PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

ENVOI 3 : ARITHMÉTIQUE
À RENVOYER AU PLUS TARD LE 13 FÉVRIER 2023

Les consignes suivantes sont à lire attentivement :

- Le groupe junior est constitué des élèves nés en 2008 ou après. Les autres élèves sont dans le groupe senior.
- Les exercices classés “Juniors” ne sont à chercher que par les élèves du groupe junior.
- Les exercices classés “Seniors” ne sont à chercher que par les élèves du groupe senior.
- Les exercices doivent être cherchés de manière individuelle.
- Utiliser des feuilles différentes pour des exercices différents.
- Respecter la numérotation des exercices.
- Bien préciser votre nom en lettres capitales, et votre prénom en minuscules sur chaque copie.

1 Exercices junior

Exercice 1. Soient a, b deux entiers. Montrer que $ab(a-b)$ est divisible par 2.

Solution de l'exercice 1 On s'intéresse à la parité d'un produit, il est donc pertinent de faire une disjonction de cas sur la parité des entiers en jeu, ici a et b. On remarque alors la chose suivante :

- Si a ou b est pair : alors ab est pair (le produit d'un nombre pair par un entier quelconque étant pair) et donc $ab(a-b)$ est bien divisible par 2.
- Sinon, si a et b sont tous les deux impairs, alors $a-b$ est pair (en tant que différence de deux impairs) et donc $ab(a-b)$ est divisible par 2

Finalement, dans tous les cas, si a et b sont des entiers, alors $ab(a-b)$ est divisible par 2.

Exercice 2. Montrer qu'il existe une infinité de couples (m, n) d'entiers strictement positifs distincts tels que $m!n!$ soit un carré parfait.

Solution de l'exercice 2 On aurait envie de prendre $m = n$ pour avoir $m!n! = (n!)^2$ et avoir un carré parfait. Mais l'énoncé force $m \neq n$. Malgré cela, on voit déjà un moyen de faire apparaître naturellement des carrés parfaits.

Supposons sans perte de généralité $m > n$ (comme $m!n! = n!m!$, quitte à remplacer (m, n) par (n, m), ça ne pose pas de problème). Alors $m!n! = m\times(m-1)\times\ldots\times(n+1)\times n!\times n! = m\times\ldots\times(n+1)\times(n!)^2$. Alors $m!n!$ sera un carré parfait si et seulement si $m \times \ldots \times (n + 1)$ l'est. Le moyen le plus simple de le faire, c'est de choisir $m = n + 1 = k^2$ pour un certain entier k ($k \geqslant 2$ car on veut $m, n \geqslant 1$). En effet on a bien $(k^2)!(k^2 - 1)! = k^2((k^2 - 1)!)^2 = [k(k^2 - 1)!]^2$.

Finalement, pour tout $k \geqslant 2$ entier, $(m, n) = (k^2, k^2 - 1)$ convient, ce qui nous fournit bien une infinité de couples de solutions.

Exercice 3. Trouver les triplets d'entiers (x, y, n) tels que $n^2 = 17x^4 - 32x^2y^2 + 41y^4$.

Solution de l'exercice 3 On va montrer par descente infinie que $(0, 0, 0)$ est la seule solution.

Comme un carré ne vaut que 0 ou 1 modulo 3 (une façon de le voir est de faire une disjonction de cas sur les valeurs modulo 3), il est pertinent de tenter une étude modulo 3 pour essayer de voir où ça nous mène. Pour ce faire, on remarque que si (x, y, n) est solution, alors modulo 3, on a

$$n^2 \equiv -x^4 - 2x^2y^2 - y^4 \equiv -(x^2 + y^2)^2 \pmod 3$$

Ainsi, $n^2 + (x^2 + y^2)^2$ est divisible par 3. Or un carré vaut 0 ou 1 modulo 3 donc la seule manière qu'une somme de carrés soit divisible par 3, c'est que chacun des termes le soit. Donc n et $x^2 + y^2$ sont divisibles par 3. De même il découle que x et y sont divisibles par 3.

En réinjectant dans l'équation, on en déduit que $3^4 = 81$ divise n^2 et donc 9 divise n, donc $\left(\frac{x}{3}, \frac{y}{3}, \frac{n}{9}\right)$ est une autre solution. Or si on avait une solution avec x, y ou n non nul (et quitte à les changer en leurs opposés, ce qui ne change pas les valeurs des carrés, positifs), on pourrait obtenir une suite strictement décroissante d'entiers naturels, ce qui est absurde (c'est le principe de la descente infinie).

On en déduit que la seule solution potentielle est $(0, 0, 0)$. Et réciproquement, on remarque que $(x, y, n) = (0, 0, 0)$ convient (les deux membres donnent 0).

L'unique solution de l'équation est donc $(0, 0, 0)$.

Exercice 4. Déterminer tous les entiers naturels n tels que 21 divise $2^{2^n} + 2^n + 1$.

Solution de l'exercice 4 Comme $21 = 3 \times 7$ et que 3 et 7 sont premiers entre eux, 21 divise $2^{2^n} + 2^n + 1$ si et seulement si 3 et 7 divisent $2^{2^n} + 2^n + 1$.

Éliminons de suite le cas $n = 0$, qui donne $2^{2^0} + 2^0 + 1 = 4$ qui n'est pas divisible par 21. On peut donc supposer $n > 0$, en particulier 2^n est pair. Alors modulo 3 : $2^{2^n} + 2^n + 1 \equiv (-1)^{2^n} + (-1)^n + 1 \equiv (-1)^n + 2 \pmod 3$. En particulier $2^{2^n} + 2^n + 1$ est divisible par 3 si est seulement si n est pair. On suppose donc désormais que cette condition est vérifiée.

Reste à traiter le cas de la divisibilité par 7. Modulo 7, les puissances de 2 sont $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1$: il s'agit donc d'étudier l'exposant modulo 3. Comme n est pair (par le cas précédent), on sait déjà que $2^n \equiv 1 \pmod 3$ donc $2^{2^n} \equiv 2 \pmod 7$. On veut donc $2^n \equiv -1 - 2 \equiv 4 \pmod 3$, et donc $n \equiv 2 \pmod 3$ (et réciproquement si $n \equiv 2 \pmod 3$, comme n est pair alors 7 divise $2^{2^n} + 2^n + 1$).

On doit avoir $n \equiv 0 \pmod 2, n \equiv 2 \pmod 3$: comme 2 et 3 sont premiers entre eux, le théorème des restes chinois donne qu'il existe une unique solution modulo $2 \times 3 = 6$, et on remarque que c'est $n \equiv 2 \pmod 6$.

En conclusion, les entiers naturels n qui conviennent sont exactement ceux qui vérifient $n \equiv 2 \pmod 6$.

Exercice 5. Soit $n \in \mathbb{N}^\star$. Montrer que si $2n+1$ et $3n+1$ sont des carrés parfaits, alors $5n+3$ n'est pas premier.

Solution de l'exercice 5 Supposons que $2n+1$ et $3n+1$ sont des carrés parfaits : on dispose de a, b deux entiers strictement positifs ($2n+1, 3n+1 > 0$) tels que $2n+1 = a^2$ et $3n+1 = b^2$. Ici, il s'agit de remarquer que $5n+3 = 4 \times (2n+1) - (3n+1) = 4a^2 - b^2$. Pour trouver cette identité, on essaie d'exprimer 5 à partir de 2 et 3 : il est naturel de prendre $5 = 2+3$ mais cela ne donne pas $5n+3$, en revanche on voit que $5 = 4 \times 2 - 3$.

On peut donc écrire $5n+3 = (2a-b)(2a+b)$. Comme $a, b > 0$ $2a+b > 2a-b$, et $2a+b > 0$. Ceci force $2a-b > 0$ (sinon on aurait $5n+3 \leqslant 0$, ce qui est exclu). Il suffit donc de montrer que $2a-b > 1$ pour conclure : on aura alors écrit $5n+3$ comme produit de deux entiers strictement plus grands que 1, et il ne pourra pas être premier.

Mais si $2a = b+1$, $5n+3 = 2a+b = 4a-1$ donc $a^2 = 2n+1 \leqslant \frac{5n+3}{2} < \frac{4a-1}{2} < 2a$ donc $a < 2$. Mais $a = 1$ donne $2n+1 = 1$ donc $n = 0$, absurde car $n > 0$. Ainsi $2a - b \neq 1$.

On a donc bien montré que si $2n+1$ et $3n+1$ sont des carrés parfaits (avec $n \in \mathbb{N}^\star$), alors $5n+3$ n'est pas un nombre premier.

Exercice 6. Trouver tous les nombres premiers p, q vérifiant $p^5 + p^3 + 2 = q^2 - q$.

Solution de l'exercice 6 Ce qu'on connaît pour des nombres premiers, c'est leurs propriétés de divisibilité. Une expression développée n'est donc pas très pratique pour étudier cela : on va d'abord chercher à factoriser.

Remarquons que $p^5 + p^3 + 2 = p^3(p^2 + 1) + 2$. On veut résoudre $p^3(p^2 + 1) = q^2 - q - 2$. Mais on reconnaît alors $q^2 - q - 2 = (q - 2)(q + 1)$ (si on ne le voit pas directement, on peut le trouver en résolvant $q^2 - q - 2 = 0$ avec la méthode classique utilisant le discriminant).

On veut donc résoudre $p^3(p^2 + 1) = (q - 2)(q + 1)$. En particulier $p^3 \mid (q - 2)(q + 1)$. Alors $\gcd(q - 2, q + 1) = \gcd(q - 2, q + 1 - (q - 2)) = \gcd(q - 2, 3)$ vaut donc 1 ou 3. Cela suggère d'étudier d'abord le cas $p = 3$: on obtient $(q - 2)(q + 1) = 270$, et en résolvant $q^2 - q - 2 = 270$ on trouve $q = 17$ (qui est bien un nombre premier) et $q = -16$ (qui n'est pas solution car ce n'est pas un nombre premier). Donc lorsque $p = 3$, il y a une unique solution $(p, q) = (3, 17)$.

On peut donc supposer $p \neq 3$. En particulier, il ne divise pas $\gcd(q - 1, q + 2)$, donc au moins un des nombres $q + 1$ et $q - 2$ est premier avec p, donc avec p^3. Or $p^3 \mid (q + 1)(q - 2)$: donc d'après le lemme de Gauss, $q + 1$ ou $q - 2$ est divisible par p^3. Or, p^3 ne peut pas diviser $q - 2$ parce que sinon, on aurait $(q - 2)(q + 1) \geqslant p^3 p^3 > p^3(p^2 + 1)$, absurde. Ainsi $p^3 \mid q + 1$, et donc $q - 2 | p^2 + 1$.

Mais les divisibilités qu'on vient d'obtenir montrent que $p^3 \leqslant q + 1 = (q - 2) + 3 \leqslant p^2 + 1 + 3 = p^2 + 4$, et donc $p^2(p - 1) \leqslant 4$. Or $p^2(p - 1)$ est strictement croissante en p, et en $p = 2$ on a égalité, donc le seul cas possible est $p = 2$ (autrement dit, pour $p > 2$, on a $p^2(p - 1) > 4$).

Lorsque $p = 2$, l'équation devient $q^2 - q - 2 = 40$, en résolvant on trouve $q = 7$ (qui convient car 7 est premier) et $q = -6$ (qui ne convient pas car n'est pas un nombre premier).

Finalement, il y a deux solutions qui sont $(p, q) = (2, 7)$ et $(p, q) = (3, 17)$.

Exercice 7. Soit $n \geqslant 2$. Montrer qu'il existe des entiers a, b tels que, pour tout entier m, le nombre $m^3 + am + b$ ne soit pas un multiple de n.

Solution de l'exercice 7 $m^3 + am + b$ est un multiple de n si et seulement si $m^3 + am \equiv -b \pmod{n}$. On remarque alors qu'il suffit de trouver a tel que $m^3 + am$ ne prend pas toutes les valeurs possibles modulo n (et de prendre pour $-b$ une des valeurs qui n'est pas prise). Comme $m^3 + am$ modulo n ne dépend que de m modulo n, on peut se restreindre à $0 \leqslant m \leqslant n - 1$.

Il s'agit de trouver un a tel que les $0^3 + a \cdot 0 \pmod{n}, 1^3 + a \cdot 1 \pmod{n}, \ldots, (n-1)^3 + a(n-1) \pmod{n}$ n'atteignent pas n valeurs distinctes (modulo n). Alors si on trouve $m_1 \neq m_2$ entre 0 et $n - 1$ tels que $m_1^3 + am_1 \equiv m_2^3 + am_2 \pmod{n}$, les $n - 2$ autres valeurs de m modulo n donneront au plus $n-2$ valeurs de $m^3 + am$ modulo n, donc au total, pour $0 \leqslant m \leqslant n-1$, $m^3 + am$ prendra au plus $n-1$ valeurs sur mes n possibles : il y en aura bien une qui ne sera pas atteinte. Or $0^3 + a \times 0 \equiv 0 \pmod{n}$, $1^3 + a \times 1 \equiv a + 1 \pmod{n}$. Si $a + 1 \equiv 0 \pmod{n}$, on sera dans la situation décrite ci-dessus.

Posons alors $a = -1$ (ou $a = n-1$ si on veut $a > 0$). Alors $m^3 + am$ est nul si $m = 0$ ou $m = 1$. Donc il existe c entier, $0 \leqslant c \leqslant n - 1$, tel que pour tout $0 \leqslant m \leqslant n - 1$, $m^3 + am \not\equiv c \pmod{n}$. Posons alors $b = -c$ (ou $b = n - c$ si on veut $b > 0$), alors pour tout $0 \leqslant m \leqslant n - 1$, $m^3 + am + b$ sera non nul modulo n, donc pour tout m entier, $m^3 + am + b$ ne sera pas un multiple de n.

Ainsi, il existe bien de tels entiers a et b.

Exercice 8. Trouver tous les entiers $a, b, c \in \mathbb{N}$ tels que $1517^a + 15^b = 1532^c$.

Solution de l'exercice 8 On commence par traiter les petites valeurs de c.

Si $c = 0$, $1517^a + 15^b = 1$ n'a pas de solution.
Si $c = 1$, on doit trouver a, b tels que $1517^a + 15^b = 1532$. Si $a \geqslant 2$ ou si $a = 0$ il n'y a pas de solution. Si $a = 1$, alors $15^b = 1532 - 1517 = 15$ donc $b = 1$: ceci fournit la solution $(1, 1, 1)$.

On suppose maintenant $c \geqslant 2$. En particulier $16 = 4^2$ divise 1532^c : ceci invite à étudier l'équation modulo des puissances de 2 plus petites que 16 pour éliminer la dépendance en c. On obtient alors $1 + (-1)^b \equiv 0 \pmod 4$ donc b est impair (en particulier, $b \geqslant 1$).

En réduisant modulo 8 : $15^b \equiv -1 \pmod 8$ (b est impair). On a alors $1517^a - 1 \equiv 5^a - 1 \equiv 0 \pmod 8$, donc a est pair.

En réduisant modulo 5 (comme 5 divise 15, cela supprime la dépendance en b), on a $2^a \equiv 2^c \pmod 5$, donc $a \equiv c \pmod 4$ (l'ordre de 2 modulo 5, est 4). Puisqu'on a montré que a était pair, c est pair. Notons $a = 2e$ et $c = 2d$, alors d et e ont la même parité (car $2e \equiv 2d \pmod 4$ donc $e \equiv d \pmod 2$), et en réinjectant dans l'équation de départ, on obtient $15^b = (1532^d - 1517^e)(1532^d + 1517^e)$.

Remarquons alors que

$$(1532^d + 1517^e) - (1532^d - 1517^e) = 2 \times 1517^e = 2 \times 37^e \times 41^e$$

Or ni 37 ni 41 ne divisent 1532 donc $1532^d - 1517^e$, et $1532^d - 1517^e$ est impair. Par conséquent, $1532^d + 1517^e$ et $1532^d - 1517^e$ sont premiers entre eux, donc l'un d'eux est 5^b et l'autre est 3^b. Puisque $1532^d + 1517^e > 1532^d - 1517^e$, il s'ensuit que $1532^d + 1517^e = 5^b$ et $1532^d - 1517^e = 3^b$.

Alors $3^b + 5^b = 2 \cdot 1532^d$. Si $d \geqslant 2$, le membre de droite est divisible par 16, mais on vérifie modulo 16 que le premier membre n'est jamais divisible par 16 ($3^4 \equiv 5^4 \equiv 1 \pmod{16}$ donc il suffit de tester $3^0 + 5^0 \equiv 2 \pmod{16}, 3^1 + 5^1 \equiv 8 \pmod{16}, 3^2 + 5^2 \equiv 2 \pmod{16}$ et $3^3 + 5^3 \equiv 5 \pmod{16}$), ce qui implique que $d = 1$ (car $2d = c \geqslant 2$) et donc e impair ($d \equiv e \pmod 2$). Comme $1532^d > 1517^e$, il s'ensuit que $e = 1$, mais $1532^d - 1517^d = 15$ n'est pas une puissance de 3, d'où une contradiction.

Finalement la seule solution est $(a, b, c) = (1, 1, 1)$.

Exercice 9. Quentin et Timothé jouent à un jeu. D'abord, Quentin choisit un nombre premier $p > 2$, puis Timothé choisit un entier strictement positif n_0. Quentin choisit alors un entier $n_1 > n_0$ et calcule $s_1 = n_0^{n_1} + n_1^{n_0}$; puis Timothé choisit un entier $n_2 > n_1$ et calcule $s_2 = n_1^{n_2} + n_2^{n_1}$. Les joueurs continuent de jouer chacun à leur tour, en choisissant au tour k un entier $n_k > n_{k-1}$ et en calculant $s_k = n_k^{n_{k-1}} + n_{k-1}^{n_k}$. Le premier joueur à choisir un entier n_k tel que p divise $s_k(s_1 + 2s_2 + 3s_3 + \ldots + ks_k)$ gagne le jeu. Déterminer lequel de Quentin et Timothé possède une stratégie gagnante.

Solution de l'exercice 9 Nous allons montré que Timothé a une stratégie gagnante. Notons que Quentin va choisir les n_{2k+1} et Timothé va choisir les n_{2k}. On fait d'abord quelques remarques.

• Remarque 1 : Remarquons d'abord que si l'un des joueurs choisit $n_k \equiv 0 \pmod p$ et ne gagne pas à cette étape, alors le joueur suivant gagne en choisissant $n_{k+1} \equiv 0 \pmod p$, car alors $s_{k+1} \equiv 0 \pmod p$, et en particulier p divise $s_{k+1}(s_1 + 2s_2 + \ldots + ks_k + (k+1)s_{k+1})$.

• Remarque 2 : Pour $a \not\equiv 0 \pmod p$, $a^{p-1} \equiv 1 \pmod p$ (Fermat). Alors si $a, b \geqslant 1$ sont deux entiers tels que a soit divisible par $p-1$ et congru à 1 modulo p et b n'est pas divisible par p, alors $a^b + b^a \equiv 1^b + 1 \equiv 2 \pmod p$. On va donc chercher une stratégie de ce côté-là.

• Stratégie : On va montrer que la stratégie suivante fonctionne : pour $k \geqslant 0$, Timothé va distinguer deux cas.

- Si $k = 0$ ou n_{2k-1} n'est pas divisible par p, alors Timothé choisit $n_{2k} > n_{2k-1}$ (resp. $n_0 > 0$) de telle sorte que $n_{2k} \equiv 0 \pmod{p-1}$ et $n_{2k} \equiv 1 \pmod p$ ($p, p-1$ sont premiers entre eux donc par le théorème des restes chinois, il existe un unique reste modulo $p(p-1)$ qui convient, en particulier il existe bien de tels nombres aussi grands que l'on veut.)
- Si n_{2k-1} est divisible par p, alors Timothé choisit $n_{2k} > n_{2k-1}$ divisible par p.

Par la première remarque, dans le second cas si Quentin n'avait pas gagné, alors Timothé gagne à cet instant. Dans le premier cas, si n_{2k-1} n'est pas divisible par p, $s_{2k} \equiv 2 \pmod p$ (d'après la deuxième remarque). Donc si Timothé ne gagne pas à un instant donné, alors il a obtenu $s_{2k} \equiv 2 \pmod p$.

• On s'intéresse alors aux valeurs prises par s_{2k+1}. On distingue deux cas.

- D'abord si à chaque étape, Quentin choisit n_{2k+1} non divisible par p. Alors d'après la deuxième remarque, il obtient $s_{2k+1} \equiv 2 \pmod p$. Autrement dit, $s_k \equiv 2 \pmod p$ pour tout k, et donc $1 + 2s_2 + \ldots + ks_k \equiv k(k+1) \pmod p$ et donc le premier k tel que cette quantité est divisible par p est $k = p-1$ (lemme d'Euclide), or $p-1$ est pair ($p > 2$), donc c'est Timothé qui vient de choisir, et c'est donc celui-ci qui gagne.
- Maintenant, si à un moment Quentin choisit n_{2k+1} divisible par p, (on considère que c'est la première fois que Quentin choisit un tel nombre), en particulier $2k+1 < p-1$ sinon on a vu au-dessus que Timothé gagne. Alors pour $m \leqslant 2k$, on a $s_m \equiv 2 \pmod p$, et $s_{2k+1} \equiv 1 \pmod p$. Alors

$$s_1 + 2s_2 + \ldots + (2k+1)s_{2k+1} \equiv 2k(2k+1) + (2k+1) \equiv (2k+1)^2 \not\equiv 0 \pmod p$$

(car $1 \leqslant 2k+1 \leqslant p-1$), donc Quentin ne gagne pas à cette étape. Mais alors, comme évoqué précédemment, en choisissant n_{2k+2} divisible par p, on a $s_{2k+2} \equiv 0 \pmod p$ donc Timothé gagne.

• Dans tous les cas, avec cette stratégie, Timothé va gagner, donc c'est Timothé qui a une stratégie gagnante.

Exercices Seniors

Exercice 10. Montrer qu'il existe une infinité de couples (m, n) d'entiers distincts tels que $m!n!$ soit un carré parfait.

Solution de l'exercice 10 On aurait envie de prendre $m = n$ pour avoir $m!n! = (n!)^2$ et avoir un carré parfait. Mais l'énoncé force $m \neq n$. Malgré cela, on voit déjà un moyen de faire apparaître naturellement des carrés parfaits.

Supposons sans perte de généralité $m > n$ (comme $m!n! = n!m!$, quitte à remplacer (m, n) par (n, m), ça ne pose pas de problème). Alors $m!n! = m\times(m-1)\times\ldots\times(n+1)\times n!\times n! = m\times\ldots\times(n+1)\times(n!)^2$. Alors $m!n!$ sera un carré parfait si et seulement si $m \times \ldots \times (n + 1)$ l'est. Le moyen le plus simple de le faire, c'est de choisir $m = n + 1 = k^2$ pour un certain entier k ($k \geqslant 2$ car on veut $m, n \geqslant 1$). En effet on a bien $(k^2)!(k^2 - 1)! = k^2((k^2 - 1)!)^2 = [k(k^2 - 1)!]^2$.

Finalement, pour tout $k \geqslant 2$ entier, $(m, n) = (k^2, k^2 - 1)$ convient, ce qui nous fournit bien une infinité de couples solutions.

Exercice 11. Déterminer tous les entiers naturels n tels que 21 divise $2^{2^n} + 2^n + 1$.

Solution de l'exercice 11 Comme $21 = 3 \times 7$ et que 3 et 7 sont premiers entre eux, 21 divise $2^{2^n} + 2^n + 1$ si et seulement si 3 et 7 divisent $2^{2^n} + 2^n + 1$.

Éliminons de suite le cas $n = 0$, qui donne $2^{2^0} + 2^0 + 1 = 4$ qui n'est pas divisible par 21. On peut donc supposer $n > 0$, en particulier 2^n est pair. Alors modulo 3 : $2^{2^n} + 2^n + 1 \equiv (-1)^{2^n} + (-1)^n + 1 \equiv (-1)^n + 2 \pmod 3$. En particulier $2^{2^n} + 2^n + 1$ est divisible par 3 si est seulement si n est pair. On suppose donc désormais que cette condition est vérifiée.

Reste à traiter le cas de la divisibilité par 7. Modulo 7, les puissances de 2 sont $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1$: il s'agit donc d'étudier l'exposant modulo 3. Comme n est pair (par le cas précédent), on sait déjà que $2^n \equiv 1 \pmod 3$ donc $2^{2^n} \equiv 2 \pmod 7$. On veut donc $2^n \equiv -1 - 2 \equiv 4 \pmod 3$, et donc $n \equiv 2 \pmod 3$ (et réciproquement si $n \equiv 2 \pmod 3$, comme n est pair alors 7 divise $2^{2^n} + 2^n + 1$).

On doit avoir $n \equiv 0 \pmod 2, n \equiv 2 \pmod 3$: comme 2 et 3 sont premiers entre eux, le théorème des restes chinois donne qu'il existe une unique solution modulo $2 \times 3 = 6$, et on remarque que c'est $n \equiv 2 \pmod 6$.

En conclusion, les entiers naturels n qui conviennent sont exactement ceux qui vérifient $n \equiv 2 \pmod 6$.

Exercice 12. Soient $k, m, n > 0$ des entiers tels que $m^2 + n = k^2 + k$. Montrer que $m \leqslant n$.

Solution de l'exercice 12 Il y a des carrés : on aimerait faire apparaître des expressions factorisées, et plus particulièrement des carrés parfaits. Remarquons alors que $(2k+1)^2 = 4k^2 + 4k + 1 = 4m^2 + 4n + 1$. On a alors $4m^2 + n + 1 > 4m^2 = (2m)^2$. Alors $(2k+1)^2 > (2m)^2$ donc $(2k+1)^2 \geqslant (2m+1)^2$ (il n'y a pas de carré entre deux carrés consécutifs). D'où, en redéveloppant : $4m^2 + 4n + 1 \geqslant 4m^2 + 4m + 1$. On obtient bien $m \leqslant n$, comme voulu.

Exercice 13. Trouver tous les nombres premiers p, q vérifiant $p^5 + p^3 + 2 = q^2 - q$.

Solution de l'exercice 13 En réarrangeant les termes et en factorisant, cela revient à résoudre $p^3(p^2 + 1) = (q-2)(q+1)$. En particulier $p^3 \mid (q-2)(q+1)$. Or $(q+1)-(q-2) = 3$ donc $\gcd(q-2, 3)$ vaut 1 ou 3. Cela suggère d'étudier d'abord le cas $p = 3$: on obtient $(q-2)(q+1) = 270$, et en résolvant $q^2-q-2 = 270$ on trouve $q = 17$ (qui convient) et $q = -16$ (qui ne convient pas). Donc lorsque $p = 3$, il y a une unique solution $(p, q) = (3, 17)$.

On peut donc supposer $p \neq 3$. En particulier, il ne divise pas $\gcd(q-1, q+2)$, donc au moins un des nombres $q+1$ et $q-2$ est premier avec p^3. Or $p^3 \mid (q+1)(q-2)$: donc $q+1$ ou $q-2$ est divisible par p^3 (Gauss). Or, p^3 ne peut pas diviser $q-2$ parce que sinon, on aurait $(q-2)(q+1) \geqslant p^3p^3 > p^3(p^2+1)$, absurde. Ainsi $p^3 \mid q+1$, et donc $q-2|p^2+1$.

Mais $p^3 \leqslant q+1 = (q-2)+3 \leqslant p^2+1+3 = p^2+4$, et donc $p^2(p-1) \leqslant 4$. Or $p^2(p-1)$ est strictement croissante en p, et en $p = 2$ on a égalité, donc le seul cas possible est $p = 2$ (autrement dit, pour $p > 2$, on a $p^2(p-1) > 4$).

Lorsque $p = 2$, l'équation devient $q^2 - q - 2 = 40$, en résolvant on trouve $q = 7$ (qui convient) et $q = -6$ (qui ne convient pas).

Finalement, il y a deux solutions qui sont $(p, q) = (2, 7)$ et $(p, q) = (3, 17)$.

Exercice 14. Anna et Elie jouent à un jeu. On leur donne à tous les deux le même ensemble A composé d'un nombre fini d'entiers strictement positifs et distincts. Anna choisit un entier $a \in A$ secrètement. Si Elie choisit un entier b (pas forcément dans A) et le donne à Anna, Anna lui donne le nombre de diviseurs strictement positifs de ab. Montrer que Elie peut choisir b de sorte à retrouver à coup sur l'entier choisi par Anna.

Solution de l'exercice 14 Notons P l'ensemble fini des nombres premiers divisant au moins un élément de A et $n \geqslant 1$ le plus grand entier tel qu'il existe $a \in A$ et $p \in P$ tels que $p^n | a$. On peut remplacer A par l'ensemble des entiers m dont les facteurs premiers sont tous dans P et tels que pour tout $p \in P$, $v_p(m) \leqslant n$. Elie propose un entier b de la forme $\prod_{p \in P} p^{b_p}$. Si Anna a choisi l'entier a, alors elle donne à Elie l'entier $\prod_{p \in P} (b_p + v_p(a) + 1)$. Il suffit donc pour Elie de choisir les b_p de sorte que tous les $\prod_{p \in P} (b_p + a_p)$ soient deux à deux distincts, pour tous les choix possibles de a_p entre 1 et $n+1$ pour chaque $p \in P$.

On propose deux solutions.

Première méthode :

L'idée de cette construction est de forcer les factorisations en produits de facteurs premiers des $\prod_p (b_p + a_p)$ à être différentes pour tous les choix possibles des a_p. On veut faire en sorte que chaque $b_p + i$ pour $1 \leqslant i \leqslant n+1$ possède un diviseur premier « distinctif », qui n'apparaît que dans la décomposition en produit de facteurs premiers de $b_p + i$, jamais dans celle d'un autre $b_q + j$.

Formellement, on choisit, pour chaque $p \in P$ et chaque $1 \leqslant i \leqslant n+1$, des nombres premiers deux à deux distincts $Q_{p,i} > n+1$. On construit les b_p grâce au théorème chinois : pour chaque $q \in P$ distinct de p et pour chaque $1 \leqslant i \leqslant n+1$, $Q_{q,i} | b_p$, et pour chaque $1 \leqslant i \leqslant n+1$, $b_p \equiv -i [Q_{p,i}]$.

Avec cette construction, si $q, p \in P$ et $1 \leqslant i, j \leqslant n+1$, alors $Q_{q,j} | b_p + i$ si et seulement si $i = j$ et $p = q$.
En particulier, étant donnés des $1 \leqslant a_p \leqslant n+1$ pour chaque $p \in P$, si $q \in P$, $\Pi = \prod_{p \in P} (b_p + a_p)$ est divisible par $Q_{q,j}$ si et seulement si $j = a_q$: ainsi Π détermine la famille (a_p).

Deuxième méthode :

La première construction était très arithmétique et utilisait des nombres premiers. Celle qu'on présente maintenant vient plus d'une idée de "taille". L'idée est que si l'on prend de gigantesques b_p, le produit $\prod_p (b_p + a_p)$ ressemblera à l'écriture d'un certain nombre en une certaine base, dont les chiffres donneront les a_i.

Passons à la construction proprement dite. Le problème tel que nous l'avons reformulé n'utilise plus le fait que P soit constitué de nombres premiers : on renumérote ses éléments en $1, \ldots, r$. Montrons que pour $N > (n+1)^r$, $b_i = N^{2^i}$ convient. En effet, dans ce cas, on voit que le développement de $\Pi = \prod_{i=1}^{r} (N^{2^i} + a_i)$ écrit un nombre en base N dont le chiffre devant $N^{2^{r+1}-2-2^i}$ est exactement a_i : ainsi Π détermine la famille des (a_i).

Exercice 15. Pour tout entier $n \geqslant 1$, on pose $u_n = 1! + 2! + \ldots + n!$. Montrer qu'il existe une infinité de nombres premiers divisant au moins l'un des termes de la suite (u_n).

Solution de l'exercice 15 Supposons l'inverse : alors il existe des nombres premiers $p_1 < \ldots < p_r$ tels que pour tout $n \geqslant 1$, $u_n := 1 + 2! + \ldots + n!$ soit le produit des $p_i^{a_i(n)}$, où les $a_i(n)$ sont des entiers positifs.

Si $n \geqslant 1$ est tel que $a_i(n) < v_{p_i}((n+1)!)$, alors

$$a_i(n+1) = v_{p_i}(u_{n+1}) = v_{p_i}(u_n + (n+1)!) = v_{p_i}(u_n) = a_i(n)$$

En particulier, $a_i(n+1) < v_{p_i}((n+2)!)$. En particulier, ou bien $a_i(n) \geqslant v_{p_i}((n+1)!)$ pour tout n, ou bien $a_i(n)$ est constante à partir d'un certain rang.

En particulier, en renommant et regroupant les p_i, on dispose d'entiers $N \geqslant 1, C \geqslant 1$ et de nombres premiers $q_1 < \ldots < q_s$ ne divisant pas C tels que pour tout $n > N$, $u_n = C \prod_{i=1}^{s} q_i^{b_i(n)}$ et $b_i(n) \geqslant v_{q_i}((n+1)!)$.

Soit maintenant $n > N + C + 1$ tel que $n+1$ soit divisible par le produit des q_i. Alors $u_n = u_{n-1} + n!$ et $v_{q_i}(u_n) = b_i(n) \geqslant v_{q_i}((n+1)!) > v_{q_i}(n!)$, donc $v_{q_i}(u_{n-1}) = v_{q_i}(n!)$. D'autre part, si $p|C$, $v_p(u_{n-1}) = v_p(C) \leqslant v_p(n!)$, donc $u_{n-1}|n!$.

Il reste à montrer que pour tout n assez grand, u_n ne divise pas $(n+1)!$.

En effet, si $n \geqslant 2$, $nu_n > n \cdot n! + n \cdot (n-1)! = (n+1) \cdot n! = (n+1)!$. D'autre part, si $n \geqslant 4$,

$$\begin{aligned}
(n-1)u_n &= (n-1)n! + (n-1)(n-1)! + (n-1)(n-2)! + (n-1)\textstyle\sum_{k=1}^{n-3} k! \\
&= n \cdot n! + (n-1)(n-3) \cdot (n-3)! < (n+1) \cdot n! \\
&= (n+1)!
\end{aligned}$$

.

Exercice 16. Soient $n \geqslant 2$ et p un nombre premier impair. Soit U l'ensemble des entiers positifs inférieurs ou égaux à p^n et premiers avec p et soit $N = |U|$. Montrer qu'il existe une permutation $a_1, \dots, a_N$ des éléments de U telle que $\sum_{k=1}^{N} a_k a_{k+1}$ (avec $a_{N+1} = a_1$) soit divisible par p^{n-1} mais pas par p^n.

Solution de l'exercice 16

On commence par traiter le cas $p = 3$, dont la solution est différente. Soit $g \in U$ un générateur modulo p^n, on pose $a_i = g^{i-1} \pmod{p^n}$. Comme $g^2 - 1$ est divisible par 3, la somme considérée S vérifie $(g^2-1)S \equiv \sum_{i=1}^{N} (g^{2i+1} - g^{2i-1}) \equiv g(g^{2N}-1)[p^{n+1}]$. Donc pour que $v_p(S) = n-1$, il faut et suffit que $v_p(g^{2N}-1) = n$ (g est premier avec p). Puisque $g^N \equiv 1[p^n]$ (par Euler-Fermat), il suffit de montrer que $v_p(g^N - 1) = n$. Mais par LTE, $v_p(g^N - 1) = v_p(g^{N/p} - 1) + 1 < n + 1$, donc $v_p(g^N - 1) \leqslant n$, de sorte que $v_p(g^N - 1) = n$, ce qui conclut.

Supposons maintenant $p > 3$: Soient $b_0, \dots, b_{m-1} \in U$ des entiers représentant exactement une fois chaque classe de congruence modulo p^{n-1}, ainsi $m = N/p = p^{n-2}(p-1)$ (et on pose $b_m = b_0$). On considère la permutation

$$\begin{aligned} &b_0, b_0 + p^{n-1}, b_0 + 2p^{n-1}, \dots, b_0 + (p-1)p^{n-1}, \\ &b_1, b_1 + p^{n-1}, \dots, b_1 + (p-1)p^{n-1}, \\ &b_2, \dots, b_{m-1}, \dots, b_{m-1} + (p-1)p^{n-1} \end{aligned}$$

(les additions sont toujours à effectuer modulo p^n).
Alors la somme correspondante S est congrue modulo p^n à

$$S_1 = \sum_{i=0}^{m-1} b_i b_{i+1} + \sum_{i=0}^{m-1} (p-1)p^{n-1} b_i + \sum_{i=0}^{m-1} \sum_{k=0}^{p-2} b_i p^{n-1}(2k+1) + (p-1) \sum_{i=0}^{m-1} b_i^2$$

. Comme la somme des b_i est divisible par p et la somme des b_i^2 par p^{n-1}, $S \equiv S_2[p^n]$, où $S_2 = \sum_{i=0}^{m-1} b_i b_{i+1} - \sum_{i=0}^{m-1} b_i^2$.
Soit alors $g \in U$ une racine primitive modulo p^n : prenons $b_i = g^i \pmod{p^n}$. Alors $(g+1)S_2 \equiv (g+1)\sum_{i=0}^{m-1} (g^{2i+1} - g^{2i}) \equiv (g^{2m} - 1)[p^n]$. D'après LTE, $v_p(g^{2m} - 1) \geqslant 1 + v_p\left(\frac{2m}{p-1}\right) = n - 1$ (puisque $p-1 | m$, $p | g^{p-1} - 1$ par Fermat, et $N = p^{n-1}(p-1)$), mais comme $2m < N$, $v_p(g^{2m} - 1) < n$, donc $v_p(g^{2m} - 1) = n - 1$. De plus, puisque $p > 3$, $g + 1$ est premier à p, et donc $v_p(S_2) = n - 1$, d'où $v_p(S) = n - 1$.

Exercice 17. Soit $(a_n)_{n\geqslant 1}$ une suite d'entiers strictement positifs telle que a_1 et a_2 soient premiers entre eux et, pour tout $n \geqslant 1$, $a_{n+2} = a_n a_{n+1} + 1$. Montrer que pour tout entier $m > 1$, il existe $n > m$ tel que $a_m^m \mid a_n^n$. Le résultat est-il encore vrai lorsque $m = 1$?

Solution de l'exercice 17 D'abord, $a_n > 0$ pour tout $n > 0$.
On commence par une observation : soit $n > m$ très grand (disons, $n > (m+1)(a_m+1)$). Alors $a_m^m | a_n^n$ si et seulement si pour chaque nombre premier $p | a_m$, $p | a_n$. Cette idée justifie le lemme qui va suivre :

Lemme : soit $(u_n)_{n\geqslant 0}$ la suite modulo un nombre premier p telle que $u_0 = 0$, $u_1 = 1$ et pour tout $n \geqslant 0$, $u_{n+2} = u_n u_{n+1} + 1$. Alors u est périodique.

Preuve : soit $v_n = (u_n, u_{n+1})$; alors u est périodique dès que v est périodique. Comme v_{n+1} dépend uniquement de v_n, v est périodique dès qu'il existe $N \geqslant 1$ tel que $v_N = v_0$. Si $N \geqslant 1$ est tel que $u_N = 0$, alors la relation de récurrence montre que $u_{N+1} = 1 = u_1$ et donc $v_N = v_0$. Par conséquent, pour montrer que u est périodique, il suffit de montrer qu'il existe $N \geqslant 1$ tel que $u_N = 0$.

Supposons donc que le seul entier n tel que $u_n = 0$ soit $n = 0$. Alors comme v est à valeurs dans un ensemble fini, il existe un entier $n \geqslant 0$ minimal tel qu'il existe un entier $m > n$ tel que $v_n = v_m$. En particulier, $u_m = u_n$ et $m \neq 0$, donc $u_m \neq 0$, et donc $u_n \neq 0$ et donc $n > 0$. Alors $m+1 > n+1 \geqslant 2$ et $u_{n+1} = u_{m+1}$, donc $u_{n-1}u_n + 1 = u_{m-1}u_m + 1$, donc $u_n(u_{n-1} - u_{m-1}) = 0$, d'où, comme $u_n \neq 0$, $u_{n-1} = u_{m-1}$, de sorte que $v_{m-1} = v_{n-1}$, ce qui contredit la minimalité de n. □

Revenons à notre preuve. Lorsque $m > 1$, pour chaque facteur premier p de a_m, $a_{m+1} = a_{m-1}a_m + 1 \equiv 1[p]$, $(a_{m+n} \pmod p)_{n\geqslant 0}$ satisfait les hypothèses du lemme, donc il existe $N_p \geqslant 1$ tel que que pour tout $n \geqslant 0$, $a_{m+n} \equiv a_{m+n+N_p}[p]$.
Soit N le produit des N_p (où p parcourt les facteurs premiers de a_m) : alors, si $n \geqslant 0$, tout diviseur premier p de a_m divise a_{m+nN}. En particulier, si $n \geqslant m a_m$, $a_m^m | a_{m+nN}^{m+nN}$ (parce que si $p | a_m$, $v_p(a_{m+nN}^{m+nN}) \geqslant m + nN \geqslant m a_m \geqslant v_p(a_m^m)$).
Le résultat est faux pour $m = 1$: prenons $a_1 = 155$, a_2 congru à 4 modulo 5 et congru à 29 modulo 31. On vérifie alors que a_n est divisible par 5 si et seulement si $n = 1$ et $n \equiv 4[7]$, alors que a_n est divisible par 31 si et seulement si $n = 1$ ou $n \equiv 5[7]$, donc si $n > 1$, a_n n'est jamais divisible par 5 et 31, et donc 155 ne divise pas a_n^n.

Exercice 18. 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 $N \geqslant 1$ tel que pour tout $n \geqslant N$, $f(n) \neq 1$ 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 de l'exercice 18 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 $b \geqslant 1$ 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 $f(1) = 1$.

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, $f(1+ta) \neq 1 = f(1)$) : soit $b = 1 + ta$. 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 $l \geqslant 1$ 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 $n > l$ assez grand, $v_p(a^{n-1-l}) + C \geqslant v_p(f(a)^n)$, donc $(n-1-l)v_p(a) + C \geqslant n v_p(f(a))$, d'où $v_p(f(a)) \leqslant v_p(a)$.
Par conséquent, pour tout $a \geqslant 1$, $f(a) | a$.
En particulier, si a est premier, $f(a)$ vaut 1 ou a, et est égal à a sauf pour un nombre fini de nombres premiers.

Soit a un nombre premier tel que $f(a) = a$: pour tout $b \geqslant 1$ et tout n assez grand, $a^n | f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$. En particulier, $f(a+b) \equiv f(b)[a]$: ainsi, la classe de congruence de $f(b)$ modulo a ne dépend que de b modulo a.

On va montrer que f est l'identité. Soit $u \geqslant 2$, soit P l'ensemble fini des nombres premiers p tels que $p \leqslant u$ 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 $0 \leqslant u - f(u) \leqslant u < q$, on en déduit que $f(u) = u$.
On propose trois 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 (il y a des prérequis, mais ils sont élémentaires et relativement classiques) :

On reprend les notations et le raisonnement de ce qui précède : on cherche à construire un entier $n > \Pi^N + u$ congru à 1 modulo Π^N tel que $f(n) = n$.

Il est connu (du moins, classique et relativement élémentaire) que si Φ_{Π^N} est le Π^N-ième polynôme cyclotomique, il existe une infinité de nombres premiers n divisant une valeur de Φ_{Π^N}, et ceux qui ne sont pas dans P sont congrus à 1 modulo Π^N et vérifient $f(n) = n$. On peut en choisir un qui est strictement supérieur à $\Pi^N + u$.

Troisième méthode (utilise un théorème relativement classique, mais dont aucune démonstration accessible au niveau olympique n'est connue) :

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 $a, b \geqslant 1$ et $n \geqslant 2$, alors par LTE, pour tout nombre premier $p|a$, $\nu_p((a+b)^{a^{n-1}} - b^{a^{n-1}}) \geqslant \nu_p(a) + \nu_p(a^{n-1}) = \nu_p(a^n)$, donc $a^n|(a+b)^{a^{n-1}} - b^{a^{n-1}}$, et donc l'identité est solution.