectivement les quadruplets $\boxed{(2, 1, 3, 2) \text{ et } (1, 2, 3, 2)}$.

Exercice 3.7. (BMO 2015 N3) Soit a un entier strictement positif. Pour tout entier n, on pose $a_n = 1 + a + a^2 + \ldots + a^{n-1}$. Soient s et t deux entiers strictement positifs tels que tout diviseur premier p de $s - t$ divise $a - 1$. Montrer que $s - t$ divise $a_s - a_t$.

Solution 3.7. Supposons $s > t$. Notons que

$$a_s - a_t = (1 + a + \ldots + a^{s-1}) - (1 + a + \ldots + a^{t-1}) = a^t + \ldots + a^{s-1} = a^t \cdot \frac{a^{s-t} - 1}{a - 1}.$$

Ainsi,

$$\frac{a_s - a_t}{s - t} = a^t \frac{a^{s-t} - 1}{(s - t)(a - 1)}.$$

Il faut donc montrer que la fraction ci-dessus est entière. Pour cela, on montre que pour tout diviseur p de $(s - t)(a - 1)$, $v_p(a^{s-t} - 1) \geqslant v_p((s - t)(a - 1))$.

Soit p un tel nombre premier. On distingue deux cas.

➢ Si $p \mid s - t$, alors $p \mid a - 1$ et d'après le lemme LTE,

$$v_p(a^{s-t} - 1) = v_p(a - 1) + v_p(s - t) = v_p((s - t)(a - 1)),$$

donc l'inégalité désirée est vraie.

➢ Si $p \mid a-1$ mais p ne divise pas $s-t$, alors le lemme LTE donne

$$v_p(a^{s-t}-1) = v_p(a-1) + v_p(s-t) = v_p(a-1),$$

donc on a également l'inégalité voulue.

Comme on a l'inégalité $v_p(a^{s-t}-1) \geqslant v_p((s-t)(a-1))$ dans tous les cas (on a même égalité), l'entier considéré est bien premier.

Exercice 3.8. *(Thailand Fall Camp 2020)* Pour tout entier $n \geqslant 1$, on note $\rho(n)$ le nombre de diviseurs positifs de n avec exactement les mêmes facteurs premiers que n. Montrer que, pour tout entier m, il existe un entier n tel que $\rho(202^n+1) \geqslant m$.

Solution 3.8.

➢ Commentaire :

> Si A est divisible par une grande puissance d'un premier p, disons $A = p^m B$ avec B premier avec p, alors les m nombres $p^\ell B$ avec $1 \leqslant \ell \leqslant m$ ont les mêmes diviseurs premiers que A. Il suffit donc de choisir n tel que 202^n+1 soit divisible par une grande puissance de nombre premier.

Notons que $202+1 = 7 \times 29$. Posons $n = 7^{m-1}$. D'après le lemme LTE,

$$v_7(202^n+1) = v_7(202+1) + v_7(n) = 1 + m - 1 = m.$$

On peut donc écrire $202^n + 1 = 7^m \cdot B$ avec B premier avec 7. Alors les nombres $7^\ell \cdot B$ avec $\ell \leqslant m$ sont des diviseurs de 202^n+1 avec les mêmes facteurs premiers que 202^n+1. On a donc bien $\rho(202^n+1) \geqslant m$.

Exercice 3.9. *(BXMO 2024)* Pour tout entier $n \geqslant 1$, on note $\mathrm{rad}(n)$ le produit des facteurs premiers distincts de n. Par exemple, $\mathrm{rad}(20) = \mathrm{rad}(2^2 \cdot 5) = 2 \cdot 5 = 10$. Montrer qu'il existe des entiers $a, b > 1$ tels que $\mathrm{PGCD}(a,b) = 1$ et

$$\mathrm{rad}(ab(a+b)) < \frac{a+b}{2024^{2024}}.$$

Solution 3.9.

➢ Commentaire :

> Le cahier des charges implicite sur a et b est qu'ils doivent tous les deux avoir peu de facteurs premiers, et que $a+b$ doit être grand tout en ayant peu de facteurs premiers distincts, afin que $\mathrm{rad}(a+b)$ soit très petit devant $a+b$. Plutôt que de contrôler $v_p(a+b)$ pour tout premier p, on peut se concentrer uniquement sur un facteur premier : si $a+b = p^k A$ avec p premier et k arbitrairement grand, alors $\mathrm{rad}(a+b) \leqslant pA$, donc $\dfrac{a+b}{\mathrm{rad}(a+b)}$ est arbitrairement petit. Le lemme LTE nous permet de connaître précisément $v_p(x^k+y^k)$, il est donc raisonnable de chercher a et b sous la forme $(a,b) = (x^k, y^k)$, avec par exemple x et y premiers pour que $\mathrm{rad}(ab) = xy$.

Soit $k \geqslant 1$ un entier que l'on peut choisir plus tard (voir condition en rouge). Posons $a = 2^{5^k}$ et $b = 3^{5^k}$. On voit que a et b sont premiers entre eux, et d'après le lemme LTE,

$$v_5(a+b) = v_5(2^{5^k} + 3^{5^k}) = v_5(2+3) + v_5(5^k) = 1 + k.$$

On peut donc écrire $a+b = 5^{k+1}A$, où A est premier avec 5. Comme a et b sont premiers entre eux, ils sont premiers avec $a+b$, et on a $\mathrm{rad}(ab(a+b)) = 2 \times 3 \times \mathrm{rad}(a+b) \leqslant 6 \times 5 \times A$. D'autre part,

$$\frac{a+b}{2024^{2024}} = \frac{5^{k+1}A}{2024^{2024}} = \frac{5^k}{2024^{2024}} \cdot 5A.$$

En prenant k tel que $\dfrac{5^k}{2024^{2024}} > 30$, on trouve bien que $\dfrac{a+b}{2024^{2024}} > \mathrm{rad}(ab(a+b))$.

Exercice 3.10. (Test de sélection français 2016-2017) Prouver qu'il existe un entier $n > 0$ tel que, parmi les 2016 chiffres de droite dans l'écriture décimale de 2^n, il y a au moins 1008 chiffres 9.

Solution 3.10.

➢ **Commentaire :**

> S'il y a beaucoup de 9 à droite de l'écriture décimale de n (et qu'ils sont consécutifs), c'est que 2^n n'est pas loin d'un entier divisible par une grande puissance de 10. Par exemple, si les 9 étaient tout à droite de l'écriture de 2^n, cela voudrait dire que 10^{1008} divise 2^n+1. Bien sûr, cela n'est jamais possible puisque l'un est pair et l'autre est impair, mais on peut répliquer l'idée avec non pas 2^n+1 mais 2^n+2^{2016}. Ceci nous inspire la démarche suivante : on va chercher $n \geqslant 2016$ tel que $5^{2016} \mid 2^n + 2^{2016}$. On aura alors $10^{2016} \mid 2^n + 2^{2016}$.

Posons $K = 2016$. D'après le lemme LTE,

$$v_5(2^{2\cdot 5^{K-1}} + 1) = v_5(2^2+1) + v_5(5^{K-1}) = 1 + K - 1 = K.$$

Ainsi, le nombre $2^{2\cdot 5^{K-1}+K} + 2^K$ est divisible par 2^K et 5^K, il est donc divisible par 10^K. On note $2^{2\cdot 5^{K-1}+K} + 2^K = A \cdot 10^K$ et $n = 2 \cdot 5^{K-1} + K$. Alors $2^n = A10^K - 2^K$. Comme $2^K < 10^{K/2}$, le nombre 2^K ne possède pas plus de 1008 chiffres. Ainsi, parmi les 2016 derniers chiffres de 2^n, au moins 1008 d'entre eux sont des 9.

Exercice 3.11. Déterminer tous les entiers strictement positifs a et b supérieurs ou égaux à 1 tels que $b^a \mid a^b - 1$.

Solution 3.11. **Réponse :** Les seuls couples sont les $(1, a)$ et $(2, 3)$.

Si $b = 1$, alors $b^a \mid a^b - 1$ pour tout a, donc tout couple $\boxed{(1,a) \text{ est solution}}$. On suppose dans la suite que $b > 1$.

On réplique le raisonnement de l'exemple du cours. Commençons par supposer que b n'est pas une puissance de 2 et notons p son plus petit diviseur premier impair. Alors $p \mid a^b - 1$, donc $a^b \equiv 1 \mod p$. a étant manifestement premier avec p, on peut noter ω son ordre modulo p. Par hypothèse, $\omega \mid b$ et par le petit théorème de Fermat, $\omega \mid p - 1$. Donc $\omega \mid \text{PGCD}(b, p-1)$. Par minimalité de p, on déduit que $\omega = 1$ et $\boxed{p \mid a - 1}$.

En vue d'appliquer le lemme LTE, on distingue deux cas :

➢ Cas 1 : p est impair. Dans ce cas, d'après le lemme LTE et l'hypothèse de l'énoncé,

$$av_p(b) \leqslant v_p(a^b - 1) = v_p(a-1) + v_p(b) \Longrightarrow (a-1)v_p(b) \leqslant v_p(a-1).$$

En notant $\alpha = v_p(a-1)$, on déduit que $\alpha \geqslant v_p(b)(a-1) \geqslant p^\alpha \geqslant 3^\alpha$. Une récurrence sur α montre que l'inégalité inverse est toujours vérifiée pour $\alpha \geqslant 1$. Il n'y a donc $\boxed{\text{pas de solutions}}$ dans ce cas.

➢ Cas 2 : $p = 2$. D'après le lemme LTE et l'hypothèse de l'énoncé,

$$av_2(b) \leqslant v_2(a^b - 1) = v_2(a-1) + v_2(a+1) + v_2(b) - 1.$$

Comme soit $v_2(a-1) = 1$ soit $v_2(a+1) = 1$, on a deux cas à vérifier.

Si $v_2(a+1) = 1$, on trouve que $(a-1)v_2(b) \leqslant v_2(a-1)$. En posant $\alpha = v_2(a-1)$, on trouve que $\alpha \geqslant v_2(b)2^\alpha \geqslant 2^\alpha$. Là encore, une récurrence montre qu'on a toujours $2^\alpha > \alpha$ pour tout $\alpha > 0$. Il n'y a donc $\boxed{\text{pas de solutions}}$ dans ce cas.

Si $v_2(a-1) = 1$, on trouve cette fois-ci que $(a-1)v_2(b) \leqslant v_2(a+1)$. Comme $a+1$ est pair et que $v_2(a-1) = 1$, on déduit que $4 \mid a+1$. Notons $a + 1 = 2^k B$ avec B impair et $k \geqslant 2$. L'inégalité donne

$$k \geqslant (2^k B - 2)v_2(b) \geqslant 2^k B - 2 \geqslant 2^k - 2.$$

Or, par récurrence à nouveau, on a $2^k > k + 2$ dès que $k \geqslant 3$. On déduit que $k = 2$. En réinjectant dans l'inégalité ci-dessus, on trouve que $4B \leqslant 4$, donc $B = 1$, ce qui donne $\boxed{a = 3}$. En revenant à l'inégalité de départ, on trouve $v_2(b) = 1$. On pose $b = 2b'$. La divisibilité implique $b'^3 \mid 9^{b'} - 1$.

On réitère le raisonnement sur le plus petit facteur premier : on note p le plus petit diviseur premier de b', qui sera bien impair. On retombe alors dans le cas 1, qui permet de déduire que $b' = 1$, soit $\boxed{b = 2}$. Réciproquement, comme $2^3 \mid 3^2 - 1$, le couple $\boxed{(3,2) \text{ est bien solution}}$.

Exercice 3.12. (IMO 1999 P4) Déterminer tous les couples d'entiers (n,p) avec p premier et $0 < n \leqslant 2p$ tels que

$$n^{p-1} \mid (p-1)^n + 1.$$

Solution 3.12. **Réponse :** Il s'agit des couples $(1,p)$ avec p premier, $(2,2)$ et $(3,3)$.

Soit (n,p) un couple solution. Le plus naturel (mais peut-être pas le plus efficace a posteriori) est d'effectuer directement l'argument classique du plus petit facteur premier (à noter que cet argument n'était probablement pas classique en 1999).

Si $n = 1$, alors tout nombre premier p est solution, on obtient $\boxed{\text{les couples } (1,p)}$, qui sont bien solutions. On suppose dans la suite que $n > 1$.

Soit q le plus petit diviseur premier de n. Alors $(p-1)^n \equiv -1 \mod q$, donc q est premier avec $p-1$, dont on note alors ω l'ordre modulo q. On a donc $(p-1)^{2n} \equiv 1 \mod q$ par hypothèse et $(p-1)^{q-1} \equiv 1 \mod q$ par le petit théorème de Fermat. On déduit que $\omega \mid \text{PGCD}(2n, q-1)$. Comme $q-1$ est premier avec n (il est strictement inférieur à q le plus petit diviseur premier de n), $\text{PGCD}(2n, q-1) \leqslant 2$, donc $\omega \in \{1,2\}$. On distingue donc deux cas :

- ➢ Si $\omega = 1$, alors $q \mid (p-1) - 1$, donc $1 \equiv (p-1)^n \equiv -1 \mod q$, ce qui conduit à $q \mid 2$ et $q = 2$. Mais alors $2 \mid (p-1)^n + 1$, donc $p-1$ est impair et $p = 2$. Donc $2 \mid n \mid 1+1 = 2$ et $n = 2$. Réciproquement, $\boxed{(2,2) \text{ est bien solution}}$.
- ➢ Si $\omega = 2$, cela veut dire que $q \mid (p-1)^2 - 1$ mais pas $(p-1) - 1$, donc $q \mid (p-1) + 1 = p$ et $q = p$. Si $p = 2$, on revient au cas précédent, on peut donc supposer que $p \neq 2$. Comme $n \leqslant 2p$ est un multiple de p, on a $n = p$ ou $n = 2p$. Mais si $n = 2p$, alors $q = 2$ donc $p = 2$, ce qui nous ramène au cas plus haut. On a donc $n = p$. D'après le lemme LTE, on a alors, puisque $p^{p-1} \mid (p-1)^p + 1$

$$p - 1 \leqslant v_p((p-1)^p + 1) = v_p((p-1)+1) + v_p(p) = 2,$$

donc $p \leqslant 3$ et $n = p = 3$. Réciproquement, $\boxed{\text{le couple } (3,3) \text{ est bien solution}}$ car $3^2 \mid 2^3 + 1$.

Exercice 3.13. (USA TSTST 2018 P8) Déterminer tous les entiers $b > 2$ tels qu'il existe une infinité d'entiers $n \geqslant 1$ tels que $n^2 \mid b^n + 1$.

Solution 3.13. **Réponse :** Les entiers b tels que $b+1$ n'est pas une puissance de 2.

➢ Commentaire :

> L'énoncé ressemble à l'exemple du cours. On commence donc par refaire le même argument que cet exemple, ce qui consiste en le raisonnement standard sur l'ordre modulo le plus petit diviseur de n (voir la sous-section "l'astuce du plus petit facteur premier"). Ceci conduit à l'étape 1.

Soit b un entier solution.

Étape 1 : Montrons que $b+1$ admet un facteur premier impair, c'est-à-dire que $b+1$ n'est pas une puissance de 2.

Puisque b est solution, on peut choisir un entier $n > 1$ un entier tel que $n^2 \mid b^n + 1$. Prenons p le plus petit facteur premier de n.

- ➢ Si $p = 2$, alors $4 \mid n^2 \mid b^n + 1$, ce qui implique que $b^n + 1$ est pair, donc b est impair. Mais alors $b^n + 1 \equiv (b^{n/2})^2 + 1 \equiv 2 \mod 4$, ce qui est absurde.
- ➢ Sinon, puisque $p \mid b^n + 1$, b est premier avec p et on peut noter ω son ordre modulo p. Alors $b^{2n} \equiv 1 \mod p$, donc $\omega \mid \text{PGCD}(2n, p-1) = 2\text{PGCD}(n, (p-1)/2)$. Par minimalité de p, ce PGCD vaut 1, donc $\omega \in \{1,2\}$. Mais si $\omega = 1$, alors $b \equiv 1$ donc $b^n + 1 \equiv 2 \neq 0 \mod p$, on a donc $\omega = 2$, soit $p \mid b^2 - 1 = (b-1)(b+1)$, et comme p ne divise âs $b-1$, $p \mid b+1$. Ainsi, $\boxed{b+1 \text{ admet un facteur premier impair}}$, et n'est donc pas une puissance de 2.

$\boxed{\text{Remarque :}}$ On a en fait montré que si $b+1$ est une puissance de 2, le seul entier n tel que $n \mid b^n + 1$ est $n = 1$.

Étape 2 : Si $b+1$ n'est pas une puissance de 2, alors on construit par récurrence une infinité d'entiers n tels que $n^2 \mid b^n + 1$.

➢ Commentaire :

> L'heuristique de la construction est de supposer avoir construit un entier n solution et d'en construire une nouvelle sous la forme np, où p est un facteur premier primitif de b^n+1. La mise en oeuvre de cette idée conduit à la formulation plus précise qui suit.

On construit par récurrence une suite (p_n) de nombres premiers duex à deux distincts telle que, si on note $m_n = p_1 \dots p_n$:
- $m_n^2 \mid b^{m_n}+1$ pour tout indice $n \geqslant 1$,
- $p_{n+1} \mid b^{m_n}+1$ mais p_{n+1} ne divise pas b^k+1 pour $k \leqslant m_n$.

La construction d'une telle suite (p_n) implique que la suite (m_n) est une suite infinie d'entiers vérifiant la divisibilité de l'énoncé.

Initialisation : On a vu dans l'étape 1 que tout entier n solution doit avoir son plus petit facteur premier p qui divise $b+1$. Réciproquement, soit p un diviseur premier impair de $b+1$. Alors d'après le lemme LTE,

$$v_p(b^p+1) = v_p(b+1) + v_p(p) = 2,$$

donc $p^2 \mid b^p+1$, donc $p_1 = p$ convient.

Hérédité : On suppose avoir construit $p_1, \dots, p_r$ les premiers termes de la suite. D'après le théorème de Zsigmondy, le nombre $b^{m_r}+1$ admet un facteur premier primitif q. Comme q ne divise aucun des $b^{m_i}+1$ avec $i \leqslant r-1$, q est distinct de $p_1, \dots, p_r$ (et q est également impair car il ne divise pas $b+1$ qui est de la même parité que $b^{m_r}+1$). On a alors la première divisibilité

$$m_r^2 \mid b^{m_r}+1 \mid b^{m_r q}+1.$$

D'autre part, d'après le lemme LTE,

$$v_q(b^{m_r q}+1) = v_q(b^{m_r}+1) + v_q(q) \geqslant 2,$$

donc $\boxed{q^2 \mid b^{m_r q}+1}$. Ainsi $p_{r+1} = q$ satisfait les conditions énoncées, ce qui achève la récurrence.

Exercice 3.14. *(RMM 2012 P4)* Montrer qu'il existe une infinité d'entiers n tels que n divise $2^{2^n+1}+1$ est mais n ne divise pas 2^n+1.

Solution 3.14. Par audace ou par soucis de simplification (ce qui va souvent de paire dans les problèmes de construction), on cherche n avec peu de facteurs premiers. Dans le but d'appliquer le lemme LTE, on peut commencer par prendre $n = 3^\ell$. D'après ce lemme,

$$v_3(2^{3^\ell}+1) = v_3(2+1) + v_3(3^\ell) = \ell+1.$$

On déduit que $3^\ell \mid n$. Puisque $2^a+1 \mid 2^b+1$ dès que $a \mid b$ et b/a est impair, que

$$3^\ell \mid 2^{3^\ell}+1 \mid 2^n+1.$$

On applique alors le théorème de Zsigmondy : d'après celui-ci, pour $\ell \geqslant 2$, le nombre $2^{2^n+1}+1$ admet un facteur premier primitif p (en particulier $p \neq 2, 3$). Posons $N = p3^\ell = pn$. Le reste est un jeu avec le fait que si $a \mid b$ et b/a est impair, alors $2^a+1 \mid 2^b+1$. Alors

$$n \mid 2^n+1 \mid 2^{np}+1 = 2^N+1, \quad \Longrightarrow 2^n+1 \,||\, 2^{2^{np}+1}+1, \quad \Longrightarrow n \mid 2^n+1 \mid 2^{2^N+1}+1.$$

et

$$p \mid 2^{2^n+1}+1 \mid 2^{2^N+1}+1,$$

donc $N \mid 2^{2^N+1}+1$. D'autre part, p ne divise par 2^N+1, puisque d'après le petit théorème de Fermat,

$$2^N+1 \equiv 2^n+1 \mod pn,$$

et p ne divise pas 2^n+1 par construction de p. On déduit que N ne divise pas 2^N+1.

Comme l'entier construit est valuation $3-$adique exactement ℓ, en faisant varier ℓ, on obtient une suite de solutions deux à deux distinctes.

Solution alternative

La solution suivante est très astucieuse et n'utilise pas le théorème de Zsigmondy. Elle montre que si n vérifie la propriété de l'énoncé, alors 2^n+1 aussi. Ainsi, à partir d'un entier n_0 solution, on obtient une infinité de solutions par récurrence immédiate. Cette solution utilise de façon cruciale que si $2^a+1 \mid 2^b+1$, alors $a \mid b$.

Soit n un entier solution. Posons $N = 2^n+1$. On a donc que $n \mid 2^N+1$ mais n ne divise pas N. Comme 2^n+1 est impair,

$$n \mid 2^{2^n+1}+1 \Longrightarrow N = 2^n+1 \mid 2^{2^{2^n+1}+1}+1 = 2^{2^N+1}+1.$$

D'autre part, comme n ne divise pas N, 2^n+1 ne divise pas 2^N+1, donc N ne divise pas 2^n+1. Ceci montre que N est solution du problème.

Il reste à initialiser et trouver n_0 - ce qui est très difficile. Il est raisonnable de chercher n_0 comme un nombre premier, ou comme le produit de deux nombres premiers. Une telle recherche peut conduire aux idées de la solution 1, c'est-à-dire de prendre $n = 3p$, avec p un diviseur premier primitif de $2^{2^3+1}+1$, à savoir $p = 19$. Cette propriété de 19 et un caclul donnent que $n_0 = 57$ est solution.

Exercice 3.15. (IMO SL 2014 N4) Soit $n > 1$ un entier. Montrer que parmi les termes de la suite $(a_k)_{k\geqslant 1}$ définie par

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$

il y en a une infinité qui sont impairs.

Solution 3.15. Notons que si n est impair, alors l'entier $k = n^\ell$ vérifie

$$a_{n^\ell} = \left\lfloor \frac{n^{n^\ell}}{n^\ell} \right\rfloor = n^{n^\ell - \ell},$$

qui est impair pour tout entier $\ell \geqslant 1$. La difficulté de l'exercice se trouve donc dans le cas où n est pair, ce que l'on suppose dans la suite.

La première observation est que, puisque $\dfrac{n^k}{k} \geqslant a_k > \dfrac{n^k-k}{k}$, il existe un entier $0 \leqslant r < k$ tel que $a_k = \dfrac{n^k-r}{k}$. Par audace ou par soucis de simplification (qui vont régulièrement de paire dans les problèmes de construction), on peut chercher k tel que $k \mid n^k - 1$.

Le théorème de Zsigmondy permet de construire une suite infinie de tels entiers k, comme dans l'exercice 3.1.1. On propose une construction alternative.

➢ **Commentaire :**

> Une fois l'idée de choisir k sous la forme pn^ℓ (c'est un multiple simple de n qui permet de simplifier la fraction), la fraction devient
>
> $$a_k = \left\lfloor \frac{n^{pn^\ell}}{pn^\ell} \right\rfloor = \left\lfloor \frac{n^{pn^\ell-\ell}}{p} \right\rfloor.$$
>
> Afin que ce nombre vaille $\dfrac{n^{pn^\ell-\ell}-1}{p}$, il faut un certain cahier des charges sur p et ℓ. Notons ω l'ordre de n modulo p. Alors $\omega \mid p-1$ par le petit théorème de Fermat, donc $pn^\ell - \ell \equiv n^\ell - \ell \mod \omega$. Pour que $p \mid n^{pn^\ell-\ell}-1$, il faut que cette congruence soit nulle. Lorsque ω est premier, construire des entiers ℓ tels que $\omega \mid n^\ell - \ell$ correspond à l'exercice 2.5. Le théorème de Zsigmondy permet alors de trouver p tel que ω est premier (cf astuce du cours).

Soit q un nombre premier impair et p un facteur premier primitif de n^q-1, qui existe d'après le théorème de Zsigmondy (on n'est pas dans les exceptions du théorème car $q \neq 6$ et n'est pas une puissance de 2). Alors q est exactement l'ordre de n modulo p, ce qui donne en particulier que $q \mid p-1$. Soit ℓ un entier solution du système suivant :

$$\begin{cases} \ell \equiv 1 \mod q \\ \ell \equiv 0 \mod q-1 \end{cases}$$

Prenons $k = pn^\ell$. Alors

$$a_k = \left\lfloor \frac{n^{pn^\ell}}{pn^\ell} \right\rfloor = \left\lfloor \frac{n^{pn^\ell - \ell}}{p} \right\rfloor.$$

Notons qu'alors $pn^\ell - \ell \equiv n^\ell - \ell \equiv 1 - 1 \equiv 0 \mod q$, de sorte que $n^{pn^\ell - \ell} - 1 \equiv 0 \mod p$. On a donc

$$a_k = \left\lfloor \frac{n^{pn^\ell - \ell}}{p} \right\rfloor = \frac{n^{pn^\ell - \ell} - 1}{p},$$

qui est bien impair. Comme le système ci-dessus admet une infinité de solutions (qui génèrent des indices k deux à deux distincts), on a bien une infinité d'entiers k impairs.

Solution alternative

On présent une construction alternative pour le cas n pair, à l'aide du lemme LTE, en supposant d'abord que $n > 2$.

Soit p un diviseur premier de $n - 1$ (en notant que p est nécessairement impair). D'après le lemme LTE, pour tout entier ℓ,

$$v_p(n^{p^\ell} - 1) = v_p(n - 1) + v_p(p^\ell) = \ell + 1.$$

On déduit que le nombre $\dfrac{n^{p^\ell} - 1}{p^\ell}$ est un entier, de sorte qu'en prenant $k = p^\ell$,

$$a_{p^\ell} = \left\lfloor \frac{n^{p^\ell}}{p^\ell} \right\rfloor = \frac{n^{p^\ell} - 1}{p^\ell},$$

est bien impair. On a donc obtenu une suite d'indices pour lesquelles le terme associé est impair.

Dans le cas où $n = 2$, qui n'est pas si simple, plusieurs constructions sont possibles. On pourra par exemple prendre $k = 2 \cdot 3^{2\ell}$, et observer que, d'après le théorème d'Euler,

$$3^{2\ell} \mid 2^{2 \cdot 3^{2\ell}} - 1 - 3^{2\ell},$$

puis que le nombre $2^{2 \cdot 3^{2\ell}} - 1 - 3^{2\ell}$ est divisible par $2 \cdot 3^{2\ell}$ mais pas par 4, ce qui implique que le nombre

$$\left\lfloor \frac{2^{2 \cdot 3^{2\ell}}}{2 \cdot 3^{2\ell}} \right\rfloor = \frac{2^{2 \cdot 3^{2\ell}} - 1 - 3^{2\ell}}{2 \cdot 3^{2\ell}}$$

est impair.

Exercice 3.16. On note $\sigma(n)$ la somme de tous les diviseurs premiers distincts de l'entier n. Déterminer tous les entiers $n \geqslant 1$ tels que

$$\sigma(2^n + 1) = \sigma(n).$$

Solution 3.16. **Réponse :** Le seul entier est $n = 3$, dont on vérifie qu'il fonctionne.

Soit $n \geqslant 1$ un entier et $n = 2^\alpha \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers, où les p_i sont impairs. On a donc $\sigma(n) \leqslant 2 + p_1 + \ldots + p_r$.

Pour tout i, d'après le théorème de Zsigmondy, sauf exception, le nombre $2^{2^\alpha p_i} + 1$ admet un facteur premier primitif q_i (qui est nécessairement impair). L'exception se produit seulement si $2^\alpha p_i = 3$, (soit $(\alpha, p_i) = (0, 3)$) auquel cas on choisit $q_i = 3$. L'ensemble $\{q_1, \ldots, q_r\}$ est alors un ensemble de r nombres premiers deux à deux distincts (même dans le cas de l'exception), qui vérifient $q_i \mid 2^{2^\alpha p_i} + 1 \mid 2^n + 1$. On a donc $\sigma(2^n + 1) \geqslant q_1 + \ldots + q_r$. Il reste alors à estimer les q_i.

Pour cela, on a le lemme suivant :

Lemme 1. *Soit $N \neq 3$ un entier et q un facteur premier primitif de $2^N + 1$. Alors $q > 2N$.*

Démonstration. On note ω l'ordre de 2 modulo q. Comme $q \mid 2^N + 1 \mid 2^{2N} - 1$, $\omega \mid 2N$. On écrit $N = 2^x \beta$ avec β impair. Si ω est impair, alors $\omega \mid \beta$ donc $2^\beta \equiv 1 \mod q$, donc $2^N + 1 \equiv 1 + 1 \mod q$, ce qui est exclu. Sinon, ω est pair, et on a la factorisation $0 \equiv 2^\omega - 1 = (2^{\omega/2} - 1)(2^{\omega/2} + 1) \mod q$. Par minimalité de ω, le premier facteur est non nul modulo q. Donc $q \mid 2^{\omega/2} + 1$, et par minimalité de q, on déduit que $\omega/2 = N$, soit $\omega = 2N$. D'après le petit théorème de Fermat, $\omega \mid q - 1$, donc $q \geqslant 2N + 1$, soit $\boxed{q > 2N}$. □

On distingue alors plusieurs cas.

- ➢ Si n est impair et admet un facteur premier, disons p_1, différent de 3, alors on a d'après le lemme que $q_1 > 2p_1 \geqslant p_1 + 2$. Pour tout autre facteur premier p_i, on a $q_i = p_i$ si $p_i = 3$ ou $q_i > 2p_i > p_i$ d'après le lemme, si bien que

$$\sigma(2^n + 1) \geqslant q_1 + \ldots + q_r > p_1 + \ldots + p_r \geqslant \sigma(n).$$

- ➢ Si n est pair et admet au moins un facteur premier impair p_1, alors d'après le lemme, $q_1 > 2^{\alpha+1} p_1 > p_1 + 2$ et de même, $q_i \geqslant p_i$ pour tout autre facteur p_i. On a à nouveau

$$\sigma(2^n + 1) \geqslant q_1 + \ldots + q_r > p_1 + \ldots + p_r + 2 = \sigma(n).$$

- ➢ Si n est une puissance de 2, alors le nombre $2^n + 1$ admet un facteur premier primitif q, qui d'après le lemme vérifie $q > 2n$. On a donc encore $\sigma(2^n + 1) \geqslant q > 2 = \sigma(n)$.
- ➢ Si n est une puissance de 3, alors soit $n = 3$, qui est bien solution, soit $n \geqslant 9$, auquel cas $2^n + 1$ admet un facteur premier primitif $q \neq 3$, et là encore $\sigma(2^n + 1) \geqslant q > 3 = \sigma(n)$

La seule solution est donc bien $n = 3$.

Exercice 3.17. (BMO 2022 P2) Soient a, b et n des entiers strictement positifs tels que $a > b$ et

- a^{2021} divise n,
- b^{2021} divise n,
- 2022 divise $a - b$.

Montrer que n admet des diviseurs positifs, deux à deux distincts, dont la somme est divisible par 2022 mais pas par 2022^2.

Solution 3.17.

➢ Commentaire :

> L'énoncé donne beaucoup de diviseurs pour n parmi les diviseurs de a^{2021} et b^{2021}, c'est parmi ces diviseurs qu'il faut chercher l'ensemble T. Dans le cas où a et b sont premiers entre eux (une première simplification qu'on peut se donner en début de problème), on a des diviseurs de n de la forme $a^i b^j$. Il reste à choisir de tels nombres dont la somme se calcule facilement. On peut essayer de prendre tous les $a^i b^j$ à i fixé mais ce ne sera pas toujours un diviseur de n. On peut également essayer de prendre tous les $a^i b^j$ avec $i + j = 2021$, ce qui permet d'utiliser pleinement les hypothèses. Ce qui suit est la mise en oeuvre technique de cette dernière idée.

Gardons en tête la décomposition en facteurs premiers $2022 = 2 \times 3 \times 337$. Montrons d'abord que pour tout $k \geqslant 1$, $a^k b^{2021-k}$ est un diviseur de n.

En effet, si p est un diviseur premier de n, on a $2021 v_p(a), 2021 v_p(b) \leqslant v_p(n)$. On a donc pour tout $0 \leqslant k \leqslant 2021$,

$$v_p(n) \geqslant 2021 \max(v_p(a), v_p(b)) = k \max(v_p(a), v_p(b)) + (2021 - k) \max(v_p(a), v_p(b)) \geqslant k v_p(a) + (2021 - k) v_p(b),$$

ce qui implique que $\boxed{a^k b^{2021-k} \mid n}$.

Posons alors $T = \{b^{2021}, ab^{2020}, \ldots, a^{2020}b, a^{2021}\} = \{a^k b^{2021-k}, k = 0, 1, \ldots, 2021\}$. La somme S des éléments de T est une somme géométrique qui vaut

$$S = b^{2021} + ab^{2020} + \ldots + a^{2020}b + a^{2021} = \frac{a^{2022} - b^{2022}}{a - b}.$$

Comme $b \equiv a \mod 2022$, la première écriture de S donne $S \equiv 2022 a^{2022} \equiv 0 \mod 2022$, donc T remplit la première condition. Pour montrer que 2022^2 ne divise pas S, il suffit de montrer que l'un des nombrs $2^2, 3^2$ ou 337^2 ne divise pas S. Le lemme LTE (pour 3 et 337) est tout indiqué pour calculer $v_p(S)$, encore faut-il que a et b remplissent les conditions du lemme : il faut pour cela écarter le cas où a et b sont divisibles par 3 et 337. Ceci nous amène à la disjonction de cas suivante :

- Si 3 ne divise pas a (alors 3 ne divise pas b) : alors $3 \mid a - b$, on peut donc appliquer le lemme LTE qui indique que
$$v_3(S) = v_3(a^{2022} - b^{2022}) - v_3(a - b) = v_3(2022) = 1,$$
ce qui conclut que 2022^2 ne divise pas S.
- Si 337 ne divise pas a, on obtient de la même façon que 337^2 ne divise pas S.
- Si $3 \times 337 = 1011$ divise a ou b, disons a, alors $1011^{2021} \mid n$, donc on peut choisir $T = \{1011, 1011^2\}$, dont la somme des éléments est divisible par $2, 1011$ mais pas par 1011^2, ce qui justifie que T vérifie la propriété.

Exercice 3.18. *(Iran TST 2022)* Un ensemble $S \subset \mathbb{N}^\star$ est dit *magique* si pour tout choix de trois entiers a, b, c distincts, tous les diviseurs strictement positifs de $\dfrac{a^c - b^c}{a-b}$ sont dans S. Pour tout entier $n > 1$, montrer qu'il existe un ensemble magique ne contenant pas n.

Solution 3.18.

➢ **Commentaire :**

> Une fois de plus, on se simplifie la tâche en travaillant avec des nombres premiers : on fixe p un diviseur premier de n et on construit un ensemble S ne contenant aucun élément divisible par p, la difficulté étant de s'assurer qu'aucune fraction $\dfrac{a^c - b^c}{a-b}$ n'est divisible par p. Pour cela, il faut vérifier que $v_p(a^c - b^c) = v_p(a-b)$ lorsque $p \mid a - b$.
>
> La propriété de stabilité $\dfrac{a^c - b^c}{a-b}$ n'est pas divisible par p n'est pas vraie si on se contente de choisir S comme l'ensemble des entiers premiers avec p. Si toutefois on essayait de travailler avec cet ensemble, une étape du raisonnement (étape en rouge) ferait apparaître la condition supplémentaire permettant de deviner l'ensemble S solution : il faut qu'aucun élément de S ne soit divisible par un diviseur de $p-1$.

Soit p un diviseur premier de n et S l'ensemble des entiers dont les facteurs premiers sont **strictement supérieurs** à p. On a que n n'est pas dans S, et il faut montrer que S vérifie la condition du problème.

Soient $a, b, c \in S$ et q un diviseur premier de $\dfrac{a^c - b^c}{a-b}$, et on suppose par l'absurde que $q \leqslant p$. Comme a, b et c sont impairs, la factorisation de $a^c - b^c$ par $a - b$ garantit que $\dfrac{a^c - b^c}{a-b}$ est impair, donc $q \neq 2$. Par hypothèse, $q \mid a^c - b^c$ mais q ne divise pas a et b. La congruence $a^c \equiv b^c \mod q$ devient $(ab^{-1})^c \equiv 1 \mod q$. Ainsi, $\omega_q(ab^{-1}) \mid c$, et d'après le petit théorème de Fermat, $\omega_q(ab^{-1}) \mid q-1$. Or, tous les diviseurs premiers de c sont supérieurs à q, donc $\mathrm{PGCD}(c, q-1) = 1$. On déduit que $\omega_q(ab^{-1}) = 1$, ce qui veut dire que $a \equiv b \mod q$, c'est-à-dire $\boxed{q \mid a - b}$. D'après le lemme LTE, on a alors si q est impair,

$$v_q\left(\frac{a^c - b^c}{a-b}\right) = v_q(a^c - b^c) - v_q(a-b) = v_q(c) = 0,$$

ce qui contredit que q divise $\dfrac{a^c - b^c}{a-b}$. Cette contradiction implique que S vérifie bien la condition de l'énoncé, ce qui conclut.

Exercice 3.19. (France TST 2016-2017) Déterminer tous les entiers $a > 0$ pour lesquels il existe des entiers strictement positifs $r, s, m_1, \ldots, m_r, k_1, \ldots, k_s$ tels que

$$(a^{m_1} - 1) \ldots (a^{m_r} - 1) = (a^{k_1} + 1) \ldots (a^{k_s} + 1).$$

Solution 3.19. **Réponse :** Les entiers solutions sont $a = 2$ et $a = 3$.

Soit a un entier solution et soient $r, s, m_1, \ldots, m_r, k_1, \ldots, k_s$ des entiers vérifiant l'équation tels que s soit minimal pour cette propriété.
On commence par constater que $a - 1$ est une puissance de 2. En effet, si p est un diviseur premier de $a - 1$, l'équation modulo p donne $0 \equiv 2^s \mod p$, ce qui implique que $p = 2$. On note $\boxed{a = 2^A + 1}$.

Si $A = 0$, alors $a = 2$ est bien solution (on a par exemple $2^2 - 1 = 2^1 + 1$). Si $A = 1$, $a = 3$ qui est également solution, car $(3 - 1)(3 - 1) = 3 + 1$. On suppose par la suite que $A \geqslant 2$.

On suppose $k_1 \leqslant \ldots \leqslant k_s$ et on choisit q un facteur premier primitif de $a^{k_s} + 1$, ce qui existe d'après le théorème de Zsigmondy. Notons que comme a est impair, on n'est pas dans l'exception du théorème. De plus, $a + 1 = 2^A + 2$ est pair mais n'est pas une puissance de 2, donc on peut choisir $q \neq 2$. Notons ω l'ordre de a modulo q. Comme $a^{k_s} \equiv -1 \mod q$, on a $\omega \mid 2k_s$. On montre qu'on a mieux et que $\omega = 2k_s$.

- ➢ Si ω est impair, alors $\omega \mid k_s$, donc $a^{k_s} \equiv 1 \mod q$, ce qui est absurde car $a^{k_s} \equiv -1 \mod q$, et q est différent de 2.
- ➢ Ainsi, ω est pair, on peut écrire $\omega = 2\ell$, avec $\ell \mid k_s$. On a alors $(a^\ell + 1)(a^\ell - 1) \equiv 0 \mod q$. Or $a^\ell \neq 1 \mod q$ (par minimalité de 2ℓ), donc $q \mid a^\ell + 1$. Puisque q est primitif, cela force $\ell = k_s$ et $\boxed{\omega = 2k_s}$.

Comme q divise $(a^{m_1} - 1) \ldots (a^{m_r} - 1)$, q divise l'un des facteurs, disons $q \mid a^{m_r} - 1$. Ceci force $2k_s \mid m_r$. Supposons maintenant que $m_r > 2k_s$. D'après le théorème de Zsigmondy, sauf exception, le nombre $a^{m_r} - 1$ admet un facteur premier primitif q'. q' divise donc un des termes du membre de droite, disons $q' \mid a^{k_i} + 1$ avec $k_i \leqslant k_r$. Mais alors $q' \mid a^{2k_i} - 1$, ce qui contredit le fait que q' est primitif, puisque $2k_i \leqslant 2k_s < m_r$. On a donc deux conclusions possibles :

- ➢ Soit $m_r = 2k_s$, on peut alors simplifier l'équation par $a^{k_s} + 1$ car $a^{m_r} - 1 = (a^{k_s} + 1)(a^{k_s} - 1)$, ce qui contredit notre hypothèse de minimalité sur s.
- ➢ Soit on est dans le cas d'une exception du théorème de Zsigmondy appliqué à $a^{m_r} - 1$. Il y a deux exceptions possibles : ou bien $(a, m_r) = (2, 6)$, ce qui est exclut car a est impair, ou bien $a + 1$ est une puissance de 2 et $n = 2$. Or, $a + 1 = 2^A + 2$ avec $A \geqslant 2$, donc il ne s'agit pas d'une puissance de 2.

Il n'y a donc $\boxed{\text{pas de solution si } A \geqslant 2}$.

Exercice 3.20. (IMO 2022 P5) Déterminer tous les triplets d'entiers strictement positifs (a, b, p) tels que p soit premier et que

$$a^p = b! + p.$$

Solution 3.20. **Réponse :** Les seuls couples solutions sont $(2, 2, 2)$ et $(3, 4, 3)$.

Il s'agit de développer les gestes habituels pour une équation diophantienne, à savoir divisibilité (qui amène à des disjonctions de cas) et taille, et de les combiner avec les gros théorèmes du chapitre.

- **Si** $b < p$, alors p ne divise pas $b!$ donc p ne divise pas a non plus. D'autre part, si q est un diviseur de a, alors $q \mid b!+p$ et q est premier avec p, donc q ne divise pas $b!$, soit $b < q$. Mais alors $b!+p \leqslant (q-1)^p+p < q^p$. En effet, la dernière inégalité vient de la formule du binôme :

  $$q^p = (q-1+1)^p \geqslant (q-1)^p + p(q-1) + 1 > (q-1)^p + p.$$

  Il n'y a donc pas de solution dans ce cas.

- **Si** $b \geqslant p$, alors p divise le membre de droite de l'égalité, donc $p \mid a^p$, donc $p \mid a$ et donc $p^p \mid a^p$. Ce qui implique que p^2 divise le membre de droite, donc p^2 ne divise pas $b!$, et donc $\boxed{b < 2p}$. Ainsi, $b! + p < (2p-1)! + p$ et $a^p \geqslant p^p$. Ce n'est pas suffisant pour conclure, mais cela amène à distinguer deux cas.
  - **Si** $a = p$, alors l'équation se réécrit $b! = p^p - p = p(p^{p-1} - 1)$. Il y a plusieurs façons de résoudre cette équation. La preuve qui suit a été proposée par Anatole Bouton pendant la compétition. D'après le théorème de Zsigmondy, sauf exception, le nombre $p^{p-1} - 1$ admet un facteur premier primitif q. Par définition, l'ordre de p modulo q est donc exactement $p - 1$, ce qui implique par le petit théorème de Fermat que $p - 1 \mid q - 1$. Or, si $p - 1 = q - 1$, $p = q$, ce qui est absurde car q est premier avec p d'après la relation de divisibilité. Donc $q - 1 \geqslant 2(p - 1)$ et $q \geqslant 2p - 1$.

    Comme $q \mid p^p - p$, $q \mid b!$ et $b \geqslant q \geqslant 2p - 1$. Combinée avec $b < 2p$, on trouve $b = 2p - 1$. On a alors

    $$b! = (2p-1)! \geqslant (2p-1)\dots p \geqslant p^p > p^p - p,$$

    ce qui contredit l'équation.

    On a est donc le cas de l'exception du théorème de Zsigmondy, ce qui implique soit que $(p, p-1) = (2, 6)$ (ce qui est absurde) ou que $p - 1 = 2$, soit $p = 3$. Dans le cas où $p = 3$, on a alors $a = 3$ donc $b! = 3^3 - 3 = 24$ donc $b = 4$, soit enfin que $p - 1 = 1$ et que $p = 2$, ce qui conduit à $a = 2$ et $b = 2$. Réciproquement, $\boxed{(2, 2, 2) \text{ et } (3, 4, 3) \text{ sont bien solutions}}$.

  - **On suppose que** $a > p$ **:** si $a \geqslant p^2$, alors on a d'après l'inégalité des moyennes arithmétique et géométrique que

    $$b! \leqslant (2p-1)! < \left(\frac{1 + \ldots + (p-1)}{2p-1}\right)^{2p-1} = p^{2p} - p \leqslant a^p - p,$$

    d'où la contradiction. Si $p < a < p^2$, alors a admet une diviseur premier $q < p$, mais comme q ne divise pas p, q ne divise pas $b!$ donc $b < q$, ce qui contredit $b \geqslant p$.

Solution alternative

On propose une autre façon de traiter le cas $a = p$. On retrouve l'équation $p(p^{p-1} - 1) = b!$. Si $p = 2$, alors $a = 2$ et $b! = 2^2 - 2 = 2$ donc $b = 2$. Réciproquement, le couple $\boxed{(2, 2, 2) \text{ est solution}}$.On suppose dans la suite que p est impair.

D'après le lemme LTE appliqué à $p = 2$, on a d'une part

$$v_2(b!) = v_2(p(p^{p-1} - 1)) = v_2(p^{p-1} - 1) = v_2(p-1) + v_2(p+1) + v_2(p-1) - 1 = v_2\left(\frac{p-1}{2} \cdot (p-1)(p+1)\right)$$

Or, dans le cas où $b \geqslant p+1$, le nombre $\frac{p-1}{2} \cdot (p-1)(p+1)$ divise $b!$. Cela signifie que les trois nombres $\frac{p-1}{2}, p-1$ et $p+1$ sont les seuls nombres pairs inférieurs ou égaux à b, ce qui implique que $(p-1)/2 = 2$ et $p = 5$. Mais alors l'équation devient $b! = 5^5 - 5$, qui n'a pas de solution.

On déduit que $b = p$, ce qui conduit à $p! = p^p - p$, que l'on peut éliminer par un argument de taille.

Remarque : D'autres solutions sont possibles en passant par LTE mais pour des nombres premiers impairs, et sont basées sur le même argument, mais nécessitant plus de cas à traiter à la main.

Exercice 3.21. (RMM 2025 P2) On considère une suite infinie d'entiers strictement positifs $a_1, a_2, \ldots$ telle que $a_1 > 1$ et $(2^{a_n} - 1)a_{n+1}$ est un carré parfait pour tout entier strictement positif n. Est-il possible que deux termes de la suite soient égaux ?

Solution 3.21.

➢ Commentaire :

> Une première difficulté du problème est qu'il s'agit d'un déguisement : les hypothèses données sont beaucoup plus fortes que ce qui est utile pour la preuve, donc les informations importantes sont cachées parmi la grande quantité de contraintes. La deuxième difficulté est de trouver comment traduire ce qu'il faut montrer. Une bonne idée serait de chercher un monovariant sur la suite (a_n), qui justifie qu'elle ne peut pas prendre deux fois la même valeur. La troisième difficulté est de trouver ce monovariant, à savoir la stricte croissance du plus grand facteur premier de a_n. Un tel monovariant peut être deviné en tentant de construire soi-même une suite (a_n), en s'efforçant de la construire non-monotone pour ne pas se faire d'illusions.

Notons p_n le plus grand facteur premier de a_n. Si l'on montre que la suite (p_n) est strictement croissante, alors la suite (a_n) ne pourra pas prendre deux fois la même valeur. Notons que si $a_n > 1$, alors $2^{a_n} - 1 \equiv 3 \mod 4$ n'est pas un carré parfait, donc a_{n+1} n'est pas un carré parfait non plus. En particulier $a_{n+1} > 1$, ce qui implique par récurrence que $a_n > 1$ pour tout n et que $2^{a_n} - 1$ n'est pas un carré parfait.

Soit n un indice fixé et $p = p_n$. Notons que $p > 1$ donc $2^p - 1$ n'est pas un carré parfait. Il admet donc un diviseur premier q tel que $v_q(2^p - 1)$ est impair. Comme $2^p \equiv 1 \mod q$ et $q > 1$, $\omega_q(2)$ divise p et est différent de 1, donc $\omega_q(2) = p$. Ainsi $p \mid q - 1$ et en particulier $\boxed{q > p}$.

Par définition de $p = p_n$, q ne divise pas a_n. Le lemme LTE implique donc que

$$v_q(2^{a_n} - 1) = v_q((2^p)^{a_n/p} - 1) = v_q(2^p - 1) + v_q(a_n/p) = v_q(2^p - 1).$$

Ainsi, $v_q(2^{a_n} - 1)$ est impair. On déduit que $q \mid a_{n+1}$, et donc $\boxed{p_n < q \leqslant p_{n+1}}$, comme voulu.

3.1.2 Dirichlet, Schur et Bertrand

Exercice 3.22. Soit $n \geqslant 3$ un entier. Alice souhaite placer n entiers naturels autour d'un cercles de sorte que les n produits de deux entiers voisins sont exactement les nombres $1, 2, \ldots, n$ (dans un certain ordre). Peut-elle y arriver ?

Solution 3.22. Supposons qu'Alice puisse réussir son objectif. Notons $a_1, \ldots, a_n$ les n entiers dans l'ordre dans lequel ils sont placés. On a alors

$$n! = 1 \cdot 2 \cdot \ldots \cdot n = a_1 a_2 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{n-1} a_n \cdot a_n a_1 = (a_1 \ldots a_n)^2.$$

D'après le postulat de Bertrand et le corollaire de la théorie, le nombre $n!$ admet un facteur premier p tel que $v_p(n!) = 1$, donc $n!$ ne peut pas être un carré parfait, ce qui contredit l'égalité ci-dessus.
Alice ne peut donc pas réussir.

Exercice 3.23. Montrer qu'il existe une infinité de nombre premier dont le premier chiffre (en partant de la gauche) en base 10 est 1.

Solution 3.23. D'après le postulat de Bertrand, pour tout n, il existe un nombre premier compris entre 10^n et $2 \cdot 10^n$. Ce nombre premier a donc un 1 pour premier chiffre. Ce qui justifie l'existence annoncée.

Exercice 3.24. Pour tout entier $n \geqslant 2$, on pose $H_n = 1 + \dfrac{1}{2} + \ldots + \dfrac{1}{n}$. Montrer que H_n n'est pas un entier.

Solution 3.24. On commence par mettre H_n sous la forme d'une fraction (pas forcément irréductible). Pour cela, on note $N_k = n!/k$. On a

$$H_n = \frac{N_1 + \ldots + N_n}{n!}.$$

D'après le postulat de Bertrand et le corollaire de la théorie, il existe un nombre premier p tel que $v_p(n!) = 1$. Ceci veut dire que p divise N_k pour $k \neq p$ mais que p ne divise pas N_p. Le numérateur de H_n n'est donc pas divisible par p, alors que son dénominateur l'est, ce n'est donc pas un entier.

Solution alternative
Il existe une preuve ne passant pas par le postulat de Bertrand.
Notons ℓ l'entier tel que $2^\ell \leqslant n < 2^{\ell+1}$. Notons qu'alors 2^ℓ est l'unique entier inférieur à n et divisible par 2^ℓ. Avec les notations précédentes, on déduit que $v_2(N_{2^\ell}) < v_2(N_k)$. Ainsi, la valuation $2-$adique du numérateur est égale à $v_2(N_{2^\ell})$ qui est strictement inférieur à $v_2(n!)$, donc à nouveau H_n n'est pas un entier.

Remarque : Le fait que H_n est le quotient d'un entier impair par un nombre pair (ce qui donne une autre preuve), peut également se montrer par récurrence sur n.

Exercice 3.25. Soit P un polynôme non constant à coefficients entiers. Pour tout entier $n \in \mathbb{N}^\star$, il existe un entier n tel que $P(n)$ admette au moins r facteurs premiers distincts.

Solution 3.25. D'après le théorème de Schur, il existe r nombre premiers $p_1, \ldots, p_r$ et r entiers $n_1, \ldots, n_r$ tels que $p_i \mid n_i$ pour tout $i = 1, \ldots, r$.
On tire partie de l'identité $a - b \mid P(a) - P(b)$ pour obtenir que pour tout indice i et pour tout entier k, $p_i \mid P(n_i + p_i k) - P(n_i)$, donc $p_i \mid P(n_i + k p_i)$.

D'après le théorème des restes chinois, il existe un entier T solution du système

$$\begin{cases} T & \equiv & n_1 & \mod p_1 \\ T & \equiv & n_2 & \mod p_2 \\ \vdots & & \vdots & \\ T & \equiv & n_r & \mod p_r. \end{cases}$$

Pour tout indice i, $p_i \mid T - n_i \mid P(T) - P(n_i)$, donc $p_i \mid P(T)$. Le nombre $P(T)$ possède donc au moins r facteurs premiers.

Exercice 3.26. Trouver tous les n tels qu'il existe une bijection σ de $\{1,\dots,n\}$ dans lui-même telle que $\sigma(k)+k$ est un nombre premier pour tout entier k de $\{1,\dots,n\}$.

Solution 3.26. **Réponse :** Il s'agit de tous les entiers n.

On montre que tous les entiers n sont solutions, en procédant par récurrence forte sur n.

Initialisation : Si $n=1$, la bijection envoyant 1 sur 1

Hérédité : On suppose la propriété vraie pour tout entier $m \leqslant n-1$, avec $n \geqslant 2$ fixé, et on montre qu'elle est vraie pour n.

Si $n+1=p$ est un nombre premier, la bijection définie par $\sigma(k)=p-k$ convient. Sinon, d'après le postulat de Bertrand, il existe un nombre premier q tel que $n<q<2n$. D'après l'hypothèse de récurrence appliqué à $0<q-n-1<n$, il existe une bijection f de $\{1,\dots,q-n-1\}$ dans lui-même telle que $f(k)+k$ est un nombre premier pour tout k. En posant

$$\sigma(k)=\begin{cases} f(k) & \text{si } k<q-n \\ q-k & \text{si } q-n\leqslant k\leqslant n, \end{cases}$$

on définit une bijection de $\{1,\dots,n\}$ dans lui-mêm : la restriction de sigma à $\{1,\dots,q-n\}$ est une bijection de l'ensemble dans lui-même et la restriction de σ à $\{q-n+1,\dots,n\}$ est une bijection de l'ensemble dans lui-même.

De plus, $\sigma(k)+k=q$ si $k>q-n$ est est premier si $k\leqslant q-n$ par hypothèse de récurrence. Ceci achève la récurrence et conclut l'exercice.

Exercice 3.27. *(Ibero-American 2019 P6)* Soient $a_1,\dots,a_{2019}$ des entiers strictement positifs. Soit P un polynôme à coefficients entiers tel que, pour tout entier n,

$$P(n) \mid a_1^n+\ldots+a_{2019}^n.$$

Montrer que P est constant.

Solution 3.27. Dans un tel problème de divisibilité, on cherche un n tel que le membre de droite soit facile à calculer et tel que le membre de gauche soit divisible par un nombre premier qui n'est pas censé diviser le membre de droite.

Soit p un nombre premier tel qu'il existe n tel que $p \mid P(n)$. D'après le théorème des restes chinois, il existe un entier N solution du système

$$\begin{cases} T &\equiv& n & \mod p \\ T &\equiv& 0 & \mod p-1 \end{cases}$$

Alors $p \mid T-n \mid P(T)-P(n)$, donc $p \mid P(T)$. Or, d'après le petit théorème de Fermat,

$$a_1^T+\ldots+a_{2019}^T \equiv 1+\ldots+1=2019 \mod p.$$

Comme $p \mid P(T) \mid a_1^T+\ldots+a_{2019}^T$, on déduit que $p \mid 2019$. Ainsi, l'ensemble des nombres premiers p considérés est fini. D'après la contraposée du théorème de Schur, cela implique que P est constant.

Exercice 3.28. (APMO 2025 P3) Soit P un polynôme non constant à coefficients entiers et tel que $P(0) \neq 0$. Soit $a_1, a_2, \ldots$ une suite infinie d'entiers telle que $P(i-j) \mid a_i - a_j$ pour tous indices i, j distincts. Montrer que la suite $a_1, a_2, \ldots$ est constante.

Solution 3.28. Après avoir effectué un changement de variable, on trouve que $P(k) \mid a_{i+k} - a_i$ pour tout indice i et tout entier $k \geqslant 1$.

Comme P est non constant, d'après le théorème de Schur, il existe une infinité de nombres premiers divisant un nombre de la forme $P(k)$. Soit q un tel nombre premier et k tel que $q \mid P(k)$. Comme $P(0) \neq 0$, on peut en plus supposer que q ne divise pas $P(0)$, ce qui implique que q ne divise pas k (sinon on aurait $q \mid k \mid P(k) - P(0)$ et donc $q \mid P(0)$).

On a alors pour tout indice i que $\boxed{a_{i+k} \equiv a_i \mod q}$. D'autre part, $q \mid P(k+q) - P(k)$ donc $q \mid P(k+q)$, ce qui implique de même que $\boxed{a_{i+k+q} \equiv a_i \mod q}$ pour tut indice i.

La suite (a_i) est donc périodique de période k et $k+q$. Or k et $k+q$ sont premiers entre eux. D'après le théorème de Bezout, on dispose d'entiers u et v tels que $1 = uk - v(k+q)$. Il vient que, pour tout i,

$$a_{i+1} = a_{i+uk-v(k+q)} \equiv a_{i+uk} \equiv a_i \mod q.$$

La suite $\boxed{(a_i) \text{ est donc constante modulo } q}$. Comme c'est le cas pour une infinité de nombres premiers q, elle est constante. Plus précisément, si m et n sont deux indices distincts, alors en choisissant $q > |a_m - a_n|$, la congruence $a_m \equiv a_n \mod q$ implique $a_m - a_n = 0$, comme voulu.

Exercice 3.29. (MEMO 2017 T8) Pour tout entier $n \geqslant 3$, la suite $\alpha_1, \ldots, \alpha_k$ désigne la suite des exposants dans la décomposition en facteurs premiers de $n! = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Déterminer tous les entiers $n \geqslant 3$ pour lesquels la suite $\alpha_1, \ldots, \alpha_k$ est géométrique.

Solution 3.29. **Réponse :** Il s'agit des entiers $3, 4, 6$ et 10.

Soit n un entier solution. Soit p_1 le plus petit nombre premier de $[\![\lfloor n/2 \rfloor, n]\!]$ et p_2 le plus grand nombre premier de l'intervalle $]\lfloor n/4 \rfloor, 2\lfloor n/4 \rfloor[$. Les nombres p_2 et p_1 sont consécutifs, et on suppose que $p_2 > 3$. L'existence de p_1 et de p_2 est garantie par le postulat de Bertrand. Vu que $2p_1 > n$, on va $v_{p_1}(n!) = 1$. Vu que $3p_2 < n < 4p_2$, on a $v_{p_2}(n!) = 3$. Ceci implique que la raison de la suite géométrique est 3.

Soit p_3 un nombre premier de l'intervalle $]\lfloor n/8 \rfloor, 2\lfloor n/8 \rfloor[$. On suppose que $p_3 > 3$. On a alors $7p_3 < n < 8p_3$, donc $v_{p_3}(n!) \leqslant 8$ (puisque $\{p_3, \ldots, 7p_3\}$ peut contenir au plus un multiple de p_3^2), ce qui est absurde car $v_{p_3}(n!) \geqslant 3v_{p_2}(n!) = 9$.

De cette contradiction, on suppose que $p_3 \leqslant 3$ ou $p_2 \leqslant 3$. Dans le premier cas, on trouve que $n \leqslant 24$ ou $n \leqslant 12$. Il reste donc à traiter les valeurs de n à la main pour $n \leqslant 24$.

Ce calcul donne les solutions annoncées.

Exercice 3.30. (RMM SL 2018 N1) Déterminer tous les polynômes f à coefficients entiers tels que, pour tout nombre premier $p \geqslant 3$, $f(p)$ divise $2^p - 2$.

Solution 3.30. **Réponse :** Les polynômes solutions sont $\pm 1, \pm 2, \pm 3, \pm 6, \pm X, \pm 2X$.

➢ **Commentaire :**

> Si $f(p)$ admet un autre facteur premier q, la divisibilité $q \mid 2^p - 2$ entraîne $p \equiv 1 \mod \omega_q(2)$. D'autre part, le théorème de Dirichlet permet de construire une infinités de nombres premiers de la forme $p' = p + kq$, qui devront tous vérifier la même congruence $p' \equiv 1 \mod \omega_2(q)$:
>
> $$p' \equiv p \mod q \Longrightarrow p' \equiv 1 \mod \omega_q(2).$$
>
> Mais le théorème de Dirichlet et le théorème des restes chinois permettent de construire des p' vérifiant le système
>
> $$\begin{cases} p' & \equiv & p & \mod q \\ p' & \equiv & -1 & \mod \omega_q(2) \end{cases}$$
>
> Ceci force $\omega_q(2)$ à être petit et borne les valeurs de q.

Soit p un nombre premier impair et q un éventuel diviseur impair de $f(p)$ distinct de p. On note ω l'ordre de 2 modulo q. Comme $\omega \mid q - 1$, ω est premier avec q. On a d'après l'énoncé

$$q \mid f(p) \mid 2^p - 2 \Longrightarrow p \equiv 1 \mod \omega.$$

Soit n une solution du système de congruence suivant, donnée par le théorème des restes chinois :

$$\begin{cases} n & \equiv & p & \mod q \\ n & \equiv & -1 & \mod \omega \end{cases}$$

L'entier n est manifestement premier avec q et ω. D'après le théorème de Dirichlet, il existe donc un nombre premier $p' > p$ tel que $p' \equiv n \equiv p \mod q\omega$. Mais alors $q \mid p' - p \mid f(p') - f(p)$, donc $q \mid f(p')$, ce qui conduit à $p' \equiv 1 \mod \omega$. Or, $p' \equiv n \equiv -1 \mod \omega$, donc $-1 \equiv 1 \mod \omega$, ce qui implique que $\omega \in \{1, 2\}$, donc $q = 3$.

On a montré que $\boxed{\text{les seuls facteurs premiers éventuels de } f(p) \text{ sont } 2, 3, p}$.

Soit à présent $\alpha \geqslant 0$ un entier et g un polynôme à coefficients entiers tel que $g(0) \neq 0$ tel que $f(X) = X^\alpha g(X)$. Comme $3^\alpha g(3) = f(3) \mid 2^3 - 2 = 6$, on déduit que $\boxed{\alpha \in \{0, 1\}}$.

Notons que g vérifie également l'énoncé, donc les facteurs de $g(p)$ sont parmi $2, 3, p$. Or, si p est un nombre premier qui divise $g(p)$, alors $p \mid g(p) - g(0)$ donc $p \mid g(0)$. Il y a donc un nombre fini de nombres premiers qui divisent $g(p)$. Soit p un grand nombre premier (de sorte que p ne divise pas $g(p)$) et tel que $p \equiv 5 \mod 3$. On peut écrire $g(p) = 2^x \cdot 3^y$. Alors $2^x \cdot 3^y \mid 2^p - 2$. On déduit que $x \leqslant 1$ et comme $2^p - 2 \equiv 2^5 - 2 \equiv 3 \mod 9$, $y \leqslant 1$. On déduit que $g(p) \mid 6$ pour un infinité de nombres premiers, ce qui impose que $\boxed{g \text{ est constant}}$ égal à c, avec $c \mid 6$.

En résumé, $f(X) = \pm cX^\alpha$, avec $\alpha \leqslant 1$ et $c \mid 6$. Réciproquement, si f est de cette forme, on vérifie que

- ➢ Si $\alpha = 0$, on vérifie que $6 \mid 2^p - 2$ pour tout nombre premier impair (notamment car $2^p - 2 \equiv 2^1 - 2 \mod 3$), donc les polynômes $\boxed{\pm 1, \pm 2, \pm 3 \text{ et } \pm 6 \text{ sont bien solutions}}$.
- ➢ Si $\alpha = 1$, comme $3c = f(3) \mid 2^3 - 2 = 6$, il faut que $c \mid 2$. Réciproquement, comme $p \mid 2^p - 2$ pour tout nombre premier impair et $2 \mid 2^p - 2$, les polynômes $\boxed{\pm X \text{ et } \pm 2X \text{ sont bien solutions}}$.

$\boxed{\text{Remarque :}}$ Pour montrer que g est constant, on aurait également pu utiliser le lemme de Schur : soit $q \geqslant 5$ premier tel qu'il existe n tel que $q \mid g(n)$. Pour les mêmes raisons que ci-dessus, comme $g(0) \neq 0$, on peut choisir q tel que l'entier n est premier avec q. D'après le théorème de Dirichlet, il existe un nombre premier $p > 5$ tel que $p \equiv n \mod q$, ce qui conduit à $q \mid g(p) \mid f(p)$, ce qui contredit que les facteurs de $f(p)$ sont $2, 3$, et p. Ainsi, g admet un nombre fini de facteurs premiers, ce qui implique que g est constant d'après le théorème de Schur.

Exercice 3.31. (Concours Mathraining 16) Soit P un polynôme non constant à coefficients entiers. Soient a et b des entiers relatifs tels que, pour tout entier n non nul, le nombre $a^n + P(n)$ est non nul et

$$a^n + P(n) \mid b^n + P(n).$$

Montrer que $a = b$.

Solution 3.31. Comme P est non constant, d'après le théorème de Schur appliqué à $P(X) + a$, on dispose d'un nombre premier $p > \max(a, b)$ et d'un entier n tel que $p \mid P(n) + a$.

Soit désormais m un entier vérifiant le système

$$\begin{cases} m & \equiv n & \mod p \\ m & \equiv 1 & \mod p-1, \end{cases}$$

dont l'existence est garantie par le théorème des restes chinois. La première congruence implique que $p \mid m-n \mid P(m)-P(n)$ et la deuxième implique, d'après le petit théorème de Fermat, que $a^m \equiv a \mod p$ (on vérifie que a est premier avec p par choix de p). On a donc $a^m + P(m) \equiv a + P(n) \equiv 0 \mod p$. On a également

$$p \mid a^m + P(m) \mid b^m + P(m) \quad \Longrightarrow 0 \equiv b^m + P(m) \equiv b + P(n) \mod p,$$

où on a utilisé le petit théorème de Fermat sur b, également premier avec p. On a donc $p \mid b+P(n)-(a+P(n)) = b-a$. En prenant de plus $p > |b-a|$, on déduit que $\boxed{a = b}$ comme voulu.

Remarque : Cet exercice est une généralisation du problème IMO SL 2005 N6.

Exercice 3.32. (Balkan MO 2023) Soit $\omega(n)$ le nombre de diviseurs premiers distincts de n (par exemple $\omega(1) = 0, \omega(12) = 2$). Déterminer tous les polynômes P à coefficients entiers tels que, pour tout entier n tel que $\omega(n) > 2023^{2023}$, l'entier $P(n)$ est strictement positif et vérifie $\omega(n) \geqslant \omega(P(n))$.

Solution 3.32. **Réponse :** les polynômes de la forme X^n, avec $n \geqslant 1$, et les polynômes constants égaux à c, avec $\omega(c) \leqslant 2023^{2023}$.

Posons $P(X) = X^\alpha Q(X)$, avec $Q(0) \neq 0$ et $\alpha \geqslant 0$ un entier. Le but est de montrer que $Q(X) = 1$.

➢ **Commentaire :**

> L'essentiel du problème consiste en fait à montrer que Q est constant, en construisant par l'absurde un entier n pour lequel $\omega(Q(n)) \geqslant \omega(n) > 2023^{2023}$. Pour cela, on procède en deux temps.
> - ➢ On commence par construire un entier n pour lequel $\omega(Q(n))$ est grand, à l'aide du théorème de Schur et du théorème des restes chinois. Cette construction correspond à l'exercice 3.25.
> - ➢ Puis on corrige n, en trouvant un entier N avec les même propriétés que n, mais dont on contrôle les facteurs premiers (pour que $\omega(N)$ soit petit), à l'aide du théorème de Dirichlet. Sans l'hyptohèse qu'il faut $\omega(N) \geqslant 2023^{2023}$, on pourrait se contenter de choisir N premier et vérifiant le système. Il faut raffiner cette idée.

Soit $r > 2023^{2023}+1$. D'après le théorème de Schur, si Q est non constant, il existe r nombres premiers $p_1, \ldots, p_r$ et des entiers $n_1, \ldots, n_r$ tels que $p_i \mid Q(n_i)$. Comme $Q(0) \neq 0$, on peut même choisir les p_i tels qu'ils ne divisent pas $Q(0)$. On a alors que, pour tout indice i, p_i ne divise pas n_i (sinon on aurait $p_i \mid n_i \mid Q(n_i) - Q(0)$ et donc $p_i \mid P(0)$). D'après le théorème des restes chinois, il existe un entier n tel que

$$\begin{cases} n & \equiv & n_1 & \mod p_1 \\ n & \equiv & n_2 & \mod p_2 \\ \vdots & & \vdots & \\ n & \equiv & n_r & \mod p_r. \end{cases}$$

On a alors que $p_i \mid n - n_i \mid Q(n) - Q(n_i)$, donc $p_i \mid Q(n)$ pour tout i. On déduit que $\boxed{\omega(Q(n)) \geqslant r}$.

On cherche à présent un entier N tel que $N \equiv n \mod p_1 \ldots p_r$ mais tel que $\omega(N) = r-1$. On pose $P = p_1 \ldots p_r$. Notons que comme n_i est premier avec p_i pour tout i, n est premier avec les p_i et donc avec P. D'après le théorème de Dirichlet, on dispose $q_1, \ldots, q_{r-2}$ des nombres premiers vérifiant $q_i \equiv 1 \mod P$ pour tout i et q un nombre premier vérifiant $q \equiv n \mod P$. Alors $N = q_1 \ldots q_{r-2} q$ vérifie $N \equiv n \mod P$ et $\omega(N) = r - 1 \geqslant 2023^{2023}$. De

plus, comme $P \mid N - n \mid Q(N) - Q(n)$ et que $P \mid Q(n)$, $P \mid Q(N)$ donc $\omega(Q(N)) \geqslant r > \omega(N)$, ce qui implique que $\omega(P(N)) > \omega(N)$, ce qui contredit l'énoncé. Ainsi, $\boxed{Q \text{ est constant}}$, et on note $c = Q(X)$.

On peut alors distinguer deux cas :

- ➢ Si $\alpha \geqslant 1$, en prenant n premier avec c et tel que $\omega(n) > 2023^{2023}$, on a $\omega(P(n)) = \omega(c) + \omega(n) > \omega(n)$, ce qui est une contradiction. Donc $c = 1$ et réciproquement, les monômes sont bien solutions.
- ➢ Si $\alpha = 0$, alors P est constant égal à c et si $\omega(c) > 2023^{2023} + 1$, l'inégalité de l'énoncé n'est plus vérifiée pour n tel que $\omega(n) = 2023^{2023} + 1$. Il faut donc $\omega(c) \leqslant 2023^{2023}$, ce qui est également suffisant.

Exercice 3.33. (Envoi 2021-2022 P18) Déterminer tous les polynômes $P \in \mathbb{Z}[X]$ tels que :

1. $P(n) \geqslant 1$ pour tout $n \geqslant 1$,
2. $P(mn)$ et $P(m)P(n)$ ont le même nombre de diviseurs premiers pour tous $m, n \geq 1$.

Solution 3.33. **Solution :** Il s'agit des polynômes de la forme cX^α avec $c \geqslant 1$ et $\alpha \geqslant 0$.

La solution qui suit a été donnée par Georges Tézé à l'occasion de l'envoi 2021-2022. Dans la suite, pour tout entier $n \in \mathbb{N}^*$, on note $\delta(n)$ le nombre de diviseurs premiers de n.

Tout d'abord, d'après l'énoncé, puisque $\delta(P(n^2)) = \delta(P(n)^2) = \delta(P(n))$ pour tout n, on a par récurrence immédiate que $\delta(P(n^{2^k})) = \delta(P(n))$ pour tout entier k.
D'autre part, pour tout entier ℓ, $\delta(P(n^\ell)) = \delta(P(n)P(n^{\ell-1})) \geqslant \delta(P(n^{\ell-1}))$. La suite $(\delta(P(n^\ell)))_\ell$ est donc croissante, mais la sous-suite $(\delta(P(n^{2^k})))_k$ est constante. On déduit que la suite $(\delta(P(n^\ell)))_\ell$ est constante, et $\boxed{\delta(P(n^\ell)) = \delta(P(n))}$ pour tout entier $n \geqslant 1$ et tout entier $\ell \geqslant 1$.

Posons $P(X) = X^\alpha Q(X)$ avec $\alpha \geqslant 0$ un entier et Q un polynôme à coefficients entiers tel que $Q(0) \neq 0$. On suppose par l'absurde que Q est non constant. Soit p un nombre premier tel $p > |Q(0)|$ et tel qu'il existe un entier n tel que $p \mid Q(n)$. On remarque que p ne divise pas n, puisque sinon on aurait $p \mid n \mid Q(n) - Q(0)$, donc p diviserait $Q(0)$, ce que la définition de p exclut.
Notons que Q vérifie également l'énoncé, et donc la propriété $\delta(Q(n^\ell)) = \delta(Q(n))$ pour tout entier ℓ. Pour tout entier ℓ, comme $\delta(Q(n)Q(n^\ell)) = \delta(Q(n^{\ell+1})) = \delta(Q(n))$, on a que $p \mid Q(n^\ell)$ pour tout ℓ. En particulier, $p \mid Q(n^{p-1})$. Or, d'après le petit théorème de Fermat,

$$p \mid n^{p-1} - 1 \mid Q(n^{p-1}) - Q(1) \Longrightarrow p \mid Q(1).$$

Ainsi, les diviseurs premier de Q divisent soit $Q(0)$ soit $Q(1)$, qui sont tous les deux non nuls. Donc Q admet un nombre fini de diviseurs premiers. D'après la contraposée du lemme de Schur, on déduit que $\boxed{Q \text{ est constant}}$.

Réciproquement, les polynômes de la forme cX^α sont bien solution du problème.

Exercice 3.34. (ELMO SL 2014) Déterminer tous les triplets (a, b, c) d'entiers strictement positifs tels que, pour tout entier n dont tous les facteurs premiers sont supérieurs à 2014, $n + c \mid a^b + b^n + n$.

Solution 3.34. **Solution :** Le seul triplet solution est $(1, 1, 2)$.

➢ **Commentaire :**

> La stratégie est de chercher n tel que $n + c$ est divisible par un nombre premier qui ne peut pas diviser $a^n + b^n + n$, sauf dans un nombre fini de cas. Il s'agit alors d'effectuer la même technique que dans les exercices sur l'ordre : on choisit $n \mod p$ pour contrôler le terme en n, et $n \mod p - 1$ pour contrôler les termes en a^n et b^n, et on remonte le système avec le théorème chinois. Le théorème de Dirichlet donne un moyen simple de s'assurer que n n'a pas de petits facteurs premiers.

Notons P le produit des nombres premiers inférieurs ou égaux à 2014. Soit $p > 2014$ un nombre premier tel que $p \equiv 1 \mod P$, l'existence d'une infinité de tel nombres premiers étant garantie par le théorème de Dirichlet. Soit n un entier solution du système de congruences

$$\begin{cases} n & \equiv -c & \mod p \\ n & \equiv 1 & \mod p-1, \end{cases}$$

l'existence d'un tel n est garantie par le théorème des restes chinois).
Comme n est premier avec $p - 1$ et que $P \mid p - 1$, n est premier avec P. Puisque $p \mid n + c \mid a^n + b^n + n$,

$$0 \equiv a^n + b^n + n \equiv a + b - c \mod p.$$

Comme cette congruence est vraie pour une infinité de nombres premiers p, on déduit que $\boxed{a + b = c}$.

On peut en fait répéter l'argument précédent en changeant la valeur de $a^n \mod p$. Notons $q > 2014, p - 1$ un nombre premier et n un entier solution du système de congruences

$$\begin{cases} n & \equiv -c & \mod p \\ n & \equiv q & \mod p-1. \end{cases}$$

Là aussi, n est premier avec $p - 1$ donc avec P. On obtient cette fois-ci

$$0 \equiv a^n + b^n + n \equiv a^q + b^q - c \mod p,$$

ce qui implique que $\boxed{a^q + b^q = c}$. On déduit que $a^q + b^q = a + b$, ce qui implique que $a = b = 1$ et $c = 2$. Réciproquement, le triplet $(1, 1, 2)$ est bien solution puisque $n + 2 \mid 1^n + 1^n + n$ pour tout n.

$\boxed{\text{Remarque :}}$ D'autres relations sur a, b et c sont possibles. Par exemple, en choisissant plutôt $n \equiv -1 \mod p-1$, on trouve $0 \equiv a^{-1} + b^{-1} - c \mod p$, ce qui imlique que $p \mid a + b - abc$. On déduit que $abc = a + b$, à partir de quoi on peut déduire que $(a, b, c) = (1, 1, 2)$.

Solution alternative

On présente une solution qui utilise le théorème de Zsigmondy.

Soit n un entier n'admettant aucun facteur premier inférieur à 2014. D'après le théorème de Zsigmondy, sauf exception, le nombre $a^n + b^n$ admet un facteur premier primitif p pour tout n. Notons que p ne divise pas n, sinon on aurait $0 \equiv a^n + b^n \equiv a^{n/p} + b^{n/p} \mod p$, ce qui contredit le caractère primitif de p.

De plus, puisque c admet un nombre fini de facteurs premiers, il existe un nombre fini d'entiers n pour lesquels le diviseur primitif p de $a^n + b^n$ est un facteur de c. On peut donc supposer, en prenant n assez grand, que p ne divise pas c.

D'après le théorème de Dirichlet, il existe un nombre premier $q > 2014$ tel que $q \equiv -\dfrac{c}{n} \mod p$, c'est-à-dire $p \mid qn + c$. Comme le nombre qn a ses facteurs premiers supérieurs à 2014, on a d'après l'énoncé

$$p \mid qn + c \mid a^{qn} + b^{qn} + qn,$$

Or, $a^n + b^n \mid a^{qn} + b^{qn}$, donc $p \mid a^{qn} + b^{qn}$ donc $p \mid qn$. Comme on a aussi $p \mid qn + c$, on obtient que $p \mid c$, ce qui est une contradiction.

On est donc dans l'exception du théorème de Zsigmondy, ce qui implique que soit $(a, b, n) = (2, 1, 3)$ - ce qui est impossible vu la construction de n, soit $\boxed{a = b}$. Si a admet un facteur premier p, on peut construire n premier

avec p comme dans la solution précédente pour que $p \mid n + c$, ce qui implique que $p \mid n + c \mid 2a^n - c$, ce qui conduit à $p \mid c$. Mais alors $p \mid n$, ce qui est exclus. On conclut que $\boxed{a = b = 1}$. Alors pour tout entier n vérifiant les conditions de l'énoncé, $n + c \mid 2 - c$, ce qui implique que $c = 2$.

3.2 Travailler modulo p - épisode 2

3.2.1 Polynômes modulo p

Exercice 3.35. Vérifier que $X^p - a \equiv (X-a)^p \mod p$.

Solution 3.35. Comme p est impair, d'après la propriété de Frobenius appliquée à $P(X) = X - a$,

$$X^p - a = P(X^p) \equiv P(X)^p \equiv (X-a)^p \mod p.$$

Exercice 3.36. Soient P et Q deux polynômes entiers. On suppose que $p \mid P(a) - Q(a)$ pour tout entier $a = 0, \dots, p-1$. Montrer qu'il existe un polynôme R à coefficients entiers tel que $X^p - X$ divise $P(X) - Q(X) + pR(X)$.

Solution 3.36. Puisque $0, \dots, p-1$ sont des racines de $P - Q$ modulo p, il existe un polynôme $B(X)$ tel que $P(X) - Q(X) \equiv X(X-1)\dots(X-(p-1))B(X) \mod p$. Comme $X(X-1)\dots(X-(p-1)) \equiv X^p - X \mod p$, on a même $P(X) - Q(X) \equiv (X^p - X)B(X) \mod p$.
En revenant à la définition de la congruence, il existe un polynôme R tel que

$$(X^p - X)B(X) = P(X) - Q(X) + pR(X),$$

ce qui est le résultat voulu.

Exercice 3.37. Soit d un diviseur de $p-1$. Montrer qu'il y a exactement $\varphi(d)$ éléments de l'ensemble $\{1, \dots, p-1\}$ d'ordre d. En particulier, il y a $\varphi(p-1)$ éléments d'ordre $p-1$.

Solution 3.37. Soit g un générateur modulo p, qui est donc d'ordre $p-1$. On note $\ell = \dfrac{p-1}{d}$. Montrons que les éléments d'ordre d sont exactement les $g^{\ell m}$, avec $1 \leqslant m \leqslant d-1$ et $\mathrm{PGCD}(m,d) = 1$. Comme il y a $\varphi(d)$ tels entiers k, cela donne la conclusion.

Soit $x = g^k$ un élément de $\{1, \dots, p-1\}$ d'ordre d. On a donc $g^{kd} \equiv 1 \mod p$, donc $p-1 \mid kd$, soit $\ell \mid k$. On dispose donc d'un entier m tel que $k = \ell m$. Notons $\delta = \mathrm{PGCD}(m,d)$. Alors

$$g^{k\frac{d}{\delta}} = (g^d)^{k/\delta} \equiv 1 \mod p \implies d \mid \frac{d}{\delta} \implies \delta = 1,$$

ce qui implique que m est premier avec d, comme annoncé.

On a donc montré que, parmi les entiers k tels que $(g^k)^d \equiv 1 \mod p$, les g^k d'ordre exactement d sont ceux de la forme annoncée, ce qui conclut.

Exercice 3.38. Soit $1 \leqslant k \leqslant p-2$. Montrer que $1^k + 2^k + \dots + (p-1)^k \equiv 0 \mod p$.

Solution 3.38. Soit $1 \leqslant k \leqslant p-2$. Soit g un générateur modulo p. Alors $\{1, \dots, p-1\} = \{g^0, g^1 \mod p, \dots, g^{p-2} \mod p\}$. En particulier, $g^k \neq 1 \mod p$. Il vient, avec la formule de la somme de termes d'une suite géométrique et d'après le petit théorème de Fermat, que

$$1^k + 2^k + \dots + (p-1)^k \equiv g^{0\cdot k} + g^k + g^{2k} + \dots + g^{k(p-1)} = \frac{(g^k)^{p-1} - 1}{g^k - 1} = \frac{(g^{p-1})^k - 1}{g^k - 1} \equiv \frac{1-1}{g^k - 1} \equiv 0 \mod p,$$

comme voulu.

Exercice 3.39. Déterminer le nombre de polynômes unitaires de degré $p-2$, admettant $p-2$ racines distinctes modulo p et dont les coefficients sont deux à deux distincts.

Solution 3.39. Soit P un tel polynôme et a l'unique élément de $\{1, \dots, p-1\}$ tel que $P(a) \neq 0 \mod p$. Comme P est unitaire et que tous les autres éléments de $\{1, \dots, p-1\}$ sont racines de P, il s'agit des $p-2$ racines de P, si bien que

$$(X-a)P(X) \equiv (X-1)\dots(X-(p-1)) \equiv X^{p-1}-1 \mod p.$$

On déduit que

$$P(X) \equiv \frac{X^{p-1}-1}{X-1} = \frac{X^{p-1}-a^{p-1}}{X-a} = X^{p-2}+aX^{p-3}+\dots+a^{p-2}X+a^{p-1} \mod p.$$

Pour que les coefficients de ce polynôme soient deux à deux distincts modulo p, il faut que les a^i soient deux à deux distincts modulo p, ce qui nécessite que $\boxed{a \text{ soit un générateur modulo } p}$.

Réciproquement, on peut remonter les calculs pour obtenir que, pour tout a qui est un générateur modulo p, le polynôme $X^{p-2}+\dots+a^{p-2} = \frac{X^{p-1}-1}{X-a}$ (où les coefficients sont pris modulo p) admet $p-2$ racines distinctes.

Comme il y a $\varphi(p-1)$ générateurs, il y a $\boxed{\varphi(p-1)}$ tels polynômes.

Exercice 3.40. *(Estonie TST 2020)* Soient p et q des nombres premiers et a un entier tel que q ne divise pas $a-1$ mais q divise a^p-1. Montrer que

$$(1+a)(1+a^2)\dots(1+a^{p-1}) \equiv 1 \mod q.$$

Solution 3.40. Le membre de gauche invite à introduire le polynôme $(X+a)\dots(X+a^{p-1})$. Pour calculer ce polynôme, il faut trouver un polynôme simple qui a pour racine $-a, -a^2, \dots$.

Or, d'après l'énoncé, $((-a)^k)^p \equiv (-1)^p(a^p)^k \equiv -1 \mod q$ pour tout $1 \leqslant k \leqslant p-1$. On déduit que $-a, -a^2, \dots, -a^{p-1}$ sont des racines du polynôme X^p+1 modulo q. Ce polynôme admet une dernière racine, à savoir $-1 = -a^0$.

D'après l'hypothèse, $a^p \equiv 1 \mod q$ donc $\omega_q(a) \mid p$, et comme q ne divise pas $a-1$, $\omega_q(a) = p$, donc les a^k sont deux à deux distincts pour $0 \leqslant k \leqslant p-1$. Ainsi, on a trouvé p racine distinctes du polynôme X^p+1. Il vient que

$$X^p+1 \equiv (X+1)(X+a)\dots(X+a^{p-1}) \mod q.$$

On déduit, en évaluant en 1, ce qui n'annule pas $X+1$,

$$(1+a)\dots(1+a^{p-1}) \equiv \frac{1^p+1}{1+1} \equiv 1 \mod q.$$

Exercice 3.41. *(Chine TST 2018 test 4 jour 2 Q4)* Soit p un nombre premier et k un entier strictement positif. On note S l'ensemble des éléments de $\{0,1,\dots,p-1\}$ pour lesquels il existe un entier x tel que $x^k \equiv a \mod p$. On suppose que $3 \leqslant |S| \leqslant p-2$. Montrer que les éléments de S ne sont pas en progression arithmétique.

Solution 3.41. Notons que si $a \equiv 0 \mod p$, alors $S = \{0\}$, donc on peut exclure ce cas.

Soit $d = \mathrm{PGCD}(k, p-1)$ et écrivons $k = d\delta$, où $\mathrm{PGCD}(\delta, p-1) = 1$. Soit g un générateur modulo p. Comme $|S| \geqslant 1$, l'équation admet au moins une solution, donc il existe r tel que $(g^r)^k \equiv a \mod p$. Montrons alors que $S = \{g^{r+\frac{p-1}{d}\ell}, \ell = 0,\dots,d-1\}$. On procède par double inclusion :

$\boxed{\supset :}$ Si $\ell \in \{0,\dots,d-1\}$, alors

$$(g^{r+\frac{p-1}{d}\ell})^k = (g^r)^k g^{\frac{p-1}{d}\ell d\delta} \equiv a(g^{\ell\delta})^{p-1} \equiv a \mod p.$$

donc $g^{r+\frac{p-1}{d}\ell} \in S$.

$\boxed{\subset :}$ Soit $x \in S$ et s tel que $x \equiv g^s \mod p$. Alors $(g^r)^k \equiv a \equiv (g^s)^k \mod p$, donc $g^{k(r-s)} \equiv 1 \mod p$. On déduit, puisque $\omega_p(g) = p-1$, que $p-1 \mid k(r-s)$ ou encore que $\frac{p-1}{d} \mid \delta(r-s)$. Comme $\mathrm{PGCD}(\frac{p-1}{d}, \delta) = 1$, on a $\frac{p-1}{d} \mid r-s$, donc on dispose de ℓ tel que $s = r + \frac{p-1}{d}\ell$. Quitte à faire la division euclidienne de ℓ par d (ce qui ne change pas la valeur de g^s), on peut supposer que $\ell \in \{0,\dots,d-1\}$.

En particulier, $|S| = d$. Supposons à présent que les éléments de S sont en progression arithmétique. On note m la raison de la suite et b le plus petit terme, de sorte que $S = \{b, b+m, \dots, b+m(d-1)\}$. D'une part, la somme des éléments de S vaut

$$b+(b+m)+\ldots+(b+m(d-1)) \equiv db+m\frac{d(d-1)}{2} \mod p,$$

d'autre part, elle vaut

$$g^r+g^{r+\frac{p-1}{d}}+\ldots+g^{r+\frac{p-1}{d}(d-1)} = g^r\frac{g^{\frac{p-1}{d}d}-1}{g^{\frac{p-1}{d}}-1} \equiv 0 \mod p.$$

Il nous faut une deuxième équation pour compléter celle-ci. On a de la même manière, en regardant la somme des carrés des éléments de S,

$$b^2+(b+m)^2+\ldots+(b+m(d-1))^2 \equiv db^2+bmd(d-1)+m^2\frac{d(d-1)(2d-1)}{6} \mod p,$$

et d'autre part cette somme vaut

$$g^{2r}+g^{2r+2\frac{p-1}{d}}+\ldots+g^{2r+2\frac{p-1}{d}(d-1)} = g^{2r}\frac{g^{2\frac{p-1}{d}d}-1}{g^{2\frac{p-1}{d}}-1} \equiv 0 \mod p.$$

Notons que $g^{2\frac{p-1}{d}} \neq 1$ car $d=|S| \neq 2$. On déduit le système de deux équations

$$\left\{\begin{array}{lll} db+m\frac{d(d-1)}{2} & \equiv 0 \mod p \\ db^2+bmd(d-1)+m^2\frac{d(d-1)(2d-1)}{6} & \equiv 0 \mod p \end{array}\right. \Longrightarrow \left\{\begin{array}{lll} b & \equiv -m\frac{(d-1)}{2} \mod p \\ bm\frac{d(d-1)}{2}+m^2\frac{d(d-1)(2d-1)}{6} & \equiv 0 \mod p \end{array}\right.$$
$$\Longrightarrow \left\{\begin{array}{lll} b & \equiv -m\frac{(d-1)}{2} \mod p \\ b+m\frac{(2d-1)}{3} & \equiv 0 \mod p \end{array}\right.$$

On déduit que $\frac{d-1}{2} \equiv \frac{2d-1}{3}$, soit $d \equiv p-1 \mod p$, contredisant que $|S|<p-1$. Ceci conclut.

Remarque : Une autre façon de montrer que la somme des éléments de S (et la somme de ses carrés) vaut 0 consiste à remarquer que si $S=\{x_1,\ldots,x_d\}$, alors en notant $xS=\{xx_1,\ldots,xx_d\}$, on constate que $x_iS=S$ pour tout indice i (c'est la même astuce que pour la preuve du petit théorème de Fermat).

On déduit, si s est la somme des éléments de S, que $s \equiv xs \mod p$. Comme $1 \notin S$ lorsque $|S|<p-1$, on déduit que $s \equiv 0$. De même, si s' est la somme des carrés des éléments de s, $s' \equiv x^2s' \mod p$, et comme $-1 \notin S$ lorsque $|S| \geqslant 3$, on déduit que $s' \equiv 0 \mod p$.

Exercice 3.42. (Envoi d'arithmétique 2019-2020) Déterminer tous les entiers n tels que la propriété suivante est vraie : pour tout entier c, il existe un entier x tel que $x^x \equiv c \mod n$.

Solution 3.42. **Réponse :** Il s'agit des entiers n de la forme $n=p_1\ldots p_r$, où les p_i sont deux à deux distincts et aucun des p_i ne divise un des p_j-1.

Notons déjà que si n vérifie la propriété, alors tout diviseur d de n la vérifie également. Posons f l'application qui à x dans $\mathbb{N}^*$ dans $\mathbb{Z}/n\mathbb{Z}$.
Pour $n=p^2$ avec p premier, notons que p n'est pas dans l'image de f. En effet, si $f(x) \equiv p \pmod{p^2}$, p divise x^x donc p divise x. En particulier, comme $x \geq p \geq 2$, p^2 divise $x^x = f(x)$ contradiction. En particulier, si n vérifie la propriété, n est sans facteur carré

Pour $n=p$ premier, donnons nous $y \in \mathbb{N}$. On cherche x entier positif tel que $x^x \equiv y \pmod p$. Pour cela, on utilise le petit théorème de Fermat : si $p-1$ divise $x-1$, $x^x \equiv x^{x-1} \times x \equiv x \pmod p$. En particulier, il suffit de prendre x strictement positif tel que $x \equiv 1 \pmod{p-1}$ et $x \equiv y \pmod p$. Ceci est possible par le théorème des restes chinois, car p et $p-1$ sont premiers entre eux, donc f est surjective.

Supposons désormais que $n=p_1\ldots p_k$ est le produit de nombres premiers distincts.

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

primitive modulo p_j, comme a est d'ordre exactement $p_j - 1$, on obtient une contradiction, l'application f n'est pas surjective.

Réciproquement, supposons que p_i ne divise jamais $p_j - 1$ pour tous indices i, j et montrons que f est surjective modulo n. On fixe $y \in \mathbb{N}$, Soit x vérifiant

$$x \equiv 1 \pmod{\prod_{i=1}^{r}(p_i - 1)}, \quad \text{et } x \equiv y \pmod{\prod_{i=1}^{r} p_i}.$$

Un tel x existe d'après le théorème des restes chinois, que l'on peut appliquer ici car les modulos sont premiers entre eux.
D'après le théorème d'euler, puisque $x \equiv 1 \mod \varphi(p_1 \dots p_r)$, $x^x \equiv x \equiv y \mod n$ et $\boxed{f \text{ est bien surjective}}$.

Ainsi l'application est surjective si et seulement si $n = p_1 \dots p_k$ avec les (p_i) premiers et deux à deux distincts et pour tout (i, j) entre 1 et k, p_i ne divise pas $p_j - 1$.

Exercice 3.43. (IMO SL 1997) Soit p un nombre premier et P un polynôme de degré d tel que $P(0) = 0, P(1) = 1$ et, pour tout entier n, soit $P(n) \equiv 0 \mod p$ soit $P(n) \equiv 1 \mod p$. Montrer que $d \geqslant p - 1$.

Solution 3.43.

➢ Commentaire :

> Il y a plusieurs tentatives possibles. La plus naturelle est d'essayer de traduire le fait que $P(n) \equiv 0, 1 \mod p$ sous la forme de racines de P ou de $P - 1$ modulo p. Toutefois, sans plus d'arithmétique, cette idée n'implique que $d \geqslant p/2$.
>
> Une autre idée, si on a toutes les valeurs de P en $\{0, \dots, p-1\}$ est de comparer P au polynôme L interpolateur de Lagrange prenant la valeur $P(i)$ en i. Par minimalité du degré du polynôme interpolateur de Lagrange, $\deg P \geqslant \deg L$. Il reste alors à montrer que $\deg L \geqslant p - 1$, en calculant son coefficient dominant.

Notons

$$L_i(X) = \prod_{j \neq i} \frac{X - j}{i - j}, \quad L(X) = \sum_{i=0}^{p-1} P(i) L_i(X).$$

L correspond au polynôme interpolateur de Lagrange envoyant les nombres $0, \dots, p-1$ sur les nombres $P(0), \dots, P(p-1)$. En effet, on vérifie que

$$L_i(x) = \begin{cases} 1 & \text{si } x = i \\ 0 & \text{si } x \in \{0, \dots, p-1\} \setminus \{i\} \end{cases}, \quad L(x) = P(x) \text{ pour } x = 0, \dots, p-1.$$

Comme les coefficients des L_i sont inversibles modulo p, le polynôme L admet un représentant également noté L qui est un polynôme à coefficients dans $\{0, \dots, p-1\}$. Le polynôme $L(X) - P(X)$ admet p racines distinctes modulo p, donc soit il est nul, soit il est de degré $\geqslant p$.

- ➢ Si $P - L = Q$ est non nul, alors $\deg P = \deg(Q + L)$. Comme $\deg Q \geqslant p$ car il admet p racines distinctes modulo p et est non nul, et que $\deg L \leqslant p - 1$, on a $\deg P \geqslant p$, ce qui conclut.
- ➢ Si $P \equiv L \mod p$, alors $\deg P = \deg L$. Il suffit alors de vérifier que $\deg L = p - 1$, et donc de calculer son coefficient dominant. Pour cela, on constate que $j \in \{0, \dots, p-1\} \mapsto i - j \mod p$ est une bijection, et donc que $\{i, i-1, \dots, i-(p-1)\} \setminus \{0\} = \{1, \dots, p-1\}$. Ainsi, d'après le théorème de Wilson, pour tout i,

$$\frac{1}{\prod_{j \neq i}(i - j)} \equiv \frac{1}{(p-1)!} \equiv -1 \mod p.$$

Il vient que le coefficient deominant de L vaut

$$\sum_{i=0}^{p-1} \frac{P(i)}{\prod_{j \neq i}(i - j)} \equiv -\sum_{i=0}^{p-1} P(i) \mod p.$$

Il s'agit d'une somme de p termes compris entre 0 et 1, dont au moins un terme $(P(0))$ vaut 0 et un terme $(P(1))$ vaut 1. Donc cette somme est non nulle modulo p, ce qui veut dire que $\deg L = p - 1$, donc $\boxed{\deg P = p - 1}$. Cela conclut.

Solution alternative
La preuve suivante est plus astucieuse. Elle se base sur l'idée assez générale de sommer les informations à disposition, et de calculer cette somme de deux façons différentes. Notons en effet que $P(0)+\ldots+P(p-1)$ somme de p termes compris entre 0 et 1, dont au moins un terme ($P(0)$) vaut 0 et un terme ($P(1)$) vaut 1. Donc cette somme est non nulle modulo p.

D'autre part, écrivons $P(X)=a_dX^d+\ldots+a_1X+a_0$. On a

$$P(0)+\ldots+P(p-1)=\sum_{i=0}^{d}a_i(0^i+\ldots+(p-1)^i).$$

Or, d'après 3.38, pour tout $i\leqslant p-2$, $\boxed{0^i+\ldots+(p-1)^i\equiv 0 \mod p}$. Donc, si $d\leqslant p-2$, on trouve que $P(0)+\ldots+P(p-1)\equiv 0 \mod p$, ce qui contredit le premier paragraphe. Ainsi $\boxed{\deg P\geqslant p-1}$.

Exercice 3.44. Soient x, y, z et p quatre entiers tels que p est premier et $0<x<y<z<p$. On suppose que x^3, y^3 et z^3 ont même reste modulo p. Montrer que $x+y+z$ divise $x^2+y^2+z^2$.

Solution 3.44. D'après l'hypothèse, x,y et z sont les racines modulo p du polynôme X^3-x^3. Posons $(X-x)(X-y)(X-z)=X^3-aX^2+bX-xyz$. On a donc

$$X^3-aX^2+bX-xyz\equiv X^3-x^3 \mod p,$$

ce qui implique que $p\mid a$ et $p\mid b$. D'autre part, on a l'encadrement $0<a<3p$, donc $\boxed{a=p \text{ ou } a=2p}$.

Or, $x^2+y^2+z^2=a^2-2b$, et comme $p\mid b$, $a\mid 2p\mid 2b$, donc $\boxed{a\mid x^2+y^2+z^2}$, comme voulu.

Exercice 3.45. (Envoi 20219-2020) Soient $m,n\geqslant 2$ des entiers tels que

$$a^n\equiv 1 \mod m$$

pour tout entier $a=1,2,\ldots,n$. Montrer que m est premier et que $n=m-1$.

Solution 3.45. Tout d'abord, on a $n<m$, sinon on aurait $m\in\{1,\ldots,n\}$ puis $1\equiv m^n\equiv 0 \mod m$, ce qui est absurde.
Supposons d'abord que m est premier. Le polynôme X^n-1 admet donc $1,\ldots,n$ comme racines, de sorte que d'après les relations de Viète,

$$0\equiv 1+\ldots+n\equiv\frac{n(n+1)}{2} \mod m.$$

On déduit que $m\mid n(n+1)$, donc soit $m\mid n$ soit $m\mid n+1$. Comme $n<m$, on déduit qu'on a $\boxed{n=m-1}$.

Montrons désormais que m est premier. Soit p un diviseur premier de m. Alors on a $a^n\equiv 1 \mod p$ pour $a=1,\ldots,n$. Le paragraphe précédent implique que $n=p-1$. Cela implique que p est l'unique facteur premier de m, c'est-à-dire que m est une puissance de p, et l'on peut écrire $m=p^k$. Or, si $k\geqslant 2$, on aurait $(p-1)^{p-1}\equiv 1 \mod p^2$. Pourtant, la formule du binôme implique que

$$(p-1)^{p-1}=1-p(p-1)+\sum_{i=2}^{p-1}\binom{p-1}{i}p^i(-1)^{p-1-i}\equiv 1+p \mod p^2.$$

On a donc une contradiction, ce qui implique que $k\leqslant 1$, donc $\boxed{m=p}$ est premier.

Exercice 3.46. (Iran MO 2024 Round 3) Soit p un nombre premier et $k\geqslant 1$ un entier. Soit P un polynôme à coefficients dans $\{0,1,\ldots,p-1\}$. On suppose que P est le polynôme de plus petit degré vérifiant la propriété suivante : on peut placer les entiers $1,2,\ldots,p-1$ dans un certain ordre autour d'un cercle de sorte que, pour tous k entiers consécutifs $a_1,\ldots,a_k$, on a

$$p\mid P(a_1)+\ldots+P(a_k).$$

Montrer qu'il existe un entier d, des entiers a et b et un polynôme Q à coefficients entiers de degré strictement inférieur à d tel que $P(X)=aX^d+b+pQ(X)$.

Solution 3.46.

➢ **Commentaire :**

> Il faut commencer par utiliser que les nombres sont autour d'un cercle. Le geste classique consiste à regarder un paquet de k nombres, puis le paquet décalé d'un cran. Ceci donne que $P(b_i) \equiv P(b_{i+k}) \mod p$. La suite est donc périodique, et on peut en extraire la plus petite période, à savoir $\delta = \mathrm{PGCD}(k, p-1)$. On obtient donc que $P(X) - P(b_1)$ admet $\dfrac{p-1}{\delta}$ racines, ce qui donne une minoration du degré de P comme $d \geqslant \dfrac{p-1}{\delta}$. La propriété de minimalité de P permet d'obtenir l'inégalité inverse. Ceci permet de faire la première moitié du problème.

Soit P un polynôme vérifiant la propriété de l'énoncé. Quitte à effectuer la division euclidienne de k par $p-1$, on peut supposer que $1 \leqslant k \leqslant p-1$.

Notons $b_1, \dots, b_{p-1}$ les entiers sur le cercle dans cet ordre. Pour tout indice i, en appliquant la propriété à $b_1, \dots, b_k$ puis à $b_2, \dots, b_{k+1}$, on trouve

$$p \mid P(b_1) + \dots + P(b_k),\ p \mid P(b_2) + \dots + P(b_{k+1}) \\ \Longrightarrow p \mid (P(b_2) + \dots + P(b_{k+1})) - (P(b_1) + \dots + P(b_k)) = P(b_{k+1}) - P(b_1).$$

Ainsi, $P(b_{k+1}) \equiv P(b_1) \mod p$ et, de la même façon, on montre que $\boxed{P(b_{i+k}) \equiv P(b_i) \mod p}$ pour tout i, où les indices sont pris modulo $p-1$. Notons alors $\delta = \mathrm{PGCD}(k, p-1)$ et u tel que $k = \delta u$. Notons u^{-1} l'inverse de u modulo $p-1$ (qui existe car $\mathrm{PGCD}(u, p-1) = 1$), de sorte que $ku^{-1} \equiv \delta u u^{-1} \equiv \delta \mod p-1$. Alors pour tout i, en itérant la congruence ci-dessus, on trouve

$$P(b_i) \equiv P(b_{i+k}) \equiv P(b_{i+2k}) \equiv \dots \equiv P(b_{i+ku^{-1}}) = P(b_{i+\delta}) \mod p.$$

La suite $\boxed{(P(b_i))_i \text{ est donc périodique de période } \delta}$.

Posons $d = \dfrac{p-1}{\delta}$. Le polynôme $P(X) - P(b_1)$ admet donc $b_1, b_{1+\delta}, \dots, b_{1+(d-1)\delta}$ comme racines modulo P. On a donc $\deg P \geqslant d$. D'autre part, le polynôme $Q(X) = X^d$ vérifie la propriété de l'énoncé : soit g un générateur modulo p. En plaçant les nombres $g^0, g^1, g^2, \dots, g^{p-2}$ (pris modulo p) dans cet ordre, on trouve que pour tous k entiers consécutifs $g^i, \dots, g^{i+k-1}$, on a (dans le cas où $d \neq p-1$)

$$\begin{aligned} Q(g^i) + \dots + Q(g^{i+k-1}) &= g^{di} + g^{di+d} + \dots + g^{di+d(k-1)} \\ &= g^{di}(1 + g^d + \dots + g^{d(k-1)}) \\ &= g^{di}\frac{g^{dk}-1}{g^d-1} \\ &\equiv g^{di}\frac{1-1}{g^d-1} \equiv 0 \mod p, \end{aligned}$$

où on a utilisé que $dk = \frac{p-1}{\delta}k = (p-1)\frac{k}{\delta}$ est divisible par $p-1$.

Dans le cas $d = p-1$, $Q(X) = X$ et $Q(b_1) + \dots + Q(b_k)$ correspond à la somme $1 + \dots + (p-1)$, qui est bien divisible par p. On a donc montré que Q satisfaisait toujours la propriété. Par minimalité du degré de P, $\boxed{\deg P = d}$.

➢ **Commentaire :**

> Pour montrer que $P(X) \equiv aX^d + b \mod p$, il faut montrer que les coefficients non dominant ou constants de $P(X)$ sont nuls. Pour cela, on peut commencer par regarder le coefficient devant X^{d-1}. Comme on a la factorisation
>
> $$P(X) \equiv a(X - b_i)(X - b_{i+\delta}) \dots (X - b_{i+(d-1)\delta}) + P(b_i) \mod p.$$
>
> pour tout i, les relations de Viète donnent que le coefficient devant X^{d-1} vaut $s = b_i + \dots + b_{i+(d-1)\delta}$, et qu'il ne dépend pas de $i \in [\![1, \delta]\!]$. On a donc

$$\delta s = (b_1 + \ldots + b_{1+(d-1)\delta}) + \ldots + (b_\delta + \ldots + b_{\delta+(d-1)\delta}) = 1 + \ldots + (p-1) \equiv 0 \mod p,$$

et donc $s = 0$.

Le point important pour obtenir que les coefficients suivants sont nuls est de penser à ne pas travailler que sur $b_1, \ldots, b_{1+(d-1)\delta}$, mais sur tous les b_i.

Montrons que $P(X) \equiv aX^d + b \mod p$. Soit a le coefficient dominant de P. Pour tout $i \leqslant d$, on a la factorisation

$$P(X) - P(b_i) \equiv a(X - b_i)(X - b_{i+\delta}) \ldots (X - b_{i+(d-1)\delta}) \mod p.$$

On déduit que les polynômes $(X - b_i)(X - b_{i+\delta}) \ldots (X - b_{i+(d-1)\delta})$ et $(X - b_1)(X - b_{1+\delta}) \ldots (X - b_{1+(d-1)\delta})$ ont les mêmes coefficients devant $X^{d-1}, \ldots, X$. On dispose donc d'entiers $a_{d-1}, \ldots, a_1$ et $c_1, \ldots, c_\delta$ tels que, pour tout i,

$$Q_i(X) = (X - b_i)(X - b_{i+\delta}) \ldots (X - b_{i+(d-1)\delta}) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + c_i.$$

On a alors

$$Q_1(X) \ldots Q_\delta(X) = (X - 1) \ldots (X - (p-1)) \equiv X^{p-1} - 1 \mod p.$$

Soit $\ell \geqslant 1$ le plus petit indice tel que $a_\ell \neq 0 \mod p$. On a alors

$$(X^d + a_\ell X^\ell + \ldots + c_1) \ldots (X^d + a_\ell X^\ell + \ldots + c_\delta) \equiv X^{p-1} - 1 \mod p.$$

En développant le terme de gauche et en comparant les coefficients devant le monôme $X^{\ell\delta}$, on trouve $0 \equiv \delta a_\ell$, soit $a_\ell \equiv 0 \mod p$, ce qui est une contradiction. On déduit que $a_1 \equiv \ldots \equiv a_{d-1} \equiv 0 \mod p$.

Exercice 3.47. (BXMO 2021) Une suite $a_1, a_2, \ldots$ d'entiers vérifie $a_1 > 5$ et $a_{n+1} = 5 + 6 + \ldots + a_n$ pour tout entier positif n. Déterminer tous les nombres premiers p tels que, quelque soit la valeur de a_1, la suite contient un multiple de p.

Solution 3.47. **Réponse :** $p = 2$ est le seul nombre premier solution.

➢ **Commentaire :**

La formule sur a_n se réécrit $a_{n+1} = \dfrac{a_n(a_n+1)}{2} - 10$. Une astuce très instructive, pour s'assurer que tous les termes sont non nuls modulo p, est de chercher à ce **qu'ils soient tous égaux** à un terme non nul modulo p. Cela revient à chercher a_1 non nul tel que $a_1 = \dfrac{a_1(a_1+1)}{2} - 10$, et donc à chercher a_1 racine d'une équation polynomiale.

Cette équation polynomiale correspond à

$$x = \frac{x(x+1)}{2} - 10 \iff x^2 - x - 20 = 0 \iff (x-5)(x+4) = 0.$$

La première équation n'ayant de sens modulo p que si 2 est inversible, il faudra encore distinguer le cas $p = 2$.

De manière générale, pour contrôler les valeurs d'une suite, on peut chercher un terme de départ comme le point fixe de la relation de récurrence, pour que la suite soit constante.

Supposons que p est impair. Prenons $a_1 \equiv -4 \mod p$, de sorte que $a_1 \equiv \dfrac{a_1(a_1+1)}{2} - 10 \equiv a_2 \mod p$. Par récurrence immédiate, on obtient que $a_n \equiv a_1 \mod p$ pour tout indice n, donc la suite (a_n) est non nulle modulo p, et $\boxed{p \text{ n'est pas une solution}}$.

➢ **Commentaire :**

Dans le cas $p = 2$, on veut montrer que toute suite contient un nombre pair. Pour cela, on regarde à quelle condition sur a_1 impair le terme a_2 est également impair. Il faut en effet que $\dfrac{a_1(a_1+1)}{2}$ soit impair, donc que $a_1 \equiv 1 \mod 4$. De même, pour que a_3 soit impair, il faut que $a_2 \equiv 1 \mod 4$. Mais pour que $a_2 \equiv 1 \mod 4$, il faut que $a_1 \equiv 5 \mod 8$. De même, pour que a_4 soit impair, il faut que $a_2 \equiv 5 \mod 8$.

On peut encore pousser les calculs : pour que $a_2 \equiv 5 \mod 8$, il faut que $a_1 \equiv 5 \mod 16$, et on peut se

convaincre qu'il faudra $a_1 \equiv 5 \mod 2^n$ pour tout n, conduisant à $a_1 = 5$, ce qui est exclus. Il reste à mettre en forme.

Supposons que $p = 2$. Montrons que toute suite (a_n) contient un nombre pair. Pour cela, on suppose que a_1 est impair. On dispose d'un entier $\alpha \geqslant 1$ et d'un entier β impair tel que $a_1 = 2^\alpha \beta + 5$. On a alors

$$a_2 = \frac{a_1(a_1+1)}{2} - 10 = (2^\alpha\beta + 5)(2^{\alpha-1}\beta + 3) - 10 = 2^{\alpha-1}(2^\alpha\beta^2 + 11\beta) + 5.$$

Par récurrence immédiate, on déduit que pour tout indice $\ell \leqslant \alpha$, il existe un entier β_ℓ tel que $a_\ell = 2^{\alpha-\ell+1}\beta_\ell + 5$. On déduit que le nombre $a_{\alpha+1}$ est pair. Donc $\boxed{\text{2 n'est pas solution}}$.

Exercice 3.48. (IMO SL 2020 N2) Soit p un nombre premier. Le royaume de $p-$Land consiste en p îles numérotées de 1 à p. Deux îles distinctes de numéros n et m sont reliées par un pont si et seulement si p divise l'entier $(n^2 - m + 1)(m^2 - n + 1)$; les ponts ne peuvent pas se croiser, mais peuvent passer l'un en-dessous de l'autre). Montrer qu'il existe une infinité de nombres premiers p pour lesquels le royaume de $p-$Land contient deux îles qui ne sont pas reliées par une suite de ponts.

Solution 3.48.

➢ **Commentaire :**

Une façon simple de s'assurer qu'il existe deux entiers qui ne sont pas reliés est de choisir p tel qu'il existe un entier a qui n'est relié à personne. Ce n'est pas vraiment possible, puisque a et $-a$ sont toujours reliés à $a^2 + 1$. En revanche, il est plus raisonnable de demander que a et $-a$ ne sont reliés à aucun autre entier. Cela revient à chercher **un point fixe** de $x \mapsto x^2 + 1$, c'est-à-dire une racine du polynôme $X^2 - X + 1$. Il reste à vérifier qu'un tel polynôme admet bien une infinité de facteurs premiers, et donc qu'il admet une racine modulo une infinité de facteurs premiers.

Soit p un nombre premier, dont on suppose qu'il vérifie que le polynôme $X^2 - X + 1$ admet une racine modulo p, notée a. Comme on a $(-a)^2 + 1 \equiv a^2 + 1 \equiv a \mod p$, les îles de numéro a et $-a$ sont reliées.

Montrons qu'il n'existe aucune autre île reliée à $-a$ ou à a. Supposons que cela soit le cas d'une île de numéro b. Alors soit $a \equiv b^2 + 1 \mod p$, soit $a^2 + 1 \equiv b \mod p$. Comme on n'est pas dans le second cas, c'est qu'on a $b^2 + 1 \equiv a \equiv a^2 + 1 \mod p$. Ainsi, $p \mid b^2 - a^2 = (b-a)(b+a)$. On a donc $b \equiv a \mod p$ ou $b \equiv -a \mod p$, ce qui est exclu. Ainsi, $\boxed{a \text{ et } -a \text{ ne sont reliés à aucune autre ville}}$.

Il reste à voir qu'il existe une infinité de nombres premiers p tels que $X^2 - X + 1$ admette une racine modulo p. C'est une conséquence du lemme de Schur.

$\boxed{\text{Remarque 1 :}}$ On peut également obtenir l'infinité de nombres premiers à la main, en considérant le nombre $(n!)^2 - n! + 1$, dont les facteurs premiers sont tous supérieurs à n. Ainsi, si on a construit r nombres premiers $p_1, \ldots, p_r$ tels que $X^2 - X + 1$ admet une racine modulo ces p_i, on peut en construire un $r+1$-ème en considérant un diviseur premier de $(n!)^2 - n! + 1$, avec $n > \max(p_1, \ldots, p_r)$.

$\boxed{\text{Remarque 2 :}}$ En réalité, tous les premiers p tels que $p \equiv 1 \mod 3$ vérifient que $X^2 - X + 1$ admet une racine modulo p. En effet, le polynôme $X^2 - X + 1$ est de discriminant -3, et si $p \equiv 1 \mod 3$, la loi de réciprocité quadratique (voir sous-sous-section suivante) indique que

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

Donc il existe a tel que $-3 \equiv a^2 \mod p$. Alors on peut résoudre l'équation $x^2 - x + 1 = 0 \mod p$ comme on le ferait dans $\mathbb{R}$, en vérifiant que le nombre $\dfrac{1+\sqrt{-3}}{2} \equiv 2^{-1}(1+a)$ est racine du polynôme donné.

Solution alternative

On peut adopter un point de vue plus combinatoire sur le problème, que l'on peut reformuler en terme de graphe dans lequel les îles sont les sommets, et où les sommets sont reliées par une arête si les îles correspondantes et sont reliées par un pont **et sont distinctes**. Le problème demande s'il existe des nombres premiers p pour lesquels le graphe formé est non connexe.

On dira qu'une arête (m, n) est *engendrée* par n si $n^2 + 1 \equiv m \mod p$. Chaque arête du graphe de notre problème est engendrée par une de ses extrémités, et chaque sommet engendre une unique arête. On a donc montré que $\boxed{\text{notre graphe admet au plus } p \text{ arêtes}}$.

D'autre part, pour que ce graphe soit connexe, il faut qu'il contienne au moins $p-1$ arêtes. Pour qu'il ne soit pas connexe, il suffit donc qu'il existe deux sommets qui n'engendrent aucune arête. C'est le cas des deux sommets qui correspondent aux racines du polynôme $X^2 - X + 1 \mod p$. Si p est tel que ce polynôme admet une racine a, alors les relations de Viète impliquent que $1 - a$ est la seconde solution de l'équation. Pour $a \neq 2^{-1}$, les deux éléments a et $1 - a$ sont distincts modulo p, donc le polynôme admet deux racines distinctes, qui n'engendrent pas d'arêtes. Le graphe a donc au plus $p - 2$ racines et n'est donc pas connexe.

On montre alors l'infinité de nombres premiers p pour lesquels $X^2 - X + 1$ admet une racine modulo p de la même façon que dans la solution 1.

Exercice 3.49. (EMC 2020) Soit p un nombre premier. Alice et Bob jouent au jeu suivant. Alice écrit un entier strictement positif X au tableau et donne une suite $a_1, a_2, \ldots$ infinie à Bob. Bob effectue alors la suite d'opérations suivantes : lors de la $n-$ème opération, Bob remplace l'entier Y écrit au tableau par l'entier $Y + a_n$ ou par l'entier $Y \cdot a_n$.

Bob gagne si, au bout d'un nombre fini d'opérations, le nombre écrit au tableau est un multiple de p. Déterminer si Bob dispose d'une stratégie gagnante quelle que soit la suite d'Alice pour les nombres premiers suivants :

1. $p = 10^9 + 7$?
2. $p = 10^9 + 9$?

Solution 3.49.

➢ **Commentaire :**

> Une fois encore, c'est un problème dans lequel on se rajoute des contraintes en vue de simplifier le problèmes. Ces contraintes s'écrivent sous la forme d'équations polynomiales.
>
> Bob semble a deux choix à chaque tour, ce qui lui laisse énormément de marge de manoeuvre. On peut donc chercher à construire une suite (a_n) qui réduit méchamment l'ensemble des choix possibles pour Bob. C'est par exemple le cas $\boxed{\text{si } a_n \text{ vérifie } a_n \cdot Y \equiv Y + a_n \mod p}$.
>
> Notons Y_n le nombre écrit au tableau au début du tour n de Bob (Notamment $Y_1 = X$). La stratégie pour Alice est donc de choisir $X, a_1, a_2, \ldots$ de sorte que, au tour n de Bob, $Y_n + a_n \equiv Y_n \cdot a_n \mod p$, pour que Bob ne puisse pas choisir. Alice contrôle dans ce cas toutes les valeurs écrites à chaque tour, ce qui lui garantit la victoire.
>
> Choisir a_n tel que $Y_n + a_n \equiv Y_n \cdot a_n \mod p$ revient à prendre $a_n \equiv \dfrac{Y_n}{Y_n - 1} \mod p$, et on a alors $Y_{n+1} = \dfrac{Y_n^2}{Y_n - 1}$. Pour que cela soit possible, il faut que $Y_n \neq 1$. Voir les conditions dans lesquelles on peut s'assurer que $Y_n \neq 1 \mod p$ constitue la suite de l'exercice.
>
> L'équation $Y_n = 1 \mod p$ est équivalente à $Y_{n-1}^2 - Y_{n-1} + 1 \equiv 0 \mod p$. Cette équation n'a pas de solution lorsque $p \equiv 2 \mod 3$, ce qui répond au cas 1. $p = 10^9 + 7$. Cette équation peut en revanche avoir des solutions dans le cas $p = 10^9 + 9$.
>
> La nouvelle idée à avoir dans le cas $p = 10^9 + 9$ est de programmer X pour que (Y_n) ne prenne qu'un nombre restreint de valeurs. Le prototype de cette construction est de choisir X tel que la suite (Y_n) est périodique de période 2, et que $Y_1 = X$ et $Y_2 = \dfrac{X^2}{X - 1}$ soient distincts de 1. Un tel X est solution d'une équation polynomiale, qui admet bien une racine modulo p lorsque $p \equiv 1 \mod 4$, ce qui résoud le cas 2.

Réponse : Alice gagne dans les deux cas.

Dans les deux cas, Alice construit la suite (a_n) par récurrence de la façon suivante : si on note $Y_n = a_{n-1} \ldots a_1 X$ (avec $Y_1 = X$), alors Alice choisit $a_n = \dfrac{Y_n}{Y_n - 1} \mod p$ tant que c'est possible, de sorte que $a_n Y_n = a_n + Y_n \mod p$.

Par récurrence, on montre que Y_n est le nombre écrit au tableau avant le $n-$ème tour de Bob. En effet, $Y_1 = X$ est le nombre écrit au tableau au début du premier tout de Bob, et si Y_n est bien le nombre écrit avant le $n-$ème tour de Bob, comme $a_n + Y_n = a_n \cdot Y_n \mod p$, Bob remplacera Y_n par $Y_n a_n = Y_{n+1}$, ce qui achève la récurrence. On a également de proche en proche que $Y_n \neq 0 \mod p$ pour tout n, ce qui implique que Bob ne peut pas gagner. Il s'agit donc de vérifier qu'Alice peut bien construire une telle suite, et en particulier qu'elle peut choisir X de sorte que $Y_n \neq 1$ pour tout n.

Cas $p = 10^9 + 7$, où on a notamment $p \equiv 2 \mod 3$: Alice commence par choisir X tel que $X \neq 1 \mod p$. Supposons qu'il existe un indice $n \geqslant 1$ tel que $Y_n = 1$. On a donc, en posant $Y = Y_{n-1}$ et puisque $a_{n-1} = \dfrac{Y}{Y-1}$,

$$1 \equiv Y_n \equiv a_{n-1} \cdot Y \equiv \frac{Y^2}{Y-1} \mod p \quad \Longrightarrow Y^2 - Y + 1 \equiv 0 \mod p.$$

On a alors $p \mid Y^2 - Y + 1 \mid Y^6 - 1$, donc l'ordre ω de Y modulo p vérifie $\omega \mid 6$. On a donc $\omega \mid \mathrm{PGCD}(6, p-1)$. Comme $p \equiv 2 \mod 3$, ce PGCD vaut 2, donc $p \mid Y^2 - 1$ et $Y \equiv \pm 1 \mod p$. Or, ni $Y = -1$ ni $Y = 1$ ne vérifient $Y^2 - Y + 1 \equiv 0 \mod p$. $\boxed{\text{L'équation n'a donc pas de solutions modulo } p}$, donc tous les termes de la suite (Y_n) sont différents de 1 modulo p, ce qui permet à Alice d'appliquer sa stratégie.

Cas $p = 10^9 + 9$, où on a notamment $p \equiv 1 \mod 4$: Cherchons X non nul tel que $Y_3 \equiv X \mod p$. Comme $Y_2 \equiv \dfrac{X^2}{X-1} \mod p$ et $Y_3 \equiv \dfrac{Y_2^2}{Y_2 - 1} \mod p$, un tel X vérifie

$$X \equiv \frac{\left(\frac{X^2}{X-1}\right)^2}{\frac{X^2}{X-1} - 1} \mod p \Leftrightarrow 2X^2 - 2X + 1 \equiv 0 \mod p.$$

Puisque $p \equiv 1 \mod 4$, le nombre -1 est un résidu quadratique modulo p. On note i un entier tel que $i^2 \equiv -1 \mod 4$. On peut alors vérifier que $\boxed{X \equiv 2^{-1}(1+i) \mod p}$ est solution de l'équation ci-dessus, et vérifie donc $Y_3 \equiv Y_1$. Par récurrence immédiate, la suite (Y_n) est périodique de période 2 et ne prend que 2 valeurs, à savoir $X = \dfrac{1+i}{2}$ et $\dfrac{X^2}{X-1} = \dfrac{i}{i-1}$. Ces deux nombres sont bien différents de 1 modulo p, ce qui permet à Alice d'appliquer sa stratégie.

➢ **Commentaire :**

> On retiendra de cet exercice deux idées très intéressantes : la recherche de (a_n) telle que Bob ne puisse rien choisir (idée que l'on peut ranger dans la case des idées "s'intéresser aux points fixes d'un protocole"), et l'idée de créer une suite (Y_n) périodique dans le cas 2. Ces deux idées visent à rajouter des contraintes pour paradoxalement simplifier un problème avec beaucoup trop de possibilités.

3.2.2 Résidus quadratiques

Exercice 3.50. Que vaut le reste de la division par p de la somme des résidus quadratiques modulo p ?

Solution 3.50. Les carrés modulo p sont exactement les $\dfrac{p-1}{2}$ racines de $X^{(p-1)/2} - 1$ modulo p. D'après les relations de Viète, leur somme est congrue au coefficient devant $-X^{(p-3)/2}$, à savoir $\boxed{0}$.

Exercice 3.51. Pour quels nombres premiers p le nombre 3 est-il un carré modulo p ? Le nombre 5 ?

Solution 3.51. Si $p = 2$, 3 et 5 sont tous les deux des carrés modulo p. On se restreint désormais aux nombres premiers impairs.
Si $p = 3$, p est bien un carré modulo p. On suppose dans la suite que $p \geqslant 5$. D'après la loi de réciprocité quadratique,

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

Pour que 3 soit un carré modulo p, ce nombre doit donc valoir 1. Or, $\left(\dfrac{p}{3}\right)$ vaut 1 si $p \equiv 1 \mod 3$ et -1 si $p \equiv 2 \mod 3$.

$$(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \mod 12 \\ -1 & \text{si } p \equiv 5 \mod 12 \\ -1 & \text{si } p \equiv 7 \mod 12 \\ 1 & \text{si } p \equiv 11 \mod 12 \end{cases}$$

Ainsi, 3 est un carré modulo p si et seulement si $\boxed{p \equiv \pm 1 \mod 12}$ ou $p = 3$.

On cherche désormais les p tels que 5 est un carré. Si $p = 5$, 5 est bien sûr un carré. On suppose dans la suite que $p \neq 2, 5$ et que 5 est un carré modulo p. D'après la loi de réciprocité quadratique,

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} \Longrightarrow \left(\frac{5}{p}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{5-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right).$$

Pour que 5 soit un carré modulo p, ce nombre doit donc valoir 1. Or, $\left(\frac{p}{5}\right)$ vaut 1 si et seulement si $\boxed{p \equiv 1, 4 \mod 5}$, ce qui conclut.

Exercice 3.52. Soit $p \equiv 1 \mod 4$. Montrer que $p \mid \left(\left(\frac{p-1}{2}\right)!\right)^2 + 1$.

Solution 3.52. D'après le théorème de Wilson,

$$-1 \equiv (p-1)! = \prod_{i=1}^{\frac{p-1}{2}}(p-x)\cdot x \equiv \prod_{i=1}^{\frac{p-1}{2}} -x^2 \equiv (-1)^{\frac{p-1}{2}}\left(\prod_{i=1}^{\frac{p-1}{2}} x\right)^2 = \left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p.$$

Ceci conclut.

Exercice 3.53. (Autriche MO 2024) Déterminer les éléments x de $\{0, 1, \ldots, p-1\}$ tels qu'il existe deux entiers a et b tels que $x \equiv a^2 + b^2 \mod p$.

Solution 3.53. **Réponse :** tous les éléments x peuvent être représentés de cette façon.
Soit $x \in \{0, 1, \ldots, p-1\}$. Les ensembles $A = \{a^2 \mod p, a \in [\![0, p-1]\!]\}$ et $B = \{x - a^2 \mod p, a \in [\![0, p-1]\!]\}$ contiennent tous les deux $\dfrac{p+1}{2}$ éléments. Comme il s'agit d'ensemble inclus dans $[\![0, p-1]\!]$, on a

$$|A \cap B| = |A| + |B| - |A \cup B| \geqslant \frac{p+1}{2} + \frac{p+1}{2} - p = 1.$$

Ainsi, il existe un élément y appartnent à A et B, ce qui implique qu'il existe un entier a et un entier b tels que $a^2 \equiv y \equiv x - b^2 \mod p$, ce qui est bien la congruence voulue.

Exercice 3.54. (Olympiade Abel 2025, Norvège) Pour quels entiers positifs a existe-t-il une infinité d'entiers n tels que $n! - a$ est un carré parfait.

Solution 3.54. **Réponse :** Non.

Soit a un tel entier. Soit p un diviseur premier de a. Il existe un entier n tel que $n! - a$ est un carré parfait et tel $p^{v_p(a)+1} \mid n!$. On déduit que $v_p(n! - a) = v_p(a)$, et comme $n! - a$ est un carré, $v_p(a)$ est pair. Comme c'est le cas pour tout nombre premier, $\boxed{a \text{ est un carré parfait}}$, que l'on note b^2.

Soit $p > a$ un nombre premier tel que $p \equiv 3 \mod 4$ (il existe une infinité de p premiers tels que $p \equiv 3 \mod 4$, donc on peut choisir un tel p qui vérifie $p > a$). Soit alors $n > p$ tel que $n! - a$ est un carré parfait, noté c^2. Alors $\boxed{p \mid n! = b^2 + c^2}$. D'après le lemme de la théorie, comme $p \equiv 3 \mod 4$, $p \mid b$ et $p \mid c$, ce qui contredit que $p > a$. Cette contradiction implique qu'il n'existe pas de tel a.

Solution alternative
Une fois que l'on a montré que $a = b^2$, on peut également choisir n tel que $n! - a$ est un carré parfait et $4b^2 \mid n!$. On peut alors écrire $n! = 4b^2k$, donc $n! - a = b^2(4k-1)$. Pour que ce nombre soit un carré parfait, il faut que $4k - 1$ soit un carré parfait, ce qui est absurde car $4k - 1 \equiv 3 \mod 4$.

Exercice 3.55. (BMO SL 2024 N3) Montrer qu'il existe une infinité de nombres premiers divisant un nombre de la forme $2^n + 3^{n+2} + 5^{n+1}$ avec $n \geqslant 1$.

Solution 3.55.
➢ Commentaire :

> Pour que la somme fasse 0 modulo p, on peut chercher des valeurs de n pour que la somme (avec éventuellement des rajouts de signes) fasse 0. Par exemple, on remarque que

$$2 - 3^3 + 5^2 = 0.$$

Il faut donc n tel que $2^n \equiv 2 \mod p$, $3^{n+2} \equiv -3^3 \mod p$ et $5^{n+1} \equiv 5^2 \mod p$. On trouve que $2^{n-1} \equiv 5^{n-1} \equiv 1 \mod p$ et $3^{n-1} \equiv -1 \mod p$. Le critère d'Euler nous invite à prendre $n-1 = \dfrac{p-1}{2}$ et de choisir p tel que $\left(\dfrac{2}{p}\right) = \left(\dfrac{5}{p}\right) = -\left(\dfrac{3}{p}\right) = 1$.

Soit p un nombre premier impair supérieur à 7 tel que $\left(\dfrac{2}{p}\right) = \left(\dfrac{5}{p}\right) = -\left(\dfrac{3}{p}\right) = 1$. On pose $n = \dfrac{p-1}{2} + 1$. On a alors d'après le critère d'Euler,

$$2^{n-1} \equiv \left(\frac{2}{p}\right) = 1 \mod p, \quad 5^{n-1} \equiv \left(\frac{5}{p}\right) = 1 \mod p, \quad 3^{n-1} \equiv \left(\frac{3}{p}\right) = -1 \mod p,$$

ce qui implique que

$$2^n + 3^{n+2} + 5^{n+1} \equiv 2 + (-1) \cdot 3^3 + 5^2 = 0 \mod p.$$

Il reste à démontrer qu'il existe une infinité de nombres premiers vérifiant $\left(\dfrac{2}{p}\right) = \left(\dfrac{5}{p}\right) = -\left(\dfrac{3}{p}\right) = 1$. D'après la loi de réciprocité quadratique, on a $p \equiv \pm 1 \mod 8$ (pour que 2 soit un carré modulo p), puis

$$\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right)(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{2}} \iff p \equiv \pm 5 \mod 12,$$

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)(-1)^{(p-1)} = 1 \iff p \equiv \pm 1, 4 \mod 5.$$

On trouve en résolvant un des nombreux systèmes chinois possibles que si $p \equiv 41 \mod 120$, alors p vérifie les conditions voulues. D'après le théorème de Dirichlet, il existe une infinité de tels nombres premiers. Ceci conclut l'exercice.

Exercice 3.56. (Iran MO 2015 Round 3/Entraînement D 2021) Soit $p > 5$ un nombre premier et $A = \{b_1, b_2, \ldots, b_{\frac{p-1}{2}}\}$ l'ensemble des résidus quadratiques non nuls modulo p. Montrer qu'il n'existe pas deux entiers a et c premiers avec p tels que les ensembles A et $B = \{ab_1 + c, \ldots, ab_{\frac{p-1}{2}} + c\}$ sont disjoints modulo p.

Solution 3.56. Comme $x \mapsto ax + c$ est injective modulo p, les éléments de B sont deux à deux distincts. Comme A et B sont de cardinal $\dfrac{p-1}{2}$, leur union correspond à $\{0, 1, \ldots, p-1\} \setminus \{r\}$.

La somme des éléments de A est la somme des résidus quadratiques non nuls, à savoir zéro (cf 3.50). Comme la somme des éléments de A, de B et r correspond à la somme des restes modulo p, à savoir 0, on trouve

$$0 = b_1 + b_2 + \ldots + b_{\frac{p-1}{2}} + a(b_1 + b_2 + \ldots + b_{\frac{p-1}{2}}) + \frac{p-1}{2}c + r \equiv r - \frac{c}{2} \mod p.$$

On a donc $\boxed{r \equiv \dfrac{c}{2} \mod p}$. On applique le même procédé mais cette fois-ci avec la somme des carrés des éléments. Dans cette somme, chaque carré non nul apparaît deux fois, si bien que

$$r^2 + b_1^2 + b_2^2 + \ldots + b_{\frac{p-1}{2}}^2 + (ab_1 + c)^2 + \ldots + (ab_{\frac{p-1}{2}} + c)^2 = 2\left(1^2 + \ldots + \left(\frac{p-1}{2}\right)^2\right) + 0^2 \equiv 0 \mod p.$$

D'autre part, on a après développement

$$\begin{aligned} &r^2 + b_1^2 + b_2^2 + \ldots + b_{\frac{p-1}{2}}^2 + (ab_1 + c)^2 + \ldots + (ab_{\frac{p-1}{2}} + c)^2 \\ &\qquad = \frac{c^2}{4} + 2\left(b_1^2 + b_2^2 + \ldots + b_{\frac{p-1}{2}}^2\right) + 2ac\underbrace{(b_1 + b_2 + \ldots + b_{\frac{p-1}{2}})}_{=0} + \frac{p-1}{2}c^2 \mod p. \end{aligned}$$

Pour calculer la somme des b_i^2, il suffit d'appliquer les relations de Viète : les b_i sont les racines de $X^{(p-1)/2}-1$. En notant $c_{(p-1)/2},\dots,c_0$ les coefficients de ce polynôme, les relations de Viète donne

$$b_1^2+b_2^2+\ldots+b_{\frac{p-1}{2}}^2 = c_{(p-3)/2}-2c_{(p-5)/2}\equiv 0 \mod p,$$

car $p>5$. En revenant au calcul ci-dessus, on déduit que

$$0\equiv \frac{c^2}{4}+\frac{p-1}{2}c^2\equiv -\frac{c^2}{4} \mod p.$$

Cela implique que $c\equiv 0 \mod p$, ce qui est exclu par l'énoncé. Cette contradiction conclut l'exercice.

Exercice 3.57. (RMM 2013 P1) Soit a un entier strictement positif. On définit la suite $x_1,x_2,\dots$ par $x_1=a$ et $x_{n+1}=2x_n+1$ pour tout $n\geqslant 1$. On pose également $y_n=2^{x_n}-1$ pour tout $n\geqslant 1$. Déterminer le plus grand entier k tel qu'il existe un entier $a\geqslant 1$ pour lequel $y_1,\dots,y_k$ sont premiers.

Solution 3.57. **Réponse :** Le plus grand entier est $k=2$.

➢ Commentaire :

> Pour mettre en défaut le fait qu'un nombre est premier, on peut soit exhiber une diviseur numérique, soit exhiber un diviseur parmi les nombres manipulés. On en vient à étudier $y_i \mod x_i$.

Soit k un entier solution et a tel que $y_1,\dots,y_k$ sont premiers. Puisque $2^{x_i}-1$ est premier, x_i est également premier pour $i=1,\dots,k$.

Si $a=2$, alors $x_2=5$ et $x_3=11$, et $2^{x_3}-1=2^{11}-1=23\cdot 89$. On peut donc supposer dans la suite que a est impair.

On a alors $x_2=2a+1$ et $x_3=4a+3$. D'où $2^{x_2}-1=2^{2a+1}-1=2^{\frac{x_3-1}{2}}-1$. Or d'après le critère d'Euler,

$$2^{x_2}=2^{\frac{x_3-1}{2}}\equiv\left(\frac{2}{x_3}\right) \mod x_3.$$

Comme a est impair, $x_3\equiv 7 \mod 8$, donc 2 est un carré modulo x_3 d'après la loi de réciprocité quadratique. On déduit que $2^{x_2}\equiv 1 \mod x_3$, donc $x_3 \mid y_3$ et $y_2=x_3$, soit $2^{2a+1}-1=4a+3$. Comme cette équation n'a pas de solution en regardant modulo 8, on déduit que $\boxed{k\leqslant 2}$.

Réciproquement, pour $a=2$, $y_1=3$ et $y_2=31$ sont bien premiers, donc $k=2$ est bien atteignable, ce qui finit le problème.

Exercice 3.58. (APMO 2014) Trouver les entiers $n\geqslant 1$ tels que pour tout entier k, il existe a tel que $n\mid a^3+a-k$.

Solution 3.58. **Réponse :** Il s'agit des puissances de 3.

Soit n un entier solution et surtout soit p un diviseur premier de n. Comme a^3+a est toujours pair, 2 ne vérifie pas l'énoncé pour $k=1$, donc $2\neq p$.

Considérons la fonction $f: x\mapsto x^3+x \mod p$. D'après l'énoncé, cette fonction doit être surjective de $\{0,\dots,p-1\}$ dans $\{0,\dots,p-1\}$. Il s'agit d'une surjection d'un ensemble dans lui-même, donc c'est une bijection. Puisque $f(0)=0$, on s'intéresse à la restriction de f à $\{1,\dots,p-1\}$, qui est à nouveau une bijection. Ainsi,

$$1\cdot\ldots\cdot(p-1)\equiv f(1)\dots f(p-1)\equiv 1(1^2+1)\dots(p-1)((p-1)^2+1)=(p-1)!\prod_{a=1}^{p-1}(a^2+1) \mod p.$$

En simplifiant par $(p-1)!$ qui est non nul, on déduit que $\prod_{a=1}^{p-1}(a^2+1)\equiv 1 \mod p$. Calculons ce produit dans le cas général. Introduisons $P(X)=X^{(p-1)/2}-1=\prod_{a=1}^{(p-1)/2}(X-a^2)$, le polynômes dont les racines sont les carrés. On a alors

$$\prod_{a=1}^{p-1}(a^2+1)=\prod_{a=1}^{(p-1)/2}(a^2+1)^2=\left(\prod_{a=1}^{(p-1)/2}(-1-a^2)\right)^2\equiv P(-1)^2 \mod p.$$

Mais

$$P(-1)^2 = ((-1)^{(p-1)/2} - 1)^2 = \begin{cases} 0 & \text{si } p \equiv 1 \mod 4 \\ 4 & \text{si } p \equiv 3 \mod 4 \end{cases}$$

On déduit que $1 \equiv 4 \mod p$ et que $\boxed{p = 3}$. On déduit que le seul diviseur premier de n est 3 puis que $\boxed{n \text{ est une puissance de } 3}$.

Réciproquement, posons $n = 3^r$. On montre que n est solution par récurrence sur r.

Initialisation : Si $r = 1$, alors $f(0) \equiv 0 \mod 3$, $f(1) \equiv 2 \mod 3$ et $f(2) \equiv 1 \mod 3$, donc f est une bijection de $\{0, 1, 2\}$ dans lui-même modulo 3, ce qui suffit à faire de 3 une solution.

Hérédité : On suppose que $n = 3^r$ est solution. Soit k un entier et a tel que $3^r \mid a^3 + a - k$. Considérons $b = a + c3^r$, avec c à choisir plus tard. On a

$$b^3 + b - k = a^3 + a - k + 3^{r+1}a^2c + 3^{2r+1}ac^2 + c^3 3^{3r} + c3^r = (a^3 + a - k + c3^r) + 3^{r+1}(a^2c + 3^r ac^2 + c^3 3^{2r-1}).$$

En choisissant c tel que $3 \mid \dfrac{a^3 + a - k}{3^r} + c$, on trouve b tel que $3^{r+1} \mid b^3 + b - k$, ce qui achève la récurrence et conclut.

Exercice 3.59. (BMO 2025 P1) Un entier $n \geqslant 1$ est dit *bon* s'il existe une permutation $a_1, a_2, \ldots, a_n$ des entiers $1, 2, \ldots, n$ telle que

- ➢ Les nombres a_i et a_{i+1} sont de parité différente pour tout $1 \leqslant i \leqslant n-1$.
- ➢ La somme $a_1 + \ldots + a_k$ est un carré modulo n pour tout indice $1 \leqslant k \leqslant n$.

Montrer qu'il existe une infinité d'entiers bons et une infinité d'entiers qui ne sont pas bons.

Solution 3.59. Existence d'une infinité d'entiers pas bons :

➢ Commentaire :

> Une information simple à aller chercher est que la somme des n nombre doit être un carré, soit $1 + \ldots + n = \dfrac{n(n+1)}{2}$ est un carré modulo n. Il reste à trouver une infinité de n tels que ce n'est pas le cas.

Soit $n = 8k + 4$ un entier. Montrons que n n'est pas bon. On suppose pour cela qu'il existe une permutation tendant n bon. On a alors

$$a_1 + \ldots + a_n = 1 + \ldots + n = \frac{n(n+1)}{2} = (4k+2)(8k+5) \equiv 4k + 2 \mod 8k + 4.$$

Puisque cette somme est un carré modulo $8k + 4$, elle est en particulier un carré modulo 4. Mais cette somme vaut 2 modulo 4, qui n'est pas un carré. D'où la contradiction.

Existence d'une inifnité d'entiers bons :

➢ Commentaire :

> Dans un tel problème (construction d'un entier n avec un gros cahier des charges), trois idées sont à envisager :
>
> - ➢ Chercher n sous la forme d'un nombre premier,
> - ➢ mettre par pair de deux les entiers a_i,
> - ➢ chercher à forcer/contrôler un maximum des termes $a_1, a_1 + a_2, \ldots, a_1 + \ldots + a_n$, par exemple, pour qu'elle prenne peu de valeurs différentes. Cette idée est bien sûr connectée à l'idée précédente : si on a bien choisi les paires (a_{2i-1}, a_{2i}), les sommes partielles seront faciles à calculer.
>
> Une fois qu'on a collecté ces trois idées, on tente les partitions de $\{1, \ldots, p-1\}$ en paires que l'on connaît, et on choisit p pour que cette partition fonctionne. La première condition du problème rajoute une condition pour bien concaténer les paires.

Soit $p \equiv 3 \mod 4$ un nombre premier. Montrons que p est bon.

On considère la partition $\{1, \ldots, p\}$ en $\{(p), (1, p-1), (2, p-2), \ldots, (x, p-x), \ldots \left(\dfrac{p-1}{2}, \dfrac{p+1}{2}\right)\}$. Pour tout x, on a $\left(\dfrac{p-x}{p}\right) = \left(\dfrac{-x}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{x}{p}\right) = -\left(\dfrac{x}{p}\right)$, (où on a utilisé que $\left(\dfrac{-1}{p}\right) = -1$ car $p \equiv 3 \mod 4$).

Donc exactement l'un des deux entiers de la paire $(x, p-x)$ est un carré modulo p. On note b_x ce nombre, et c_x l'autre nombre de la paire.

Notons $A = \{1 \leqslant x \leqslant \frac{p-1}{2}, b_x \text{ est impair}\} = \{x_1, \ldots, x_k\}$ et $B = \{x_{k+1}, \ldots, x_{(p-1)/2}\}$ son complémentaire. On choisit alors la permutation

$$(b_{x_1}, c_{x_1}, \ldots, b_{x_k}, c_{x_k}, p, b_{x_{k+1}}, c_{x_{k+1}}, \ldots, b_{x_{(p-1)/2}}, c_{x_{(p-1)/2}}).$$

On vérifie que modulo 2, cette permutation vaut $(1, 0, \ldots 1, 0, 1, 0, 1, \ldots, 1, 0)$, donc le premier item est bien respecté.

D'autre part, pour tout ℓ, on a

$$\underbrace{b_{x_1} + c_{x_1}}_{\equiv 0} + \ldots + b_{x_\ell} \equiv b_{x_\ell} \mod p, \quad \underbrace{b_{x_1} + c_{x_1}}_{\equiv 0} + \ldots + \underbrace{b_{x_\ell} + c_{x_\ell}}_{\equiv 0} \equiv 0 \mod p,$$

Comme en plus $b_{x_1} + \ldots + c_{x_k} + p \equiv 0 \mod p$, toutes els sommes partielles valent 0 ou un b_x qui est bien un carré, donc toutes les sommes partielles sont des carrés modulo p. Le nombre p est donc bon.

Exercice 3.60. (Iran TST 2020) Soit $p \geqslant 5$ un nombre premier impair. Déterminer tous les $\frac{p-1}{2}-$uplets $(x_1, \ldots, x_{(p-1)/2})$ d'éléments de $\{0, \ldots, p-1\}$ tels que

$$\sum_{i=1}^{\frac{p-1}{2}} x_i \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^2 \equiv \ldots \equiv \sum_{i=1}^{\frac{p-1}{2}} x_i^{\frac{p-1}{2}} \mod p.$$

Solution 3.60. **Réponse :** Les $\frac{p-1}{2}-$uplets d'entiers appartenant à $\{0, 1\}$.

Notons A la valeur commune des $\frac{p-1}{2}$ somme. Pour tout polynôme $P(X) = a_d X^d + \ldots + a_0$ de degré $d \leqslant \frac{p-1}{2}$, on trouve

$$\sum_{i=1}^{\frac{p-1}{2}} P(x_i) = \sum_{k=0}^{d} a_k \sum_{i=1}^{\frac{p-1}{2}} x_i^k \equiv \frac{p-1}{2} P(0) + (a_1 + \ldots + a_d)A \mod p \equiv \frac{p-1}{2} P(0) + (P(1) - P(0))A \mod p.$$

Il faut désormais appliquer ce principe au bon polynôme P.

➢ **Commentaire :**

> Plusieurs tentatives sont raisonnables. On peut vouloir appliquer l'hypothèse à un bon polynôme interpolateur de Lagrange des x_i (par exemple celui valant 1 en x_1 et 0 en les x_i qui lui sont distincts), mais le membre de droite ne s'exprime alors pas très bien.
>
> Si l'on abandonne cette piste, on doit garder à l'esprit que pour utiliser pleinement toutes les hypothèses, notre polynôme doit être de degré $(p-1)/2$. D'autre part, sa valeur en 0 et sa valeur en 1 doivent être faciles à calculer. Enfin, le critère d'Euclide indique qu'une puissance $(p-1)/2$-ème prend très peu de valeurs. Le choix du polynôme $P(X) = (X-r)^{(p-1)/2}$ est alors tout indiqué.

Posons $d = \frac{p-1}{2}$. Soit r un entier de $\{1, \ldots, p-1\}$ et $P(X) = (X-r)^d$. On a alors

$$\sum_{i=1}^{d} (x_i - r)^d \equiv d(-r)^d + ((1-r)^d - (-r)^d)A \mod p.$$

En simplifiant par $-r^d$ et en posant $t = -r^{-1}$, on obtient

$$\sum_{i=1}^{d} (1 + t x_i)^d \equiv d + ((1+t)^d - 1)A \mod p.$$

Notons que la fonction qui à r associe t est bien une bijection de $\{1, \ldots, p-1\}$ dans lui-même modulo p, donc chaque choix de t peut être déterminé par un unique entier r. En prenant t tel que $1 + t$ est un

résidu quadratique, le membre de droite vaut d. Le membre de gauche est une somme de d nombres compris entre -1 et 1, et la seule possibilité pour que leur somme vaille d est qu'ils vaillent tous 1. On déduit que $\boxed{\text{si } 1+t \text{ est un carré (différent de 1), } 1+tx_i \text{ est un carré pour tout } x_i}$.

Fixons un x_i non nul. La fonction $1+t \mapsto 1+tx_i$ est une bijection de $\{0,\dots,p-1\}\setminus\{1\}$ dans lui-même. Ainsi, lorsque $1+t$ parcourt l'ensemble des carrés (différents de 1), $1+tx_i$ parcourt également l'ensemble des carrés (différents de 1). Si $1+t$ est un carré a^2, alors $1+tx_i = 1+x_i(a^2-1)$. La somme de ces carrés vaut -1 (la somme des carrés modulo p vaut 0), donc en sommant sur toutes les valeurs de a différentes de 1,

$$-1 \equiv \sum_{a=2}^{(p-1)/2} a^2 \equiv \sum_{a=2}^{(p-1)/2} 1+x_i(a^2-1) \equiv \frac{p-3}{2}(1-x_i)+x_i(-1) \mod p \iff (x_i-1)d \equiv 0 \mod p.$$

On déduit que $\boxed{x_i = 1}$. Ainsi, on a montré que tous les x_i valent soit 0 soit 1.

Réciproquement, tous les $\dfrac{p-1}{2}-$uplets composés de 1 et de 0 vérifient la propriété.

Exercice 3.61. Soit n un entier (non nécessairement positif) qui est un carré modulo p pour tout nombre premier p. Montrer que n est un carré parfait.

Solution 3.61. Donnons nous un entier n qui n'est pas un carré parfait et trouvons un nombre premier p tel que n n'est pas un carré modulo p. Notons

$$n = (-1)^{\varepsilon} 2^{\alpha} \prod_{i=1}^{r} q_i^{\beta_i}$$

la décomposition en facteurs premiers de n, où les q_i sont des nombres premiers impairs distincts. On pose $A = \{i \in \{1,\dots,r\}, \beta_i \equiv 1 \mod 2\}$ et $B = \{i \in \{1,\dots,r\}, \beta_i \equiv 0 \mod 2\}$. La multiplicativité du symbole de Legendre donne que, pour tout nombre premier impair $p \notin \{q_1,\dots,q_r\}$,

$$\begin{aligned}\left(\frac{n}{p}\right) &= \left(\frac{(-1)^{\varepsilon}2^{\alpha}\prod_{i=1}^{r} q_i^{\beta_i}}{p}\right) = \left(\frac{(-1)^{\varepsilon}2^{\alpha}}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i^{\beta_i}}{p}\right) \\ &= \left(\frac{(-1)^{\varepsilon}2^{\alpha}}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right)^{\beta_i} = \left(\frac{(-1)^{\varepsilon}2^{\alpha}}{p}\right)\prod_{i\in A}\left(\frac{q_i}{p}\right).\end{aligned}$$

On distingue alors deux cas :

➢ Cas 1 : A est vide. On a alors

$$\left(\frac{n}{p}\right) = \left(\frac{(-1)^{\varepsilon}2^{\alpha}}{p}\right).$$

Comme n n'est pas un carré parfait, l'un de ε et de α est impair.

- Si ε est pair et α est impair on prend un nombre premier p vérifiant $p \equiv 5 \mod 8$ et $p \notin \{q_1,\dots,q_r\}$ (un tel nombre premier existe d'après le Théorème 2). On vérifie alors à l'aide du Théorème 1 que

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

de sorte que n n'est pas un carré modulo p.

- Si ε est impair on prend cette fois-ci $p \equiv 7 \mod 8$, et un calcul similaire montre que n n'est pas un carré parfait modulo p.

➢ Cas 2 : A est non vide
Soit $i_0 \in A$. Il existe un résidu a tel que a n'est pas un carré modulo q_{i_0} (il y a $(q_{i_0}-1)/2$ tels résidus). D'après le théorème des restes chinois, il existe un entier m vérifiant

$$\begin{cases} m & \equiv & a & \mod q_{i_0}\ ; \\ m & \equiv & 1 & \mod 8\prod_{i\in[\![1;r]\!]\setminus\{i_0\}} q_i. \end{cases}$$

Notons qu'un tel m est alors premier avec $8\prod_{i=1}^{r} q_i$. D'après le Théorème de Dirichlet, il existe un nombre premier p tel que $p \equiv m \mod 8\prod_{i=1}^{r} q_i$. Un tel nombre premier vérifie alors

$$\left(\frac{n}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)^{\varepsilon}}_{=1}\underbrace{\left(\frac{2}{p}\right)^{\alpha}}_{=1}\prod_{i\in A}\left(\frac{q_i}{p}\right) = \prod_{i\in A}\left(\frac{p}{q_i}\right) = \left(\frac{p}{q_{i_0}}\right)\prod_{i\in A\setminus\{i_0\}}\underbrace{\left(\frac{p}{q_i}\right)}_{=1} = -1\ ,$$

et n n'est pas un carré modulo p.

Exercice 3.62. (ELMO SL 2014 N1) Montrer qu'il existe une suite infinie (a_k) d'entiers telle que, pour tout entier $k \geqslant 1$, $13^k \mid a_k^2 + 1$.

Solution 3.62. Considérons le polynôme $P(X) = X^2 + 1$, dont la dérivée vaut $P'(X) = 2X$. Modulo 13, ce polynôme admet pour racine $a_1 = 5$, qui vérifie $P'(5) \neq 0 \mod 13$. D'après le lemme de Hensel, P admet une racine a_k modulo 13^k, comme voulu.

Exercice 3.63. Soit p un nombre premier, $n \geqslant 1$ et k un entier non divisible par p. Montrer que x est une puissance $k-$ème modulo p si et seulement si x est une puissance $k-$ème modulo p^n.

Solution 3.63. $\boxed{\Leftarrow :}$ Si x est une puissance $k-$ème modulo p^n, c'est en particulier une puissance $k-$ème modulo p.

$\boxed{\Rightarrow :}$ Le polynôme $P(X) = X^k - x$ a pour dérivée $P'(X) = kX^{k-1}$. Comme x est non nul et k est non divisible par p, $P'(x) \neq 0 \mod p$. D'après le lemme de Hensel, le polynôme P admet donc une racine y modulo p^n, ce qui signifie que x est une puissance $k-$ème modulo p^n.

Exercice 3.64. (Thailand TSTST 2021) Un nombre premier p impair est dit *incroyable* si il existe un entier n tel que p^{2022} divise $n^{2022} + 2022$. Montrer qu'il existe une infinité de nombres premiers incroyables.

Solution 3.64. Posons $P(X) = X^{2022} + 2022$. D'après le théorème de Schur, le polynôme P admet une infinité de diviseurs premiers. en particulier, il admet une infinité de nombres premiers qui ne divisent pas 2022. Pour un tel nombre premier p, on choisit n un entier tel que $p \mid P(n)$.

Si on avait $p \mid n$, on aurait $p \mid n \mid P(n) - P(0)$ et donc $p \mid P(0) = 2022$, ce qui est exclu. Ainsi, p ne divise ni n ni 2022, donc $P'(n) \neq 0 \mod p$. D'après le lemme de Hensel, il existe un entier m tel que $p^{2022} \mid P(m)$. Le nombre p est donc incroyable, et on en a bien une infinité.

Exercice 3.65. (IMO 1999 N3) Montrer qu'il existe deux suites strictement croissantes (a_n) et (b_n) telles que, pour tout entier n, $a_n(a_n + 1) \mid b_n^2 + 1$.

Solution 3.65.

➢ **Commentaire :**

> Essayons de créer un couple (a, b) tel que $a(a+1) \mid b^2+1$. Si p est un diviseur premier impair de b^2+1, alors $-1 \equiv b^2 \mod p$, donc -1 est un carré modulo p, ce qui implique que $p \equiv 1 \mod 4$. Ainsi, les facteurs premiers impairs de $b^2 + 1$ sont congrus à -1 modulo 4.
>
> On commence donc par chercher a tel que les facteurs premiers impairs de a et $a + 1$ sont congrus à 1 modulo 4. Pour cela, on peut s'inspirer de notre observation précédente et chercher $a + 1$ de la forme $a + 1 = x^2 + 1$. Pour que $a = x^2$ ait ses facteurs impairs congrus à 1 modulo 4, il reste à prendre $x = y^2 + 1$. Cette partie du problème est très astucieuse, mais très instructive.
>
> Supposons ensuite que l'on a trouvé un tel a, et on construit b. Pour cela, on décompose $a(a + 1) = 2\prod_{i=1}^{r} p_i^{\alpha_i}$. Pour tout i, on cherche y_i tel que $y_i^2 \equiv -1 \mod q_i^{\alpha_i}$, ce qui se construit grâce au lemme de Hensel. Puis, on construit b à partir des y_i à l'aide du théorème des restes chinois.

Soit $n \geqslant 1$ un entier et $a_n = (4n^2 + 1)^2$. On vérifie que si p est un facteur premier de a_n, il est impair et vérifie $p \mid 4n^2 + 1$, donc $-1 \equiv (2n)^2 \mod p$. Puisque -1 est un carré modulo p, on a $p \equiv 1 \mod 4$.

D'autre part, $a_n+1 \equiv 2 \mod 4$, et si p est un diviseur premier impair de a_n+1, alors on a que $-1 \equiv (4n^2+1)^2 \mod 4$, donc on déduit de même que $p \equiv 1 \mod 4$.

En résumé, la décomposition en facteurs premiers de $a_n(a_n+1)$ est $a_n(a_n+1) = 2p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où les p_i vérifient $p_i \equiv 1 mod 4$ pour tout i.

La suite (a_n) est strictement croissante. Supposons avoir construit $b_1 < \dots < b_{n-1}$ tels que $a_k(a_k+1) \mid b_k^2+1$ pour tout $k = 1, \dots, n-1$. Construisons à présent $b_n > b_{n-1}$ tel que $a_n(a_n+1) \mid b_n^2+1$.

Pour tout indice $1 \leqslant i \leqslant r$, $p_i \equiv 1 \mod 4$, donc il existe un entier y_i tel que $p_i \mid y_i^2+1$. D'après le lemme de Hensel, on peut trouver z_i tel que $p_i^{\alpha_i} \mid z_i^2+1$. Enfin, d'après le théorème des restes chinois, il existe un entier b_n (que l'on peut prendre arbitrairement grand, et donc plus grand que b_{n-1}) solution du système :

$$\begin{cases} b_n & \equiv 1 & \mod 2 \\ b_n & \equiv z_i & \mod p_i^{\alpha_i} \quad \text{pour } i = 1, \dots, r \end{cases}$$

On a donc que $a_n(a_n+1) \mid b_n^2+1$. Par construction, les deux suites sont strictement croissantes, ce qui conclut l'exercice.

Remarque : On a construit la suite (b_n) par récurrence, mais on n'a pas présenté l'initialisation dans notre preuve. C'est parce que celle-ci est en quelque sorte contenue dans l'hérédité : si $n = 0$, la condition $b_n > b_{n-1}$ est une condition vide.

3.3 Problèmes de taille, épisode 2 - arguments asymptotiques

Exercice 3.66. (Thaïlande TSTST 2023) Soit $a \geqslant 2$ un entier. Montrer qu'il n'existe pas de fonction $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telle que

$$(m + f(n))^2 \geqslant af(m)^2 + n^2$$

pour tous entiers $m, n \in \mathbb{N}^\star$.

Solution 3.66. Soit f une fonction solution. En fixant m, en divisant l'équation par n et en faisant tendre n vers $+\infty$, on trouve

$$\frac{f(n)}{n} \geqslant \sqrt{\frac{af(m)^2}{n^2} + 1} - \frac{m}{n} \longrightarrow 1.$$

D'autre part, en fixant n, en divisant par m^2 et en faisant tendre m vers $+\infty$, on trouve

$$\frac{f(m)}{m} \leqslant \frac{1}{\sqrt{a}}\sqrt{-\left(1 + \frac{f(n)}{m}\right) - \frac{n^2}{m^2}} \longrightarrow \frac{1}{\sqrt{a}}.$$

Soit $1 > \delta > \dfrac{1}{\sqrt{a}}$. La première inégalité nous dit qu'il existe un rang M tel que si $m \geqslant M$, $f(n)/n > \delta$. La deuxième inégalité nous dit qu'il existe un rang N tel que si $n \geqslant N$, $f(n)/n < \delta$. Ainsi, pour tout $n \geqslant \max(N, M)$, on a $f(n)/n > \delta > f(n)/n$, ce qui est absurde. Il n'y a donc pas de fonction solution.

Exercice 3.67. Soient a et b des entiers tels que a est non nul et $an^2 + b$ est un carré parfait pour tout entier n. Montrer que $b = 0$ et que a est un carré parfait.

Solution 3.67. Pour tout entier $n \geqslant 1$, notons x_n l'entier tel que $an^2 + b = x_n^2$. On a

$$x_{n+1} - x_n = \sqrt{a(n+1)^2 + b} - \sqrt{an^2 + b} = \frac{a[(n+1)^2 - n^2]}{\sqrt{a(n+1)^2 + b} + \sqrt{an^2 + b}} \longrightarrow \sqrt{a}.$$

Comme la suite $(x_{n+1} - x_n)$ est une suite d'entiers sa limite $\sqrt{a}$ est un entier donc $\boxed{a \text{ est un carré parfait}}$. De plus, pour n suffisamment grand, on a

$$(\sqrt{a}n)^2 \leqslant an^2 + n < (\sqrt{a}n + 1)^2,$$

ce qui implique que $(\sqrt{a}n)^2 = an^2 + b$ et $\boxed{b = 0}$.

Exercice 3.68. Soient a et b des entiers tels que $a \cdot 2^n + b$ est un carré parfait pour tout entier $n \geqslant 1$. Montrer que $a = 0$.

Solution 3.68. Supposons par l'absurde que $a \neq 0$. Notons x_n l'entier tel que $a \cdot 2^n + b = x_n^2$. Il est légitime d'étudier la croissance de x_n. En notant que $x_n \sim \sqrt{a}2^{n/2}$, on trouve $x_{n+1} \sim \sqrt{2}x_n$. Pour faire apparaître des entiers, il faut étudier étudier $x_{n+2} - 2x_n$:

$$x_{n+2} - 2x_n = \sqrt{a \cdot 2^n \cdot 4 + b} - \sqrt{4 \cdot a \cdot 2^n + 4b} = \frac{-3b}{\sqrt{a \cdot 2^n \cdot 4 + b} + \sqrt{4a \cdot 2^n + 4b}} \longrightarrow 0,$$

où on a utilisé que $a \neq 0$ pour établir cette limite. Comme la suite $(x_{n+2} - 2x_n)$ est une suite d'entiers, on déduit qu'elle est nulle à partir d'un certain rang N. Mais alors $\sqrt{a \cdot 2^n \cdot 4 + b} = \sqrt{4 \cdot a \cdot 2^n + 4b}$, soit $3b = 0$ et $b = 0$. Mais alors $a2^N$ et $a2^{N+1}$ sont tous les deux des carrés, ce qui est absurde car leur valuation $2-$adique sont de parité opposée. On déduit que $a = 0$.

Exercice 3.69. (Concours 18 MT P6/création de Gaëtan Dautzenberg) Trouver tous les polynômes P à coefficients entiers tels qu'il existe des entiers strictement positifs $a < b < c < d$ vérifiant la propriété suivante : pour tout entier $k \geqslant 1$, le nombre $P(ak) + P(bk)$ est non nul et

$$P(ak) + P(bk) \mid P(ck) + P(dk).$$

Solution 3.69. **Réponse :** Les polynômes de la forme $P(X) = x_d X^d$ avec $x_d \neq 0$ et $d \geqslant 1$.

Notons $P(X) = x_n X^n + \ldots + x_0$ un tel polynôme.
Pour tout entier $k \geqslant 1$, on note N_k l'entier tel que $P(ck) + P(dk) = N_k(P(ak) + P(bk))$. On a

$$N_k = \frac{P(ck) + P(dk)}{P(ak) + P(bk)} = \frac{\frac{P(ck)+P(dk)}{k^n}}{\frac{P(ak)+P(bk)}{k^n}} \longrightarrow \frac{x_n c^n + x_n d^n}{x_n a^n + x_n b^n} = \frac{c^n + d^n}{a^n + b^n}.$$

La suite (N_k) est une suite convergente d'entiers, elle est donc constante égale à $N = \dfrac{c^n + d^n}{a^n + b^n}$ (qui est donc un entier) à partir d'un certain rang ℓ. On déduit que pour tout entier $k \geqslant \ell$,

$$P(ck) + P(dk) = N(P(ak) + P(bk)).$$

Comme le polynôme $P(cX) + P(dX) - N(P(aX) + P(bX))$ s'annule en une infinité d'entiers, il est nul. On a donc $\boxed{P(cX) + P(dX) = N(P(aX) + P(bX))}$. Par identification des coefficients, on trouve que, pour tout exposant i tel que $x_i \neq 0$, $c^i + d^i = N(a^i + b^i)$.
Ainsi, s'il existe $0 \leqslant i \leqslant n-1$ tel que $x_i \neq 0$, on a

$$\frac{c^n + d^n}{a^n + b^n} = N = \frac{c^i + d^i}{a^i + b^i}$$

ce qui est équivalent à

$$(c^{n-i} - a^{n-i})(ac)^i + (d^{n-i} - a^{n-i})(ad)^{n-d} + (c^{n-i} - b^{n-i})(bc)^i + (d^{n-i} - b^{n-i})(bd)^{n-d} = 0.$$

Au vu de l'ordre $a < b < c < d$ supposé, cette dernière égalité ne peut avoir lieu. On déduit que $x_i = 0$ pour tout $1 \leqslant i \leqslant n-1$. Ainsi, $P(X) = x_d X^d$. De plus x_d est non nul car P est non nul pour au moins une valeur.

Réciproquement, si $P(X) = x_d X^d$ pour un certain $x_d \neq 0$ et un certain $d \geqslant 1$, on a bien $P(k) + P(2k) \neq 0$ pour tout $k \geqslant 1$ et

$$P(k) + P(2k) = x_d k^d (1 + 2^d) \mid x_d k^d 3^d (1 + 2^d) = P(3k) + P(6k),$$

donc le quadruplet $(1, 2, 3, 6)$ permet à P de vérifier les conditions de l'énoncé.

Exercice 3.70. (USA TSTST 2021 P4) Soient a et b des entiers strictement positifs. On suppose qu'il existe une infinité de couples (m, n) tels que $m^2 + an + b$ et $n^2 + am + b$ sont tous les deux des carrés parfaits. Montrer que a divise $2b$.

Solution 3.70. Notons $(m_1, n_1), (m_2, n_2), \ldots$ les couples solutions.

Étape 1 : Les suites $(m_r)_r$ et $(n_r)_r$ tendent vers $+\infty$.

Commençons par remarquer que, pour un m fixé, il existe un nombre fini de valeurs n telles que $n^2 + am + b$ soit un carré, en vertue de l'encadrement $n^2 < n^2 + am + b < (n+1)^2$ qui est vérifié lorsque $n > (am + b - 1)/2$. En particulier, en , on obtient qu'aucune des deux suites $(m_r)_r$ et $(n_r)_r$ ne peut être bornée. Ainsi, les deux suites divergent.

Pour tout couple (m_r, n_r), on a par définition deux entiers k_r et ℓ_r tels que

$$\begin{cases} m_r^2 + an_r + b &= (m_r + k_r)^2 \\ n_r^2 + am_r + b &= (n_r + \ell_r)^2 \end{cases} \iff \begin{cases} an_r + b &= 2k_r m_r + k_r^2 \\ am_r + b &= 2\ell_r n_r + \ell_r^2 \end{cases}$$

Étape 2 : Montrons que $(k_r)_r$ et $(\ell_r)_r$ sont bornées et admettent une sous-suite constante.

Supposons, quitte à échanger les lettres, que $m_r \leqslant n_r$. On déduit que $2\ell_r n_r \leqslant am_r + b \leqslant an_r + b$. Pour n_r suffisamment grand, cela implique que $2\ell_r \leqslant a$. La suite (ℓ_r) est bornée, on dispose donc, d'après le principe

des tiroirs, d'un entier ℓ tel que $\boxed{\ell_r = \ell}$ pour une infinité d'indices r. Dans la suite, on ne considère que ces indices. La deuxième égalité implique que

$$2\ell n_r + \ell^2 \leqslant am_r + b \quad \Longrightarrow \quad n_r \leqslant \frac{a}{2\ell} m_r + \frac{b-\ell^2}{2\ell}.$$

En réinjectant dans la première équation cette inégalité, on trouve

$$2k_r m_r \leqslant an_r + b \leqslant \frac{a^2}{2\ell} m_r + b + a\frac{b-\ell^2}{\cdot}$$

Cette inégalité implique, lorsque m_r est suffisamment grand, que $2k_r \leqslant a^2/2\ell$. La suite (k_r) est donc bornée et on dispose donc, d'après le principe des tiroirs, d'un entier k tel que $\boxed{k_r = k}$ pour une infinité d'indices r. Dans la suite, on ne considère que ces indices.

Étape 3 : On prouve que $a^2 = 4k\ell$ et on conclut (avec un peu de bidouillage).

On revient à notre système d'équations, qui donne

$$\begin{cases} an_r + b &= 2km_r + k^2 \\ am_r + b &= 2\ell n_r + \ell^2 \end{cases} \quad \Longrightarrow \quad (4k\ell - a^2)m = 2\ell(b-k^2) - a(\ell^2 - b).$$

Si $4k\ell - a^2 \neq 0$, alors le membre de gauche est non borné lorsque r tend vers $+\infty$, alors que le membre de droite est constant. On déduit que $\boxed{a^2 = 4k\ell}$. L'entier a est donc pair et on introduit un entier c tel que $a = 2c$, et donc $c^2 = k\ell$. L'égalité ci-dessus devient, après simplification,

$$b(\ell + c) = c\ell^2 + c^2 k.$$

Notons $d = \mathrm{PGCD}(k, \ell)$ et $k = dx, \ell = dy$. Comme $xy = (c/d)^2$ et que x et y sont premiers entre eux, ce sont tous les deux des carrés, et on pose $x = x_1^2$ et $y = y_1^2$. Alors $c = dx_1y_1$ et l'équation se simplifie encore en

$$b(dy_1^2 + dx_1y_1) = dx_1y_1d^2y_1^4 + d^2x_1^2y_1^2dx_1^2 \quad \Longleftrightarrow \quad b(y_1 + x_1) = d^3x_1y_1^2(y_1^3 + x_1^3) = d^3x_1y_1^2(y_1^2 - y_1x_1 + x_1^2).$$

On déduit que $c = dx_1y_1 \mid b$ puis que $\boxed{a = 2c \mid 2b}$ comme voulu.

Exercice 3.71.

1. Soit $(a_n), (b_n), (c_n)$ et (d_n) des suites non nulles. On suppose que $a_n \sim b_n$ et $c_n \sim d_n$. Montrer que $a_nc_n \sim b_nd_n$.
2. Soit (a_n) et (b_n) deux suites non nulles qui tendent vers $+\infty$ et telles que $a_n \sim b_n$. Montrer que $\ln a_n \sim \ln b_n$.
3. Soit (a_n) et (b_n) deux suites telles que $a_n - b_n \longrightarrow 0$. Montrer que $2^{a_n} \sim 2^{b_n}$.
4. En prenant $a_n = n^2 + n$ et $b_n = n^2$, vérifier que l'implication de la question précédente est fausse si on remplace l'hypothèse $a_n - b_n \longrightarrow 0$ par l'hypothèse $a_n \sim b_n$.
5. Soient $(a_n), (b_n), (c_n)$ et (d_n) des suites à valeurs strictement positives. On suppose que $a_n \sim b_n$ et $c_n \sim d_n$. Montrer que $a_n + c_n \sim b_n + d_n$.

Solution 3.71.

1. Par produit des limites,
$$\frac{a_nc_n}{b_nd_n} = \frac{a_n}{b_n} \cdot \frac{c_n}{d_n} \longrightarrow 1.$$
2. Pour n suffisamment grand, $b_n > 1$ donc $\ln b_n \neq 0$. Alors
$$\frac{\ln a_n}{\ln b_n} = \frac{\ln b_n + \ln(a_n/b_n)}{\ln b_n} = 1 + \frac{\ln(a_n/b_n)}{\ln b_n} \longrightarrow 1.$$
3. On a
$$\frac{2^{a_n}}{2^{b_n}} = 2^{a_n - b_n} \longrightarrow 1.$$

4. Avec $a_n = n^2 + n$ et $b_n = n^2$, on a bien $a_n \sim b_n$, en revanche
$$\frac{2^{a_n}}{2^{b_n}} = 2^n \longrightarrow +\infty,$$
donc on n'a pas $2^{a_n} \sim 2^{b_n}$.
5. On utilise que si $a_n \sim b_n$ et $c_n \sim d_n$, alors $a_n = b_n + o(b_n)$ et $c_n = d_n + o(d_n)$. On a alors
$$\frac{a_n + c_n}{b_n + d_n} = 1 + \frac{a_n - b_n}{b_n + d_n} + \frac{c_n - d_n}{b_n + d_n}.$$
Comme (b_n) et (d_n) sont positives, on a
$$\left|\frac{a_n - b_n}{b_n + d_n}\right| \leqslant \frac{|a_n - b_n|}{b_n} = \frac{1}{b_n} o(b_n) = o(1).$$
et de même $\dfrac{c_n - d_n}{b_n + d_n} = o(1)$. On a donc $\dfrac{a_n + c_n}{b_n + d_n} \longrightarrow 1$ et $a_n + c_b \sim b_n + d_n$

Exercice 3.72. (RMM 2024 P4) Soient a et b des entiers strictement plus grands que 1. Pour tout entier $n \geqslant 1$, on note r_n le reste de la division euclidienne de b^n par a^n. On suppose qu'il existe un entier $N \geqslant 1$ tel que $r_n < \dfrac{2^n}{n}$ pour tout entier $n \geqslant N$. Montrer que a divise b.

Solution 3.72. On effectue la division euclidienne de b^n par a^n : pour tout indice $n \geqslant 1$, on note q_n et r_n les entiers tels que $0 \leqslant r_n < a^n$ et $b^n = q_n a^n + r_n$.
Un bon geste dans ces situations est de confronter les relations obtenues pour deux indices consécutifs. On a en effet à n fixé, en regardant modulo a^n,
$$r_{n+1} \equiv b^{n+1} = b(q_n a^n + r_n) \equiv b r_n \mod a^n.$$
Notre but est de convertir cette congruence en égalité. Pour n suffisamment grand, par croissance comparée, $br_n < b\frac{2^n}{n} < a^n$ (il suffit de choisir $n > b$ et d'utiliser que $2 \leqslant a$). De même, $r_{n+1} < \dfrac{2^{n+1}}{n+1} < a^n$ (il suffit d'avoir $n + 1 > 2$). Donc r_{n+1} et br_n sont tous les deux dans l'intervalle $[\![0, a^n - 1[\![$ et sont congrus. On déduit qu'on dispose d'un rang N (et on a même montré qu'on pouvait prendre $N = b + 1$) tel que $\boxed{r_{n+1} = br_n}$ pour tout indice $n \geqslant N$.
On a alors, pour tout $n \geqslant N$, $r_n = b^{n-N} r_N$. Par croissance comparée à nouveau, si $r_N > 0$, l'inégalité
$$b^n \frac{r_N}{b^N} < \frac{2^n}{n},$$
est fausse pour n suffisamment grand. Cette absurdité conduit à $r_N = 0$, soit $a^N \mid b^N$. On déduit que $\boxed{a \mid b}$.

Exercice 3.73. (IMO P4 2019) Déterminer toutes les paires d'entiers (k, n) strictement positifs telles que

$$k! = (2^n - 1)(2^n - 2)(2^n - 4)\dots(2^n - 2^{n-1}).$$

Solution 3.73. **Réponse :** Les paires sont $(1, 1)$ et $(3, 2)$.

➢ **Commentaire :**

> La gymnastique est la suivante, et sans surprise elle combine arguments de divisbilité et arguments de taille : une grande puissance de 2 divise le membre de droite, ce qui force k à être grand. Mais si k est grand $k!$ est grand, et peut-être trop grand par rapport au membre de droite.

Pour tout $i = 0, \dots, n-1$, $v_2(2^n - 2^i) = 2^i$. On déduit que

$$v_2((2^n - 1)\dots(2^n - 2^{n-1}) = 0 + 1 + \dots + n - 1 = \frac{n(n-1)}{2}.$$

D'autre part, d'après la formule de Legendre et l'inégalité qui en découle,

$$v_2(k!) = \left\lfloor \frac{k}{2} \right\rfloor + \left\lfloor \frac{k}{4} \right\rfloor + \dots \leqslant \frac{k}{2} + \frac{k}{4} + \dots < k.$$

On déduit que $\boxed{k > \frac{n(n-1)}{2}}$.

La formule de Stirling et son inégalité $k! > \left(\frac{k}{3}\right)^k$ ainsi qu'une majoration grossière du membre de droite donnent alors

$$\left(\frac{n(n-1)}{6}\right)^{\frac{n(n-1)}{2}} < k! < 2^n \cdot 2^n \cdot 2^{n-1} < 2^{n(n-1)}.$$

En passant cette inégalité à la racine, on trouve que n doit satisfaire

$$\frac{n(n-1)}{6} < 2^2.$$

Cela implique que $n < 6$. Il reste à tester les valeurs $n = 1, 2, 3, 4$, qui donnent les solutions $(k, n) = (1, 1)$ et $(k, n) = (2, 3)$.

Exercice 3.74. (IMO SL 2011 A2) Déterminer tous les $2011-$uplets $(x_1, \dots, x_{2011})$ d'entiers strictement positifs tels que, pour tout entier n, il existe un entier a_n tel que

$$x_1^n + 2x_2^n + \dots + 2011x_{2011}^n = a_n^{n+1} + 1.$$

Solution 3.74. **Réponse :** En notant $k = 2 + \dots + 2011$, le seul $2011-$uplet solution est $(1, k, \dots, k)$.

Tout d'abord, on vérifie que la suite (a_n) est bornée. Soit M le maximum des x_i. Pour tout entier $n \geqslant 1$, on a

$$a_n^{n+1} + 1 = x_1^n + 2x_2^n + \dots + 2011x_{2011}^n \leqslant M^n + 2M^n + \dots + 2011M^n \leqslant (k+1)M^n \leqslant \max(k+1, M)^{n+1}.$$

On déduit que $a_n \leqslant \max(k+1, M)$. D'après le principe des tiroirs infini, il existe un entier a et une infinité d'entiers n pour lesquels $a_n = a$. On travaille uniquement avec ces indices n par la suite. Notons que $a > 1$, puisque le membre de gauche de l'énoncé est supérieur à $k + 1$. Pour les indices n mis en évidence, l'équation se réécrit, en divisant par a^n :

$$a + \frac{1}{a^n} = \sum_{i=1}^{2011} i \left(\frac{x_i}{a}\right)^n.$$

Comme $a > 1$, le côté gauche tend vers a lorsque $n \to +\infty$, donc il en est de même du côté droit. Or,

$$\left(\frac{x_i}{a}\right)^n \longrightarrow \begin{cases} +\infty & \text{si } x_i > a \\ 1 & \text{si } x_i = a \\ 0 & \text{si } x_i < a \end{cases}$$

On déduit que $x_i \leqslant a$ pour tout i (sinon le membre de droite tendrait vers $+\infty$ avec n). Notons $A = \{a \in [\![1, 2011]\!], x_i = a\}$ l'ensemble des indices i tels que $x_i = a$ et B sont complémentaire. En passant à la limite l'équation ci-dessus, on trouve

$$a = \sum_{i \in A} i.$$

Mais alors

$$a^{n+1} + 1 = \sum_{i \in A} i x_i^n + \sum_{i \in B} i x_i^n = \sum_{i \in A} i a^n + \sum_{i \in B} i x_i^n = a^{n+1} + \sum_{i \in B} i x_i^n.$$

On déduit que $B = \{1\}$. Ainsi, $(x_1, \ldots, x_{2011}) = (1, k, \ldots, k)$.
Réciproquement, ce $2011-$uplet est bien solution puisque

$$1^n + 2 \cdot k^n + \ldots + 2011 k^n = 1 + (2 + \ldots + 2011) k^n = 1 + k^{n+1},$$

donc $a_n = k$ convient.

Exercice 3.75. Trouver les polynômes P à coefficients entiers tels que, pour tout entier n, le nombre $P(n)$ est un palindrome.

Solution 3.75. **Réponse :** Il s'agit des polynômes constants égaux à un nombre palindrome.

Supposons que P ne soit pas constante et notons d son degré et a_d son coefficient dominant. On note $s_n = \lceil \log_{10}(P(n)) \rceil \sim \log_{10}(P(n))$ le nombre de chiffres de $P(n)$.
Tout d'abord, puisque $10 \mid P(n+10) - P(n)$, la suite $(P(n))_n$ est périodique modulo 10. Supposons d'abord qu'elle n'est pas constante modulo 10 : on peut trouver deux entiers consécutifs n et $n+1$ tels que le chiffre b des unités de $P(n+k)$ et le chiffre c des unités de $P(n)$ sont distincts et vérifient $b/(c+1) > 1$. Notons qu'alors b et c sont également les premiers chiffres respectifs de $P(n+k)$ et $P(n)$. L'idée est de déduire que P croît trop vite pour une croissance polynomiale.
En prenant n suffisamment grand, on peut supposer que $P(n+k) > P(n)$, de sorte que $s_{n+1} \geqslant s_n$. On a ensuite

$$\frac{P(n+k)}{P(n)} \geqslant \frac{b 10^{s_{n+1}}}{(c+1) 10^{s_n}} \geqslant \frac{b}{c+1} > 1.$$

Ce résultat étant vrai en remplaçant n par $n+10a$ pour tout a, il est vrai pour une infinité d'entiers n. Pourtant, de $P(n) \sim a_d n^d$, on déduit que

$$\frac{P(n+k)}{P(n)} \sim \frac{a_d (n+k)^d}{a_d n^d} \to 1,$$

ce qui contredit l'inégalité ci-dessus.

On déduit que $P(n)$ est constant modulo 10 et on note b cette constante. Comme $P(n)$ tend vers $+\infty$, on dispose d'une infinité d'indices n tels que $s_{n+1} > s_n$. On a pour ces entiers

$$\frac{P(n+k)}{P(n)} \geqslant \frac{b 10^{s_{n+1}}}{(b+1) 10^{s_n}} \geqslant 10 \frac{b}{b+1} > 1.$$

On a là encore un contradiction avec $P(n+k) \sim P(n)$. Ainsi $\boxed{P \text{ est constant}}$.

Exercice 3.76. *(P6 EGMO 2021)* Existe-t-il un entier $a \geqslant 0$ tel que l'équation

$$\left\lfloor \frac{m}{1} \right\rfloor + \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{3} \right\rfloor + \ldots + \left\lfloor \frac{m}{m} \right\rfloor = n^2 + a$$

admet plus de un million de solutions différentes (m, n) pour lesquelles m et n sont des entiers strictement positifs ?

Solution 3.76. **Réponse :** Il existe un tel entier.
➢ **Commentaire :**

> Notons S_m le membre de gauche. La première chose à identifier, c'est que $S_m \sim m \ln m$.
>
> La deuxième chose, c'est que puisque d'eventuels n et m solution ont vocation à être grand, on peut supposer qu'ils sont grands devant a et chercher n en fonction de m comme le plus grand entier tel que $n^2 \leqslant S_m$, soit $n_m = \lfloor \sqrt{S_m} \rfloor \sim \sqrt{m \ln m}$.
>
> On a alors l'encadrement $S_m - n_m^2 \leqslant (n_m+1)^2 - n_m^2 \sim 2\sqrt{m \ln m} = o(m)$. Donc lorsque m est grand, les m entiers $S_1 - n_1^2, \ldots, S_m - n_m^2$ sont tous majorées par $2\sqrt{m \ln m}$ (qui est un petit nombre par rapport à m). On peut appliquer le principe des tiroirs pour dire que beaucoup de ces nombres prennent la même valeurs a. Il reste à calibrer.

Notons $S_m = \left\lfloor \frac{m}{1} \right\rfloor + \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{3} \right\rfloor + \ldots + \left\lfloor \frac{m}{m} \right\rfloor$. L'inégalité $x - 1 < \lfloor x \rfloor \leqslant x$ conduit à l'encadrement

$$m\left(1 + \frac{1}{2} + \ldots + \frac{1}{m}\right) - m \leqslant S_m \leqslant m\left(1 + \frac{1}{2} + \ldots + \frac{1}{m}\right),$$

ce qui, avec l'équivalent $1 + \frac{1}{2} + \ldots + \frac{1}{m} \sim \ln m$ conduit à $\boxed{S_m \sim m \ln m}$. En particulier, pour m suffisamment grand, on a l'encadrement $\dfrac{1}{2} m \ln m S_m < 2m \ln m$.

Pour tout entier m, on pose $n_m = \lfloor \sqrt{S_m} \rfloor$, correspondant au plus grand entier n tel que $n^2 \leqslant S_m$. On a alors l'encadrement

$$0 \leqslant S_m - n_m^2 < (n_m + 1)^2 - n_m^2 = 2n_m + 1 \leqslant 2\sqrt{m \ln m} + 1.$$

Posons $M = 10^6$ et prenons m un entier suffisamment grand pour que $\dfrac{m}{2\sqrt{m \ln m} + 1} > M$, ce qui est possible par croissance comparée. D'après le principe des tiroirs appliqué au m chaussettes $S_1 - n_1^2, \ldots, S_m - n_m^2$ dans les $\lceil 2\sqrt{m \ln m} + 1 \rceil + 1$ tiroirs $[\![0, \lceil 2\sqrt{m \ln m} + 1 \rceil + 1]\!]$, il existe un entier $a \leqslant \lceil 2\sqrt{m \ln m} + 1 \rceil + 1$ tel qu'au moins $\dfrac{m}{2\sqrt{m \ln m} + 1} > M$ nombres $S_k - n_k^2$ prennent la valeur a. Les couples (k, n_k) constituent alors plus de M solutions à l'équation de problème, ce qui conclut.

Exercice 3.77. (EMC 2014/Mexico Regional 2021) Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs telle que

- ➢ pour tous indices m et n, $a_{mn} = a_m a_n$.
- ➢ il existe une infinité d'entiers n tels que $(a_1, \ldots, a_n)$ est une permutation de $(1, 2, \ldots, n)$.

Montrer que $a_n = n$ pour tout indice n.

Solution 3.77. On procède par récurrence forte sur n.

Initialisation : La première relation implique que $a_1 = a_1^2$, donc $a_1 = 1$.

Hérédité : On suppose que $a_k = k$ pour tout indice $k \leqslant n-1$. On souhaite montrer que $a_n = n$. Notons d'abord $a_n = N$. Soit $m \geqslant n$ un indice tel que $\{1, \ldots, m\} = \{a_1, \ldots, a_m\}$. On déduit déjà que N ne peut pas valoir $1, \ldots, n-1$, sinon $(a_1, \ldots, a_m)$ ne serait pas une permutation de $(1, \ldots, m)$, donc $\boxed{N \geqslant n}$. De plus, d'après la première relation, pour tout $k \leqslant \left\lfloor \frac{m}{n} \right\rfloor$, $a_n \mid a_{kn}$, donc l'ensemble $\{a_1, \ldots, a_m\}$ contient au moins $\left\lfloor \frac{m}{n} \right\rfloor$ multiples de $a_n = N$. Or, l'ensemble $\{1, \ldots, m\}$ contient exactement $\left\lfloor \frac{m}{N} \right\rfloor$ multiples de N. Comme ces deux ensembles sont égaux, on déduit l'inégalité

$$\left\lfloor \frac{m}{N} \right\rfloor \geqslant \left\lfloor \frac{m}{n} \right\rfloor.$$

Cette égalité est vraie pour une suite infinie (m_ℓ) d'entiers m, et on a en passant à la limite :

$$\frac{1}{N} = \lim_{\ell \to \infty} \frac{1}{m_\ell} \left\lfloor \frac{m_\ell}{N} \right\rfloor \geqslant \lim_{\ell \to \infty} \frac{1}{m_\ell} \left\lfloor \frac{m_\ell}{n} \right\rfloor = \frac{1}{n} \quad \Longrightarrow \quad \boxed{N \leqslant n}.$$

Comme on a en plus $N \geqslant n-1$, on déduit que $a_n = N = n$, ce qui achève la récurrence.

Exercice 3.78. (IMO 2024 P1) Déterminer tous les réels α tels que, pour tout entier n strictement positif, l'entier

$$\lfloor \alpha \rfloor + \lfloor 2\alpha \rfloor + \ldots + \lfloor n\alpha \rfloor$$

soit un mutiple de n. (On rappelle que $\lfloor z \rfloor$ désigne le plus grand entier inférieur ou égal à z. Par exemple, $\lfloor -\pi \rfloor = -4$ et $\lfloor 2 \rfloor = \lfloor 2.9 \rfloor = 2$.)

Solution 3.78. **Réponse :** Tous les entiers pairs.

Notons S_n la somme $\lfloor \alpha \rfloor + \lfloor 2\alpha \rfloor + \ldots + \lfloor n\alpha \rfloor$. En employant l'encadrement $x - 1 < \lfloor x \rfloor \leqslant x$, on trouve

$$\frac{n+1}{2}\alpha - 1 = \frac{\alpha - 1 + 2\alpha - 1 + \ldots + n\alpha - 1}{n} < \frac{S_n}{n} \leqslant \frac{\alpha + 2\alpha + \ldots n\alpha}{n} = \frac{n+1}{2}\alpha.$$

Puisque $\dfrac{S_n}{n}$ est un entier, on déduit de cet encadrement que

$$\frac{S_n}{n} = \left\lfloor \frac{n+1}{2}\alpha \right\rfloor.$$

D'autre part, pour tout entier n, on a

$$\frac{S_{n+1}}{n+1} - \frac{S_n}{n} = S_n \left(\frac{1}{n+1} - \frac{1}{n} \right) + \frac{\lfloor (n+1)\alpha \rfloor}{n+1} = -\frac{n \left\lfloor \frac{n+1}{2}\alpha \right\rfloor}{n(n+1)} + \frac{\lfloor (n+1)\alpha \rfloor}{n+1}.$$

En utilisant que, pour tout réel x, $\dfrac{\lfloor nx \rfloor}{n} \to x$ lorsque $n \to +\infty$, on vérifie que

$$\frac{S_{n+1}}{n+1} - \frac{S_n}{n} \longrightarrow \frac{\alpha}{2}.$$

Puisque la suite $\frac{S_{n+1}}{n+1} - \frac{S_n}{n}$ est à valeurs entières, on déduit que $-\dfrac{\alpha}{2}$ est un entier. Ainsi, les seules solutions possibles sont les entiers pairs. Réciproquement, si α est un entier pair, on a pour tout entier $n \geqslant 1$

$$\sum_{k=1}^{n} \lfloor k\alpha \rfloor = \sum_{k=1}^{n} k\alpha = \frac{\alpha}{2} n(n+1)$$

qui est bien divisible par n.

Exercice 3.79. (IMO SL 2011 N2) Soient $d_1, \dots, d_9$ des entiers distincts et soit $P(x) = (x+d_1)(x+d_2)\cdot\ldots\cdot(x+d_9)$. Montrer qu'il existe un entier $N \geqslant 1$ tel que pour tous les entiers $x \geqslant N$, le nombre $P(x)$ est divisible par un nombre premier plus grand que 20.

Solution 3.79.

➢ **Commentaire :**

> L'idée est de remarquer qu'il y a 8 nombres premiers inférieurs ou égaux à 20 et d'appliquer le principe des tiroirs puisque qu'il y a 9 facteurs.
> Pour deviner l'entier N à choisir, on commence naïvement par procéder par l'absurde : On suppose qu'il existe une infinité d'entiers n tels que $P(n)$ n'admet que des facteurs premiers inférieurs ou égaux à 20. Pour un tel entier n, on dispose donc de deux indices i et j et d'un nombre premier p parmi les nombres $2, 3, 5, 7, 11, 13, 17, 19$ tels que p divise $n+d_i$ et $n+d_j$. Ainsi, p divise $d_i - d_j$.
>
> A partir de cette remarque, on propose la preuve suivante.

On suppose par l'absurde que l'on dispose d'une suite (x_n) d'entiers strictement positifs tels que les nombres $P(x_n)$ n'admettent pas de facteurs premiers strictement supérieurs à 20.
La suite $(x_n+d_1)_n$ n'est pas bornée, on dipose donc d'un nombre premier $p_1 < 20$ tel que la suite $(v_{p_1}(x_n+d_1))_n$ ne soit pas bornée non plus. Quitte à extraire une sous-suite y_n de la suite x_n telle que la suite $(v_{p_1}(y_n+d_1))_n$ tende vers $+\infty$, on peut supposer que la suite (x_n) satisfait déjà cette propriété.

A nouveau, quitte à extraire de la suite (x_n), on peut supposer que l'on dispose de nombres premiers $p_2, \dots p_9$ tels que la suite $(v_{p_i}(x_n+d_i))_n$ tende vers $+\infty$ pour tout entier i.
D'après le principe des tiroirs, on dispose de deux indices i et j tels que $p_i = p_j$, que l'on note désormais p. Ainsi, les suites $(v_p(x_n+d_i))_n$ et $(v_p(x_n+d_j))_n$ tendent toutes les deux vers $+\infty$. En particulier, on dispose d'un entier n tel que $v_p(x_n+d_i) > v_p(d_i-d_j)$ et $v_p(x_n+d_j) > v_p(d_i-d_j)$. En notant $k = v_p(d_i-d_j)$, on déduit que p^{k+1} divise x_n+d_j et x_n+d_i mais pas d_i-d_j, ce qui donne la contradiction attendue.

Exercice 3.80. (OFM 2021 Senior) Soient $a_1, a_2, \dots$ et $b_1, b_2, \dots$ deux suites satisfaisant respectivement, pour tout $n \geqslant 1$, $a_{n+2} = a_{n+1} + a_n$ et $b_{n+2} = b_{n+1} + b_n$. On suppose que a_n divise b_n pour une infinité d'indices n. Montrer qu'il existe un entier c tel que $a_n = cb_n$ pour tout entier $n \geqslant 1$.

Solution 3.80. La solution naturelle, si l'on connaît la méthode de résolution des suites récurrentes linéaires, est la suivante.
Notons $\varphi = \dfrac{1+\sqrt{5}}{2}$ et $\psi = \dfrac{1-\sqrt{5}}{2}$. On dispose de quatre constantes A, B, C et D telles que, pour tout entier n,

$$a_n = A\varphi^n + B\psi^n, \quad b_n = C\varphi^n + D\psi^n.$$

On déduit que $a_n \sim A\varphi^n$ et $b_n \sim B\varphi^n$. On ne considère désormais que les indices n tels que $b_n \mid a_n$. La suite a_n/b_n converge donc vers la constante A/C. On dispose alors d'un rang N tel que, si $n \geqslant N$, alors $a_n/b_n = A/C = c$. Comme $b_n \mid a_n$, le nombre c est un entier. On a donc $\boxed{a_n = cb_n \text{ pour } n \geqslant N}$.
L'ensemble des indices n tels que $a_n \neq cb_n$ est donc majoré par N. S'il est non vide, on note n_0 son plus grand élément. Alors

$$a_{n_0} = a_{n_0+2} - a_{n_0+1} = c(b_{n_0+2} - b_{n_0+1}) = cb_{n_0},$$

une claire contradiction avec l'hypohtèse sur n_0. On a donc $\boxed{a_n = cb_n \text{ pour tout indice } n}$.

Exercice 3.81. (Iran 2024 round 3 P6) Soit P un polynôme à coefficients entiers et positifs ou nuls. On suppose qu'il existe une suite (x_n) d'entiers strictement positifs telle que $x_1 = 1$ et, pour tout indice $n \geqslant 1$,

$$x_{n+1}^2 + P(n) = x_n x_{n+2}.$$

Montrer que P est un polynôme constant.

Solution 3.81. Cet exercice combine les arguments de divisibilités liés au caractère entier de la suite avec le contrôle de la croissance du polynôme P par rapport à la croissance de la suite (x_n).

On suppose que P est non nul. Regardons la relation de récurrence aux indices $n-1$, n et $n+1$, à savoir les trois égalités suivantes :

$$\begin{array}{lcl} x_n^2 + P(n-1) & = & x_{n-1}x_{n+1}; \\ x_{n+1}^2 + P(n) & = & x_n x_{n+2}; \\ x_{n+2}^2 + P(n+1) & = & x_{n+1}x_{n+3}. \end{array}$$

Puisque l'entier x_{n+1} est présent dans les trois équations, il est pertinent de combiner ces trois équations modulo x_{n+1}. On obtient

$$P(n-1) \equiv -x_n^2\,, \quad P(n) \equiv x_n x_{n+2}, \quad P(n+1) \equiv -x_{n+2}^2 \qquad \mod x_{n+1}.$$

On déduit que

$$P(n+1)P(n-1) \equiv x_n^2 x_{n+2}^2 \equiv P(n)^2 \mod x_{n+1}.$$

On a donc montré que x_{n+1} est un diviseur de $P(n)^2 - P(n+1)P(n-1)$.

On montre à présent que lorsque n est suffisamment grand, $x_{n+1} > |P(n)^2 - P(n-1)P(n+1)|$. Puisque P est à coefficients positifs, $P(n)$ est positif pour tout entier n et on trouve que, pour tout entier naturel n,

$$x_n x_{n+2} \geqslant x_{n+1}^2,$$

ce qui se réécrit comme $\dfrac{x_{n+2}}{x_{n+1}} \geqslant \dfrac{x_{n+1}}{x_n}$. Soit d le degré de P et c_d son coefficient dominant. Puisque $x_2 \geqslant 1$, on a

$$\frac{x_3}{x_2} = \frac{x_2}{x_1} + \frac{P(1)}{x_1 x_2} \geqslant 1 + \frac{P(1)}{x_1 x_2}.$$

Notons $c = 1 + \frac{P(1)}{x_1 x_2}$, qui vérifie $c > 1$. En utilisant la croissance de $\left(\dfrac{x_{n+1}}{x_n}\right)$ on a par récurrence immédiate que $x_n \geqslant c^{n-2}$ pour tout entier $n \geqslant 3$. Notons que $P(n)^2 - P(n-1)P(n+1)$ est un polynôme de degré $d-1$, et par croissance comparée, il existe un entier N tel que, pour tout $n \geqslant N$, $|P(n)^2 - P(n-1)P(n+1)| \leqslant n^d < c^{n-2}$. On déduit que

$$|P(n)^2 - P(n-1)P(n+1)| < n^d < c^{n-2} \leqslant x_{n+1}.$$

On déduit que $P(n)^2 = P(n-1)P(n+1)$ pour tout entier n suffisamment grand. Par rigidité, cette égalité devient vraie pour tout entier n. La suite $\left(\dfrac{P(n)}{P(n-1)}\right)$ est donc constante égale à un réel c. Comme P est à coefficients positifs, il est croissant, donc $c \geqslant 1$.

Si $c > 1$, on montre par récurrence immédiate que $P(n) = c^{n-1}P(1)$. Or, pour tout entier n suffisamment grand, par croissance comparée, $P(n) \leqslant n^{d+1}$. On déduit que $c^{n-1}P(1) < n^{d+1}$ pour tout entier n suffisamment grand, ce qui est absurde par croissance comparée.

On déduit que $c = 1$. Mais alors $P(n) = P(n-1)$ pour tout entier n, ce qui implique que tous les entiers n sont racines du polynôme $P(X) - P(0)$, ce qui implique que $P(X) - P(0)$ est le polynôme nul, donc que P est constant.

Remarque : On présente une deuxième façon de montrer que P est constant à partir de l'égalité $P(n)^2 = P(n-1)P(n+1)$ vraie pour tout entier n suffisamment grand. Par rigidité, on a que $P(X)^2 = P(X-1)P(X+1)$. Supposons que P est non constant. Soit α une racine complexe de P (qui existe d'après le théorème de D'Alembert-Gauss). Alors $P(\alpha+1)^2 = P(\alpha)P(\alpha+2) = 0$, donc $\alpha+1$ est également une racine de P. Par récurrence immédiate, $\alpha+n$ est une racine de P pour tout n, ce qui implique que P admet une infinité de racine et qu'il s'agit du polynôme nul, d'où la contradiction.

Exercice 3.82. (Chine TST 2004 P2/France TST 2018-2019) Soit u un entier strictement positif. Montrer qu'il n'existe qu'un nombre fini de triplets (n, α, β) d'entiers strictements positifs tels que $n! = u^\alpha - u^\beta$.

Solution 3.82. Pour que l'équation ait une solution au moins, il faut que $u \geqslant 2$ et que $\alpha > \beta$.

Fixons l'entier n. L'équation s'écrit $n! = u^\beta(u^{\alpha-\beta} - 1)$ et implique, puisque $u \geqslant 2$, $n! \geqslant u^\beta(2^{\alpha-\beta} - 1) \geqslant u^\beta$. Cela implique que β peut prendre un nombre fini de valeurs en fonction de n. Puisque $u^\alpha = n! + u^\beta$, α ne peut également prendre qu'un nombre fini de valeurs possibles. Conclusion, à n fixé, il y a un nombre fini de triplets solutions. Il suffit donc de montrer que l'équation n'a pas de solutions lorsque n est suffisamment grand.

Fixons un entier n assez grand. Soit p le plus petit nombre premier impair ne divisant pas u. Pour n suffisamment grand, $p \leqslant n$, donc $p \mid n!$ et donc $p \mid u^{\alpha-\beta} - 1$. Posons ω l'ordre de u modulo p. On a d'après la divisibilité et le petit théorème de Fermat que $\omega \mid \mathrm{PGCD}(\alpha - \beta, p - 1$. En particulier, $\omega < p$. D'après le lemme LTE, on a

$$v_p(u^{\alpha-\beta} - 1) = v_p(u^k - 1) + v_p((\alpha - \beta)/k) = v_p(u^k - 1) + v_p(\alpha - \beta).$$

Pour tout entier m, puisque $p^{v_p(m)} \leqslant m$, on a $v_p(m) \leqslant \log_p(m)$. On a donc

$$v_p(u^{\alpha-\beta} - 1) \leqslant \log_p(u^k - 1) + \log_p(\alpha - \beta).$$

Puisque $u^{\alpha-\beta} \leqslant n!$, on a d'après la formule de Striling passée au logarithme,

$$\alpha - \beta \leqslant \log_u(n!) \sim n \log_u(n).$$

Pour n assez grand, on a donc $\alpha - \beta \leqslant 2n \log_u(n)$. En conclusion, en posant $C = \log_p(u^k - 1)$ qui est une constante ne dépendant que de u, on trouve pour n assez grand que

$$v_p(u^{\alpha-\beta} - 1) \leqslant C + \log_p 2n \log_u n = C + \log_p(2) + \log_p(n) + \log_p \log_u(n) \leqslant 2 \log_p(n).$$

D'autre part, d'après la formule de Legendre, on a

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots \geqslant \left\lfloor \frac{n}{p} \right\rfloor \geqslant \frac{n}{p} - 1.$$

D'où

$$\frac{n}{p} - 1 \leqslant v_p(n!) = v_p(u^{\alpha-\beta} - 1) \leqslant 2 \log_p(n).$$

Cette inégalité étant fausse pour n assez grand, on déduit que l'équation donnée n'a pas de solution lorsque n est trop grand, ce qui conclut.

Exercice 3.83. (ELMO 2017 N3) Pour tout entier $C > 1$, déterminer s'il existe des entiers $a_1, a_2, \ldots$ deux à deux distincts tels que, pour tout indice $k \geqslant 1$, $a_{k+1}^k \mid C^k a_1 a_2 \ldots a_k$.

Solution 3.83. **Réponse :** Il n'existe pas de suite vérifiant l'énoncé, quelle que soit la valeur de C.

Pour tout nombre premier p, en comparant les valuations $p-$adiques, on trouve que

$$kv_p(a_{k+1}) \leqslant kv_p(C) + v_p(a_1) + \ldots + v_p(a_k).$$

Posons $H_k = 1 + 1/2 + \ldots + 1/k$. On cherche à déduire une borne sur la suite $(v_p(a_n))$.

On commence par faire un changement de variable pour avoir une relation de récurrence sur deux termes consécutifs. On pose $S_k = v_p(a_1) + \ldots + v_p(a_k)$. L'inégalité s'écrit

$$k(S_{k+1} - S_k) \leqslant kv_p(C) + S_k \quad \Longleftrightarrow \quad \frac{1}{k+1} S_{k+1} \leqslant \frac{1}{k+1} v_p(C) + \frac{1}{k} S_k.$$

On déduit par télescopage que

$$\frac{1}{k} S_k \leqslant S_1 + \frac{1}{2} v_p(C) + \frac{1}{3} v_p(C) + \ldots + \frac{1}{k+1} v_p(C) = v_p(a_1) + (H_{k+1} - 1) v_p(C).$$

Enfin, en revenant à la relation initiale,

$$v_p(a_{k+1}) \leqslant v_p(C) + \frac{S_k}{k} \leqslant v_p(a_1) + H_{k+1} v_p(C).$$

De l'inégalité ci-dessus (ou même de la relation de départ), on déduit que les diviseurs premiers de la suite (a_k) sont compris dans les diviseurs premiers de C et de a_1. On note $\mathcal{P}$ l'ensemble de ces diviseurs premiers, qui est donc fini.

➢ **Commentaire :**

> De là, le but est de trouver deux indices i et j tels que $v_p(a_i) = v_p(a_j)$ pour tout nombre premier, concluant que $a_i = a_j$ et contredisant l'hypothèse de l'énoncé. La suite $H_{k+1} v_p(C)$ a une croissance logarithmique.
> En conséquence, pour k assez grand, on a
>
> $$v_p(a_k) \leqslant v_p(a_1) + H_k v_p(C) \leqslant v_p(a_1) + 2 \ln k v_p(C) \leqslant k - 1.$$
>
> Cela veut dire que $\{v_p(a_1), \ldots, v_p(a_k)\} \subset [\![1, k-1]\!]$, ce qui implique par principe des tiroirs qu'on a deux indices i et j tels que $v_p(a_i) = v_p(a_j)$. Pour obtenir un principe des tiroirs applicable à tous les nombres premiers en même temps, et avoir deux indices i et j tels que $v_p(a_i) = v_p(a_j)$ pour tout p, il suffit de raffiner le raisonnement précédent.

Posons $A = \max_{p \in \mathcal{P}} v_p(a_1)$ et $B = \max_{p \in \mathcal{P}} v_p(C)$. Pour k assez grand, on a $H_k \leqslant 2 \ln k$. D'après l'estimation précédente, par croissance comparée, pour tout $i \leqslant k$,

$$v_p(a_i) \leqslant v_p(a_1) + H_i v_p(C) \leqslant \max_{p \in \mathcal{P}} v_p(a_1) + H_k \max_{p \in \mathcal{P}} v_p(C) \leqslant A + 2B \ln k$$

Ainsi, pour tout $p \in \mathcal{P}$, on a $v_p(a_i) \in [\![0, \lfloor A + 2B \ln k \rfloor]\!]$. Or il y a $(\lfloor A + 2B \ln k \rfloor + 1)^{|\mathcal{P}|}$ entier n vérifiant que $v_p(n) \in [\![0, \lfloor A + 2B \ln k \rfloor]\!]$ pour tout $p \in \mathcal{P}$. Pour k suffisamment grand, par croissance comparée, on a $(A + B \ln k + 1)^{|\mathcal{P}|} \leqslant k - 1$. Cela implique, par principe des tiroirs (les chaussettes sont les entiers $a_1, \ldots, a_k$ et les tiroirs sont les $(A + B \ln k + 1)^{|\mathcal{P}|}$ entiers dont les valuations $p-$adiques vérifient la contrainte ci-dessus), qu'il existe deux indices distincts i et j tels que $v_p(a_i) = v_p(a_j)$ pour tout $p \in \mathcal{P}$. Autrement dit, $a_i = a_j$.

Comme cela contredit l'hypothèse de l'énoncé, on déduit qu'il n'y a pas de suite vérifiant l'énoncé.

Exercice 3.84. (USA 2022 TSTST P8) Déterminer toutes les fonctions f allant de $\mathbb{N}^\star$ dans $\mathbb{Z}$ telles que, pour tout couple d'entiers strictement positifs (m,n) :

$$\left\lfloor \frac{f(mn)}{n} \right\rfloor = f(m)$$

On pourra admettre le théorème suivant : Soit (u_n) une suite telle que, pour tout $\varepsilon > 0$, il existe un rang N tel que

$$\text{pour tout } p,q \geqslant N, |u_p - u_q| < \varepsilon.$$

Alors la suite (u_n) converge.

Solution 3.84. **Réponse :** Il s'agit des fonctions f de la forme $f(n) = \lfloor rn \rfloor$ pour tout n ou $f(n) = \lceil rn \rceil - 1$ pour tout n, où r est un réel.

On écrit la division euclidienne de $f(mn)$ par n : il existe un entier $0 \leqslant r_n(m) < n$ tel que

$$f(mn) = \left\lfloor \frac{f(mn)}{n} \right\rfloor n + r_n(m) = nf(m) + r_n(m)$$

On a donc par symétrie :

$$mf(n) + r_m(n) = nf(m) + r_n(m)$$

On déduit en divisant par m et n que

$$\left| \frac{f(n)}{n} - \frac{f(m)}{m} \right| = \frac{r_n(m) + r_m(n)}{mn} < \frac{1}{n} + \frac{1}{m}$$

La suite $(f(n)/n)$ vérifie donc le théorème admis, elle converge vers un réel r. Avec les encadrements de la partie réelle :

$$r - \frac{1}{m} = \lim_{n\to+\infty} \frac{1}{m}\left(\frac{f(mn)}{n} - 1\right) \leqslant \frac{f(m)}{m} \leqslant \lim_{n\to+\infty} \frac{1}{m} \cdot \frac{f(mn)}{n} = r$$

On déduit que pour tout m, $rm - 1 \leqslant f(m) \leqslant rm$.

Si r est irrationnel, $rm - 1$ n'est jamais entier, donc $rm - 1 < f(m) \leqslant rm$, donc $f(m) = \lfloor rm \rfloor$ pour tout m.

Si r est rationnel, on l'écrit $r = p/q$. Notons que lorsque q ne divise pas m, $rm - 1$ n'est pas entier, donc à nouveau $f(m) = \lfloor rm \rfloor = \lceil rm \rceil - 1$. On a ensuite $f(q) = p - 1$ ou $f(q) = p$. Notons que

- ➢ Si $f(q) = p - 1$, on a alors $p - 1 = [f(kq)/k]$, ce qui force $f(kq)$ (qui vaut $kp - 1$ ou kp), à valoir $kp - 1$. On déduit que $f(kq) = \lceil rkp \rceil - 1$, c'est-à-dire $f(m) = \lceil rm \rceil - 1$ pour tout m. Ceci est bien solution.
- ➢ Si $f(q) = p$, on fait le même raisonnement pour avoir $f(kq) = kp$ et retrouver $f(m) = \lfloor rm \rfloor$.

Réciproquement, les fonctions annoncées sont bien solutions. Pour tous entier m et n, on a

$$\lfloor rm \rfloor - 1 \leqslant rm - \frac{1}{n} < \frac{\lfloor rmn \rfloor}{n} \leqslant rm < \lfloor rm \rfloor + 1, \quad \Longrightarrow \left\lfloor \frac{\lfloor rmn \rfloor}{n} \right\rfloor = \lfloor rm \rfloor$$

La fonction $f(m) = \lfloor rm \rfloor$ est donc bien solution. Une vérification similaire donne que la fonction définie par $f(n) = \lceil rn \rceil - 1$ est également solution. Notons que lorsque r est rationnel, ces deux fonctions ne coïncident pas.

Exercice 3.85. (IMO SL 2021 N5) Montrer que l'équation $n! = a^{n-1} + b^{n-1} + c^{n-1}$ admet un nombre fini de quadruplets solutions (a, b, c, n) d'entiers strictement positifs.

Solution 3.85.

➢ **Commentaire :**

> L'idée est de montrer que si n est trop grand, il n'y a pas de solutions.
>
> Il faut commencer par se placer dans un cas "générique", c'est-à-dire un cas suffisamment favorable aux divers raisonnements que l'on veut appliquer et suffisamment générique pour que les autres cas soient résiduels.
>
> D'après la formule de Stirling, si l'un des a, b et c est trop grand, disons $a \geqslant n/2$, alors $a^{n-1} + b^{n-1} + c^{n-1} \geqslant (n/2)^{n-1} > n!$ pour n assez grand. Donc pour n assez grand, les diviseurs premiers de a, b et c sont inférieurs à $n/2$. En particulier, si p divise deux des trois entiers, il divise le troisième.
>
> Si $p \mid a, b, c$, alors $p^{n-1} \mid n!$ donc $v_p(n!) \geqslant n - 1$. Comme on a l'encadrement $v_p(n!) \leqslant \dfrac{n}{p-1}$, donc la divisibilité ne peut pas se produire pour p impaire.
>
> Si $p \mid c$ mais p ne divise ni a ni b, alors $p \mid a^{n-1} + b^{n-1}$. On touche au raisonnement générique, qui est le coeur de la preuve. Si $p \mid a + b$ alors d'après le lemme LTE, pour peu que $n - 1$ soit impair,
>
> $$v_p(a^{n-1} + b^{n-1}) = v_p(a + b) + v_p(n - 1).$$
>
> Cette valuation est petite, alors que $v_p(n! - c^{n-1})$ a vocation à être grand car $v_p(n!)$ et $v_p(c^{n-1})$ sont grands. Donc il faut s'assurer que p est impair et que $n - 1$ est impair avant de faire marcher ce raisonnement.
>
> L'idée clée qui fait réellement décoller la preuve, c'est de prendre le paragraphe précédent à rebours : ne pas considérer un diviseur premier éventuel de c et espérer qu'il divise $a + b$, on considère une diviseur premier p de $a + b$. Il suffit alors de traiter à part le cas où $a + b, b + c$ et $c + a$ sont des puissances de 2.

Tout d'abord, pour un entier n fixé, il y a un nombre fini de solutions à l'équation, puisque a, b et c sont alors tous majorés par $(n!)^{1/(n-1)}$. Il suffit dès lors de montrer que si n est suffisamment grand, l'équation écrite n'a pas de solutions. Dans la suite, on considère un quadruplet solution (n, a, b, c) avec n un entier très grand.

Étape 1 : une majoration sur les entiers a, b et c.

Montrons que $a, b, c < \frac{n}{2}$. Si l'inégalité annoncée est fausse pour un entier, disons a, alors

$$n! = a^{n-1} + b^{n-1} + c^{n-1} \geqslant \left(\frac{n}{2}\right)^{n-1}.$$

La formule de Stirling indique pourtant que $n! \sim (n/e)^n \sqrt{2\pi n}$. Les croissances comparées donnent alors

$$\frac{n!}{(n/2)^{n-1}} \sim \frac{n}{2}\left(\frac{2}{e}\right)^n \sqrt{2\pi n} \longrightarrow 0,$$

d'où la contradiction.

Étape 2 : $n - 1$ est nécessairement impair.

Si $n - 1$ est pair, les nombres a^{n-1}, b^{n-1} et c^{n-1} sont des carrés. Si au moins l'un d'eux est impair, alors $a^{n-1} + b^{n-1} + c^{n-1} \neq 0 \mod 4$, alors que $4 \mid n!$. De cette contradiction, on déduit que a, b et c sont tous pairs. Mais alors $2^{n-1} \mid n!$, alors, que d'après la formule de Legendre, n étant impair, on a

$$v_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \ldots = \left\lfloor \frac{n-1}{2} \right\rfloor + \left\lfloor \frac{n-1}{4} \right\rfloor < (n-1)\left(\frac{1}{2} + \frac{1}{4} + \ldots\right) = n - 1.$$

Ceci conclut que $n - 1$ est impair.

Étape 3 : Raisonnement générique : cas où $a + b$ admet un facteur premier impair.

Supposons que l'un au moins des nombres $a + b, b + c$ et $c + a$, disons $a + b$, admette un diviseur premier p impair. D'après l'étape 1, on a $a + b < n$, donc $p < n$ et $p \mid n!$. D'après la formule de Legendre, on a (en utilisant que $p \geqslant 3$,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots \leqslant n\left(\frac{1}{p} + \frac{1}{p^2} + \ldots\right) = \frac{n}{p-1} < n - 1.$$

Comme $n-1$ est impair, $p \mid a+b \mid a^{n-1}+b^{n-1}$ et finalement $p \mid c^{n-1}$. Si $p \mid a$, alors $p \mid b$. Mais alors $p^{n-1} \mid n!$ et $v_p(n!) \geqslant n-1$, ce qui contredit la majoration ci-dessus. D'après le lemme LTE (p est bien impair, $n-1$ aussi et p ne divise pas a et b),

$$v_p(a^{n-1}+b^{n-1}) = v_p(a+b) + v_p(n-1).$$

D'autre part, puisque $v_p(c^{n-1}) \geqslant n-1 > v_p(n!)$, on déduit que $v_p(n!-c^{n-1}) = v_p(n!)$. On déduit que

$$v_p(2)+v_p(3)+\ldots+v_p(n-1)+v_p(n) = v_p(n!) = v_p(n!-c^{n-1}) = v_p(a^{n-1}+b^{n-1}) = v_p(a+b)+v_p(n-1).$$

En simplifiant, puisque $a, b < n/2$ et que n est pair, on a $a+b < n-1$ et donc

$$v_p(2)+\ldots+v_p(a+b-1)+v_p(a+b+1)+\ldots+v_p(n-2)+v_p(n) = 0.$$

Donc p ne divise que deux entiers de $[\![1,n]\!]$, à savoir $a+b$ et $n-1$. Cela implique que $p = a+b$ et $2p = n-1$, ce qui est absurde car $n-1$ est impair. Donc lorsque n est assez grand, l'équation n'a pas de solutions.

Étape 4 : Cas marginal : si $a+b, b+c$ et $c+a$ sont tous les trois des puissances de 2.

Puisque $a, b, c \geqslant 1$, ces puissances de 2 sont paires. Cela implique que a, b et c sont de même parité. S'ils étaient impairs, $n!$ serait impair, ce qui est faux pour $n \geqslant 2$. Ils sont donc tous les trois pairs. On a vu que $v_2(n!) \leqslant n-1$, donc les trois entiers ne sont pas tous divisibles par 4. Mais alors $2a = (a+b)+(a+c)-(b+c)$ n'est pas divisible par 8, ce qui veut dire que l'une des puissances de 2 est inférieure à 4. Disons que $b+c \leqslant 4$. Comme $b+c \geqslant 2+2 = 4$, on a $b+c = 4$ et $b = c = 2$.

On écrit $a = a+b-2 = 2^\alpha - 2$. Il vient que $a \mid n! \mid 2^{n-1}+2^{n-1}+a^{n-1}$, donc $a \mid 2^n$ et a est une puissance de 2. On a $a \geqslant 2$ donc $\alpha \geqslant 2$. Mais alors $v_2(a) = 1$ et $a = 2$. Mais alors $n! = 3 \cdot 2^{n-1}$, ce qui est absurde pour n assez grand par croissances comparées avec la formule de Stirling (ou simplement parce qu'alors 5 ne divise pas $n!$). Donc lorsque n est assez grand, l'équation n'a pas de solutions.

4 Exercices de style

4.1 L'arithmétique et les suites

Exercice 4.1. (Baltic Way 2021 P3) Déterminer toutes les suites d'entiers strictement positifs $a_1, a_2, \ldots$ telles que, pour tout $n \geqslant 1$,

$$a_{n+1}^2 = 1 + (n + 2021)a_n.$$

Solution 4.1. **Réponse :** La seule solution est la suite définie par $a_n = n + 2019$ pour tout entier n.

Soit (a_n) une suite solution. En soustrayant les relations correspondant à deux indices consécutifs, on a

$$a_{n+2}^2 - a_{n+1}^2 = (n + 2021)(a_{n+1} - a_n) + a_{n+1}.$$

De cette relation, on déduit que si $a_{n+1} \geqslant a_n$ alors $a_{n+2}^2 - a_{n+1}^2 \geqslant a_{n+1} > 0$ et $a_{n+2} > a_{n+1}$. Comme la suite (a_n) ne peut décroître strictement indéfiniement, il existe un rang N tel que $a_{N+1} \geqslant a_N$ et il vient que $\boxed{a_{n+1} > a_n \text{ pour tout } n > N}$.

Soit $n \geqslant N + 1$. On a donc $a_{n+1} \geqslant a_n + 1$. En injectant dans la relation de récurrence, on trouve

$$1 + (n + 2021)a_n \geqslant (a_n + 1)^2 \quad \Longleftrightarrow \quad \boxed{n + 2019 \geqslant a_n}.$$

Or, on a, pour tout n, $a_n - n \leqslant a_{n+1} - (n + 1)$, donc la suite $(a_n - n)$ est croissante et majorée par 2019. Elle stationne donc : il existe un rang M tel que, si $n \geqslant M$, alors $a_n = n + \ell$, avec ℓ un entier. En injectant cette égalité dans l'énoncé, on trouve

$$(n + 1 + \ell)^2 = 1 + (n + 2021)(n + \ell) \quad \Longleftrightarrow \quad (2019 - \ell)n = \ell^2 - 2019\ell.$$

Pour que cette égalité soit vraie pour tout $n \geqslant M$, il faut que $\ell - 2019 = 0$ soit $\boxed{\ell = 2019}$.

Supposons enfin que $a_{n+1} = n + 1 + 2019$. Un calcul direct donne

$$(n + 2021)a_n = a_{n+1}^2 - 1 = (n + 2021)(n + 2019) \quad \Longrightarrow a_n = n + 2019.$$

Par récurrence descendante, on déduit que $\boxed{a_n = n + 2019}$ pour tout n.

Réciproquement, un calcul direct montre que cette suite vérifie bien la propriété de l'énoncé.

Exercice 4.2. (OFM 2025) Déterminer toutes les suites bornées d'entiers strictement positifs $(a_1, a_2, \ldots)$ vérifiant que, pour tout nombre premier p et tout indice $n \geqslant 1$, le nombre

$$a_n a_{n+1} \ldots a_{n+p-1} - a_{n+p}$$

est un multiple de p.

Solution 4.2. **Réponse :** Les seules suites solutions sont les suites constantes.

Commençons par vérifier que les suites constantes sont bien solutions du problème. Soit (a_n) une suite constante égale à b. Alors a_n est bornée donc elle vérifie la première condition. Si p est un nombre premier, on a d'après le petit théorème de Fermat, pour tout indice n,

$$a_n \cdot \ldots \cdot a_{n+p-1} = b^p \equiv b = a_{n+p} \mod p.$$

La suite (a_n) vérifie donc la deuxième condition et est donc bien solution du problème.

La suite de la solution est consacrée à la preuve que toute suite vérifiant les deux conditions est bien constante.

Soit $q > M^2$ un nombre premier.

Étape 1 : Pour tout $i \geqslant 0$, $a_{q+i}^2 = a_i a_{q+i+1}$.
En effet, prenons i un indice quelconque. En appliquant l'hypothèse de l'énoncé au nombre premier q et aux indices i et $i+1$, on trouve

$$a_{q+i}^2 = a_{q+i} \cdot a_{q+i} \equiv (a_i \cdot \ldots \cdot a_{q+i-1}) a_{q+i} = a_i \cdot (a_{i+1} \cdot \ldots a_{q+i}) \equiv a_i a_{q+i+1} \mod q.$$

Ainsi, q divise $a_{q+i}^2 - a_i a_{q+i+1}$. Or, a_{q+i}^2 et $a_i a_{q+i+1}$ sont tous les deux compris entre 0 et M^2, de sorte que $0 \leqslant |a_{q+i}^2 - a_i a_{q+i+1}| \leqslant M^2 < q$, donc $a_{q+i}^2 = a_i a_{q+i+1}$.

Étape 2 : Il existe un indice i et un entier a tel que $a_n = b$ pour tout $n \geqslant i$.
Comme la suite (a_n) est une suite bornée d'entiers, il existe une valeur prise une infinité de fois par la suite. Soit b le plus grand entier pris une infinité de fois par la suite (a_n). On dispose donc d'un indice N tel que, si $n \geqslant N$, $a_n \leqslant b$. Soit $j \geqslant N + q + 1$ un indice tel que $a_j = b$. Supposons que la suite (a_n) ne se soit pas constante à partir du rang j et notons k le plus petit indice supérieur à j tel que $a_{k+1} \neq b$. On a donc $a_{k+1} < b$. En appliquant l'étape 1 à $i = k - q$, on trouve

$$b^2 = a_k^2 = a_{k+1} a_{k-q+1} < b \cdot a_{k-q+1} \leqslant b^2.$$

On a donc une contradiction, ce qui signifie que la suite (a_n) est constante à partir du rang i.

Étape 3 : La suite (a_n) est constante égale à b.
Supposons que cela ne soit pas le cas et prenons l'indice k maximal tel que $a_k \neq b$ (l'existence d'un tel maximum étant garantie par l'étape 2). En appliquant l'étape 1 à $i = k$, on trouve

$$a_k = \frac{a_{k+q-1}^2}{a_{k+q}} = \frac{b^2}{b} = b,$$

ce qui est absurde. La suite (a_n) est donc constante égale à b.
Remarque Alternative aux étapes 2 et 3 : Supposons avoir établi l'étape 1 pour tout nombre premier q suffisamment grand. On choisit alors deux nombres premiers $p < q$ suffisamment grands. En appliquant la relation de l'étape 1 à ces deux nombres premiers, on trouve pour tout indice $i > q$,

$$a_{i-q} = \frac{a_i^2}{a_{i+1}} = a_{i-p}.$$

En particulier, pour tout indice i, on a $a_i = a_{i+q-p}$. La suite (a_i) est donc périodique de période $q - p$. On peut donc conclure à nouveau conclure comme dans l'étape 4 en posant $r = q - p$.

Solution alternative
Dans cette solution, on propose une deuxième façon de démontrer que les seules suites solutions au problème sont les suites constantes.
Étape A : La suite (a_n) est périodique à partir d'un certain rang.

Soit $p > M$ un nombre premier. Tous les termes de la suite ont un reste non nul modulo p. L'ensemble des valeurs que les $p-$uplets $(a_n, \ldots, a_{n+p-1})$ peuvent prendre est un ensemble fini, il existe donc d'après le principe des tiroirs un $p-$uplet $(b_0, \ldots, b_{p-1})$ et deux indice i et $i+T$ tels que $(a_i, \ldots, a_{i+p-1}) = (a_{i+T}, \ldots, a_{i+T+p-1}) = (b_0, \ldots, b_{p-1})$. En particulier, $a_{j+T} = a_j$ pour tout $i \leqslant j \leqslant i+p-1$. On montre alors que $a_{j+T} = a_j$ pour tout $j \geqslant i$.

En effet, supposons que cela ne soit pas le cas et prenons j_0 le plus petit indice tel que $a_{j_0+T} \neq a_{j_0}$. On a $j_0 \geqslant i+p$. En appliquant l'hypothèse de l'énoncé successivement à $n = j_0 - p$ et $n = j_0 - p + T$, on trouve

$$a_{j_0} \equiv a_{j_0-p} \cdot \ldots \cdot a_{j_0-1} = a_{j_0-p+T} \cdot \ldots \cdot a_{j_0-1+T} \equiv a_{j_0+T} \mod p.$$

Ainsi, a_{j_0} et a_{j_0+T} sont deux entiers compris entre 1 et $p-1$ ayant le même reste modulo p, ils sont donc égaux, ce qui est une contradiction.

Ainsi, la suite est périodique de période T à partir du rang i.

Étape A bis : La suite (a_n) est périodique.

Soit T la période de l'étape 1 et $p > M$ un nombre premier. Supposons que la suite ne soit pas périodique et prenons l'indice k maximal tel que $a_k \neq a_{k+T}$ (l'existence d'un tel maximum est garantie par l'étape 1). En appliquant l'hypothèse de l'énoncé à $n = k$, on trouve

$$a_k \cdot a_{k+1} \cdot \ldots \cdot a_{k+p-1} \equiv a_{k+p} \mod p.$$

Puisque tous les termes de la suite sont non nuls et inférieurs à $p-1$, ils sont inversibles modulo p et

$$a_k \equiv a_{k+p} a_{k+1}^{-1} \cdot \ldots a_{k+p-1}^{-1} = a_{k+p+T} a_{k+1+T}^{-1} \cdot \ldots a_{k+p-1+T}^{-1} \equiv a_{k+T} \mod p,$$

où on a utilisé l'hypothèse de l'énoncé pour $n = k+T$. Ainsi, a_k et a_{k+T} sont deux entiers compris entre 1 et $p-1$ ayant le même reste modulo p, ils sont donc égaux, ce qui est une contradiction. La suite est donc bien périodique de période T.

Étape C : Pour tout n, $a_{n+r}^2 = a_{n+1} a_{n+r+1}$.

Il s'agit de l'étape 1 de la solution 1.

Étape D : La suite est constante.

Soit b le maximum de la suite. Puisque la suite est périodique, il existe une infinité d'indices n tels que $a_n = b$. Supposons qu'il existe au moins un terme de la suite qui n'est pas égal à b. Alors on dispose d'un indice $n \geqslant T$ tel que $a_n = b$ et $a_{n+1} \neq b$. En appliquant l'étape 3, on trouve

$$b^2 = a_n^2 = a_{n-r+1} a_{n+1} < a_{n-r+1} b \leqslant b^2,$$

ce qui est absurde. La suite est donc constante égale à b.

Exercice 4.3. (IMO SL 2024 N3) Déterminer toutes les suites infinies $a_1, a_2, \ldots$ d'entiers strictement positifs telles que, pour toute paire (m, n) d'entiers strictement positifs pour laquelle $m \leqslant n$, les nombres

$$\frac{a_m + a_{m+1} + \ldots + a_n}{n-m+1} \quad \text{et} \quad (a_m a_{m+1} \ldots a_n)^{\frac{1}{n-m+1}}$$

sont tous les deux entiers.

Solution 4.3. **Réponse :** Seules les suites constantes sont solutions.

On vérifie que les suites constantes sont bien solutions du problème. Le problème consiste à montrer que ce sont les seules. La première étape de l'exercice est commune à toutes les solutions. On présente ensuite plusieurs façons différentes d'utiliser cette étape pour résoudre l'exercice.

Pour tout nombre premier et tout entier a, on note $v_p(a)$ la valuation $p-$adique de a.

Étape 1 :

Soit n un indice fixé. Montrons que, pour tout nombre premier p, les suites $(a_k)_k$ et $(v_p(a_k))_k$ sont périodiques modulo n de période n. Si $k \geqslant 1$, l'hypothèse de l'énoncé indique que

$$n \mid a_k + a_{k+1} + \ldots + a_{k+n-1} \quad \text{et} \quad n \mid a_{k+1} + a_{k+2} + \ldots + a_{k+n}.$$

Donc n divise la différence de ces deux sommes, à savoir $a_{k+n} - a_k$, ce qui signifie bien que $\boxed{a_{k+n} \equiv a_k \mod n}$.

On prouve de la même manière que $\boxed{v_p(a_{k+n}) \equiv v_p(a_k) \mod n}$ en remarquant que la seconde hypothèse de l'énoncé se réécrit comme la propriété que $\dfrac{v_p(a_n) + \ldots + v_p(a_m)}{n-m+1}$ est un entier pour tous entiers $m < n$ et tout nombre premier p.

Étape 2 : Conclusion.

Soit p un nombre premier. Posons $\alpha = v_p(a_1)$. Pour tout entier m, d'après l'étape précédente, $a_{mp^{\alpha+1}+1} \equiv a_1 \equiv 0 \mod p^\alpha$ et $a_{mp^{\alpha+1}+1} \equiv a_1 \neq 0 \mod p^{\alpha+1}$, donc $v_p(a_{mp^{\alpha+1}+1}) = \alpha$. Mais alors pour tout indice k et tout indice m, on a $mp^{\alpha+1} - k \mid v_p(a_{mp^{\alpha+1}+1}) - v_p(a_k) = \alpha - v_p(a_k)$. Comme cette divisibilité est vraie pour tout entier m, le nombre $\alpha - v_p(a_k)$ admet une infinité de diviseurs, il est donc nul et $v_p(a_k) = \alpha = v_p(a_1)$ pour tout indice k. Comme cette relation est vraie pour tout nombre premier p et tout indice k, la suite (a_n) est constante.

Remarque : Il ne faut pas se laisser prendre par la concision de la solution : la première étape est beaucoup plus simple à obtenir que la seconde, et pourrait raisonnablement être estimée à 2/7.

Solution alternative

Soit m un entier fixé. Montrons que a_m divise tous les termes de la suite à partir d'un certain rang. Pour cela, on pose $n_0 = \max\{v_p(a_m) + m + 1, p \text{ premier}\}$. D'après l'étape 1, si $n \geqslant n_0$ et p est un nombre premier, $v_p(a_n) \equiv v_p(a_m) \mod (n-m)$, ce qui implique notamment que $v_p(a_m) \leqslant v_p(a_n)$. Ainsi, a_m divise a_n dès que $n_0 \geqslant n$.

En supposant qu'il existe au moins un terme de la suite que a_m ne divise pas, notons $k = \max\{n, a_m \text{ ne divise pas } a_n\}$. On a alors modulo a_m,

$$0 \equiv a_k + a_{k+1} + \ldots + a_{k+a_m-1} \equiv a_k \mod a_m,$$

ce qui contredit l'hypothèse faite sur k. Ainsi, a_m divise tous les termes de la suite. Mais alors en particulier $a_m \mid a_1$ et par symétrie $a_1 \mid a_m$, donc $a_1 = a_m$ et à nouveau, la suite est constante.

Solution alternative

On veut montrer ici aussi que tous les termes de la suite se divisent entre eux. On suppose que la suite est non constante. On dispose donc de deux indices i et j tels que $a_i \neq a_j$. On a donc a_i qui ne divise pas a_j ou a_j qui ne divise pas a_i. Disons, quitte à inverser les rôles, que a_i ne divise pas a_j. Il existe donc un nombre premier p, un entier r et deux indices i et j tels que $p^r \mid a_i$ mais p^r ne divise pas a_j. Soit $q > \max(p^r, v_p(a_i))$ un entier non divisible par p. Alors d'après l'étape 1, $v_p(a_{i+qm}) \equiv v_p(a_i) \mod q$ pour tout m, ce qui signifie en particulier que $v_p(a_{i+qm})$ est non nul pour tout m.

En choisissant un entier m tel que $i + qm \equiv j \mod p^r$ (un tel entier existe car q est premier avec p). On déduit que

$$a_j \equiv a_{i+qm} = 0 \mod p^r,$$

ce qui est absurde. Ainsi, la suite (a_n) est constante, ce que nous souhaitions.

Solution alternative

Dans cette solution, on commence par prouver que $a_{n+1} \mid a_n$. On suppose pour cela que ce n'est pas le cas et qu'il existe un nombre premier p tel que $v_p(a_{n+1}) > v_p(a_n)$. Notons $r = v_p(a_{n+1})$. D'après l'étape 1, pour tout entier k, on a alors $a_{n+kp^r} \equiv a_n \neq 0 \mod p^r$, de sorte que $v_p(a_{n+kp^r}) < r$. Mais alors, d'après l'étape 1,

$$kp^r - 1 \mid v_p(a_{n+1}) - v_p(n + kp^r).$$

Le temre de droite de cette expression est bien non nul, ce qui implique $kp^r - 1 \leqslant v_p(a_{n+1}) - v_p(n + kp^r) \leqslant r$, ce qui est absurde.

Ainsi, $a_{n+1} \mid a_n$ pour tout n. En particulier, $a_{n+1} \leqslant a_n$. La suite (a_n) est donc une suite décroissante d'entiers strictement positifs, ce qui implique qu'à partir d'un certain rang, cette suite est constante égale à c. Mais alors pour tout entier m et tout entier n, il existe un entier k suffisamment grand tel que $a_{n+km} = c$. Comme $a_n \equiv a_{n+km} = c \mod m$, m est un diviseur de $a_n - c$. L'entier $a_n - c$ admet une infinité de diviseurs, il est donc nul et la suite est constante égale à c.

Exercice 4.4. (Balkan MO 2019 SL A1) Soit a_0 un entier strictement positif. Soit (a_n) une suite dans laquelle $a_0 \geqslant 1$ est un entier et, pour tout $n \geqslant 1$, a_n est le plus petit entier strictement positif pour lequel $a_0 + a_1 + \ldots + a_n$ est divisible par n. Montrer qu'il existe un rang M tel que $a_n = a_{n+1}$ pour tout $n \geqslant M$.

Solution 4.4. Posons $S_n = a_0 + \ldots + a_{n-1}$. On dispose de la valeur explicite de a_n en fonction de S_{n-1} : le plus petit multiple de n supérieur à S_{n-1} est $n\lceil S_{n-1}/n \rceil$, donc $a_n = n\lceil S_{n-1}/n \rceil - S_{n-1}$.

D'autre part, puisque $[\![S_{n-1}, S_{n-1} + n - 1]\!]$ contient un multiple de n, on a $a_n \leqslant n - 1$. Ainsi, $S_n \leqslant a_0 + 1 + \ldots + n - 1 = a_0 + \dfrac{n(n-1)}{2}$.

On introduit la suite auxiliaire des quotients : on note b_n l'entier tel que $S_n = n \cdot b_n$. On a alors

$$a_n = S_n - S_{n-1} = nb_n - (n-1)b_{n-1} = b_n + (n-1)(b_n - b_{n-1}), \quad \Longrightarrow n - 1 \mid a_n - b_n.$$

Du fait de la majoration $S_n \leqslant a_0 + \dfrac{n(n-1)}{2}$, il existe un rang N tel que, pour tout $n \geqslant N$, on a $S_n \leqslant n(n-1)$, ce qui implique que $b_n \leqslant n - 1$. Ainsi, les entiers a_n et b_n sont tous les deux dans l'intervalle $[\![1, n-1]\!]$ et leur différence est divisible par $n - 1$. On déduit que $\boxed{a_n = b_n \text{ pour tout } n \geqslant N}$.

Mais alors pour tout $n \geqslant N+1$, $a_n = nb_n - (n-1)b_{n-1} = na_n - (n-1)a_{n-1}$, ce qui conduit après simplification à $\boxed{a_n = a_{n-1}}$ comme annoncé.

Exercice 4.5. (Taiwan IMOC 2021 N3) Pour tout entier $x \geqslant 2$, on note $f(x)$ son plus grand facteur premier. Soient M et k des entiers strictement positifs. Une suite (a_n) d'entiers strictement positifs est définie par $a_1 = M > 1$ et

$$a_{n+1} = \begin{cases} a_n - f(a_n) & \text{si } a_n \text{ est composé} \\ a_n + k & \text{sinon} \end{cases}$$

Montrer que la suite (a_n) est bornée.

Solution 4.5.

➢ **Commentaire :**

> D'après la définition, si a_n est composé alors $a_{n+1} < a_n$ et si a_n est premier, $a_{n+1} = a_n + k$. Donc pour que la suite prenne de grandes valeurs, elle doit contenir beaucoup de termes consécutifs qui sont des nombres premiers, et qui forment alors une sous-suite arithmétique de raison k. Donc la suite (a_n) ne peut pas traverser un intervalle de longueur $k+1$ ne contenant que des nombres composés. Or, il est classique qu'il existe des intervalles d'entiers arbitrairement grands qui ne contiennent pas de nombres premiers, et si la suite ne peut pas traverser ces intervalles, elle sera bornée. C'est ce que l'on formalise ci-après.

Considérons l'intervalle $[\![(M+k)!+2, (M+k)!+k+2]\!]$. Les entiers de cet intervalle sont de la forme $(M+k)!+\ell$, qui est divisible par ℓ sans lui être égal. Donc cet intervalle contient k nombres composés. Supposons par l'absurde que la suite (a_n) soit non bornée et qu'il existe donc un indice $n \geqslant 1$, choisi minimal, tel que $a_n \geqslant (M+k)!+k+2$. Par minimalité de n, $a_{n-1} < a_n$ donc non seulement a_{n-1} est premier mais en plus il vérifie $a_{n-1} < (M+k)!+k+3$. On a donc $a_{n-1} = a_n - k \geqslant (M+k)!+2$. Il vient que $a_{n-1} \in [\![(M+k)!+2, (M+k)!+k+2]\!]$, ce qui est absurde car il est premier. La suite (a_n) prend donc toujours des valeurs inférieures à $(M+k)!+k+2$, ce qui conclut.

Solution alternative

➢ **Commentaire :**

> La difficulté est qu'on ne sait pas comment caractériser la borne attendue, et un raisonnement par l'absurde en extraillant une sous-suite infinie n'a pas l'air de produire d'effet tel quel.
>
> Commençons par examiner les changements d'état du système. Par exemple, cherchons les conditions sur ℓ tel qu'il existe n tel que $a_n, a_{n+1}, \ldots, a_{n+\ell}$ sont premiers (ce qui implique notamment que $a_{n+r} = a_n + kr$ pour tout $k \leqslant \ell$). C'est pertinent dans la mesure où, si la suite est bornée, un tel ℓ est nécessairement petit. Remarquons que si p est un nombre premier avec k, k est inversible donc les entiers $a_n + kr$ avec r qui varie sont deux à deux distincts modulo p. En particulier, si $\ell \geqslant p+1$, l'un de ces termes est nul modulo p, donc égal à p (car premier par hypothèse). Ainsi, si ℓ est grand, a_n doit être petit.

Supposons que la suite est non bornée et choisissons un entier A, supposé grand, dont la taille exacte sera précisée plus tard (voir lignes violettes qui donnent les conditions). Comme la suite (a_n) est non bornée, il existe un indice n, que l'on prend minimal, tel que $a_n \geqslant A$. Par minimalité de n, $a_{n-1} < A \leqslant a_n$, donc a_{n-1} est premier.

Soit p le plus petit nombre premier ne divisant pas k. **On montre désormais que $a_{n-1}, a_{n-2}, \ldots, a_{n-p}$ sont premiers**, en procédant par récurrence décroissante sur l'indice de la suite. On a déjà que a_{n-1} est premier.

Supposons que $a_{n-1}, \ldots, a_{n-r}$ sont premiers avec $p-1 \geqslant r \geqslant 1$. Alors $a_n = a_{n-r} + kr$, donc $a_{n-r} \geqslant A - kr$. Si a_{n-r-1} est composé, $a_{n-r-1} = a_{n-r} + f(a_{n-r-1})$. De cette relation, on déduit $f(a_{n-r-1}) \mid a_{n-r}$, ce qui force $a_{n-r} = f(a_{n-r-1})$ (car a_{n-r} est premier). Mais alors $a_{n-r-1} = 2a_{n-r} \geqslant 2(A-kr)$. En choisissant A assez grand, par exemple A tel que $2(A-kp) \geqslant A$ (ce qui revient à choisir $A \geqslant 2kp$), on obtient que $2(A-kr) \geqslant A$. Cela contredit la minimalité de n. on déduit que a_{n-r-1} est également premier, ce qui achève la récurrence.

Cela implique que $a_{n-1}, \ldots, a_{n-p}$ sont tous premiers et deux à deux distincts modulo p, sont tous premiers. L'un d'entre eux, disons a_{n-i} étant nul modulo p, il vaut p. Mais alors $a_n = a_{n-i} + ik = p + ik$. En choisissant A suffisamment grand, par exemple A tel que $A > p + pk$, on obtient une contradiction car $a_n = p + ik \leqslant p + pk < A$. D'où la contradiction espérée.

Exercice 4.6. (BXMO 2012) Soit $a_1, a_2, \ldots$ une suite d'entiers positifs telle que, pour tout indice $n \geqslant 1$,

$$a_{n+1} = a_n + b_n,$$

où b_n est le dernier chiffre de a_n. Montrer que la suite (a_n) contient une infinité de puissances de 2 si et seulement si a_1 n'est pas divisible par 5.

Solution 4.6. On procède par double implication.

$\boxed{\Rightarrow :}$ Si $5 \mid a_1$, alors soit $b_1 = 0$ donc $a_2 = a_1$ et la suite est constante égale à a_1, soit $b_1 = 5$ et alors $b_2 = 0$ et $a_3 = a_2$ et la suite $(a_n)_{n\geqslant 2}$ est constante égale à a_2. Dans les deux cas, comme a_1 et a_2 sont divisibles par 5, ce ne sont pas des puissances de 2.

$\boxed{\Leftarrow :}$ Supposons que 5 ne divise pas a_1. Comme a_1 et b_1 sont de même parité, a_2 est pair et, pour tout $n \geqslant 2$, a_n est pair.

On observe ensuite que, pour tout $n \geqslant 2$, la suite (b_n) est périodique de période 4, et prend alternativement les valeurs $2, 4, 8, 6$(il suffit de distinguer selon la valeur de $b_n \in \{2, 4, 6, 8\}$). Ainsi, $\boxed{a_{n+4} = a_n + 20}$ pour tout entier $n \geqslant 2$.

Fixons désormais un indice m tel que $b_m = 2$. On a donc $a_m \equiv 2 \mod 20$ ou $a_m \equiv 12 \mod 20$. Remarquons que la suite (2^n) est périodique modulo 20 à partir du rang 2, et prend une infinité de fois les valeurs $4, 8, 16, 12$.

- ➢ Si $a_m \equiv 12 \mod 20$, la suite $(a_{m+4k})_k$ parcourt tous les entiers congrus à 12 modulo 20 et supérieurs à a_m. Comme la suite $(2^n)_n$ prend une infinité de fois la valeur 12 modulo 20, la suite (a_n) contient une infinité de puissances de 2.
- ➢ Si $a_m \equiv 2 \mod 20$, alors $a_{m+1} \equiv 4 \mod 20$. La suite $(a_{m+4k+1})_k$ parcourt tous les entiers congrus à 4 modulo 20 et supérieurs à a_m. Comme la suite $(2^n)_n$ prend une infinité de fois la valeur 4 modulo 20, la suite (a_n) contient une infinité de puissances de 2.

Dans tous les cas, la suite (a_n) contient une infinité de puissances de 2.

Exercice 4.7. (St Petersbourg 2017) Soit (a_n) une suite d'entiers définie par $a_1 > 10$ et, pour tout entier $n \geqslant 2$,

$$a_n = a_{n-1} + \mathrm{PGCD}(n, a_{n-1}),$$

On suppose qu'il existe un indice k tel que $a_k = 2k$. Montrer qu'il existe une infinité d'indices k tels que $a_k = 2k$.

Solution 4.7.

➢ **Commentaire :**

> Pour avancer sur le problème, il faut chercher à calculer $a_{k+1}, a_{k+2}, \ldots$. Par exemple, $a_{k+1} = 2k + \mathrm{PGCD}(k+1, 2k)$, et le PGCD vaut 1 si 2 ne divise pas $k-1$ et vaut 2 sinon. S'il vaut 2, on a le résultat voulu. S'il vaut 1, alors $a_{k+1} = 2k+1$.
>
> On a ensuite $a_{k+2} = a_{k+1} + \mathrm{PGCD}(k+2, 2k+1)$. Ce PGCD vaut 1 si 3 ne divise pas $k-1$, et 3 sinon. S'il vaut 3, on a alors $a_{k+2} = 2(k+2)$.
>
> De ces calculs, on observe le rôle du plus petit diviseur (premier) de $k-1$.

Soit p le plus petit diviseur premier de $k+1$. On montre par récurrence sur $0 \leqslant \ell \leqslant p-2$ que $a_{k+\ell} = 2k + \ell$.

- ➢ Initialisation : Pour $\ell = 0$, on a bien $a_k = 2k$.
- ➢ Hérédité : On suppose avoir montré $a_{k+\ell} = 2k + \ell$ pour un certain $0 \leqslant \ell \leqslant p-3$. On a alors

$$a_{k+\ell+1} = a_{k+\ell} + \mathrm{PGCD}(k+\ell+1, a_{k+\ell}) = 2k + \ell + \mathrm{PGCD}(k+\ell+1, 2k+\ell).$$

Or, si d divise $k+\ell+1$ et $2k+\ell$, il divise aussi $k-1$ et $\ell+2$. Puisque $\ell+2 \leqslant p-1$, ce PGCD vaut 1. Il en résulte que $a_{k+\ell+1} = 2k+\ell+1$, ce qui achève la récurrence.

On a alors

$$a_{k+p-1} = a_{k+p-2} + \mathrm{PGCD}(k+p-1, a_{k+p-2}) = 2k + p - 2 + \mathrm{PGCD}(k+p-1, 2k+p-2).$$

Là, $\mathrm{PGCD}(k+p-1, 2k+p-2) = \mathrm{PGCD}(k-1, p) = p$, ce qui implique que $a_{k+p-1} = 2k+p-2+p = 2(k+p-1)$, ce qui conclut l'exercice.

Exercice 4.8. (PAMO 2021 P3) Soit (a_n) une suite d'entiers définie par $a_1 \geqslant 2$ et, pour tout entier $n \geqslant 1$, $a_{n+1} = a_n + a_n/p_n$, où p_n est le plus petit diviseur premier de a_n.
Montrer qu'il existe un entier $N \geqslant 1$ tel que $a_{n+3} = 3a_n$ pour tout $n > N$.

Solution 4.8.

➢ **Commentaire :**

> On peut faire deux observations :
> ➢ Si a_n est pair, alors $v_2(a_{n+1}) = v_2(a_n) - 1$.
> ➢ Si $p_n = 3$, alors $a_{n+3} = 3a_n$ et on a facilement que $a_{k+3} = 3a_k$ pour tout $k \geqslant 3$.
> Il suffit donc de montrer que $p_n = 3$ pour un certain indice n.

Si a_1 est impair, alors a_1/p_1 est impair donc a_2 est pair. On peut donc d'emblée supposer que a_1 est impair quitte à décaler d'un cran la suite.

Étape 1 : Il existe un indice n tel que $p_n = 3$.

On écrit $a_1 = 2^\alpha\beta$ avec β impair et $\alpha \geqslant 1$. On déduit que

$$a_2 = 2^\alpha\beta + 2^{\alpha-1}\beta = 2^{\alpha-1}3\beta \quad \Longrightarrow \quad v_2(a_2) = v_2(a_1) - 1.$$

Par récurrence immédiate, on déduit que $a_{1+\alpha} = 3^\alpha\beta$ et $p_{1+\alpha} = 3$.

Étape 2 : Si $p_n = 3$, alors $a_{k+3} = 3a_k$ pour tout $k \geqslant n$.

On montre par récurrence sur $k \geqslant 0$ sur $(a_{n+1+3k}, a_{n+2+3k}, a_{n+3+3k}) = (3a_{n+1+3(k-1)}, 3a_{n+2+3(k-1)}, 3a_{n+3+3(k-1)})$ et $(p_{n+1+3k}, p_{n+2+3k}, p_{n+3+3k}) = (2, 2, 3)$.
Initialisation : Puisque $a_n = 3^\alpha\beta$ avec $\alpha \geqslant 1$ et β impair, $p_n = 3$ et un calcul direct donne

$$a_{n+1} = \frac{4}{3}a_n,\ p_{n+1} = 2, \quad a_{n+2} = 2a_n,\ p_{n+2} = 2, \quad a_{n+3} = 3a_n, ; p_{n+3} = 3.$$

On suppose la propriété vérifiée pour $k \geqslant 0$ fixé. Posons $N = n + 3k$. C'est le même calcul direct :

$$a_{N+1} = \frac{4}{3}a_N,\ p_{N+1} = 2, \quad a_{N+2} = 2a_N,\ p_{N+2} = 2, \quad a_{N+3} = 3a_N, ; p_{N+3} = 3.$$

Ceci achève la récurrence et conclut.

Exercice 4.9. (Belarus Iran 2022) Pour tout entier $n \geqslant 1$, on note $d(n)$ est le nombre de diviseurs positifs de n. Existe-t-il une suite $a_1, a_2, \ldots$ d'entiers strictement positifs telle que pour tous indices i et j,

$$d(a_i + a_j) = i + j\,?$$

Solution 4.9. **Réponse :** Il n'existe pas de telle suite.

Deviner la réponse (et s'il faut plutôt chercher une construction ou un argument pour réfuter l'énoncé) fait partie de la difficulté de l'exercice. Heureusement, quelle que soit la conjecture que l'on formule, chercher à la démontrer passe par l'extraction d'un maximum d'informations sur la suite. Supposons donc qu'une telle suite existe.

Tout d'abord, on remarque que pour $i = j$, on trouve $d(2a_i) = 2i$. En particulier, la suite (a_i) est injective.

D'autre part, pour tout entier $i \geqslant 1$, on a $d(a_{2i} + a_1) = 2i + 1$. Cela signifie que le nombre $a_{2i} + a_1$ est un carré parfait pour tout entier i. De la même façon, le nombre $a_{2i} + a_3$ est un carré parfait pour tout i.

Le dernier ingrédient pour conclure est la croissance des carrés parfaits, qui est linéaire. Ainsi, les suites $(a_{2i}+a_1)$ et $(a_{2i} + a_3)$ ne peuvent pas être des suites de carrés parfaits qui tendent vers $+\infty$ et donc la différence est bornée.

Plus précisément, on pose $A = |a_3 - a_1|$, qui est non nul par injectivité. Comme $d(2a_{2i}) = 4i$ pour tout i, la suite $(d(2a_{2i}))_i$ est non bornée, donc la suite (a_{2i}) est également non bornée. On dispose d'un indice i tel que $a_{2i} + a_1 > 4A^2$. Mais alors $a_{2i} + a_1$ est un carré parfait vérifiant

$$(\sqrt{a_{2i} + a_1} - 1)^2 < a_{2i} + a_1 - A \leqslant a_{2i} + a_3 \leqslant a_{2i} + a_1 + A < (\sqrt{a_{2i} + a_1} + 1)^2,$$

mais qui est distinct de $a_{2i} + a_1$, ce qui est absurde. Il n'existe donc pas de telle suite.

Exercice 4.10. (Dutch BXMO TST 2019) Existe-t-il un entier $k \geqslant 1$ et une suite non constante $a_1, a_2, \ldots$ telle que $a_n = \mathrm{PGCD}(a_{n+k}, a_{n+k+1})$ pour tout indice $n \geqslant 1$?

Solution 4.10. Pour comprendre l'exercice, il est essentiel de comprendre les cas $k = 2$ et $k = 3$. Ces cas mettent en lumière la stratégie à adopter : on va montrer que $a_n \mid a_{n+1}$ pour tout n. Cela implique d'abord que la suite est croissante, mais aussi que $a_n = \mathrm{PGCD}(a_{n+k}, a_{n+k+1}) = a_{n+k}$, donc la suite est croissante et périodique, elle est donc constante.

Puisque $a_n \mid a_{n+k}$ et $a_n \mid a_{n+k+1}$ pour tout indice n, on a par récurrence que $\boxed{a_n \mid a_{n+ak+b(k+1)}}$ pour toute paire d'entiers positifs (a, b). Pour montrer que $a_n \mid a_{n+1}$, il suffit de montrer que a_n divise a_{n+k+1} et a_{n+k+2}. La première divisibilité vient de la relation de l'énoncé, on montre désormais la deuxième divisibilité. On a $a_n \mid a_{n+k^2}$ et $a_n \mid a_{n+(k-1)(k+1)}$, donc $a_n \mid \mathrm{PGCD}(a_{n+k^2}, a_{n+k^2-1}) = a_{n+k^2-k-1}$. On montre alors par récurrence descendante sur r que $a_n \mid a_{n+k+2+(k+1)r}$. C'est déjà le cas pour $r = k - 2$. On suppose que c'est le cas pour un certain $r \leqslant k - 2$. On a donc $a_n \mid a_{n+k+2+(k+1)r}$ et $a_n \mid a_{n+(k+1)(r+1)}$, donc $a_n \mid \mathrm{PGCD}(a_{n+(k+1)(r+1)}, a_{n+k+2+(k+1)r}) = a_{n+(k+1)r-k} = a_{n+k+2+(k+1)(r-1)}$. Ceci achève la récurrence. En particulier, pour $r = 0$, on trouve $a_n \mid a_{n+k+2}$, donc $a_n \mid a_{n+1}$, ce qui nous permet de conclure.

Exercice 4.11. (Iran 2017 Round 2)

1. Montrer qu'il n'existe pas de suites $a_1, a_2, \ldots$ d'entiers strictement positifs telles que pour toute pair (i, j) d'indices distincts, $\mathrm{PGCD}(a_i + j, a_j + i) = 1$.
2. Soit p un nombre premier impair. Montrer qu'il existe une suite $a_1, a_2, \ldots$ d'entiers strictement positifs telle que pour toute pair (i, j) d'indices distincts, $\mathrm{PGCD}(a_i + j, a_j + i)$ n'est pas divisible par p.

Solution 4.11.

1. Montrons qu'il existe un couple (i, j) tel que $a_i + j$ et $a_j + i$ sont pairs. En effet, si ce n'est pas le cas, alors $(a_i + j) + (a_j + i)$ est toujours impair. Comme ce nombre vaut $(a_i + i) + (a_j + j)$, cela veut dire que $a_i + i$ et $a_j + j$ ne sont jamais de même parité, ce qui est absurde en appliquant le principe des tiroirs à trois indices i, j et k.
2. La question précédente nous incite à construire une suite satisfaisant la condition plus forte que $(a_i + i) + (a_j + j)$ n'est jamais divisible par p. Pour cela, il suffit de choisir $a_i \equiv 1 - i \mod p$ (ce qui est le cas par exemple en posant $a_i = pi + 1 - i$. On a alors $(a_i + i) + (a_j + j) \equiv 2 \mod p$, donc p ne peut pas diviser à la fois $a_i + j$ et $a_j + i$.

Exercice 4.12. (IMO 2017 P1) Pour tout entier $a_0 > 1$, on définit la suite $a_0, a_1, \ldots$ par

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } a_n \text{ est un carré parfait} \\ a_n + 3 & \text{sinon} \end{cases}$$

Déterminer toutes les valeurs de a_0 pour lesquelles il existe un nombre A tel que $a_n = A$ pour une infinité de valeurs de n.

Solution 4.12. **Réponsé :** Il s'agit des a_0 qui sont multiples de 3.

On regarde les valeurs de la suite pour les petites valeurs de a_0 pour deviner la réponse.

On remarque alors par exemple que si $a_0 \equiv 2 \mod 3$, alors a_0 n'est pas un carré parfait, donc $a_1 = a_0 + 3 \equiv 2 \mod 3$. On déduit que a_1 n'est pas un carré parfait non plus. Un récurrence immédiate nous donne alors que $a_{n+1} = a_n + 3$ pour tout entier n, de sorte que la suite est strictement croissante, elle ne peut donc pas prendre une même valeur une infinité de fois et elle ne vérifie pas l'énoncé.

On traite les deux autres cas.

- Si $a_0 \equiv 0 \mod 3$, on remarque après quelques essais que la suite finit par "boucler" et prendre consécutivement les valeurs $3, 6$ et 9 à partir d'un certain rang. Montrons-le.
  Soit j tel que a_j est le minimum de l'ensemble des valeurs prises par la suite (a_n). Supposons que $a_j > 9$. Soit k tel que $[3(k-1)]^2 < a_j \leqslant (3k)^2$. On a alors $k \geqslant 2$. La suite $(a_{j+n})_n$ parcourt tous les multiples de 3 jusqu'à atteindre $9k^2$, disons au rang N. On a alors, puisque $k \geqslant 2$,

  $$a_{n+1} = 3k < 9(k-1)^2 < a_j$$

  ce qui contredit la minimalité de a_j. On déduit que $a_j \leqslant 9$. Mais alors $a_j \in \{0, 3, 6, 9\}$. Dans chaque cas, la suite (a_{j+n}) est périodique à partir du rang j, de sorte qu'elle vérifie la propriété de l'énoncé.
- Si $a_0 \equiv 1 \mod 3$: Montrons qu'il existe un terme de la suite congru à 2 modulo 3. C'est le cas si $a_0 = 4$ ou 7. Supposons que $a_0 \geqslant 10$ et prenons à nouveau j tel que a_j est le minimum de la suite (a_n). Supposons que $a_j \geqslant 10$. Prenons t^2 le plus petit carré supérieur ou égal à a_j. Alors la suite (a_{j+n}) prend l'une des valeurs $t^2, (t+1)^2, (t+2)^2$, disons au rang N. Mais alors

  $$a_{N+1} \leqslant t + 2 \leqslant (t-1)^2 < a_j$$

  ce qui contredit la minimalité de a_j. Ainsi, $a_j \leqslant 7$, ce qui nous ramène aux cas traités. Comme la suite prend une valeur congrue à 2 mod 3, elle est strictement croissante à partir d'un certain rang et ne vérifie pas la propriété de l'énoncé.

Les valeurs recherchées sont donc les multiples de 3.

Exercice 4.13. (ELMO 2019 P1) Soit P un polynôme à coefficients entiers tel que $P(0) = 1$ et soit $c > 1$ un entier. On définit la suite (x_n) par $x_0 = 0$ et $x_{n+1} = P(x_n)$ pour tout $n \geqslant 0$. Montrer qu'il existe une infinité d'entiers n tels que $\text{PGCD}(x_n, n + c) = 1$.

Solution 4.13.

➢ Commentaire :

> Le premier réflexe est d'écrire ce qu'implique la relation $a - b \mid P(a) - P(b)$, valide puisque P est à coefficients entiers. Celle-ci implique notamment que $x_n - x_m \mid x_{n+k} - x_{m+k}$ pour tous entiers m, n, k.
>
> Le deuxième réflexe, c'est de chercher les indices n pour lesquels $n + c$ est un nombre premier p, puisqu'alors il suffit de vérifier que p ne divise pas x_n. Si on suppose qu'au contraire $p \mid x_n$, alors $x_n \equiv x_0 \mod p$, et la relation ci-dessus implique que la suite (x_n) est périodique modulo p, de période n. On remarque qu'en plus $x_1 \neq 0 \mod p$, donc cette suite n'est pas la suite nulle modulo p.
>
> Comme aucune contradiction ne semble sortir, la dernière idée à sortir pour ce problème est d'envisager un résultat du type "si $p \mid x_n$, alors on trouve un entier k tel que p ne divise pas $x_{p^k - c}$", ce qui est suffisant car alors $\text{PGCD}(x_{p^k-c}, p^k) = 1$. Il faut pour cela jouer avec la période n de la suite. Les calculs font apparaître un cahier des charges sur p, et il ne reste plus qu'à mettre en forme.

Si $x_{c^2-c} = 0$, alors la suite (x_n) est périodique de période $c^2 - c$ et en particulier $x_{k(c^2-c)+1} = x_1 = 1$ pour tout entier k. Il suffit donc de choisir $n = k(c^2 - c) + 1$, puisqu'alors $\text{PGCD}(x_n, n + c) = \text{PGCD}(1, n + c) = 1$. On a alors l'infinité voulue. Dans la suite, on suppose que $x_{c^2-c} \neq 0$.

Soit p un nombre premier ne divisant ni x_{c^2-c} ni c. On montre que l'entier $n = p - c$ ou l'entier $n = p^2 - c$ vérifie $\text{PGCD}(x_n, n+c) = 1$. En faisant varier p, cela donne bien une famille infinie d'indice, puisque les entiers $n + c$ ainsi obtenus sont bien deux à deux distincts.

On pose $n_0 = p - c$. Si p ne divise pas x_{n_0}, alors le choix de $k = 1$ convient. On suppose désormais que $p \mid x_{n_0}$. Puisque, pour tout k, $p \mid x_{n_0} - x_0 \mid P^{(k)}(x_{n_0}) - P^{(k)}(x_0) = x_{n_0+k} - x_k$, la suite (x_n) est périodique modulo p. On note t sa plus petite période. Notons que $t \geqslant 2$ car $x_1 = P(0) = 1 \neq x_0 \mod p$. De plus, t est un diviseur de n_0 : si on pose $n_0 = qt + r$ avec $r < t$ la division euclidienne de n_0 par t, et que l'on suppose que $r > 0$, alors on trouve que $x_r \equiv x_n \equiv 0 \mod p$ par $t-$périodicité, et le raisonnement ci-dessus permettrait d'établir que la suite (x_n) est $r-$périodique, contredisant la minimalité de t.

Notons que $c^2 - c \neq 0 \mod t$, puisque le contraire impliquerait $x_{c^2-c} \equiv x_0 \equiv 0 \mod p$, ce qui est exclu par notre choix de p. On déduit que

$$p^2 - c \equiv c^2 - c \neq 0 \mod t, \Longrightarrow x_{p^2-c} \neq 0 \mod p,$$

et alors $\text{PGCD}(x_{p^2-c}, p^2 - c + c) = 1$, comme voulu.

Exercice 4.14. *(Balkan MO SL 2021 N2)* Pour tout $n > 1$, on note $\ell(n)$ le plus grand facteur premier de n. Soit (a_n) la suite définie par $a_1 = 2$ et $a_{n+1} = a_n + \ell(a_n)$ pour tout $n \geqslant 1$. Déterminer tous les entiers k tels qu'il existe au moins un indice n pour lequel $a_n = k^2$.

Solution 4.14. **Réponse :** Les entiers k sont exactement les nombres premiers.

Notons $p_1 = 2, p_2, p_3, \dots$ la suite croissante des nombres premiers.

En calculant les premières valeurs de la suite, on devine que, la suite (a_n) est la concaténation de blocs de la forme

$$p_i^2, p_i(p_i+1), \dots, p_i(p_{i+1}-1), p_ip_{i+1}, p_{i+1}(p_i+1), p_{i+1}(p_i+2), \dots p_{i+1}(p_{i+1}-1), p_{i+1}^2.$$

C'est ce que l'on prouve par récurrence sur i.

- **Initialisation :** Si $i = 1$, on a $a_1 = 2$ puis $a_2 = 2^2$. De plus, on vérifie que les termes suivants de la suite sont $6, 9$, qui correspondent aux derniers temres des blocs bleus et violets ci-dessus.
- **Hérédité :** On suppose avoir montré que les premiers termes de la suite pouvaient être rangés en blocs consécutifs bleus et violets de la forme ci-dessus, et ce jusqu'au terme d'indice k tel que $a_k = p_i^2$, avec $i \geqslant 2$ fixé.

  Notons $\delta = p_{i+1} - p_i$. Puisque p_{i+1} est le plus petit nombre premier supérieur à p_i, les facteurs premiers des nombres $p_i+1, p_i+2, \dots, p_i+\delta-1$ sont tous inférieurs ou égaux à p_i. Cela signifie que $\ell(p_i(p_i+k)) = p_i$ pour tout $k = 0, \dots, \delta-1$. Un récurrence immédiate donne alors que

  $$(a_k, a_{k+1}, \dots, a_{k+\delta}) = (p_i^2, p_i(p_i+1), \dots, p_i(p_i+\delta)).$$

  Mais alors $\ell(p_i(p_i+\delta)) = \ell(p_ip_{i+1}) = p_{i+1}$. Comme on a encore $\ell(p_{i+1}(p_i+k)) = p_{i+1}$ pour tout $k = 0, \dots, \delta-1$, une récurrence donne

  $$(a_{k+\delta+1}, \dots, a_{k+2\delta}) = (p_{i+1}(p_i+1), p_{i+1}(p_i+2), \dots p_{i+1}(p_{i+1}-1), p_{i+1}^2).$$

  Ceci achève l'hérédité.

On déduit que tous les nombres premiers sont solutions de l'exercice. Pour montrer que ce sont les seuls, il suffit de vérifier qu'aucun autre carré que p_i^2 ou p_{i+1}^2 n'est contenu dans les blocs bleus et violets précédents.

Il n'y a pas d'autre carré dans le bloc violet car p_{i+1} ne divise aucun des nombres $p_i + k$ pour $k = 0, \dots, \delta-1$ (il est strictement plus grand que ces nombres), donc la valuation $p_{i+1}-$adique de ces nombres vaut 1.

D'autre part, d'après le postulat de Bertand, $p_i < p_{i+1} < 2p_i$ donc $\delta < p_i$. Ainsi, p_i ne divise aucun des nombres $p_i + k$ pour $k = 1, \dots, \delta$ (ils sont tous dans l'intervalle $[\![p_i+1, 2p_i-1]\!]$), donc la valuation p_i-adique de ces nombres vaut 1.

Ceci prouve que les seuls carrés apparaissant dans la suites sont les carrés des nombres premiers.

Exercice 4.15. *(IMO SL 2008 N3)* Soit $a_0, a_1, \ldots$ une suite d'entiers strictement positifs telle que $\mathrm{PGCD}(a_{i+1}, a_i) > a_{i-1}$ pour tout indice $i \geqslant 1$. Montrer que, pour tout entier $n \geqslant 0$, $a_n \geqslant 2^n$.

Solution 4.15. L'une des premières choses raisonnables à essayer sur cet exercice est de procéder par récurrence sur n. On remarque d'emblée que, pour tout indice n, $a_n \geqslant \mathrm{PGCD}(a_{n+1}, a_n) > a_{n-1}$, de sorte que la suite est strictement croissante. On peut alors raffiner l'inégalité (ce qui épargne quelques disjonctions de cas plus tard) pour trouver que, puisque $\mathrm{PGCD}(a_n, a_{n-1})$ divise $a_n - a_{n-1}$,

$$a_n - a_{n-1} \geqslant \mathrm{PGCD}(a_n, a_{n-1}) > a_{n-2} \Longrightarrow a_n \geqslant a_{n-1} + a_{n-2} + 1.$$

Initialisation : On s'en rend compte au moment de l'hérédité, il y a besoin de montrer le résultat pour a_0, a_1, a_2 et a_3. On a déjà $a_0 \geqslant 1 = 2^0$. De plus, $\mathrm{PGCD}(a_1, a_2) > a_0 = 1$ donc $a_1 \geqslant \mathrm{PGCD}(a_1, a_2) \geqslant 2$. Au vu de l'inégalité ci-dessus, $a_2 \geqslant a_1 + a_0 + 1 \geqslant 4$. De même $a_3 \geqslant a_2 + a_1 + 1 \geqslant 7$. Mais si $a_3 = 7$, on a $a_2 + a_1 + 1 = 7$, donc $a_2 = 4$ et $a_1 = 2$, mais alors $2 > 1 = \mathrm{PGCD}(a_2, a_3)$, ce qui est absurde, si bien que $a_3 \geqslant 8$. L'énoncé est donc vérifie pour $n = 0, 1, 2, 3$.

Hérédité : On suppose que $a_k \geqslant 2^k$ pour tout $k \leqslant n$, avec $n \geqslant 3$ un entier fixé. On suppose par l'absurde que $a_{n+1} < 2^{n+1}$.

Pour tout $k \geqslant 0$, on pose $d_k = \mathrm{PGCD}(a_{k+1}, a_k)$. On pose α et β tels que $a_{n+1} = \alpha d_n$ et $a_n = \beta d_n$, avec $1 \leqslant \beta < \alpha$ par stricte croissance de la suite. Par hypothèse de l'énoncé et par hypothèse de récurrence, $d_n > a_{n-1} \geqslant 2^{n-1}$. Comme en plus $\alpha d_n < 2^{n+1}$, on trouve que $\alpha < 4$. D'autre part, si $\beta = 1$, on a $d_n = \beta d_n = a_n \geqslant 2^n$, donc $a_{n+1} \geqslant 2d_n \geqslant 2^{n+1}$, ce qui est absurde. On déduit que $\beta \geqslant 2$ et $\alpha \leqslant 3$, ce qui conduti à $\boxed{a_n = 2d_n \text{ et } a_{n+1} = 3d_n}$.

➢ Commentaire :

> L'idée est alors d'itérer ce raisonnement jusqu'à ce que mort s'ensuive. De nombreuses tentatives de solutions (sur internet) ne semblaient utiliser que les indices $n-1, n$ et $n+1$, mais se sont avérées infructueuses. Faire une récurrence avec au moins trois crans semble nécessaire. La précaution est donc de mise si vous disposez d'une solution n'utilisant que les indices $n-1, n$ et $n+1$.

Soit γ tel que $a_n = \gamma d_{n-1}$. Puisque $\gamma d_{n-1} = a_n = 2d_n > 2d_n$, on a $\gamma \geqslant 3$. D'autre part,

$$\frac{2^{n+2}}{3} > \frac{2}{3} a_{n+1} = a_n = \gamma d_{n-1} > \gamma a_{n-2} \geqslant \gamma 2^{n-2},$$

ce qui implique que $\gamma \leqslant 5$. Mais si $\gamma \leqslant 4$, on a $a_{n-1} < d_n = \frac{1}{2} a_n = \frac{1}{2} \gamma d_{n-1} \leqslant 2d_{n-1}$. Comme d_{n-1} divise a_{n-1}, l'inégalité $a_{n-1} < 2d_{n-1}$ implique que $a_{n-1} = d_{n-1}$. Il vient

$$2^{n+1} > a_{n+1} = \frac{3}{2} a_n = \frac{3}{2} \gamma d_{n-1} = \frac{3}{2} \gamma a_{n-1} \geqslant \frac{3}{2} \cdot 32^{n-1},$$

ce qui est une contradiction. On déduit que $\gamma = 5$ et que $\boxed{a_n = 5d_{n-1}}$. Mais alors $a_{n+1} = \frac{15}{2} d_{n-1}$ et $d_n = \frac{5}{2} d_{n-1}$. Comme $d_n > a_{n-1}$, on a $a_{n-1} = d_{n-1}$ ou $a_{n-1} = 2d_{n-1}$.

Plutôt que de considérer le rapport $\frac{a_{n-1}}{d_{n-2}}$ comme dans les cas précédents, on va directement considérer $\frac{2d_{n-1}}{d_{n-2}}$ et poser δ tel que $2d_{n-1} = \delta d_{n-2}$. Comme $d_{n-2} < d_{n-1}$, on a $\delta \geqslant 3$. On écrit toutes les données en fonction de d_{n-2} et δ, à savoir

$$a_{n+1} = \frac{15}{4} \delta d_{n-2}, \quad a_n = \frac{5}{4} \delta d_{n-2}, d_{n-1} = \frac{\delta}{2} d_{n-2}.$$

Si $\delta \geqslant 5$, alors

$$a_{n+1} \geqslant \frac{15}{4} \cdot 5d_{n-2} \geqslant \frac{75}{4} a_{n-3} \geqslant \frac{75}{4} 2^{n-3} > 2^{n+1},$$

ce qui est absurde. Si $3 \leqslant \delta \leqslant 4$, alors $a_{n-2} < d_{n-1} = 2d_{n-2}$, donc $a_{n-2} = d_{n-2}$. Il vient que

$$a_{n+1} \geqslant \frac{15}{4} \delta d_{n-2} = \frac{15}{4} \delta a_{n-2} \geqslant \frac{15}{4} \cdot 3 \cdot 2^{n-2} > 2^{n+1},$$

ce qui est encore absurde. On a donc conclu.

Solution alternative

La solution suivante, très astucieuse, voit le problème comme un problème d'inégalités. Avec la notation $d_n = \mathrm{PGCD}(a_n, a_{n+1})$, pour tout indice $n \geqslant 1$, on dispose de deux entiers x_n et y_n premiers entre eux tels que $a_{n+1} = x_n d_n$ et $a_n = y_n d_n$. La condition de l'énoncé donne alors

$$a_{n-1} < \mathrm{PGCD}(a_n, a_{n+1}) = d_n = \frac{a_n}{y_n}.$$

Il vient que $y_n < \dfrac{a_n}{a_{n-1}} = \frac{x_{n-1}}{y_{n-1}}$, soit $x_n \geqslant 1 + y_n y_{n-1}$, soit encore $\dfrac{x_{n-1}}{y_{n-1}} \geqslant y_n + \dfrac{1}{y_{n-1}}$. On a alors le télescopage suivant, que l'on combina avec l'inégalité des moyennes :

$$\begin{aligned} a_n &= \frac{a_n}{a_{n-1}} \cdot \frac{a_{n-1}}{a_{n-2}} \cdot \ldots \cdot \frac{a_1}{a_0} a_0 \\ &\geqslant \left(y_n + \frac{1}{y_{n-1}}\right)\left(y_{n-1} + \frac{1}{y_{n-2}}\right) \ldots \left(y_1 + \frac{1}{y_0}\right) a_0 \\ &\geqslant 2\sqrt{\frac{y_n}{y_{n-1}}} \cdot 2\sqrt{\frac{y_{n-1}}{y_{n-2}}} \cdot \ldots \cdot \sqrt{\frac{y_1}{y_0}} a_0 \\ &= 2^n a_0 \sqrt{\frac{y_n}{y_0}}. \end{aligned}$$

Or $a_0 = y_0 d_0 \geqslant y_0$, soit $a_0\sqrt{\frac{y_n}{y_0}} \geqslant \sqrt{y_0 y_n} = 1$. On a donc le résultat voulu.

Exercice 4.16. (IMO SL 2015 N4) Soient $a_0, a_1, \ldots$ et $b_0, b_1, \ldots$ des suites d'entiers strictement positifs vérifiant $a_0, b_0 \geqslant 2$ et, pour tout entier $n \geqslant 0$,

$$a_{n+1} = \mathrm{PGCD}(a_n, b_n) + 1, \quad b_{n+1} = \mathrm{PPCM}(a_n, b_n) - 1.$$

Montrer qu'il existe un entier N et un entier t tels que, pour tout $n \geqslant N$, $a_{n+t} = a_n$.

Solution 4.16.

➢ Commentaire :

> Il convient de tester l'énoncé pour des suites particulières pour conjecturer les comportements des suites. Dans les premiers pas, on étudie les variations de la suite a_n, et effectuant quelques comparaisons.
>
> Par exemple, on a que $a_{n+1} \leqslant a_n + 1$, avec égalité si et seulement si $a_n \mid b_n$, auquel cas $b_{n+1} = b_n - 1$. Comme la suite (b_n) n'est pas strictement décroissante, le cas précédent ne peut pas se produire pour tout n, et on a $a_{n+1} \leqslant a_n$ pour une infinité d'indices n. De cette première discussion, on comprend qu'on ne peut pas attendre de variations claires sur la suite (a_n).
>
> Dans les énoncés visant à montrer qu'une suite est périodique, une étape intermédiaire est souvent de montrer qu'elle est bornée. Dans le cas de la suite (a_n), pour montrer qu'elle est bornée, il faut donc étudier les indices n pour lesquels $a_{n+1} \leqslant a_n$, puisqu'ils correspondent à des maxima locaux de la suite. Si ces maxima locaux sont bornés, la suite (a_n) le sera aussi.

Pour tout entier n, $a_{n+1} = \mathrm{PGCD}(a_n, b_n) + 1 \leqslant a_n + 1$, avec égalité si et seulement si $a_n \mid b_n$.

Si on avait $a_{n+1} \geqslant a_n$ pour tout indice n à partir d'un certain rang N, on aurait $a_n \mid b_n$ pour tout $n \geqslant N$ et alors $b_{n+1} = b_n - 1$ pour tout $n \geqslant N$, faisant de la suite (b_n) une suite strictement décroissante d'entiers positifs, ce qui est absurde. Ainsi, on dispose d'une suite (n_i) d'indices tels que $a_{n_i+1} \leqslant a_{n_i}$ pour tout indice i. On suppose dans la suite que les n_i sont consécutifs pour cette propriété. Le lemme suivant se conjecture en testant l'énoncé pour des cas particuliers.

Lemme : la suite $(a_{n_i})_i$ est décroissante.

Preuve : Supposons qu'il existe un indice i tel que $a_{n_{i+1}} > a_{n_i}$. On note $n = n_i$ et $N = n_{i+1}$. Par définition de la suite (n_i), on a $a_m = a_{m-1} + 1$ pour tout $n + 1 \leqslant m \leqslant N - 1$. En notant $d = \mathrm{PGCD}(a_n, b_n)$ et $(\alpha, \beta) = (a_n/d, b_n/d)$, on a $(a_m, b_m) = (d + m - n, d\alpha\beta - (m - n))$ pour tout $n + 1 \leqslant m \leqslant N$.

Comme $a_{n+1} < a_{n_i} < a_N$, il existe un indice $n + 1 \leqslant k \leqslant N - 1$ tel que $a_n = a_k$. On a alors, au vu de la relation plus haut, $d\alpha = d + k - n$, d'où $(a_k, b_k) = (d\alpha, d\alpha\beta + d - d\alpha)$. Mais alors $\mathrm{PGCD}(d\alpha, d\alpha\beta + d - d\alpha) = \mathrm{PGCD}(d, d\alpha) = d$, donc $a_{k+1} = d + 1 = a_{n+1} \leqslant a_n = a_k$. Cela contredit le fait que n et N sont consécutifs pour cette propriété. □

Ainsi, la suite (a_{n_i}) est décroissante. Comme il s'agit d'une suite positive, elle est constante égale à un entier A à partir d'un certain rang N. Or, pour tout $n_i \geqslant N$ et tout $n_{i-1} + 1 \leqslant m \leqslant n_i$, on a $a_m \leqslant a_{n_i} = A$, donc la suite $(a_n)_{n \geqslant n_N}$ est également bornée par A, forçant la suite (a_n) à être bornée.

➢ Commentaire :

> D'après le principe des tiroirs, on a donc deux indices n et m tels que $a_n = a_m$. Mais pour en déduire que $a_{n+1} = a_{m+1}$, on constate qu'il faut connaître les valeurs de b_n et b_m. Il faudrait donc un principe des tiroirs sur le couple (a_n, b_n), sauf que la suite (b_n) n'a pas vocation à être bornée. En revanche, l'algorithme d'Euclide ne nécessite pas la valeur de b_n mais plutôt la valeur de $b_n \mod a_n$. En raffinant cet argument, c'est comme cela que l'on conclut.

Notons $M = \mathrm{PPCM}(a_0, a_1, \ldots)$ le plus petit commun multiple des a_i, qui est bien fini car la suite (a_n) prend un nombre fini de valeurs. Notons r_n le reste de la division de b_n par M. La suite (r_n) est alors bornée par M. D'après le principe des tiroirs, il existe deux indices $n < m$ tels que $(a_n, r_n) = (a_m, r_m)$. Notons que, pour tout indice ℓ, on a $\mathrm{PGCD}(a_\ell, b_\ell) = \mathrm{PGCD}(a_\ell, r_\ell)$. On a alors

$$r_{\ell+1} \equiv b_{\ell+1} = \mathrm{PPCM}(a_\ell, b_\ell) - 1 = \frac{a_\ell}{\mathrm{PGCD}(a_\ell, b_\ell)} b_\ell - 1 \equiv \frac{a_\ell}{\mathrm{PGCD}(a_\ell, r_\ell)} - 1 \mod M,$$

de sorte que

$$r_{n+1} \equiv \frac{a_n}{\mathrm{PGCD}(a_n, r_n)} - 1 = \frac{a_m}{\mathrm{PGCD}(a_m, r_m)} - 1 \equiv r_{m+1} \mod M \implies r_{n+1} = r_{m+1}$$

et $a_{n+1} = \mathrm{PGCD}(a_n, r_n) + 1 = \mathrm{PGCD}(a_m, r_m) + 1 = a_{m+1}$. On a alors, pour $t = m - n$, par récurrence immédiate, que $(a_{\ell+t}, r_{\ell+t}) = (a_\ell, r_\ell)$ pour tout $\ell \geqslant n$.

Exercice 4.17. (China TST 2016) Soit $c, d \geqslant 2$ des entiers naturels. Soit (a_n) la suite définie par $a_1 = c$ et $a_{n+1} = a_n^d + c$. Montrer que pour tout $n \geqslant 2$, il existe un nombre premier p tel que $p \mid a_n$ et p ne divise aucun des a_i pour $i = 1, \ldots, n-1$.

Solution 4.17. On commence par examiner les propriétés de la suite. En posant $P(X) = X^d + c$, cette suite satisfait $a_1 = P(0)$ et $a_{n+1} = P(a_n) = P^{(n)}(0)$, où la notation $P^{(n)}$ désigne la $n-$ème itérée de P. Ainsi, puisque P est à coefficients entier, l'itération de la relation $x - y \mid P(x) - P(y)$ donne que pour tout n,

$$a_n = a_n - 0 \mid P^{(\ell)}(a_n) - P^{(\ell)}(0) = a_{n+\ell} - a_\ell.$$

En particulier, si d divise a_n et a_m, puisqu'on a $a_{n-m} \equiv a_n \mod a_m$ donc d divise a_{n-m}. Mais on a aussi que si $d \mid a_m$ et a_{n-m}, alors puisqu'on a $a_n \equiv a_{n-m} \mod a_m$, on a déduit que $d \mid a_n$. On déduit que $\boxed{\mathrm{PGCD}(a_n, a_m) = \mathrm{PGCD}(a_n, a_{n-m})}$. Cette relation est suffisante pour enclencher l'algorithme d'Euclide, qui implique que $\mathrm{PGCD}(a_n, a_m) = \mathrm{PGCD}(a_{\mathrm{PGCD}(n,m)}, a_0) = a_{\mathrm{PGCD}(n,m)}$, avec la convention que $a_0 = 0$.

On n'a pas encore utilisé la forme particulière de P. On a la divisibilité raffinée suivante :

$$a_n^d = P(a_n) - c = P(a_n) - P(0) \mid P^{(\ell)}(a_n) - P^{(\ell)}(0) = a_{n+\ell} - a_\ell.$$

On va conclure avec cette relation. Supposons par l'absurde que a_n ne possède aucun facteur premier ne divisant pas $a_1 \ldots a_{n-1}$. Soit p un facteur premier quelconque de a_n. On dispose d'un indice j, qu'on suppose minimal, tel que $p \mid a_j$. Au vu de la minimalité de j et de la relation $\mathrm{PGCD}(a_j, a_n) = a_{\mathrm{PGCD}(n,j)}$, on déduit que $j \mid n$. On a alors, du fait de la relation précédente, $a_n \equiv a_j \mod a_j^d$ et en particulier, $a_n \equiv a_j \mod p^{dv_p(a_j)}$. On déduit que $v_p(a_n) = v_p(a_j)$.

Comme $v_p(a_n) \in \{v_p(a_{n-1}), v_p(a_{n-2}), \ldots, v_p(a_1)\}$ pour tout p, on déduit que $a_n < a_1 \ldots a_{n-1}$. Mais une récurrence immédiate prouve l'inégalité contraire, ce qui prouve que a_n admet au moins un nombre premier qui ne divise aucun des termes précédents de la suite.

Exercice 4.18. (IMO 2018 P5) Soit $a_1, a_2, \ldots$ une suite infinie d'entiers strictement positifs. On suppose qu'il existe un entier $N > 1$ tel que, pour tout entier $n \geqslant N$, le nombre

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \ldots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

est un entier. Montrer qu'il existe un entier M tel que $a_m = a_{m+1}$ pour tout entier $m \geqslant M$.

Solution 4.18. Notons brièvement S_n la somme considérée. Le premier réflexe est d'examiner l'hypothèse de l'énoncé pour les indices n et $n+1$. Cela donne que le nombre $S_{n+1} - S_n = \dfrac{a_{n+1} - a_n}{a_1} + \frac{a_n}{a_{n+1}}$ est entier. C'est avec cette hypothèse, à savoir que $\boxed{a_{n+1}a_1 \mid a_{n+1}(a_{n+1} - a_n) + a_1 a_n}$ pour tout $n \geqslant N$, que nous allons travailler par la suite.

Cette hypothèse implique notamment que $a_{n+1} \mid a_1 a_n$, ce qui implique que l'ensemble des facteurs premiers divisant les termes de la suite (a_n) est fini.

Soit p un nombre premier. La relation de divisibilité implique

$$v_p(a_1) + v_p(a_{n+1}) \leqslant v_p(a_{n+1}(a_{n+1} - a_n) + a_1 a_n).$$

C'est en voulant expliciter le terme de droite en fonction de $v_p(a_1), v_p(a_n)$ et $v_p(a_{n+1})$ que l'on aboutit à la disjonction de cas qui suit, et dans laquelle on pose $\alpha_n = v_p(a_n)$ et $\alpha = \alpha_1$.

- ➢ Si $\alpha_n \geqslant \alpha$, alors $\alpha \leqslant \alpha_{n+1} \leqslant \alpha_n$. Supposons d'abord que $\alpha_{n+1} < \alpha \leqslant \alpha_n$. Alors $v_p(a_{n+1}(a_{n+1} - a_n) + a_1 a_n) = 2\alpha_{n+1} < \alpha + \alpha_{n+1}$, ce qui est absurde. D'autre part, si $\alpha \leqslant \alpha_n < \alpha_{n+1}$, alors $v_p(a_{n+1}(a_{n+1} - a_n) + a_1 a_n) = \alpha + \alpha_n < \alpha + \alpha_{n+1}$, également en contradiction avec la relation ci-dessus.

  Par récurrence immédiate, $\boxed{\text{la suite } (\alpha_k) \text{ est alors minorée et décroissante}}$, donc, à partir d'un certain rang N_p, elle est constante.

- ➢ Si $\alpha_n < \alpha$, alors $\alpha_{n+1} \geqslant \alpha_n$. En effet, si on avait $\alpha_{n+1} < \alpha_n$, alors $v_p(a_{n+1}(a_{n+1} - a_n) + a_1 a_n) = 2\alpha_{n+1} < \alpha + \alpha_{n+1}$, ce qui est en contradiction avec la relation de divisibilité.

  Ainsi, si aucun indice n ne vérifie $\alpha_n \geqslant \alpha$, ce qu'on est en droit de supposer au vu du premier cas, $\boxed{\text{la suite } (\alpha_k) \text{ est croissante et majorée par } \alpha}$, donc, à partir d'un certain rang N_p, elle est constante.

Vu que l'ensemble $\mathcal{P}$ des facteurs premiers divisant un terme de la suite est fini, on peut prendre $M = \max\{N_p, p \in \mathcal{P}\}$. A partir de ce rang M, les suites $v_p(a_n)$ sont toutes constantes, ce qui veut dire que (a_n) elle-même est constante.

Exercice 4.19. (ELMO 2018 P2) Soit $a_1, a_2, \ldots$ une suite d'entiers strictement positifs telle que $a_1 = 1$ et, pour tous entiers $k, n \geqslant 1$,

$$a_n \mid a_k + a_{k+1} + \ldots + a_{n+k-1}.$$

Soit $m \geqslant 1$ un entier. Déterminer la plus grande valeur que peut prendre a_{2m}.

Solution 4.19.

➢ **Commentaire :**

> Il y a beaucoup d'idées à explorer dans ce problème : appliquer l'hypothèse pour deux indices consécutifs k et $k+1$ ou n et $n+1$, s'intéresser à la suite auxiliaire (S_n) correspondant à la somme des premiers termes... mais cet enthousiasme ne doit pas nous empêcher de regarder les petits cas pour faire des conjectures.
>
> Par exemple, on constate pour $k = 1$ que $a_n \mid a_1 + \ldots + a_{n-1}$. On peut alors vouloir, pour maximiser a_n, à forcer l'égalité $a_n = a_1 + \ldots + a_{n-1}$, au moins pour les indices n pairs. Toutefois, si c'est le cas, alors on a
>
> $$a_{n+1} \mid a_1 + \ldots + a_n = 2(a_1 + \ldots + a_{n-1}),$$
>
> $$a_{n+1} \mid a_2 + \ldots + a_{n+1} = a_{n+1} + 2(a_1 + \ldots + a_{n-1}) - a_1 \quad \Longrightarrow a_{n+1} \mid a_1 = 1 \quad \Longrightarrow a_{n+1} = 1.$$
>
> Mais si $a_{n+1} = 1$, alors la somme $a_1 + \ldots + a_n + a_{n+1}$ est petite et donc a_{n+2} aussi.
>
> Ceci, en plus de la forme de l'énoncé qui demande de regarder uniquement les indices pairs, nous invite à considérer non pas uniquement a_{2m} mais aussi a_{2m-1}. L'étude des petits cas nous donne alors les conjectures nécessaires. Dans le procédé, on n'oublie pas la méthode classique qui est d'appliquer l'énoncé à deux indices consécutifs k et $k+1$ ou n et $n+1$.

Réponse : La valeur maximale est $a_{2m} = 2^m - 1$.

Analyse : On montre que $a_{2n} \leqslant 2^n - 1$ pour tout n.

Soit (a_n) une suite solution du problème. On prouve par récurrence forte sur m que $a_{2m-1} + a_{2m} \leqslant 2^m$ pour tout $m \geqslant 1$. Si c'est le cas, alors $a_{2m} \leqslant 2^m - a_{2m-1} \leqslant 2^m - 1$.

➢ **Initialisation :** On a $a_2 \mid a_1 + a_2$ d'après l'énoncé, donc $a_2 \mid a_1 = 1$ donc $a_2 = 1$ et $a_1 + a_2 \leqslant 2^1$.

➢ **Hérédité :** On suppose que $a_{2m-1} + a_{2m} \leqslant 2^m$ pour tout entier $m \leqslant n$, avec $n \geqslant 1$ fixé.

On applique l'énoncé à $2n+1$ et aux deux entiers consécutifs $k = 1$ et $k = 2$. On pose également $S_{2n} = a_1 + \ldots + a_{2n}$. Cela donne

$$a_{2n+1} \mid a_1 + \ldots + a_{2n} + a_{2n+1}, \quad \Longrightarrow a_{2n+1} \mid S_{2n},$$

$$a_{2n+1} \mid a_2 + \ldots + a_{2n+2} = S_{2n} + a_{2n+1} + a_{2n+2} - a_1 \quad \Longrightarrow a_{2n+1} \mid a_{2n+2} - 1.$$

On déduit que $\boxed{a_{2n+1} \text{ et } a_{2n+2} \text{ sont premiers entre eux}}$. En appliquant l'énoncé à $2n+2$ et $k = 1$, on trouve $a_{2n+2} \mid S_{2n} + a_{2n+1} + a_{2n+2}$, donc $a_{2n+2} \mid S_{2n} + a_{2n+1}$. Puisque a_{2n+1} et a_{2n+2} sont de $S_{2n} + a_{2n+1}$ premiers entre eux, on déduit que $\boxed{a_{2n+1}a_{2n+2} \mid S_{2n} + a_{2n+1}}$. Pour finir, on utilise cette divisibilité pour exprimer a_{2n+2} en fonction de a_{2n+1} dans la somme $a_{2n+1} + a_{2n+2}$. Cela donne

$$a_{2n+1} + a_{2n+2} \leqslant a_{2n+1} + \frac{S_{2n} + a_{2n+1}}{a_{2n+1}} \leqslant a_{2n+1} + \frac{S_{2n}}{a_{2n+1}} + 1.$$

Notons que $a_{2n+1} \leqslant S_{2n}$ car $a_{2n+1} \mid S_{2n}$. La fonction $x \mapsto x + \dfrac{S_{2n}}{x}$ atteignant son maximum sur $[1, S_{2n}]$ en 1 et S_{2n}, on déduit que $a_{2n+1} + \dfrac{S_{2n}}{a_{2n+1}} \leqslant 1 + S_{2n}$ et que $\boxed{a_{2n+1} + a_{2n+2} \leqslant S_{2n} + 2}$.

D'après l'hypothèse de récurrence, $S_{2n} = (a_1 + a_2) + \ldots + (a_{2n-1} + a_{2n}) \leqslant 2^{n+1} - 2$. On a donc l'inégalité $a_{2n+1} + a_{2n+2} \leqslant 2^{n+1}$ comme voulu, ce qui achève la récurrence et conclut l'analyse.

Construction : On donne un exemple de suite qui vérifie l'énoncé et tel que $a_{2n} = 2^n - 1$ pour tout n.

L'analyse précédente montre que si $a_{2n} = 2^n - 1$, alors $a_{2n-1} = 1$. Il suffit donc de montrer que la suite définie par ces valeurs vérifie l'énoncé. Si n est impair, on a la divisibilité de l'énoncé car $a_n = 1$. On suppose que $n = 2n'$ est pair.

➢ Si $k = 2k' - 1$ est impair, alors

$$\begin{aligned} a_k + \ldots + a_{k+n-1} &= (a_{2k'-1} + a_{2k'}) + \ldots + (a_{2k'-1+n-2} + a_{2k'-1+n-1}) \\ &= 2^{k'} + \ldots + 2^{k'+n'-1} \\ &= 2^{k'+n'} - 2^{k'} \equiv 0 \mod (2^{n'} - 1). \end{aligned}$$

➢ Si $k = 2k'$ est pair, alors

$$\begin{aligned} a_k + \ldots + a_{k+n-1} &= (a_{2k'+1} + a_{2k'+2}) + \ldots + (a_{2k'+n-1} + \underbrace{a_{2k'}}_{=1=a_{2k'+n}}) \\ &= 2^{k'+1} + \ldots + 2^{k'+n'-1} \\ &= 2^{k'+n'} - 2^{k'} \equiv 0 \mod (2^{n'} - 1). \end{aligned}$$

Dans tous les cas $a_n \mid a_k + \ldots + a_{k+n-1}$, et la suite donnée vérifie bien l'énoncé.

Exercice 4.20. (France TST 2020-2021 P2) On dit qu'une suite $(u_n)_{n\geqslant 0}$ d'entiers naturels non nuls est *sicilienne* si

$$u_{n+1} \in \{u_n/2, u_n/3, 2u_n+1, 3u_n+1\}$$

pour tout $n \geqslant 0$. Démontrer que, pour tout entier $k \geqslant 1$, il existe une suite sicilienne $(u_n)_{n\geqslant 0}$ et un entier $\ell \geqslant 0$ tels que $u_0 = k$ et $u_\ell = 1$.

Solution 4.20. Nous allons démontrer, pour tout entier $k \geqslant 2$, la propriété $\mathcal{P}_k$ suivante : il existe une suite sicilienne finie $(u_0, \dots, u_\ell)$ telle que $u_0 = k$ et $u_\ell < k$. On itère alors cet énoncé en repartant de l'entier u_ℓ obtenu, qui est strictement plus petit que u_0, jusqu'à obtenir un terme valant 1.

Si k est pair, il suffit de choisir $u_1 = k/2$ pour avoir la propriété $\mathcal{P}_k$. On suppose donc dans la suite que k est impair. Soit α et κ les entiers naturels non nuls tels que $k = 2^\alpha\kappa - 1$, l'entier κ étant impair. On construit alors notre suite sicilienne comme suit.

On commence par supprimer le facteur 2 dans la décomposition donnée. Pour tout $i \leqslant \alpha$, on pose $u_{2i+1} = 3u_{2i}+1$ et $u_{2i+2} = u_{2i+1}/2$, ce qui donne $u_{2i} = 2^{\alpha-i}3^i\kappa - 1$ et $u_{2i+1} = 2^{\alpha-i}3^{i+1}\kappa - 2$. On a en particulier $u_{2\alpha} = 3^\alpha\kappa - 1$ et $u_{2\alpha+1} = (3^\alpha\kappa - 1)/2$.

On choisit ensuite $u_{2\alpha+1} = u_{2\alpha}/2 = (3^\alpha\kappa - 1)/2$ qui est bien un entier puisque κ est impair, et $\boxed{u_{2\alpha+2} = 2u_{2\alpha+1} + 1 = 3^\alpha\kappa}$.

Enfin, pour tout $i \leqslant \alpha$, on pose $u_{2\alpha+2+i} = u_{2\alpha+2+i-1}/3 = 3^{\alpha-i}\kappa$. On obtient $u_{3\alpha+2} = \kappa \leqslant (k+1)/2 < k$, cela achève de démontrer la propriété $\mathcal{P}_k$, et conclut l'exercice.

Exercice 4.21. (IMO 2005 P2) Soit $a_1, a_2, \dots$ une suite d'entiers contenant une infinité de termes positifs et une infinité de termes négatifs. On suppose que pour tout entier $n \geqslant 1$, les nombres $a_1, \dots, a_n$ donnent n restes distincts modulo n.

Montrer que chaque entier apparaît exactement une fois dans la suite.

Solution 4.21.

➢ Commentaire :

> Même si la solution est courte, l'exercice est assez difficile : les idées du type "appliquer l'hyptohèse aux entiers n et $n+1$" ne semblent pas porter leurs fruits immédiatemment et l'hypothèse "il y a une infinité de termes de chaque signe" demeure plutôt enigmatique.
>
> La clé est d'obtenir des inégalités sur les termes : si deux termes de la suite ont des valeurs trop éloignées, il donneront le même reste modulo un certain entier n bien choisi.

Tout d'abord, un même entier ne peut apparaître deux fois : si on avait $a_i = a_j$ pour deux indices $i < j$ distincts, alors l'ensemble $a_1, \dots, a_{j+1}$ ne contiendrait pas $j+1$ restes distincts modulo $j+1$.

On peut même améliorer l'argument. Fixons un entier m, et notons $a_i = \max(a_1, \dots, a_m)$ et $a_j = \min(a_1, \dots, a_m)$. Comme on a $a_i \equiv a_j \mod (a_i - a_j)$, on déduit que $j \geqslant (a_i - a_j)$, (sinon appliquer l'énoncé à $n = a_i - a_j$ produirait une contradiction). En particulier, $a_i - a_j \leqslant j \leqslant m$. Cela signifie que l'intervalle $[\![a_j, a_i]\!]$ est de longueur au plus m et contient les m entiers distincts $a_1, \dots, a_m$, il est donc de longueur exactement m. En d'autres termes, $\boxed{\text{les nombres } a_1, \dots, a_m \text{ sont consécutifs pour tout } m}$.

On peut à présent conclure à partir de l'hypothèse que la suite contient une infinité de nombres positifs et de nombres négatifs. Soit a un entier. Puisque la suite contient une infinité d'entiers positifs et négatifs, elle contient en particulier un entier b supérieur à a et un entier c inférieur à a, et on note k et ℓ les indices tels que $a_k = b$ et $a_\ell = c$, avec disons $k < \ell$. Comme les entiers $a_1, \dots, a_\ell$ sont consécutifs, l'ensemble $\{a_1, \dots, a_\ell\}$ contient l'intervalle $[\![b, c]\!]$ auquel appartient a, comme voulu.

Exercice 4.22. (EGMO 2022 P3) Une suite infinie d'entiers strictement positifs $a_1, a_2, \ldots$ est dite *bonne* si

(1) a_1 est un carré parfait.

(2) Pour tout entier $n \geqslant 2$, a_n est le plus petit entier strictement positif tel que

$$na_1 + (n-1)a_2 + \ldots + 2a_{n-1} + a_n$$

est un carré parfait.

Montrer que pour tout suite bonne $a_1, a_2, \ldots$, il existe un entier k tel que $a_n = a_k$ pour tout entier $n \geqslant k$.

Solution 4.22.

➢ **Commentaire :**

> Cet exercice combine beaucoup d'idées assez générales qui peuvent devenir des réflexes :
> - ➢ Introduire des bonnes suites intermédiaires pour avoir une relation faisant intervenir un nombre fini de termes (plutôt que n termes),
> - ➢ montrer qu'une suite est constante à partir d'un certain rang en montrant qu'elle est monotone et bornée (ce ne sera pas le cas de la suite (a_n) mais d'une suite intermédiaire,
> - ➢ Examiner ce que deviennent les suites intermédiaires introduites si l'énoncé est vrai/dans un cas particulier pour faire des conjectures.
>
> En présence d'une relation faisant intervenir les n premiers termes, on cherche un changement de variable/une suite intermédiaire pour laquelle la relation en question ne fait intervenir qu'un nombre restreint de termes (par exemple les termes d'indices n et $n-1$). Cette motivation guide les premiers calculs.
>
> En l'occurence, introduire la suite des sommes $S_n = a_1 + \ldots + a_n$ permet de réécrire l'expression comme $S_1 + \ldots + S_n$, ce qui n'est pas encore satisfaisant au regard de la motivation ci-dessus, mais permet de supprimer les facteurs n.
>
> Bien sûr, il ne faut pas oublier d'introduire la suite (b_n), où b_n est le nombre tel que $S_1 + \ldots + S_n = b_n^2$. Pour enfin obtenir une relation de récurrence sur peu d'indices, on peut chercher à réécrire S_n puis a_n en fonction de (b_n).

Posons $S_n = a_1 + \ldots + a_n$. D'après l'énoncé, pour tout entier n, il existe un entier b_n tel que

$$b_n^2 = na_1 + (n-1)a_2 + \ldots + 2a_{n-1} + a_n = S_1 + \ldots + S_n.$$

Il vient que, pour tout $n \geqslant 2$,

$$b_n^2 = S_n + b_{n-1}^2 = a_n + S_{n-1} + b_{n-1}^2 = a_n + (b_{n-1}^2 - b_{n-2}^2) + b_{n-1}^2 = a_n + 2b_{n-1}^2 - b_{n-2}^2.$$

Ainsi, l'énoncé signifie que a_n est le plus petit entier tel que le nombre $a_n + 2b_{n-1}^2 - b_{n-2}^2$ est un carré parfait, ou encore que b_n^2 est le plus petit carré supérieur ou égal à $2b_{n-1}^2 - b_{n-2}^2$.

➢ **Commentaire :**

> On vérifie que les termes n'obéissent à aucune autre contrainte, ce qui signifie que jusqu'ici, notre réécriture est strictement équivalente à celle de l'énoncé, et elle a complètement effacé la suite (a_n).
>
> Avant de continuer, il faut comprendre quelle propriété sur la suite (b_n) implique que la suite (a_n) est constante à partir d'un certain rang. Dans le cas d'une suite (a_n) constante égale à x, on a $b_n^2 - b_{n-1}^2 = nx$, ce qui signifie aussi que $b_n - b_{n-1}$ est constant. On peut donc chercher à montrer que la suite $(b_n - b_{n-1})$ est constante à partir d'un certain rang. En général, un tel résultat s'obtient en étudiant la monotonie de cette suite. On chercher donc une relation du type $b_n - b_{n-1} \leqslant b_{n-1} - b_{n-2}$, ou encore $b_n \leqslant 2b_{n-1} - b_{n-2}$ et c'est cette relation qui guide la suite de nos calculs.

Montrons que $b_n - b_{n-1} \leqslant b_{n-1} - b_{n-2}$ pour tout entier n. Comme b_n^2 est le plus petit carré parfait supérieur ou égal à $2b_{n-1}^2 - b_{n-2}^2$, il suffit de vérifier que $2b_{n-1}^2 - b_{n-2}^2 \leqslant (2b_{n-1} - b_{n-2})^2$ pour tout indice n, puisque alors $b_n \leqslant 2b_{n-1} - b_{n-2}$. Or, on a

$$2b_{n-1}^2 - b_{n-2}^2 \leqslant (2b_{n-1} - b_{n-2})^2 \Leftrightarrow 0 \leqslant 2(b_{n-1}^2 + b_{n-2}^2 - b_{n-1}b_{n-2}),$$

ce qui est toujours vrai. (On pourra voir qu'il s'agit également de l'inégalité des moyennes quadratiques et arithmétiques)

De cette inégalité, on déduit que la suite $(b_n - b_{n-1})$ est décroissante. Comme elle est minorée par 0 (la suite (b_n) est croissante), elle est constante à partir d'un certain rang N. On a alors, pour tout entier $n \geqslant N$, $b_n = b_N + (n-N)x$ pour un certain entier x. Mais alors pour tout $n \geqslant N+2$,

$$a_n = b_n^2 - 2b_{n-1}^2 + b_{n-2}^2 = 2x^2.$$

Ceci conclut que la suite (a_n) est constante à partir d'un certain rang.

Remarque : On aurait aussi pu faire le contraire : ne pas avoir d'idée précise sur la monotonie de (b_n) mais chercher à majorer b_n en cherchant un carré parfait raisonnable supérieur à $2b_{n-1}^2 - b_{n-2}^2$. On vérifie que

$$\begin{aligned} 2b_{n-1}^2 - b_{n-2}^2 &= b_{n-1}^2 + (b_{n-1} - b_{n-2})(b_{n-1} + b_{n-2}) \\ &= b_{n-1}^2 + 2b_{n-1}(b_{n-1} - b_{n-2}) + b_{n-2}^2 - 2(b_{n-1} - b_{n-2})^2 = (2b_{n-1} - b_{n-2})^2 - 2(b_{n-1} - b_{n-2})^2. \end{aligned}$$

Donc $(2b_{n-1} - b_{n-2})^2$ est un carré supérieur à $2b_{n-1}^2 - b_{n-2}^2$, ce qui implique que $b_n^2 \leqslant (2b_{n-1} - b_{n-2})^2$ et redonne l'inégalité $b_n \leqslant 2b_{n-1} - b_{n-2}$, à partir de laquelle on peut conclure.

Exercice 4.23. (IMO SL 2023 N5) Soit $a_1, a_2, a_3, \ldots$ une suite d'entiers strictement positifs, strictement croissante, telle que a_{k+1} divise $2(a_1 + a_2 + \cdots + a_k)$ pour tout entier $k \geqslant 1$. On suppose qu'il existe une infinité de nombres premiers p qui divisent au moins un terme parmi $a_1, a_2, a_3, \ldots$.
Démontrer que tout entier $n \geqslant 1$ divise au moins un terme parmi $a_1, a_2, a_3, \ldots$

Solution 4.23. Pour tout $k \geqslant 0$, on pose $s_k = a_1 + a_2 + \cdots + a_k$ et $b_k = 2s_k/a_{k+1}$. Il s'agit là d'un entier lorsque $k \geqslant 1$, mais également lorsque $k = 0$, car $b_0 = 2s_0/a_1 = 0$. De la sorte, $s_{k+1} = s_k + a_{k+1} = s_k(1 + 2/b_k)$. L'inégalité $a_{k+2} > a_{k+1}$ se réécrit alors comme

$$\frac{2s_{k+1}}{b_{k+1}} = a_{k+2} > a_{k+1} = \frac{2s_k}{b_k} = \frac{2s_{k+1}}{b_k + 2},$$

de sorte que $b_{k+1} < b_k + 2$, c'est-à-dire $b_{k+1} \leqslant b_k + 1$.
Soit maintenant p un nombre premier impair, arbitrairement grand, qui divise un entier a_k. Il divise aussi $2s_{k-1}$, et même s_{k-1} ; on note ℓ le plus petit entier naturel non nul tel que p divise s_ℓ. Comme $b_{\ell-1}s_\ell = (b_{\ell-1} + 2)s_{\ell-1}$, on en déduit que p divise $b_{\ell-1} + 2$ donc que $b_{\ell-1} \geqslant p - 2$. Ainsi, la suite $(b_k)_{k \geqslant 0}$ prend des valeurs arbitrairement grandes.
Soit alors n un entier naturel non nul, puis c un entier tel que $2cn \geqslant b_1 + 3$, et k le plus petit entier tel que $b_k \geqslant 2cn - 1$. Puisque $b_k \leqslant b_{k-1} + 1$, on sait que $b_{k-1} = 2cn - 2$. Ainsi, $2n$ divise $2cns_{k-1} = (b_{k-1} + 2)s_{k-1} = b_{k-1}s_k$. Comme $\mathsf{PGCD}(2n, b_{k-1})$ divise $2cn - b_{k-1} = 2$, on en déduit que n divise donc s_k. Mais alors n divise également $(b_k + 2)s_k = b_k s_{k+1} = (2cn - 1)s_{k+1}$, donc divise aussi s_{k+1}. On en conclut comme souhaité que n divise $s_{k+1} - s_k = a_k$.

Solution alternative
Pour tout $k \geqslant 0$, on pose $s_k = a_1 + a_2 + \cdots + a_k$ et $b_k = 2s_k/a_{k+1}$. Il s'agit là d'un entier lorsque $k \geqslant 1$, mais également lorsque $k = 0$, car $b_0 = 2s_0/a_1 = 0$. On constate alors que

$$b_{k+1}a_{k+2} = 2s_{k+1} = 2s_k + 2a_{k+1} = (b_k + 2)a_{k+1}.$$

Puisque $a_{k+1} < a_{k+2}$, on en déduit que $b_{k+1} < b_k + 2$, c'est-à-dire $b_{k+1} \leqslant b_k + 1$. En particulier, $b_k \leqslant k$ pour tout entier $k \geqslant 0$.
Soit maintenant p un nombre premier arbitrairement grand, qui divise un entier a_k mais pas a_1, de sorte que $k \geqslant 2$. Comme a_k divise $b_{k-1}a_k = (b_{k-2} + 2)a_{k-1}$, et en enchaînant de telles relations de divisibilité, on constate que p et a_k divisent $(b_0 + 2)(b_1 + 2) \cdots (b_{k-2} + 2)a_1$. Par conséquent, p divise l'un des facteurs $b_i + 2$, et $b_i \geqslant p - 2$. Puisque l'on a choisi p arbitrairement grand, la suite $(b_k)_{k \geqslant 0}$ elle-même prend donc des valeurs arbitrairement grandes. Comme elle augmente d'au plus 1 à chaque fois et commence par valoir $b_0 = 0$, elle prend même toutes les valeurs entières positives.
Enfin, soit n un entier naturel non nul, et soit $\ell \geqslant n$ le plus petit entier tel que $b_\ell \geqslant n$. Puisque $n \leqslant b_\ell \leqslant b_{\ell-1} + 1 \leqslant (n-1) + 1 = n$, on sait que $b_\ell = n$ et $b_{\ell-1} = n - 1$. Ainsi,

$$na_{\ell+1} = b_\ell a_{\ell+1} = (b_{\ell-1} + 2)a_\ell = (n+1)a_\ell,$$

donc n divise a_ℓ.

Exercice 4.24. (IMO SL 2025 N5) La suite de triplets d'entiers strictement positifs $(a_0, b_0, c_0), (a_1, b_1, c_1)$,..., $(a_{2025}, b_{2025}, c_{2025})$ vérifie

$$(a_{i+1}, b_{i+1}, c_{i+1}) = (a_i + \mathrm{PGCD}(b_i, c_i), b_i + \mathrm{PGCD}(c_i, a_i), c_i + \mathrm{PGCD}(a_i, b_i))$$

pour tout indice $0 \leqslant i \leqslant 2024$.

Déterminer la plus petite valeur que peut prendre a_{2025}.

Solution 4.24. **Réponse :** La valeur minimale de $a_{2025} = 3 \cdot 2^{2025/3} = 3 \cdot 2^{675}$.

Le problème demande de déterminer le plus petit entier vérifiant une propriété, il contient donc nécessairement deux parties. D'une part, on montre que, quel que soit le triplet (a_0, b_0, c_0) de départ, a_{2025} est toujours supérieur à $3 \cdot 2^{675}$, cette étape s'appelle *l'analyse*. D'autre part, on donne un exemple de triplet (a_0, b_0, c_0) pour lequel $a_{2025} = 3 \cdot 2^{675}$, cette étape s'appelle *la construction*.

Analyse :

En testant l'énoncé pour des petits indices et des valeurs particulières de (a_0, b_0, c_0), on s'aperçoit qu'à partir d'un certain rang k, les trois entiers du triplet (a_k, b_k, c_k) sont divisibles par 2. Cette observation nous laisse penser qu'a fortiori, à partir d'un certain rang, les entiers des triplets seront tous divisibles par une grande puissance de deux.

On note $v_2(x)$ la valutation 2−adique de x. On prouve le lemme suivant :

Lemme : Soit $k \geqslant 0$ un indice. Alors $v_2(\mathrm{PGCD}(a_{k+3}, b_{k+3}, c_{k+3})) \geqslant 1 + v_2(\mathrm{PGCD}(a_k, b_k, c_k))$.

Preuve : On pose $x = v_2(\mathrm{PGCD}(a_k, b_k, c_k))$. Une récurrence immédiate donne que 2^x divise $\mathrm{PGCD}(a_j, b_j, c_j)$ pour tout indice $j \geqslant k$. Pour tout $j \geqslant k$, on note $\alpha_j, \beta_j, \gamma_j$ les entiers tels que $a_j = 2^x \alpha_j, b_j = 2^x \beta_j$ et $c_j = 2^x \gamma_j$. La suite $(\alpha_j, \beta_j, \gamma_j)$ vérifie alors la même relation de récurrence que la suite (a_j, b_j, c_j). Pour prouver le lemme, il suffit de montrer que $\alpha_{k+3}, \beta_{k+3}$ et γ_{k+3} sont pairs.

Le triplet $(\alpha_k, \beta_k, \gamma_k)$ contient zéro, un ou deux nombres paires. Comme la relation de récurrence est symétrique en les trois suites, on peut supposer que les éventuels nombres pairs du triplet $(\alpha_k, \beta_k, \gamma_k)$ sont α_k et β_k. Les trois tableaux qui donnent les restes modulo 2 des suites α, β, γ aux rangs $k+1, k+2$ et $k+3$ en fonction des restes au rang k :

rang	α	β	γ
k	1	1	1
$k+1$	0	0	0
$k+2$	0	0	0
$k+3$	0	0	0

rang	α	β	γ
k	0	1	1
$k+1$	1	0	0
$k+2$	1	1	1
$k+3$	0	0	0

rang	α	β	γ
k	0	0	1
$k+1$	1	1	1
$k+2$	0	0	0
$k+3$	0	0	0

Pour compléter les tableaux, on a utilisé que le PGCD de deux nombres pairs vaut $0 \mod 2$ et que le PGCD d'un nombre impair avec un autre nombre vaut $1 \mod 2$. On voit que, quels que soient les restes au rang k, $\alpha_{k+3}, \beta_{k+3}$ et γ_{k+3} sont toujours pairs, ce qui conclut. □

On revient à l'exercice. Notons pour tout indice $k \geqslant 0$, $x_k = v_2(\mathrm{PGCD}(a_k, b_k, c_k))$. La suite (x_k) est croissante et vérifie $x_{k+3} \geqslant x_k + 1$. Par récurrence immédiate, on déduit que $x_{3k}, x_{3k+1}, x_{3k+2} \geqslant k$. Puisque $2^{x_k} \mid \mathrm{PGCD}(a_k, b_k, c_k)$, alors $2^{x_k} \mid \mathrm{PGCD}(b_k, c_k)$ et en particulier $2^{x_k} \leqslant \mathrm{PGCD}(b_k, c_k)$. On a alors

$$\begin{aligned} a_{2025} &= a_0 + \sum_{k=0}^{2024} \mathrm{PGCD}(b_k, c_k) \geqslant a_0 + \sum_{k=0}^{2024} 2^{x_k} = a_0 + \sum_{k=0}^{674} (2^{x_{3k}} + 2^{x_{3k+1}} + 2^{x_{3k+2}}) \\ &\geqslant a_0 + 3 \sum_{k=0}^{674} 2^k = a_0 + 3(2^{675} - 1). \end{aligned}$$

D'autre part, comme $x_{2025} \geqslant 675$ et $2^{x_{2025}} \mid a_{2025}$, on déduit que a_{2025} est un multiple de 2^{675} supérieur à $3 \cdot 2^{675} - 3$. Ainsi, $a_{2025} \geqslant 3 \cdot 2^{675}$.

Construction :

Pour réaliser la construction, on veut des égalités dans les inégalités de l'analyse. On souhaite donc $a_{3k} = 3 \cdot 2^k$ et $x_{3k} = x_{3k+1} = x_{3k+2} = k$ pour tout indice k. Les tableaux de congruence de l'analyse suggèrent qu'il faut

pour cela qu'exactement un des nombres $v_2(b_{3k}), v_2(c_{3k})$ soit égal à k. Le tatônnement permet alors d'obtenir la construction suivante.

On pose $(a_0, b_0, c_0) = (3, 5, 6)$. On vérifie que $(a_3, b_3, c_3) = (2 \cdot 3, 2 \cdot 5, 2 \cdot 6)$ et une récurrence immédiate donne $(a_{3k}, b_{3k}, c_{3k}) = (2^k \cdot 3, 2^k \cdot 5, 2^k \cdot 6)$. On trouve alors bien $a_{2025} = 3 \cdot 2^{675}$.

Remarque : Une autre construction possible part du triplet $(a_0, b_0, c_0) = (3, 4, 9)$, avec une preuve similaire.

Exercice 4.25. (IMO SL 2021 N7) Soit $(a_n)_{n \geqslant 1}$ une suite d'entiers naturels non nuls telle que a_{n+2m} divise $a_n + a_{n+m}$ pour tous les entiers $m \geqslant 1$ et $n \geqslant 1$. Démontrer que cette suite est ultimement périodique, c'est-à-dire qu'il existe deux entiers $N \geqslant 1$ et $d \geqslant 1$ tels que $a_n = a_{n+d}$ pour tout $n \geqslant N$.

Solution 4.25.

Étape 1 : La suite (a_n) est bornée.

Supposons qu'il existe un entier $k \geqslant 9$ tel que $a_i < a_k$ pour tout $i \leqslant k-1$. Dans ces conditions, et pour tout entier $i < k/2$, on sait que $a_{k-2i} + a_{k-i}$ est un multiple de a_k et que $a_{k-2i} + a_{k-i} < 2a_k$, de sorte que $a_{k-2i} + a_{k-i} = a_k$. En choisissant $i = 1$, $i = 2$ et $i = 4$, on en déduit que

$$a_{k-8} + a_{k-4} = a_{k-4} + a_{k-2} = a_k = a_{k-2} + a_{k-1},$$

donc que $a_{k-8} = a_{k-2}$ et $a_{k-4} = a_{k-1}$.
Une récurrence sur ℓ indique alors que a_{k-1} divise $a_{k-1-3\ell}$ pour tout $\ell \leqslant (k-2)/3$, de sorte que $a_{k-1} \leqslant \max\{a_1, a_2, a_3\}$, et que a_{k-2} divise $a_{k-2-6\ell}$ pour tout $\ell \leqslant (k-3)/6$, de sorte que $a_{k-2} \leqslant \max\{a_1, a_2, \ldots, a_6\}$. On en conclut que

$$a_k = a_{k-1} + a_{k-2} \leqslant 2\max\{a_1, a_2, \ldots, a_6\}.$$

Par conséquent, la suite $(a_n)_{n \geqslant 1}$ est bornée.

Soit λ la valeur maximale que prend infiniment souvent la suite $(a_n)_{n \geqslant 1}$, et soit $\kappa \geqslant 0$ un entier tel que $a_n \leqslant \lambda$ pour tout $n \geqslant \kappa + 1$. Quitte à oublier les κ premiers termes de la suite, ce qui ne change rien à l'énoncé, on suppose que $\kappa = 0$, c'est-à-dire que $a_n \leqslant \lambda$ pour tout $n \geqslant 1$.

Étape 2 : L'ensemble d'indices $\mathcal{E} = \{k \geqslant 1 \colon a_k = \lambda\}$ est une suite arithmétique.

Considérons trois éléments consécutifs $k < \ell < m$ de $\mathcal{E}$. Si $k \equiv \ell \pmod 2$, on sait que $\lambda = a_\ell$ divise $a_k + a_{(k+\ell)/2} = \lambda + a_{(k+\ell)/2}$, donc que $a_{(k+\ell)/2} = \lambda$, en contradiction avec le fait que k et ℓ étaient des éléments consécutifs de $\mathcal{E}$.

On en déduit que $k \not\equiv \ell \pmod 2$ et, de même, que $\ell \not\equiv m \pmod 2$. Mais alors $\lambda = a_m$ divise $a_k + a_{(k+m)/2} = \lambda + a_{(k+m)/2}$, donc $a_{(k+m)/2} = \lambda$, et $(k+m)/2$ est un élément de $\mathcal{E}$ compris entre k et m, de sorte que $(k+m)/2 = \ell$. Cela signifie que $\ell - k = m - \ell$ et, plus généralement, que les éléments de $\mathcal{E}$ forment une progression arithmétique infinie, dont on note d la raison.

Étape 3 : Conclusion

Enfin, soit $n \geqslant 1$ un entier quelconque, puis soit $m \geqslant 1$ un entier tel que $m + n \in \mathcal{E}$. Alors $\lambda = a_{m+n}$ divise $a_n + a_m$, et $m + n + d \in \mathcal{E}$, donc $\lambda = a_{m+n+d}$ divise $a_{n+d} + a_m$. On en conclut que $a_n \equiv -a_m \equiv a_{n+d} \pmod \lambda$. Comme a_n et a_{n+d} sont compris entre 1 et λ, cela signifie que $a_n = a_{n+d}$. Par conséquent, la suite $(a_n)_{n \geqslant 1}$ est d-périodique, ce qui conclut.

4.2 Équations fonctionnelles en arithmétiques

Exercice 4.26. (IMO SL 2013 N1) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$m^2 + f(n) \mid mf(m) + n$$

pour tous $n, m \in \mathbb{N}^\star$.

Solution 4.26. **Réponse :** L'identité est la seule solution.

En posant $m = n$, on obtient que

$$f(n) \mid f(n)(f(n) + 1) = (f(n))^2 + f(n) \mid f(n)f(f(n)) + n.$$

On déduit que $f(n) \mid n$. En particulier, $\boxed{f(n) \leqslant n}$ pour tout n et $f(1) \mid 1$ donc $f(1) = 1$.

En posant $n = 1$, on trouver que

$$m^2 + 1 \mid mf(m) + 1 \quad \Longrightarrow m^2 + 1 \leqslant mf(m) + 1 \quad \Longrightarrow m \leqslant f(m).$$

En combinant les deux inégalités, on déduit que $m = f(m)$ pour tout entier $m \geqslant 1$.

Réciproquement, l'identité est bien solution du problème.

Exercice 4.27. (TST Suisse 2017, P1) Trouver toutes les fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$ telles que $f(p) > 0$ pour tout nombre premier p et pour tout p premier et x entier,

$$p \mid (f(x) + f(p))^{f(p)} - x.$$

Solution 4.27. **Réponse :** La seule solution est l'identité.

En substituant x par p, on obtient que $p \mid (2f(p))^{f(p)} - p$ puis que $\boxed{p \mid f(p) \text{ si } p \text{ est impair}}$.

En posant $x = 0$, et en prenant p impair, on trouve que p divise $(f(0) + f(p))^{f(p)}$ puis que $p \mid f(0) + f(p)$, puis que $p \mid f(0)$. Comme cette divisibilité est vraie pour tout nombre premier p impair, on déduit que $\boxed{f(0) = 0}$.

Mais alors en prenant $p = 2$ et $x = 0$, on trouve que Alors $2 \mid f(2)^{f(2)}$ et donc que $\boxed{2 \mid f(2)}$. En résumé, $p \mid f(p)$ pour tout nombre premier p.

Montrons à présent que $f(p)$ est une puissance de p pour tout nombre premier p. Soit p un nombre premier et soit q un éventuel diviseur premier de $f(p)$ qui n'est pas p. On applique alors l'hypothèse de l'énoncé au nombre premier q et à $x = p$. On déduit

$$q \mid (f(p) + f(q))^{f(q)} - p$$

Comme $q \mid f(q)$ et $q \mid f(p)$, on déduit que $q \mid p$, ce qui est absurde. Ainsi, $\boxed{f(p) \text{ est une puissance de } p}$.

Modulo p on a donc pour x fixé, d'après le petit théorème de Fermat,

$$x \equiv f(x)^{f(p)} \equiv f(x) \mod p.$$

donc p divise $f(x) - x$. Comme cette divisibilité est vraie pour tout p premier, on trouve $\boxed{f(x) = x}$ pour tout $x \in \mathbb{Z}$.

Réciproquement, la fonction identité est bien solution, puisque $(x + p)^p \equiv x^p \equiv x \mod p$ pour tout nombre premier p.

Exercice 4.28. (IMO SL 2004 N3) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$(f(m)^2 + f(n)) \mid (m^2 + n)^2$$

pour tous $n, m \in \mathbb{N}^\star$.

Solution 4.28. **Réponse :** La seule solution est l'identité.

Pour $m = n = 1$, on a alors $f(1)^2 + f(1) \mid 2^2$, soit $f(1)^2 + f(1) \in \{1, 2, 4\}$. Une rapide disjonction de cas conduit à $\boxed{f(1) = 1}$.

Afin de réduire le nombre de diviseurs de $m^2 + n$, on choisit m et n tels que $m^2 + n$ est un nombre premier. Prenons $m = 1$ et $n = p - 1$ dans la divisibilité, on trouve

$$1 + f(p-1) = f(1)^2 + f(p-1) \mid (1^2 + p - 1)^2 = p^2.$$

Puisque $1 + f(p-1) \geqslant 2$, on déduit que $1 + f(p-1) \in \{p, p^2\}$.

Montrons que si p est suffisamment grand, alors $f(p-1) \neq p^2 - 1$. Soit p un nombre premier tel que $f(p-1) = p^2 - 1$. En posant $m = p - 1$ et $n = 1$ dans la divisibilité, on trouve

$$(p^2-1)^2 + 1 = f(p-1)^2 + f(1) \mid ((p-1)^2 + 1)^2.$$

Ceci implique, après développement, que $p^4 - 2p^2 + 2 \leqslant (p^2 - 2p + 2)^2 = p^4 - 4p^3 + 6p^2 - 8p + 4$, ce qui implique que $2p^3 \leqslant 4p^2 - 4p + 1$, ce qui n'est pas vrai lorsque p est suffisamment grand, par croissance comparée.

Ainsi, il existe un entier $M \geqslant 1$ tel que $\boxed{\text{pour tout nombre premier } p \geqslant M,\ f(p-1) = p - 1}$.

Soit $n \geqslant 1$ un entier quelconque et $p \geqslant M$ un nombre premier. En posant $m = p - 1$ dans la relation, on trouve, puisque $f(n) \equiv -(p-1)^2 \mod (p-1)^2 + f(n)$,

$$0 \equiv ((p-1)^2 + n)^2 \equiv (n - f(n))^2 \mod (p-1)^2 + f(n).$$

Le nombre $(n - f(n))^2$ admet donc une infinité de diviseurs, ce qui implique qu'il est nul, et $\boxed{f(n) = n \text{ pour tout } n}$.

Réciproquement, la fonction identité est bien solution du problème.

Exercice 4.29. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que pour tout nombre premier p, $p \mid f(a)^{f(p)} - f(b)^p$ si et seulement si $p \mid a - b$.

Solution 4.29. **Réponse :** La seule solution est l'identité .

En posant $b = a$ dans la divisbilité, on a pour tout nombre premier que $p \mid a - a$, donc d'après le petit théorème de Fermat,

$$0 \equiv f(a)^{f(p)} - f(a)^p \equiv f(a)^{f(p)} - f(a) \mod p.$$

Ainsi, pour tout a et tout nombre premier p, $f(a)^{f(p)} \equiv f(a) \mod p$. On déduit que, à nouveau à l'aide du petit théorème de Fermat , pour tout a, b, $f(a)^{f(p)} - f(b)^p \equiv f(a) - f(b) \mod p$. On a donc l'équivalence

$$p \mid a - b \iff p \mid f(a) - f(b).$$

Montrons à partir de là que $|f(n+1) - f(n)| = 1$. Soit $n \geqslant 1$ un entier et p un éventuel diviseur premier de $f(n+1) - f(n)$. D'après l'équivalence ci-dessus, cela implique que $p \mid (n+1) - n = 1$, ce qui est absurde. Le nombre $f(n+1) - f(n)$ n'a donc aucun facteur premier, d'où $\boxed{|f(n+1) - f(n)| = 1}$.

D'autre part, si on avait $f(n+2) = f(n)$ pour un certain entier n, on aurait que $3 \mid f(n+2) - f(n)$ donc $3 \mid (n+2) - n = 2$, ce qui est absurde. La quantité $f(n+1) - f(n)$ ne change donc jamais de signe. On a donc soit $f(n+1) - f(n) = 1$ pour tout n, soit $f(n+1) - f(n) = -1$ pour tout n.

Dans le second cas, on déduit que $g(n) = -n + g(1) + 1$, pour tout n, par récurrance immédiate, ce qui est absurde car f ne peut pas prendre de valeurs négatives.

Dans le premier cas, on déduit par récurrence que $\boxed{f(n) = n + f(1) - 1 \text{ pour tout } n}$ par récurrence immédiate.

Réciproquement, si f est de la forme $f(n) = n + c$, avec $c \geqslant 0$, alors on a pour tout nombre premier p et tout entier a,

$$0 \equiv f(a)^{f(p)} - f(a) = (a+c)^{p+c} - (a+c) \equiv (a+c)^c - (a+c) \mod p.$$

On déduit que la polynôme $X^{c+1} - X$ admet au moins p racines modulo p, ce qui implique que $c = 0$ ou que $c+1 \geqslant p$. Comme la deuxième inégalité ne peut pas être vraie pour tout nombre premier p, on déduit que $c = 0$, donc f est forcément l'identité. L'identité est bien solution puisque $a^p - b^p \equiv a - b \mod p$ pour tout nombre premier p d'après le petit théorème de Fermat.

Exercice 4.30. *(Taiwan IMOC 2017)* Déterminer les $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$f(x) + f(y) \mid x^2 - y^2 \quad \forall x, y \in \mathbb{N}^\star.$$

Solution 4.30. **Réponse :** La seule fonction solution est l'identité, dont on vérifie qu'elle est solution puisque $x + y \mid x^2 - y^2$ pour tout couple (x, y) d'entiers.

Soit f une fonction solution. Commeçons par montrer que f est non bornée. Soit x un entier tel que $2x + 1 = p$ est un nombre premier. En prenant $y = x + 1$ dans l'équation, on trouve $f(x) + f(x + 1) \mid (x + 1)^2 - x^2 = p$, et comme $f(x) + f(x + 1) > 1$, on déduit que $f(x + f(x + 1) = p$. En prenant p arbitrairement grand, on déduit que f peut prendre des valeurs arbitrairement grandes, donc $\boxed{f \text{ est non bornée}}$.

Motrons à présent que f est injective. Soient u et v tels que $f(u) = f(v) = c$. Alors pour tout x, on a $f(x) + f(u) \mid x^2 - u^2$ et $f(x) + f(v) \mid x^2 - v^2$, donc $f(x) + c \mid u^2 - v^2$. Comme $f(x)$ peut prendre des valeurs arbitrairement grandes, l'entier $u^2 - v^2$ admet une infinité de diviseurs, donc $u^2 = v^2$ et $u = v$. Ainsi $\boxed{f \text{ est injective}}$.

Montrons enfin par récurrence que $f(x) = x$ pour tout x.

Initialisation : On a $f(1) + f(2) \mid 2^2 - 1^2 = 3$ donc $\{f(1), f(2)\} = \{1, 2\}$. Supposons que $f(1) = 2$. Alors $f(2) = 1$. De plus, $f(1) + f(3) \mid 8$ et $f(2) + f(3) \mid 5$, donc $1 + f(3) = 5$ et $f(3) = 4$ mais $f(1) + f(3) = 6$ n'est pas un diviseur de 8. C'est absurde, donc $\boxed{f(1) = 1}$.

Hérédité : On suppose que $f(x) = x$ pour un certain $x \geqslant 1$ fixé. On a $f(x)+f(x+1) \mid 2x+1$, donc $x+f(x+1)$ est un diviseur de $2x + 1$ qui est supérieur strictement à $\lfloor (2x+1)/2 \rfloor = x$. On déduit que $x + f(x + 1) = 2x + 1$, donc que $\boxed{f(x + 1) = x + 1}$, ce qui achève la récurrence.

Exercice 4.31. *(Canada MO 2017)* Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction telle que, pour tout entier $n \geq 1$, $f(f(n))$ soit égal au nombre de diviseurs positifs de n. Montrer que, si p est un nombre premier, alors $f(p)$ est aussi un nombre premier.

Solution 4.31.

➢ Commentaire :

> Une erreur fréquente sur ce problème est de penser que si $d(n) = n$, alors nécessairement $n = 2$, et d'oublier qu'on peut aussi avoir $n = 1$.

Dans la suite, on note $d(n)$ le nombre de diviseurs positifs de n.

Si p est premier, on a $f(f(p)) = 2$ par définition. En appliquant f des deux côtés de l'égalité, on voit que $f(2) = d(f(p))$. On veut donc montrer que $f(2) = 2$, ce qui prouvera que $f(p)$ a exactement deux diviseurs et est donc premier.

Or, on a aussi $f(2) = d(f(2))$. Pour qu'un entier $n \geqslant 2$ vérifie $n = d(n)$, tous les nombres inférieurs à n doivent diviser n, y compris $n-1$ qui est toujours premier avec n, donc $n-1 = 1$ et $n = 2$. On déduit que $\boxed{f(2) \in \{1, 2\}}$.

On suppose par l'absurde que $f(2) = 1$. Alors $d(f(p)) = 1$ pour tout p premier, donc $f(p) = 1$ pour tout nombre p premier, puisque 1 est le seul entier à admettre un seul diviseur. Mais alors

$$1 = f(3) = f(d(2^2)) = f(f(f(2^2))) = d(f(2^2))$$

et l'on déduit que $f(4) = 1$. Mais alors

$$f(f(4)) = f(1) = f(f(2)) = d(2) = 2 \neq d(4)$$

ce qui fournit la contradiction désirée. On a donc bien $f(2) = 2$, ce qui conclut.

Exercice 4.32. (Iran round 3 2023 P1) Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction. Pour tout entier $n \geqslant 1$, on pose $P(n) = f(1) \cdot \ldots \cdot f(n)$. Déterminer toutes les fonctions f pour lesquelles

$$P(a) + P(b) \mid a! + b!$$

pour tous entiers $a, b \geqslant 1$.

Solution 4.32. **Réponse :** La seule solution est l'identité.

On prouve que $f(n) = n$ pour tout entier $n \geqslant 1$ par récurrence forte sur n.

Initialisation : En posant $a = b = 1$ dans la divisibilité, on trouve $2f(1) \mid 2 \cdot 1!$ donc $\boxed{f(1) = 1}$.

Hérédité : Supposons que $f(k) = k$ pour tout entier $k \leqslant n$, avec $n \geqslant 1$ fixé. Montrons que $f(n+1) = n+1$. Par hypothèse de récurrence, on a $P(n) = n!$ et $P(n+1) = n!f(n+1)$. D'une part, en posant $(a, b) = (n+1, n)$ dans la divisibilité, on trouve

$$f(n+1)n! + n! \mid (n+1)! + n! \Longrightarrow n!(f(n+1)+1) \mid n!(n+2) \Longrightarrow f(n+1)+1 \mid n+2.$$

En particulier, $f(n+1)+1 \leqslant n+2$ et $\boxed{f(n+1) \leqslant n+1}$.

Maintenant, en posant $(a, b) = (n+1, 1)$, on trouve

$$f(n+1)n! + 1! \mid (n+1)! + 1.$$

De cette divisibilité, on déduit que

$$f(n+1)n! + 1 \mid (n+1)! + 1 - [f(n+1)n! + 1] = n!(n+1-f(n+1)).$$

Or, $f(n+1)n!+1$ est premier avec $n!$. D'après le lemme de Gauss, on déduit que $n!f(n+1)+1 \mid (n+1)-f(n+1)$. Or, puisque $f(n+1) \leqslant n+1$, on a l'encadrement $0 \leqslant (n+1) - f(n+1) < n+1 \leqslant n!f(n+1)+1$. Ceci implique que $\boxed{f(n+1) = n+1}$, ce qui achève la récurrence.

Exercice 4.33. (Canada MO 2008, modifié) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tout entier $n \in \mathbb{N}^\star$ et tout nombre premier p,

$$f(n)^p \equiv n \mod f(p).$$

Solution 4.33. **Réponse :** Les fonctions solutions sont

1. La fonction identité définie par $f(n) = n$ pour tout n,
2. Toute fonction telle que $f(p) = 1$ pour tout nombre premier p,
3. Toute fonction telle que $f(p) = 1$ pour tout nombre premier impair et $f(2) = 2$ et telle que $f(n) - n$ est pair.

On commence par vérifier que ces fonctions sont bien solutions. C'est trivial pour les deux premières fonctions. Pour la troisième, si $p = 2$, on a bien $f(n)^2 \equiv f(n) \equiv n \mod 2$, donc toutes les fonctions de la troisième forme sont solutions.

Soit à présent f une fonction solution. En posant $n = p$ dans la congruence, on trouve que $p \equiv f(p)^p \equiv 0 \mod f(p)$ donc $f(p) \mid p$ et $\boxed{f(p) \in \{1, p\}}$.

➢ Cas 1 : Si $f(p) = p$ pour une infinité de nombres premiers. Soit n un entier et p tel que $f(p) = p$. D'après le petit théorème de Fermat, $f(n) \equiv f(n)^p \equiv n \mod p$, donc $p \mid f(n) - n$. Puisque cette divisibilité est vrai pour une infinité de nombres premiers, on a $\boxed{f(n) = n}$ pour tout entier n.

➢ Cas 2 : Si $f(p) = p$ pour un nombre fini de nombres premiers impairs. Prenons p un tel nombre premier. D'après le théorème de Dirichlet, il existe une infinité de nombres premiers q tels que $q \equiv -1 \mod p$. On peut en particulier en choisir un tel que $f(q) = 1$. Alors en prenant $n = q$ dans la congruence, on trouve $1 \equiv q \equiv -1 \mod p$, ce qui est absurde. On déduit que $\boxed{f(p) = 1 \text{ pour tout nombre premier } p \text{ impair}}$.

Si $f(2) = 1$, alors f est de la deuxième forme annoncée. Si $f(2) = 2$, il faut alors que $f(n) \equiv f(n)^2 \equiv n \mod 2$, donc f doit être de la troisième forme. Ceci conclut.

Exercice 4.34. (BMO 2017 P3) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$n + f(m) \mid f(n) + nf(m)$$

pour tous $n, m \in \mathbb{N}^\star$.

Solution 4.34. **Réponse :** Les deux fonctions solutions sont la fonction définie par $f(n) = n^2$ pour tout n et la fonction constante égale à 1.

La divisibilité implique, pour toute paire (m, n),

$$n + f(m) \mid f(n) + nf(m) - n(n + f(m)) = f(n) - n^2.$$

Ainsi, si f prend une infinité de valeurs, pour tout entier n, le nombre $f(n) - n^2$ admet une infinité de diviseurs (tous les nombres de la forme $n + f(m)$, qui sont en quantité infinie par hypothèse) et est donc nul. On a donc $\boxed{f(n) = n^2}$. Réciproquement, puisque $n + m^2 \mid n(n + m^2) = n^2 + nm^2$, la fonction carrée est bien solution.

On suppose dans la suite que f prend un nombre fini de valeurs, ce qui implique en particulier que f est bornée par une constante $C > 0$.
En prenant $n = m = 1$, on obtient que $1 + f(1) \mid f(1) - 1$. Mais alors $1 + f(1) \mid f(1) - 1 - (f(1) + 1) = 2$, donc $f(1) + 1 = 2$ et $\boxed{f(1) = 1}$.
En prenant $m = 1$, l'équation de départ donne $n + 1 \mid f(n) + n$, donc $n + 1 \mid f(n) + n - (n + 1) = f(n) - 1$. En prenant n tel que $n > C$, on a pourtant $|f(n) - 1| \leqslant C + 1 < n + 1$, ce qui conduit à $f(n) = 1$. On a donc montré que $\boxed{\text{si } n > C,\ f(n) = 1}$.

Soit maintenant m un entier quelconque et $n > C$. La divisibilité de l'énoncé implique que $n+f(m) \mid 1+nf(m)$. On déduit que $n + f(m) \mid 1 + nf(m) - f(m)(n + f(m)) = 1 - f(m)^2$. En prenant $n > C^2$, on a pourtant $|1-f(m)^2| \leqslant C^2 < n+f(m)$, ce qui implique que $f(m)^2 = 1$ puis que $\boxed{f(m) = 1 \text{ pour tout } m}$. Réciproquement, la fonction constante égale à 1 est bien solution du problème.

Exercice 4.35. (BMO SL 2017 N2) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que $xf(x) + f(y)^2 + 2xf(y)$ est un carré parfait pour tous $x, y \in \mathbb{N}^\star$.

Solution 4.35. **Réponse :** La seule solution est l'identité.

➢ **Commentaire :**

> L'idée principale de ce problème est de comparer la croissance des carrés (croissance quadratique) à la croissance de l'expression considérée, qui est "linéaire" en x. Cette comparaison se matérialise par de bon encadrements de l'expression considérée.
>
> On commence par réécrire l'énoncé sous la forme
>
> $$(x + f(y))^2 + x(f(x) - x) = A_{x,y}^2.$$
>
> On utilise ensuite que la suite des différences de deux carrés consécutifs est non bornée : pour tout constante C, pour tout Y suffisamment grand, l'encadrement $Y^2 < Y^2 + C < (Y + 1)^2$ implique que $Y^2 + C$ n'est pas un carré parfait.
>
> En vertue de ce principe, si f est non borné, en prenant y tel que $f(y)$ est grand et en fixant x, le carré du membre de gauche est arbitrairement grand, ce qui force l'égalité $f(x) = x$.
>
> Dans le cas où f est bornée, le même principe va s'appliquer : Comme $A_{x,1}^2 = x(f(x)+2f(1))+f(1)^2 \geqslant 2xf(1)$, la suite $(A_{x,1}^2)$ est croissante, mais, d'autre part, un calcul de $A_{x+c,1}^2 - A_{x,1}^2$ invite à considérer c tel que $f(x+c) = f(x)$ (ce qui se produit pour plusieurs x), auquel cas la différence $A_{x+c,1}^2 - A_{x,1}^2$ est petite, ce qui n'est pas possible lorsque $A_{x,1}$ est trop grand.

Pour tout x et y, on réécrit on note $A_{x,y}$ l'entier tel que $xf(x) + f(y)^2 + 2xf(y) = A_{x,y}^2$. L'égalité se réécrit

$$(f(y) + x)^2 + x(f(x) - x) = A_{x,y}^2.$$

On distingue alors deux cas :

➢ Si f est non bornée : dans ce cas, pour tout n, il existe un entier y_n tel que $f(y_n) \geqslant n$. Soit $x \in \mathbb{N}^\star$ un entier quelconque. Pour n tel que $2(x+n) > x|f(x)-x|$ (qui se produit lorsque n est suffisamment grand), on a en particulier $2(x+f(y_n)) > x|f(x)-x|$ et donc l'encadrement suivant

$$(x+f(y_n)-1)^2 < (x+f(y_n))^2 + x(f(x)-x) < (x+f(y_n)+1)^2.$$

Cet encadrement implique que $(f(y_n)+x)^2+x(f(x)-x) = (f(y_n)+x)^2$, soit $\boxed{f(x)=x}$. Réciproquement, l'identité est bien solution, en vertue de l'identité

$$x^2+y^2+2xy = (x+y)^2.$$

➢ Si f est bornée : Soit C un entier tel que $1 \leqslant f(x) \leqslant C$ pour tout entier x. Notons par ailleurs que, pour tout entier x, $A_{x,1} \geqslant 2xf(1)$. Soit x un entier suffisamment grand (voir condition en rouge). D'après le principe des tiroirs, parmi les entiers $x, x+1, \ldots, x+C$, il en existe, notés $x+a$ et $x+b$ tels que $f(x+a) = f(x+b)$. On a alors

$$A_{x+a,1}^2 - A_{x+b,1}^2 = (x+a)f(x+a) - (x+b)f(x+b) + 2(a-b)f(1) = (a-b)f(x+a) + 2(a-b)f(1) < 3(a-b)C < 3C^2.$$

On déduit également de ce calcul que $A_{x+a,1}^2 - A_{x+b,1}^2 > 0$. En particulier, $A_{x+a,1} \geqslant A_{x+b,1}+1$, soit $A_{x+a,1}^2 \geqslant (A_{x+b,1}+1)^2$. Il vient

$$3C^2 > A_{x+a,1}^2 - A_{x+b,1}^2 \geqslant (A_{x+b,1}+1)^2 - A_{x+b,1}^2 = 2A_{x+b,1} \geqslant 2\sqrt{2xf(1)}.$$

Lorsque $x > \dfrac{9C^4}{8f(1)}$, cette inégalité est fausse, ce qui apporte la contradiction. Il n'y a donc $\boxed{\text{pas de solutions}}$ dans ce cas.

$\boxed{\text{Remarque :}}$ Dans le cas où f est bornée, on peut également conclure de la façon suivante : en prenant $x = p$ un grand nombre premier, on a

$$pf(p) + f(1)^2 + 2pf(1) = A_{p,1}^2 \quad \Longleftrightarrow p(f(p)+3f(y)) = (A_{p,1}-f(1))(A_{p,1}+f(1)).$$

On déduit notamment que $A_{p,1} \equiv \pm f(1) \mod p$. Comme $A_{p,1} > 2pf(1)$, pour p suffisamment grand, on a en particulier $A_{p,1} > p - f(1) > p/2$. On a alors

$$4Cp \geqslant A_{p,1}^2 - f(1)^2 > \frac{p^2}{4} - f(1)^2,$$

ce qui est faux lorsque p est suffisamment grand.

Exercice 4.36. (Canada MO 2021) Une fonction f de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ est dite *canadienne* si pour tous $x, y \in \mathbb{N}^\star$,

$$\mathrm{PGCD}(f(f(x)), f(x+y)) = \mathrm{PGCD}(x,y).$$

Déterminer tous les entiers m tels que $f(m) = m$ pour toute fonction canadienne.

Solution 4.36. **Réponse :** Les entiers n qui ne sont pas puissance d'un nombre premier.

Soit f une fonction canadienne.

En prenant $y = x$ dans l'équation, on trouve

$$x = \mathrm{PGCD}(x,x) = \mathrm{PGCD}(f(f(x)), f(2x)) \quad \Longrightarrow x \mid f(f(x)) \text{ et } x \mid f(2x).$$

En particulier, $x \leqslant f(f(x))$, on peut donc poser $y = 2f(f(x)) - x$. On trouve alors, puisque $f(f(x)) \mid f(2f(f(x)))$,

$$f(f(x)) = \mathrm{PGCD}\big(f(f(x)), f\big(2f(f(x))\big)\big) = \mathrm{PGCD}(x, 2f(f(x)) - x) = \mathrm{PGCD}(x, 2f(f(x))).$$

Ceci conduit à $f(f(x)) \mid x$, et on déduit que $\boxed{f(f(x)) = x}$ pour tout x. En particulier, l'équation devient

$$\mathrm{PGCD}(x, f(x+y)) = \mathrm{PGCD}(x,y) \quad \text{pour tout } x, y \in \mathbb{N}^\star.$$

En faisant le changement de variable $z = x+y$, on trouve (puisque $\mathrm{PGCD}(x,y) = \mathrm{PGCD}(x, y+x)$),

$$\mathrm{PGCD}(x, f(z)) = \mathrm{PGCD}(x, z) \quad \text{pour tout } x < z.$$

Étape 1 : Si n n'est pas puissance de nombre premier, $f(n) = n$. Soit n un entier qui n'est pas une puissance de nombre premier. On peut écrire $n = ab$ avec a et b des nombres premiers entre eux. On a alors, en prenant $x = a$,

$$a = \mathrm{PGCD}(a, n) = \mathrm{PGCD}(a, f(ab)),$$

ce qui implique que $a \mid f(ab)$. De même, $b \mid f(ab)$, donc $\boxed{n \mid f(n)}$. Mais alors $n \mid f(n) \mid f(f(n)) = n$ donc $\boxed{n = f(n) \text{ si } n \text{ n'est pas une puissance de nombre premier}}$.

Étape 2 : Soit maintenant p un nombre premier et α un entier. On construit f canadienne telle que $f(p^\alpha) \neq p^\alpha$.
On pose

$$f(n) = \begin{cases} p^{\alpha+1} & \text{si } n = p^\alpha \\ p^\alpha & \text{si } n = p^{\alpha+1} \\ n & \text{sinon} \end{cases}$$

On vérifie que f vérifie $f(f(x)) = x$ pour tout x, puis que :

➢ Si $x + y \neq p^\alpha, p^{\alpha+1}$, alors on a bien

$$\mathrm{PGCD}(f(f(x)), f(x + y)) = \mathrm{PGCD}(x, x + y) = \mathrm{PGCD}(x, y).$$

➢ Si $x + y = p^\alpha$, alors notons que $x, y < p^\alpha$ et donc que $v_p(x), v_p(y) < \alpha$,

$$\mathrm{PGCD}(f(f(x)), f(x + y)) = \mathrm{PGCD}(x, p^{\alpha+1}) = \mathrm{PGCD}(x, p^\alpha) = \mathrm{PGCD}(x, x + y) = \mathrm{PGCD}(x, y).$$

➢ Si $x + y = p^{\alpha+1}$, alors notons que $x, y < p^{\alpha+1}$ et donc que $v_p(x), v_p(y) < \alpha + 1$,

$$\mathrm{PGCD}(f(f(x)), f(x + y)) = \mathrm{PGCD}(x, p^\alpha) == \mathrm{PGCD}(x, p^{\alpha+1})\mathrm{PGCD}(x, x + y) = \mathrm{PGCD}(x, y).$$

Ainsi, la fonction construite est canadienne, et vérifie $f(p^\alpha) \neq p^\alpha$, donc $\boxed{p^\alpha \text{ n'est pas solution}}$. Ceci achève le problème.
$\boxed{\text{Remarque :}}$ Pour montrer que $f(f(x)) = x$, on aurait également pu procéder comme suit. Soit p un diviseur premier de x. En prenant $x = y = p^n$ dans l'équation, on obtient que $p^n \mid f(2p^n)$. En prenant $y = 2p^n - x$, avec $n > \max(v_p(x), v_p(f(f(x))))$, on déduit que

$$v_p(x) = v_p\big(\mathrm{PGCD}(x, 2p^n - x)\big) = v_p\big(\mathrm{PGCD}(f(f(x)), f(2p^n))\big) = \min(v_p(f(f(x))), v_p(f(2p^n))) = v_p(f(f(x))).$$

On a donc bien $f(f(x)) = x$.

Exercice 4.37. (Balkan MO SL 2020 N3) Soit $k \geqslant 2$. Trouver toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers strictements positifs $x_1, ..., x_k$, on ait

$$x_1! + ... + x_k! \mid f(x_1)! + ... + f(x_k)!$$

Solution 4.37.
Réponse : La seule fonction est la fonction identité.

➢ Commentaire :

> On a une relation du type $A \mid B$.
>
> Poser $x_1 = \ldots = x_k$ donne $x \leqslant f(x)$. Pour montrer l'inégalité inverse, il faut un résultat de non divisibilité : si $x + 1$ ne divise pas $f(x)!$, c'est que $f(x) \leqslant x$.
>
> Pour deviner la méthode, on pourra se restreindre au cas $k = 2$. Le jeu est de choisir un nombre premier p tel que $p \mid A = x_1! + x_2!$ mais tel que $p > x_1, x_2$. Cela force p à diviser B de façon non triviale.

L'ingrédient clé pour cela est l'identité de Wilson, qui donne que

$$p \mid (p-1)! + 1 \mid f(p-1)! + f(1)!.$$

Pour p suffisamment grand, p ne divise pas $f(1)!$, donc il ne divise pas $f(p-1)!$, ce qui donne $f(p-1) \leqslant p-1$. f a alors une infinité de points fixes. Conclure à partir de cel est plus technique que difficile, et passe par la méthode classique de produire des diviseurs arbitrairement grands d'une quantité fixe pour montrer qu'elle est nulle.

La preuve qui suit adapte ce raisonnement au cas général $k \geqslant 2$.

Soit f une solution éventuelle. En prenant $x_1 = \ldots = x_k = x$, la relation donne que $k \cdot x! \mid k \cdot f(x)!$, ce qui implique que $x! \mid f(x)!$. On déduit que $\boxed{x \leqslant f(x)}$ pour tout entier x strictement positif.

Fixons désormais un nombre premier $p > f(1)$, $x_1 = 1, x_2 = p-1$ et $x_3 = \ldots = x_k = N$ avec $N \geqslant p$. Puisque $f(N) \geqslant N \geqslant p$, $p \mid f(N)!$ et $p \mid N!$. De plus, d'après le théorème de Wilson, $p \mid (p-1)! + 1$. Ainsi, la relation de l'énoncé implique que

$$p \mid 1 + (p-1)! + (k-2)N! \mid f(1)! + f(p-1)! + (k-2)f(N)!$$

Comme p divise $f(N)!$, on a $p \mid f(1)! + f(p-1)!$. Mais $p > f(1)$ donc p ne divise pas $f(1)!$. Donc p ne divise pas non plus $f(p-1)!$. On a donc $f(p-1) \leqslant p-1$ et $\boxed{f(p-1) = p-1}$ pour tout entier $p > f(1)$.

Prenons alors n un entier strictement positif et $p > f(1)$ un nombre premier. On pose $x_1 = n, x_2 = \ldots = x_k = p-1$. La relation de l'énoncé donne

$$n! + (k-1) \cdot (p-1)! \mid f(n)! + (k-1) \cdot f(p-1)! = f(n)! + (k-1) \cdot (p-1)!.$$

Mais alors

$$n! + (k-1) \cdot (p-1)! \mid f(n)! + (k-1) \cdot (p-1)! - (n! + (k-1) \cdot (p-1)!) = f(n)! - n!.$$

Cette relation de divisibilité étant vraie pour tout nombre premier $p > f(1)$, le nombre $f(n)! - n!$ admet une infinité de diviseurs, il est donc nul. On a bien $\boxed{f(n) = n}$ pour tout entier n.

Réciproquement, on vérifie que la fonction f vérifie la relation de divisibilité.

Exercice 4.38. (USAMO 2012 P4) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que $f(n!) = f(n)!$ pour tout entier $n \geqslant 1$ et $m - n \mid f(m) - f(n)$ pour tous entiers $m, n \in \mathbb{N}^\star$ distincts.

Solution 4.38. **Réponse :** Les solutions sont $f(n) = 1$ pour tout n, $f(n) = 2$ pour tout n et $f(n) = n$ pour tout n.

➢ Commentaire :

Dans ce problème, il faut regarder les valeurs de f sur des petits entiers. Pour les grands entiers, le jeu est d'utiliser la relation

$$n! - k! \mid f(n)! - f(k)!$$

pour des valeurs quelconques de n et des petites valeurs de k. Par exemple, si $k = 3$, on trouve que $3 \mid f(n)! - f(3)!$. Donc si $f(3) < 3$, 3 ne divise pas $f(3)!$ donc il ne divise pas $f(n)!$, et donc $f(n) < 3$.

En posant $n = 1$ dans l'équation, on a $f(1) = f(1)!$. Les seuls entiers k tels que $k = k!$ sont $k = 1$ et $k = 2$. On déduit que $\boxed{f(1) \in \{1, 2\}}$. On distingue alors deux cas :

- Si $f(1) = 2$: En posant $(m, n) = (3!, 1)$ dans la divisibilité, on obtient $5 = 3! - 1 \mid f(3)! - f(1) = f(3)! - 2$, soit $f(3)! \equiv 2 \mod 5$. Cela implique que $f(3) < 5$ (sinon on aurait $5 \mid f(3)!$). Le seul entier $k \in \{1, 2, 3, 4\}$ tel que $k! \equiv 2 \mod 5$ est $k = 2$, donc $\boxed{f(3) = 2}$.

  En posant $(m, n) = (k!, 3!)$ dans la divisibilité, on obtient que $k! - 6 \mid f(k)! - 2$. En particulier, si $k > 3$, on déduit que $3 \mid f(k)! - 2$, donc $f(k)! \equiv 2 \mod 4$. Ceci implique que $\boxed{f(k) = 2 \text{ pour tout } m \geqslant 3}$. Enfin, en posant $(m, n) = (3!, 2!)$ dans la divisibilité, on a $4 \mid 3! - 2! \mid f(3)! - f(2)!$, donc $f(2)! \equiv 2 \mod 4$, ce qui implique également que $f(2) = 2$.

  Réciproquement, la fonction constante égale à 2 est bien solution du problème.

➢ Si $f(1) = 1$: En posant $n = 2$ dans l'équation, on a $f(2)! = f(2!) = f(2)$, donc $f(2) \in \{1, 2\}$. Ceci appelle à deux sous-cas :

- Si $f(2) = 1$: pour tout $m > 2$, en prenant $m!$ et 2 dans la divisbilité, on trouve $2 \mid m! - 2! \mid f(m)! - f(2)! = f(m)! - 1$. Donc $f(m)!$ est impair et $\boxed{f(m) = 1 \text{ pour tout } m > 2}$. Réciproquement, la fonction constante égale à 1 est solution du problème.
- Si $f(2) = 2$: On prouve par récurrence sur n que $f(n) = n$ pour tout entier n. C'est le cas pour $n = 1, 2$. Supposons que $f(n) = n$ pour un certain entier $n \geqslant 2$ fixé. En prenant $((n+1)!, n!)$ dans la divisibilité, on trouve

$$n \cdot n! = (n+1)! - n! \mid f(n+1)! - f(n)! = f(n+1)! - n!.$$

On déduit d'une part que $n! \mid f(n+1)!$ et donc que $f(n+1) \geqslant n$, mais aussi que $f(n) < 2n$, sinon on aurait $n \cdot n! \mid f(n)!$.

En prenant $(n+1, 1)$ dans la divisbilité, on trouve

$$n \mid (n+1) - 1 \mid f(n+1) - f(1) = f(n+1) - 1.$$

Ainsi, $f(n+1)$ est un entier compris entre n et $2n$ tel que $f(n+1) \equiv 1 \mod n$. On déduit que $\boxed{f(n+1) = n+1}$, ce qui achève la récurrence.

Réciproquement, la fonction identité est solution du problème.

Exercice 4.39. (RMM 2020 P4) Un sous-ensemble A de $\mathbb{N}^\star$ est dit *sans somme* si, pour toute paire (x, y) d'entiers de A (pas forcément distincts), le nombre $x + y$ n'est pas dans A. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ surjectives telles que, pour tout ensemble A sans somme, l'ensemble $\{f(a), a \in A\}$ est également sans somme.

Solution 4.39. **Réponse :** Les fonctiosn solutions sont les fonctions affines.

➢ **Commentaire :**

> Il faut appliquer l'énoncé à des ensembles sans somme petits. Le jeu du problème est le suivant. Soient x et y deux entiers. Par surjectivité de f, il existe z tel que $f(z) = f(x)+f(y)$. En posant $A = \{x, y, z\}$, A ne peut pas être sans somme, sinon $\{f(x), f(y), f(z)\}$ serait sans somme. On déduit qu'il y a une relation de liaison entre x, y et z, et l'erreur serait de penser qu'elle implique directement que $z = x+y$. On a en fait les valeurs suivantes possibles pour z :
>
> $$z \in \left\{\frac{x}{2}, \frac{y}{2}, |x - y|, x + y, 2x, 2y\right\}.$$
>
> Le reste du problème consiste à jongler astucieusement avec ces valeurs possibles.
>
> Dans le cas plus simple où $x = y$, z ne peut plus prendre que les valeurs $x/2$ et $2x$. Lorsque x est impair, cela force $z = 2x$.

Soient x et y des entiers strictement positifs. Par surjectivité de f, il existe un entier z tel que $f(z) = f(x)+f(y)$. Ainsi, l'ensemble $\{f(x), f(y), f(z)\}$, donc l'ensemble $\{x, y, z\}$ ne l'est pas non plus, par hypothèse. On a donc l'une des relations suivantes :

$$x + y = z, x + z = y, y + z = x, 2x = z, 2x = y, 2y = z, 2y = x, 2z = x, 2z = y.$$

Étape 1 : Montrons que $f(2x) = 2f(x)$ pour tout x.

On procède par récurrence sur $v_2(x)$.

Initialisation : Soit x tel que $v_2(x) = 0$ et z tel que $2f(x) = f(z)$, qui existe par surjectivité de f. D'après la discussion ci-dessus, on a $2z = x$ ou $2x = z$. Comme x est impair, on a nécessairement $2x = z$, donc $f(2x) = 2f(x)$.

Hérédité : Supposons que $f(2x) = 2f(x)$ pour tout entier x tel que $v_2(x) \leqslant k$, où $k \geqslant 0$ est fixé. Soit x un entier tel que $v_2(x) = k + 1$ et soit z tel que $2f(x) = f(z)$. De même que précédemment, on a $2z = x$ ou $2x = z$. Si $2z = x$, on aurait, par hypothèse de récurrence, $f(z) = f(x/2) = f(x)/2$, ce qui est absurde puisque $f(z) = 2f(x)$. On a donc $2x = z$, ce qui achève la récurrence.

➢ **Commentaire :**

> Une approche naturelle à partir de l'égalité $f(2x) = 2f(x)$ est de chercher à calculer $f(nx)$ pour tout n. Sans gourmandise, on peut commencer par chercher à calculer $f(3x)$ pour comprendre le prototype de preuve. Ensuite, quitte à montrer que $f(nx) = nf(x)$ pour tout x, autant le faire directement pour $x = 1$.

Étape 2 : Pour tout n, $f(n) = nf(1)$.

On procède par récurrence sur n.

Initialisation : On a déjà montré que $f(2) = 2f(1)$.

Hérédité : Supposons que $f(k) = kf(1)$ pour tout $k \leqslant n$, avec $n \geqslant 2$ fixé. Montrons que $f(n+1) = (n+1)f(1)$. Si $n + 1$ est pair, on a par hypothèse de récurrence, puisque $\dfrac{n+1}{2} \leqslant n$,

$$f(n + 1) = f\left(2 \cdot \frac{n+1}{2}\right) = 2f\left(\frac{n+1}{2}\right) = 2 \cdot \frac{n+1}{2} f(1) = (n + 1)f(1).$$

On se focalise désormais sur le cas où $n + 1$ est impair. Soit z tel que $f(z) = f(n + 1) + f(1)$. Comme $\{f(z), f(n+1), f(1)\}$ est sans somme, il en est de même de $\{z, n+1, 1\}$. On déduit que $z \in \{2(n+1), 2, n, n+2\}$ (notons qu'on a utilisé que $n \geqslant 2$ pour s'assurer qu'il n'y a pas de relation de somme entre 1 et $n + 1$).

- ➢ Si $z = 2(n + 1)$, alors $f(n + 1) + f(1) = f(2(n + 1)) = 2f(n + 1)$, donc $f(1) = f(n + 1)$. Mais alors l'ensemble $\{1, 2(n + 1)\}$ est sans somme alors que l'ensemble $\{f(1), f(2(n + 1))\} = \{f(1), 2f(n + 1)\}$ ne l'est pas, ce qui est une contradiction.
- ➢ Si $z = 2$, alors $f(n + 1) = f(2) - f(1) = f(1)$. On revient à la contradiction du cas précédent.

➢ Si $z = n$, alors $f(n+1) + f(1) = f(n) = nf(1)$, ce qui impose $f(n+1) = (n-1)f(1) = f(n-1)$. Mais alors l'ensemble $\{n-1, 2(n+1)\}$ est sans somme alors que l'ensemble $\{f(n-1), f(2(n+1))\} = \{f(n-1), 2f(n-1)\}$ ne l'est pas, ce qui est une contradiction.

On déduit que $z = n+2$, qui est pair. Comme $\dfrac{n+2}{2} \leqslant n$, par hypothèse de récurrence on a

$$f(n+1) = f(n+2) - f(1) = f\left(2 \cdot \frac{n+2}{2}\right) - f(1) = 2f\left(\frac{n+2}{2}\right) - f(1) = 2 \cdot \frac{n+2}{2} f(1) - f(1) = (n+1)f(1).$$

Ceci achève la récurrence.

On déduit que $f(n) = nf(1)$ pour tout n, donc f est linéaire. Comme f est surjective sur $\mathbb{N}^\star$, il s'agit de l'identité. Réciproquement, l'identité est bien solution du problème.

Remarque : On a implicitement utilisé dans l'hérédité que f est injective : si $f(a) = f(b)$ avec $a < b$, alors l'ensemble $\{a, 2b\}$ est sans somme mais pas l'ensemble $\{f(a), f(2b)\} = \{f(a), 2f(a)\}$, ce qui est absurde.

Remarque 2 : Une erreur fréquente sur ce problème est de penser que f vérifie directement l'équation de Cauchy à partir de sa définition. Cela revient à penser que si $f(x) + f(y) = f(z)$, alors $z = x + y$ en supposant que l'ensemble $\{x, y, z\}$ serait sans somme sinon, ce qui correspond à oublier toutes les autres relations de somme possibles sur x, y et z.

Exercice 4.40. (EGMO 2022 P2) Déterminer toutes les fonctions de $\mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers a et b,

1. $f(ab) = f(a)f(b)$ et
2. au moins deux des entiers $f(a), f(b)$ et $f(a+b)$ sont égaux.

Solution 4.40. **Réponse :** La fonction constante égale à 1 et la fonction $f(n) = c^{v_p(n)}$ pour tout n, où p est un nombre premier fixé et c un nombre entier.

Si f est constante égale à c, alors d'après la première relation, $c = c^2$, donc $c = 1$ et $f = 1$, et il s'agit bien d'une solution.

Si f est non constante égale à 1, on note $S = \{x, f(x) > 1\}$. D'après la première relation pour $a = b = 1$, $f(1)^2 = f(1)$ donc $f(1) = 1$, donc $1 \notin S$. Au vu de la première relation, si $x \in S$, l'un de ses diviseurs l'est aussi, donc l'élément minimal de S est un nombre premier que l'on note p. Nous allons alors montrer que $f(x) = f(p)^{v_p(n)}$. (On vérifie bien qu'une telle fonction est solution). D'après la première condition, $f(p^\alpha) = f(p)^\alpha$, et si $n = \prod_{i=1}^r p_i^{\alpha_i}$, on a $f(n) = \prod_{i=1}^r f(p_i)^{\alpha_i}$. Il suffit de montrer que $f(q) = 1$ pour tout premier $q \neq p$.

➢ Commentaire :

| Ici, le but est de créer un multiple un multiple de p qui soit proche de q

Soit alors $q \in S$ un nombre premier distinct de p. Il faut utiliser la deuxième relation pour rassembler ces informations. Pour cela, on va créé un multiple de q qui soit proche d'une puissance de p. D'après le petit théorème de Fermat, $q \mid p^{q-1} - 1$, donc $f(q) \mid f(p^{q-1} - 1)$ et $f(p^{q-1} - 1) > 1$. Or deux des nombres $f(1) = 1, f(p^{q-1} - 1)$ et $f(p^{q-1}) = f(p)^{q-1}$ sont égaux. Il vient que $f(p^{q-1} - 1) = f(p)^{q-1}$.

D'autre part, on vérifie que $f(p+1) = 1$ (ses facteurs premiers sont inférieurs à p) donc $f(p^2+p) = f(p)$. Ainsi, $f(p^2 + p + 1) = 1$ ou $f(p)$ d'après la deuxième condition. Par récurrence sur k, on montre que $f(p^k + p^{k-1} + \ldots + p + 1) \in \{1, f(p), \ldots, f(p)^{k-1}\}$. Or,

$$f(p^{q-2} + \ldots + p + 1) = \frac{f(p^{q-1} - 1)}{f(p-1)} = f(p)^{q-1},$$

ce qui est absurde. Cela conclut.

Exercice 4.41. (USA TSTST 2022, P4) Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que, pour tout couple d'entiers strictement positifs m et n, exactement un des entiers

$$f(m+1), \ldots, f(m+f(n))$$

est divisible par n. Montrer que $f(n) = n$ pour une infinité d'entiers n.

Solution 4.41. Soit $n \geqslant 1$. Pour tout entier $m \geqslant 1$, chacun des deux ensembles

$$\{f(m+1), \ldots, f(m+f(n))\} \quad \text{et} \quad \{f(m+2), \ldots, f(m+1+f(n))\}$$

contient exactement un entier divisible par n. Ainsi, si $n \mid f(m+1)$, aucun des entiers $f(m+2), \ldots, f(m+f(n))$ n'est divisible par n, de sorte que n divise $f(m+1+f(n))$. De même, si n ne divise pas $f(m+1)$, n divise un des entiers $f(m+2), \ldots, f(m+f(n))$, donc n ne divise pas $f(m+1+f(n))$. En conclusion, pour tout entier $m \geqslant 2$, $\boxed{n \mid f(m) \text{ si et seulement si } n \mid f(m+f(n))}$.

Cette équivalence signifie également que pour toute paire (x, y) d'entiers strictement supérieurs à 2, on a $\boxed{n \mid f(x) \text{ et } n \mid f(y) \text{ si et seulement si } f(n) \mid x-y}$.

Soient maintenant $k \geqslant 1$ un entier et x un entier tel que $kn \mid f(x)$. Alors kn divise également $f(x+f(kn))$, de sorte que n divise $f(x)$ et $f(x+f(kn))$. On déduit que $\boxed{f(n) \mid f(kn)}$ pour tout entier $k \geqslant 1$.

En particulier $f(n) \mid f(n)$ et $f(n) \mid f(2n)$, donc $f(f(n)) \mid 2n-n = n$. Remarquons alors que si n divise $f(n)$, alors il existe un entier k tel que $f(n) = kn$. Mais alors $f(kn) = f(f(n)) \mid n \mid f(n) \mid f(kn)$, de sorte que $f(kn) = f(n)$, donc $n \mid f(n) = f(kn) = f(f(n)) \mid n$ et $f(n) = n$. On a donc montré que $\boxed{\text{Si } n \mid f(n), \text{ alors } f(n) = n}$. Ainsi, il suffit de trouver des entiers n tels que $f(n) \mid n$.

D'autre part, puisque $f(f(n))$ divise n, on a en particulier pour tout nombre premier, $f(f(p))$ divise p, donc $f(f(p)) \in \{1, p\}$. Supposons que x soit tel que $f(x) = 1$. Alors pour tout entier $m \geqslant 1$, l'ensemble $\{f(m+1), \ldots, f(m+f(x))\}$ est réduit à $\{f(m+1)\}$, de sorte que x divise $f(m+1)$ pour tout m. En particulier, x divise $f(x) = 1$, donc $x = 1$. Ainsi, $f(p) \neq 1$ et $f(f(p)) \neq 1$ donc $\boxed{f(f(p)) = p}$ pour tout nombre premier p.

Si p divise $f(p)$ pour une infinité de nombres premiers p, alors d'après la discussion précédente, $f(p) = p$ pour une infinité de nombres premiers, ce qui donne le résultat voulu. Sinon, pour tout nombre premier p suffisamment grand, $f(p)$ et p sont premiers entre eux. On a alors $f(p) \mid f(pf(p))$ et $p = f(f(p)) \mid f(pf(p))$, de sorte $pf(p) \mid f(pf(p))$ et $f(pf(p)) = pf(p)$.

Il reste à voir que $pf(p)$ peut prendre une infinité de valeurs différentes. Pour cela, on suppose que l'on a construit k entiers différents de la forme $pf(p)$ et on choisit q un nombre premier sitrictement plus grand que ces k entiers. Alors $qf(q)$ est un bien un entier distincts des k précédents, car il est divisible par q mais pas les précédents.

La fonction f admet donc une infinité de points fixes.

Exercice 4.42. (IMO SL 2011 N3) Soit $n \geqslant 1$ un entier impair. Déterminer toutes les fonctions f de $\mathbb{Z}$ dans $\mathbb{Z}$ telles que, pour tous entiers x, y,

$$f(x) - f(y) \mid x^n - y^n.$$

Solution 4.42. **Réponse :** Les solutions sont les fonctions f définies par $f(x) = \varepsilon x^d + c$, où $\varepsilon \in \{-1, 1\}$, d est un diviseur de n et c est un entier.

On peut commencer par vérifier qu'une telle fonction f est solution, en vertu de l'identité

$$f(x) - f(y) = \varepsilon(x^d - y^d) \mid x^n - y^n,$$

vraie pour tous x et y.

Soit f une fonction solution. Quitte à considérer $f(x) - f(0)$, ce qui ne change pas la relation de divisibilité, on peut supposer que $f(0) = 0$. En remplaçant $(x, y) = (p, 0)$ dans la divisibilité, où p est un nombre premier, on obtient que $f(p) \mid p^n$. Ainsi, $f(p) \in \{\pm 1, \pm p, \ldots, \pm p^n\}$. D'après le principe des tiroirs infinis, il existe un couple (ε, d) avec $\varepsilon \in \{-1, 1\}$ et $d \geqslant 0$ tel que, $\boxed{\text{pour une infinité de nombres premiers } p,\ f(p) = \varepsilon p^d}$. Quitte à considérer $-f$ plutôt que f, on peut supposer que $\varepsilon = 1$.

Notons que si $d = 0$, alors f est constante, mais alors la relation signifie que 0 est diviseur de $x^n - y^n$ pour tout x, y, ce qui est absurde. On travaille donc avec $d \geqslant 1$ dans la suite. Notons $n = kd + r$ la division euclidienne de n par d, avec $0 \leqslant r < d$. On fixe désormais un entier x. En posant $y = p$, où p est un nombre premier tel que $f(p) = p^d$, on trouve que $f(x) - p^d \mid x^n - p^n$. Puisque $p^d \equiv f(x) \mod f(x) - p^d$, on déduit que

$$0 \equiv x^n - p^n = x^n - p^r(p^d)^k \equiv x^n - p^r f(x)^k \mod f(x) - p^d.$$

Puisque $r < d$, lorsque p est suffisamment grand, on a $|f(x) - p^d| > |x^n - p^r f(x)|$ (puisque x est fixé, c'est de la croissance comparée). On déduit alors que $x^n = p^r f(x)^k$. Si $r > 0$, cette égalité est fausse pour p suffisamment grand. Donc $r = 0$. On trouve que $f(x)^k = x^n$, soit $f(x) = x^{n/k} = x^d$.

On a donc que $f(x) = x^d$ pour tout entier x. En revenant au cas général, on déduit que les seules solutions sont de la forme annoncée.

Exercice 4.43. (IMO SL 2019 N4) Soit C un entier naturel non nul. Trouver toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que, pour tous les entiers a et b de somme $a + b \geqslant C$, l'entier $a + f(b)$ divise $a^2 + bf(a)$.

Solution 4.43. **Réponse :** Les fonctions de la forme $f(x) = ax$ avec $a \geqslant 1$.

Tout d'abord, toute fonction linéaire strictement croissante est solution. En effet, pour tout entier $k \geqslant 1$, l'entier $a + kb$ divise bien $a^2 + b \times (ka) = a(a + kb)$. Réciproquement, montrons que toute solution est une fonction linéaire (qui sera strictement croissante, puisque à valeurs dans $\mathbb{N}^*$).

Notons d'abord que si a et b sont des entiers tels que $a + b \geq C$, alors en substituant a par 1, on obtient que pour tout $b \geqslant C$:

$$1 + f(b) \mid 1 + bf(1)$$

soit $1 + f(b) \leqslant 1 + bf(1)$ donc $\boxed{f(b) \leqslant bf(1)}$ pour tout entier $b \geqslant C$.

De plus, si a et b vérifient que $a + b \geqslant C$:

$$a + f(b) \mid a^2 + bf(a) - (a + f(b))(a - f(b)) = f(b)^2 + bf(a)$$

Soit $b \geqslant 1$ un entier. On choisit un entier $n \geqslant 1$ tel que $b^n - f(b) \geqslant C$. On pose alors $a = b^n - f(b)$ pour obtenir que

$$b \mid b^n = b^n - f(b) + f(b) \mid f(b)^2 + bf(b^n - f(b))$$

On déduit que $\boxed{b \mid f(b)^2}$ pour tout entier strictement positif b. En particulier si p est un nombre premier, $p \mid f(p)$.

On montre à présent que $f(p) = pf(1)$ pour une infinité de nombres premiers p. Soit p un nombre premier strictement supérieur à $f(1)$ et à C. Alors en remplaçant a par p et b par 1 on trouve

$$p + f(1) \mid p^2 + f(p)$$

Or p est premier avec $p + f(1)$ et p divise chacun des termes p^2 et $f(p)$ donc $p(p + f(1))$ divise $p^2 + f(p)$. On déduit $p^2 + pf(1) \leqslant p^2 + f(p)$ soit $pf(1) \leqslant f(p)$. Ceci combiné avec l'inégalité $f(p) \leqslant pf(1)$ si p est suffisamment grand donne $\boxed{f(p) = pf(1)}$ pour une infinité de nombres premiers p.

Soit a un entier et soit p un nombre premier tel que $f(p) = pf(1)$ et tel que p et $a + pf(1)$ soient premiers entre eux (la deuxième condition s'obtient en prenant p suffisamment grand). Alors en substituant b par p, on obtient

$$a + pf(1) \mid a^2 + pf(a) - a(a + pf(1)) = p(f(a) - af(1))$$

Or $a + pf(1)$ est premier avec p donc $a + pf(1)$ divise $f(a) - af(1)$. Mais cette relation de dvisibilité est vraie pour une infinité de nombres premiers p. On déduit que $\boxed{f(a) = af(1)}$ pour tout entier a. f est bien linéaire strictement croissante.

Solution alternative

On présente une autre façon de conclure une fois que l'on a montré que $p \mid f(p)$ pour tout nombre premier p.

Soit p un nombre premier. On dispose d'un entier c_p tel que $f(p) = c_p p$. Etant donné que pour p suffisemment grand, $f(p) \leqslant pf(1)$, la suite (c_p) est bornée. Donc il existe un entier c et une infinité de nombres premiers p tels que $c_p = c$.
Soit alors a un entier et p un nombre premier suffisamment grand tel que $f(p) = cp$ et p soit premier avec a. En particulier, p est premier avec $a + cp$. En substituant b par p, on trouve

$$a + cp \mid a^2 + pf(a) - a(a + cp) = p(f(a) - ca)$$

Mais comme p est premier avec $a + cp$, on déduit que $a + cp \mid f(a) - ca$. Comme cette divisibilité est vrai pour une infinité d'entiers p, on obtient que $f(a) = ca$ pour tout entier a. En remplaçant a par 1, on trouve $c = f(1)$ donc f est linéaire strictement croissante.

Solution alternative
Une façon de conclure à partir de l'inégalité $1 + f(b) \mid 1 + bf(1)$ est d'utiliser le théorème de Dirichlet : il existe une infinité d'entiers b tels que $1 + bf(1)$ est premier. Pour ces entiers b, on trouve que $1 + f(b) = 1 + bf(1)$, ce qui donne une infinité d'entiers b tels que $f(b) = bf(1)$. On peut alors conclure comme dans la solution 1.

Exercice 4.44. (IMO 2011 P5) Soit $f : \mathbb{Z} \to \mathbb{N}^\star$ une fonction. On suppose que pour tous entiers m, n, on a $f(m - n) \mid f(m) - f(n)$. Montrer que pour tous entiers m et n tels que $f(m) \leqslant f(n)$, on a $f(m) \mid f(n)$.

Solution 4.44. Si $f(m) = f(n)$, on a la divisibilité. Soient maintenant m et n des entiers tels que $f(m) < f(n)$. Comme $f(m - n) \mid f(n) - f(m)$, on a $f(m - n) \leqslant f(n) - f(m) < f(n)$. On déduit l'encadrement

$$-f(n) < -f(m - n) < f(m) - f(m - n) < f(m)f(n).$$

En appliquant l'énoncé à m et $m - n$, on a alors $f(n) \mid f(m) - f(m - n)$. On déduit de l'encadrement ci-dessus que $\boxed{f(m) = f(m - n)}$. Mais alors $f(m) = f(m - n) \mid f(m) - f(n)$ donc $\boxed{f(m) \mid f(n)}$ comme voulu.

Exercice 4.45. (IMO SL 2007 N5) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ surjectives telles que, pour tout nombre premier p et tous entiers $m, n \in \mathbb{N}^\star$, $f(m+n)$ est divisible par p si et seulement si $f(m)+f(n)$ est divisible par p.

Solution 4.45. **Réponse :** La seule solution est l'identité.

On vérifie que l'identité est bien solution. On fixe à présent f une solution du problème. Montrons que $|f(n+1) - f(n)| = 1$ pour tout entier n. On fixe $n \geqslant 1$ un entier et on considère p un éventuel diviseur premier de $f(n+1) - f(n)$.

Soit m un entier tel que $p \mid f(m+n)$. Cet entier existe par surjectivité de f : si p ne divisait aucun des nombres $f(n+1), f(n+2), \ldots$, alors il y aurait au plus n multiples de p dans l'image de f (qui sont parmi les nombres $f(1), \ldots, f(n)$), contredisant sa surjectivité. D'après l'énoncé, on a donc que

$$p \mid f(m+n) \Longrightarrow p \mid f(m)+f(n) \Longrightarrow p \mid f(m)+f(n)+(f(n+1)-f(n)) = f(m)+f(n+1) \Longrightarrow f(m+n+1).$$

On déduit par récurrence immédiate que $p \mid f(m+n+\ell)$ pour tout $\ell \geqslant 1$. Mais cela signifie que l'image de f contient au plus $m+n$ non multiples de p (qui sont parmin les nombres $f(1), f(2), \ldots, f(m+n-1)$). Cela contredit à nouveau la surjectivité de p.

Ainsi, $f(n+1) - f(n)$ n'admet pas de diviseurs premiers, donc $\boxed{|f(n+1) - f(n)| = 1}$.

Montrons à présent qu'on ne peut jamais avoir $f(n+2) = f(n)$. Soit n un entier tel que $f(n+2) = f(n)$. Pour tout entier m, le nombre $f(m+n)$ a les mêmes facteurs premiers que $f(m)+f(n) = f(m)+f(n+2)$ qui a les mêmes facteurs premiers que $f(m+n+2)$. Par récurrence immédiate, on déduit que pour tout $\ell \geqslant n+1$, le nombre $f(\ell)$ a les mêmes facteurs premiers que $f(n+1)$ ou que $f(n)$. Cela contredit encore la surjectivité de f.

En conséquence, les deux nombres $f(n+2)-f(n+1)$ et $f(n+1)-f(n)$ ne peuvent jamais être opposés, sinon on aurait $f(n+2)-f(n+1) = -(f(n+1)-f(n))$ et donc $f(n+2) = f(n)$. On a donc soit $f(n+1)-f(n) = 1$ pour tout n, soit $f(n+1)-f(n) = -1$ pour tout n.

Dans le premier cas, on déduit par récurrence que $\boxed{f(n) = n + f(1) - 1 \text{ pour tout } n}$ par récurrence immédiate. Réciproquement, si la fonction définie par $f(n) = n+c$, avec $c \geqslant 0$, est solution, alors les nombres $f(m)+f(n) = m+n+2c$ et $f(m+n) = m+n+c$ ont toujours les mêmes facteurs premiers. En choisissant m et n tels que $m+n+2c = p$ est premiers, on déduit que $p \mid m+n+c$, ce qui implique $c = 0$. La fonction identité est alors la seule solution.

Dans le second cas, on déduit que $f(n) = -n + f(1) + 1$, pour tout n, ce qui est absurde car f ne peut pas prendre de valeurs négatives.

Exercice 4.46. (IMO SL 2016 N6) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous $n, m \in \mathbb{N}^\star$, le nombre $f(m) + f(n) - mn$ est non nul et divise $mf(m) + nf(n)$.

Solution 4.46. **Réponse :** La seule fonction solution est la fonction carrée définie par $f(n) = n^2$ pour tout n.

➢ Commentaire :

> Tout comme dans l'exemple, on cherche à déterminer $f(p)$ pour tout p premier, puis, une fois qu'on a $f(p) = p^2$ pour une infinité de nombres premiers, on travaille la relation pour qu'elle soit de la forme $A(n, p) \mid f(n) - n^2$, ce qui implique que $f(n) - n^2$ admet une infinité de diviseurs.
>
> Le calcul de $f(p)$ va nous amener à nous restreindre aux nombres premiers p tels que $p \geqslant C$, avec C une certaine constante.

En posant $n = m = 1$, on trouve $2f(1) - 1 \mid 2f(1)$, donc $2f(1) - 1 \mid 2f(1) - (2f(1) - 1) = 1$, ce qui conduit à $\boxed{f(1) = 1}$.

En posant $m = 1$, la relation de divisibilité donne $1 + f(n) - n \mid 1 + nf(n)$, ce qui conduit à

$$0 \equiv 1 + nf(n) \equiv 1 + n(n-1) \mod 1 + f(n) - n,$$

ce implique que $1 + f(n) - n \leqslant 1 + n^2 - n$, ce qui conduit à $\boxed{f(n) \leqslant n^2}$.

En prenant p un nombre premier impair et $m = n = p$, la relation de divisibilité donne $2f(p) - p^2 \mid 2pf(p)$, ce qui conduit à

$$0 \equiv 2pf(p) \equiv 2p \cdot p^2 \mod 2f(p) - p^2.$$

On déduit que $2f(p) - p^2$ divise p^3. Combinée avec l'inégalité $f(p) \leqslant p^2$, on déduit que $|2f(p) - p^2| \leqslant p^2$. Il vient que

$$f(p) \in \left\{ \frac{p^2 - p}{2}, \frac{p^2 - 1}{2}, \frac{p^2 + 1}{2}, \frac{p^2 + p}{2}, p^2 \right\}.$$

Il faut donc raffiner nos estimations à partir de la divisibilité $f(p) - p + 1 \mid p^2 - p + 1$. Parmi les diverses façons de faire (qui occasionnent plus ou moins de calculs), on propose la solution de la SL. Si $f(p) \neq p^2$, alors $f(p) \geqslant \dfrac{p^2 - 1}{2}$. On a également que $f(p) - p + 1 \neq p^2 - p + 1$. Puisque ce nombre est impair, son plus grand diviseur est inférieur à son tier, on a donc

$$\frac{p^2 - 1}{2} - p + 1 \leqslant f(p) - p + 1 \leqslant \frac{1}{3}(p^2 - p + 1).$$

Cette inégalité est fausse pour tout p suffisamment grand. Donc il existe une constante $C > 0$ telle que, $\boxed{\text{pour tout } p \geqslant C \text{ premier, } f(p) = p^2}$.

Soit n un entier fixé et p un nombre premier tel que $p > f(n), C$. La divisibilité de l'énoncé donne $p^2 + f(n) - pn \mid p^3 + nf(n)$, ce qui conduit à

$$0 \equiv p^3 + n(-p^2 + pn) \equiv p(p^2 - np + n^2) \mod p^2 + f(n) - pn.$$

Comme p ne divise pas $f(n)$, p est premier avec $p + f(n) - pn$, donc $p^2 + f(n) - pn \mid p^2 - np + n^2$. On déduit par combinaison que $p^2 + f(n) - pn \mid p^2 - np + n^2 - (p^2 + f(n) - pn) = f(n) - n^2$. Le nombre $f(n) - n^2$ admet donc une infinité de diviseurs, il est donc nul, et $\boxed{f(n) = n^2}$ pour tout entier n.

Réciproquement, la fonction carrée est bien solution, en vertue de l'identité

$$m^3 + n^3 = (m + n)(m^2 + n^2 - mn) \Longrightarrow m^2 + n^2 - mn \mid m^3 + n^3.$$

Exercice 4.47. Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$xf(x) + yf(y) \mid (x^2 + y^2)^{2022}$$

pour tous $x, y \in \mathbb{N}^\star$.

Solution 4.47. **Réponse :** La seule solution est l'identité.

Il faut essayer de manipuler des p divisant le membre de droite et des p divisnat le membre de gauche. Ce sont ces derniers p qui vont nous intéresser.

Soit p un diviseur premier éventuel de 1. En prenant $x = p$, on a $p \mid pf(p) + f(1) \mid (p^2 + 1)^{2022}$, ce qui est manifestement absurde. Donc $f(1)$ n'a pas de diviseurs premiers et $\boxed{f(1) = 1}$.

En prenant $x = y = p$ un nombre premier impair, on trouve que $2pf(p) \mid 2^{2022}p^{4044}$. Supposons un instant que $2 \mid f(p)$. Alors $2 \mid 2f(2) + pf(p) \mid (2^2 + p^2)^{2022}$, ce qui est manifestement absurde. Donc 2 ne divise pas $f(p)$ et on déduit que $\boxed{f(p) \text{ est une puissance de } p}$.

Supposons que $f(p) = p^\alpha$ avec $\alpha > 1$. En prenant $x = 1$ et $y = p$, on a $1 + p^{\alpha+1} \mid (1 + p^2)^{2022}$. Mais comme $p > 2$, d'après le théorème de Zsigmondy, le nombre $p^{\alpha+1} + 1$ admet un diviseur premier ne divisant pas $1 + p^2$, ce qui est une contradiction. Donc $\alpha = 1$ et $\boxed{f(p) = p}$ pour tout nombre premier p impair.

en prenant x quelconque et p premier, on a

$$0 \equiv (x^2 + p^2)^{2022} \equiv (x^2 - xf(x))^{2022} \mod xf(x) + p^2.$$

En faisant varier p, le nombre $(x^2 - xf(x))^{2022}$ admet donc une infinité de diviseurs, il est donc nul et $\boxed{f(x) = x}$ pour tout entier $x \geqslant 1$.

Réciproquement, la fonction identité est bien solution.

Exercice 4.48. (IMO SL 2008 N5) Pour tout entier $n \in \mathbb{N}$, on pose $d(n)$ le nombre de diviseurs positifs de n. Déterminer toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que

(i) $d(f(x)) = x$ pour tout $x \in \mathbb{N}$.

(ii) $f(xy)$ divise $(x-1)y^{xy-1}f(x)$ pour tous $x, y \in \mathbb{N}$.

Solution 4.48. **Réponse :** $f(n) = \prod_{i=1}^{r} p_i^{p_i^{\alpha_i}-1}$ lorsque $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $f(1) = 1$.

Tout d'abord, on vérifie qu'une telle solution fonctionne bien.

Soit maintenant f une solution du problème. La première condition donne que $f(1) = 1$. D'autre part, la première condition donne que f est injective. Enfin, la première condition donne que $f(2)$ est un nombre premier.

En appliquant toujours la première condition à $x = p$, on déduit que $f(p)$ admet exactement p diviseurs. Au vu de la formule sur le nombre de diviseurs, cela implique que $f(p)$ est une puissance d'un nombre premier, disons $f(p) = q^{p-1}$. En posant $x = 2, y = p$ dans l'hypothèse 2, on a $f(2p) \mid p^{2p-1}f(2)$, tandis qu'en $x = p, y = 2$, on trouve $f(2p) \mid (p-1)2^{2p-1}q^{p-1}$. En particulier, si p est impair et si $q \neq p$, p est premier avec $(p-1)2^{2p-1}q^{p-1}$, donc

$$f(2p) \mid \gcd(p^{2p-1}f(2), (p-1)2^{2p-1}q^{p-1}) \mid \gcd(f(2), (p-1)2^{2p-1}q^{p-1}) \mid f(2).$$

Donc $f(2p)$ est un diviseur de $f(2)$ qui est premier. Comme $d(f(2p)) = 2p$, $f(2p) > 1$ donc $f(2p) = f(2)$ et par injectivité $p = 1$, ce qui est absurde. Donc $f(p) = p^{p-1}$ si p est impair.

On calcule désormais $f(2)$: en posant $x = 2, y = 3$ et $x = 3, y = 2$, on trouve que $f(6)$ divise $2^6 f(3) = 2^6\$cdot3^2$ et $3^5 f(2)$. Si $f(2)$ est impair, alors $f(6) \mid 3^2$. Or $f(6)$ admet 6 diviseurs. Donc $f(2)$ un nombre premier pair et $f(2) = 2$.

On prouve à présent que les seuls facteurs premiers de $f(n)$ sont des facteurs premiers de n. Notons $n = \prod p_i^{\alpha_i}$. On suppose que p_1 est le plus petit diviseur premier de n et on suppose qu'existe A divisant $f(n)$ et distinct des p_i. En posant $x = p_1$ et $y = n/p$, on trouve que $A \mid f(n) \mid (p_1 - 1)(n/p_1)^{n-1}p_1^{p_1-1}$. Donc $A \mid p_1 - 1$. Autrement dit, si $f(n) = AB$, avec d premier avec A et B ayant ses facteurs premiers parmi ceux de n, on a

$$d(A)d(B) = d(AB) = d(f(n)) = n.$$

Donc $d(A)$ divise n, mais ses éventuels facteurs premiers sont tous inférieurs à $p_1 - 1$. On déduit que $d(A) = 1$ et $A = 1$. Ceci donne le résultat annoncé.

Ceci implique directement que $f(p^\alpha)$ est une puissance de p. L'hypothèsé 1 donne alors que $p^\alpha = df(p^\alpha)) = v_p(f(p^\alpha)) + 1$, donc $f(p^\alpha) = p^{p^\alpha - 1}$.

On passe à la forme générale de $f(n)$. On écrit $n = \prod p_i^{\alpha_i}$ et $f(n) = \prod p_i^{\beta_i}$. En posant $x = p_i^{\alpha_i}$ et $y = n/x$, on a

$$p_i^{\beta_i} \mid f(n) \mid (p_i^{\alpha_i} - 1)y^{n-1}p_i^{p_i^{\alpha_i}-1}.$$

Donc $p_i^{\beta_i} \mid p_i^{p_i^{\alpha_i}-1}$ donc $\beta_i \leqslant p_i^{\alpha_i} - 1$. Mais l'hypothèsé 1 permet de saturer cette inégalité :

$$p_1^{\alpha_1} \dots p_r^{\alpha_r} \geqslant (\beta_1 + 1) \dots (\beta_r + 1) = d(f(n)) = n = \prod p_i^{\alpha_i}.$$

Ainsi $\beta_i = p_i^{\alpha_i}$, ce qui conclut.

Exercice 4.49. (IMO SL 2020 N5) Trouver les fonctions $f\colon \mathbb{N}^\star \to \mathbb{N}$ vérifiant les deux conditions suivantes :

1. $f(xy) = f(x) + f(y)$ pour tous les entiers $x \geqslant 1$ et $y \geqslant 1$;
2. il existe une infinité d'entiers $n \geqslant 1$ tels que l'égalité $f(k) = f(n-k)$ est vraie pour tout entier k tel que $1 \leqslant k \leqslant n-1$.

Solution 4.49. **Réponse :** Les fonctions recherchées sont les fonctions de la forme $f\colon n \mapsto cv_p(n)$, où c est un entier naturel, p est un nombre premier, et $v_p(n)$ et la valuation p-adique de n. Tout d'abord, il est clair que ces fonctions sont bien solutions du problème.

Réciproquement, soit f une solution non nulle du problème. On dit qu'un entier n est *joli* si l'égalité $f(k) = f(n-k)$ est vraie pour tout entier $k \leqslant 1$. Remarquons que tout diviseur d'un joli entier est joli. En effet, si d divise un joli entier $n = ad$, alors

$$f(k) = f(ak) - f(a) = f(n-ak) - f(a) = f(a(d-k)) - f(a) = f(d-k)$$

pour tout entier $k \leqslant d-1$.

En outre, la condition 1 signifie que $f\left(\prod_i p_i^{\alpha_i}\right) = \sum_i \alpha_i f(p_i)$ pour toute décomposition en produit de facteurs premiers. Il s'agit donc de démontrer qu'il existe au plus un nombre premier p pour lequel $f(p) > 0$. On considère alors le plus petit entier p tel que $f(p) > 0$. La formule ci-dessus indique que p est premier, et on pose $c = f(p)$. S'il existe un joli entier $n \geqslant p$ que p ne divise pas, posons $n = pq + r$, avec q entier et $1 \leqslant r \leqslant p-1$. Puisque n est joli, on sait que $f(r) = f(n-pq) = f(pq) \geqslant f(p) > 0$, en contradiction avec la définition de p. Ainsi, tout entier joli est de la forme ap^b avec b entier et $1 \leqslant a \leqslant p-1$. Réciproquement, puisqu'il existe une infinité d'entiers jolis et que a ne peut prendre qu'un nombre fini de valeurs, toute puissance de p divise un joli entier, et est donc elle-même jolie.

Par conséquent, pour tout nombre premier q distinct de p, l'entier p^{q-1} est joli. Puisque q divise $p^{q-1}-1$, on en déduit en particulier que $0 = f(1) = f(p^{q-1}-1) \geqslant f(q)$, ce qui conclut.

Solution alternative

Une fois acquis le fait que tout entier joli est de la forme ap^b, avec b entier et $1 \leqslant a \leqslant p-1$, et que tout diviseur d'un entier joli est joli, on peut aussi procéder comme suit.

Supposons qu'il existe un nombre premier $q \neq p$ pour lequel $f(q) > 0$, et soit q le plus petit tel nombre premier. On considère alors le plus petit entier joli $n > q$, puis on écrit n sous la forme $n = ap^b = uq + v$, avec u entier et $0 \leqslant v \leqslant q-1$.

Puisque $n > q > p$, on sait que $b \geqslant 1$, donc que p divise n, et comme q ne divise pas n, on sait que $v \geqslant 1$. Dans ces conditions, $f(v) = f(uq) > 0$, et la minimalité de q indique que p divise v. Mais alors p divise aussi $uq = n-v$, et p est premier avec q, donc p divise u. On en déduit que $n > pq$, donc que le joli entier n/p satisfait lui aussi l'inégalité $n/p > q$, en contradiction avec la minimalité de n. Notre supposition est ainsi invalide, ce qui conclut.

Exercice 4.50. (IMO 2010 P3) Déterminer toutes les fonctions $g : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que le nombre

$$(g(m) + n)(g(n) + m)$$

est un carré parfait pour toute paire (m, n) d'entiers strictement positifs.

Solution 4.50. **Réponse :** les fonction solutions sont toutes les fonctions de la forme $f(n) = n + c$ pour tout entier n, avec $c \geqslant 0$ un entier.

➢ **Commentaire :**

> On essaye la méthode de l'exemple, qui consiste à montrer que $|f(k+1) - f(k)| = 1$, en supposant par l'absurde que $f(k+1) - f(k)$ admet un facteur premier p.
>
> La première chose pour se débloquer, c'est de ne pas chercher à poser $(n, m) = (k, k+1)$ dans l'équation, mais plutôt à poser successivement $(n, m) = (k, m)$ et $(n, m) = (k+1, m)$, avec un m à bien construire pour faire sortir les propriétés sur $g(k)$ et $g(k+1)$.
>
> Plus concrètement, avec ces substitutions, $(g(k) + m)(g(m) + k)$ et $(g(k+1) + m)(g(m) + k + 1)$. Si on construit m tel que $v_p(g(k+1) + m)$ et $v_p(g(k) + m)$ sont impaires, cela implique que $v_p(g(m) + k)$ et $v_p(g(m) + k + 1)$ sont également impairs, donc p divise les deux nombres $g(m) + k$ et $g(m) + k + 1$, ce qui est absurde car ils sont consécutifs. Il s'agit alors de construire un tel entier m.
>
> Pour une telle construction, on peut aller au plus simple et chercher m tel que $m + g(n) = p^\ell$, et établir un cahier des charges sur ℓ.

Commençons par montrer que $|g(k+1) - g(k)| = 1$ pour tout entier k. Soit $k \geqslant 1$. Supposons par l'absurde que ce n'est pas le cas et prenons p un diviseur premier de $g(k+1) - g(k)$. Montrons qu'il existe un entier m tel que $v_p(g(k) + m)$ et $v_p(g(k+1) + m)$ sont impairs.

Si $g(k+1) = g(k)$, il suffit de prendre $m = p^{2\ell+1} - g(k)$, où ℓ est assez grand pour que $p^{2\ell+1} > g(k)$. Sinon, on écrit $g(k+1) - g(k) = p^\ell A$, avec $\ell \geqslant 1$ et A est premier avec p. On distingue alors deux cas :

- ➢ Si ℓ est impair : prenons r un entier suffisamment grand pour que $p^{\ell+2r} \geqslant g(k)$. On pose alors $m = p^{\ell+2r} - g(k)$. On vérifie alors que $m + g(k+1) = p^{\ell+2r} + p^\ell A = p^\ell(p^{2r} + A)$, si bien que $v_p(m + g(k)) = \ell + 2r$ et $v_p(m + g(k+1)) = \ell$ sont impairs.
- ➢ Si ℓ est pair : prenons $r \geqslant \ell$ un entier suffisamment grand pour que $p^{\ell-1} + p^r \geqslant g(k)$. On pose alors $m = p^{\ell-1} + p^r - g(k)$. On vérifie alors que $m + g(k+1) = p^{\ell-1} + p^r + p^\ell A = p^{\ell-1}(1 + pA + p^{r-\ell+1})$, si bien que $v_p(m + g(k)) = v_p(m + g(k+1)) = \ell - 1$ qui est bien impair.

Une fois cet entier m construit, revenons à l'équation. D'après l'énoncé, puisque le nombre $(m + g(k))(k + g(m))$ est un carré parfait, sa valuation $p-$adique est paire. Comme $v_p(m + g(k))$ est impair, on déduit que $v_p(k + g(m))$ est également impair et en particulier, $p \mid k + g(m)$. De la même manière, $p \mid k + 1 + g(m)$. Mais alors $p \mid k + 1 + g(m) - (k + g(m)) = 1$, ce qui est absurde.

On déduit que $g(k+1) - g(k)$ n'a pas de diviseur premier, ce qui implique que $|g(k+1) - g(k)| = 1$.

Remarquons ensuite qu'on ne peut pas avoir $g(n) = g(n+2)$: En effet, si c'était le cas, en posant $a = g(n)$, on aurait que le nombre $(g(n) + n + 2)(g(n+2) + n) = (a + n)(a + n + 2)$ est un carré parfait. Or, on a l'encadrement $(a+n)^2 < (a+n)(a+n+2) < (a+n+1)^2$. On déduit que $\boxed{g(n) \neq g(n+2) \text{ pour tout entier } n}$.

En conséquence, les deux nombres $g(n+2) - g(n+1)$ et $g(n+1) - g(n)$ ne peuvent jamais être opposés, sinon on aurait $g(n+2) - g(n+1) = -(g(n+1) - g(n))$ et donc $g(n+2) = g(n)$. On a donc soit $g(n+1) - g(n) = 1$ pour tout n, soit $g(n+1) - g(n) = -1$ pour tout n.

Dans le premier cas, on déduit par récurrence que $\boxed{g(n) = n + g(1) - 1 \text{ pour tout } n}$ par récurrence immédiate. Réciproquement, la fonction définie par $g(n) = n + c$, avec $c \geqslant 0$, est bien solution.

Dans le second cas, on déduit que $g(n) = -n + g(1) + 1$, pour tout n, ce qui est absurde car g ne peut pas prendre de valeurs négatives.

Ceci conclut que les fonction annoncées sont les seules solutions.

Solution alternative

Une variation de la solution précédente est la suivante.

➢ **Commentaire :**

Une motivation de la solution qui suit survient lorsqu'on cherche, par exemple, à prouver l'injectivité de g. La solution précédente donne un aperçu des calculs possibles pour montrer que $g(n+2) \neq g(n)$. Supposons que l'on a $g(u) = g(v) = a$ pour un certain couple (u, v) avec $u < v$. En prenant $(n, m) = (u, v)$ dans l'équation, le nombre $(a+u)(a+v)$ est donc un carré parfait. On a alors l'encadrement

$$(a+u)^2 < (a+u)(a+v) = (a+u)^2 + (v-u)(a+u) < \left(a + \frac{v-u}{2}\right).$$

Cet encadrement n'est pas satisfaisant, car il ne limite pas assez les valeurs possibles pour $v-u$.

L'idée, audacieuse, est alors de montrer l'injectivité modulo p pour tout p : si $g(n) \equiv g(m) \mod p$, alors $n \equiv m \mod p$. Ceci entraîne l'injectivité et l'égalité $|g(k+1) - g(k)| = 1$. La preuve de l'injectivité modulo p est similaire à la construction de m de la solution 1.

Il faut avoir conscience que se convaincre de chercher une telle propriété fait partie de la difficulté du problème, et les problèmes difficiles d'Olympiades Internationales nécessitent souvent de s'intéresser à des résultats de ce type. C'est une expérience batîe sur une grande banque de problèmes qui permet de comprendre quels résultats on peut raisonnablement attendre.

Montrons le lemme suivant :

Lemme 2. *Soient k et n deux entiers tels que $g(k) \equiv g(n) \mod p$. Alors $k \equiv n \mod p$.*

Démonstration. Montrons qu'il existe un entier m tel que $v_p(g(k)+m)$ et $v_p(g(n)+m)$ sont impairs. Si $g(k) = g(n)$, il suffit de prendre $m = p^{2\ell+1} - g(k)$, où ℓ est assez grand pour que $p^{2\ell+1} > g(k)$. Sinon, on écrit $g(n) - g(k) = p^\ell A$, avec $\ell \geqslant 1$ et A est premier avec p. On distingue alors deux cas :

- ➢ Si ℓ est impair : prenons r un entier suffisamment grand pour que $p^{\ell+2r} \geqslant g(k)$. On pose alors $m = p^{\ell+2r} - g(k)$. On vérifie alors que $m + g(n) = p^{\ell+2r} + p^\ell A = p^\ell(p^{2r} + A)$, si bien que $v_p(m+g(k)) = \ell + 2r$ et $v_p(m+g(n)) = \ell$ sont impairs.
- ➢ Si ℓ est pair : prenons $r \geqslant \ell$ un entier suffisamment grand pour que $p^{\ell-1} + p^r \geqslant g(k)$. On pose alors $m = p^{\ell-1} + p^r - g(k)$. On vérifie alors que $m + g(n) = p^{\ell-1} + p^r + p^\ell A = p^{\ell-1}(1 + pA + p^{r-\ell+1})$, si bien que $v_p(m+g(k)) = v_p(m+g(n)) = \ell - 1$ qui est bien impair.

Une fois cet entier m construit, revenons à l'équation. D'après l'énoncé, puisque le nombre $(m+g(k))(k+g(m))$ est un carré parfait, sa valuation $p-$adique est paire. Comme $v_p(m+g(k))$ est impair, on déduit que $v_p(k+g(m))$ est également impair et en particulier, $p \mid k + g(m)$. De la même manière, $p \mid n + g(m)$. Mais alors p divise $k + g(m) - (n + g(m)) = k - n$, comme annoncé. □

Montrons à présent l'injectivité de g. Soient u et v des entiers tels que $g(u) = g(v)$. Alors, pour tout nombre premier, $p \mid g(u) - g(v)$ dont $p \mid u - v$. Donc $u - v$ admet une infinité de diviseurs et est donc nul. Ainsi, $\boxed{g \text{ est injective}}$.

D'autre part, on a $|g(n+1) - g(n)| = 1$ pour tout n. En effet, par injectivité, $|g(n+1) - g(n)| \geqslant 1$, et si p divise $g(n+1) - g(n)$, le lemme impliquerait que $p \mid 1$, ce qui est absurde. On a donc bien l'égalité annoncée.

L'injectivité et l'égalité $|g(n+1) - g(n)| = 1$ permettent de conclure comme dans la solution précédente.

Exercice 4.51. (IMO 2025 P3) Une fonction $f : \mathbb{N}^\star \to \mathbb{N}^\star$ est dite *australienne* si

$$f(a) \mid b^a - f(b)^{f(a)}$$

pour tous entiers strictement positifs a et b.
Déterminer le plus petit réel $c > 0$ tel que $f(n) \leqslant cn$ pour toute fonction australienne et tout entier $n \geqslant 1$.

Solution 4.51. **Réponse :** Le plus petit réel est $c = 4$.

➢ Commentaire :

> L'énoncé doit éveiller deux choses : d'abord, on peut s'attendre à ce qu'on ne puisse pas caractériser toutes les fonctions vérifiant la divisibilité. Il y aura probablement des entiers n pour lesquels on ne pourra rien dire de $f(n)$. Il faut donc se focaliser sur les entiers n sur lesquels on peut espérer récupérer de l'information. La deuxième chose, c'est qu'il faudra probablement construire des fonctions "inhabituelles" solutions de la divisibilité et qui permettront de réaliser la borne ou de l'approcher. Ce style d'équation fonctionnelle est récent mais à la mode (on pourra notamment voir les A7 2019, A6 2022 et A2 2023), il convient de développer des stratégies.

Soit f une fonction vérifiant la propriété (auquel cas on a alors $f(n) \leqslant 4n$)) mais telle que f n'est pas l'identité. Il existe donc un entier x tel que $f(x) \neq x$.
En posant $a = b$ dans la relation, on trouve $f(a) \mid a^a - f(a)^{f(a)}$, donc $f(a) \mid a^a$. En particulier, si p est un nombre premier, on déduit que $\boxed{f(p) \text{ est une puissance de } p}$.

Pour tout p tel que $v_p(f(p)) \geqslant 1$, en posant $a = p$ et $b = x$ dans la relation de l'énoncé, on trouve avec le petit théorème de Fermat :

$$0 \equiv x^p - f(x)^{f(p)} = x^p - f(x)^{p^{v_p(f(p))}} \equiv x - f(x) \mod p.$$

Comme $x - f(x)$ est non nul, il admet un nombre fini de diviseurs premiers. on déduit qu'il existe un nombre fini de nombre premiers p tels que $v_p(f(p)) \geqslant 1$. Autrement dit, il existe $M \geqslant 1$ tel que $\boxed{\text{pour tout } p \geqslant M,\ f(p) = 1}$.

Soit p un nombre premier impair et $q \geqslant M$ un nombre premier. En posant $(a, b) = (p, q)$ dans la relation, on trouve que $f(p) \mid q^p - f(q)^{f(p)} = q^p - 1$. Si $v_p(f(p)) \geqslant 1$, alors d'après le petit théorème de Fermat, on aurait $0 \equiv q^p - 1 \equiv q - 1 \mod p$, soit $p \mid q - 1$. Or, d'après le théorème de Dirichlet, il existe une infinité de nombres premiers q tels que $q \equiv -1 \mod p$. Comme p est impair, les deux congruences $q \equiv 1$ et $q \equiv -1$ sont incompatibles. Cette contradiction implique que $\boxed{f(p) = 1 \text{ pour tout } p \text{ premier impair}}$.

Soit n un entier quelconque. Si p est un diviseur premier de $f(n)$, alors $p \mid f(n) \mid n^n$, dont p divise n. En remplaçant $(a, b) = (n, p)$ dans la relation, on trouve $p \mid f(n) \mid p^n - f(p)^{f(n)}$. Dès que p est impair, cela implique que $p \mid p^n - 1$, ce qui est absurde. Ainsi, $f(n)$ n'admet aucun facteur impair, il s'agit d'une puissance de 2. En particulier, puisque $f(n) \mid n^n$, on déduit que $\boxed{f(n) = 1 \text{ pour tout } n \text{ impair}}$.

➢ Commentaire :

> Lorsque $n = 2^\alpha\beta$ et $f(n) = 2^\gamma$, la dernière étape est d'estimer γ en fonction de α. En posant $a = n$ dans la relation, on trouve $2^\gamma \mid b^{2^\alpha\beta} - 1$. Il reste à choisir b pour que $v_2(b^{2^\alpha\beta} - 1)$ soit petit.

Soit $n = 2^\alpha\beta$ un entier pair. Soit γ un entier tel que $f(n) = 2^\gamma$. En prenant $(a, b) = (n, 3)$, on trouve

$$2^\gamma = f(n) \mid 3^n - f(3)^{f(n)} = 3^{2^\alpha\beta} - 1.$$

D'après le lemme LTE,

$$v_2(3^{2^\alpha\beta} - 1) = v_2(3 + 1) + v_2(3 - 1) + v_2(2^\alpha\beta) - 1 = 2 + \alpha \quad \Longrightarrow \quad \gamma \leqslant \alpha + 2.$$

On déduit que, pour tout entier n pair, $f(n) \leqslant 2^{v_2(n)+2} \leqslant 4n$. En particulier, en combinant les valeurs de f sur les entiers impairs et sur les entiers impairs, on déduit que $\boxed{f(n) \leqslant 4n}$ pour tout entier n. Comme en plus la fonction identité, que l'on avait exclue de notre raisonnement, vérifie également l'inégalité, on trouve que $\boxed{c \leqslant 4}$.

Trouvons désormais f australienne telle que, pour au moins un entier n, $f(n) = 4n$. Ceci montrera que $c \geqslant 4$ et donc que $c = 4$. Beaucoup de construction sont possibles, présentons la suivante : soit f définie par

$$f(n) = \begin{cases} 1 & \text{si } n \text{ est impair} \\ 16 & \text{si } n = 4 \\ 2 & \text{sinon} \end{cases}$$

Vérifions que f est autralienne :

- ➢ Si a est impair, $f(a) = 1$ donc la divisibilité est vérifiée pour tout b.
- ➢ Si $a = 4$, alors pour tout b pair, on a $2 \mid b$ et $2 \mid f(b)$, donc $16 \mid b^4 - f(b)^{16}$. Lorsque b est impair, on peut vérifier à la main que $b^4 \equiv 1 \mod 16$, de sorte que $16 \mid b^4 - f(b)^{16}$.
- ➢ Si $a \neq 4$ est pair, les nombres b^a et $f(b)^{f(a)}$ étant toujours de même parité, on a toujours $f(a) = 2 \mid b^a - f(b)^{f(a)}$.

f est donc australienne, ce qui conclut le problème.

Exercice 4.52. (EMC 2021 P3 senior) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$x^2 - y^2 + 2y(f(x) + f(y))$$

est un carré parfait pour tous $x, y > 0$.

Solution 4.52. Soit f une solution. Pour $x = y = p$ un nombre premier, on voit que $4pf(p)$ est un carré pour tout p, donc $pf(p)$ est un carré pour tout p et $p \mid f(p)$.

On déduit en posant $x = p$ dans l'hypothèse que $-y^2 + 2yf(y)$ est un carré modulo p, et ce pour tout p. Ceci implique que $-y^2 + 2yf(y)$ est un carré parfait. On pose c_y l'entier tel que $c_y^2 = -y^2 + 2yf(y)$. En réinjectant dans l'hypothèse et en prenant $x = 1$, on a

$$1 + 2yf(1) + c_y^2$$

qui est un carré parfait strictement plus grand que c_y^2. Ainsi, $1 + 2yf(1) + c_y^2 \geqslant (c_y + 1)$, soit $yf(1) \geqslant c_y$, ce qui donne $y^2 f(1)^2 \geqslant c_y^2$, et finalement

$$f(y) \leqslant \frac{f(1)^2 + 1}{2} y.$$

Ainsi, $\dfrac{f(p)}{p}$ ne peut prendre qu'une nombre fini de valeurs, comprises entre 1 et $\dfrac{f(1)^2+1}{2}$. Le principe des tiroirs infini, il existe donc un entier a et une infinité de nombres premierrs p tels que $f(p) = ap$.

On remplace x par un tel p dans l'hypothèse et on trouve que

$$p^2 - y^2 + 2yap + 2yf(y) = (p + ya)^2 - y^2 - y^2a^2 + 2yf(y)$$

est un carré pour tout nombre premier p. En posant $D = -y^2 - y^2a^2 + 2yf(y)$, on trouve que $(p + ya)^2 - D$ est un carré pour une infinité de p, ce qui implique (puisque la différence entre deux carrés consécutifs est plus grand que D à partir d'un certain rang) que $D = 0$. Donc $f(y) = \dfrac{a^2+1}{2} y$. En remplaçant y par p, on trouve que $a = 1$. Ainsi, $f(y) = y$ pour tout y, et c'est bien une solution de l'équation.

Exercice 4.53. (SL ELMO 2014 N8) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que :

(i) les entiers $f(1), f(2), \ldots$ sont premiers entre dans leur ensemble,

(ii) il existe un entier $N \geqslant 1$ tel que pour tout $n \geq N$, $f(n) \neq 1$ et pour tous $a, b \in \mathbb{N}^\star$,

$$f(a)^n \mid f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}.$$

Solution 4.53. **Réponse :** La seule solution est la fonction identité.

Soit f une solution. Comme les valeurs de f sont premières entre elles dans leur ensemble, si f est constante, elle égale 1, ce qui est exclu.

Avec $a = 1$, on voit que $f(1)^n | f(b+1) - f(b)$ pour tout $b \geq 1$ et tout n assez grand. Comme f est non constante, il existe b tel que $f(b+1) \neq f(b)$. Il s'ensuit que $\boxed{f(1) = 1}$.

Soit $a \geqslant 2$. Il existe un $t \geqslant 0$ tel que $f(1 + (t+1)a) \neq f(1+ta)$ (car, pour t assez grand, $f(1+ta) \neq 1 = f(1)$). On prend alors $b = 1 + ta$. Pour tout $n \geqslant 1$ assez grand, $f(a)^n | f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$.

Soit p un nombre premier divisant $f(a)$. Alors il existe un $l \geq 1$ tel que $p | f(a+b)^{a^l} - f(b)^{a^l}$. Pour $n > l$, par LTE, la valuation p-adique de $f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$ est $v_p(a^{n-1-l}) + C$ pour une certaine constante C qui ne dépend que de f, a, b, l (mais pas de n).

Donc pour $n > \ell$ assez grand, $v_p(a^{n-1-\ell}) + C \geqslant v_p(f(a)^n)$, donc $(n-1-\ell)v_p(a) + C \geqslant n v_p(f(a))$, d'où $v_p(f(a)) \leqslant v_p(a)$.

Par conséquent, pour tout $a \geqslant 1$, $\boxed{f(a) | a}$.

En particulier, si p est premier, $f(p)$ vaut 1 ou p, et est égal à p sauf pour un nombre fini de nombres premiers.

Soit p un nombre premier tel que $f(p) = p$: pour tout $b \geqslant 1$ et tout n assez grand, $p^n | f(p+b)^{p^{n-1}} - f(b)^{p^{n-1}}$.

En particulier, $\boxed{f(p+b) \equiv f(b) \mod p}$: ainsi, la classe de congruence de $f(b)$ modulo p ne dépend que de b modulo p.

On va montrer que f est l'identité. Soit $u \geqslant 2$, soit P l'ensemble fini des nombres premiers p tels que $p \leq u$ ou $f(p) = 1$. Supposons qu'il existe un nombre premier $q \notin P$ et un entier n tels que $q | n - u$ et $f(n) = n$.

Alors $q | f(n) - f(u)$, et donc $q | n - f(u)$, d'où $q | u - f(u)$. Comme $0 \leq u - f(u) \leq u < q$, on en déduit que $\boxed{f(u) = u}$.

On propose deux méthodes, de la plus élémentaire à la moins élémentaire, d'exhiber un tel couple (q, n).

Première méthode (complètement élémentaire) :

Soit Π le produit des nombres premiers de P, et soit $N \geqslant 1$ tel que pour tout $p \in P$, p^N ne divise pas $u - 1$.

Supposons que $n > \Pi^N + u$ soit congru à 1 modulo Π^N et tel que $f(n) = n$. Alors, si $p \in P$, $v_p(n-u) < N$, et $n - u > \Pi^N$, de sorte que $n - u$ possède un diviseur premier $q \notin P$, et on a gagné.

Soit n un produit de nombres premiers deux à deux distincts, tous hors de P. Alors, si $p | n$ est un diviseur premier, $n \equiv p[p]$ et $f(p) = p$, donc $p | f(n) - f(p)$, d'où $p | f(n)$. Comme $f(n) | n$, on en déduit que $f(n) = n$.

Comme il existe une infinité de nombres premiers, il existe une progression arithmétique C de raison Π^N et de premier terme premier à Π et contenant une infinité de nombres premiers. En prenant pour n le produit de $\varphi(\Pi^N)$ premiers $q \in C$ tels que $q > \Pi^N + u$, n convient.

Deuxième méthode :

Soit $q \notin P$ premier : alors $f(q) = q$. D'après le théorème de Dirichlet, il existe un nombre premier $p > u + q$ congru à u modulo q tel que $f(p) = p$. Alors le couple (q, p) convient.

Ainsi, l'identité est la seule solution potentielle. Réciproquement, l'identité vérifie la première condition et si $a, b \geq 1$ et $n \geq 2$, alors par LTE, pour tout nombre premier $p | a$, $v_p((a+b)^{a^{n-1}} - b^{a^{n-1}}) \geq v_p(a) + v_p(a^{n-1}) = v_p(a^n)$, donc $a^n | (a+b)^{a^{n-1}} - b^{a^{n-1}}$, et donc l'identité est solution.

4.3 Théorie des nombres combinatoire

Exercice 4.54. (OFM 2025 junior) Charlotte écrit au tableau les entiers $1, \dots, 2025$. Charlotte dispose de deux opérations, l'opération *PGCD* et l'opération *PPCM*. L'opération *PGCD* consiste à choisir deux entiers a et b écrits au tableau, à les effacer et à écrire l'entier $\mathrm{PGCD}(a, b)$. L'opération *PPCM* consiste à choisir deux entiers a et b écrits au tableau, à les effacer et à écrire l'entier $\mathrm{PPCM}(a, b)$. Un entier N est dit *gagnant* s'il existe une suite d'opérations à l'issue desquelles le seul entier encore écrit au tableau est l'entier N.

Déterminer tous les entiers gagnants parmi $\{1, \dots, 2025\}$ et donner, pour chacun d'eux, le nombre minimum d'opérations *PGCD* que Charlotte doit utiliser.

Solution 4.54. Montrons que, quel que soit l'entier $N \in \{1, \dots, 2025\}$, Charlotte peut se débrouiller pour que le dernier entier écrit au tableau soit l'entier N et, ce en utilisant au minimum une opération *PGCD*.

Notons $(i, j) \to \mathrm{PGCD}(i, j)$ le fait de remplacer i et j par leur pgcd et $(i, j) \to \mathrm{PPCM}(i, j)$ celle de les remplacer par leur PPCM.

Notons qu'à chaque opération, le nombre d'entiers écrits au tableau diminue d'exactement 1, si bien qu'au bout de 2024 opérations, il ne reste plus qu'un seul entier. Pour tout entier N, Charlotte peut effectuer la suite d'actions suivantes : tant qu'elle le peut, Charlotte choisit deux entiers a et b distincts de 1 et N et effectue l'opération $(a, b) \to \mathrm{PPCM}(a, b)$. Lorsqu'elle ne peut plus effectuer cette opération, cela signifie qu'il reste au tableau uniquement les entiers $1, N$ et un certain entier a. Charlotte effectue alors $(1, a) \to \mathrm{PGCD}(1, a) = 1$ et $(1, N) \to \mathrm{PPCM}(1, N) = N$.

D'autre part, étant donné que $\mathrm{PPCM}(a, b, c) = \mathrm{PPCM}(a, \mathrm{PPCM}(b, c))$ pour tous a, b, c, si Charlotte n'utilise que l'action PPCM, le dernier nombre écrit au tableau sera $\mathrm{PPCM}(1, 2, \dots, 2025)$ qui vérifie

$$\mathrm{PPCM}(1, 2, \dots, 2025) \geqslant 2025 \times 2024 > N.$$

Ainsi, Charlotte doit utiliser au moins une fois l'action PGCD.

Exercice 4.55. (All Russia 2025) Soit $n \geqslant 1$ un entier. On écrit les nombres $1, 2, \dots, n$ en ligne dans un certain ordre. Pour toute paire de nombres adjacents, on calcule leur PGCD. Quel est le plus grand nombre de valeurs distinctes que l'on peut obtenir avec ces $n - 1$ valeurs ?

Solution 4.55. **Réponse :** Au plus $\lfloor \frac{n}{2} \rfloor$.

Analyse :

Le PGCD de deux nombres adjacents a et b divise chacun des deux nombres. Si disons $a < b$, alors on déduit que $\boxed{\mathrm{PGCD}(a, b) \leqslant b/2 \leqslant n/2}$. Cela signifie que les valeurs obtenues dans l'exercices sont dans l'intervalle $[\![1, \lfloor n/2 \rfloor]\!]$. Il y en a donc au plus $\lfloor n/2 \rfloor$ distinctes.

Construction : On répartit les entiers par paires de la forme $(x, 2x)$ avec $x \in [\![1, \lfloor n/2 \rfloor]\!]$, en rajoutant éventuellement le singleton $\{n\}$ si n est impaire. En mettant les paires bout à bout sur la droite, et puisque $\mathrm{PGCD}(x, 2x) = x$, on obtient bien au moins $\lfloor n/2 \rfloor$ valeurs distinctes.

Exercice 4.56. (IZhO 2025 P4) Au tableau, il y a 999 entiers consécutifs. Pour tout $i \in \{2, 3, \dots 1000\}$, Alice écrit sur un papier la phrase "ce nombre n'est pas divisible par i". Elle place ensuite les papiers sous les entiers écrits, de sorte qu'en dessous de chaque entier se trouve exactement un papier. Alice gagne un point chaque fois que l'information d'un papier est correcte. Combien de points, au maximum, Alice peut-elle s'assurer de gagner, quels que soient les 999 entiers consécutifs inscrits ?

Solution 4.56. **Réponse :** Alice peut s'assurer d'avoir 998 points, mais pas plus.

On montre par récurrence sur n le résultat plus général suivant : étant donné n entiers consécutifs et n étiquettes "ce nombre est divisible par i" pour $i \in \{2, 3, \dots, n + 1\}$, Alice peut s'assurer d'avoir $n - 1$ points.

Si $n = 1$, il n'y a rien à faire donc on se concentre sur l'hérédité. On suppose que la propriété est vraie pour un $n \geqslant 1$ fixé. Notons $a, a + 1, \dots, a + n$ les $n + 1$ entiers consécutifs présentés à Alice. Parmi les entiers a et $a + n$, l'un d'entre eux n'est pas divisible par $n + 1$, donc Alice peut placer l'étiquette "n'est pas divisible par $n + 1$" sur celui-ci et remporter un point. Par hypothèse de récurrence, avec les n entiers (consécutifs donc) restants et les n étiquettes restantes, Alice peut remporter au moins $n - 1$ points, ce qui achève l'hérédité.

En particulier, Alice peut s'assurer d'avoir au plus 998 points.

D'autre part, si les entiers écrits sont $n!, n!+1, \ldots, n!+(n-1)$, quelle que soit l'étiquette placée sour l'entier $n!$, elle ne rapportera pas de points à Alice. Donc Alice ne peut pas s'assurer d'avoir 999 points. La combinaison des deux raisonnements donne la borne voulue.

Exercice 4.57. (JBMO SL 2024 C1, Israël MO 2021) Déterminer le plus petit entier strictement positif k vérifiant la propriété suivante : pour tout sous-ensemble S de $\{1, \ldots, 2024\}$ de taille k, il existe deux entiers distincts $a, b \in S$ tels que $ab+1$ est un carré parfait.

Solution 4.57. **Réponse :** $k = 1013$.

➢ Commentaire :

> Une façon simple de former un carré avec la conidition est de tirer parti de l'identité $n(n+2)+1 = (n+1)^2$. Cette identité nous dit que si S contient les entiers n et $n+2$ (pour un certain entier n, alors S vérifie la condition de l'énoncé. On cherche alors un entier k suffisamment grand pour que tout ensemble S de taille contienne nécessairement deux entiers dont la différence vaut 2. Cela nous guide également pour construire un ensemble S ne vérifiant pas la propriété.

Analyse :

Montrons que tout sous-ensemble S de $\{1, \ldots, 2024\}$ de taille 1013 possède deux éléments a et b tels que $ab+1$ est un carré parfait.

Pour $0 \leqslant k \leqslant 505$, considérons les paires de la forme $(4k, 4k+2)$, $(4k+1, 4k+3)$, qui constituent une partition de $\{1, \ldots, 2024\}$ en 1012 paires disjointes de la forme $(n, n+2)$. D'après le principe des tiroirs, l'une de ces paires est incluse dans l'ensemble S. Autrement dit, il existe un entier $n \leqslant 2022$ tel que n et $n+2$ sont dans S. Alors $n(n+2)+1 = (n+1)^2$ est bien un carré parfait.

Construction :

Construisons un ensemble S de taille 1012 ne vérifiant pas la condition de l'énoncé. L'argument précédent nous indique que S ne peut pas contenir deux entiers dont la différence vaut 2, mais cela n'est pas suffisant. Une façon de s'assurer qu'aucun nombre de la forme $ab+1$ est un carré parfait est de construire un ensemble S tel que les nombres de la forme $ab+1$ avec a et b dans S ne sont jamais congrus à 0 ou à 1 modulo 4.

Soit S l'ensemble composé de tous les nombres de $\{1, \ldots, 2024\}$ qui sont congrus à 1 ou à 2 modulo 4. S est bien de taille 1012. Soient a et b deux éléments quelconques de S.

- Si $a \equiv b \equiv 1 \mod 4$, alors $ab+1 \equiv 2 \mod 4$, ce ne peut donc pas être un carré parfait, car les carrés parfaits sont congurs à 0 ou à 1 modulo 4.
- Si $a \equiv 1 \mod 4$ et $b \equiv 2 \mod 4$, alors $ab+1 \equiv 3 \mod 4$, ce ne peut donc pas être un carré parfait non plus.
- Si $a \equiv 2$ et $b \equiv 2 \mod 4$, alors on dispose des deux entiers k et k' tels que $a = 4k+2$ et $b = 4k'+2$. Alors

$$ab+1 = (4k+2)(4k'+2)+1 = 16kk' + 8(k+k') + 5 \equiv 5 \mod 8,$$

ce qui l'empêche d'être un carré parfait puisque les carrés sont congrus à $0, 1$ ou 4 modulo 8.

Dans tous les cas $ab+1$ n'est jamais un carré parfait, donc S ne vérifie pas les conditions de l'énoncé.

Exercice 4.58. (BMO 2019 N2) Soit $n \geqslant 1$ un entier et soit $S \subset \{1, \ldots, n\}$ un ensemble. On note s le PGCD des éléments de S. On suppose que $s \neq 1$ et on note d son plus petit diviseur strict. Soit $T \subset \{1, \ldots, n\}$ un ensemble tel que $S \subset T$ et $|T| \geqslant 1 + \left\lfloor \frac{n}{d} \right\rfloor$. Montrer que le plus grand commun diviseur des éléments de T est 1.

Solution 4.58. Soit p un éventuel diviseur du PGCD des éléments de T. Comme $\{1, \ldots, n\}$ contient $\lfloor n/p \rfloor$ multiples de p, et que T est contenu dans l'ensemble de ces multiples, on a

$$\left\lfloor \frac{n}{p} \right\rfloor \geqslant |T| \geqslant 1 + \left\lfloor \frac{n}{d} \right\rfloor \quad \Longrightarrow p < d.$$

D'autre part, p divise tous les éléments de S, donc p divise s, ce qui conduit à $p \geqslant d$. Ces deux inégalités mises bout à bout donnent une contradiction donc le PGCD des éléments de T vaut 1.

Exercice 4.59. (Hong-Kong TST 2016 Test 2 P4) Alice et Bob jouent au jeu suivant :

1. Alice commence par écrire sur une ligne 2015 nombres premiers dans l'ordre croissant. Son score correspond au produit de ces nombres premiers.
2. Bob écrit un entier strictement positif.
3. Alice dessine une barre verticale entre deux nombres premiers adjacents et calcule le produit de tous les nombres premiers à gauche de la barre verticale.
4. Bob ajoute ce produit à l'entier qu'il a inscrit. Son score correspond à cette somme.

Alice gagne si les scores d'Alice et Bob ont un facteur premier commun. Bob gagne sinon. Lequel des deux joueurs possède une stratégie gagnante ?

Solution 4.59. **Réponse :** Bob peut toujours s'arranger pour gagner.

Notons $p_1 < \ldots < p_{2015}$ les nombres premiers inscrits. Il s'agit pour Bob de trouver un entier n tel que chacun des entiers $n+p_1, n+p_1p_2, \ldots, n+p_1\ldots p_{2014}$ est premier avec $p_1\ldots p_{2015}$.

On emploie pour cela le théorème des restes chinois. Comme $p_i \geqslant i+1$ pour tout i, il existe un élément $x_i \in \{0,\ldots,p_i-1\}$ tel que $x \neq -p_1\ldots p_j$ pour tout $j<i$ et $x \neq 0$ (x peut prendre au moins i valeurs non nulles et il y a au plus $i-1$ valeurs non nulles que x ne peut pas prendre, à savoir les $-p_j$).

Bob choisit alors n solution du système $n \equiv x_i \mod p_i$ pour tout i. Par définition, pour tout i, les nombres $n, n+p_1, n+p_1p_2, \ldots, n+p_1\ldots p_{i-1}$ ne sont pas divisibles par p_i.

Ainsi, quel que soit l'indice i choisit par Alice, le nombre $n+p_1\ldots p_{i-1}$ ne sera pas divisible par $p_1,\ldots,p_{2015}$. On commence par choisir n premier avec p_1 (disons $n \equiv 1 \mod p_1$). Puis, il faut que n soit premier avec p_2 et que $n \neq -p_1 \mod p_2$.

Exercice 4.60. (France TST Novembre, Japan MO 2023) Alice et Bob jouent au jeu suivant. Avant que le jeu ne commence, leur amie Clara a écrit les entiers $2,3,4,\ldots,30$ au tableau. Puis, chacun à leur tour, Alice et Bob effacent certains entiers encore présents sur le tableau ; on note S_k l'ensemble des entiers effacés au $k^{\text{ème}}$ tour de jeu. Pour corser le jeu, Clara a elle-même choisi l'ensemble S_1 dont elle force Alice à effacer les éléments au premier tour.
De plus, pour tout entier $k \geqslant 2$, au moment de choisir l'ensemble S_k des nombres qu'il s'apprête à effacer, le joueur qui joue au $k^{\text{ème}}$ tour doit respecter la contrainte suivante : pour chaque élément x de S_k, il doit exister au moins un élément y de S_{k-1} tel que $\mathsf{PGCD}(x,y) \neq 1$.
Par exemple, si Clara choisit l'ensemble $S_1 = \{2,5\}$, Bob peut choisir, au deuxième tour, l'ensemble $S_2 = \{14,25,26\}$; au troisième tour, Alice peut alors effacer les entiers 15 et 22, mais pas 27.
Le premier joueur qui choisit un ensemble vide perd la partie. Pour combien d'ensembles S_1 non vides Alice pourra-t-elle se débrouiller pour gagner quels que soient les choix de Bob ?

Solution 4.60. **Réponse :** 1023 ensembles.

Pour tout entier $k \geqslant 1$, on notera $S_{\leqslant k}$ l'ensemble $S_1 \cup S_2 \cup \cdots \cup S_k$.

On dit qu'un ensemble S est *primitif* s'il existe des nombres premiers $p_1, p_2, \ldots, p_\ell$ pour lequel S est formé des entiers n compris entre 2 et 30 dont les seuls facteurs premiers figurent parmi les nombres $p_1, p_2, \ldots, p_\ell$. On dit alors que $p_1, p_2, \ldots, p_\ell$ *engendrent* l'ensemble S ; il s'agit des éléments de S qui sont des nombres premiers. Remarquons au passage que deux familles de nombres premiers distinctes engendrent des ensembles primitifs différents.

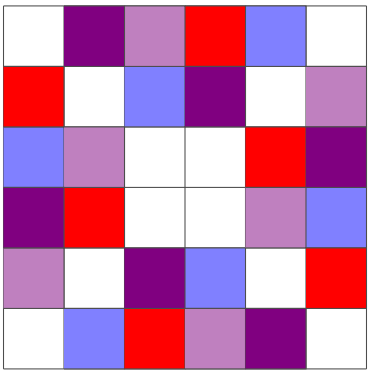
Si S_1 est primitif, Alice peut se débrouiller pour gagner, en choisissant à chaque fois un ensemble S_{2k+1} tel que $S_{\leqslant 2k+1}$ soit primitif. En effet, c'est le cas pour $k=0$. Puis, étant donné un entier $k \geqslant 0$ pour lequel $S_{\leqslant 2k+1}$ est primitif, Bob devra nécessairement inclure dans son ensemble S_{2k+2} un entier n divisible par un nombre premier $p \notin S_{\leqslant k}$. Cependant, Bob ne peut pas inclure p dans l'ensemble S_{2k+2}, car p ne figure pas parmi les facteurs premiers des éléments de $S_{\leqslant 2k+1}$. Alice pourra alors choisir S_{2k+3} de sorte que $S_{\leqslant 2k+3}$ soit l'ensemble primitif engendré par tous les nombres premiers divisant un élément de $S_{\leqslant 2k+2}$; cet ensemble S_{2k+3} est non vide, car il contient p. Ainsi, à chaque étape, Alice pourra toujours effacer au moins un nombre, donc elle ne perdra pas, et c'est Bob qui perdra.

Si, au contraire, S_1 n'est pas primitif, Bob commence par choisir l'ensemble S_2 de sorte que $S_{\leqslant 2}$ soit l'ensemble primitif engendré par tous les nombres premiers divisant un élément de S_1. Il applique désormais la même stratégie qu'Alice aurait appliquée si elle avait débuté avec l'ensemble primitif $S_{\leqslant 2}$ au lieu de l'ensemble S_1, et s'assure la victoire.

En conclusion, Alice gagne si et seulement si S_1 est primitif. Or, les nombres premiers compris entre 2 et 30 sont 2, 3, 5, 7, 11, 13, 17, 19, 23 et 29. Comme il y a 10 nombres premiers compris entre 2 et 30, et que chaque ensemble non vide formé de ces nombres premiers engendre un ensemble primitif, il existe donc 2^{10} ensembles primitifs, dont l'un est vide, et $2^{10}-1$ sont non vides et propres à assurer la victoire d'Alice. La réponse attendue est donc $2^{10}-1=1023$.

Exercice 4.61. (Polish MO Round 2 2023 P6) Soit $p \geqslant 5$ un nombre premier et soit $n = p-1$. On considère un échiquier de $n \times n$ cases. Un ensemble de n cases est dit *tactique* si, après avoir placé une dame sur chacune des n cases, deux dames quelconques ne s'attaquent jamais. Montrer qu'il existe $n-2$ ensembles tactiques disjoints n'ayant deux à deux aucune case en commun et ne contenant aucune case des deux diagonales principales.

Solution 4.61. On propose la partition suivante, dont l'exemple est illustré ci-dessous pour $n = 6$:



On numérote Les indices étant considérés modulo p, on prétend que les ensembles $A_k = \{(x, kx), x \in \{1, \dots, p-1\}\}$ pour $k = 2, \dots, p-2$ sont tactiques. Il y en a bien $p-3$, et l'on va montrer qu'ils sont disjoints.

Les A_k sont disjoints si $(x, kx) = (y, \ell y)$ est dans A_k et A_ℓ, il vient que $x = y$ et que $kx \equiv \ell y \mod p$ puis que $k = \ell$ en simplifiant par x qui est bien inversible modulo p. Ainsi, si $k \neq \ell$, A_k et A_ℓ n'ont aucun élément en commun.

A_k est tactique pour tout k : prenons deux cases distinctes (x, kx) et (y, ky) de l'ensemble A_k. Comme $x \neq y$ et $kx \neq ky \mod p$, ces deux cases ne sont ni sur la même ligne ni sur la même colonne. Pour vérifier qu'elles ne sont pas sur la même diagonale, il suffit de vérifier que $|x-y| \neq |kx-ky| = |k||x-y| \mod p$. Mais $|x-y|$ est inversible modulo p et $|k| \neq 1$, donc on a toujours $|x-y| \neq |kx-ky|$. L'ensemble A_k est bien tactique.

Exercice 4.62. (Nordic 2021) Alice a écrit des entiers au tableau. Puis, à chaque minute, elle ajoute à la liste des nombres du tableau le plus petit entier supérieur aux entiers déjà écrits et non divisible par l'un d'entre eux. Montrer qu'à partir d'un certain temps, Alice n'écrit plus que des nombres premiers.

Solution 4.62. Notons A le plus grand entier parmi les entiers écrits au tableau au départ. La liste des entiers écrits par Alice à partir de la première minute est une suite strictement croissante.

On commence par remarquer que Alice écrit tous les nombres premiers supérieurs strictement à A : pour tout $p \geqslant A$, notons a le plus petit entier inférieur à p écrit par Alice. Le nombre p est alors supérieur à tous les nombres du tableau et n'est divisible par aucun des nombres du tableau. Par définition de a, p est le plus petit nombre à vérifier cette propriété, donc Alice écrit p après a. Comme tous les nombres premiers supérieurs à A sont écrits, Alice n'écrit aucun multiple de ces nombres premiers.

Notons donc $p_1, \dots, p_r$ les nombres premiers inférieurs à A. Ainsi, tous les entiers composés écrit par Alice après la première minute ont leurs facteurs premiers parmi $p_1, \dots, p_r$. Supposons par l'absurde qu'Alice écrive une infinité de nombres composés $b_1, b_2, \dots$. Notons $b_i = p_1^{\alpha_1^i} \dots p_r^{\alpha_r^i}$ la décomposition en facteurs premiers pour chaque i.

De la suite (b_i), on peut extraire une sous-suite infinie $b_{i_1}, b_{i_2}, \dots$ telle que $(\alpha_1^{i_n})_n$ est croissante. De la suite $b_{i_1}, \dots$, on peut extraire une sous-suite infinie $b_{j_1}, b_{j_2}, \dots$ telle que $(\alpha_2^{j_n})_n$ est croissante. En itérant r fois ces extractions successives, on peut extraire de la suite (b_i) une sous suite $b_{x_1}, b_{x_2}, \dots$ telle que les suites $(\alpha_k^{x_n})_n$ sont toutes croissantes. Mais alors $b_{x_1} \mid b_{x_2}$, ce qui est absurde. Ainsi, Alice écrit un nombre fini d'entiers composés.

Remarque : Dans notre dernier paragraphe, on a utilisé qu'un ensemble dont les facteurs premiers sont tous inférieurs ou égaux à A est soit fini soit contient deux entiers dont l'un divise l'autre. Il s'agit d'un cas particulier d'un théorème plus général appelé lemme de Dickson.

Exercice 4.63. (Canada MO 2018, Envoi TN 2021-2022) On dit que deux entiers $a, b \in \mathbb{N}^\star$ sont *reliés* s'il existe un nombre premier p tel que $a = pb$ ou $b = pa$.

Trouver tous les entiers $n \geqslant 1$ ayant la propriété suivante : on peut écrire tous les diviseurs positifs de n (1 et n compris) exactement une fois sur un cercle de sorte que tout diviseur soit relié avec chacun de ses deux voisins ?

Solution 4.63. Traitons d'abord le cas où n n'a qu'un seul facteur premier, donc $n = p^\alpha$. Si $\alpha \leq 1$, n'importe quelle configuration marche. En revanche, si $\alpha \geq 2$, 1 doit être placé à côté de deux nombres différents, et n'est relié qu'à un seul autre diviseur de p^α (celui-ci étant p), ce n'est donc pas possible.

Remarquons que la parité du nombre de diviseurs premiers comptés avec multiplicité change forcément entre un nombre et un nombre qui lui est relié. Ainsi, si n a un nombre impair de diviseurs, l'existence d'une telle configuration impliquerait que 1 a à la fois un nombre pair et un nombre impair de diviseurs premiers, ce qui n'est pas possible. Les nombres ayant un nombre impair de diviseurs étant les carrés parfaits, ceux-ci ne vérifient pas non plus la propriété de l'énoncé.

Maintenant, essayons de résoudre le cas où on a deux facteurs premiers, mettons $n = p^a q^b$ avec l'un des nombres a ou b étant impair, et l'on suppose sans perte de généralité qu'il s'agit de a.

L'arrangement suivant fonctionne :

$$1, q, q^2, \ldots, q^b, pq^b, pq^{b-1}, \ldots, pq, p^2q, \ldots, p^{a-1}q^b, p^aq^b, p^aq^{b-1}, \ldots, p^aq, p^a, p^{a-1}, \ldots, p, 1$$

On utilise le fait que a est impair pour dire qu'on a effectivement écrit $p^{a-1}q^b$ juste avant p^aq^b.

On procède maintenant par récurrence sur le nombre de diviseurs premiers : supposons avoir montré pour un $k \geq 2$ que tous les nombres de la forme $\prod_{i=1}^{k} p_i^{\alpha_i}$ avec au moins l'un des α_i impair vérifient la propriété de l'énoncé, et soit $n = \prod_{i=1}^{k+1} p_i^{\alpha_i}$ avec au moins l'un des α_i impairs, disons α_1. Alors l'hypothèse de récurrence nous dit qu'on peut ordonner les diviseurs de $n' = \prod_{i=1}^{k} p_i^{\alpha_i}$ de la forme $d_1, \ldots d_m$ de sorte que d_i et d_{i+1} soient tous reliés, de même que d_m et d_1. Alors l'arrangement suivant fonctionne pour m (car m est pair) :

$$d_1, p_{k+1}d_1, \ldots, p_{k+1}^{\alpha_{k+1}}d_1, p_{k+1}^{\alpha_{k+1}}d_2, \ldots p_{k+1}d_2, d_2, d_3, \ldots, p_{k+1}^{\alpha_{k+1}}d_m, \ldots p_{k+1}d_m, d_m, d_1$$

Ainsi les nombres qui ne vérifient pas cette propriété sont les carrés (différents de 1) et le puissances (plus grandes que 2) de nombres premiers.

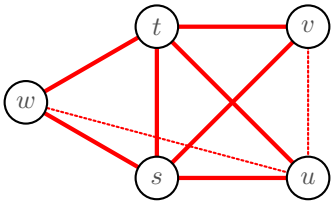
Exercice 4.64. (IMO SL 2021 C1) Soit $\mathcal{S}$ un ensemble infini d'entiers naturels non nuls contenant quatre entiers a, b, c, d deux à deux distincts tels que $\mathrm{PGCD}(a,b) \neq \mathrm{PGCD}(c,d)$. Démontrer que $\mathcal{S}$ contient trois entiers x, y, z deux à deux distincts tels que $\mathrm{PGCD}(x,y) = \mathrm{PGCD}(y,z) \neq \mathrm{PGCD}(z,x)$.

Solution 4.64. Ci-dessous, on note $m \wedge n$ le plus grand diviseur commun à deux entiers m et n. On considère alors le graphe colorié infini dont les sommets sont les éléments de $\mathcal{S}$, et où chaque paire de sommets (u,v) distincts l'un de l'autre est reliée par une arête de couleur $u \wedge v$.
Supposons que les entiers x, y, z n'existent pas. Cela signifie que tout triangle est colorié en utilisant soit une seule couleur, soit exactement trois couleurs.

Soit maintenant u, v et w trois éléments de $\mathcal{S}$. Puisque u, v et w comptent chacun un nombre fini de diviseurs, la fonction $f : x \mapsto (u \wedge x, v \wedge x, w \wedge x)$ ne prend qu'un nombre fini de valeurs. Parmi l'infinité d'éléments de $\mathcal{S}$ distincts de u, v et w, il en existe donc deux, disons s et t, tels que $f(s) = f(t)$, c'est-à-dire que

$$s \wedge u = t \wedge u, \quad s \wedge v = t \wedge v \quad \text{et} \quad s \wedge w = t \wedge w.$$

Les triangles (s,t,u), (s,t,v) et (s,t,w) sont donc monochromes, et puisqu'ils partagent l'arête (s,t), ils sont de la même couleur, disons $\mathcal{C}$. Mais alors les triangles (s,u,v) et (s,u,w) ont chacun deux arêtes de couleur $\mathcal{C}$, dont ils sont eux aussi monochromes de couleur $\mathcal{C}$, de sorte que $u \wedge v = u \wedge w$.



Ainsi, deux arêtes ayant un sommet commun sont nécessairement de la même couleur, et notre graphe est monochrome. Cela signifie en particulier que

$$a \wedge b = c \wedge d,$$

en contradiction avec les hypothèses de l'énoncé. Notre hypothèse initiale était donc invalide, ce qui conclut.

Solution alternative
Soit k le PGCD des éléments de $\mathcal{S}$. Si l'on divise chaque élément de $\mathcal{S}$ par k, on obtient un ensemble $\mathcal{S}'$ qui vérifie toujours l'énoncé et, réciproquement, si $\mathcal{S}'$ vérifie l'énoncé, $\mathcal{S}$ le vérifie aussi. On remplace donc $\mathcal{S}$ par $\mathcal{S}'$, c'est-à-dire que l'on suppose désormais que $k = 1$.

Soit x et y deux éléments de $\mathcal{S}$ tels que $x \wedge y \neq 1$. Il suffit, par exemple, de choisir $(x,y) = (a,b)$ ou $(x,y) = (c,d)$. Si $\mathcal{S}$ admet un élément z premier avec x et y, on a $x \wedge z = y \wedge z = 1 \neq x \wedge y$, ce qui constitue le résultat souhaité.

Sinon, parmi les facteurs premiers de xy, il en existe au moins un, disons p, qui divise une infinité d'éléments de $\mathcal{S}$. Notons $\mathcal{S}_p$ l'ensemble des éléments de $\mathcal{S}$ qui sont divisibles par p. Puisque $k = 1$, il existe un élément t de $\mathcal{S}$ qui n'appartient pas à $\mathcal{S}_p$. Comme $\mathcal{S}_p$ est infini, et puisque la fonction $n \mapsto t \wedge n$ ne prend qu'un nombre fini de valeurs lorsque n varie, il existe deux éléments u et v de $\mathcal{S}_p$ tels que $t \wedge u = t \wedge v$. Puisque p divise $u \wedge v$ mais pas $u \wedge v$, on en conclut que $t \wedge u = t \wedge v \neq u \wedge v$, ce qui donne de nouveau le résultat souhaité.

Exercice 4.65. (IMO 2021 P1) Soit $n \geqslant 100$ un entier. On écrit les entiers $n, n+1, \ldots, 2n$ chacun sur une carte. On mélange ensuite les $n+1$ cartes et on les divise en deux piles. Montrer qu'au moins une pile contient deux cartes dont la somme des numéros est un carré parfait.

Solution 4.65. La meilleure façon de forcer cette situation, c'est d'exhiber trois entiers $n \leqslant a < b < c \leqslant 2n$ et trois entiers k, ℓ et m tels que

$$\begin{cases} a+b &= k^2 \\ a+c &= \ell^2 \\ b+c &= m^2 \end{cases}$$

Si on fixe k, ℓ et m consécutifs, c'est-à-dire en prenant $\ell = k+1$ et $m = k+2$, on trouve

$$\begin{cases} a &= \dfrac{k^2-2k-3}{2} \\ b &= \dfrac{k^2+2k+3}{2} \\ c &= \dfrac{k^2+6k+5}{2} \end{cases}$$

On voit ici que l'entier k doit être impair pour que cela fonctionne. On remplace donc k par $2x-1$ dans les équations, ce qui donne

$$\begin{cases} a &= 2x^2-4x \\ b &= 2x^2+1 \\ c &= 2x^2+4x. \end{cases}$$

L'entier x doit donc satisfaire

$$n \leqslant 2x^2-4x < 2x^2+4x \leqslant 2n.$$

ou encore

$$x^2+2x \leqslant n \leqslant 2x^2-4x.$$

Notons A_x l'ensemble des entiers n vérifiant cette inégalité. Il suffit de montrer que A_x et A_{x+1} ne sont jamais disjoints pour x suffisamment grand, de sorte que tout entier $n \geqslant 100$ appartient bien à l'un des A_x. Pour cela, il suffit de vérifier que

$$2x^2-4x \geqslant (x+1)^2+2(x+1),$$

ce qui est vrai lorsque $x \geqslant 9$. Ainsi, $A_9 \cup \ldots \cup A_k \cup \ldots$ contient tous les entiers supérieurs ou égaux à $9^2+2\times 9 = 99$, ce qui permet de conclure.

Remarque : Si l'on n'utilise pas le caractère impaire de k et qu'on poursuit avec k quelconque, on obtient des inégalités qui ne sont pas suffisamment précises pour inclure $n = 100$ dans l'union des A_k.

Exercice 4.66. (BMO 2024 N1) Soit $n \geqslant 1$ un entier. Existe-t-il deux entiers strictement positifs x et y distincts possédant chacun n chiffres, dont les chiffres sont chacun $1, 2, 3$ ou 4 et tels que $4^n \mid x-y$?

Solution 4.66. Supposons par l'absurde que ce n'est pas le cas. En particulier l'ensemble des nombres à n chiffres dans $\{1,2,3,4\}$ forme un système complet de résidus modulo 4^n.

Pour toute suite $b = b_1, \ldots, b_{n-1}$ de $n-1$ chiffres de $\{1,2,3,4\}$, les quatre nombres $\overline{b1}, \overline{b2}, \overline{b3}, \overline{b4}$ sont consécutifs, ils représentent donc des résidus consécutifs modulo 4. Ainsi, l'ensemble des restes modulo 4^n dans l'ordre est la concaténation de 4^{n-1} blocs de 4 nombres consécutifs de la forme ci-dessus :

$$\overline{b1}, \overline{b2}, \overline{b3}, \overline{b4}, \quad \overline{c1}, \overline{c2}, \overline{c3}, \overline{c4}, \quad \ldots \quad \overline{d1}, \overline{d2}, \overline{d3}, \overline{d4}.$$

On déduit en particulier que les nombres finissant par 1 ont tous les même résidu modulo 4. C'est absurde, puisque $\overline{1\ldots121} = \overline{1\ldots111}+10 \equiv \overline{1\ldots111}+2 \mod 4$. Cette contradiction implique qu'il y a bien deux entiers x et y avec le même reste modulo 4^n, comme voulu.

Exercice 4.67. (IMO SL 2009 N2) Un entier strictement positif N est dit joli si $N = 1$ ou si N s'écrit comme un produit d'un nombre pair de facteurs premiers (pas forcément distincts). Pour toute paire (a, b) d'entiers strictement positifs, on pose $P(x) = (x + a)(x + b)$.

a) Montrer qu'il existe des entiers strictement positifs distincts (a, b) tels que $P(1), P(2), \ldots, P(50)$ sont jolis.

b) Montrer que si $P(n)$ est joli pour tout entier $n > 0$, alors $a = b$

Solution 4.67. a) On désire trouver des entiers a et b tels que le nombre de facteurs premiers des entiers $x+a$ et $x+b$ ont la même parité. Cela revient à trouver deux suites de 50 entiers consécutifs $a+1, \ldots, a+50$ et $b+1, \ldots, b+50$ tels que le nombre de facteurs premiers de $a+1$ et $b+1$ aient la même parité, le nombre de facteurs premiers de $a+2$ et $b+2$ aient la même parité, etc...
Si on pose $f(x) = 0$ si le nombre de facteurs premiers de x est pair et $f(x) = 1$ s'il est impair, on constate qu'il n'y a que 2^50 suites de 0 ou 1 possibles pour la suite $f(a+1), \ldots, f(a+50)$.
Ainsi, parmi les suites $(f(1), \ldots, f(50))$; $(f(51), \ldots, f(100))$; ... ; $(f(2^{50}+1), \ldots f(2^{50}+50))$, il y a deux suites égales. On dispose donc de deux entiers a et b tels que $(f(a+1), \ldots f(a+50))$ et $(f(b+1), \ldots, f(b+50))$ soient égales. Les entiers a et b conviennent donc.
b) On peut se convaincre, à la lumière de la question précédente, que la fonction $f(x)$ introduite à la question précédente n'est as périodique à partir d'un certain rang et donc que les entiers a et b ne peuvent pas être distincts, mais on propose un raisonnement rigoureux :
On suppose par l'absurde que $a \neq b$. On observe que $P(k(b-a)-a) = k(k+1)(b-a)^2$ pour k un entier suffisamment grand pour que $k(b-a)-a$ soit strictement positif. Le nombre $P(k(b-a)-a)$ admet cond un nombre pair de facteurs premiers si et seulement si $k(k+1)$ admet un nombre pair de facteurs premiers. Comme par l'absurde c'est le cas pour tout entier k suffisamment grand, cela implique que $f(k) = f(k+1)$ pour tout entier k suffisamment grand et donc que la fonction f soit constante à partir d'un certain rang. Mais pour tout nombre premier p, $f(p) = 1$ et pour tout entier k, $f(k^2) = 0$. La fonction n'est donc pas constante donc on a obtenu la contradiction désirée.

Exercice 4.68. (France EGMO TST 2019) Jean dispose de 503 pièces, qu'il a réparties dans deux saladiers, chaque saladier contenant au moins une pièce. Puis, tant que chacun des deux saladiers contient deux pièces ou plus, il effectue l'opération suivante : à chaque opération, il choisit le saladier qui contient un nombre pair de pièces, prend la moitié de ces pièces, et les met dans l'autre saladier ; si l'un des deux saladiers contient une pièce ou moins, il s'arrête.
Est-il possible que ce processus ne s'arrête jamais ?

Solution 4.68. Dans la suite, on pose $n = 503$, et on va démontrer que ce processus va nécessairement finir par s'arrêter.
On numérote alors nos saladiers, et on note a_ℓ le nombre de pièces dans le saladier n°1 après ℓ opérations. On remarque alors que :

- ➢ si a_ℓ est pair, alors $a_{\ell+1} = a_\ell/2$;
- ➢ sinon, $a_{\ell+1} = a_\ell + (n - a_\ell)/2 = (n + a_\ell)/2$.

Dans tous les cas, on constate que $2a_{\ell+1} \equiv a_\ell \pmod n$, donc que $2^\ell a_\ell \equiv a_0 \pmod n$.

Or, on souhaite démontrer qu'il existe un entier ℓ tel que a_ℓ soit égal à 1 ou à $n-1$, c'est-à-dire tel que $a_\ell \equiv \pm 1 \pmod n$. Il nous faut donc démontrer que tout entier a_0 compris entre 1 et $n-1$ peut s'exprimer sous la forme $\pm 2^\ell \pmod n$ pour un certain ℓ : notons $(*)$ cette propriété.

Une première chose à faire est de décomposer n en produit de facteurs premiers. Puisque $23^2 = 529 > 503$, il nous suffit de tester si n est divisible par un nombre premier $p \leqslant 19$. On constate alors aisément que

$$\begin{aligned} n &= 1 + 2 \times 251 = 2 + 3 \times 167 = 3 + 5 \times 100 = 6 + 7 \times 71 \\ &= 8 + 11 \times 45 = 9 + 2 \times 13 \times 19 = 10 + 17 \times 29, \end{aligned}$$

ce qui démontre bien que n est premier.

Soit alors ω l'ordre de 2 modulo n. Afin de calculer ω, et comme ω divise $n-1$, on commence par factoriser $n - 1 = 2 \times 251$. Puisque $17^2 = 289^2 > 251$ et que

$$251 = 1 + 2 \times 5^3 = 2 + 3 \times 83 = 6 + 7 \times 35 = 9 + 11 \times 22 = 4 + 13 \times 19,$$

les deux facteurs premiers de $n-1$ sont bien 2 et 251, de sorte que $\omega \in \{1, 2, (n-1)/2, n-1\}$. Or, ω n'est manifestement pas égal à 1 ni à 2, donc $\omega \in \{(n-1)/2, n-1\}$. Mais alors :

- ➢ si $\omega = n-1$, alors tout entier compris entre 1 et $n-1$ s'exprime même sous la forme $2^\ell \pmod n$, donc $(*)$ est vérifiée ;
- ➢ si $\omega = (n-1)/2$, tout carré s'exprime également sous la forme $2^\ell \pmod n$; en outre, comme $n \equiv 3 \pmod 4$, on sait que -1 n'est pas un carré modulo n, et donc que tout non carré est l'opposé d'un carré ; ainsi, $(*)$ est vérifiée dans ce cas également, ce qui conclut.

Exercice 4.69. (BXMO 2017) Un $n-$carré est une grille $n \times n$ dans laquelle on inscrit n^2 entiers strictement positifs deux à deux distincts et vérifiant la propriété suivante :

Si on calcule le plus grand commun diviseur de chaque ligne et le plus grand commun diviseur de chaque colonne, les $2n$ nombres obtenus sont distincts.

1. Montrer qu'un $n-$carré contient au moins un nombre supérieur ou égal à $2n^2$.
2. On suppose que tous les nombres de la grilles sont majorés par $2n^2$. Trouver les valeurs possibles de n.

Solution 4.69. 1) Comme les PGCD sont deux à deux distincts, l'un des pgcd est supérieur ou égal à $2n$. Disons que ce PGCD, noté δ, est celui des éléments de la ligne L. Les éléments de la ligne L sont donc de la forme $\delta \times k$ avec $k \geqslant 1$, et deux à deux distincts. Donc l'un des éléments est de la forme $\delta \times k$ avec $k \geqslant n$, de sorte qu'il est plus grand que $2n \times n$.

2) Soit n une solution. On écarte le cas $n = 1$ qui est impossible. Si le plus grand élément est $2n^2$, cela signifie qu'il y a égalité dans les inégalités de la question 1 et que $\delta = 2n$, donc les PGCD des lignes et colonnes sont exactement les nombres $1, \dots 2n$. De plus, les éléments de la ligne L sont exactement les éléments de la forme $2n \times k$ avec $1 \leqslant k \leqslant n$.

Notons qu'aucun élément n'est divisible par $2n$ et $2n-1$, car leur produit est supérieur à $2n^2$. Ainsi, $2n-1$ est le PGCD d'éléments d'une ligne L_2. De même, comme aucun élément n'est divisible par $(2n-1)$ et $(2n-2)$, $2n-2$ est le PGCD des éléments d'une ligne L_3. Comme $(2n-1)(n+1) > 2n^2$, les éléments de L' sont les $(2n-1)k$ avec $1 \leqslant k \leqslant n$. Ainsi, si n est le PGCD des éléments d'une ligne L', on trouve que l'ensemble $L' \cup L_2 \cup L$ contient $n+1+n$ multiples de n distincts, ce qui est absurde. n est donc le PGCD des éléments d'une colonne C.

Cas 1 : Si n est impair, alors il y a n multiples de n qui sont pairs parmi $\{1, \dots, 2n^2\}$. Ils sont donc tous dans la ligne L, ce qui signifie que les $n-1$ autres éléments de C sont tous impairs, donc les PGCD des $n-2$ autres lignes du tableau sont tous impairs, ce qui contredit le fait que les éléments de L'' sont divisibles par $2n-2$. Ce cas n'est donc pas possible.

Cas 2 : Si n est pair et suffisamment grand, le même argument implique que $2n-3$ et $2n-4$ sont les PGCD d'éléments d'une ligne, notées L_4 et L_5. Notons qu'il y a alors $n+1$ multiples de $n-1$ qui sont pairs et inférieurs à $2n^2$, et n d'entre eux sont dans la ligne L_3. Mais si $n-1$ est le PGCD d'une ligne, alors cette ligne contient au moins $n-1$ termes impairs, donc donc au moins $n-1$ nombres impairs sont PGCD d'une colonne, ce qui contredit le fait que $2n-1$ et $2n-3$ sont PGCD d'une ligne. Donc $n-1$ est le PGCd d'une ligne L'', mais alors cette ligne contient un multiple de $2n$ et un multiple de $2n-4$, donc cette ligne contient au moins 2 termes pairs, d'où la contradiction.

n est donc petit et vérifie notamment $(2n-3)(2n-4) \leqslant 2n^2$, soit $n \leqslant 6$.

Si $n = 6$, pour les mêmes raisons que dans le cas précédents, $10, 11$ et 12 sont les PGCD de trois lignes, ce qui force $7, 8$ et 9 à être également PGCD de lignes, puisque $7 \times 11, 8 \times 11$ et 9×11 ne sont pas des éléments du carré, ce qui nous ramène à la situation précédente.

On a par ailleurs les constructions suivantes pour $n = 2$ et $n = 4$:

5	6	7	8
10	30	14	16
15	18	21	24
20	12	28	32

3	4
6	8

Exercice 4.70. (IMO SL 2017 N3) Déterminer tous les entiers $n \geqslant 2$ possédant la propriété suivante : pour tout choix de n entiers $a_1, a_2, \ldots, a_n$ dont la somme n'est pas divisible par n, il existe un indice $1 \leqslant i \leqslant n$ tel qu'aucun des nombres

$$a_i, a_i + a_{i+1}, \ldots, a_i + a_{i+1} + \ldots + a_{i+n-1}$$

n'est divisible par n. (Ici, on adopte la convention $a_{i+n} = a_i$).

Solution 4.70. **Réponse :** Les entiers vérifiant la propriété sont les nombres premiers.

Dans la suite, les indices sont pris modulo p.

Supposons d'abord que n n'est pas premier, et on l'écrit sous la forme ab avec $1 < a, b < n$. On considère alors les entiers

$$\underbrace{a, a, \ldots, a}_{b+1 \text{ fois}}, 0, \ldots, 0$$

La somme des éléments vaut $a(b+1)$ qui est compris strictement entre n et $2n$ donc non divisible par n. En revanche, en prenant $i = 1$, on tombe sur $a_1 + \ldots + a_b = ab = n$. Ainsi, si n est composé, il ne vérifie pas la propriété.

Supposons désormais que $n = p$ est premier et montrons que n vérifie la propriété. Soient $a_1, \ldots, a_n$ des entiers dont la somme n'est pas divisible par n. Pour trouver l'indice i, il faut les "essayer tous" et parcourir l'ensemble des sommes $a_i + \ldots + a_j$.

Supposons par l'absurde que, pour tout indice i, il existe un indice $f(i) < i + p$ tel que $a_i + \ldots + a_{f(i)-1}$ soit divisible par p. L'idée est d'itérer f pour obtenir des blocs disjoints de sommes divisible par i :

$$\underbrace{a_1 + \ldots + a_{f(1)-1}}_{p|}, \underbrace{a_{f(1)} + \ldots + a_{f(f(1))-1}}_{p|}, \ldots, \underbrace{a_{f^k(1)} + \ldots + a_{f^{k+1}(1)-1}}_{p|}.$$

D'après le principe des tiroirs, parmi les entiers $1, f(1), \ldots, f^{p-1}(1)$, il existe deux entiers $i = f^k(1)$ et $\ell = f^j(1)$ égaux. La somme

$$(a_i + \ldots + a_{f(i)-1}) + \ldots + (a_{f^{j-k-1}(1)} + \ldots + a_{\ell-1})$$

est donc une somme de blocs (de taille $< p$) divisibles par p, donc elle est divisible par p. Mais il s'agit aussi, par construction de f, de la somme d'un certain nombre de blocs de la forme $a_i + \ldots + a_{i-1}$, qui contient tous les entiers. Comme ce nombre c de blocs est compris entre 1 et $p-1$, on déduit que

$$0 \equiv (a_i + \ldots + a_{f(i)-1}) + \ldots + (a_{f^{j-k-1}(1)} + \ldots + a_{\ell-1}) = c(a_1 + \ldots + a_p) \mod p,$$

ce qui conduit à $p \mid a_1 + \ldots + a_p$, ce qui est absurde. On conclut donc à l'existence d'un indice i.

Voici une autre façon de voir la preuve dans le cas $p = 5$, avec $f(1) = 5, f(f(1)) = 4, f^3(1) = 2$ et $f^4(1) = 1$:

$$\begin{array}{ccccc} a_1 & a_2 & a_3 & a_a| & a_5 \\ a_1 & a_2 & a_3| & a_4 & a_5 \\ a_1| & a_2 & a_3 & a_4 & a_5| \\ a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{array} \longrightarrow \begin{array}{l} 0 \equiv a_1 + a_2 + a_3 + a_4 + a_5 + a_1 + a_2 + a_3 + a_4 + a_5 + a_1 + a_2 + a_3 + a_4 + a_5 \\ = 3(a_1 + a_2 + a_3 + a_4 + a_5) \mod p. \end{array}$$

Exercice 4.71. (EGMO 2026 P2) Soit $n \geqslant 1$ un entier. Marie joue au jeu suivant. Elle commence par écrire l'entier 1 au tableau. Autant de fois qu'elle peut, elle peut choisir un entier j tel que $1 \leqslant j \leqslant n$ et remplacer l'entier V écrit au tableau par le nombre $j \cdot R(V/j)$, où $R(x)$ désigne l'entier le plus proche de V/j.

1. Montrer que, pour tout entier n, il existe un entier B strictement positif tel que Marie ne peut jamais écrire un entier strictement supérieur à B.
2. Pour tout entier n, on note $f(n)$ le plus grand entier que Marie peut écrire au tableau. Montrer qu'il existe un entier N strictement positif tel que, pour tout $n \geqslant N$, on a $2026 \mid f(n)$.

Solution 4.71.

➢ Commentaire :

> En s'essayant au jeu pour des petites valeurs de n (par exemple $n = 5, 6, 7...$), on tombe sur les observations suivantes. D'abord, si V vérifie $j \cdot R(V/j) \leqslant V$ pour tout $j \leqslant n$, alors on ne pourra pas écrire un entier plus grand V au tableau. Ensuite, pour que $j \cdot R(V/j) \leqslant V$ pour tout $j \leqslant n$, il faut que le reste de V modulo j soit inférieur à $j/2$. Cette dernière propriété est le point de départ du problème.

Notons $g_n(k)$ le reste de la division euclidienne de n par k.

Notons M le plus petit entier strictement positif tel que, pour tout $j \leqslant n$, le reste de la division de M par j soit inférieur strictement à $j/2$, soit $g_M(j) < j/2$. Comme cette condition est réalisée par exemple par $n!$ et par $\mathrm{PPCM}(1, 2, \ldots, n)$, l'existence d'un entier M minimal est garantie. Bien que cela ne soit pas nécessaire pour la question 2), on montre que $M = f(n)$.

1) Montrons que Marie ne peut pas écrire de valeur plus grande que M. Supposons au contraire que c'est le cas, notons L le premier entier strictement plus grand que M que Marie écrit et $m \leqslant M$ l'entier écrit juste avant. On note également j l'entier tel que $jR(m/j) = L$. Comme $R(m/j) = \lfloor m/j \rfloor$ ou $\lfloor m/j \rfloor + 1$ et que $j\lfloor m/j \rfloor \leqslant m \leqslant M$, on déduit que $L = j(1 + \lfloor m/j \rfloor)$. Cela signifie que $m/j \geqslant 1/2 + \lfloor m/j \rfloor$, et donc que

$$j\left(1 + \left\lfloor \frac{m}{j} \right\rfloor\right) = L > M \geqslant m \geqslant \frac{j}{2} + \left\lfloor \frac{m}{j} \right\rfloor,$$

ce qui implique que $g_M(j) \geqslant j/2$, ce qui est une contradiction.

Remarque : Le même raisonnement tient en considérant $n!$ ou $\mathrm{PPPCM}(1, 2, \ldots, n)$ plutôt que l'entier M ci-dessus.

2) Montrons d'abord que $M = f(n)$. On a déjà que $f(n) \leqslant M$. Si $f(n) < M$, alors par définition de M, il existe un entier $j \leqslant n$ tel que le reste de $f(n)$ modulo j est supérieur à $j/2$. Lorsque Marie écrit $f(n)$ au tableau, elle peut alors le remplacer par $jR(f(n)/j)$, et puisque $R(f(n)/j) = 1 + \lfloor f(n)/j \rfloor$, le nouveau nombre inscrit est strictement plus grand que $f(n)$, ce qui est absurde. On a donc $\boxed{f(n) = M}$.

Prenons désormais un entier pair $A \geqslant 1$ quelconque. Lorsque $n \geqslant A$, on obtient que $g_{f(n)}(A) \in [\![0, \frac{A}{2} - 1]\!]$. Lorsque $n \geqslant 2A$, on a $g_{f(n)}(A) \in [\![0, \frac{A}{2} - 1]\!]$ et $g_{f(n)}(2A) \in [\![0, A - 1]\!]$. Ces deux informations combinées impliquent que $\boxed{g_{f(n)}(2A) \in [\![0, \frac{A}{2} - 1]\!]}$.

Ce résultat étant vrai pour tout A tel que $n \geqslant 2A$, on peut l'itérer et obtenir que, pour tout k et tout A tel que $n \geqslant 2^k A$, on a $\boxed{g_{f(n)}(2^k A) \in [\![0, \frac{A}{2} - 1]\!]}$.

Lorsque ce résultat est appliqué à $A = 2$, on déduit notamment que, pour $n \geqslant 2^k$, on a $g_{f(n)}(2^k) = 0$ soit $\boxed{2^k \mid f(n)}$. Il reste à calibrer k et n de sorte que l'intervalle $[\![0, \frac{A}{2} - 1]\!]$ ne contienne pas 2^k. On choisit k tel que $2^k > A = 2026$ et n tel que $n \geqslant 2^k A$. D'après la discussion précédente, $g_{f(n)}(2^k A) \in [\![0, \frac{A}{2} - 1]\!]$. Cependant, $2^k \mid f(n)$ donc $g_{f(n)}(2^k A)$ est un multiple de 2^k, mais $0 \leqslant A/2 < 2^k$. On déduit que $g_{f(n)}(2^k A) = 0$, ce qui veut dire que $\boxed{A \mid f(n)}$ comme voulu.

Exercice 4.72. (BXMO 2025) Soient $a_0, a_1, \ldots, a_{10}$ des entiers tels que, pour tout $i \in \{0, 1, \ldots, 2047\}$, il existe certains indices notés $i_1, \ldots, i_r$ tels que

$$a_{i_1} + \ldots + a_{i_r} \equiv i \mod 2048.$$

Montrer que pour tout $i \in \{0, 1, \ldots, 10\}$, il existe exactement un indice $j \in \{0, 1, \ldots, 10\}$ tel que a_j est divisible par 2^i mais pas par 2^{i+1}.

Solution 4.72.

➢ **Commentaire :**

> Il est très tentant de généraliser le résultat en remplaçant 10 par n et 2048 par 2^{n+1}, et de montrer ce résultat par récurrence. C'est ce que l'on fait.
>
> La deuxième idée abordable du problème est de se rendre compte que le résultat est très facilement héréditaire : si l'on montre qu'il existe au moins un a_i impair et qu'il est unique, il suffit d'appliquer l'hypothèse de récurrence aux autres nombres divisés par 2. L'existence d'un tel a_i est facile à établir, mais l'unicité constitue en fait le coeur de l'exercice.
>
> Dans l'autre sens, si l'on arrive à trouver un a_i tel que $v_2(a_i) = n$, il est facile de se ramener à l'hypothèse de récurrence. L'existence d'un tel a_i est toutefois difficile et fait l'objet d'une deuxième solution.

On procède par récurrence sur n pour montrer le résultat suivant : étant donnés $a_0, \ldots, a_n$ des entiers tels les 2^{n+1} sommes de certains de ces entiers sont deux à deux distinctes modulo 2^{n+1}, alors pour tout $0 \leqslant i \leqslant n$, il existe un unique indice j tel que $v_2(a_j) = i$.

Initialisation : Pour $n = 0$, comme $\{0, a_0\} = \{0, 1 \mod 2\}$, il faut que a_0 soit impaire.

Hérédité : On suppose la propriété vraie pour un certain $n - 1 \geqslant 0$ fixé et on désire la démontrer pour l'entier n. On se donne $a_0, \ldots, a_n$ des entiers vérifiant la propriété de l'énoncé.

Étape 1 : Il suffit de montrer qu'il existe un unique entier impair parmi les a_i.
Supposons que l'on ait prouvé que parmi les entiers, un et un seul, disons a_0 quitte à reunméroter, est pair. Comme il y a 2^n sommes contenant a_0 et que toutes celles-ci sont impaires (les autres entiers sont pairs par hypothèse) les sommes formées avec $a_1, \ldots, a_n$ sont exactement les sommes paires et prennent donc toutes les valeurs paires modulo 2^{n+1}. On déduit que les sommes formées avec $a_1/2, \ldots, a_n/2$ donnent toutes les valeurs modulo 2^{n-1}. On peut donc leur appliquer l'hypothèse de récurrence pour obtenir que $\{v_2(a_i/2), i \geqslant 1\} = [\![0, n-1]\!]$, d'où $\{v_2(a_i), i \geqslant 0\} = [\![0, n]\!]$, comme voulu.

Étape 2 : Il existe au moins un entier impair parmi les a_i : si tous les a_i étaient paires, aucune somme ne pourrait valoir 1 modulo 2^n. Disons donc que a_0 est impair.

Étape 3 : Il existe au plus un entier a_i impair.
Comme il y a 2^{n+1} valeurs possibles modulo 2^{n+1} et qu'il y a 2^{n+1} sommes possibles avec les a_i, on déduit que pour chaque reste i, il existe un unique ensemble noté S_i d'indices tels que $\sum_{j \in S_i} a_j \equiv i \mod 2^{n+1}$. Puisque chaque a_j apparaît dans 2^n sommes S_i, en sommant tous les S_i, on trouve

$$2^n(a_0 + \ldots + a_n) = \sum_{i=0}^{2^{n+1}-1} \sum_{j \in S_i} a_j \equiv \sum_{i=0}^{2^{n+1}-1} i \equiv 2^n(2^{n+1} - 1) \mod 2^{n+1},$$

ce qui implique que $\boxed{a_0 + \ldots + a_n \text{ est impair}}$.

On considère la somme de tous les groupes d'entiers de somme paire, que l'on va calculer de deux façons différentes :

$$\sum_{i \text{ pair}} \sum_{j \in S_i} a_j \equiv \sum_{i \text{ pair}} i = 0 + 2 + \ldots + 2^{n+1} - 2 = 2^n(2^n + 1) \mod 2^{n+1}.$$

Pour un indice j fixé, on montre que a_j apparaît deux fois dans la somme précédente. Si a_j est pair, alors on peut partitionner les S_i en paires de la forme $(S, S + a_j)$ (où a_j n'apparaît pas dans S), ce qui implique que a_j apparaît dans la moitié des S_i, soit 2^{n-1} fois. Si a_j est impair, on note a_k un autre entier impair (qui existe par hypothèse. Pour chaque somme S paire ne contenant par a_j et a_k, $S + a_j + a_k$ est également pair. Comme il y a 2^{n-1} telles S, l'ensemble des S_i peut être partitionné en paires $(S, S + a_j + a_k)$, justifiant encore que a_j apparaît 2^{n-1} fois.

On déduit que

$$2^{n-1}(a_0+\ldots+a_n)\equiv 2^n(2^n+1) \mod 2^{n+1}-1.$$

Cela implique que la somme des a_i est paire, ce qui contredit l'affirmation plus haut. On a donc un unique a_i impair, ce qui conclut l'hérédité et l'exercice.

Solution alternative

On donne une autre preuve de l'hérédité. Une approche naturelle pour ce genre de problème est l'approche par les séries génératrices. Considérons le produit

$$P(X)=(X^{a_0}+1)(X^{a_1}+1)\ldots(X^{a_{10}}+1)=\sum_{r=0}^{11}\sum_{i_1<\ldots<i_r} X^{a_{i_1}+\ldots+a_{i_r}},$$

qui est un polynôme à coefficients modulo 2. Après développement de ce polynôme, on obtient la somme des monômes dont les exposants sont les sommes possibles que l'on peut faire avec les a_i. D'après l'hypothèse de l'énoncé, on a en fait

$$P(X)=(X^{a_0}+1)(X^{a_1}+1)\ldots(X^{a_{10}}+1)\equiv X^0+\ldots+X^{2^n-1}=\frac{X^{2^n}-1}{X-1}\cdot(X^{2^n}+1) \mod X^{2^{n+1}}-1.$$

Bref, il existe un polynôme Q tel que $P(X)=(X^{2^{n+1}}-1)Q(X)+\frac{X^{2^n}-1}{X-1}\cdot(X^{2^n}+1)$. En évaluant en $\omega=\exp(2i\pi/2^{n+1})$ une racine complexe de $X^{2^n}+1$, on trouve que $P(\omega)=0$. Ainsi, il existe un a_j, disons a_n, tel que $\omega^{a_j}=-1$. Comme $\omega^{2^{n+1}}=1$ et $\omega^{2^n}=-1$, on déquit que $2\pi a_n/2^{n+1}\equiv\pi \mod 2\pi$, soit que $v_2(a_n)=n$.
On peut partitionner toutes les sommes d'éléments en les paires $(S,S+a_n)$, où S ne contient pas a_n. Or, $S+a_n\equiv S \mod 2^n$, car $a_n\equiv 0 \mod 2^n$. On déduit que les sommes des $a_0,\ldots,a_{n-1}$ parcourent toutes les valeurs modulo 2^n, ce qui permet de se ramener à l'hypothèse de récurrence.

Exercice 4.73. (France TST 2020-2021) Morgane a écrit les trois entiers 3, 4 et 12 au tableau. Elle effectue ensuite des changements successifs en procédant comme suit : elle choisit deux nombres a et b écrits au tableau, les efface, et les remplace par $(3a+4b)/5$ et $(4a-3b)/5$.
Morgane peut-elle, après un nombre fini de tels changements,

1. parvenir à écrire le nombre 13 au tableau ?
2. parvenir à écrire le nombre -12 au tableau ?

Solution 4.73. Nous allons démontrer que la réponse est *négative* dans les deux cas.
Soit $\mathcal{S}$ la somme des carrés des nombres écrits au tableau, et soit f et g les fonctions définies par $f:(x,y)\to(3x+4y)/5$ et $g:(x,y)\to(4x-3y)/5$. La relation

$$f(x,y)^2+g(x,y)^2=x^2+y^2$$

nous assure que, lorsque Morgane remplace deux nombres a et b par $f(a,b)$ et $g(a,b)$, elle ne change pas la valeur de $\mathcal{S}$.
En outre, les égalités $f(f(x,y),g(x,y))=x$ et $g(f(x,y),g(x,y))=y$ nous indiquent que les changements qu'effectue Morgane sont réversibles : si elle transforme un triplet non ordonné $\mathbf{t}=(a,b,c)$ en un autre triplet $\mathbf{t}'=(a',b',c)$ tel que $a'=f(a,b)$ et $b'=g(a,b)$, elle peut retransformer $\mathbf{t}'$ en $\mathbf{t}$.

On traite maintenant les deux questions séparément.

1) Si jamais elle réussit à écrire trois nombres x, y et z tels que $z=13$, alors

$$x^2+y^2+13^2=x^2+y^2+z^2=\mathcal{S}=3^2+4^2+12^2=13^2,$$

de sorte que $x=y=0$. Cela signifie que Morgane peut transformer, en plusieurs étapes, le triplet $(3,4,12)$ en $(0,0,13)$. Elle peut donc également transformer $(0,0,13)$ et $(3,4,12)$.
On dit alors qu'un triplet (x,y,z) de nombres rationnels est *sympathique* si $v_{13}(u)\geqslant 1$ pour tout $u\in\{x,y,z\}$. Si Morgane transforme un triplet (x,y,z) sympathique en un nouveau triplet (x',y',z'), ce dernier est clairement sympathique lui aussi. Ainsi, à partir du triplet sympathique $(0,0,13)$, Morgane ne peut obtenir que des triplets sympathiques. Elle ne peut donc pas obtenir le triplet $(3,4,12)$. Ceci démontre bien qu'elle ne pouvait pas transformer le triplet $(3,4,12)$ en $(0,0,13)$.

2) Nous allons carrément démontrer que Morgane ne peut pas écrire d'entier autre que les éléments de l'ensemble $\Omega=\{0,\pm3,\pm4,\pm5,12\}$. [1]

1. Cela répondrait aussi à la question a), mais de manière nettement plus compliquée.

Considérons un triplet ordonné (x_1, x_2, x_3). Pour tous les entiers i et j distincts l'un de l'autre, on note $\Theta_{i,j}(x_1, x_2, x_3)$ le triplet obtenu à partir de (x_1, x_2, x_3) en remplaçant les nombres x_i et x_j par $f(x_i, x_j)$ et $g(x_i, x_j)$. Par ailleurs, on dit que (x_1, x_2, x_3) est d'*ordre* n si $\min\{v_5(x_1), v_5(x_2), v_5(x_3)\} = -n$, et qu'il s'agit d'un triplet *égalitaire* s'il y a au moins deux indices i tels qu $v_5(x_i) = -n$.

Tout triplet d'ordre $n \geqslant 1$ qu'obtiendra Morgane est égalitaire. En effet, supposons que cela ne soit pas le cas. Sans perte de généralité, on a $v_5(x_1) = -n$, $v_5(x_2) \geqslant 1 - n$ et $v_5(x_3) \geqslant 1 - n$. Alors, en posant $X_i = 5^n x_i$, on constate que $X_1 \not\equiv 0 \pmod 5$ et que $X_2 \equiv X_3 \equiv 0 \pmod 5$, de sorte que

$$0 \equiv 5^{2n} \times 13^2 \equiv 5^{2n}(x_1^2 + x_2^2 + x_3^2) \equiv X_1^2 + X_2^2 + X_3^2 \equiv X_1^2 \not\equiv 0 \pmod 5,$$

ce qui est absurde.
Soit alors $n \geqslant 0$ un entier, puis (x_1, x_2, x_3) et (y_1, y_2, y_3) deux triplets d'ordres $\ell \leqslant n$ et $n + 1$ que Morgane peut obtenir successivement. Il existe deux entiers i et j tels que $\Theta_{i,j}(x_1, x_2, x_3) = (y_1, y_2, y_3)$, et le triplet (y_1, y_2, y_3) est égalitaire. En notant k l'élément de $\{1, 2, 3\}$ autre que i et j, puis $X_u = 5^n x_u$ et $Y_u = 5^{n+1} y_u$ pour tout $u \in \{1, 2, 3\}$, on constate que

$$Y_i = 3X_i + 4X_j \not\equiv 0 \mod 5,\ Y_j = 4X_i - 3X_j \not\equiv 0 \mod 5 \text{ et } Y_k \equiv 0 \mod 5.$$

On en déduit immédiatement que les triplets $\Theta_{i,k}(y_1, y_2, y_3)$, $\Theta_{j,k}(y_1, y_2, y_3)$, $\Theta_{k,i}(y_1, y_2, y_3)$ et $\Theta_{k,j}(y_1, y_2, y_3)$ sont tous d'ordre $n + 2$. De même,

$$f(y_j, y_i) = (24X_i + 7X_j)/5^{n+2} \text{ et } g(y_j, y_i) = (7X_i - 24X_j)/5^{n+2}.$$

Puisque $24X_i + 7X_j \equiv Y_j \pmod 5$ et $7X_i - 24X_j \equiv -Y_i \pmod 5$, le triplet $\Theta_{j,i}(y_1, y_2, y_3)$ est lui aussi d'ordre $n+2$. Enfin, comme dans la solution n°1, on vérifie aisément que $\Theta_{i,j}$ est une involution, de sorte que $\Theta_{i,j}(y_1, y_2, y_3)$ est d'ordre $\ell \leqslant n$.
Pour finir, soit $\mathbf{T}$ un triplet, avec au moins une coordonnée x entière, que Morgane peut écrire. Supposons que Morgane a écrit successivement des triplets $\mathbf{T}_0, \ldots, \mathbf{T}_k$ tels que $\mathbf{T}_0 = (3, 4, 12)$ et $\mathbf{T}_k = \mathbf{T}$ soit à coordonnées entières, avec k minimal.
Soit $\mathbf{T}_i$ un triplet d'ordre n maximal parmi les triplets $\mathbf{T}_0, \ldots, \mathbf{T}_k$. Si $n \geqslant 1$ et si $i \leqslant k - 1$, on vient de démontrer que $\mathbf{T}_{i-1} = \mathbf{T}_{i+1}$, ce qui vient contredire la minimalité de k. Si $n \geqslant 1$ et si $i = k$, alors $\mathbf{T}_k$ contient une coordonnée déjà présente dans $\mathbf{T}_{k-1}$ et deux coordonnées de valuation 5-adique égale à $-n$, donc distinctes de x. Ceci vient là encore contredire la minimalité de k.
Il suffit maintenant de démontrer que, partant d'un triplet $\mathbf{t} = (x_1, x_2, x_3)$ d'éléments de Ω tel que $x_1^2 + x_2^2 + x_3^2 = 13^2$, tout triplet $\mathbf{t}' = (y_1, y_2, y_3)$ à coordonnées entières que Morgane peut former est à coordonnées dans Ω. Tout d'abord, on peut supposer sans perte de généralité que $|x_1| \leqslant |x_2| \leqslant |x_3|$, de sorte que $3 \times 5^2 < 13^2 \leqslant 3x_3^2$, donc que $x_3 = 12$ et que $(x_1, x_2) \in \{(0, \pm 5), (\pm 3, \pm 4)\}$.
On suppose alors que $\mathbf{t}'$ a une coordonnée entière qui n'appartient pas à Ω. Soit i et j les entiers tels que $\mathbf{t}' = \Theta_{i,j}(\mathbf{t})$. Si $\{x_i, x_j\} \subseteq \{0, \pm 3, \pm 4, \pm 5\}$, alors $y_i^2 + y_j^2 = x_i^2 + x_j^2 = 5^2$, donc $\{y_i, y_j\} \subseteq \Omega$. Ainsi, l'un des deux entiers x_i et x_j est égal à 12. Or,

$$0 \equiv 5y_i \equiv 3x_i + 4x_j \equiv 3(x_i - 2x_j) \mod 5,$$

donc $x_i \equiv 2x_j \pmod 5$.
Si $x_i = 12$, alors $x_j \equiv 1 \pmod 5$, donc $x_j = -4$, et $(y_i, y_j) = (4, 12)$; si $x_j = 12$, alors $x_i \equiv -1 \pmod 5$, donc $x_j = 4$, et $(y_i, y_j) = (12, -4)$. Dans les deux cas, on a bien $\{y_i, y_j\} \subseteq \Omega$. En conclusion, tout nombre entier que peut écrire Morgane appartient nécessairement à Ω. Elle ne peut donc pas écrire le nombre -12 au tableau.

Solution alternative

On peut présenter la solution à la partie a) d'une autre manière. Tout d'abord, tout nombre qu'écrira Morgane appartiendra nécessairement à l'ensemble $\mathbb{L} = \{d/5^k : d, k \in \mathbb{Z}\}$. Puisque 5 et 13 sont premiers entre eux, on identifie chaque élément de $\mathbb{L}$ à son résidu modulo 13.
Mais alors, si Morgane parvient à remplacer deux nombres a et b par des nombres $a' = f(a, b)$ et $b' = g(a, b)$ tels que $a' \equiv b' \equiv 0 \pmod{13}$, cela signifie que $3a + 4b \equiv 4a - 3b \equiv 0 \pmod{13}$, et donc que

$$a \equiv -25a \equiv -3(3a + 4b) - 4(4a - 3b) \equiv 0 \pmod{13} ;$$
$$b \equiv -25b \equiv -4(3a + 4b) + 3(4a - 3b) \equiv 0 \pmod{13}.$$

Par conséquent, une récurrence immédiate indique que les nombres que Morgane écrira au tableau ne seront jamais tous congrus à 0 modulo 13.

Solution alternative

On peut également répondre à la partie a) avec une version simplifiée du raisonnement utilisé pour la partie b). En effet, il s'agit de démontrer que l'on ne peut pas atteindre le triplet $\mathbf{T} = (0, 0, 13)$, à l'ordre près des coordonnées. Si Morgane atteint ce triplet, et en raisonnant comme ci-dessus, elle a nécessairement dû écrire des triplets $\mathbf{T}_0 = (3, 4, 12), \mathbf{T}_1, \ldots, \mathbf{T}_k = \mathbf{T}$, chaque $\mathbf{T}_i$ étant à coordonnées entières.

Mais alors, puisque chaque opération $\Theta_{i,j}$ est une involution, on peut écrire $\mathbf{T}_{k-1}$ sous la forme $\Theta_{i,j}(\mathbf{T})$. À l'ordre près de ses coordonnées, le triplet $\mathbf{T}_{k-1}$ donc est égal à $\Theta_{2,3}(0, 0, 13)$ ou à $\Theta_{3,2}(0, 0, 13)$, c'est-à-dire à $(0, 52/5, -39/5)$ ou à $(0, 39/5, 52/5)$. Cette contradiction démontre que Morgane ne pourra jamais écrire le nombre 13 au tableau.

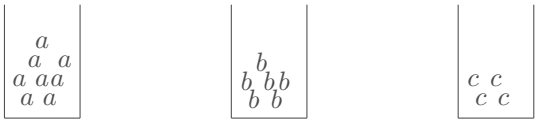
Exercice 4.74. (RMM 2024 P2) Soit p un nombre premier impair et $N < 50p$ un entier. Soient $a_1, \ldots, a_N$ des entiers strictement inférieurs à p et tels que chaque entier apparaît au plus $\frac{51}{100}N$ fois parmi les entiers a_i. On suppose également que $a_1 + \ldots + a_N$ n'est pas divisible par p. Montrer qu'il existe une permutation $b_1, \ldots, b_N$ des entiers a_i telle que, pour tout $k = 1, 2, \ldots, N$, la somme $b_1 + b_2 + \ldots + b_k$ n'est pas divisible par p.

Solution 4.74.

➢ **Commentaire :**

> Le problème est bien sûr très difficile, mais sa solution est très instructive, puisqu'elle n'utilise que des idées simples et assez sensées.
>
> Les hypothèses sont assez opaques, il faut donc proposer un algorithme et l'intérêt des bornes données apparaîtra au moment de la preuve que l'algorithme fonctionne.
>
> L'algorithme est un algorithme glouton : on choisit chaque fois la valeur la plus présente. Si ce n'est pas possible, on choisit la deuxième valeur la plus présente. Il faut alors démontrer que cet algorithme fonctionne.

On commence par trier les entiers a_i par paquets de même valeurs, de l'entier avec la plus grande fréquence d'apparition dans la liste à l'entier apparaissant le moins. On notera par la suite $s_j = b_1 + \ldots + b_j$ pour tout indice j.



Notre algorithme est le suivant : on choisit les entiers $b_1, b_2, \ldots$ un par un en commençant par b_1. A l'étape j, au moment de choisir b_j, on choisit b_j comme étant l'entier apparaissant le plus de fois parmi les nombres non encore utilisés (cette action est notée (I)). Si $b_1 + b_2 + \ldots + b_j \equiv 0 \mod p$, alors au lieu de choisir l'entier le plus fréquent, on choisit le deuxième entier le plus fréquent de la liste (cette action est notée (II)). Il s'agit d'un algorithme glouton. Notons que, tant qu'il reste au moins deux nombres distincts a et b parmi les entiers a_i non encore utilisés, alors soit l'action (I) soit l'action (II) sera possible et permettra une somme partielle non nulle modulo p, puisque pour tout k, au moins un des nombres $s_k + a$ et $s_k + b$ est non nul.

Notons qu'après une opération de type (II) vient toujours une opération de type (I). Supposons qu'à l'étape j, on a effectué une opération de type (II) en prenant $b_j = b$. Notons a l'entier apparaissant le plus fréquemment parmi les entiers restants à l'étape j, et $s = b_1 + \ldots + b_{j-1}$. Alors a est toujours l'entier le plus fréquent parmi les entiers restants à l'étape $j+1$. Comme l'opération à l'étape j était du type (II), on a $s + a \equiv 0 \mod p$ et en particulier $s + b \neq 0 \mod p$. Il vient que $b_1 + \ldots + b_j + a = s + b + a \equiv b \mod p$, donc $b_{j+1} = a$ ne fait pas échouer l'algorithme.

Supposons que notre algorithme échoue. Cela signifie qu'il existe une étape $k+1$ (supposée minimale) à partir de laquelle il ne reste qu'un seul entier parmi les a_i non utilisés, noté a, et qu'il vérifie $s_k + a \equiv 0 \mod p$. Puisque la somme totale des a_i n'est pas divisible par p, on a $k + 1 \leqslant N - 1$. Notons $j \leqslant k+1$ le plus petit entier tel que, à partir de l'étape j, l'entier a est le nombre avec la plus grande fréquence à chaque étape (j existe car $k+1$ vérifie cette propriété).

$j-1$	j	$j+1$	$\ldots$		$\ldots$	k	$k+1$	$\ldots$	N
b	a	a	$\ldots$	aba	$\ldots$	a	a	$\ldots$	a

Si $j = 1$, cela signifie que a est toujours le plus représenté à chaque étape. Ainsi, les $p-1$ premières opérations sont du type (I), la p−ème du type (II) et puis au moins une opération sur deux est du type (I) entre l'étape $p+1$ et l'étape k. Cela signifie que, dans la liste des a_i, l'entier a apparaît au moins

$$(p-1) + \frac{k-p}{2} + N - k = N - \frac{k}{2} + \frac{p}{2} - 1 > N - \frac{N-2}{2} + \frac{N}{100} - 1 = \frac{51}{100}N,$$

ce qui est une contradiction. On a donc $\boxed{j > 1}$.

Si $j > 1$: par définition, l'opération de l'étape $j-1$ est de type (II), et on note $b = b_{j-1}$. On note q le nombre d'entiers a restants dans la liste des a_i à partir de cette étape et $\ell = k - j + 1$. Entre les étapes j et k, d'après l'observation ci-dessus, a est choisi au moins une fois sur 2, et a est systématiquement choisi entre les étapes

$k+1$ et N. On déduit que $q \geqslant \lfloor \ell/2 \rfloor + (N-k) \geqslant \lfloor \ell/2 \rfloor + 2$. Comme b a été choisi au plus $\ell - \lfloor \ell/2 \rfloor$ mais que b apparaissait plus que a dans la liste à l'étape j, on a $\ell - \lfloor \ell/2 \rfloor \geqslant q \geqslant \lfloor \ell/2 \rfloor + 2$. Ceci est absurde.

Ainsi, l'algorithme permet toujours de donner une permutaiton satisfaisant l'énoncé.

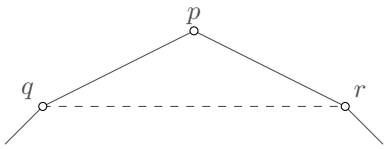
Exercice 4.75. (IMO 2022 P3) Soit $k \geqslant 1$ un entier et S un ensemble fini de nombres premiers impairs. Montrer qu'il existe au plus une façon (à rotation et symétrie près) de placer les éléments de S autour d'une cercle de sorte que le produit de deux nombres voisins soit de la forme $x^2 + x + k$, où x est un entier.

Solution 4.75.

➢ **Commentaire :**

> Dans ce problème, est très instructif et est un modèle du fonctionnement d'un problème de niveau 3/6 d'Olympiades Internationales. Il contient trois idées. La première idée, c'est de s'intéresser au plus grand nombre premier inscrit sur le cercle. La deuxième idée, la plus difficile et qui rapportait le plus de points, c'est de montrer que les deux voisins de ce nombre premier ont un produit également de la forme $x^2 + x + k$, ce qui permet d'engager une récurrence sur la taille de S (c'est la troisième idée). La réalisation de chacune de ces idées n'est pas difficile, en revanche il faut beaucoup de lucidité et d'habitude pour être capable de les enchaîner.

On procède par récurrence sur $|S|$. Si $|S| = 1, 2$ ou 3, il n'y a rien à faire. On suppose donc la propriété vérifiée pour tout ensemble de nombres premiers de taille n, avec $n \geqslant 3$ fixé. On se donne désormais un ensemble S de taille $n + 1$ satisfaisant la condition de l'énoncé.



Soit p le plus grand nombre premier de S et q et r ses deux voisins sur le cercle. On dispose de deux entiers x et y tels que $pq = x^2 + x + k$ et $pr = y^2 + y + k$. Observons que, puisque $p \geqslant q, r$, $x^2 < pq < p^2$ donc $x < p$ et de même $y < p$. En soustrayant les deux équations, on trouve

$$(x - y)(x + y + 1) = p(q - r).$$

Donc $p \mid x - y$ ou $p \mid x + y + 1$. Comme $0 < x, y < p$, on a nécessairement $p \mid x + y + 1$, ce qui conduit, puisque $0 < x + y + 1 < 2p$, à $\boxed{p = x + y + 1}$.

Montrons à présent qu'il existe un entier z tel que $\boxed{qr = z^2 + z + k}$. En effet, de l'égalité ci-dessus on déduit que $q - r = x - y$. Il vient que

$$qr = q(q + y - x) = q(q + p - 1 - 2x) = q^2 + pq - q - 2xq = q^2 + x^2 + x + q - 2xq + k = (x - q)^2 + (x - q) + k.$$

On peut à présent conclure. D'après ce qu'il vient d'être montré, l'ensemble $S \setminus \{p\}$ est également un ensemble vérifiant la propriété, il y a donc au plus une façon de disposer les nombres premiers autre que p autour du cercle, d'après l'hypothèse de récurrence. Il suffit donc de montrer qu'il y alors au plus un emplacement possible pour p. Supposons qu'il soit possible pour p d'avoir au moins un autre voisin s différent de q et r. On aurait un entier z tel que $ps = z^2 + z + k$. D'après la relation montrée plus haut, cela implique que $p = z + x + 1$ et $p = x + y + 1$, ce qui force $z = y$ puis $s = r$. Ainsi, les seuls voisins possibles pour p sont bien q et r, donc il y a bien au plus une configuration possible, ce qui achève la récurrence.

4.4 Problèmes de construction d'entiers

Exercice 4.76. (Extrait BXMO 2011) Un couple d'entiers (m, n) vérifiant $1 < m < n$ est appelé *couple Benelux* si m a les mêmes diviseurs premiers que n et $m+1$ a les mêmes diviseurs premiers que $n+1$.
Montrer qu'il existe une infinité de couples Benelux.

Solution 4.76.

➢ **Commentaire :**

> Une façon facile de garantir que a et b ont les mêmes facteurs est que $b = a^k$. On peut donc chercher (m, n) de sorte que $n = m^k$ ou que $n+1 = (m+1)^k$ pour un certain k, en commençant par $k = 2$. Comme on maitrise mieux la factorisation de $a^2 - 1$ que celle de a^2, il est préférable de viser $n + 1 = (m + 1)^2$. Les entiers m et n ont les mêmes facteurs si m et $(m + 1)^2 - 1 = m(m + 2)$, ont les mêmes facteurs premiers. Comme $\text{PGCD}(m, m + 2) \in \{1, 2\}$, on déduit que $m + 2$ doit être une puissance de 2.

Pour tout $k \geqslant 2$, on pose $\boxed{m = 2^k - 2 \text{ et } n = m(m + 2) = 2^k(2^k - 2)}$. On observe que m et n ont les mêmes facteurs premiers et que $n + 1 = (m + 1)^2$ et $m + 1$ ont les mêmes facteurs premiers. Le couple (m, n) est donc un couple Benelux, d'où l'infinité annoncée.

Exercice 4.77. (IMO 2013 P1) Soient k et n deux entiers. Montrer qu'il existe des entiers $m_1, \ldots, m_k$ tels que

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \ldots \left(1 + \frac{1}{m_k}\right).$$

Solution 4.77. On teste des pettis cas et très vite, on s'aperçoit que le plus simple est de tenter une récurrence sur k.
Initialisation : Si $k = 1$, alors on vérifie bien que

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

Hérédité : On fixe $k \geqslant 1$ et on suppose que, pour tout entier n, il existe $m_1, \ldots, m_k$ tels que

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \ldots \left(1 + \frac{1}{m_k}\right).$$

On souhaite montrer l'énoncé pour $k + 1$. Pour cela, on distingue deux cas.

Cas 1 : Si n est impair, on peut l'écrire sous la forme $n = 2m + 1$. Dans l'écriture qui suit, l'objectif est de faire apparaître un numérateur pair, de sorte à factoriser par 2, ce qui fait apparaître 2^k plutôt que 2^{k+1}. Une fois cette idée acquise, le reste n'est que du bidouillage.

$$\begin{aligned} 1 + \frac{2^{k+1} - 1}{2m + 1} &= \frac{2m + 2^{k+1}}{2m + 1} \\ &= 2 \cdot \frac{m + 1 + (2^k - 1)}{m + 1} \cdot \frac{m + 1}{2m + 1} \\ &= \left(1 + \frac{2^k - 1}{m + 1}\right) \cdot \left(1 + \frac{1}{2m + 1}\right). \end{aligned}$$

D'après l'hypothèse, $1 + \dfrac{2^k - 1}{m + 1}$ admet une écriture sous la forme $\left(1 + \dfrac{1}{m_1}\right) \ldots \left(1 + \dfrac{1}{m_k}\right)$, ce qui permet de conclure.

Cas 2 : Si n est pair, on peut l'écrire sous la forme $n = 2m$. On a alors dans la même veine

$$\begin{aligned} 1 + \tfrac{2^{k+1}-1}{2m} &= \tfrac{2m+2^{k+1}-1}{2m}. \\ &= \tfrac{2m+2^{k+1}-1}{2m+2^{k+1}-2} \cdot \tfrac{2m+2^{k+1}-2}{2m} \\ &= \left(1 + \tfrac{1}{2m+2^{k+1}-2}\right) \cdot \left(1 + \tfrac{2^k-1}{m}\right). \end{aligned}$$

D'après l'hypothèse, $1+\frac{2^k-1}{m}$ admet une écriture sous la forme $\left(1+\frac{1}{m_1}\right)\dots\left(1+\frac{1}{m_k}\right)$, ce qui permet de conclure.

Remarque : Notons que dans le cas impair, l'astuce que l'on a employée, c'est d'écrire

$$\frac{a}{b}=\frac{a}{b+1}\frac{b+1}{b},$$

tandis que dans la cas pair, le télescopage était

$$\frac{a}{b}=\frac{a}{a-1}\cdot\frac{a-1}{b}.$$

Il est fréquent qu'il faille essayer une astuce "d'un côté" puis "de l'autre" du problème, et pas toujours du même côté. De même, si une astuce ne marche pas "d'un côté", ce n'est pas pour cela qu'elle ne marche pas du tout, il faut d'abord essayer de l'appliquer dans tous les sens possibles.

Exercice 4.78. *(Envoi d'arithmétique 2020-2021)* Déterminer s'il existe une suite infinie d'entiers (a_n) d'entiers strictement positifs vérifiant les deux propriétés suivantes :

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

Solution 4.78. On applique un algorithme glouton.

On commence avec $a_1=1$. On suppose construits les k premiers termes et on note x le plus petit entier qui n'apparaît pas dans la suite. On construit a_{k+1} de sorte à pouvoir faire apparaître $a_{k+2}=x$.

Etablissons le cahier des charges en posant $\prod a_i=\prod p_i^{kb_i}$ et $x=\prod p_i^{c_i}$. Donc on veut $a_{k+1}=\prod p_i^{d_i}$ de sorte que pour tout i, on a

$$\begin{aligned} d_i+kb_i &\equiv 0 \mod k+1\\ d_i+kb_i+c_i &\equiv 0 \mod k+2\end{aligned}$$

D'après le théorème des restes chinois, ce système admet une infinité de solutions. On peut donc choisir une solution a_{k+1} qui ne figure pas parmi $a_1,\dots,a_k$.
On peut donc caser x, ce qui achève la récurrence et conclut.

Exercice 4.79. *(France TST 2019/2020)* Soit $a_0,a_1,\dots$ une suite d'entiers positifs, et soit (b_n) la suite définie par $b_n=\mathrm{PGCD}(a_n,a_{n+1})$ pour tout $n\geqslant 0$. Montrer qu'il est possible de choisir la suite (a_n) de sorte que tout entier naturel non nul soit égal à exactement un des termes $a_0,b_0,a_1,b_1,\dots$.

Solution 4.79. On utilise un algorithme glouton, et on commence par $a_0=2,a_1=9$, de sorte que $b_0=1$.

On suppose que $a_0,\dots,a_n$ et $b_0,\dots,b_{n-1}$ sont construits, et on impose la condition supplémentaire que a_n possède un diviseur d n'apparaissant pas dans les termes déjà construits des suites a et b (condition qu'il faudra garantir dans l'hérédité de notre algorithme). On note x le plus petit entier n'apparaissant pas déjà dans les suites a et b. On va chercher à construire b_n et b_{n+1} de sorte que $x=b_{n+2}$.

$$\begin{array}{ccccccc} a_n & & a_{n+1} & & a_{n+2} & & a_{n+3}\\ & b_n & & b_{n+1} & & b_{n+2} & \end{array}$$

On pose les décompositions en facteurs premiers $d=\prod p_i^{c_i}$, $a_n=\prod p_i^{e_i}$ et enfin $x=\prod p_i^{f_i}$, dans lesquelles les c_i,e_i et f_i peuvent être nuls. Une raison pour laquelle on ne peut pas guarantir $x=b_{n+1}$ est qu'on ne peut pas éviter le cas $d_i,e_i>c_i$. On a donc la situation suivante, dans laquelle on doit choisir ε_i et boucher les trous (?) :

$$\begin{array}{ccccccc} \prod p_i^{e_i} & & \prod p_i^{c_i+\varepsilon_i} & & ? & & ?\\ & \prod p_i^{c_i} & & ? & & \prod p_i^{f_i} & \end{array}$$

Pour cela, on choisit j_1,j_2 tels que, pour $j=j_1,j_2$, $e_j=f_j=c_j=0$ et tel que p_j n'est diviseur premier d'aucun des termes précédemment construits dans les suites (a_n) et (b_n). On choisit également q un autre nombre premier ne divisant aucun terme a_k ou b_k déjà construit. On prend alors $\varepsilon_i=0$ si $i\neq j_1,j_2$ et on complète ensuite comme suit :

$$\prod p_i^{e_i} \qquad p_{j_1}^3 p_{j_2} \prod p_i^{c_i} \qquad p_{j_1} p_{j_2}^3 \prod p_i^{f_i} \qquad \prod p_i^{f_i} q$$
$$\prod p_i^{c_i} \qquad p_{j_1} p_{j_2} \prod p_i^{\min(c_i,f_i)} \qquad \prod p_i^{d_i}$$

(la complexité de la construction vient du fait qu'il faut s'assurer à chaque étape qu'on n'écrit pas deux fois le même nombre)

D'après la définition de p_{j_1}, p_{j_2} et q, les nombres construits n'étaient pas déjà dans la suite et le nombre a_{n+3} possède un diviseur qui n'apparaît pas dans la liste, ce qui complète l'hérédité de notre algorithme.

Ainsi, tout entier strictement positif apparaît exactement une fois dans l'union des suites (a_n) et (b_n).

Exercice 4.80. *(Polish MO round 2 2012)* Pour tout entier $n \geqslant 1$, notons $S(n)$ la somme des chiffres de n. Montrer qu'il existe une infinité d'entiers strictement positifs n tels que $S(2^n + n) < S(2^n)$.

Solution 4.80. Prenons $n = 10^k - 2$ avec $k \geqslant 1$. L'idée est que l'addition $2^n + n$ provoque beaucoup de retenues. Notons $a_r a_{r-1} \dots a_k \dots a_1 a_0$ l'écriture décimale de 2^n. On a donc $S(2^n) = a_r + a_{r-1} + \dots + a_1 + a_0$. Il s'agit de majorer $S(2^n + n)$.

Notons $b_{r+1}, b_r, \dots b_0$, les chiffres de la représentation décimale de $2^n + n$. L'addition $2^n + n$ est représentée ci-dessous :

$$\begin{array}{cccccccc} & {\scriptstyle +1} & {\scriptstyle +1} & & {\scriptstyle +1} & {\scriptstyle +1} & & \\ & 0 & 9 & \dots & 9 & 9 & 8 & \\ + & a_k & a_{k-1} & \dots & a_2 & a_1 & a_0 & \\ \hline & b_k & b_{k-1} & \dots & b_2 & b_1 & b_0 & \end{array}$$

Comme $a_0 \in \{2, 4, 6, 8\}$, on a $b_0 = a_0 - 2$ et une retenue, de sorte que $b_1 = a_1$ avec une retenue également, et par récurrence immédiate, on trouve que $b_i = a_i$ pour tout $i \geqslant 1$. Par la suite, s'il n'y a pas eu de retenue à l'addition d'indice $i \geqslant k$, on a $b_i = a_i$, tandis que s'il y a eu une retenu alors $b_i = 0$ si $a_i = 9$ ou $b_i = a_i + 1$ si $a_i < 9$ (et il n'y a alors plus de retenue). Notons i_0 le dernier indice recevant une retenue (éventuellement $i_0 = r + 1$). Pour tout $k \leqslant i \leqslant i_0 - 1$, on a $b_i - a_i = -9$. Ainsi, au total, on a

$$S(2^n + n) = b_{r+1} + b_r + \dots + b_0 = a_{r+1} + \dots + a_{i_0} + 1 + 0 + \dots + 0 + a_k + \dots + a_0 - 2 \leqslant a_{r+1} + \dots + a_0 - 1 < S(2^n).$$

Remarque : Il est bien sûr naturel de commencer par considérer $n = 10^k - 1$. Dans ce cas, lors de la dernière étape, on se rend compte que la dernière inégalité n'est pas nécessairement stricte, ce qui conduit à prendre plutôt $n = 10^k - 2$.

Exercice 4.81. *(IMO SL 2016 N1)* Pour tout entier strictement positif k, on note $S(k)$ la somme de ses chiffres. Déterminer les polynômes P à coefficients entiers tels que, pour tout entier $n \geqslant 2016$, on a $P(n) > 0$ et

$$S(P(n)) = P(S(n)).$$

Solution 4.81. Si P est constant égal à c, on a $S(c) = c$. Comme $S(x) \leqslant x$ pour tout x, avec égalité seulement si c n'a qu'un chiffre, on déduit que $1 \leqslant c \leqslant 9$, et réciproquement ces constantes sont solutions.

On suppose que P est non constant.
Commençons par noter qu'en prenant $n = \overline{99\dots9}$ (avec k chiffres), alors $P(S(n)) = P(9k)$ est un nombre positif (car il vaut $S(P(n))$), donc le coefficient dominant de P est strictement positif.

L'objectif est de construire des entiers n grand dont on maitrise $S(n)$. Les candidats idéaux sont les nombres de la forme $x \cdot 10^k$ avec $x \in \{1, \dots, 9\}$, car ce sont de grands nombres et qu'ils ont un seul chiffre non nul. Notons d le degré de P et $P(X) = c_d X^d + \dots + c_0$.

Prenons $n = 10^k$ avec k suffisamment grand, c'est-à-dire tel que $|c_i| < 10^k$ pour tout indice i. On a

$$P(1) = S(P(10^k)) = S(c_d 10^{kd} + \dots + c_0).$$

Supposons que l'un des c_i soit négatif et prenons l'indice i maximal pour cette propriété. Notons que $i \leqslant d - 1$. Si on note $c_j = \overline{b_1^j b_2^j \dots b_{r_j}^j}$ pour tout j, on trouve

$$\begin{aligned} S(P(10^k)) &\geqslant S(c_{i+1}10^{i+1} - |c_i|10^i) \\ &= S\left(\overline{b_1^{i+1}b_2^{i+1}\dots b_{r_{i+1}}^{i+1}}\ \underbrace{9\dots9}_{k-r_i \text{ chiffres}}\ \overline{(9-b_1^i)(9-b_2^i)\dots(9-b_{r_i})}\right) \\ &\geqslant 9(k-r_i). \end{aligned}$$

Mais alors $P(S(10^k)) = 1 \geqslant 9(k-r_i)$, ce qui est absurde. Ainsi, tous les coefficients de P sont positifs.
On recommence cette fois-ci avec $n = 9 \times 10^k$. Là aussi, en prenant k suffisamment grand,

$$P(9\times 10^k) = \overline{9^d c_d}0\dots0\overline{9^{d-1}c_{d-1}}0\dots0\dots\dots\overline{9c_1}0\dots0\overline{c_0},$$

de sorte que

$$9^d c_d + \dots + c_0 = P(9) = P(S(9\times 10^k)) = S(P(9\times 10^k)) = S(9^d c_d) + \dots + S(c_0).$$

Sachant que $S(m) \leqslant m$ avec égalité seulement si $m \leqslant 9$, on trouve que $S(9^i c_i) = 9^i c_i$ pour tout i et que $9^d c_d \leqslant 9$, si bien que $d \leqslant 1$.
Si $d = 1$, comme $9c_1 \leqslant 9$, $c_1 = 1$. L'égalité devient $S(n + c_0) = S(n) + c_0$. Prenons alors $n = 10^k + 10 - c_0$, l'égalité donne $2 = S(n + c_0) = 1 + 10 - c_0 + c_0 = 11$, ce qui est absurde.
Ainsi $d \leqslant 0$ et P est constant, ce qui nous ramène au cas traité plus haut.

Les seules solutions sont les polynômes constants égaux à un nombre compris entre 1 et 9.

Exercice 4.82. Montrer qu'il existe une infinité de paires (m, n) d'entiers distincts telles que $m!n!$ est un carré parfait.

Solution 4.82. Soit $a \geqslant 2$ un entier. En prenant $(m, n) = (a^2, a^2 - 1)$, on a $m!n! = (n+1)n!n! = a^2(a^2-1)^2$, qui est bien un carré parfait.

Exercice 4.83. (Roumanie MO SL 2023) Montrer qu'il existe une infinité d'entiers x tels que $x + S(x)$ est un carré parfait, où $S(x)$ désigne la somme des chiffres de x.

Solution 4.83. Il suffit de choisir un $x + S(x)$ de la forme $(10^k + m)^2$, Cela revient à choisir x de la forme $x = 10^{2k} + 2a\cdot 10^k + b$ et à bien choisir a et b. On a $S(x) = 1 + 2a + b$, donc a et b doivent vérifier $1 + 2a + 2b + b = a^2$.
Après calculs, le nombre $x = (10^k + 3)^2 - 8 = 10^{2k} + 6 \cdot 10^k + 1$ pour $k \geqslant 1$ quelconque vérifie $S(x) = 8$ donc $x + S(x) = (10^k + 3)^2$, comme voulu.

Exercice 4.84. (Estonie 2023 TST) Deux entiers m et n distincts sont dits *amis* si $n - m$ divise m et n. Montrer que, pour tout entier $k \geqslant 1$, il existe k entiers distincts tels que deux quelconques d'entre eux sont toujours amis.

Solution 4.84. Appelons un ensemble d'entiers *amical* si deux entiers quelconques sont toujours amis. On construit un ensemble amical de taille k par récurrence sur k.

➢ **Commentaire :**

> Pour un tel problème, une question très pertinente est de se demander "si E est amical, quels autres ensembels sont amicaux". Ici, on remarque que si $E = \{a_1, \dots, a_k\}$ est amical, alors $\{aa_1, \dots, aa_k\}$ est également amical (dilatations de E). On peut aussi chercher les translations de E et les t tels que $\{a_1 + t, \dots, a_k + t\}$ est amical. Une condition simple est par exemple que t soit multiple de $\prod_{i\neq j} |a_i - a_j|$. Pour trouver la récurrence, on essaye de greffer un nouveau nombre à chacune des deux transformations de E.

Initialisation : Si $k = 1$, le résultat est clair. Pour $k = 2$, on peut prendre 2 et 4.

Hérédité : Supposons que l'on dispose dispose d'un ensemble amical pour $k \geqslant 2$ un entier fixé. Notons $E = \{a_1, \dots, a_k\}$ cet ensemble et notons $P = \prod_{i\neq j} |a_i - a_j|$. On remarque alors que l'ensemble $E_\ell = \{a_1 + \ell P, \dots, a_k + \ell P\}$ est également amical pour tout entier $\ell \geqslant 1$. L'idée est de rajouter un nouvel élément à un ensemble E_ℓ pour ℓ bien choisi.

Posons $\ell = \prod_{i=1}^{k} a_i$, prenons $\boxed{a_{k+1} = \ell \times P}$ et montrons que $E' = \{a_1+\ell P, \ldots, a_k+\ell P, P\}$ est amical. Prenons deux indices i et j distincts.

- ➢ Si $i, j \leqslant k$, alors on a déjà $a_i + \ell P - (a_j + \ell P) = a_i - a_j$, qui divise a_i et a_j par hypothèse de récurrence et qui divise P, et divise donc chacun des nombres $a_i + \ell P$ et $a_j + \ell P$.
- ➢ Si $j = k+1$, on a $a_i + \ell P - a_{k+1} = a_i$, qui divise ℓ donc il divise bien $a_i + \ell P$ et a_{k+1}.

L'ensemble E' est donc bien amical, ce qui achève la récurrence.

Remarque : Une forme très proche de cet exercice et de sa solution apparaît dans la Shortlist JBMO 2025, au numéro N3.

Exercice 4.85. (Polish MO 2016 round 2 P4) Soit $k \geqslant 1$ un entier. Montrer qu'il existe un entier $n \geqslant 1$ tels que les deux ensembles $A = \{1^2, 2^2, 3^2, \ldots\}$ et $B = \{1^2 + n, 2^2 + n, 3^2 + n, \ldots\}$ ont exactement k termes en commun.

Solution 4.85. Commençons par regarder les propriétés d'un entier n tel que les ensembles A et B ont un élément en commun.
Fixons un entier n quelconque et supposons qu'il existe un entier x appartenant à A et à B. On dispose donc de deux entiers a et b tels que $a^2 = b^2 + n$. Puisque n est strictement positif, $a^2 > b^2$, donc $a > b$. En réarrangeant l'égalité, on trouve

$$n = a^2 - b^2 = (a-b)(a+b).$$

On déduit que $a - b$ et $a + b$ sont nécessairement des diviseurs de n.

Notons également que $a - b$ et $a + b$ sont des diviseurs de même parité, puisque leur différence vaut $2b$ qui est paire.

Réciproquement, si $d \leqslant \sqrt{n}$ est un diviseur de n tel que n/d est de même parité que d, alors les nombres $a = \dfrac{d + n/d}{2}$ et $b = \dfrac{n/d - d}{2}$ vérifient le système

$$\begin{cases} a+b &= \frac{n}{d} \\ a-b &= d \end{cases}$$

de sorte que $n = (a+b)(a-b) = a^2 - b^2$ et l'élément a^2 appartient aux ensembles A et B.

Ainsi, il suffit de trouver un entier n ayant exactement 2024 diviseurs $d \leqslant \sqrt{n}$ tels que d et n/d sont de même parité.

Une façon simple de créer un entiers avec un nombre fixé de diviseurs est de considérer une puissance d'un nombre premier : si p est un nombre premier, les seuls diviseurs de p^k sont les $k+1$ nombres $1, p, \ldots, p^k$. Utilisons cette idée pour construire l'entier n.

Montrons alors que $n = 3^{4048}$ vérifie la propriété de l'énoncé. Soit x un entier appartenant à A et B. Il existe alors deux entiers a et b tels que $a^2 = n + b^2 = x$. On déduit que $3^{4048} = a^2 - b^2 = (a-b)(a+b)$. On a alors k entier tel que $a - b = 3^k$ et $a + b = 3^{4048-k}$. Comme $a - b < a + b$, on a $k < 4048 - k$, de sorte que $0 \leqslant k \leqslant 2023$. En résolvant le système

$$\begin{cases} a+b &= 3^{4048-k} \\ a-b &= 3^k \end{cases}$$

on trouve $a = \dfrac{3^{4048-k} + 3^k}{2}$ et $b = \dfrac{3^{4048-k} - 3^k}{2}$, de sorte que $x = \left(\dfrac{3^{4048-k} + 3^k}{2}\right)^2$. Les seuls éléments qui sont en commun aux ensembles A et B sont de cette forme.

Réciproquement, les 2024 entiers de la forme $x = \left(\dfrac{3^{4048-k} + 3^k}{2}\right)^2 = 3^{4048} + \left(\dfrac{3^{4048-k} - 3^k}{2}\right)^2$ pour $k = 0, 1, \ldots, 2023$ appartiennent aux ensembles A et B.

Exercice 4.86. Soit $n \geqslant 1$ un entier. Dans une classe de n élèves numérotés de 1 à n, certains élèves sont amis de façon réciproque. Peut-on toujours trouver un entier $N \geqslant 1$ et n entiers $a_1, \ldots, a_n$ tels que les élèves numéros i et j sont amis si et seulement si N divise $a_i a_j$?

Solution 4.86. Le point de vue graphe est bien sûr le bienvenu ici. On introduit G le graphe dont les sommets sont les élèves et où deux élèves i et j sont reliés si ils **ne** sont **pas** amis. Pour chaque arête (i, j) on choisit un nombre premier $p_{i,j}$.

On pose N le produit des $p_{i,j}$ et on pose a_i le produit des $p_{j,k}$ tels que j et k sont distincts de i, autrement dit le produit des nombres premiers associés à des arêtes ne concernant pas le sommet i.

Si deux élèves i et j ne sont pas amis, alors $p_{i,j}$ ne divise pas $a_i a_j$ donc N non plus. Si i et j sont amis, alors chaque $p_{\ell,k}$ divise au moins l'un de a_i et a_j car l'un au moins des deux sommets n'est pas extrémité de l'arête (ℓ, k).

Notre entier N et nos entiers a_i satisfont donc l'énoncé.

Exercice 4.87. (TST Suisse 2022) Soit n un entier strictement positif. Montrer qu'il existe une suite finie S de 0 et de 1 telle que, pour tout entier $d \geqslant 2$, le nombre dont l'écriture en base d correspond à la suite S est non nul et divisible par n.

Solution 4.87. On note $\overline{a_0 a_1 \ldots a_k}^d$ l'entier $a_0 d^k + \ldots + a_{k-1} d^1 + a_k$, correspondant à l'écriture de l'entier dans la base d.

Soit d un entier fixé. D'après le principe des tiroirs, parmi les $n+1$ nombres

$$\overline{1}^d, \overline{11}^d, \ldots, \overline{\underbrace{11\ldots1}_{n+1}}^d,$$

il en existe deux avec le même reste modulo n. Leur différence s'écrit alors

$$\overline{\underbrace{11\ldots1}_{a}\underbrace{0\ldots0}_{b}}^d = d^{a+b-1} + d^{a+b-2} + \ldots + d^b,$$

où $a \leqslant n$.

➢ **Commentaire :**

> Le seul ennui est que les entiers a et b dépendent de l'entier d.
>
> On ne peut pas laisser tomber pour autant cette bonnée idée, il faut seulement l'adapter pour trouver un nombre de la même forme mais dont les paramètres a et b ne dépendent pas de d, en cherchant des bon multiples du nombre ci-dessus. Par exemple, multiplier par d le nombre ci-dessus correspond à lui ajouter un 0 dans son écriture décimale. Dans ce cas, la somme de nombres de la forme $\overline{\underbrace{11\ldots1}_{a \text{ chiffres}}\underbrace{0\ldots0}_{}}^d$ avec un nombre variable de 0 est également un multiple de n. Il suffit de bien choisir cette somme.

L'entier n divise également tous les multiples de ce nombre, et donc en particulier les nombres de la forme $d^k \cdot (d^{a+b-1} + d^{a+b-2} + \ldots + d^b) = \overline{11\ldots1\underbrace{0\ldots0}_{b+k}}^d$. Par somme, pour tout entier k, l'entier n divise également le nombre

$$\overline{\underbrace{11\ldots1}_{a}\underbrace{0\ldots0}_{n}}^d + \overline{\underbrace{11\ldots1}_{a}\underbrace{0\ldots0}_{n+a}}^d + \ldots + \overline{\underbrace{11\ldots1}_{a}\underbrace{0\ldots0}_{n+ka}}^d = \overline{\underbrace{11\ldots1}_{ka}\underbrace{0\ldots0}_{n}}^d$$

Comme $a \leqslant n$, a divise $N = \mathrm{PPCM}(1, \ldots, n)$. On déduit que

$$n \mid \overline{\underbrace{11\ldots1}_{N}\underbrace{0\ldots0}_{n}}^d \quad \forall d \geqslant 1.$$

Ainsi, la suite $\boxed{S = \underbrace{11\ldots1}_{N}\underbrace{0\ldots0}_{n}}$ convient.

Solution alternative

Dans le cas où d est premier avec n, on a $d^{\varphi(n)} \equiv 1 \mod n$, donc

$$S_d = d^{\varphi(n)} + d^{2\varphi(n)} + \ldots + d^{n\varphi(n)} \equiv n \equiv 0 \mod n,$$

donc le nombre $\boxed{\overline{\underbrace{10\ldots0}_{\varphi(n)}10\ldots0\ldots10\ldots0}^{d}}$ formé de n blocs est divisible par n.

Il faut alors adapter cet argument dans le cas où d n'est pas premier avec n. En réalité, dans ce cas là, le nombre ci-dessus est également divisible par n. En effet, posons a le plus grand diviseur de n dont tous les facteurs premiers divisent d et posons $b = n/a$. L'entier b est alors premier avec a. Pour tout nombre premier p divisant a (et donc a fortiori d), comme $\alpha \leqslant p^{\alpha-1}(p-1)$, on a $v_p(n) \leqslant \varphi(n)$. Il vient que $a \mid d^{\varphi(n)}$ et donc $a \mid S_d$. D'autre part, l'entier b est premier avec $d^{\varphi(n)}$, d'où $d^{\varphi(n)} \equiv 1 \mod b$ et, de même que plus haut, on trouve que $b \mid S_d$. Ainsi, on déduit que $ab \mid S_d$.

En conclusion, la suite $S = \underbrace{10\ldots0}_{\varphi(n)}10\ldots0\ldots10\ldots0$ convient.

Exercice 4.88. (RMM 2015 P1) Existe-t-il une suite infinie d'entiers strictement positifs $a_1, \ldots$ telle que a_m et a_n sont premiers entre eux si et seulement si $|m-n| = 1$?

Solution 4.88. Encore une fois par un algo glouton, mais qui nécessite de la préparation en amont. Pour se simplifier la vie, on va choisir nos termes comme des produits de facteurs premiers distincts.

Tout comme dans l'exercice précédent, on va raisonner sur deux étages. On se donne deux familles (p) et (q) de nombres premiers, et on cherche une suite avec cette tête :

$$\prod p_i \qquad \prod p_i \qquad \prod p_i \qquad \prod p_i$$
$$\prod q_i \qquad \prod q_i \qquad \prod q_i$$

Avec cette construction, malheureusement, deux membres de deux étages différents sont premiers entre eux. Il faudrait donc multiplier les membres du premier étage par un facteur q, et inversement. Comme suit

$$q_1 \prod p_i \qquad q_2 \prod p_i \qquad q_3 \prod p_i \qquad q_4 \prod p_i$$
$$p_1 \prod q_i \qquad p_2 \prod q_i \qquad p_3 \prod q_i$$

Le problème, c'est qu'alors deux nombres consécutifs ne sont plus forcément premiers entre eux. On pourrait ajuster les indices, mais en essayant on voit qu'il va falloir organiser un "roulement" des facteurs p et des facteurs q présents à chaque étage. Ceci motive la construction suivante :

$$c_{n+1}b_{n+1}\prod^{n} a_k b_k \qquad c_{n+2}b_{n+2}\prod^{n+1} a_k b_k$$
$$d_{n+1}a_{n+1}\prod^{n} c_k d_k \qquad d_{n+2}a_{n+2}\prod^{n+1} c_k d_k$$

Exercice 4.89. (BMO 2018 SL N1) Pour tous entiers strictement positifs m et n, on note $d(m,n)$ le nombre de nombres premiers distincts divisant à la fois m et n. Par exemple $d(60,126) = d(2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 7) = 2$. Existe-t-il une suite (a_n) d'entiers strictement positifs telle que

- $a_1 \geqslant 2018^{2018}$,
- $a_m \leqslant a_n$ pour tous entiers $m \leqslant n$,
- $d(m,n) = d(a_m, a_n)$ pour tous entiers m et n distincts ?

Solution 4.89. **Réponse :** Une telle suite existe.

➢ Commentaire :

> On peut commencer par vouloir renuméroter les nombres premiers : on note $(p_i)_i$ la suite des nombres premiers et on introduit $2018^{2018} < q_1 < q_2 < \dots$ la suite croissante des nombres premiers supérieurs à 2018^{2018} et on souhaiter envoyer $\prod p_i^{\alpha_i}$ sur $\prod q_i^{\alpha_i}$.
>
> Toutefois, cette construction ne respecte pas la condition de croissance de la suite (a_n). Il faut donc également modifier les exposants α_i.

On note $(p_i)_i$ la suite des nombres premiers et on introduit $2018^{2018} < q_0 < q_1 < q_2 < \dots$ la suite croissante des nombres premiers supérieurs à 2018^{2018}. On construit la suite (a_n) par récurrence.

On pose $a_1 = q_0$. Puis, pour tout entier n, en supposant construits $a_1, \dots, a_n$ satisfaisant les deux dernières conditions, on construit a_{n+1} comme suit : si $n+1 = \prod_{j=1}^{r} p_{i_j}^{\alpha_j}$, alors

$$a_{n+1} = \prod_{j=1}^{r-1} q_{i_j}^{\alpha_j} \times q_{i_r}^{\beta_r},$$

où β_r est choisi suffisamment grand pour que $a_{n+1} > a_n$.

On vérifie que, pour tout $m \leqslant n$,

$$d(a_m, a_{n+1}) = |\{q \text{ premiers}, q \mid a_m \text{ et } q \mid a_{n+1}\}| = |\{p \text{ premiers}, p_i \mid m \text{ et } p \mid n+1\}| = d(m, n+1).$$

La suite (a_n) ainsi construite satisfait donc bien les conditions de l'énoncé.

Exercice 4.90. (OFM 2023 senior) Existe-t-il des entiers a et b tels que, parmi les entiers $a, a+1, \dots, a+2023, b, b+1, \dots, b+2023$, aucun entier n'en divise un autre, mais

$$a(a+1)\dots(a+2023) \mid b(b+1)\dots(b+2023).$$

Solution 4.90.

➢ Commentaire :

> Le plus dur dans l'exercice est d'établir le cahier des charges précis. Pour chaque condition, on trouve une manière d'imposer que cette condition soit satisfaite, puis on combine le tout avec le théorème des restes chinois, indiquant qu'il existe des entiers a et b respectant simultanément toutes les conditions.
>
> - ➢ Pour que $a+i$ ne divise pas $a+j$, il suffit que $a+i$ ne divise pas $|i-j|$. Il suffit donc que $a \geqslant 2024$, de sorte que $a+i > |i-j|$.
> - ➢ Pour que $a+i$ ne divise aucun $b+j$, il faut trouver un nombre premier p tel que $p \mid a+i$ mais p ne divise pas $b+j$.
> - ➢ Pour que $A = a(a+1)\dots(a+2023)$ divise $B = b(b+1)\dots(b+2023)$, il faut tout de même que les diviseurs premiers des $a+i$ divisent l'un au moins des $b+j$. On peut donc modifier l'idée précédente, et construire a et b de sorte que, pour toute paire (i,j), il existe un facteur $p_{i,j}$ divisant $a+i$ et $b+j$ mais ne divisant aucun des autres facteurs $b+k$. Cela garantit que $a+i$ ne divise pas $b+k$ quels que soient i et k.
>
> La difficulté pour réaliser la troisième condition est qu'on ne contrôle à priori pas les facteurs premiers de $a(a+1), \dots (a+2023)$ autres que les $p_{i,j}$. On pourrait donc décréter qu'on choisit b tel que b est divisible par tous les autres diviseurs premiers de $a\dots(a+2023)$. Ce choix ne permet pas de vérifier que $v_p(A) \leqslant v_p(B)$ pour les facteurs premiers évoqués dans la condition 2. Le plus simple est donc de s'arranger pour que $v_p(a+i) = 1$ pour tous les facteurs premiers choisis dans la condition 2.

Soit $(p_{i,j})_{1 \leqslant i,j \leqslant 2023}$ un ensemble de 2024^2 facteurs premiers, tous supérieurs ou égaux à 2024.

D'après le théorème des restes chinois, il existe un entier a vérifiant les 2024^2 équations modulaires suivantes

$$a \equiv p_{i,j} - i \mod p_{i,j}^2, \quad \text{pour tout } 0 \leqslant i,j \leqslant 2023.$$

Cela garantit notamment que $v_{p_{i,j}}(a+i) = 1$ pour tout (i,j) (c'est la même idée que pour le problème 5 des Olympiades Internationales 1989, proposé dans la section sur le théorème des restes chinois). On a aussi que $p_{i,j}$ divise $a+i$ mais aucun autre $a+k$ pour $k \neq i$. En effet, si c'était le cas, on aurait $p_{i,j} \mid a+k-(a+i) = k-i$, ce qui est absurde puisque $0 < |k-i| \leqslant 2023 < p_{i,j}$. En particulier, $a+i$ ne divise jamais $a+k$ pour $k \neq i$.

Posons à présent

$$C = \frac{a(a+1)\dots(a+2023)}{\prod_{0 \leqslant i,j \leqslant 2023} p_{i,j}}.$$

Puisque $v_{p_{i,j}}(a+i) = 1$ et que $p_{i,j}$ ne divise pas les autres facteurs, le nombre C est premier avec $\prod_{0 \leqslant i,j \leqslant 2023} p_{i,j}$.

On choisit désormais b un entier supérieur à $a+2023$ et vérifiant $b \equiv 0 \mod C$ et

$$b \equiv p_{i,j} - j \mod p_{i,j}^2, \quad \text{pour tout } 0 \leqslant i,j \leqslant 2023,$$

dont l'existence est donnée par le théorème des restes chinois. Une fois de plus, $p_{i,j} \mid b+j$ mais ne divise aucun des autres facteurs $b+k$. Puisqu'en plus C divise b, on déduit que $a(a+1)\dots(a+2023) = C\prod_{0 \leqslant i,j \leqslant 2023} p_{i,j}$ divise $b(b+1)\dots(b+2023)$.

Enfin, pour deux entiers i et j, pour tout entier $k \neq j$, on a $p_{i,k}$ qui divise $a+i$ mais pas $b+j$, donc $a+i$ ne divise pas $b+j$ (et on a bien sûr $b+j > a+i$ donc $b+j$ ne divise pas $a+i$).

Ceci conclut le résultat annoncé.

Exercice 4.91. (Iran TST 2012) Soit $t > 0$ un entier. Montrer qu'il existe un entier $n > 1$, premier avec t tel qu'aucun des termes de la suite $n+t, n^2+t, n^3+t, \dots$ ne soit une puissance parfaite.

Solution 4.91. Oublions premièrement la condition que n doit être premier à t. Si, pour un entier N, on choisit $n \equiv 1 \pmod N$, on a $n^k + t \equiv t+1 \mod N$ pour tout k. En particulier, si $N = (t+1)^2$, on sait que pour tout $p \mid t+1$ premier, $v_p(n^k+t) = v_p(t+1)$. Cela signifie qu'on contrôle très bien les valuations $p-$adiques

des $n^k + t$, au moins pour les p qui divisent $t+1$. En particulier, si $t+1$ n'est pas une puissance, le problème est résolu.

Si $t+1$ est une puissance $\ell-$ième (mais pas une puissance $m-$ème pour $m > \ell$), alors si un terme $n^k + t$ est une puissance, ça doit être une puissance $d-$ième pour un diviseur d de ℓ.

Si de plus, n était une puissance ℓ-ième, on aurait que $n^k + t$ devrait être une puissance $d-$ème à distance t de la puissance $d-$ème n^k. Si finalement $\sqrt[\ell]{n} \geq t$, on aurait une contradiction puisque pour tout $x > 0$, $(x+1)^d > x^d + x$ et que donc, avec $x = \sqrt[d]{n} > t$, on aurait que $n^k + t$ est encadré entre deux puissances $d-$ème.

On cherche donc un entier n, premier à t, congru à 1 modulo $(t+1)^2$, et qui est une puissance $\ell-$ème d'un entier au moins égal à t. Il suffit de choisir $\boxed{n = (1 + t(t+1)^2)^\ell}$.

Exercice 4.92. (MEMO 2021) Montrer qu'il existe une infinité d'entiers n tels que l'écriture de n^2 en base 4 ne contient que des 1 et des 2.

Solution 4.92. On montre un résultat un peu plus fort, qui se prête mieux à un raisonnement par récurrence : il existe une infinité d'entiers n tels que l'écriture de n^2 en base 4 ne contient que des 1 et des 2, et tels que le premier et le dernier chiffre de l'écriture en base 4 de n^2 vaut 1. Un premier exemple est le nombre $5^2 = 25 = 121_4$. Ensuite, on montre que si l'on a un tel n, on peut en construire un nouveau qui lui est strictement supérieur, ce qui montrera bien qu'il existe une infinité d'entiers ayant la propriété recherchée.
Soit donc n tel que l'écriture de n^2 en base 4 ne contient que des 1 et des 2, et commence et se termine par un 1. On suppose que cette écriture contient k chiffres. On pose alors $m = 2^{2k-1} \cdot n + n$. On a

$$m^2 = 4^{2k-1} \cdot n^2 + 4^k \cdot n^2 + n^2$$

En base 4, m^2 est donc constitué de trois copies de n^2, avec n^2 et $4^k \cdot n^2$ qui sont deux copies disjointes adjacentes, et $4^{2k-1} \cdot n^2$ et $4^k \cdot n^2$ qui ont exactement une puissance de 4 en commun dans leur écriture, à savoir 4^{2k-1}. Mais par hypothèse, les coefficients devant 1 et devant 4^{k-1} de n^2 sont des 1, donc le coefficient devant 4^{2k-1} de m^2 est un 2. En outre, tous les autres coefficients de l'écriture en base 4 de m^2 apparaissaient dans celle de n^2, et sont donc bien des 1 ou des 2. Enfin, les premiers et derniers coefficients de l'écriture en base 4 de m^2, à savoir les coefficients devant 4^0 et 4^{3k-2}, sont bien des 1 par hypothèse de récurrence.

Exercice 4.93. (BXMO 2020) Existe-t-il un entier n admettant exactement 2020 diviseurs d tels que $\sqrt{n} < d < 2\sqrt{n}$?

Solution 4.93. Première idée : 3^{2019} a exactement 2020 diviseurs (impairs, c'est important pour la suite).

Deuxième idée : Si n n'est pas un carré et est divisible par 2^x avec x "grand", pour tout diviseur impair $d < 2\sqrt{n}$, il existe un unique entier $0 \leq y \leq x$ avec $\sqrt{n} < 2^y d < 2\sqrt{n}$ et ces différents d donnent des différents $2^y d$. De plus, chacun des diviseurs entre $\sqrt{n}$ et $2\sqrt{n}$ est de cette forme.

Troisième idée : combiner les deux idées !

Prenons $n = 2^{42^{42}} \times 3^{2019}$. Puisque 2019 est impair, n n'est pas un carré, et n a exactement 2020 diviseurs impairs inférieurs à $2\sqrt{n}$ car $3^{2019} < 2^{42^{42}/2+1} \times 3^{2019/2} = 2\sqrt{n}$. De plus, pour chacun de ces diviseurs d il existe un unique entier $y \leq 42^{42}$ qui vérifie $\sqrt{n} < 2^y d < 2\sqrt{n}$; en effet, cela résulte de $2^{42^{42}} > 2^{42^{42}/2} \times 3^{2019/2} = \sqrt{n}$. Cela conclut.

Exercice 4.94. (Balkan MO SL 2025 N3) Étant donné un entier $k \geqslant 1$, on dit qu'un couple (a, b) d'entiers strictement positifs est $k-$sympa si $a \mid b^k + 1$ et $b \mid a^k + 1$.
Déterminer les entiers k pour lesquels il existe une infinité de couples $k-$sympas.

Solution 4.94. **Réponse :** Tous les entiers $k \geqslant 2$.

Supposons $k = 1$. Soit (a, b) un couple $1-$sympa. Puisque $a \mid b + 1$, on a $a \leqslant b + 1$. Puisque $b \mid a + 1$, on a $b - 1 \leqslant a \leqslant b + 1$. Si $a = b - 1$, alors $b - 1 \mid b + 1$ donc $b - 1 \mid 2$ et $b = 2$ ou 3. Si $a = b$, alors $b \mid b + 1$ et $b = 1$. Si $a = b + 1$, alors $b \mid b + 2$ d'où $b \mid 2$ et $b = 1, 2$. Dans tous les cas, on trouve que $a, b \leqslant 3$. Il y a donc un nombre fini de couples $1-$sympas.

Soit $k \geqslant 2$ un entier. Montrons qu'il y a une infinité de couples (a, b) qui sont $k-$sympas. Supposons en avoir construit un (a, b) tel que $a < b$ et construisons en un nouveau à partir de là. On dispose donc d'un entier c tel

que $b^k+1=ac$. Un peu à la manière du Vieta jumping, on considère le couple $\boxed{(c,b)=\left(\frac{b^k+1}{a},b\right)}$ et on montre qu'il est sympa.

On a déjà que $c \mid b^k+1$. D'autre part, puisque b et a sont manifestement premiers entre eux et puisque $a^k+1 \mid b$, on a

$$c^k+1=\left((b^k+1)a^{-1}\right)^k+1 \equiv (1\cdot a^{-1})^k+1 \equiv \frac{1}{a^k}+1 \equiv \frac{a^k+1}{a^k} \equiv 0 \mod b.$$

Le couple (c,b) est donc $k-$sympa. De plus, $c=\dfrac{b^k+1}{a} \geqslant \dfrac{b^2}{a} > b$, le couple (c,b) est bien distinct du couple (a,b). On construit ainsi une infinité de couples k-sympas, comme voulu.

Exercice 4.95. (Iran TST 2021 P4) Pour tout entier $n \geqslant 1$, on note $\Omega(n)$ le plus grand facteur premier de n et $\omega(n)$ le plus petit facteur premier de n (avec la conventien $\Omega(1)=\omega(1)=1$). Alice et Bob jouent au jeu suivant : Alice commence par choisir 1400 polynômes à coefficients entiers. Bob les répartit ensuite en deux ensembles A et B. Bob gagne le jeu si, pour tout entier $n \geqslant 2$,

$$\max_{P\in A}(\Omega(P(n))) \geqslant \min_{P\in B}(\omega(P(n))).$$

Lequel des deux joueurs possède une stratégie gagnante ?

Solution 4.95.

La réalisation suivante est dûe à Antoine Derimay. Montrons que c'est Alice qui dispose d'une stratégie gagnante.

Lemme : Soit m un entier, et $a_i, 1 \leqslant i \leqslant m$ des entiers tels que les a_i ne prennent qu'une seule valeur modulo $m!$. Alors le polynôme P interpolateur de degré $m-1$ tel que $P(i)=a_i$ pour tout $1 \leqslant i \leqslant m$ est à coefficients entiers.

Preuve : Commençons par considérer le cas où $m! \mid a_i$. Pour $i \in [\![1,m]\!]$, on pose$L_i=\dfrac{\prod_{j\neq i} X-j}{\prod_{j\neq i} i-j}$. On a (au signe près) $\prod_{j\neq i} i-j=(j-1)!(m-j)!$, donc $\dfrac{m!}{\prod_{j\neq i} i-j}=m\binom{m-1}{j}$ (toujours au signe près). En particulier, $m!L_j$ est à coefficients entiers. Ainsi, puisqu'on a $P=\sum a_iL_i$, le polynôme P est également à coefficients entiers. Pour le cas général, mettons qu'on a $a_i=N \pmod{m!}$. On applique le résultat à $b_i=a_i-N,$, on obtient alors un polynôme P tel que $P(i)=b_i$ pour tout i, et le polynôme $P+N$ convient alors. □

Posons $n=700$ et $m=(2n)!$. D'après le principe des tiroirs, il existe une infinité de nombres premiers ayant le même reste N modulo $m!$. Posons $p_1,\dots,p_{2n}$ les $2n$ plus petits tels nombres dans l'ordre croissant.

Soit $\mathcal{S}_{2n}$ l'ensemble des permutations de $[\![1,2n]\!]$, et soit f une bijection de $[\![1,m]\!]$ vers $\mathcal{S}_{2n}$. Pour $i \leqslant 2n$, on définit le polynôme P_i comme étant le polynôme tel que $P_i(j)=p_{f(j)(i)}$ pour tout $1 \leqslant j \leqslant m$. D'après le lemme, puisque les p_k sont tous congrus à $N \pmod{m!}$, les P_i sont à coefficients entiers.

Soit à présent E un sous-ensemble de $[\![1,2n]\!]$ de cardinal n. Il existe une permutation $\sigma \in S_{2n}$ telle que $\sigma(E)=[\![1,n]\!]$ (et donc $\sigma([\![1,2n]\!]\setminus E)=[\![n+1,2n]\!]$). Si Bob venait à choisir les polynômes P_i, $i\in E$, on aurait alors

$$\max_{i\in E}\Omega(P_i(f^{-1}(\sigma))) = \max_{i\in E}\Omega(p_{\sigma(i)}) = \max_{i\in E} p_{\sigma(i)} = \max_{i\in\sigma(E)} p_i = p_n,$$

et de même,

$$\min_{i\notin E}\omega(P_i(f^{-1}(\sigma))) = p_{n+1},$$

si bien que $\max_{i\in E}\Omega(P_i(k)) < \min_{i\notin E}\omega(P_i(k))$ pour $k=f^{-1}(\sigma)$. Ainsi, Alice gagne si Bob choisit le sous-ensemble E. Ceci étant bien sûr vrai pour tout sous-ensemble E, Alice est sûre de gagner, c'est donc bien Alice qui a une stratégie gagnante.

Solution alternative

La solution suivante, très astucieuse a été proposée par Vincent Jugé.

Notons $M = \binom{1400}{700}$ et notons $\mathcal{P}_1, \dots, \mathcal{P}_M$ les partitions de $\{1, \dots, 1400\}$ en deux ensembles de même cardinal. Prenons également des entiers $a_1, \dots, a_M$ deux à deux distincts. Alice choisit les 1400 polynômes $P_1, \dots, P_{1400}$ de la façon suivante :

$$P_k(X) = 1 + 3 \prod_{i \in [\![1,1400]\!],\quad k \in \mathcal{P}_i} (X - a_i).$$

Laissons maintenant Bob choisir une partition de l'ensemble des polynômes en deux sous-ensembles A et B. Notons $A' = \{i \in [\![1, 1400]\!], P_i \in A\}$ et $B' = \{i \in [\![1, 1400]\!], P_i \in B\}$. Soit n l'entier tel que $\mathcal{P}_n = A' \sqcup B'$. Alors on vérifie que, d'après la définition de chaque polynôme, pour tout $k \in A'$, $P_k(n) = 1$ et pour tout $k \in B'$, $P_k(n) \neq 1$ et $P_k(n) \equiv 1 \mod 3$, de sorte que $|P_k(n)| > 1$ admet un facteur premier. Ainsi,

$$\max_{P \in A} \Omega(P(n)) = 1 < \min_{P \in B} \omega(P(n)).$$

Comme cette inégalité est vraie quelle que soit la partition choisie par Bob, cela assure sa défaite.

Exercice 4.96. (USA TST 2015 Decembre P2) Montrer que, pour tout entier $n \geqslant 1$, il existe un ensemble S de n entiers strictement positifs, tel que, pour tous $a, b \in S$ distincts, $a - b$ divise a et b mais aucun autre élément de S.

Solution 4.96. On procède par récurrence sur la taille n de S.

Initialisation : Si $n = 1$, il n'y a rien à faire.

Hérédité : On suppose avoir construit un ensemble S de taille n vérifiant la condition, avec $n \geqslant 1$ fixé. On note $S = \{a_1, \dots, a_n\}$.

➢ **Commentaire :**

> Tout comme un exercice précédent, on cherche à rajouter un élément à une variante de S. Il faut pour cela chercher des variantes de l'ensemble S qui vérifient la condition.
>
> Par exemple, remarquons que l'ensemble $\{ka_1, ka_2, \dots, ka_n\}$ vérifie également la condition pour tout entier $k \geqslant 1$. De plus, si on pose $P = \text{PPCM}(a_1, \dots, a_n)$, alors l'ensemble $S = \{a_1 + \ell P, \dots, a_n + \ell P\}$ vérifie également la condition.
>
> On veut donc rajouter un nouvel élément $a = x + kP$ à l'ensemble $\{ka_1 + k\ell P, \dots, ka_n + k\ell P\}$ pour des valeurs bien choisies de k et ℓ. Les entiers x, k et ℓ doivent vérifier
>
> - ➢ $x - ka_i \mid ka_i + k\ell P$ pour tout i ($a - b$ doit diviser a pour tous a, b distincts, et cela implique automatiquement que $a - b \mid b$),
> - ➢ $x - ka_i$ ne divise pas $ka_j + k\ell P$ dès que $j \neq i$,
> - ➢ $k(a_i - a_j)$ ne divise pas $x + k\ell P$ pour tous a_i et a_j de S.
>
> Pour que la dernière condition tienne, il suffit d'exiger que x ne soit pas divisible par k. Pour que la condition 2 tienne, il suffit, pour peu que la condition 1 soit vraie, de demander que $x > k \max\{|a_i - a_j|, i \neq j\}$. On a alors que $x - ka_i$ ne divise pas $k(a_i - a_j)$, donc si $x - ka_i \mid ka_i + k\ell P$, $x - ka_i$ ne divise pas $ka_j + k\ell P = (ka_i + k\ell P) + k(a_j - a_i)$.
>
> Enfin, pour que la première condition soit vérifiée, il faut commencer par choisir k et x. L'entier ℓ vérifie alors un système chinois qui a une solution si l'on a bien choisi k et x.

On pose $P = \text{PPCM}(a_1, \dots, a_n)$. Prenons x un grand entier premier avec $2, a_1, \dots, a_n$ et aussi premier avec les $a_i - a_j$ pour $i \neq j$.

Notons que les nombres $x - 2a_i$ sont premiers entre eux deux à deux : si $p \mid x - 2a_i$ et $p \mid x - 2a_j$, alors $p \mid 2(a_i - a_j)$. Si $p = 2$, alors x est pair, ce qui est exclu d'après la construction de x. Sinon, $p \mid a_i - a_j \mid a_i$, donc $p \mid x = (x - 2a_i) + 2a_i$, ce qui est exclu encore. Ainsi, les nombres $x - 2a_i$ sont premiers entre eux deux à deux.

D'après le théorème des restes chinois, il existe un entier ℓ tel que

$$2\ell P \equiv -2a_i \mod x - 2a_i, \quad \text{pour tout } i,$$

en vérifiant en effet que $2P$ est inversible modulo $x - ka_i$.

On a donc $x - 2a_i \mid 2a_i + 2\ell P$ et donc on a aussi $x - 2a_i \mid x + 2\ell P = x - 2a_i + 2a_i + 2\ell P$ pour tout i. De plus, si on avait $x - 2a_i \mid 2a_j + 2\ell P$, alors on aurait $x - 2a_i \mid 2a_j + 2\ell P - (2a_i + 2\ell P) = 2(a_i - a_j)$, mais cette divisibilité est impossible si x est pris suffisamment grand.

Enfin, pour tous i, j distincts, $2a_i - 2a_j$ ne divise pas $x + 2\ell P$ puisque x est impair, mais $2(a_i - a_j) \mid 2a_i + 2\ell P$ pour tout i.

Toutes ces conditions garantissent que l'ensemble $S' = \{a_1 + 2\ell P, a_2 + 2\ell P, \ldots, a_n + 2\ell P, x + 2\ell P\}$ vérifie la condition de l'énoncé. Ceci achève la récurrence.

Poubelle

Exercice 4.97. (IMO SL 2022 N5) Soit $n \geqslant 1$ un entier. Morgane écrit au tableau, en base 10, les nombres $2023, 2023 \times 2, \ldots, 2023 \times n$. Pour tout chiffre c compris entre 1 et 9, elle note alors $\mathsf{d}_c(n)$ le nombre d'apparitions du chiffre c sur le tableau. Par exemple, si $n = 3$, elle écrit les nombres 2023, 4046 et 6069, donc $\mathsf{d}_1(3) = \mathsf{d}_5(3) = \mathsf{d}_7(3) = \mathsf{d}_8(3) = 0$, $\mathsf{d}_3(3) = \mathsf{d}_9(3) = 1$, $\mathsf{d}_2(3) = \mathsf{d}_4(3) = 2$ et $\mathsf{d}_6(3) = 3$; ces neuf nombres prennent donc exactement quatre valeurs.
Démontrer qu'il existe une infinité d'entiers $n \geqslant 1$ pour lesquels les neuf nombres $\mathsf{d}_1(n), \mathsf{d}_2(n), \ldots, \mathsf{d}_9(n)$ prennent exactement deux valeurs.

Solution 4.97. Soit k un multiple de $\varphi(2023)$, soit $\ell = (10^k - 1)/2023$. Nous allons démontrer que ℓ est une solution. Pour ce faire, on introduit l'ensemble

$$\Omega = \{2023n \colon 1 \leqslant n \leqslant \ell\}.$$

Les éléments de Ω décrivent précisément l'ensemble des résidus modulo $10^k - 1$ qui sont des multiples de 2023, chaque résidu étant obtenu exactement une fois. Par conséquent, l'application $\phi \colon x \mapsto 10x$, qui définit une permutation de $\mathbb{Z}/(10^k - 1)\mathbb{Z}$, définit aussi une permutation de l'ensemble des résidus qui sont des multiples de 2023, et induit donc une permutation de Ω lui-même. Concrètement, si l'on écrit les éléments de Ω en base 10 avec k chiffres (quitte à laisser des 0 en apparence inutiles sur la gauche), ϕ envoie $\overline{a_{k-1}a_{k-2}\ldots a_1a_0}^{10}$ sur $\overline{a_{k-2}a_{k-3}\ldots a_1a_0a_{k-1}}^{10}$.
Pour tout chiffre c et tout entier i tel que $0 \leqslant i \leqslant k-1$, on note $\Omega(c, i)$ l'ensemble des éléments de Ω dont le chiffre a_i, de poids 10^i, est égal à c ; on pose abusivement $\Omega(c, k) = \Omega(c, 0)$. Lorsque $0 \leqslant i \leqslant k-1$, la bijection ϕ induit une bijection de $\Omega(c, i)$ vers $\Omega(c, i+1)$. Ainsi, les ensembles $\Omega(c, 0), \Omega(c, 1), \ldots, \Omega(c, k-1)$ sont tous de même cardinal, et

$$\mathsf{d}_c(\ell) = |\Omega(c, 0)| + |\Omega(c, 1)| + \cdots + |\Omega(c, k-1)| = k\,|\Omega(c, 0)|.$$

Or, $\Omega(c, 0)$ est formé des nombres $2023n$ pour lesquels $1 \leqslant n \leqslant \ell$ et $c \equiv 3n \pmod{10}$. Puisque $\ell \equiv -1/3 \equiv 3 \pmod{10}$, on en déduit que $|\Omega(c, 0)|$ vaut $(\ell + 7)/10$ si c vaut 3, 6 ou 9, et vaut $(\ell - 3)/10$ sinon. Cela signifie que les cardinaux $|\Omega(c, 0)|$ prennent exactement deux valeurs lorsque c varie de 1 à 9, et donc que les entiers $\mathsf{d}_c(\ell)$ prennent eux aussi deux valeurs.

Exercice 4.98. (IMO SL 2019 N7) Démontrer qu'il existe un réel $c > 0$ et une infinité d'entiers $n \geqslant 1$ ayant la propriété suivante :

> Il existe une infinité d'entiers naturels que l'on ne peut pas écrire comme une somme d'au plus $cn\ln(n)$ puissances $n^{\text{èmes}}$ deux à deux premières entre elles.

Solution 4.98. Soit $\mathcal{P} = \{p_1, p_2, \ldots, p_a\}$ un ensemble de nombres premiers. Posons $n = \text{PPCM}(p_1 - 1, p_2 - 1, \ldots, p_a - 1)$ et $m = p_1 p_2 \cdots p_a$. Alors, pour tout nombre premier $p \in \mathcal{P}$ et tout entier ℓ :

- ➢ si p divise ℓ, alors $\ell^n \equiv 0 \pmod{p}$;
- ➢ sinon, alors l'ordre de ℓ modulo p divise $p-1$, donc divise n aussi, et $\ell^n \equiv 1 \pmod{p}$.

En particulier, si $\ell_1, \ldots, \ell_b$ sont des entiers deux à deux premiers entre eux, alors $\ell_1^n + \ldots + \ell_b^n \equiv b - 1$ ou $b \pmod{p}$. Par conséquent, et en vertu du théorème Chinois, à chaque entier b, on peut associer un ensemble E_b d'au plus 2^a résidus modulo m, et tel que, quelle que soit la manière de choisir des entiers $\ell_1, \ldots, \ell_b$ deux à deux premiers entre eux, on aura

$$\ell_1^n + \ldots + \ell_b^n \in E_b \pmod{m}.$$

Posons alors $d = \lfloor cn\log_2(n) \rfloor$. Les ensembles $E_1, E_2, \ldots, E_d$ couvrent au plus $2^a d$ résidus modulo m. Par conséquent, si $m > 2^a d$, il existe un résidu modulo m, disons κ, tel que nul entier $k \equiv \kappa \pmod{m}$ n'est égal à une de nos sommes $\ell_1^n + \ldots + \ell_b^n$ lorsque $1 \leqslant b \leqslant d$. Évidemment, si $k \neq 0$, il n'est pas non plus égal à une telle somme telle que $b = 0$. Afin de conclure, il nous suffit donc d'avoir $m > 2^a cn\log_2(n)$, et ce pour une infinité d'entiers n, c'est-à-dire d'ensembles $\mathcal{P}$.

On va alors faire en sorte que nos nombres premiers $p_1, p_2, \ldots, p_a$ soient tous congrus à 1 (mod 6). Pour ce faire, il suffit de poser $p_0 = 6$ puis, pour tout entier $i \geqslant 0$, de poser $q_i = p_0 p_1 \cdots p_i$ et de définir p_{i+1} comme le plus petit facteur premier de $q_i^2 - q_i + 1$. Notons déjà que, ce faisant, les nombres premiers $p_1, \ldots, p_a$ sont deux à deux distincts.

En outre, soit ω l'ordre de q_i modulo p_{i+1}. Comme $q_i^3 + 1 = (q_i + 1)(q_i^2 - q_i + 1)$, c'est que $q_i^3 \equiv -1 \pmod{p_{i+1}}$. Notons ici que, puisque 6 divise q_i, c'est que p_{i+1} est premier avec 6, donc que $q_i^3 \not\equiv 1 \pmod{p_{i+1}}$, et donc que ω divise 6 mais pas 3. De plus, si $\omega = 2$, alors $0 \equiv q_i^2 - q_i + 1 \equiv 2 - q_i \pmod{p_{i+1}}$, donc $3 \equiv 2^2 - 1 \equiv q_i^2 - 1 \equiv 0 \pmod{p_{i+1}}$, ce qui est faux également. On en déduit ainsi, comme prévu, que $\omega = 6$, et donc que $p_{i+1} \equiv 1 \pmod{6}$.

Revenons à notre construction, et posons $r_i = \log_2(p_i)$. On constate ici que $p_{i+1} \leqslant q_i^2 - q_i + 1 \leqslant q_i^2$, donc que $r_{i+1} \leqslant 2(r_0 + r_1 + \ldots + r_i)$. Une récurrence immédiate nous permet d'en déduire que $r_i \leqslant 3^i r_0$ pour tout $i \geqslant 0$, donc que $\log_2(m) = r_1 + \ldots + r_a \leqslant 2r_0 \times 3^a$.

De surcroît, comme 6 divise tous les entiers $p_i - 1$, on sait que

$$6^{a-1} n \leqslant (p_1 - 1)(p_2 - 1)\cdots(p_a - 1) < m.$$

En en déduit tout d'abord que $\log_2(n) \leqslant \log_2(m)$, puis que

$$2^a n\log_2(n) \leqslant 2r_0 n \times 6^a < 12r_0 m.$$

Il ne nous reste donc plus qu'à choisir $c = 1/(12r_0)$ pour conclure.

Solution alternative

Voici une autre manière de choisir l'ensemble $\mathcal{P}$. Soit $t \geqslant 1$ un entier, et puis soit p_1 et p_2 des facteurs premiers respectifs de $2^{2^t} + 1$ et de $2^{2^{t+1}} + 1$. Alors p_1 est impair, donc l'ordre de 2 (mod p_1) n'est pas égal à 2^t mais il divise 2^{t+1}, et il est donc égal à 2^{t+1}, de sorte que $p_1 \equiv 1 \pmod{2^{t+1}}$. De même, 2 est d'ordre $2^{t+2} \pmod{p_2}$, de sorte que $p_1 \neq p_2$ et que $p_2 \equiv 1 \pmod{2^{t+2}}$.

Par conséquent, on a $2^{t+1} n \leqslant (p_1 - 1)(p_2 - 1) < m$ et $\log_2(n) \leqslant 2^t + 2^{t+1} - (t+1) \leqslant 2^{t+2}$, ce qui fait que $2^a n\log_2(n) \leqslant 2^{t+4} n < 8m$, et qu'il suffit donc de choisir $c = 1/8$ pour conclure.

4.5 Autour des diviseurs

Exercice 4.99. (OFM 2024 Senior) Soit p un nombre premier. Déterminer tous les entiers $n \geqslant 1$ avec la propriété suivante : il est possible de partitionner l'ensemble des diviseurs de n en paires (d, d') telles que $d < d'$ et p divise $\left\lfloor \frac{d'}{d} \right\rfloor$.

Solution 4.99. **Réponse :** Il s'agit des multiples de p qui ne sont pas des carrés parfaits.

Soit n un entier vérifiant l'énoncé. Si n est un carré parfait, il admet un nombre impair de diviseurs et donc ceux-ci ne peuvent pas être rangés par paire. De plus, si d est le diviseur apparié avec 1, alors $p \mid \left\lfloor \frac{d}{1} \right\rfloor = d$, donc $\boxed{p \mid n}$.

Réciproquement, prenons un multiple n de p qui n'est pas un carré et montrons qu'il vérifie les conditions. On pose $s = v_p(n) \geqslant 1$.

- Si $v_p(n)$ est impair, on peut poser $v_p(n) = 2k+1$. Notons $a_1, \ldots, a_k$ les diviseurs de n/p^s. Les diviseurs de n sont les nombres de la forme $p^x a_i$ pour $0 \leqslant x \leqslant v_p(n)$. On apparie les diviseurs de n en les paires de la forme $(p^{2j}a_i, p^{2j+1}a_i)$ avec $0 \leqslant j \leqslant k$. Chaque paire vérifie bien la division voulue.
- Si $v_p(n)$ est pair, on peut poser $v_p(n) = 2k$. On dispose toutefois, puisque n n'est pas un carré parfait, d'un nombre premier q tel que $v_q(n) = 2\ell$ est pair. Les diviseurs de n sont les entiers de la forme $p^x q^y d$ avec d divisant $n/p^{v_p(n)}q^{v_q(n)}$, $x \leqslant v_p(n)$ et $y \leqslant v_q(n)$. Pour chaque diviseur d de $n/p^{v_p(n)}q^{v_q(n)}$, on forme les paires suivantes :
  - $(p^{2i-1}q^{2j}d, p^{2i}q^{2j}d)$ pour $1 \leqslant i \leqslant k$ et $j \leqslant \ell$,
  - $(p^{2i}q^{2j+1}d, p^{2i+1}q^{2j+1}d)$ avec $i \leqslant k-1$ et $j \leqslant \ell$,
  - $(q^{2j}d, p^{v_p(n)}q^{2j}d)$ pour $j \leqslant \ell$.

  On vérifie que chaque diviseur appartient à exactement une paire et que chacune d'entre elles vérifient la divisibilité voulue.

Exercice 4.100. (USAMO 2024 P1) Déterminer tous les entiers $n \geqslant 3$ tels que si on note $d_1 < \ldots < d_k$ les diviseurs de $n!$, alors $d_2 - d_1 \leqslant d_3 - d_2 \leqslant \ldots \leqslant d_k - d_{k-1}$.

Solution 4.100. **Réponse :** Les entiers solutions sont $n = 3$ et $n = 4$.

➢ **Commentaire :**

> L'idée est que si d_i, d_{i+1}, d_{i+2} sont des diviseurs consécutifs, alors $n!/d_i, n!/d_{i+1}, n!/d_{i+2}$ sont consécutifs de sens contraire. On a donc l'inégalité
>
> $$\frac{1}{d_{i+1}} - \frac{1}{d_{i+2}} \leqslant \frac{1}{d_i} - \frac{1}{d_{i+1}}.$$
>
> En posant $(d_i, d_{i+1}, d_{i+2}) = (d, d+x, d+x+y)$, avec $y \geqslant x$ par hypothèse, l'inégalité ci-dessus se réécrit $(y-x)d \leqslant x(x+y)$. Pour tenir cette inégalité en échec, il faut donc que $y > x$. Cela revient à considérer l'indice auquel $d_{k+1} - d_k > d_2 - d_1 = 1$. Une fois cet indice identifié, il ne reste que des petits cas à traiter.

Puisque $n \geqslant 3$, le nombre $n! - 1$ n'est pas un diviseur de $n!$. Ainsi, $d_k - d_{k-1} > 1$. Puisqu'en revanche $d_2 - d_1 = 2 - 1 = 1$, il existe un indice i, que l'on prend minimal, tel que $d_{i+2} - d_{i+1} > d_{i+1} - d_i$.

Supposons $n \geqslant 5$. Posons $(d_i, d_{i+1}, d_{i+2}) = (d, d+1, d+x)$ avec $x \geqslant 3$. Alors $(d_1, d_2, d_3, d_4, d_5) = (1, 2, 3, 4, 5)$ donc $d \geqslant 6$. Les nombres $n!/(d+x), n!/(d+1)$ et $n!/d$ sont des diviseurs consécutifs de $n!$ et vérifient donc

$$\frac{n!}{d+1} - \frac{n!}{d+x} \leqslant \frac{n!}{d} - \frac{n!}{d+1} \quad \Longleftrightarrow \quad (x-2)d \leqslant x.$$

Comme $d \geqslant 6$, on a au contraire $d(x-2) > 5(x-2) > x$. De cette contradiction, on déduit que $\boxed{n \leqslant 4}$.

Réciproquement, si $n = 3$, les diviseurs de 6 sont $1, 2, 3, 4, 6$ et vérifient bien la propriété. Si $n = 4$, les diviseurs de 24 sont $1, 2, 3, 4, 6, 8, 12$ et vérifient bien la propriété.

Exercice 4.101. (EGMO 2025 P1) Déterminer tous les entiers $N \geqslant 3$ tels que, si on note $c_1 < \ldots < c_m$ les entiers strictement positifs premiers avec N et inférieurs à N, alors $\mathrm{PGCD}(N, c_i + c_{i+1}) \neq 1$ pour tout i vérifiant $1 \leqslant i \leqslant m-1$.

Solution 4.101. **Réponse :** Les entiers pairs et les puissances de 3.

Soit N un entier solution. Si N est pair, alors les c_i sont tous impairs, donc $c_i + c_{i+1}$ est pair et $\mathrm{PGCD}(N, c_i + c_{i+1}) \geqslant 2$ pour tout indice i, donc $\boxed{\text{les entiers pairs sont solutions}}$.

Supposons désormais que N est impair. On a donc $c_1 = 1$ et $c_2 = 2$, d'où $\mathrm{PGCD}(N, 3) \neq 1$ et $\boxed{3 \mid N}$. On écrit alors $N = 3^\alpha A$ avec $\alpha \geqslant 1$ et A impair premier avec 3. On suppose par l'absurde que N n'est pas une puissance de 3 et donc que $A > 1$ (ce qui implique que $A \geqslant 5$). On distingue alors plusieurs cas :

- ➢ Si $A \equiv 1 \mod 3$, alors les entiers A et $A-1$ ne sont pas premiers avec N mais les entiers $A-2$ et $A+1$ le sont (en effet, $3 \mid A-1$ mais pas $A-2$ et $A+1$, et on a bien $\mathrm{PGCD}(A-2, A) = \mathrm{PGCD}(A+1, A) = 1$). On déduit que $\mathrm{PGCD}(N, A-2+A+1) = \mathrm{PGCD}(N, 2A-1) \neq 1$. Or $2A - 1 \equiv 1 \mod 3$ n'est pas divisible par 3 et est premier avec A. On a donc une contradiction.
- ➢ Si $A \equiv 2 \mod 3$, alors les entiers A et $A+1$ ne sont pas premiers avec N mais les entiers $A-1$ et $A+2$ le sont. On déduit que $\mathrm{PGCD}(N, 2A+1) \neq 1$. Or $2A+1$ n'est pas divisible par 3 et est premier avec A, d'où la contradiction.

On déduit que $\boxed{A = 1}$ et que N est une puissance de 3.

Réciproquement, si N est une puissance de 3, les entiers premiers avec N sont les entiers congrus à 1 et 2 modulo 3. Pour tout indice i, l'un des entiers c_i et c_{i+1} est alors congru à 1 modulo 3 et l'autre à 2. Ainsi, $c_i + c_{i+1} \equiv 0 \mod 3$, donc on a bien $\mathrm{PGCD}(N, c_i + c_{i+1}) \geqslant 3$ et N vérifie bien la condition.

Exercice 4.102. (Coupe Animath de Printemps 2020) Déterminer les triplets (m, n, k) d'entiers tels que $m \geqslant 2$, $n \geqslant 2$ et $k \geqslant 3$ et ayant la propriété suivante : m et n ont chacun k diviseurs positifs et, si l'on note $d_1 < \ldots < d_k$ les diviseurs positifs de m (avec $d_1 = 1$ et $d_k = m$) et $d'_1 < \ldots < d'_k$ les diviseurs positifs de n (avec $d'_1 = 1$ et $d'_k = n$), alors $d'_i = d_i + 1$ pour tout entier i tel que $2 \leqslant i \leqslant k-1$.

Solution 4.102. **Réponse :** Il s'agit des triplets $(4, 9, 3)$ et $(8, 15, 4)$.

Tout d'abord notons que les plus petits diviseurs strictement plus grands que 1 de m et n sont d_2 et $d_2 + 1$ qui sont donc forcément premiers. Or ces deux nombres étant consécutifs, l'un d'entre eux est pair donc vaut 2. Si $d_2 + 1 = 2$, $d_2 = 1$ ce qui contredit l'énoncé. On a donc $\boxed{d_2 = 2 \text{ et } d_2 + 1 = 3}$.

Si m est divisible par un nombre impair ℓ, celui-ci est un diviseur strict car m est divisible par 2 donc il est pair. Comme $\ell + 1$ est pair et divise n, $2 \mid n$, ce qui contredit le fait que $d_2 + 1$ est le plus petit diviseur de n. Ainsi, $\boxed{m \text{ est une puissance de } 2}$. Si $m \geqslant 16$, alors 8 et 4 sont des diviseurs stricts de m. Ainsi 9 et 5 divisent n, donc $45 \mid n$. Mais alors 15 est un facteur strict de n donc $15 - 1 = 14$ est un facteur strict de m, ce qui est absurde.

Ainsi, $m = 4$ ou $m = 8$. Si $m = 4$, le seul diviseur strict de 4 est 2 donc le seul diviseur strict de n est 3 donc $n = 9$. Comme le seul diviseur strict de 4 vaut 2 et le seul diviseur strict de 9 vaut 3, le couple $\boxed{(4, 9, 3)}$ convient. Si $m = 8$, m a pour diviseurs stricts 2 et 4, n a pour diviseurs stricts 3 et 5 donc $n = 15$.Réciproquement, les seuls diviseurs stricts de 8 valant 2 et 4 et ceux de 15 valant 3 et 5, $\boxed{(8, 15, 4)}$ vérifie l'énoncé.

Exercice 4.103. (Roumanie MO 2023) Soit n un entier composé et $1 = d_1 < d_2 < \ldots < d_k = n$ ses diviseurs. On suppose que $d_{i+1}^2 \geqslant d_i d_{i+2}$ pour tout $i \leqslant k-2$.
Montrer que n est la puissance d'un nombre premier.

Solution 4.103. L'inégalité se réécrit $\dfrac{d_{i+1}}{d_i} \geqslant \dfrac{d_{i+2}}{d_{i+1}}$. Notons $p = d_2$ le plus petit diviseur premier de n. Alors $d_{k-1} = n/p$. En faisant le produit télescopique de cette l'inégalité ci-dessus pour tout indice i, on trouve

$$\frac{n}{p} = \frac{d_{k-1}}{d_1} = \frac{d_{k-1}}{d_{k-2}} \cdot \ldots \cdot \frac{d_3}{d_2} \cdot \frac{d_2}{d_1} \geqslant \frac{d_k}{d_{k-1}} \cdot \frac{d_{k-1}}{d_{k-2}} \cdot \ldots \cdot \frac{d_3}{d_2} = \frac{d_k}{d_2} = \frac{n}{p}.$$

On déduit que les inégalités sont toutes des égalités, c'est-à-dire que $\dfrac{d_{i+1}}{d_i} \geqslant \dfrac{d_{i+2}}{d_{i+1}}$, ce qui donne par récurrence immédiate que $d_i = d_2^{i-1}$ et en particulier $n = d_2^{k-1} = p^{k-1}$ est une puissance de nombre premier.

Exercice 4.104. (EMC 2020 junior) Un entier $k \geqslant 3$ est dit *sympa* s'il existe un entier n et k entiers strictement positifs $d_1 < \ldots < d_k$ vérifiant :
- ➢ $d_{j+2} = d_j + d_{j+1}$ pour tout $1 \leqslant j \leqslant k-2$,
- ➢ les entiers $d_1, \ldots, d_k$ sont des diviseurs de n,
- ➢ tout diviseur positif de n autre que les d_i est soit inférieur à d_1 soit supérieur à d_k.

Déterminer tous les entiers sympas.

Solution 4.104. **Réponse :** Les seuls entiers sympas sont $k = 3$ et $k = 4$.
L'idée est que si k est trop grand, on peut trouver des diviseurs des potentiels diviseurs de n compris entre d_k et d_{k+1}. Par exemple, comme $d_4 = 2d_1 + d_2$ et $d_5 = 3d_1 + 2d_2$, donc $2(d_1 + d_2)$ n'est pas un diviseur de n, ce qui donne des informations sur n.
Supposons que $k \geqslant 5$ vérifie la propriété et prenons un entier n vérifiant les conditions de l'énoncé. On vérifie que, puisque $d_1 < d_2$, $d_3 = d_1 + d_2 < 2d_2 < d_1 + 2d_2 = d_4$, donc $2d_2$ n'est pas un diviseur de n. On écrit $n = d_2 a$ avec a un entier impair.
De même, $d_4 = d_1 + 2d_2 < 2(d_1 + d_2) < 3d_1 + 2d_2 = d_5$, donc $2d_3$ n'est pas un diviseur de n. On écrit $n = (d_1 + d_2)b$ avec b un entier impair.
Enfin, on a $d_1 < \dfrac{d_1 + d_2}{2} < d_2$, donc le nombre $\dfrac{d_1 + d_2}{2}$ ne peut pas être un diviseur de n, alors $d_1 + d_2$ l'est. On déduit que ce nombre n'est pas entier et que $d_1 + d_2$ est impair.
On a donc l'égalité $d_2 a = (d_1 + d_2)b$. On s'empresse d'homogénéiser cette égalité en simplifiant par $d = \mathrm{PGCD}(d_1, d_2)$: on pose $d_1 = dx$ et $d_2 = dy$, où x et y sont premiers entre eux. Comme $d_1 + d_2$ est impair, il en est de même pour $x + y$.
On a alors $ya = (x + y)b$. Si y était pair, 2 diviserait $x + y \mid d_1 + d_2$, ce qui est exclu. Ainsi, y est impair et on déduit que x est pair. Mais comme $n = dyb$ et que d est impair (d_1 et d_2 sont de parité différente), n ne peut pas être divisible par 2, ce qui est une contradiction. On a donc $\boxed{k < 5}$.
Réciproquement, si $k = 3$ on peut prendre $(d_1, d_2, d_3) = (1, 2, 3)$ et vérifier que $n = 6$ satisfait les conditions de l'énoncé. Si $k = 4$, on peut prendre $(d_1, d_2, d_3, d_4) = (1, 2, 3, 5)$ et à nouveau $n = 30$ vérifie les conditions de l'énoncé. Donc $k = 3$ et $k = 4$ sont sympas.

Exercice 4.105. (BXMO 2014) Déterminer tous les entiers n vérifiant la propriété suivante : pour tous diviseurs positifs k, ℓ de n vérifiant $k < n$ et $\ell < n$, l'un au moins des nombres $2k - \ell$ et $2\ell - k$ est également un diviseur (pas forcément positif) de n.

Solution 4.105. **Réponse :** les entiers $n = 6, 9$ et 15.
Soit n un entier solution. On suppose que n est un nombre composé et on note p son plus petit facteur premier et $A = n/p$. En appliquant la propriété à $(k, \ell) = (A, 1)$, on trouve que $2A - 1$ où $2 - A$ est un diviseur de n. Or $\mathrm{PGCD}(2A - 1, pA) = \mathrm{PGCD}(1, pA) = 1$. On déduit que si $2A - 1 \min n$, alors $2A - 1 = 1$ et $A = 1$, ce qui est exclu. Ainsi, $\boxed{A - 2 \mid n}$. On déduit que $A - 2 \mid n - p(A - 2) = 2p$ et donc $\boxed{A - 2 \in \{1, 2, p, 2p\}}$.

- ➢ Si $A - 2 = 1$, alors $A = 3$. Comme p est le plus petit facteur premier de n, on a $p = 2, 3$ donc $\boxed{n = 6, 9}$. Réciproquement, en testant les différentes paires d'entiers parmi $(1, 2, 3, 6)$ et $(1, 3, 9)$ respectivement, on trouve que ces deux entiers sont bien solutions.

➢ Si $A-2=2$, alors $A=4$. Là encore, par minimalité de p, on trouve $p=2$ donc $n=8$. Toutefois, en prenant $(k,\ell)=(2,1)$, on voit que ni 3 ni 0 ne sont des diviseurs de 8, donc celui-ci n'est pas solution.

➢ Si $A-2=p$, alors $A=p+2$. On peut suppose que $p\geqslant 3$, puisque le cas $p=4$ a été traité plus haut. On a alors $n=p(p+2)$. En appliquant l'hypothèse de l'énoncé à $(k,\ell)=(p,1)$, on trouve que $2p-1$ ou $p-2$ est un diviseur de $p(p+2)$.

- Si $2p-1\mid n$, comme $\mathrm{PGCD}(p,2p-1)=1$, on a par le lemme de Gauss que $2p-1\mid p+2$, d'où $2p-1\leqslant p+2$ et $p\leqslant 3$. On trouve alors $n=8$ (traité plus haut) ou $\boxed{n=15}$. Réciproquement, en testant les différentes paires d'entiers parmi $(1,3,5,15)$, on trouve que $n=15$ est bien solution.
- Si $p-2\mid n$, alors $p-2=1$ (dans le cas contraire n admet un diviseur premier strictement inférieur à p) et $p=3$, donc $n=15$, ce qui conduit à nouveau au cas précédent.

➢ Si $A-2=2p$, alors $n=2p+2$. Il vient que n est pair donc $p=2$ et $n=8$, cas déjà traité plus haut.

En conclusion, les seuls entiers solutions sont $n=6,9,15$.

Exercice 4.106. (BXMO 2016) Soit n un entier strictement positif. On suppose que ses diviseurs positifs peuvent être répartis par paires de telle sorte que la somme de chaque paire est un nombre premier. Prouver que ces nombres premiers sont tous distincts et qu'aucun d'eux ne divise n.

Solution 4.106. Examinons l'hypothèse donnée. Etant donnée un couple (d_1,d_2) de dvisieurs, si ces diviseurs admettent un diviseur premier commun p, ce diviseur divise également leur somme, qui n'est donc pas un nombre premier. En conclusion, dans un couple (d_1,d_2), les nombres d_1 et d_2 sont premiers entre eux. En particulier, $d_1d_2\leqslant n$.
Or, le produit de tous les diviseurs de n vaut $n^{d(n)/2}$, avec $d()$ le nombre de diviseurs de n, et il y a $d(n)/2$ paires de diviseurs et le produit de chaque paire vaut au plus n. Donc le produit des produits de chaque n vaut au plus $n^{d(n)/2}$. Comme ce produit est effectivement égal à $n^{d(n)/2}$ donc il y a égalité dans chaque paire. En conclusion, dans chaque paire, $d_1d_2=n$. Autrement dit, les paires de diviseurs sont de la forme $\left(d,\frac{n}{d}\right)$.

A présent, on résoud le problème. Soit d un diviseur de n et $p=d+\frac{n}{d}$ le nombre premier somme des éléments de la paire $\left(d,\frac{n}{d}\right)$. Si p divise n, p divise d ou n/d et est donc strictement inférieur à la somme $d+\frac{n}{d}=p$ ce qui est absurde. Ainsi, les nombres premiers des diverses paires ne divisent pas n.

On montre que les nombres premiers sont distincts. En effet, soient d_1 et d_2 deux diviseurs, il s'agit de montrer que $d_1+\frac{n}{d_1}\neq d_2+\frac{n}{d_2}$. Mais l'égalité est équivalente à $(n-d_1d_2)(d_1-d_2)=0$. Or les éléments d_1 et d_2 sont supposés être distincts et dans des paires distinctes. Ainsi, on ne peut ni avoir $d_2=d_1$ ni avoir $d_2=\frac{n}{d_1}$. On a donc le résultat désiré.

Exercice 4.107. (EMC 2025 senior) Soit $k\geqslant 2$ un entier. Soient $m<n$ deux entiers strictement positifs, premiers entre eux et possédant tous les deux exactement k diviseurs positifs. Pour tout $1\leqslant i\leqslant k$, on note respectivement f_i et d_i les $i-$èmes plus petits diviseurs de m et n. On suppose que, pour tout indice $i\geqslant 2$,

$$d_i-f_i\mid n-m.$$

Montrer que, pour tout $i\leqslant k/2$, on a $d_i\geqslant f_i$.

Solution 4.107. Pour tout indice i, la condition implique, modulo d_i-f_i,

$$0\equiv n-m=d_i\cdot\frac{n}{d_i}-f_i\cdot\frac{m}{f_i}\equiv f_i\left(\frac{n}{d_i}-\frac{m}{f_i}\right)\mod d_i-f_i.$$

Comme m et n sont premiers entre eux, les entiers d_i-f_i et f_i sont également premiers entre eux. Il vient que $d_i-f_i\mid\frac{n}{d_i}-\frac{m}{f_i}$. Symétriquement, $\frac{n}{d_i}-\frac{m}{f_i}\mid d_i-f_i$ donc $\boxed{|d_i-f_i|=\left|\frac{n}{d_i}-\frac{m}{f_i}\right|}$.

Supposons désormais que $d_i<f_i$ pour un certain indice $i\leqslant k/2$. Il vient déjà, en combinant avec l'hypothèse $m<n$, que $n/d_i>m/f_i$. On peut poser $f_i=d_i+\delta$, et d'après l'inégalité ci-dessus, $n/d_i=m/f_i+\delta$. Il vient que

$$n-m=d_i\cdot\frac{n}{d_i}+f_i\cdot\frac{m}{f_i}=d_i\frac{m}{f_i}+d_i\delta-(d_i+\delta)\frac{m}{f_i}=\delta\left(d_i-\frac{m}{f_i}\right).$$

Mais comme $i\leqslant k/2$, on a que $d_i<f_i<\frac{m}{f_i}$, donc l'expression ci-dessus est strictement négative, ce qui est absurde. On a donc conclu.

Exercice 4.108. (IMO 2025 P4) On considère une suite infinie $a_1, a_2, \ldots$ d'entiers strictement positifs telle que chaque a_i possède au moins trois diviseurs propres. Pour tout $n \geqslant 1$, on suppose que a_{n+1} est la somme des trois plus grands diviseurs propres de a_n.

Déterminer toutes les valeurs possibles de a_1.

Solution 4.108. **Réponse :** Il s'agit des nombre de la forme $12^N \cdot 6k$, avec N est entier et k est premier avec 10.

Pour tout entier n, notons $d_1(n), d_2(n)$ et $d_3(n)$ respectivement, le plus, le deuxième plus grand et le troisième plus grand diviseur de n (pour peu qu'ils existent).

Analyse : Soit (a_n) une suite solution.

Si a_n est impair, alors

$$a_{n+1} = d_1(a_n) + d_2(a_n) + d_3(a_n) \leqslant \frac{a_n}{3} + \frac{a_n}{5} + \frac{a_n}{7} < a_n.$$

De plus, a_{n+1} est la somme de trois nombres impairs donc est impair. Par récurrence immédiate, on obtient que la suite est une suite strictement décroissante de termes impairs positifs, ce qui est absurde. En particulier $\boxed{\text{tous les termes de la suite sont pairs}}$, et $d_1(a_n) = a_n/2$ pour tout n.

Montrons désormais que tous les termes de la suite sont divisibles par 3. Supposons qu'un terme a_n ne soit pas divisible par 3. On montre que a_{n+1} n'est pas divisible par 3 non plus, ce qui donne $a_{n+1} \leqslant \frac{a_n}{2} + \frac{a_n}{4} + \frac{a_n}{5} < a_n$, ce qui s'itère par récurrence. On a donc à nouveau une suite strictement décroissante, ce qui est absurde.

- ➢ Si $4 \mid a_n$, alors $d_1(a_n) = a_n/2$, $d_2(a_n) = a_n/4$ et $d_3(a_n) \neq 0 \mod 3$. On a donc

$$a_{n+1} = \frac{a_n}{2} + \frac{a_n}{4} + d_3(a_n) = 3\frac{a_n}{4} + d_3(a_n) \equiv d_3(a_n) \neq 0 \mod 3.$$

- ➢ Si 4 ne divise pas a_n, on note p le deuxième plus petit diviseur premier de a_n. Alors $d_1(a_n)$ est impair, $d_2(a_n) = a_n/p$ est pair, donc $d_3(a_n) = a_{n+1} - d_1(a_n) - d_2(a_n)$ est impair. Le troisième plus petit diviseur de a_n doit donc être pair, et comme ce n'est pas 4, c'est $2p$ par minimalité de p. Il vient

$$a_{n+1} = \frac{a_n}{2} + \frac{a_n}{p} + \frac{a_n}{2p} = \frac{a_n}{2} + 3\frac{a_n}{2p} \equiv \frac{a_n}{2} \neq 0 \mod 3.$$

Dans les deux cas, on conclut que 3 ne divise pas a_{n+1}, ce qui nous amène la contradiction évoquée plus haut. En conclusion, $\boxed{\text{tous les termes sont divisibles par 3}}$ et donc $\boxed{6 \mid a_n}$ pour tout n. Il vient que $d_2(a_n) = a_n/3$ et $d_3(a_n) \in \{a_n/4, a_n/5, a_n/6\}$. On distingue les cas :

- ➢ Si $d_3(a_n) = a_n/6$, alors $a_{n+1} = a_n$.
- ➢ Si $d_3(a_n) = a_n/5$, alors 4 ne divise pas a_n et $a_{n+1} = 31a_n/30$ est impair, ce qui est exclus.
- ➢ Si $d_3(a_n) = a_n/4$, alors $a_{n+1} = 13a_n/12$.

Notons que, tant que $v_2(a_n) \geqslant 2$, on est dans le cas 3. La suite $(v_2(a_n))$ est donc strictement décroissante jusqu'à atteindre une valeur valant 0 ou 1. Comme tous les termes sont pairs, la suite $(v_2(a_n))$ décroît strictement jusqu'à atteindre la valeur 1 en un rang noté N. Comme a_N est divisible par 2 et 3 mais pas 4 ni 5 (puisque $d_3(a_N) = a_N/6$, on peut écrire $a_N = 6k$ avec k premier avec 2 et 5.

Comme pour tout $n \leqslant N$, on est dans le cas 3, on a $a_N = \frac{13^{N-1}}{12^{N-1}} a_1$, soit $\boxed{a_1 = 12^{N-1} \cdot 6k/13^{N-1}}$, ce qui est la forme annoncée.

Construction :

Réciproquement, si $a_1 = 12^N \cdot 6k$ avec k premier avec 10, on a par récurrence que $a_{\ell+1} = 12^{N-\ell}13^\ell 6k$ pour $\ell \leqslant N$ et $a_\ell = 6 \cdot 13^N k$ pour $\ell \geqslant N$, et la suite est à valeurs entières.

Exercice 4.109. (USAMO 2021 P4) Un ensemble fini S d'entiers strictement positifs possède la propriété que pour tout entier $s \in S$ et tout diviseur d de s, il existe un unique élément t de S tel que $\mathrm{PGCD}(s,t) = d$. Déterminer toutes les valeurs que peut prendre $|S|$.

Solution 4.109. **Réponse :** les puissances de 2.
On suppose que S est non vide et contient au moins deux éléments.
Notons que 1 n'est pas dans S car il est premier avec tous les autres nombres de S (y compris lui-même), donc on n'a pas unicité du t tel que $\gcd(1,t) = 1$.

Ensuite, on remarque que $|S| \geqslant d(a)$ pour tout a, puisque pour chaque diviseur de a, on peut associer de façon injective un élément t de S. Si $|S| > d(a)$, par principe des tirois on a deux éléments t et s vérifiant $\gcd(s,a) = \gcd(t,a)$. Donc $|S| = d(a)$ pour tout a.

Soit p diviseur premier de a et $\beta = v_p(a)$. La condition implique alors qu'il y a exactement $d(a/p^\beta)$ éléments de S non divisibles par p. Comme $\dfrac{d(a/p^\beta)}{d(a)} = \dfrac{1}{\beta+1}$, inversement, exactement $\beta/(\beta+1)$ des éléments de S sont divisibles par p. Comme on doit pouvoir mettre par pair les éléments premiers entre eux, on a $\beta/(\beta+1) \leqslant 1/2$, donc $\beta \leqslant 1$. On déduit que $\beta = 1$. Ainsi, a est un produit de nombres premiers distincts et $d(a) = 2^k$.

Réciproquement, si $|S| = 2^k$, on prend $a_1, \ldots, a_k$ des nombres premiers, et $b_1 \ldots, b_k$ d'autres nombres premiers distincts et on vérifie que l'ensemble $S = \{\prod_{i\in I} a_i \prod_{i\in J} b_j, I \sqcup J = \{1,\ldots,n\}\}$ satisfait les conditions de l'énoncé.

Exercice 4.110. (IMO SL 2021 N3) Trouver tous les entiers $n \geqslant 1$ ayant la propriété suivante : il existe une permutation $d_1, d_2, \ldots, d_k$ des diviseurs positifs de n telle que, pour tout $i \leqslant k$, la somme $d_1 + d_2 + \ldots + d_i$ soit un carré parfait.

Solution 4.110. Soit n un des entiers recherchés, et $d_1, d_2, \ldots, d_k$ une permutation adéquate des diviseurs positifs de n. Pour tout entier $i \leqslant k$, on pose $s_i = \sqrt{d_1 + d_2 + \ldots + d_i}$.
On dit qu'un entier ℓ est *bon* si $s_i = i$ et $d_i = 2i - 1$ pour tout $i \leqslant \ell$. Ci-dessous, nous allons démontrer que tout entier $\ell \leqslant k$ est bon.
Tout d'abord, pour tout entier $i \geqslant 2$, on remarque déjà que

$$d_i = s_i^2 - s_{i-1}^2 = (s_i - s_{i-1})(s_i + s_{i-1}) \geqslant s_i + s_{i-1} \geqslant 2.$$

Par conséquent, $d_1 = s_1 = 1$.
Considérons maintenant un bon entier $\ell \leqslant k-1$. Nous allons démontrer que $\ell+1$ est bon lui aussi. En effet, si $s_{\ell+1} + s_\ell$ divise $(s_{\ell+1} - s_\ell)(s_{\ell+1} + s_\ell) = d_{\ell+1}$, donc divise n. Il existe donc un entier m tel que

$$d_m = s_{\ell+1} + s_\ell \geqslant 2s_\ell + 1 \geqslant 2\ell + 1.$$

Comme $d_m > d_i$ pour tout $i \leqslant \ell$, on en déduit que $m \geqslant \ell + 1$. Mais alors

$$s_{\ell+1} + s_\ell = d_m = (s_m - s_{m-1})(s_m + s_{m-1}) \geqslant (s_m - s_{m-1})(s_{\ell+1} + s_\ell) \geqslant s_{\ell+1} + s_\ell.$$

Les inégalités sont donc des égalités, ce qui signifie que $s_m + s_{m-1} = s_{\ell+1} + s_\ell$, donc que que $m = \ell + 1$, et que $s_m - s_{m-1} = 1$, c'est-à-dire que $s_{\ell+1} = s_\ell + 1 = \ell + 1$. On en conclut que

$$d_{\ell+1} = (s_{\ell+1} - s_\ell)(s_{\ell+1} + s_\ell) = 2\ell + 1,$$

ce qui signifie comme prévu que $\ell + 1$ est bon.
En conclusion, les diviseurs de n sont les entiers $1, 3, \ldots, 2k-1$. Réciproquement, si les diviseurs de n sont les entiers $1, 3, \ldots, 2k-1$, l'entier n convient assurément.
En particulier, si $k \geqslant 2$, l'entier d_{k-1} est un diviseur impair de $n - d_{k-1} = 2$, donc $d_{k-1} = 1$ et $k = 2$. Ainsi, soit $k = 1$, auquel cas $n = 1$, soit $k = 2$, auquel cas $n = 3$. Dans les deux cas, ces valeurs de n conviennent. Les entiers recherchés sont donc $n = 1$ et $n = 3$.

Exercice 4.111. (IMO SL 2024 C2) On considère une grille carrée de taille $n \times n$ composée de n^2 cases. Pour tout diviseur positif d de n, la $d-$*division* de la grille est définie comme la division de la grille en $(n/d)^2$ sous-grilles carrées, toutes de taille $d \times d$, de sorte que chaque case appartient à exactement une sous-grille.

On dit qu'un entier n est *régulier* s'il est possible d'écrire les entiers $1, 2, \ldots, n^2$ dans les cases de la grille en vérifiant les conditions suivantes :

- ▷ chaque case contient exactement un entier,
- ▷ chacun des entiers $1, 2, \ldots, n^2$ est écrit dans exactement une case,
- ▷ pour tout diviseur d de n tel que $1 < d < n$ et pour toute sous-grille de la $d-$division de la grille, la somme des entiers écrits dans les cases de la sous-grille n'est pas divisible par d.

Déterminer tous les entiers pairs réguliers.

Solution 4.111.

Réponse : Tous les entiers de la forme 2^k, avec $k \in \mathbb{N}^\star$.

L'exercice possède deux parties. Dans un premier temps, on montre que si n est un entier pair régulier, alors n est une puissance de 2, cette partie s'appelle *l'analyse*.Dans un second temps, on montre que réciproquement, toute puissance de 2 différente de 1 est bien un entier pair régulier, cette étape s'appelle *la construction*. Dans la suite, pour tout diviseur d de n, on appelle $d-$sous-grille une sous-grille appartenant à la $d-$ division de la grille.

Analyse : Soit n un entier pair régulier. On peut écrire n sous la forme $n = 2^k\beta$, où β est un entier impair. On suppose dans la suite que $\beta > 1$. Notons que, dans ce cas, 2^k est un diviseur strict de n, ce qui nous autorise par la suite à considérer la 2^k division de la grille. Nous allons commencer par montrer que, pour tout $1 \leqslant i \leqslant s$, la somme des cases dans chaque 2^i-grille est congrue à 2^{i-1} modulo 2^i. On procède pour cela par récurrence sur i.

Initialisation : Si $i = 1$, pour toute $2-$sous-grille, la somme de ses cases n'est pas divisible par 2. Cette somme est donc congrue à 1 modulo 2.

Hérédité : On suppose que, pour un i fixé dans $[\![1, k-1]\!]$, la somme des cases dans chaque 2^i-sous-grille est congrue à 2^{i-1} modulo 2^i. On considère à présent une $2^{i+1}-$sous-grille. Elle est composée de quatre 2^i-sous-grilles. Par hypothèse de récurrence, la somme des cases de chacune de ces 2^i-sous-grilles est congrue à 2^{i-1} modulo 2^i. Ainsi, la somme des cases de la $2^{i+1}-$sous-grille est elle-même congrue à 2^i modulo 2^i, c'est-à-dire que cette somme est un multiple de 2^i. Comme cette somme n'est, par ailleurs, pas divisible par 2^{i+1}, elle est bien congrue à 2^i modulo 2^{i+1}, ce qui achève la récurrence.

En particulier, la somme des cases d'une 2^k-sous-grille est congrue à 2^{k-1} modulo 2^k. En additionnant les sommes des cases de toutes les 2^k-sous-grilles, on trouve que la somme des cases du tableau est congrue à

$$\underbrace{2^{k-1} + \ldots + 2^{k-1}}_{\beta^2 \text{ fois}} \equiv 2^{k-1}\beta^2 \equiv 2^{k-1} \mod 2^k.$$

D'autre part, cette somme correspond à la somme de tous les entiers de 1 à n^2, à savoir

$$1 + 2 + \ldots + n^2 = \frac{n^2(n^2+1)}{2} = \frac{2^{2k}\beta^2(2^{2k}\beta^2+1)}{2} = 2^{2k-1}\beta^2(2^{2k}\beta^2+1) \equiv 0 \mod 2^k.$$

Cette contradiction implique qu'on ne peut pas avoir $\beta > 1$. Donc $\beta = 1$ et n est une puissance de 2.

Construction : Montrons que 2^k est régulier pour tout $k \geqslant 1$. On procède par récurrence sur k.

Initialisation : Si $k = 1$, le nombre 2 n'a pas de diviseur propre donc il est bien régulier.

Hérédité : On suppose que 2^k est régulier pour un entier k fixé. On considère à présent une grille de taille $2^{k+1} \times 2^{k+1}$, que l'on découpe en quatre carrés de taille $2^k \times 2^k$. D'après l'hypothèse de récurrence, on dispose d'une numérotation $a_1, \ldots, a_{2^{2k}}$ des entiers $1, \ldots, 2^{2k}$ de sorte que la 2^k-sous-grille située en haut à gauche ainsi numérotée vérifie les trois conditions de l'énoncé. On pose alors $b_i = a_i + 2^{2k}$, $c_i = a_1 + 2 \cdot 2^{2k}$ et $d_i = a_i + 3 \cdot 2^{2k}$, de sorte que l'ensemble des entiers a_i, b_i, c_i, d_i constitue une permutation des entiers $1, \ldots, 2^{2(k+1)}$. On numérote les cases des trois autres 2^k-grilles à l'aide des numérotation $(b_i), (c_i)$ et (d_i) comme dans la figure de gauche ci-dessous.

a_1	$\cdots$			b_1	$\cdots$		
		2^{2k}					
						$2^{2k}+2^{k-1}$	
		$\cdots$	$a_{2^{2k}}$			$\cdots$	$b_{2^{2k}}$
c_1	$\cdots$			d_1	$\cdots$		
		$3\cdot 2^{2k}$					
						$3\cdot 2^{2k}+2^{k-1}$	
		$\cdots$	$c_{2^{2k}}$			$\cdots$	$d_{2^{2k}}$

a_1	$\cdots$			b_1	$\cdots$		
		$2^{2k}+2^{k-1}$					
						2^{2k}	
		$\cdots$	$a_{2^{2k}}$			$\cdots$	$b_{2^{2k}}$
c_1	$\cdots$			d_1	$\cdots$		
		$3\cdot 2^{2k}+2^{k-1}$					
						$3\cdot 2^{2k}$	
		$\cdots$	$c_{2^{2k}}$			$\cdots$	$d_{2^{2k}}$

Pour l'instant, une telle numérotation ne vérifie pas la troisième condition de l'énoncé, puisque la somme des cases de la grille supérieure gauche est divisible par 2^k. On va donc permuter certaines cases des 2^k grilles.

Nous allons échanger les places des cases contenant l'entier 2^{2k} et l'entier $2^{2k}+2^{k-1}$, ainsi que les cases contenant l'entier $3\cdot 2^{2k}$ et $3\cdot 2^{2k}+2^{k-1}$. La numérotation obtenue correspond à la grille de droite.

Montrons que la configuration ci-dessus convient. Prenons $i \leqslant k-1$. Toute 2^i-sous-grille est alors contenue dans l'une des quatre 2^k-sous-grille. Puisque $2^{2k} \equiv 2^{2k}+2^{k-1} \mod 2^i$ et $3\cdot 2^{2k}+2^{k-1} \equiv 3\cdot 2^{2k} \mod 2^i$, les sommes des 2^i-sous-grilles restent inchangées après nos deux permutations. Par hypothèse de récurrence, ces sommes n'étaient pas divisibles par 2^i, donc les sommes des 2^i-sous-grilles ne sont pas divisibles par 2^i. D'autre part, on vérifie que les sommes des cases des quatre 2^k-sous-grilles sont respectivement

$$a_1+\ldots+a_{2^{2k}}+2^{k-1} = 1+\ldots+2^{2k}+2^{k-1} = 2^{2k-1}(2^{2k}+1)+2^{k-1} \equiv 2^{k-1} \mod 2^k\,;$$

$$b_1+\ldots+b_{2^{2k}}-2^{k-1} = (2^{2k}+1)+\ldots+2\cdot 2^{2k}-2^{k-1} \equiv 2^{k-1} \mod 2^k\,;$$

$$c_1+\ldots+c_{2^{2k}}-2^{k-1} = (2\cdot 2^{2k}+1)+\ldots+3\cdot 2^{2k}+2^{k-1} \equiv 2^{k-1} \mod 2^k\,;$$

$$d_1+\ldots+d_{2^{2k}}-2^{k-1} = (3\cdot 2^{2k}+1)+\ldots+4\cdot 2^{2k}-2^{k-1} \equiv 2^{k-1} \mod 2^k\,;$$

de sorte que la grille vérifie à présent les conditions de l'énoncé. Ceci conclut que 2^{k+1} est régulier et achève la récurrence.

Exercice 4.112. (RMM SL 2021/France TST 2021-2022) Étant donnés deux entiers naturels non nuls a et b, on dit que b est a-gréable si, pour toute liste $d_1, d_2, \ldots, d_k$ de diviseurs de b, non nécessairement distincts, telle que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} > a,$$

il existe un ensemble I inclus dans $\{1, 2, \ldots, k\}$ tel que

$$\sum_{i \in I} \frac{1}{d_i} = a.$$

L'entier a étant fixé, quels sont les entiers a-gréables ?

Solution 4.112. Tout d'abord, soit b un entier qui admet au moins deux facteurs premiers distincts $p < q$. On pose alors $d_1 = p$ et $d_2 = d_3 = \ldots = d_{aq} = q$, de sorte que

$$\sum_{i=1}^{aq} \frac{1}{d_i} = a + \frac{1}{p} - \frac{1}{q} > a.$$

Cependant, si $1 \notin I$, on sait que

$$\sum_{i \in I} \frac{1}{d_i} = \frac{|I|}{q} \leqslant \frac{aq - 1}{q} < a,$$

et si $1 \in I$,

$$\sum_{i \in I} \frac{1}{d_i} = \frac{1}{p} + \frac{|I| - 1}{q} = \frac{q + (|I| - 1)p}{pq}$$

ne peut être égal à a, car p ne divise pas $q + (|I| - 1)p$. Ainsi, l'entier b n'est pas a-gréable.
Réciproquement, supposons que b est une puissance de nombre premier, disons $b = p^\alpha$, et soit $d_1, d_2, \ldots, d_k$ une liste de diviseurs de b, ordonnée dans l'ordre croissant, telle que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} > a.$$

Soit ℓ le plus petit entier tel que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_\ell} \geqslant a.$$

Tous les diviseurs d_i tels que $i \leqslant \ell$ divisent d_ℓ, et on pose $t_i = d_\ell / d_i$. Alors

$$t_1 + t_2 + \ldots + t_{\ell-1} < a d_\ell \leqslant t_1 + t_2 + \ldots + t_{\ell-1} + t_\ell$$

et $t_\ell = 1$, donc l'inégalité $a d_\ell \leqslant t_1 + t_2 + \ldots + t_{\ell-1} + t_\ell$ est une égalité, ce qui signifie bien que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_\ell} = a.$$

Par conséquent, l'entier b est a-gréable.
En conclusion, les entiers a-gréables sont les puissances de nombres premiers.

Solution alternative
Voici une manière alternative de démontrer que toute puissance de nombre premier est a-gréable. Nous allons démontrer par récurrence forte sur k la propriété $\mathcal{P}_k$ suivante :

> Pour tout entier $a \geqslant 0$, toute puissance de nombre premier $n = p^\alpha$ et toute suite $(d_i)_{1 \leqslant i \leqslant k}$ formée de k diviseurs de n telle que
>
> $$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} \geqslant a,$$
>
> il existe un entier I inclus dans $\{1, 2, \ldots, k\}$ pour lequel
>
> $$\sum_{i \in I} \frac{1}{d_i} \neq a.$$

Tout d'abord, si $k = 0$, la somme des inverses des diviseurs d_i est nulle, donc $a = 0$ et choisir $I = \emptyset$ nous assure que

$$\sum_{i \in I} \frac{1}{d_i} = 0 = a.$$

Ainsi, $\mathcal{P}_0$ est vraie.
On considère maintenant un entier $k \geqslant 1$ tel que $\mathcal{P}_0, \ldots, \mathcal{P}_{k-1}$ soient vraies, puis un entier $a \geqslant 0$, un nombre premier $n = p^\alpha$ et une suite $(d_i)_{1 \leqslant i \leqslant k}$ formée de k diviseurs de n telle que

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} \geqslant a.$$

Si l'un des diviseurs d_i est égal à 1, et quitte à réordonner les nombres d_i, on suppose que $i = k$. Mais alors

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_{k-1}} \geqslant a - 1.$$

D'après $\mathcal{P}_{k-1}$, il existe donc un ensemble J inclus dans $\{1, 2, \ldots, k-1\}$ tel que

$$\sum_{i \in J} \frac{1}{d_i} = a - 1,$$

de sorte que choisir $I = J \cup \{k\}$ nous permet d'obtenir l'égalité

$$\sum_{i \in J} \frac{1}{d_i} = a.$$

De même, si $k \geqslant p$ et s'il existe p diviseurs d_i égaux à un même nombre p^t, avec $t \geqslant 1$, on suppose sans perte de généralité qu'il s'agit des diviseurs $d_1, d_2, \ldots, d_p$. Quitte à remplacer ces p diviseurs par un nouveau diviseur $d'_p = p^{t-1}$, et à poser $d'_i = d_i$ lorsque $p + 1 \leqslant i \leqslant k$, on sait que

$$\frac{1}{d'_p} + \frac{1}{d'_{p+1}} + \ldots + \frac{1}{d'_k} = \frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_k} \geqslant a.$$

D'après $\mathcal{P}_{k-p+1}$, il existe un ensemble J inclus dans $\{p, p+1, \ldots, k\}$ tel que

$$\sum_{i \in J} \frac{1}{d'_i} = a.$$

Mais alors choisir $I = J$ si $p \notin J$, ou bien $I = J \cup \{1, 2, \ldots, p-1\}$ si $p \in J$, nous permet d'obtenir l'égalité

$$\sum_{i \in J} \frac{1}{d_i} = a.$$

Enfin, si nul diviseur p^t n'est obtenu plus de $p - 1$ fois, et et le diviseur p^0 n'est même jamais obtenu, on sait que

$$\sum_{i=1}^{k} \frac{1}{d_i} \leqslant \sum_{t=1}^{\alpha} \frac{p-1}{p^t} < 1,$$

de sorte que $a = 0$, donc que choisir $I = \emptyset$ permet d'obtenir l'égalité

$$\sum_{i \in I} \frac{1}{d_i} = 0 = a.$$

Ainsi, $\mathcal{P}_k$ est vraie. Ceci conclut notre récurrence et notre démonstration.

Exercice 4.113. (EMC 2022 senior) On dit qu'un entier n est *joli* s'il existe un entier k et des entiers non nécessairement distincts $d_1, \dots d_k$ tels que $n = d_1 d_2 \dots d_k$ et $d_i^2 \mid n + d_i$ pour tout $1 \leqslant i \leqslant k$.
1) Existe-t-il une infinité d'entiers jolis ?
2) Existe-t-il un carré parfait joli différent de 1 ?

Solution 4.113. 1) On construit l'infinité d'entiers jolis par récurrence. On commence par remarque que $n = 2 \times 3$ est joli puisque $2^2 \mid 6 + 2$ et $3^2 \mid 6 + 3$. Puis on suppose avoir construit un entier $n = d_1 \dots d_k$ qui est joli. On pose alors $N = n(n+1) = d_1 \dots d_k (n+1)$. On vérifie que

$$d_i^2 \mid n^2, \quad d_i^2 \mid n + d_i \quad \Longrightarrow \quad d_i^2 \mid n^2 + n + d_i = N + d_i$$

et

$$(n+1)^2 \mid (n+1)^2 = N + (n+1).$$

Donc $\boxed{n(n+1) \text{ est joli}}$ et strictement plus grand que n, ce qui garantit l'existence d'une infinité d'entiers jolis.

2) Montrons qu'il n'existe pas de carré joli. On se donne $n = d_1 \dots d_k$ un éventuel carré joli. On commence par écarter les $d_i = 1$, que l'on peut retirer de la décomposition pour supposer que les d_i sont tous strictement plus grands que 1.

On remarque que $d_i \mid d_1 \dots d_{i-1} d_{i+1} \dots d_k + 1$, donc d_i est premier avec tous les autres d_j. En particulier, les d_i sont tous des carrés.

De plus, pour tout i, et pour tout $j \neq i$, $d_i \mid \frac{n}{d_j}$, et par hypothèse $d_i \mid \frac{n}{d_i} + 1$. En sommant, on obtient

$$d_i \mid \sum_{j=1}^{k} \frac{n}{d_j} + 1.$$

Comme c'est vrai pour tout i et que les d_i sont premiers entre eux, on déduit que

$$n \mid \sum_{j=1}^{k} \frac{n}{d_j} + 1 \quad \Longrightarrow \quad 1 < \sum_{j=1}^{k} \frac{1}{d_j} + \frac{1}{n}.$$

Or, comme les d_i sont des carrés distincts strictement plus grands que 1, on a

$$\sum_{j=1}^{k} \frac{1}{d_j} + \frac{1}{n} < \sum_{m=2}^{\infty} \frac{1}{m^2}.$$

Cette somme est notoirement égale à $\frac{\pi^2}{6} - 1 < 1$, ce qui donne la contradiction. Toutefois, sans cette connaissance, on peut aussi la majorer par le télescopage suivant :

$$\sum_{m=2}^{\infty} \frac{1}{m^2} < \sum_{m=2}^{\infty} \frac{1}{m(m-1)} = \sum_{m=2}^{\infty} \left(\frac{1}{m-1} - \frac{1}{m} \right) = 1,$$

qui permet aussi de retrouver la contradiction voulue.

Exercice 4.114. *(EGMO 2024 P3)* Un entier $n \geqslant 1$ est dit *spécial* si, pour tout diviseur d de n, $d(d+1) \mid n(n+1)$. Montrer que si quatre entiers distincts A, B, C et D sont tous spéciaux, alors $\mathrm{PGCD}(A, B, C, D) = 1$.

Solution 4.114. **Étape 1 :** Si $n \geqslant 2$ est spécial, il est sans facteur carré.

Supposons que n admette une facteur premier p tel que $v_p(n) \geqslant 2$. Notons $n = p^\alpha b$ avec $\alpha \geqslant 2$. On applique la propriété de l'énoncé au diviseur $p^{\alpha-1}b$, ce qui donne

$$p^{\alpha-1}b(p^{\alpha-1}b+1) \mid p^\alpha b(p^\alpha b+1) \Longrightarrow p^{\alpha-1}b+1 \mid p(p^\alpha b+1).$$

Comme $\alpha \geqslant 2$, p est premier avec $p^{\alpha-1}b+1$. On déduit que $p^{\alpha-1}b+1 \mid p^\alpha b+1$. Il vient que $p^{\alpha-1}b+1 \mid p^\alpha b+1-p(p^{\alpha-1}b+1) = 1-p$, mais $0 < p-1 < p^{\alpha-1}b+1$ car $\alpha \geqslant 2$. On a donc une contradiction et n n'admet pas de facteur carré.

Étape 2 : n admet au plus deux facteurs premiers.

On écrit $n = p_1 \dots p_k$ avec $p_1 < \dots < p_k$ et on suppose par l'absurde que $k \geqslant 3$. On applique la propriété de l'énoncé au diviseur $p_2 \dots p_k$ et il vient

$$p_2 \dots p_k(p_2 \dots p_k+1) \mid p_1 p_2 \dots p_k(p_1 p_2 \dots p_k+1) \Longrightarrow p_2 \dots p_k+1 \mid p_1(p_1 p_2 \dots p_k+1).$$

Or $p_1(p_1 p_2 \dots p_k+1) \equiv p_1 - p_1^2 \mod p_2 \dots p_k+1$, donc $p_2 \dots p_k+1 \mid p_1^2-p_1$. Mais $0 < p_1^2-p_1 < p_1^2 < p_2 \dots p_k+1$, ce qui est une contradiction. On a donc bien $k \leqslant 2$.

Étape 3 : Si $n = pq$ avec $p < q$, alors $q = p^2-p-1$.

En appliquant l'hypothèse de l'énoncé au diviseur p, on trouve que $p(p+1) \mid pq(pq+1)$, ou encore que $p+1 \mid q(pq+1)$. Puisque $pq+1 \equiv 1-q \mod p+1$, on trouve que $\boxed{p+1 \mid q(q-1)}$. De même, on obtient que $\boxed{q+1 \mid p(p-1)}$.

Si p était premier avec $q+1$, on aurait dans la seconde relation que $q+1 \mid p-1$, ce qui contredit $p < q$. Donc $\boxed{p \mid q+1}$. D'autre part, si $q \mid p+1$, alors $q \leqslant p+1 < q+1$, donc $q = p+1$ et $(p, q) = (2, 3)$. Mais 6 n'est pas joli car $3(3+1)$ ne divise par $6(6+1)$. Ainsi, q ne divise pas $p+1$ et donc $p+1$ est premier avec q, ce qui conduit à $\boxed{p+1 \mid q-1}$.

On pose $q+1 = kp$ avec k entier. De la division $q+1 \mid p(p-1)$ on déduit que $k \mid p-1$. De la division $p+1 \mid q-1 = kp-2$, on trouve que $0 \equiv kp-2 \equiv -k-2 \mod p+1$, donc $p+1 \mid k+2$. On écrit $p-1 = ka$ avec a entier. On déduit que $ka+2 = p+1 \mid k+2$, donc $a = 1$. Il vient que $p-1 = k$ puis que $\boxed{q = p^2-p-1}$.

Étape 4 : Conclusion

Prenons quatre entiers jolis disitncts A, B, C et D. Prenons p un diviseur premier éventuel de $\mathrm{PGCD}(A, B, C, D)$. Les seuls entiers jolis divisibles par p étant $p, p(p^2-p-1)$ et qp avec $p = q^2-q-1$, il y a un des quatre nombres B, C et D qui n'est pas divisible par p. Cette contradiction conclut.

Exercice 4.115. (EMO 2026 J2) Déterminer tous les entiers $n \geqslant 2$ vérifiant la propriété suivante : pour tout diviseur d de n, le produit de tous les autres diviseurs est une puissance parfaite.

Solution 4.115. **Réponse :** Il s'agit des entiers de la forme p^k pour p un nombre premier et $k \geqslant 2$.

Soit n un entier vérifiant l'énoncé. Supposons que n possède deux facteurs premiers distincts p_1 et p_2. On écrit $n = p_1^\alpha p_2^\beta A$, où A est premier avec n. On applique désormais la propriété de l'énoncé au diviseur p_1^x, p_2^y, avec x, y bien choisis.

Rappelons que le produit des diviseurs vaut $P(n) = n^{d(n)/2}$, où $d(n)$ est le nombre de diviseurs de n. En particulier, $P(n) = p_1^{\alpha d(n)/2} p_2^{\beta d(n)/2} A^{d(n)/2}$. Pour que $P(n)/p_1^x p_2^y$ ne soit pas une puissance parfaite, il suffit donc de trouver x et y tels que $\mathrm{PGCD}(\alpha d(n)/2 - x, \beta d(n)/2 - y) = 1$.

D'après le théorème de Bezout, il existe deux entiers x et y tels que $\alpha y - \beta x = \mathrm{PGCD}(\alpha, \beta)$. De plus, on peut choisir x et y de sorte que $0 \leqslant x \leqslant \alpha$ et $0 \leqslant y \leqslant \beta$: si $y > \beta$, alors $\beta x > \alpha\beta - \mathrm{PGCD}(\alpha, \beta) \geqslant \beta(\alpha - 1)$, ce qui donne $x \geqslant \alpha$. Mais alors on peut remplacer (x, y) par $(x - \alpha, y - \beta)$ et obtenir de proche en proche un couple d'entiers vérifiant la relation de Bezout et les encadrements annoncés.

A présent, on remarque que $\dfrac{\alpha}{\mathrm{PGCD}(\alpha,\beta)} x - \dfrac{\beta}{\mathrm{PGCD}(\alpha,\beta)} y = 1$, donc x et y sont premiers entre eux. Si p est désormais un diviseur premier de $\mathrm{PGCD}(\alpha d(n)/2 - x, \beta d(n)/2 - y)$, on a que

$$p \mid \left(\alpha \frac{d(n)}{2} - x\right) y - \left(\beta \frac{d(n)}{2} - y\right) x = \frac{d(n)}{2}(\alpha y - x\beta) = \frac{d(n)}{2}\mathrm{PGCD}(\alpha, \beta).$$

Mais alors

$$p \mid \frac{d(n)}{2}\mathrm{PGCD}(\alpha, \beta) \mid \alpha d(n)/2,$$

donc p divise aussi x. Comme de même p divise y et que x et y sont premiers entre eux, on conclut une contradiction. Ainsi, n ne peut pas avoir deux facteurs premiers distincts et $\boxed{n \text{ est une puissance d'un nombre premier.}}$

Réciproquement, si $n = p^k$ est une puissance d'un nombre premier, alors il faut $k \geqslant 3$ (sinon on pourrait prendre p^k comme diviseur pour contredire l'énoncé). Dans le cas $k \geqslant 2$, le produit de ses diviseurs est bien une puissance de p et supérieure à 1, ce qui conclut.

5 Prendre son envol

Exercice 5.1. (St Pétersbourg 2016 grade 9 round 2) Soient p et q des nombres premiers distincts tels que $p < 2q$ et $q < 2p$. Montrer qu'il existe deux entiers consécutifs tels que le plus grand diviseur premier de l'un d'entre eux est p et le plus grand diviseur premier de l'autre est q.

Solution 5.1. Supposons que $p < q$. Soit a un inverse de q modulo p appartenant à $[\![1, p-1]\!]$. Parmi les nombres aq et $(p-a)q$, l'un d'eux est strictement inférieur à p^2 : si $aq > p^2$, alors $(p-a)q < pq - p^2 < p^2$ car $q < 2p$.

- Si $n = aq < p^2$, alors n est un multiple de q vérifiant $0 < n < pq$. Ainsi, tout diviseur premier de n autre que q est inférieur à p, donc q est le plus grand diviseur premier de n. Ensuite, $n-1 = aq-1$ est divisible par p par hypothèse. Comme $n - 1 \leqslant p^2$, alors tout diviseur premier de $n-1$ autre que p est inférieur à p.
- Si $m = (p-a)q < p^2$, alors de même, le plus grand facteur premier de m est q. D'autre part, $m + 1 \equiv -aq + 1 = 0 \mod p$ donc $m+1$ est multiple de p et comme $m + 1 < p^2 + 1$, $m + 1 \leqslant p^2$ et de même le plus grand facteur premier de $m + 1$ est p.

Exercice 5.2. (Pologne MO 2010 Round final) Soit p un nombre premier tel que $p \equiv 2 \mod 3$. Pour tout entier $k \geqslant 1$, on pose $a_k = k^2 + k + 1$. Montrer que $a_1 \dots a_{p-1} \equiv 3 \mod p$.

Solution 5.2. Notons que si $kneq1$, $a_k = \dfrac{k^3-1}{k-1}$ et

$$a_2 \dots a_{p-1} \equiv \prod_{k=2}^{p-1} \frac{k^3-1}{k-1} \mod p.$$

Notons que $k \mapsto k^3 \mod p$ est injective modulo p. En effet, si k et k' sont deux éléments de $\{2, \dots, p-1\}$ tels que $k^3 \equiv k'^3 \mod p$, alors $(kk'^{-1})^3 \equiv 1 \mod p$. L'ordre ω de kki^{-1} modulo p vérifie donc $\omega \mid \mathrm{PGCD}(3, p-1) = 1$ (puisque $p \equiv 2 \mod 3$). Ainsi, $kk'^{-1} \equiv 1 \mod p$ et $k \equiv k' \mod p$, ce qui montre l'injectivité. Ainsi, la fonction $k \mapsto k^3 \mod p$ est une bijection de $\{2, \dots, p-1\}$ dans lui-même. On déduit que

$$\prod_{k=2}^{p-1} \frac{k^3-1}{k-1} \equiv \frac{\prod_{k=2}^{p-1}(k^3-1)}{\prod_{k=2}^{p-1}(k-1)} = \frac{\prod_{k=2}^{p-1}(k-1)}{\prod_{k=2}^{p-1}(k-1)} \equiv 1 \mod p.$$

Finalement,

$$a_1 \dots a_{p-1} \equiv a_1 \equiv 3 \mod p.$$

Exercice 5.3. (BXMO 2022) Un sous-ensemble A de $\mathbb{N}$ est dit *convenable* si chaque entier $n > 0$ admet au plus un facteur premier p tel que $n - p \in A$.

1. Montrer que l'ensemble des carrés parfaits est convenable.
2. Donner un ensemble convenable infini et ne contenant aucun carré parfait.

Solution 5.3. 1) Soit n un entier admettant deux facteurs premiers p et q tels que $n - p = a^2$ et $n - q = b^2$. On peut alors poser $a = pc$ et $b = qd$, poser $n = pqk$.
On obtient que $p^2c^2 + p = q^2d^2 + q$. Maintenant

$$p^2c^2 = q^2d^2 + q - p < (qd+1)^2$$

donc $pc < qd + 1$ et de même $qd < pc + 1$, de sorte que $qd = pc$ donc $p = q$, ce qui est absurde.

2) On prend un de nos ensembles préférés avec une croissance sur linéaire, pour espérer adapter l'argument plus haut. Mon ensemble préféré, c'est l'ensemble des $n!$ avec $n \geqslant 2$. Comme il existe p ne divisant qu'une fois $n!$, l'ensemble est disjoint de l'ensemble des carrés parfaits.

Maintenant on prend n et on écrit $n-p = a!$ et $n-q = b!$. Si $a > b$, alors $b!$ divise $a!$, donc q divise $b! + q = a! + p$ et q divise $a!$, donc q divise p, ce qui est absurde. L'ensemble est bien convenable.

Exercice 5.4. (Cyberspace Mathematical Competition P2) On définit la fonction f par $f(x) = 3x^2 + 1$ pour tout entier x. Montrer que, pour tout entier n, le produit

$$f(1)f(2)\dots f(n)$$

possède au plus n diviseurs premiers distincts.

Solution 5.4. On procède par récurrence sur n.

Initialisation : $f(1) = 4$ admet un unique diviseur premier.

Hérédité : On suppose la propriété vraie pour $n - 1 \geqslant 1$ un entier. Soit p un éventuel diviseur de $f(n)$ ne divisant aucun des $f(i)$ précédents. Comme $p \mid f(n) = 3n^2 + 1$, p est différent de 3 et premier avec n. Il s'agit de démontrer que p est grand et donc qu'il n'y a pas plusieurs tels p.

Si $p < n$, alors $f(n-p) \equiv f(n) \equiv 0 \mod p$, contredisant l'hypothèse sur p.

Si $n < p < 2n$, alors $1 \leqslant p - n < n$ et $f(p-n) \equiv f(n) \equiv 0 \mod p$, contredisant à nouveau l'hypothèse sur p.

On déduit que $\boxed{p > 2n}$. S'il y avait un autre diviseur premier q ne divisant pas les précédents $f(i)$, on aurait alors $q > 2n$ également et $f(n) \geqslant pq > 4n^2$, ce qui est absurde. Donc il y au plus un diviseur premier de $f(n)$ ne divisant pas les $f(i)$ précédent, donc le produit donné a au plus n facteurs premiers distincts, ce qui achève la récurrence.

Exercice 5.5. (Iran MO 2009 Round 2) Soient $a_1 < \ldots < a_n$ des entiers strictement positifs. On suppose que pour toute paire d'entiers (i, j) vérifiant $1 \leqslant i < j \leqslant n$, le nombre $\dfrac{a_i}{a_j - a_i}$ est un entier.

Montrer que pour tous indices $i < j$, $ia_j \leqslant ja_i$.

Solution 5.5. Soit m vérifiant $1 \leqslant m \leqslant n - 1$.
Notons $k_i = \dfrac{a_i}{a_{m+1} - a_i}$ pour tout $i \leqslant m$. L'énoncé nous dit que les termes de la suite (k_i) sont des entiers strictement positifs. Remarquons également que si $i < j$, on a $a_i < a_j$ et donc

$$k_i = \frac{a_i}{a_{m+1} - a_i} = \frac{1}{\frac{a_{m+1}}{a_i} - 1} < \frac{1}{\frac{a_{m+1}}{a_j} - 1} = \frac{a_j}{a_{m+1} - a_j} = k_j$$

La suite $(k_i)_{i \leqslant m}$ est donc une suite strictement croissante d'entiers strictement positifs. on a donc $k_i \geqslant i$ pour tout $i \leqslant m$.
En particulier, $\dfrac{a_m}{a_{m+1} - a_m} = k_m \geqslant m$. Cette inégalité se réécrit $\boxed{(m+1)a_m \geqslant ma_{m+1}}$.

Prenons à présent $i < j$. Pour tout $i \leqslant k \leqslant j - 1$, d'après la question précédente, $\frac{a_{k+1}}{a_k} \leqslant \frac{k+1}{k}$. En multipliant ces inégalités pour k allant de i à $j - 1$, on trouve via un télescopage :

$$\frac{a_j}{a_i} = \frac{a_j}{a_{j-1}} \cdot \frac{a_{j-1}}{a_{j-2}} \cdot \ldots \cdot \frac{a_{i+2}}{a_{i+1}} \cdot \frac{a_{i+1}}{a_i} \leqslant \frac{j}{j-1} \cdot \frac{j-1}{j-2} \cdot \ldots \cdot \frac{i+2}{i+1} \cdot \frac{i+1}{i} = \frac{j}{i}$$

ce qui se réécrit $ia_j \leqslant ja_i$, comme voulu.

Exercice 5.6. (IMO SL 2015 N1) Déterminer tous les entiers M pour lesquels la suite $a_0, a_1, \ldots$ définie par

$$a_0 = M + \frac{1}{2}, \quad \text{et} \quad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{pour } k = 0, 1, \ldots$$

contient au moins un entier.

Solution 5.6. **Réponse :** Il s'agit de tous les entiers $M > 1$.

➢ **Commentaire :**

> Pour voir des entiers M non solutions, on s'intéresse aux suites vérifiant la relation et qui sont constantes. Pour que $a_{k+1} = a_k$, il faut que $\lfloor a_k \rfloor = 1$.
>
> Pour voir quels entiers M sont solutions, on calcule les premiers termes de la suite en mettant les termes sous forme de fraction irréductible. C'est alors qu'on est amené à s'intéresser à la valuation $2-$adique de $M - 1$.

Tout d'abord, si $M = 1$, alors $a_0 = 3/2$ et $a_1 = 3/2$. Par récurrence immédiate, la suite (a_k) est constante égale à $3/2$ et ne contient aucun entier.

Supposons que $M > 1$. On procède par récurrence sur $\alpha = v_2(M-1)$ pour montrer que la suite contient un terme entier.

Initialisation : Si $\alpha = 0$, alors $M-1$ est impair donc M est pair et $a_1 = M(M+1/2) = (2M+1)M/2$ est bien entier.

Hérédité : On suppose la propriété vraie pour tout M tel que $v_2(M-1) \leqslant \alpha$, avec $\alpha \geqslant 0$ fixé. On a

$$a_1 = M\left(M + \frac{1}{2}\right) = \frac{2M^2 - 2M + 1}{2} + \frac{1}{2}.$$

Posons $N = \frac{2M^2-2M+1}{2}$. On a $N - 1 = \dfrac{2M^2 - 2M + 3}{2} = \dfrac{(2M+3)(M-1)}{2}$. Comme $2M+3$ est impair, on déduit que $v_2(N-1) = v_2((M-1)/2) = v_2(M-1) - 1$. D'après l'hypothèse de récurrence, il existe un terme de la suite $(a_{k+1})_k$ qui est entier, donc la suite (a_k) contient elle-même un entier. Ceci achève la récurrence et conclut l'exercice.

Exercice 5.7. (Thaïlande TSTST 2025) Soient a et b des entiers strictement positifs. Montrer qu'il existe une infinité d'entiers n tels que $a^n + b^n + n!$ n'est pas un carré parfait.

Solution 5.7.

➢ **Commentaire :**

> On a plusieurs choix : soit on trouve n et p premier tel que $v_p(a^n + b^n + n!) = 1$, soit on trouve n et p tels que $a^n + b^n + n!$ n'est pas un carré modulo p. Ceci donne les deux solutions qui suivent.

On distingue plusieurs cas :

➢ Si a et b ont un diviseur commun p, on choisit $n = p^k$ avec k à choisir. Notons $c = \min(v_p(a), v_p(b))$. On a d'une part

$$v_p(a^n + b^n) \geqslant nc = p^k c$$

et

$$v_p(n!) = \frac{p^k}{p} + \frac{p^k}{p^2} + \ldots + \frac{p^k}{p^k} = \frac{k(k-1)}{2}.$$

Pour k suffisamment grand, $v_p(a^n+b^n) > v_p(n!)$ et $v_p(a^n+b^n+n!) = v_p(n!) = k(k-1)/2$. En choisissant $k \equiv 2 \mod 4$, cette valuation est impaire donc $a^n + b^n + n!$ n'est pas un carré.

➢ Si $\mathrm{PGCD}(a,b) = 1$ et $a+b$ admet un diviseur premier impair p ne divisant ni a ni b, on fait le même jeu : on choisit $n = p^k$. On a toujours $v_p(n!) = k(k-1)/2$. D'autre part, d'après le lemme LTE,

$$v_p(a^n + b^n) = v_p(a+b) + v_p(n) = v_p(a+b) + k.$$

Pour k suffisamment grand, $v_p(a^n + b^n) < v_p(n!)$ et $v_p(a^n + b^n + n!) = v_p(a+b) + k$. En choisissant k tel que $v_p(a+b) + k$ est impair, on trouve que $v_p(a^n + b^n + n!)$ est impair donc $a^n + b^n + n!$ n'est pas un carré.

➢ Si $\mathrm{PGCD}(a,b) = 1$ et $a + b = 2^k$ est une puissance de 2, (ce qui correspond au cas restant), alors a et b sont impairs et pour tout entier pair $n \geqslant 4$, on a $4 \mid n!$ et $a^n + b^n \equiv 1 + 1 = 2 \mod 4$. Ainsi, $a^n + b^n + n! \equiv 2 \mod 4$ donc n'est pas un carré parfait.

Solution alternative

Soit $p \equiv 5 \mod 8$ un nombre premier ne divisant pas a ou b. On dispose d'une infinité de tels nombres premiers d'après le théorème de Dirichlet. En prenant $n = 2(p-1)$, on a que $p \mid n!$ et $a^n + b^n + n! \equiv (a^2)^{p-1} + (b^2)^{p-1} \equiv 2 \mod p$.

La loi de réciprocité quadratique indique que 2 n'est pas un carré modulo p, donc $a^n + b^n + n!$ n'est pas un carré modulo p et donc pas un carré parfait.

Exercice 5.8. (MEMO 2018 T7) Soit $a_1, \dots$ une suite d'entiers strictement positifs telle que $a_1 = 1$ et pour tout $k \geqslant 1$,

$$a_{k+1} = 1 + a_k^3.$$

Montrer que pour tout nombre premier p de la forme $3\ell + 2$, p divise un terme de la suite (a_k).

Solution 5.8. La fonction $f : x \mod p \mapsto 1 + x^3 \mod p$ est injective : en effet, si $1 + x^3 \equiv 1 + y^3 \mod p$. Si $p \mid x$, on a $y^3 \equiv 0 \mod p$ donc $p \mid y$ et $x = y \mod p$. Sinon, l'équation devient $(x^{-1}y)^3 \equiv 1 \mod p$. L'ordre de $x^{-1}y$ est donc un diviseur de 3 et de $p - 1 = 3\ell + 1$ (d'après le petit théorème de Fermat), ce qui implique que cet ordre vaut 1. On a donc $x^{-1}y \equiv 1 \mod p$ donc $x \equiv y \mod p$ et f est bien injective.

D'après le principe des tiroirs, la suite (a_k) prenant un nombre fini de valeurs modulo p, on dispose de deux entiers a_m et a_n égaux modulo p, avec $m < n$. On a alors $f(a_{m-1}) = f(a_{n-1}) \mod p$ et par injectivité de f, on déduit $a_{m-1} \equiv a_{n-1} \mod p$. Par récurrence descendante, $a_{m-r} \equiv a_{n-r} \mod p$ pour tout r. En particulier $a_{n-m+1} \equiv a_1 = 1 \mod p$, donc $f(a_{n-m}) \equiv f(0) \mod p$, ce qui amène $\boxed{a_{m-n} \equiv 0 \mod p}$ comme voulu.

Exercice 5.9. (BMO 2018 N2) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que, pour tous entiers $m, n \geqslant 1$,

$$n! + f(m)! \mid f(n)! + f(m!).$$

Solution 5.9. En posant $m = n = 1$, on trouve $1 + f(1)! \mid f(1)! + f(1)$, donc $1 + f(1)! \mid f(1) - 1$. Comme pourtant $0 \leqslant f(1) - 1 < 1 + f(1)!$, on déduit que $\boxed{f(1) = 1}$.

En prenant $m = 1$, on trouve $n! + 1 \mid f(n)! + 1$ ce qui implique que $n! \leqslant f(n)!$, soit $\boxed{n \leqslant f(n)}$.

Soit désormais p un nombre premier impair. En posant $m = 1$ et $n = p - 1$, on a $(p-1)! + 1 \mid f(p-1)! + 1$. Or, d'après le théorème de Wilson, $p \mid (p-1)! + 1$, ce qui implique que $p \mid f(p-1)! + 1$ et donc p ne divise pas $f(p-1)!$. On a donc $f(p-1) \leqslant p - 1$ et $\boxed{f(p-1) = p-1}$ pour tout nombre premier.

Fixons à présent m un entier et prenons $n = p-1$. On a $(p-1)! + f(m)! \mid (p-1)! + f(m!)$, soit $(p-1)! + f(m)! \mid (p-1)! + f(m!) - ((p-1)! + f(m)!) = f(m!) - f(m)!$. Comme cette divisibilité est vraie pour une infinité de p premiers, on a $\boxed{f(m!) = f(m)!}$ pour tout m.

Enfin, pour tout n, on a donc $n! + f(m)! \mid f(n)! + f(m!) = f(n)! + f(m)!$. La même manipulation donne donc $n! + f(m)! \mid f(n)! - n!$ pour tout m, donc $f(n)! = n!$ et $\boxed{f(n) = n}$ pour tout entier n.

Réciproquement, la fonction identité est bien solution.

Exercice 5.10. *(IMO SL 2024 N2)* Déterminer tous les ensembles $\mathcal{S}$ finis non vides d'entiers strictement positifs ayant la propriété suivante :

Pour tout choix de deux entiers a et b dans $\mathcal{S}$, il existe un entier c dans $\mathcal{S}$ tel que a divise $b+2c$.

Solution 5.10.

Réponse : Les seuls ensembles solutions sont les ensembles de la forme $\{k, 3k\}$ et $\{k\}$, ou k peut prendre n'importe quelle valeur entière strictement positive.

Soit $\mathcal{S} = \{a_1, \ldots, a_n\}$ un ensemble solution. Notons que si $n = 1$, tout singleton vérifie la propriété de l'énoncé. Dans la suite, on suppose donc $n \geqslant 2$.

On commence par remarquer que les ensembles $\{ka_1, \ldots, ka_n\}$ et $\{a_1/d, \ldots, a_n/d\}$ sont également solutions du problème pour tout entier $k \geqslant 1$ et tout diviseur d commun à chacun des a_i. Ainsi, quitte à diviser chacun des a_i par le PGCD des a_i, on peut supposer que les entiers $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble.

Montrons dans ce cas que les entiers sont tous impairs. Puisqu'ils sont premiers entre eux dans leur ensemble, les a_i ne peuvent pas tous être pairs. Supposons alors qu'il existe un entier a de $\mathcal{S}$ qui soit pair et un entier b de $\mathcal{S}$ qui est impair. D'après la propriété, il existe un entier c de $\mathcal{S}$ tel que $a \mid b + 2c$. Or, $b + 2c$ est impair et a est pair, la divisibilité est donc absurde. Ainsi, tous les entiers de $\mathcal{S}$ sont impairs.

Quitte à renuméroter les entiers, on peut supposer que $a_1 < \ldots < a_n$. Pour tout indice $i < n$, en appliquant la propriété de l'énoncé à la paire (a_n, a_i), il existe un indice $f(i)$ tel que $a_n \mid a_i + 2a_{f(i)}$. On déduit que

$$a_n \leqslant a_i + 2a_{f(i)} < a_n + 2a_n = 3a_n.$$

De plus, $a_i + 2a_{f(i)}$ est impair, donc il s'agit d'un multiple impair de a_n strictement inférieur à $3a_n$, donc $a_i + 2a_{f(i)} = a_n$. En particulier, $a_{f(i)} < a_n$ donc $f(i) < n$.

Si $i < j$, on remarque que

$$2a_{f(i)} = a_n - a_i > a_n - a_j = 2a_{f(j)},$$

si bien que $f(i) > f(j)$. La fonction f est donc une bijection décroissante de $\{1, \ldots, n-1\}$, de sorte que $f(i) = n - i$ pour tout indice i. En particulier, on a

$$a_1 + 2a_{n-1} = a_1 + 2a_{f(1)} = a_n = a_{n-1} + 2a_{f(n-1)} = a_{n-1} + 2a_1,$$

si bien que $a_{n-1} = a_1$ et $n = 2$.

En appliquant la propriété de l'énoncé à la paire (a_2, a_1), on trouve que $a_2 \mid a_1 + 2a_2$ ou $a_2 \mid a_1 + 2a_1$. Dans le premier cas, on trouve que $a_2 \mid a_1$, ce qui est impossible car $0 < a_1 < a_2$. Dans le second cas, on trouve $a_2 \mid 3a_1$. Comme a_2 et a_1 sont premiers entre eux, on trouve $a_2 \mid 3$, et comme $a_2 > a_1 \geqslant 1$, on trouve $a_2 = 3$. Mais alors en appliquant la propriété de l'énoncé à la paire (a_1, a_2), on a $a_1 \mid a_2 = 3$ ou $a_1 \mid 3a_2 = 9$. Dans tous les cas, comme a_1 est premier avec a_2, on déduit que $a_1 = 1$.

Réciproquement, on vérifie que la paire $(1, 3)$ satisfait l'énoncé. Ainsi, les ensembles de la formes $\{k, 3k\}$ avec $k \geqslant 1$ entier sont les seuls ensembles solutions du problème si $n \geqslant 2$.

Exercice 5.11. (BXMO 2013) 1) Déterminer tous les entiers g avec la propriété suivante : pour tout nombre premier p impair, il existe un entier strictement positif n tel que p divise les deux entiers

$$g^n - n \quad \text{et} \quad g^{n+1} - (n+1).$$

2) Déterminer tous les entiers g avec la propriété suivante : pour tout nombre premier p impair, il existe un entier strictement positif n tel que p divise les deux entiers

$$g^n - n^2 \quad \text{et} \quad g^{n+1} - (n+1)^2.$$

Solution 5.11. 1) **Réponse :** L'unique entier est $g = 2$.

Si g admet un diviseur p impair et vérifie la propriété, il existe un entier n tel que $p \mid g^n - n$ et $p \mid g^{n+1} - (n+1)$. Comme $p \mid g$, cela implique que p divise n et $n+1$, ce qui est absurde. On déduit que g n'admet pas de diviseur impair et que $\boxed{g \text{ est une puissance de } 2}$.

Posons $g = 2^k$. Si $k \geqslant 2$, alors le nombre $2^k - 1$ admet un diviseur premier impair p. Mais alors

$$g^n - n \equiv (2^k)^n - n \equiv 1 - n \mod p, \quad g^{n+1} - (n+1) \equiv (2^k)^{n+1} - (n+1) \equiv 1 - (n+1) = -n \mod p.$$

Comme il n'existe pas d'entier n tel que $1 - n$ et n soient tous les deux divisibles par p, on conclut que g ne vérifie pas la propriété.

Réciproquement, si $g = 2$ et p un nombre premier impair, d'après le théorème des restes chinois, il existe un entier n vérifiant

$$n \equiv 0 \mod (p-1), \quad n \equiv 1 \mod p.$$

Alors d'après le petit théorème de Fermat, $2^n - n \equiv 1 - n = 0 \mod p$. De plus $2^{n+1} = 2 \cdot 2^n \equiv 2n \equiv n + 1 \mod p$ car $p \mid n - 1$. L'entier 2 vérifie donc la propriété.

2) **Réponse :** Seul 4 est solution.

De même que précédemment, on trouve que g doit être une puissance de 2.

- Si $g = 1$, on applique la propriété à $p = 5$. il existe un entier n tel que $5 \mid 1 - n^2$ (donc $n \equiv 1, 4 \mod 5$) et $5 \mid 1 - (n+1)^2$ (donc $n \equiv 0, 3 \mod 5$). On a donc une contradiction.
- Si $g = 2$, on applique la propriété à $p = 3$. On dispose d'un entier n tel que $2^n \equiv n^2 \mod 3$ (donc $n \neq 0 \mod 3$) et $2^{n+1} \equiv (n+1)^2 \mod 3$ (donc $n+1 \neq 0 \mod 3$). on trouve que $2^{n+1} \equiv (n+1)^2 \equiv 1 \equiv n^2 \equiv 2^n \mod 3$, ce qui est absurde.
- Si $g = 2^k$ avec $k \geqslant 2$, on choisit p un diviseur premier de $g - 1$. L'entier n donné par l'énoncé doit vérifie $(n+1)^2 \equiv n^2 \equiv 1 \mod p$. De $n^2 \equiv 1 \mod p$, on déduit que $n \equiv \pm 1 \mod p$. De $(n+1)^2 \equiv 1 \mod p$, on déduit que $n \equiv 0, -2 \mod p$. La seule possibilité est donc que $-2 \equiv 1 \mod p$ et $p = 3$. Cela signifie que $2^k - 1$ a pour seul facteur premier le nombre 3 et qu'il existe m tel que $2^k - 1 = 3^m$. Comme $2^k \equiv 1 \mod 3$, l'entier k est pair et on écrit $k = 2a$. Mais alors $3^m = (2^a - 1)(2^a + 1)$ donc $2^a - 1$ et $2^a + 1$ sont tous les deux des puissances de 3, dont la différence fait 2. On déduit que $2^a - 1 = 1$ et $2^a + 1 = 3$ et $a = 1$ et $\boxed{g = 4}$.

  Réciproquement, prenons un nombre premier p impair. D'après la question 1), il existe n tel que $2^n \equiv n \mod p$ et $2^{n+1} \equiv (n+1) \mod p$. Mais alors en élevant au carré, $4^n \equiv n^2 \mod p$ et $4^{n+1} \equiv (n+1)^2 \mod p$, ce qui conclut.

Exercice 5.12. (EMC 2024 P1) Une paire d'entiers distincts (a, b) est dite *binaire* si $ab+1$ est une puissance de 2. Quel est le plus grand nombre de paires binaires que peut contenir un ensemble S de n entiers strictement positifs ?

Solution 5.12. **Réponse :** le nombre maximal est $n-1$.

Le problème demande de trouver le plus grand entier vérifiant une propriété, il contient donc nécessairement deux parties : l'analyse où l'on montre que tout ensemble de taille n contient au plus $n-1$ paires binaires, et la construction où l'on donne un exemple d'ensemble contenant au moins $n-1$ paires binaires.

Construction : Posons $S = \{2^k - 1, 1 \leqslant k \leqslant n\}$. S est de taille n et pour tout k, la paire $(1, 2^k - 1)$ est binaire. Donc l'ensemble S contient au moins $n-1$ paires binaires.

Analyse : Soit $S = \{a_1, \ldots, a_n\}$ un ensemble de taille n. On introduit le graphe G dont les sommets sont les a_i et où deux sommets a et b sont reliés si et seulement si (a, b) est binaire. Nous allons montrer que G ne contient pas de cycle. Comme un graphe de taille n sans cycle contient au plus $n-1$ arêtes, il y a au plus $n-1$ arêtes dans G donc au plus $n-1$ paires binaires dans S.

Supposons que G contienne un cycle $(b_1 \ldots b_k)$. On dispose d'entiers $x_1, \ldots, x_k$ tels que

$$b_1 b_2 = 2^{x_1} - 1, \quad b_2 b_3 = 2^{x_2} - 1, \quad \ldots \quad b_k b_1 = 2^{x_k} - 1.$$

Comme les b_i sont strictement positifs et distincts, $x_i \geqslant 2$ pour tout i et donc les b_i sont impairs. Supposons, quitte à renuméroter, que x_1 est le plus grand des x_i. En soustrayant les équations, on a

$$b_1(b_2 - b_n) = 2^{x_1} - 2^{x_n} = 2^{x_n}(2^{x_1 - x_n} - 1) \quad \Longrightarrow \quad b_1 \mid 2^{x_1 - x_n} - 1,$$

$$b_2(b_1 - b_3) = 2^{x_1} - 2^{x_2} = 2^{x_2}(2^{x_1 - x_2} - 1) \quad \Longrightarrow \quad b_2 \mid 2^{x_1 - x_2} - 1.$$

Il vient

$$2^{x_1} - 1 = b_1 b_2 \leqslant (2^{x_1 - x_n} - 1)(2^{x_1 - x_2} - 1).$$

D'autre part, puisque

$$2^{x_1} = b_1 b_2 + 1 \leqslant b_1 b_2 b_3 b_n + 1 < (b_1 b_n + 1)(b_2 b_3 + 1) < 2^{x_n + x_2},$$

on a $x_1 < x_2 + x_n$. Ainsi, on a

$$2^{x_1} - 1 \leqslant (2^{x_1 - x_n} - 1)(2^{x_1 - x_2} - 1) = 2^{x_1 + x_1 - x_2 - x_n} - 2^{x_1 - x_n} - 2^{x_1 - x_2} + 1 < 2^{x_1} + 1 - 2^{x_1 - x_n} - 2^{x_1 - x_2} \leqslant 2^{x_1} - 1.$$

Cela implique que $(2^{x_1 - x_n} - 1)(2^{x_1 - x_2} - 1) = 0$, ce qui conduit à $b_n = b_1$ ou $b_1 = b_2$, contredisant que les b_i sont distincts. Cette contradiction conclut.

Remarque : Il est également possible d'invoquer le théorème de Zsigmondy pour trouver une contradiction dans la divisibilité $2^{x_1} - 1 \mid (2^{x_1 - x_n} - 1)(2^{x_1 - x_2} - 1)$. Il faut alors éviter l'exception $x_1 = 6$, soit $b_1 b_2 = 63$, ce qui occasionne une disjonction de cas sur les valeurs de b_i.

Exercice 5.13. (Vietnam TST 2001) Soit $a_0 < a_1 < \dots$ une suite strictement croissante d'entiers strictement positifs. On suppose qu'il existe une constante $C > 0$ telle que, pour tout indice n, $a_{n+1} - a_n < C$. Montrer qu'il existe des indices i et j distincts tels que $a_i \mid a_j$.

Solution 5.13. Il n'y a pas beaucoup de contrôle sur la suite (a_n), l'une des seules certitudes que l'on possède est que tout intervalle de longueur C contient un terme de la suite. L'idée est alors de construire des intervalles $[\![b_i, b_i + C - 1]\!]$ dont les termes se divisent deux à deux d'un intervalle à l'autre. Plus précisément on montre le lemme suivant :

Lemme : Soit b un entier. Il existe un entier c tel que, pour tout $0 \leqslant \ell \leqslant C - 1$, $b + \ell \mid c + \ell$.

Preuve : Il suffit de prendre $c = b + b(b+1)\dots(b+C-1)$. En effet, pour tout entier ℓ, on $b + \ell \mid c - b$ donc $b + \ell \mid c - b + (b + \ell) = c + \ell$. □

On peut désormais conclure l'exercice. Soit (b_i) une suite construite par récurrence telle que, pour tout indice i et tout entier $\ell \in [\![0, C-1]\!]$, on a $b_i + \ell \mid b_{i+1} + \ell$. Puisque $a_{n+1} - a_n < C$ pour tout indice n, chaque intervalle $[\![b_i, b_i + C - 1]\!]$ contient au moins un terme a_{n_i} de la suite. D'après le principe des tiroirs, il existe deux indices $i < j$ et un entier ℓ tels que $a_{n_i} = b_i + \ell$ et $a_{n_j} = b_j + \ell$. Par construction,

$$a_{n_i} = b_i + \ell \mid b_{i+1} + \ell \mid \dots \mid b_j + \ell = a_{n_j},$$

ce qui est le résultat voulu.

Exercice 5.14. (MEMO 2023 P8) Soient A et B des entiers strictement positifs. Soit (x_n) la suite définie par

$$x_{n+1} = A \cdot \mathrm{PGCD}(x_n, x_{n-1}) + B.$$

Montrer que la suite (x_n) ne prend qu'un nombre fini de valeurs distinctes.

Solution 5.14. Il suffit de montrer que la suite (x_n) est bornée. Il suffit pour cela de montrer que la suite $\mathrm{PGCD}(x_n, x_{n-1})$ est elle-même bornée. On pose donc $d_n = \mathrm{PGCD}(x_n, x_{n-1})$.

On commence par montrer que $\delta_n = \mathrm{PGCD}(d_n, B)$ est constant à partir d'un certain rang. En effet, on a par combinaison linéaire que

$$\delta_n \mid Ad_n + B = x_{n+1}, \quad \delta_n \mid d_n \mid x_n, \quad \Longrightarrow \quad \delta_n \mid d_{n+1} = \mathrm{PGCD}(x_n, x_{n+1}), \quad \Longrightarrow \quad \boxed{\delta_n \mid \delta_{n+1}}.$$

La suite (δ_n) est donc une suite croissante de diviseurs de B, donc elle stationne en un entier δ à partir du rang N. Quitte à diviser la relation par δ et à considérer les suites (x_n/δ) et (d_n/δ) à partir du rang n, on peut considérer que $\delta = 1$ et que $\mathrm{PGCD}(d_n, B) = 1$. Notons alors que si un nombre premier divise A et B, alors $p \mid x_{N+1}, x_{N+2}$ donc $p \mid d_{N+1}$, contredisant notre hypothèse. On a donc $\mathrm{PGCD}(A, B) = 1$.

Soit $n \geqslant N$. On a désormais $d_{n+1} \mid x_{n+1} = Ad_n + B$ et $d_{n+1} \mid x_n = Ad_{n-1} + B$. On déduit que $d_{n+1} \mid A(d_n - d_{n-1})$. Si un nombre premier divise d_{n+1} et A, alors $p \mid Ad_n + B$ donc $p \mid B$, ce qui est encore absurde. Donc d_{n+1} est premier avec A et $\boxed{d_{n+1} \mid d_n - d_{n-1}}$.

Si on avait $d_n = d_{n-1}$, on aurait $d_n \mid x_n = Ad_{n-1} + B$ donc $d_n \mid B$, ce qui implique $d_{n-1} = d_n = 1$ puis $x_{n+1} = Ad_n + B = Ad_{n-1} = x_n$, donc $d_n = x_n$ et $1 = x_n = Ad_{n-1} + B = A + B$, ce qui est absurde. Bref, $d_n \neq d_{n-1}$.

Mais alors $d_{n+1} \leqslant |d_n - d_{n-1}| \leqslant \max\{d_n, d_{n-1}\}$, donc la suite (d_n) est bien bornée, comme voulue.

Exercice 5.15. (EGMO 2017 P5) Soit $n \geqslant 2$ un entier. Un $n-$uplet $(a_1, \ldots, a_n)$ d'entiers strictement positifs (pas forcément distincts) est dit *onéreux* s'il existe un entier strictement positif k tel que

$$(a_1 + a_2)(a_2 + a_3)\ldots(a_n + a_1) = 2^{2k-1}$$

1) Trouver tous les entiers $n \geqslant 2$ pour lesquels il existe un $n-$uplet onéreux.
2) Montrer que pour tout entier positif m, il existe un entier $n \geqslant 2$ tel que m appartient à un $n-$uplet onéreux.

Solution 5.15. 1) Si n est impair, le $n-$uplet $(1, \ldots, 1)$ convient. Supposons que $n = 2\ell$ et qu'il existe un $n-$uplet onéreux $(a_1, \ldots, a_n)$ tel que $(a_1 + a_2)(a_2 + a_3)\ldots(a_n + a_1) = 2^{2k-1}$ avec k entier.
Si a_t est le plus grand élément du $n-$uplet, alors

$$2^k = a_t + a_{t-1} \leqslant 2a_t < 2(a_t + a_{t+1}) = 2^{k'+1}$$

$$2^{k'} = a_t + a_{t+1} \leqslant 2a_t < 2(a_t + a_{t-1}) = 2^{k+1}$$

On déduit que $2^k = 2^{k'}$ et $a_{t-1} = a_{t+1}$. On peut alors retirer a_{t-1} et a_t, on obtient un $n-2$ uplet onéreux. Par récurrence descendante, on déduit que si n est solution, alors 2 est également solution. Or pour $n = 2$, les entiers a_1 et a_2 doivent satisfaire $(a_1 + a_2)^2 = 2^{2k-1}$ ce qui est absurde. Les entiers pairs ne vérifient donc pas la question.

2) On remarque que si m vérifie la propriété, alors $2m$ aussi : il suffit de remplacer $(a_1, \ldots, a_n)$ par $(2a_1, \ldots, 2a_n)$, qui est également $n-$onéreux car n est impair. Il suffit donc de traiter le cas où m est impair. On procède pour cela par récurrence forte.

Initialisation : Si $m = 1$, le $n-$uplet $(1, 1, \ldots, 1)$ est $n-$onéreux pour tout n.

Hérédité : On suppose la propriété vraie pour tout entier impair $m \leqslant 2^k$ avec $k \geqslant 0$ fixé. Soit $2^k < m \leqslant 2^{k+1}$ et $r = 2^{k+1} - m \leqslant 2^k$. D'après l'hypothèse de récurrence, il existe un entier n et un $n-$uplet $(r, a_2, \ldots, a_n)$ qui est $n-$onéreux. Mais alors le $n+2-$uplet $(r, 2^{k+1} - r, a_2, \ldots, a_n, r)$ est également onéreux et contient $m = 2^{k+1} - r$. Ceci achève la récurrence et conclut l'exercice.

Exercice 5.16. (IMO 2020 P5) On écrit un entier sur chaque carte d'un paquet de $n > 1$ cartes. On suppose que, pour chaque paire de cartes, la moyenne arithmétique des entiers inscrits est égale à la moyenne géométrique des entiers d'un certain nombre de cartes.

Pour quels entiers n les entiers inscrits sur les cartes sont-ils nécessairement égaux ?

Solution 5.16. L'énoncé est faussement énigmatique, et le traitement de petites valeurs nous laisse penser que tous les entiers n vérifient cette propriété.

Notons $a_1 < \ldots < a_n$ les entiers qui composent le paquet de cartes. Commençons par remarquer que si un entier a divise tous les entiers, alors le paquet dont les cartes sont $a_1/a, \ldots, a_n/a$ vérifie également la propriété. On peut donc supposer sans perte de généralité que les a_i sont premiers entre eux dans leur ensemble, et l'on cherche à montrer qu'ils valent tous 1.

Considérons p un facteur premier de a_1 et considérons l'indice i tel que $p \mid a_k$ pour tout $k \geqslant i$. Supposons par l'absurde que $i \geqslant 2$. Notons $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ les r nombres tels que

$$\frac{a_n + a_{i-1}}{2} = \sqrt[r]{a_{i_1} \ldots a_{i_r}}.$$

Notons que si p divise l'un des termes du membre de droite, alors le nombre $a_{i_1} \ldots a_{i_r}$ est divisible par p donc par p^r pour être rationnel, donc le nombre $2\sqrt[r]{a_{i_1} \ldots a_{i_r}}$ est un entier divisible par p. Ceci implique que $p \mid a_{i-1}$, ce qui est absurde.

Donc p ne divise aucun des termes du membre de droite. Mais alors par définition de i, et puisque $a_{i-1} \neq a_i$ car p divise a_i mais p ne divise pas a_{i-1}, on a

$$\sqrt[r]{a_{i_1} \ldots a_{i_r}} \leqslant \sqrt[r]{a_{i-1} \ldots a_{i-1}} = a_{i-1} < \frac{a_n + a_i}{2},$$

ce qui est absurde.

On en conclut qu'aucun p ne peut diviser a_n, donc $a_n = 1$ et tous les entiers valent 1.

Exercice 5.17. (Chine TST 2019 Day 2 P4) Existe-t-il un ensemble fini A d'entiers strictement positifs et un ensemble infini B d'entiers strictement positifs vérifiant la condition suivante : les entiers distincts de l'ensemble $S = \{a + b, a \in A, b \in B\}$ sont deux à deux premiers entre eux et, pour tous entiers m et n premiers entre eux, il existe un entier $x \in S$ tels que $x \equiv m \mod n$?

Solution 5.17. **Réponse :** Il n'existe pas de tels ensembles.

On écrit $A = \{a_1, \ldots, a_k\}$. On commence par montrer que pour tous m, n premiers entre eux, il existe une infinité de x de S tels que $x \equiv m \mod n$.

Supposons au contraire qu'il existe deux entiers m et n contredisant cette affirmation. Notons x le plus grand entier de S tel que $x \equiv m \mod n$. Prenons $p, q > x$ des nombres premiers tels que q ne divise pas $m + pn$. Les entiers $m + pn$ et qn sont premiers entre eux donc il existe $x \in S$ tel que $x \equiv m + pn \mod qn$, donc $x \equiv m \mod n$ et $x \geqslant m + pn > x$, ce qui amène la contradiction.

➢ Commentaire :

> Il faut désormais tirer parti du caractère fini de A et du caractère infini de B, par exemple en forçant que la congruence $a_k + b \equiv m \mod n$ soit vraie pour une infinité d'entiers $b \in B$.
>
> Si $m \equiv a_k - a_1 \mod n$, cela implique que $n \mid b + a_1$, ce qui n'a lieu que pour une nombre fini de b puisque les éléments de S sont premiers entre eux deux à deux.

Notons $p_0, \ldots, p_{k-1}$ des nombres premiers de divisant aucun des a_i, posons $n = p_1 \ldots p_k$ et prenons m vérifiant $m \equiv a_i - a_{i-1} \mod p_{i-1}$ pour tout $i \geqslant 1$ (avec la convention $a_0 = a_k$). Les entiers m et n sont premiers entre eux car les p_i ne divisent pas les $a_{i+1} - a_i$. Il existe donc une infinité d'entiers x tels que $x \equiv m \mod n$. Tout entier x s'écrit sous la forme $x = a_i + b$ avec $b \in B$. Comme A est fini, d'après le principe des tiroirs, il existe un indice $i \geqslant 1$ tel qu'il existe une infinité d'entiers b tels que $a_i + b \equiv m \mod n$.

Mais alors on a $a_i + b \equiv m \equiv a_i - a_{i-1} \mod p_{i-1}$ pour tout tels entiers b, donc $p_{i-1} \mid a_{i-1} + b$ pour tous ces entiers b, et comme les $a_{i-1} + b$ sont deux à deux distincts, cela contredit que les éléments de S sont premiers entre eux deux à deux. Il n'y a donc pas de tels ensembles.

Exercice 5.18. (IMO SL N3 2015) Soient m et n des entiers strictement positifs tels que $m > n$. On pose $x_k = \dfrac{m+k}{n+k}$ pour $k = 1, \ldots, n+1$. Montrer que si les nombres $x_1, \ldots, x_{n+1}$ sont tous entiers, alors $x_1 \ldots x_{n+1} - 1$ admet un diviseur premier impair.

Solution 5.18. On pose $y_k = \frac{m-n}{n+k} = x_k + 1$ qui est également un entier. On doit montrer que $(y_1+1)\ldots(y_{n+1}+1) - 1$ n'est pas une puissance de 2. Pour cela, on pose $P = \text{ppcm}(n+1, \ldots, 2n+1)$. Par hypothèse, P divise $m - n$, donc on peut écrire $m - n = Pr$.

L'objectif est maintenant de trouver une puissance de 2 qui est la plus grande à diviser le nombre $x_1 \ldots x_n - 1$ mais qui est trop petite pour lui être égale.

Pour cela, on remarque que l'intervalle $[n+1, 2n+1]$ contient une unique puissance de 2 exactement, notée $2^j = n + k$. Alors $y_k = \dfrac{P}{2^j} r$ (car $2^j = v_2(P)$). On pose $x = v_2(r)$, de sorte que $v_2(y_k) = x$. Toutefois, $v_2(y_\ell) > x$ pour tout autre ℓ. On a donc $y_\ell + 1 = 1 \mod 2^{x+1}$. Ainsi

$$(y_1 + 1)\ldots(y_{n+1} + 1) - 1 \equiv (2^x + 1) - 1 \mod 2^{x+1}$$

Donc on a nécessairement $(y_1 + 1)\ldots(y_{n+1} + 1) - 1 = 2^x$. Or $y_k > 2^x$, d'où la contradiction.

Exercice 5.19. On note $\mathbb{N}^\star$ l'ensemble des entiers strictement positifs. Déterminer toutes les fonctions f de $\mathbb{N}^\star$ dans $\mathbb{Z}$ telles que, pour tout entier $n \in \mathbb{N}^\star$, et pour tout diviseur strictement positif d de n, il existe un diviseur strictement positif e de n tel que n divise $d + f(e)$.

Solution 5.19. **Réponse :** L'unique fonction solution est la fonction définie par $f(n) = -n$ pour tout $n \in \mathbb{N}^\star$.

On vérifie que cette fonction est bien solution : si $n \in \mathbb{N}^\star$ et d est un diviseur positif de n, alors n divise $0 = d + f(d)$. On démontre désormais que cette fonction est la seule. On se donne dans la suite f une éventuelle fonction solution. On suppose les diviseurs considérés toujours strictement positifs, et on note $\textsc{Div}(n)$ l'ensemble des diviseurs strictement positifs de n.

Étape 1 : Soit n un entier fixé. Pour tout diviseur $e \in \textsc{Div}(n)$, il existe un unique diviseur d tel que $n \mid d + f(e)$.

Tout d'abord, considérons un diviseur e de n et supposons qu'il existe deux diviseurs distincts d et d' tels que $n \mid d + f(e)$ et $n \mid d' + f(e)$. Alors n divise la différence $d - d'$. Mais puisque les diviseurs sont distincts et compris entre 1 et $n - 1$, on a $0 < |d - d'| < n$, ce qui implique que $d = d'$.

Ainsi, pour tout diviseur e, il existe au plus un diviseur d tel que $d \equiv -f(e)$. Pour tout d, on considère le diviseur $g(d)$ tel que $n \mid d + f(g(d))$. Le paragraphe ci-dessus démontre que g est une fonction injective de $\textsc{Div}(n)$ dans lui-même. La fonction g est donc une bijection de $\textsc{Div}(n)$ dans lui-même, d'où l'unicité annoncée.

Étape 2 : La fonction f est injective.

On suppose le contraire et considère e et e' deux entiers distincts tels que $f(e) = f(e')$. On pose $n = ee'$. On dispose, d'après l'étape 1, de deux diviseurs distincts d et d' de n tels que $n \mid d + f(e)$ et $n \mid d' + f(e')$. Alors n divise également la différence $d - d'$, ce qui nous permet de déduire, comme dans l'étape 1, une contradiction puisque $0 < |d - d'| < n$. La fonction f est donc bien injective.

Étape 3 : On montre que $f(n) = -n$ pour tout n.

On commence par le lemme suivant :

Lemme : Pour tout entier n, soit $f(n) = 0$, soit $f(n) = -d$ avec d un diviseur de n.

Preuve : On suppose qu'un entier n ne vérifie pas le lemme. On choisit $p > n + |f(n)|$ un nombre premier et on applique l'énoncé à np. Il existe un entier d tel que $np \mid d + f(n)$. Si p ne divise pas d, alors d est un diviseur de n, mais alors $0 \leqslant |d + f(n)| < n + |f(n)| < p$, donc $f(n) = -d$. Si p divise d, alors p divise $f(n)$, or $0 \leqslant |f(n)| < p$, ce qui implique que $f(n) = 0$. D'où la dichotomie annoncée. □

On suppose que $f(n) = 0$ pour un certain entier n. D'après le lemme, $-f(d) \in \textsc{Div}(d)$ pour tout diviseur propre de n. Par injectivité de $-f$, $-f$ induit une permutation de $\textsc{Div}(d)$ sur lui-même.

Soit désormais p un nombre premier ne divisant pas n. Il existe deux diviseurs e et e' distincts de np tels que $np \mid n + f(e)$ et $np \mid np + f(e')$. On a alors $n \mid f(e)$ et $f(e')$. Si $e \neq n$, alors $-f(e) \mid e$, donc $n \mid e$, si bien que $e \in \{n, np\}$ (et il en est de même pour e'). On déduit que $\{e, e'\} = \{n, np\}$. Comme $np \mid f(n)$, il vient que $np \mid np + f(n)$, si bien que $np \mid n + f(np)$. Comme $-f(np)$ est un diviseur strictement positif de np, on a l'encadrement $-np < n + f(pn) < n < np$, de sorte que $f(np) = -n$. Comme c'est vrai pour tout nombre premier p ne divisant pas n, cela contredit l'injectivité de f. On déduit que $f(n) \neq 0$.

On a montré que $-f(n)$ est un diviseur de n pour tout entier n, une récurrence forte permet alors de conclure que $-f(n) = n$ pour tout entier n.

Remarque 1 : L'étape 1 peut être obtenue plus rapidement de la façon suivante : comme pour tout diviseur d il existe un diviseur e tel que $d \equiv -f(e) \mod n$, la fonction $-f$, vue modulo n, induit une surjection de l'ensemble des diviseurs dans lui-même. C'est donc une bijection de l'ensemble des diviseurs de n modulo n.

Remarque 2 : Il existe de nombreuses variantes de la solution précédente. En voici une : une fois le lemme acquis, on pouvait également procéder comme suit. Supposons à présent que $f(n) \neq -n$ pour au moins un entier n, et prenons le plus petit entier n avec cette propriété. Comme tous ses diviseurs propres vérifient $f(d) = -d$ et que f est injective, on a $f(n) = 0$.

Soit désormais p un nombre premier ne divisant pas n. On considère d le diviseur de np tel que $pn \mid n + f(d)$. Comme $pn \mid np + f(n)$, $d \neq n$ (d'après l'étape 1). De même, d n'est pas un diviseur propre de n, car $np \mid d + f(d) = 0$ d'après le lemme. On déduit que $p \mid d$.

Or, $f(d)$ est un diviseur négatif de pn d'après le lemme. On déduit que $n - np \leqslant n + f(d) \leqslant n$. Comme le seul multiple de np dans cet intervalle est 0, $f(d) = -n$. Ainsi, p admet un multiple dont l'image par f vaut $-n$. Ceci étant vrai pour tout nombre premier p suffisamment grand, on contredit l'injectivité de f, et cela conclut.

Exercice 5.20. (IMO SL N5 2014) Déterminer tous les triplets d'entiers (p, x, y) tels que p est premier et $x^{p-1} + y$ et $y^{p-1} + x$ sont des puissances de p.

Solution 5.20. **Réponse :** Il s'agit de $(3, 2, 5), (3, 5, 2)$ et $(2, n, 2^k - n)$ pour tous entiers k, n positifs.

Si $p = 2$, alors il s'agit de tous les (x, y) dont la somme est une puissance de 2. On suppose dans la suite que p est impaire. Quitte à échanger les rôles de x et y, on suppose $x \leqslant y$, ce qui implique que $x^{p-1} + y \leqslant y^{p-1} + x$. On pose $p^a = x^{p-1} + y$ et $p^b = y^{p-1} + x$. On a alors

$$0 \equiv y^{p-1} + x \equiv (x^{p-1} - p^a)^{p-1} + x \equiv x^{(p-1)^2} + x \mod p^a.$$

Notons que x et $x^{(p-1)^2-1} + 1$ sont premiers entre eux. Si $p^a \mid x$, alors $x^{p-1} + y > x \geqslant p^a$ ce qui est absurde. Donc $p^a \mid x^{(p-1)^2-1} + 1$. D'après le petit théorème de Fermat, on a par ailleurs

$$0 \equiv x^{(p-1)^2-1} + 1 \equiv x^{-1} + 1 = \frac{x+1}{x} \mod p,$$

ce qui implique que $\boxed{p \mid x + 1}$. D'après le lemme LTE, on a alors

$$a \leqslant v_p(x^{(p-1)^2-1} + 1) = v_p(x + 1) + v_p((p - 1)^2 - 1) = v_p(x + 1) + 1.$$

D'autre part, $p^{v_p(x+1)} \leqslant x + 1 \leqslant x^{p-1} + 1 = p^a$, avec égalité seulement si $x = x^{p-1}$ et $1 = y$, c'est-à-dire si $x = y = 1$ et $p = 2$. Pourtant, on a supposé p impair. On a donc $v_p(x + 1) < a \leqslant v_p(x + 1) + 1$ et donc $\boxed{a = v_p(x + 1) + 1}$.

On raffine l'inégalité du paragraphe précédent :

$$p^a = x^{p-1} + y \geqslant x^2 + x = xp^{a-1},$$

soit $x \leqslant p$. Comme $p \mid x + 1$, il vient que $p = x + 1$, $v_p(x + 1) = 1$ et $a = 2$.
On déduit que $p^2 > x^{p-1} = (p - 1)^{p-1}$. Une récurrence montre que cette inégalité est fausse dès que $p \geqslant 5$, d'où $\boxed{p = 3}$, ce qui conduit à $x = 2$ et $y = 5$. Réciproquement, ce triplet est bien solution car $2^2 + 5 = 3^2$ et $5^2 + 2 = 3^3$.

Exercice 5.21. (IMO SL 2022 N3) Soit $a \geqslant 2$ et $d \geqslant 2$ deux entiers premiers entre eux. On pose $x_1 = 1$; puis, pour tout entier $k \geqslant 1$, on pose $x_{k+1} = x_k/a$ si a divise x_k, et $x_{k+1} = x_k + d$ sinon.
Trouver, en fonction de a et de d, l'entier ℓ maximal pour lequel a^ℓ divise l'un des termes $x_1, x_2, x_3, \ldots$

Solution 5.21. **Réponse :** ℓ est l'unique entier m pour lequel $d < a^m < ad$.

Étape 1 : Montrons que la suite (x_k) est bornée par ad, ce qui implique que $\ell \leqslant m$, car a^m est l'entier de $[\![1, ad]\!]$ qui est divisible par la plus grande puissance de a.

Pour cela, on procède par récurrence forte : on suppose en effet que $x_1, \ldots, x_k$ sont tous inférieurs strictement à da. Notons j le plus grand indice inférieur à k tel que x_j est divisible par a (avec $j = 0$ si aucun terme n'a été divisible par a). Notons qu'alors $x_{j+1} = x_j/a < d$ d'après l'hypothèse de récurrence (et $x_{j+1} = 1 < d$ si $j = 0$). Par définition, on a ensuite $x_{j+r} = x_{j+1} + (r-1)d$ pour tout $1 \leqslant r \leqslant k+1$.

Prenons r l'élément de $[\![1, a-1]\!]$ tel que $r - 1 \equiv -x_{j+1}d^{-1} \mod a$, alors $x_{j+1} + (r-1)d \equiv 0 \mod a$. Comme $x_{j+1}, \ldots, x_{j+(k-j)}$ ne sont pas divisibles par a, c'est que $k - j \leqslant r \leqslant a - 1$ et $x_k \leqslant x_{j+1} + (k-j-1)d < d + (a-2)d = (a-1)d$. On a donc $x_{k+1} < ad$, ce qui achève la récurrence.

Étape 2 : On montre qu'il existe un terme de la suite valant a^m.

Notons que si $x_{k+1} = x_k + d$, alors $x_{k+1} \equiv x_k \mod d$, tandis que si $x_{k+1} = x_k/a$, alors $x_{k+1} \equiv x_k a^{-1} \mod d$. On déduit que la suite (x_k) modulo d a la forme suivante :

$$1, \ldots, 1, a^{-1}, \ldots, a^{-1}, a^{-2}, \ldots, a^{-2}, a^{-3}, \ldots.$$

Soit ω l'ordre de a modulo d. Par $\omega-$périodicité de la suite $(a^k)_{k\in\mathbb{Z}}$, on dispose d'un entier k tel que $-k \equiv m \mod \omega$. On dispose alors d'un indice k_0, pris minimal pour cette propriété, tel que $x_{k_0} \equiv a^{-k} \equiv a^m \mod d$. Par minimalité de k_0, l'entier x_{k_0-1} est divisible par a. D'après l'étape 1, cela conduit à $x_{k_0} = x_{k_0-1}/a < da/a = d$. Ainsi, x_{k_0} est de la forme $a^m - rd$ avec $a - 1 \geqslant r \geqslant 1$ un entier. Un récurrence donne que $x_{k_0+s} = x_{k_0} + sd$ et finalement, $x_{k_0+r} = a^m$ comme voulu.

Exercice 5.22. (Iran TST 2019 P2, Envoi 2021 P17) Soit n un entier strictement positif et soient $a, a_1, \ldots, a_n$ des entiers strictement positifs. On suppose que pour tout entier k pour lequel l'entier $ak+1$ est un carré parfait, au moins l'un des entiers $a_1k+1, \ldots, a_nk+1$ est également un carré parfait.
Montrer qu'il existe un indice $1 \leqslant i \leqslant n$ tel que $a = a_i$.

Solution 5.22. Cette solution a été proposée par plusieurs élèves de la POFM lorsque l'exercice avait été donné en envoi.

Commeçons par chercher des entiers k génériques pour lesquels $ak+1$ est un carré parfait, afin de faire fonctionner l'énoncé.

Pour tout entier t, en prenant $k = at^2 + 2t$, le nombre $ak+1 = (at+1)^2$ est un carré donc il existe un a_i tel que $a_ik + 1 = t(a_iat + 2a_i) + 1$ est un carré, noté x_t^2. En particulier, si $t = p$ est un nombre premier, on trouve que

$$p \mid p(a_iap + 2a_i) = (x_p - 1)(x_p + 1),$$

donc $p \mid x_p - 1$ ou $p \mid x_p + 1$. En appliquant cela pour une infinité de nombres premiers p, on trouve un indice i tel que $p(a_ia + 2p) + 1$ soit un carré pour une infinité de p et tel que $p \mid x_p - 1$ pour une infinité de p ou tel que $p \mid x_p + 1$ pour une infinité de p.

- ➢ Si $p \mid x_p + 1$ pour une infinité de valeurs de p. Posons $x_p = pk_p - 1$, avec k_p un entier. Comme $x_p - 1$ est premier avec p et qu'il divise $p(a_iap + 2a_i)$, on déduit que $x_p - 1 \mid a_iap + 2a_i$. On déduit que $pk_p - 2 \mid a_iap + 2a_i$, soit $pk_p - 2 \leqslant a_iap + 2a_i$. Lorsque p est suffisamment grand, cela implique que $k_p \leqslant a_ia$. Mais alors

  $$pk_p - 2 \mid k_p(a_iap + 2a_i) - a_ia(pk_p - 2) = 2a_i(a + k_p).$$

  Ce nombre est non nul, inférieur à $2a_i(a + aa_i)$ et admet des diviseurs arbitrairement grands. Cela est impossible, le cas traité ne peut donc pas se produire.

- ➢ Si $p \mid x_p - 1$ pour une infinité de valeurs de p. Posons $x_p = pk_p + 1$. Pour p différent de 2, p ne divise pas $x_p + 1$, et $x_p + 1 \mid p(a_iap + 2a_i)$. On déduit que $pk_p + 2 \mid a_iap + 2a_i$. Là encore, on déduit que $k_p \leqslant a_ia$ lorsque p est assez grand. On a alors

  $$pk_p + 2 \mid k_p(a_iap + 2a_i) - a_ia(pk_p + 2) = 2a_i(k_p - a).$$

  Or, pour k_p suffisamment grand, on a $|2a_i(k_p - a)| \leqslant 2a_i(a_ia + a)$. Pour p assez grand, le seul multiple de $pk_p + 2$ vérifiant cette borne est 0, donc $k_p = a$. On remonte nos équations, cela signifie que $(ap+1)^2 = a_iap^2 + 2a_ip + 1$ pour une infinité de valeurs de p, ce qui conduit à l'égalité des coefficients dominants a^2 et a_ia, soit $\boxed{a = a_i}$ comme voulu.

Solution alternative

Commençons par deux lemmes sur les résidus quadratiques.

Lemme 1 : Si x est résidu quadratique modulo p avec p premier impair, il l'est aussi modulo p^2 (et même p^m, mais on n'en a pas besoin ici).

Démonstration : En effet, soit a tel que $a^2 \equiv x \pmod p$, ce qu'on réécrit sous la forme $a^2 - x = kp$. Mais alors on obtient $(a - 2^{-1}kp)^2 \equiv a^2 - kp \equiv x \pmod{p^2}$, et 2 est inversible modulo p^2 car p est impair. Ainsi, x est bien un résidu quadratique modulo p^2. □

Lemme 2 : Sii t est un entier non nul et p est un nombre premier tel que $p \equiv 1 \pmod{8t}$, alors $\left(\frac{t}{p}\right) = 1$.

Démonstration : En effet, soit q un diviseur premier de t et $\alpha = v_q(t)$. Si $q = 2$, $\left(\frac{2}{p}\right) = 1$ car $p \equiv 1 \pmod 8$. donc q est résidu quadratique modulo p. Notons maintenant que α est pair, alors q^α est automatiquement un carré modulo p, et si α est impair, q^α est le produit de q (qui est un carré) avec $q^{\alpha-1}$ qui est un carré, donc q^α est un carré modulo p. Si $q \geq 3$, comme $p \equiv 1 \pmod 4$, la loi de réciprocité quadratique nous donne $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$,. De même que précédemment, on déduit que $\left(\frac{q^\alpha}{p}\right) = 1$. La multiplicativité des symboles de Legendre permet de conclure que $\left(\frac{t}{p}\right) = 1$. □

On rappelle également un cas particulier du théorème de la progression arithmétique de Dirichlet : pour tout t entier, il existe une infinité de nombres premiers p tels que $p \equiv 1 \mod 8t$.

Revenons à l'exercice. Supposons par l'absurde que tous les a_i sont différents de a.
Posons $M = \max\{a, a_1, \ldots, a_n\} \geq 2$. On construit alors une suite de nombres premiers $p_1, \ldots p_n$ par récurrence comme suit : par le théorème de la progression arithmétique de Dirichlet, il existe au moins un nombre premier $p_1 \equiv 1 \pmod{8a_1(a_1 - a)}$ avec $p_1 > M$. (On utilise ici le fait que $a_1 - a \neq 0$).
Pour $2 \leq i \leq n$, on prend ensuite p_i tel que $p_i \equiv 1 \pmod{8a_i(a_i - a)}$ avec $p_i > p_{i-1}$ (qui existe pour les mêmes raisons que p_1).
En particulier les p_i sont deux-à-deux distincts, et $p_i \equiv 1 \mod 8a_i$ et $p_i \equiv 1 \mod 8(a_i - a)$, de sorte que d'après le deuxième lemme, pour tout i, $\left(\frac{a_i}{p_i}\right) = \left(\frac{a_i - a}{p_i}\right) = 1$.
Par définition, pour tout i il existe n_i tel que $n_i^2 \equiv a_i - a \pmod{p_i}$, et quitte à remplacer n_i par $n_i + p_i$, on peut supposer $p_i^2 \nmid n_i^2 - (a_i - a)$ ($p_i \neq 2$). Ainsi, on peut écrire $n_i^2 \equiv ac_ip_i + (a_i - a) \pmod{p_i^2}$ avec $p_i \nmid c_i$ puisque a et p_i sont premiers entre eux ($a < p_i$).
Ensuite, comme a_i est inversible modulo p_i pour tout i, le théorème des restes chinois indique que l'on peut trouver un entier k vérifiant que pour tout i, $k \equiv (c_ip_i - 1)a_i^{-1} \mod p_i^2$, ou encore $a_ik + 1 \equiv c_ip_i \pmod{p_i^2}$.
Remarquons que, par construction,

$$ak + 1 \equiv a\frac{c_ip_i - 1}{a_i} + 1 \equiv \frac{ac_ip_i - a + a_i}{a_i} \equiv \frac{n_i^2}{a_i} \equiv a_i\left(\frac{n_i}{a_i}\right)^2 \pmod{p_i^2}$$

Or $\left(\frac{a_i}{p_i}\right) = 1$, donc a_i est également un résidu quadratique modulo p_i^2 par le premier lemme, donc on a un entier, mettons N_i, tel que $ak + 1 \equiv N_i^2 \pmod{p_i^2}$.
Alors le théorème des restes chinois nous donne un entier x tel que $x \equiv N_i \pmod{p_i^2}$ pour tout i et $x \equiv 1 \pmod{a}$ (car a est premier avec les p_i). Mais alors $x^2 \equiv N_i^2 \equiv ak + 1 \pmod{p_i^2}$ pour tout i, et $x^2 \equiv 1^2 \equiv ak + 1 \pmod{a}$, donc $x^2 \equiv ak + 1 \pmod{aP^2}$, où on a posé $P = \prod_{i=1}^{n} p_i$.
On réécrit maintenant la congruence sous la forme $x^2 = ak + 1 + maP^2 = a(P^2m + k) + 1$. On utilise enfin l'hypothèse de l'énoncé : il existe un indice j tel que $a_j(P^2m + k) + 1$ soit un carré parfait. Mais alors $a_j(P^2m + k) + 1 \equiv a_jk + 1 \equiv c_jp_j \pmod{p_j^2}$, et comme $p_j \nmid c_j$, $v_{p_j}(a_j(P^2m + k) + 1) = 1$, ce qui est en contradiction avec le fait que c'est un carré parfait. Notre affirmation de départ était donc fausse, et l'un des $a_i - a$ est non nul.

Exercice 5.23. (EGMO 2026 P6) Soit p un nombre premier et n un entier strictement positif non divisible par p. On note k le nombre de diviseurs positifs de n et $1 = d_1 < d_2 < \ldots < d_k = n$ ses diviseurs. Pour tout indice $i = 1, 2, \ldots, k$, on note c_i le nombre de diviseurs strictement positifs ℓ de d_i^2 tels que $d_i - \ell$ est divisible par p. Montrer que

$$(p-1)(c_1 + c_2 + \ldots + c_k) \geqslant k^2.$$

Solution 5.23. La somme $c_1 + c_2 + \ldots + c_k$ dénombre le nombre de paires (d, ℓ) telles que $d \mid n$, $\ell^2 \mid d$ et $d \equiv \ell \mod p$.

Soient d et ℓ des entiers tels que $\ell \mid d^2$ et $d \mid n$. Soit $\delta = \mathrm{PGCD}(\ell, d)$ et a et b des entiers tels que $\ell = \delta a$ et $d = \delta b$. Comme a et b sont premiers entre eux et que $\ell \mid d^2 = \delta^2$, on a $\delta a \mid \delta^2 b^2$ puis $a \mid \delta$. On peut donc écrire $\delta = ma$, de sorte que $d = mab$.

L'une des clés essentielles du problème est de remarquer que ma et mb sont des diviseurs de n, puisqu'ils divisent tous les deux d. De plus, on a $p \mid d - \ell = \delta a - \delta b$ donc $p \mid a - b$ donc $\boxed{p \mid ma - mb}$, où on a utilisé que p est premier avec tous les diviseurs de n. Autrement dit, pour toute paire (d, ℓ), on peut associer une paire $(d_1, d_2) = (ma, mb)$ de diviseurs de n tels que $d_1 \equiv d_2 \mod p$. On vérifie que cette association est injective : si (d_1, d_2) est associée à (d, ℓ) et (d', ℓ'), alors

$$d = \frac{d_1 d_2}{\mathrm{PGCD}(d_1 d_2)} = d'$$

puis $\ell = d_1 d / d_2 = d_1 d' / d_2 = \ell'$.

Autrement dit, le nombre de paires (d, ℓ) solutions est au moins le nombre de paires (d, d') de diviseurs de n telles que $d \equiv d' \mod p$. On va alors dénombre ces paires.

On répartit les diviseurs de n en fonction de leur reste modulo p : notons $N_i = |\{d \text{ diviseur de } n, d \equiv i \mod p\}|$ le nombre de diviseurs de n congrus à i modulo p. Le nombre de paires recherchées est alors $N_1^2 + \ldots + N_{p-1}^2$. De plus, $N_1 + \ldots + N_{p-1} = k$. D'après l'inégalité de Cauchy-Schwarz, on a donc

$$c_1 + \ldots + c_k \geqslant N_1^2 + \ldots + N_k^2 \geqslant \frac{(N_1 + \ldots + N_k)^2}{p-1} = \frac{k^2}{p-1}.$$

Exercice 5.24. (Chine TSTST 2012 P3) Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que :

1. si $\text{PGCD}(m,n)=1$, alors $\text{PGCD}(f(m),f(n))=1$,
2. pour tout entier $n\in\mathbb{N}^\star$, $n\leqslant f(n)\leqslant n+2012$.

Montrer que, pour tout entier $n\geqslant 1$, tout facteur premier de n divise $f(n)$.

Solution 5.24.

➢ **Commentaire :**

> Si l'énoncé est vrai, f a probablement une infinité de points fixes : il s'agirait des n dont tous les facteurs premiers ne divisent aucun des autres entiers de l'intervalle $[\![n,n+2012]\!]$.
>
> Réciproquement, si f admet un point fixe N tel que $p\mid N$, alors pour tout multiple $f(n)$ de p, on a $p\mid\text{PGCD}(f(n),f(N))$ donc $\text{PGCD}(f(n),f(N))\neq 1$ et donc $\text{PGCD}(n,N)\neq 1$.
>
> Autrement dit, pour tout n, et tout diviseur p de $f(n)$, si on trouve un point fixe N premier avec n et tel que $p\mid N$, on aura une contradiction.
>
> Pour créer un point fixe de f, il faut créer un entier N tel que $f(N)$ est premier avec $N+1,\dots,N+2012$, ce qui force que $f(N)=N$ par encadrement. Pour cela, il suffit de trouver un entier M premier avec N tel que $\text{PGCD}(f(M),N+i)\neq 1$ pour tout $i\leqslant 2012$. Comme on ne maitrise pas la valeur de $f(M)$, on peut carrément chercher M tel que $\text{PGCD}(M+j,N+i)\neq 1$ pour tout $0\leqslant j\leqslant 2012$. La construction est une adaptation de construction déjà croisées dans les exercices 2.100 et 4.90.

Soit n un entier et p un diviseur premier de $f(n)$. On suppose par l'absurde que p ne divise pas n.

On construit un entier N tel que $f(N)=N$, N est premier avec n et $p\mid N$. Pour cela, on construit deux entiers M et N tels que

1. $N\equiv 1 \mod n$,
2. $N\equiv 0 \mod p$,
3. $M\equiv 1 \mod N$,
4. Pour tout $1\leqslant i\leqslant 2012$ et pour tout $0\leqslant j\leqslant 2012$, $\text{PGCD}(N+i,M+j)\neq 1$.

Supposons en effet avoir construit de tels entiers M et N. Soit $j\in[\![0,2012]\!]$ l'indice tel que $f(M)=M+j$. Comme $\text{PGCD}(M,N)=1$, on a $\text{PGCD}(M+j,f(N))=1$. Or pour tout $i\neq 0$, $\text{PGCD}(M+j,N+i)\neq 1$, on déduit que $\boxed{f(N)=N}$.

On a pourtant $\text{PGCD}(n,N)=1$ et $p\mid\text{PGCD}(f(n),f(N))$, ce qui contredit la condition de l'énoncé, et conclut notre raisonnement par l'absurde.

Il reste à faire la construction des entiers N et M. Soit $\{p_{i,j},1\leqslant i\leqslant 2012,0\leqslant j\leqslant 2012\}$ une famille de 2012×2013 nombres premiers distincts de p et qui ne divisent pas n. D'après le théorème des restes chinois, il existe un entier N tel que

$$N\equiv 0 \mod p,\quad N\equiv 1 \mod n,\quad N\equiv -i \mod p_{i,j},\quad \text{pour tous } 1\leqslant i\leqslant 2012 \text{ et } 0\leqslant j\leqslant 2012.$$

Comme N est premier avec les $p_{k,\ell}$, toujours avec le théorème des restes chinoi, il existe un entier M tel que

$$M\equiv 1 \mod N,\quad M\equiv -j \mod p_{i,j},\qquad \text{pour tous } 1\leqslant i\leqslant 2012 \text{ et } 0\leqslant j\leqslant 2012.$$

Pour tout $1\leqslant i\leqslant 2012$ et $0\leqslant j\leqslant 2012$, on a $p_{i,j}\mid\text{PGCD}(N+i,M+j)$ donc $\text{PGCD}(N+i,M+j)\neq 1$ comme voulu.

Exercice 5.25. (Entraînement groupe E Valbonne 2025, India IMO training camp 2025) Soit $k \geqslant 1$, $a_1, \ldots, a_k$ des entiers strictement positifs et P leur produit. On suppose que l'équation

$$n = \sum_{i=1}^{k} \left\lceil \frac{n}{a_i} \right\rceil.$$

admet strictement plus de $P/2$ solutions strictement positives. Montrer qu'elle admet au moins P solutions positives.

Solution 5.25. On suppose que les a_i remplissent les conditions de l'énoncé. Soit n une éventuelle solution. Les inégalités usuelles sur les parties supérieures indiquent

$$n = \sum_{i=1}^{k} \left\lceil \frac{n}{a_i} \right\rceil \geqslant \sum_{i=1}^{k} \frac{n}{a_i}.$$

On obtient que $1 \geqslant \sum_{i=1}^{k} \frac{1}{a_i}$. Si $1 = \sum_{i=1}^{k} \frac{1}{a_i}$, alors $n = \ell P$ est une solution de l'équation pour tout entier ℓ, puisque chaque terme de la somme est alors entier et on a égalité dans l'inégalité précédente. Ceci implique que l'équation admet une infinité de solutions.

On suppose dans la suite que $1 > \sum_{i=1}^{k} \frac{1}{a_i}$ et on pose $\delta = 1 - \sum_{i=1}^{k} \frac{1}{a_i}$. On note que δ peut s'écrire sous la forme $\delta = \frac{a}{P}$.

Étape 1 : Les a_i sont premiers entre eux deux à deux.

On pose pour tout entier n,

$$f(n) = n - \sum_{i=1}^{k} \left\lceil \frac{n}{a_i} \right\rceil.$$

Si l'on pose $M = \text{ppcm}(a_1, \ldots, a_k)$, alors pour tout entier n, on vérifie que

$$f(n+M) = n + M - \sum_{i=1}^{k} \left\lceil \frac{n+M}{a_i} \right\rceil = n + M - \sum_{i=1}^{k} \left\lceil \frac{n}{a_i} \right\rceil - \sum_{i=1}^{k} \frac{M}{a_i} = f(n) + M\delta.$$

Ainsi, pour tout résidu r modulo M, la suite $(f(r+\ell M))_\ell$ est une suite strictement croissante à valeur entière, elle prend donc la valeur 0 au plus une fois. En particulier, l'équation de l'énoncé admet au plus une solution dans la classe de congruence de chaque résidu modulo M et donc au plus M solutions. On a donc l'inégalité $M > P/2$. Or, M est un diviseur de P, donc on a exactement $M = P$, ce qui implique que les a_i sont premiers entre eux deux à deux.

Étape 2 : On a $a \leqslant 2$.

Puisque les a_i sont premiers entre eux, a est premier avec P. En effet, soit p un nombre premier qui divise P. Soit i_0 l'unique indice tel que p divise a_{i_0}. On a donc que $\prod_{j \neq i} a_j$ est divisible par p si et seulement si $i \neq i_0$. Or,

$$\sum_{i=1}^{k} \frac{1}{a_i} = \frac{\sum_{i=1}^{k} \prod_{j \neq i} a_j}{P} = \frac{P - a}{P},$$

donc p ne divise pas $P - a$, donc ne divise pas a.

Pour tout indice i, on note r_i l'entier tel que $\left\lceil \frac{n}{a_i} \right\rceil = \frac{n}{a_i} + \frac{r_i}{a_i}$. Notons que r_i est l'unique entier vérifiant $0 \leqslant r \leqslant a_i - 1$ et $r_i \equiv -n \mod a_i$. L'équation devient

$$n = \sum_{i=1}^{k} \frac{n}{a_i} + \sum_{i=1}^{k} \frac{r_i}{a_i},$$

ou encore, après réarrangement,

$$n = \frac{r_1 \frac{P}{a_1} + \ldots + r_k \frac{P}{a_k}}{a}.$$

Si n est une solution, la fraction de droite doit être entière. Réciproquement, pour tout choix de $(r_1, \ldots, r_n)$ tels que le membre de droite est entier, l'entier obtenu n vérifie $n \equiv -r_i \mod a_i$ et est solution de l'équation, de sorte que deux $n-$uplets $(r_1, \ldots, r_k)$ distincts fournissent deux entiers n distincts. Ainsi, le nombre de solutions à l'équations correspond au nombre de $k-$uplets $(r_1, \ldots, r_k)$ vérifiant les encadrements annoncés et tels que la fraction de droite est un entier, puisqu'il y a au plus une solution dans chaque classe modulo P.

Fixons $r_1, \ldots, r_{k-1}$ des entiers vérifiant les encadrements $0 \leqslant r_i \leqslant a_i - 1$ pour tout i. Pour que la fraction de droite soit un entier, il faut et il suffit que

$$r_k \frac{P}{a_k} \equiv -r_1 \frac{P}{a_1} - \ldots - r_{k-1} \frac{P}{a_{k-1}} \mod a.$$

Notons que a est premier avec P donc avec P/a_k, de sorte que P/a_k est inversible modulo a. Ainsi, le nombre de r_k vérifiant la congruence et compris entre 0 et $a_k - 1$ est majoré par $\left\lceil \frac{a_k}{a} \right\rceil$. Comme il y a au plus $a_1 \ldots a_{k-1}$ façons de choisir $(r_1, \ldots, r_{k-1})$, on obtient la majoration

$$\frac{P}{2} < a_1 \ldots a_{k-1} \left\lceil \frac{a_k}{a} \right\rceil = P \frac{1}{a_k} \left\lceil \frac{a_k}{a} \right\rceil.$$

On déduit que $\frac{a_k}{2} < \left\lceil \frac{a_k}{a} \right\rceil < \frac{a_k}{a} + 1$. Notons que si $a \geqslant 3$, cette inégalité implique que $a_k < 6$ et on vérifie à la main que l'inégalité $\frac{a_k}{2} < \left\lceil \frac{a_k}{3} \right\rceil$ n'a pas de solutions pour $a_k = 1, \ldots, 5$. On a donc montré que $a = 1$ ou $a = 2$.

Étape 3 : Conclusion

Si $a = 2$: Comme a est premier avec P, a est premier avec les a_i, donc les a_i sont impairs. Le numérateur de la fraction dans l'expression de n est alors de la même parité que $r_1 + \ldots + r_k$. Parmi les $k-$uplets $(r_1, \ldots, r_k)$ vérifiant les encadrements nécessaires, on note A l'ensemble de ceux dont la somme est pair et B l'ensemble de ceux dont la somme est impaire. On désire montrer que $A < \frac{P}{2}$. On peut pour cela (entre autres méthodes telles qu'une récurrence sur k), considérer l'égalité entre séries génératrices suivante :

$$\sum_{(r_1,\ldots,r_k)\in A} X^{r_1+\ldots+r_k} + \sum_{(r_1,\ldots,r_k)\in B} X^{r_1+\ldots+r_k} = \prod_{i=1}^{k} \left(\sum_{r_i=0}^{a_i-1} X^{r_i} \right) = \prod_{i=1}^{k} \frac{X^{a_i} - 1}{X - 1}.$$

En évaluant cette égalité en $X = -1$, le côté gauche vaut $|A| - |B|$ tandis que le côté droit vaut 1 (les a_i sont impairs donc chaque terme du produit vaut 1). On déduit que $|A| = \frac{P+1}{2}$. Or, $n = 0$ n'est pas parmi les $P/2$ solutions de l'équation données par l'énoncé, donc les $(r_1, \ldots, r_k)$ donnant des solutions sont parmi $A \setminus \{(0, \ldots, 0)\}$. Ainsi, il y a $(P-1)/2$ solutions dans ce cas, ce qui contredit l'énoncé.

Si $a = 1$: Alors le numérateur de la fraction dans l'expression de n est toujours un multiple de a, donc n est solution pour chaque $(r_1, \ldots, r_k)$, ce qui implique qu'il y a exactement $a_1 \ldots a_k = P$ solutions dans ce cas.