PRÉPARATION OLYMPIQUE FRANÇAISE DE MATHÉMATIQUES

POFM

TEST DU 19 ET DU 20 FÉVRIER 2020

DURÉE : 4H

Instructions

- **Rédigez les différents problèmes sur des copies distinctes. Sur chaque copie, écrivez en haut à gauche votre nom en majuscules, votre prénom en minuscules. Écrivez votre classe et le numéro du problème traité en haut à droite.**
- Merci de respecter **impérativement** la numérotation des exercices.
- Le **groupe Junior** est constitué des élèves nés en 2005 ou après.
  Ces élèves doivent traiter les exercices 1 à 4.
- Le **groupe Senior** est constitué des élèves nés en 2004 ou avant.
  Ces élèves doivent traiter les exercices 5 à 7.
- Le **groupe EGMO** est constitué des élèves nées en 2004 ou avant et éligibles à l'EGMO.
  Ces élèves doivent traiter les exercices 8 à 10.
- On demande des solutions **complètement rédigées**, où toute affirmation est soigneusement **justifiée**. La notation tiendra compte de la **clarté** et de la **précision** de la copie. Travaillez d'abord au brouillon, et rédigez ensuite au propre votre solution, ou une tentative, rédigée, de solution contenant des résultats significatifs pour le problème. Ne rendez pas vos brouillons : ils ne seraient pas pris en compte.
- Une solution complète rapportera plus de points que plusieurs tentatives inachevées. Il vaut mieux terminer un petit nombre de problèmes que de tous les aborder.
- Règles, équerres et compas sont autorisés. Les rapporteurs sont interdits.
  Les calculatrices sont interdites, ainsi que tous les instruments électroniques.
- Dans le cas d'un exercice de géométrie, faire une (voire plusieurs) figure sur une feuille blanche séparée. Cette figure devra être propre, grande, et la propriété que l'on cherche à démontrer devra être apparente : par exemple, s'il faut démontrer que des points sont alignés (ou cocycliques), il faut tracer la droite (ou le cercle) qui passe par ces points.
- Le respect de la consigne précédente rapportera automatiquement un point. Si elle n'est pas respectée, la copie ne sera pas corrigée.

  Chaque exercice est noté sur 7 points.

Après l'épreuve, merci de renvoyer les copies

- soit par voie postale, à l'adresse suivante :

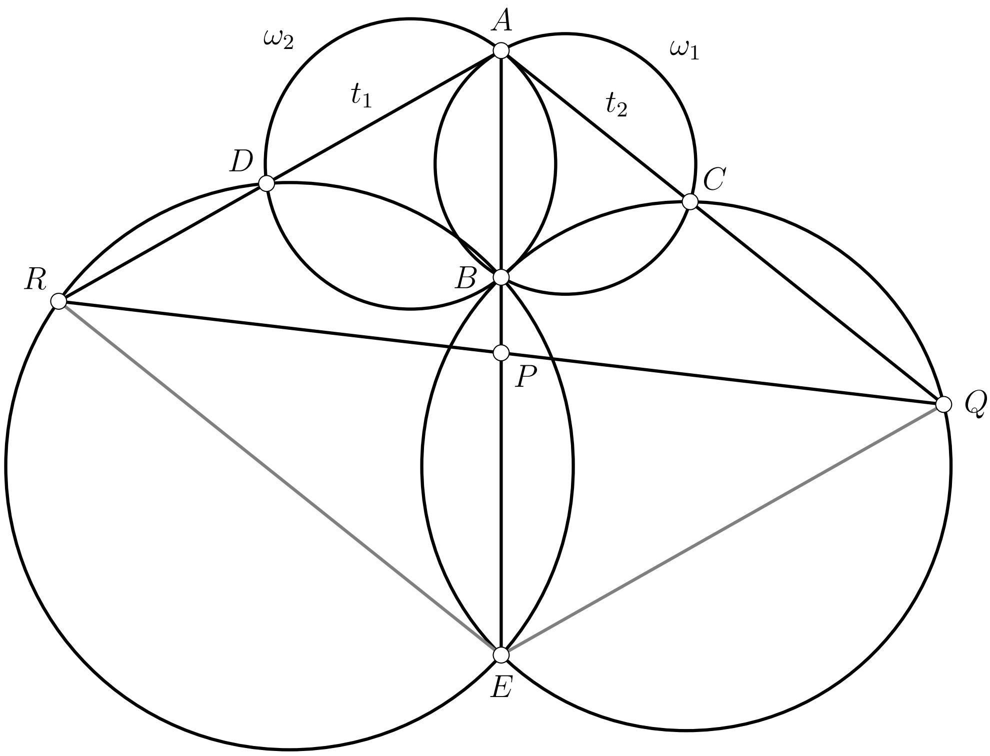
  Animath, Préparation Olympique Française de Mathématiques
  11-13 rue Pierre et Marie Curie
  75005 Paris
- soit par voie électronique, à l'adresse suivante : `copies.ofm@gmail.com`

Exercices Junior

Exercice 1. Soit A, B, E et P quatre points deux à deux distincts, tels que P soit le milieu du segment $[AE]$ et que B appartienne au segment $[AP]$. Soit ω_1 et ω_2 deux cercles passant par A et B. On note t_1 et t_2 les tangentes respectives à ω_1 et à ω_2 passant par A. Soit C le point d'intersection, autre que A, entre t_2 et ω_1, et soit Q le point d'intersection, autre que C, entre t_2 et le cercle circonscrit à BCE. De même, soit D le point d'intersection, autre que A, entre t_1 et ω_2, et soit R le point d'intersection, autre que D, entre t_1 et le cercle circonscrit à BDE.

Démontrer que les points P, Q et R sont alignés.

<u>*Solution de l'exercice 1*</u> Commençons par tracer une figure.



Une première remarque que l'on peut faire est que, a priori, une chasse aux angles naïve ne suffira pas : le point P est le seul point de la figure qui n'appartient à aucun cercle ! Il convient donc d'exploiter à fond le fait que P soit au milieu de $[AE]$.

Dans ces conditions, on remarque qu'il semble aussi être le milieu de $[RQ]$, ce qui signifierait que $AQER$ est un parallélogramme. On s'empresse donc de placer le milieu du segment $[RQ]$, qui semble effectivement coïncider avec P, et de tracer les droites (EQ) et (ER), qui semblent effectivement parallèles à (AR) et à (AQ).

Nous allons donc nous efforcer de démontrer ces deux relations de parallélisme, à l'aide d'une chasse aux angles et du cas limite du théorème de l'angle inscrit :

$$\begin{aligned}(EQ, AR) &= (EQ, AQ) + (AQ, AB) + (AB, AR) = (EQ, CQ) + (AC, AB) + (AB, AD) \\ &= (EB, CB) + (AC, AB) + (AB, t_1) = (AB, CB) + (AC, AB) + (CB, CA) = 0°.\end{aligned}$$

Les droites (EQ) et (AR) sont donc parallèles. De manière symétrique, les droites (ER) et (AQ) sont elles aussi parallèles. Ainsi, $AQER$ est bien un parallélogramme, donc les diagonales $[AE]$ et $[QR]$ se coupent en leur milieu, ce qui conclut.

Commentaire des correcteurs L'exercice nécessitait une figure exacte pour pouvoir conjecturer plusieurs résultats. Ces éventuelles conjectures, même non démontrées, ont été largement valorisées.

Quelques élèves ont remarqué, à raison, que plusieurs configurations étaient possibles (notemment sur l'ordre des points A, D et R sur la droite t_1) mais que toutes ces configurations se traitent de la même façon. Cependant, aucun n'élève n'a utilisé les angles orientés pour traiter toutes les configurations d'un seul coup.

Le fait de ne pas utiliser les angles orientés n'était pas pénalisé et les élèves qui ont traité correctement une seule configuration se sont vus attribuer la note de 7/7.

Exercice 2.

1. Trouver le plus petit entier $k \geqslant 1$ ayant la propriété suivante : pour tous les entiers naturels non nuls x et y tels que x divise y^2 et y divise x^2, le produit xy divise $(x+y)^k$.
2. Trouver le plus petit entier $\ell \geqslant 1$ ayant la propriété suivante : pour tous les entiers naturels non nuls x, y et z tels que x divise y^2, y divise z^2 et z divise x^2, le produit xyz divise $(x+y+z)^\ell$.

Solution de l'exercice 2 Notons tout d'abord que, si un entier k a la propriété désirée, alors tout entier $k' \geqslant k$ aura aussi cette propriété. En effet, si xy divise $(x+y)^k$ et si $k' \geqslant k$, alors xy divise aussi $(x+y)^{k'}$. Par conséquent, il nous suffit de trouver un entier k ayant la propriété désirée, et tel que $k-1$ n'ait pas cette propriété. En outre, cette démarche fonctionnera aussi pour la deuxième question.

1. Étudions les petites valeurs de k. Tout d'abord, pour $k = 1$, on souhaterait que xy divise $x+y$, ce qui est impossible dès lors que x et y sont grands. Par exemple, si $x = y = 3$, alors x divise bien y^2, et y divise x^2, mais $xy = 9$ ne divise pas $x+y$.

   Choisir $x = y$ ne fournit plus un contre-exemple pour $k = 2$, puisque alors xy divise bien sûr $(x+y)^2 = 4xy$. On regarde donc ce qui se passe si l'on choisit $x \neq y$, par exemple si l'on change la valeur de y : dans ce cas, puisque l'on a toujours $x = 3$, on est obligé de choisir $y = 9$. Et là, on constate bien que x divise y^2 et que y divise x^2, mais que $xy = 3^3$ ne divise pas $(x+y)^2 = 2^4 \times 3^2$.

   Enfin, pour $k = 3$, on n'arrive plus à trouver de contre-exemple. On va donc démontrer que $k = 3$ est bien le plus petit entier ayant la propriété désirée. En effet, si l'on pose $a = y^2/x$ et $b = x^2/y$, alors on constate bien que

   $$(x+y)^3 = x^3 + 3xy(x+y) + y^3 = xy(a+b+3x+3y)$$

   est un multiple de xy dès lors que a et b sont entiers.
2. Forts de notre expérience précédente, il semble qu'un cas permettant de trouver autant de contre-exemples que possible soit celui où x et un nombre premier p, puis $z = p^2$ et $y = p^4$. Dans ce cas, on constate bien que x, y et z divisent respectivement y^2, z^2 et x^2. On peut alors écrire $xyz = p^7$ et $(x+y+z)^\ell = p^\ell(1+p+p^3)^\ell$.

   Or, puisque p est premier, on sait que $1+p+p^3$ est premier avec p, donc $(1+p+p^3)^\ell$ est lui aussi premier avec $xyz = p^7$. Par conséquent, si xyz divise $(x+y+z)^\ell$, c'est que p^7 divise p^ℓ, ou encore que $\ell \geqslant 7$.

   Réciproquement, si $\ell \geqslant 7$, l'expression $(x+y+z)^7$ se décompose comme une somme de termes de la forme $x^\alpha y^\beta z^\gamma$, où α, β et γ sont des entiers de somme 7. Il suffit donc de démontrer que xyz divise chacun de ces termes dès lors que les nombres $a = y^2/x$, $b = z^2/y$ et $c = x^2/z$ sont des entiers. Or, on peut noter que xyz divise $x^7 = bc^3xyz$ et que, de même, xyz divise y^7 et z^7. Mais alors $(xyz)^7 = (xyz)^\alpha(xyz)^\beta(xyz)^\gamma$ divise $x^{7\alpha}y^{7\beta}z^{7\gamma} = (x^\alpha y^\beta z^\gamma)^7$, ce qui signifie bien que xyz divise $x^\alpha y^\beta z^\gamma$.

   Le plus petit entier recherché est donc $\ell = 7$.

Solution alternative n°1 Ci-dessus, nous avons cherché à expliquer comment on pouvait être amené à découvrir que les valeurs recherchées seraient $k = 3$ et $\ell = 7$. On aurait bien sûr pu parachuter directement des exemples permettant de démontrer que $k \geqslant 3$ et $\ell \geqslant 7$, par exemple en procédant comme suit :

1. pour $x = 2$ et $y = 4$, on voit bien que x divise y^2 et que y divise x^2, mais que $xy = 2^3$ ne divise $(x+y)^k = 2^k \times 3^k$ que si $k \geqslant 3$;

2. pour $x = 2$, $y = 16$ et $z = 4$, on voit bien que x, y et z divisent respectivement y^2, z^2 et x^2, mais que $xyz = 2^7$ ne divise $(x + y + z)^k = 2^\ell \times 11^\ell$ que si $\ell \geqslant 7$.

<u>*Solution alternative n°2*</u> On peut également utiliser les valuations p-adiques pour démontrer que $k = 3$ et $\ell = 7$ conviennent, par exemple en procédant comme suit.

1. Nous allons démontrer que, pour tout nombre premier p, si x divise y^2 et y divise x^2, alors $v_p(xy) \leqslant 3v_p(x + y)$. En effet, si l'on suppose, sans perte de généralité, que $v_p(x) \leqslant v_p(y)$, alors

$$3v_p(x + y) \geqslant 3v_p(x) = v_p(x) + v_p(x^2) \geqslant v_p(x) + v_p(y) = v_p(xy).$$

2. De même, pour tout nombre premier p, si x, y et z divisent respectivement y^2, z^2 et x^2, alors $v_p(xyz) \leqslant 7v_p(x + y + z)$. En effet, si l'on suppose, sans perte de généralité, que $v_p(x) = \min\{v_p(x), v_p(y), v_p(z)\}$, alors

$$\begin{aligned} 7v_p(x + y + z) &\geqslant 7v_p(x) = v_p(x) + v_p(x^4) + v_p(x^2) \\ &\geqslant v_p(x) + v_p(z^2) + v_p(z) \\ &\geqslant v_p(x) + v_p(y) + v_p(z) = v_p(xyz). \end{aligned}$$

<u>*Solution alternative n°3*</u> Pour démontrer que xyz divise chaque terme de la forme $x^\alpha y^\beta z^\gamma$ tel que $\alpha+\beta+\gamma = 7$ (et en déduire que $\ell \geqslant 7$ convient), on peut également utiliser une approche moins systématique mais plus facile d'accès. En effet, sans perte de généralité, supposons que $\alpha = \min\{\alpha, \beta, \gamma\}$, et posons $a = y^2/x$, $b = z^2/y$ et $c = x^2/z$:

- ▷ Si $\alpha \geqslant 1$, alors $\beta \geqslant 1$ et $\gamma \geqslant 1$ aussi, donc xyz divise bien $x^\alpha y^\beta z^\gamma = xyz \times x^{\alpha-1}y^{\beta-1}z^{\gamma-1}$. On suppose donc désormais que $\alpha = 0$
- ▷ Si $\alpha = \beta = 0$, on montre comme dans la solution originelle que xyz divise $x^\alpha y^\beta z^\gamma = z^7$ et, si $\alpha = \gamma = 0$, on montre de même que xyz divise $x^\alpha y^\beta z^\gamma = y^7$. On suppose donc désormais que $\beta \geqslant 1$ et $\gamma \geqslant 1$.
- ▷ Si $\alpha = 0$, $\beta \geqslant 3$ et $\gamma \geqslant 1$, alors xyz divise $x^\alpha y^\beta z^\gamma = y^3 z \times y^{\beta-3}z^{\gamma-1} = xyz \times ay^{\beta-3}z^{\gamma-1}$.
- ▷ Si $\alpha = 0$ et $1 \leqslant \beta \leqslant 2$, alors $\gamma \geqslant 5$, et xyz divise, comme prévu, le produit

$$x^\alpha y^\beta z^\gamma = yz^5 \times y^{\beta-1}z^{\gamma-5} = xyz \times ab^2y^{\beta-1}z^{\gamma-5}.$$

<u>*Commentaire des correcteurs*</u> Cet exercice a été bien réussi par les élèves ayant testé la propriété de l'énoncé pour des petites valeurs de x, y et z. Cela permettait notamment d'éviter de croire que x divisait y ou réciproquement, erreur qui est arrivée fréquemment.

Beaucoup d'élèves ont montré pour la question a) que $k = 3$ convenait et en on conlu que c'était la réponse à la question posée. Attention, cependant ! Il fallait non seulement démontrer que $k = 3$ convient, mais également que c'est le plus petit entier k qui convient. Cela nécessitait donc de trouver un contre-exemple explicite pour $k = 2$ (et $k = 1$) et de ne pas se contenter de dire que « ça ne marche pas dans ces cas là » sans exhiber de contre-exemple démontrer cette affirmation.

Exercice 3. Une classe compte n élèves. Quelque soit la manière de choisir deux élèves, il y en a au moins un qui a déjà déjeuné chez l'autre. On dispose en outre de l'information suivante : pour chaque élève $\mathbf{E}$, et parmi les élèves chez qui $\mathbf{E}$ a déjeuné, la moitié exactement a déjeuné chez $\mathbf{E}$.

Trouver toutes les valeurs possibles de n.

Solution de l'exercice 3 Soit $\mathbf{E}_1, \ldots, \mathbf{E}_n$ nos élèves. On note a_k le nombre d'élèves chez qui $\mathbf{E}_k$ a déjeuné, et b_k le nombre d'élèves que $\mathbf{E}_k$ a invités à déjeuner. L'énoncé nous indique alors que ces b_k élèves-là sont, d'une part, les $n-1-a_k$ élèves chez qui $\mathbf{E}_k$ n'a pas déjeuné et, d'autre part, $a_k/2$ des élèves chez qui $\mathbf{E}_k$ a déjeuné, de sorte que $b_k = n-1-a_k/2$.

On va maintenant compter le nombre de repas, que l'on note $\mathbf{C}$, de deux manières différentes. D'une part, il s'agit du nombre de fois où un élève a déjeuné chez un ami, de sorte que $\mathbf{C} = a_1 + \ldots + a_n$. D'autre part, il s'agit aussi du nombre de fois où un élève a invité un ami à déjeuner, de sorte que $\mathbf{C} = b_1 + \ldots + b_n$. On en en déduit que

$$\mathbf{C} = \sum_{1 \leqslant k \leqslant n} b_k = \sum_{1 \leqslant k \leqslant n} (n-1-a_k/2) = n(n-1) - \mathbf{C}/2,$$

c'est-à-dire que $3\mathbf{C} = 2n(n-1)$. On sait donc que 3 divise soit n, soit $n-1$, et on étudie ces deux cas séparément :

- ▷ Si 3 divise $n-1$, posons $\ell = (n-1)/3$. Ci-dessous, on identifie les élèves aux entiers $0, 1, \ldots, n-1$ considérés modulo n : l'élève 0 est confondu avec l'élève n, l'élève 1 est confondu avec l'élève $n+1$, etc. Une manière d'obtenir la situation décrite dans l'énoncé est alors que chaque élève k aille déjeuner chez les élèves $k+1, k+2, \ldots, k+2\ell$ (soit 2ℓ élèves), et reçoive donc à déjeuner les élèves $k-2\ell, \ldots, k-1$. En effet, et puisque $-2\ell \equiv \ell + 1 \pmod{n}$, les élèves qui ont invité k à déjeuner et ont déjeuné chez lui sont les élèves $k+\ell+1, \ldots, k+2\ell$ (soit ℓ élèves).
- ▷ Si 3 divise n, posons $\ell = n/3$. Cette fois, on identifie les élèves aux entiers $0, 1, \ldots, n-2$ considérés modulo $n-1$, ainsi qu'à un élément spécial, que l'on notera $\bullet$. On décide alors que l'élève $\bullet$ recevra tout le monde à déjeuner mais n'ira manger chez personne, puis que chaque élève k (avec $k \neq \bullet$) ira déjeuner chez $k+1, \ldots, k+2\ell-1, \bullet$ (soit 2ℓ élèves), et recevra les élèves $k-2\ell+1, \ldots, k-1$ à déjeuner. Cette fois-ci, puisque $-2\ell+1 \equiv \ell \pmod{n-1}$, les élèves qui ont invité k à déjeuner et ont déjeuné chez lui sont les élèves $k+\ell, \ldots, k+2\ell-1$ (soit ℓ élèves).

Par conséquent, les valeurs de n possibles sont tous les entiers n tels que $n \not\equiv 2 \pmod{3}$.

Commentaire des correcteurs L'exercice était difficile, et peu ont réussi à identifier la congruence modulo 3. Certains élèves ont cru obtenir une congruence modulo 6 en utilisant le fait que 6 divise $k(k+1)$, souhaitant en déduire que 6 divisait soit k, soit $k+1$. Cependant, le théorème de Gauss n'est valable que pour des nombres premiers.

Par ailleurs, il y a eu beaucoup d'erreurs de compréhension de l'énoncé.

Enfin, peu nombreux sont les élèves qui, après avoir trouvé la condition nécessaire sur n, ont réussi à fournir une construction valable pour ces valeurs de n ; fournir une telle construction était bien sûr indispensable. Un élève s'est ici distingué par une preuve élégante utilisant des cycles hamiltoniens dans le cas où n est impair et une variante dans le cas pair.

Exercice 4. Soit a, b et c des réels strictement positifs tels que $a+b+c=3$. Démontrer que
$$a^{12}+b^{12}+c^{12}+8(ab+bc+ca) \geqslant 27,$$
et trouver les cas d'égalité.

Solution de l'exercice 4 Soit $\mathbf{S}$ la quantité $a^{12}+b^{12}+c^{12}+8(ab+bc+ca)-27$: on souhaite démontrer que $\mathbf{S} \geqslant 0$. Tout d'abord, puisque $a+b+c=3$, on constate déjà que
$$\begin{aligned}\mathbf{S} &= (a^{12}+b^{12}+c^{12})+4\left((a+b+c)^2-(a^2+b^2+c^2)\right)-27\\ &= (a^{12}+b^{12}+c^{12})-4(a^2+b^2+c^2)+9\\ &= f(a)+f(b)+f(c),\end{aligned}$$
où l'on a posé $f : t \mapsto t^{12}-4t^2+3$.
Or, d'après l'inégalité arithmético-géométrique, on sait, pour tout $t \geqslant 0$, que
$$t^{12}+3 = t^{12}+1+1+1 \geqslant 4t^3,$$
et donc que $f(t) \geqslant 4(t^3-t^2)$.
Enfin, d'après l'inégalité de Tchebychev, puisque les triplets (a,b,c) et (a^2,b^2,c^2) sont ordonnés dans le même ordre, on sait que
$$a^3+b^3+c^3 \geqslant \frac{(a+b+c)(a^2+b^2+c^2)}{3} = a^2+b^2+c^2.$$
On en déduit que
$$\mathbf{S} \geqslant 4(a^3+b^3+c^3)-4(a^2+b^2+c^2) \geqslant 0,$$
ce qui conclut.

Solution alternative n°1 On montre de même que précédemment que
$$\mathbf{S} = (a^{12}+b^{12}+c^{12})-4(a^2+b^2+c^2)+9.$$
Or, d'après l'inégalité de Tchebychev, on sait que (a,b,c) et (a^8,b^8,c^8) sont ordonnés dans le même ordre, on sait que
$$a^{12}+b^{12}+c^{12} \geqslant \frac{(a+b+c)^4(a^8+b^8+c^8)}{3^4} = a^8+b^8+c^8.$$
Cela signifie que $\mathbf{S} \geqslant g(a)+g(b)+g(c)$, où l'on a posé $g : t \mapsto t^8-4t^2+3$.
Or, d'après l'inégalité arithmético-géométrique, on sait, pour tout $t \geqslant 0$, que
$$t^8+3 = t^8+1+1+1 \geqslant 4t^2,$$
et donc que $g(t) \geqslant 0$. On en déduit que $\mathbf{S} \geqslant 0$, ce qui conclut.

Remarque On constate ici que, plus l'entier k est petit, plus il risque d'être difficile de démontrer que la somme
$$\mathbf{S}_k = a^k+b^k+c^k+8(ab+bc+ca)-27 = a^k+b^k+c^k-4(a^2+b^2+c^2)+9$$
est positive ou nulle. Pour $k=3$, c'est d'autant plus difficile que $\mathbf{S}_3 = -9/4 < 0$ lorsque $a=b=3/2$ et $c=0$. En revanche, pour $k=4$, on peut tout de même démontrer que $\mathbf{S}_4 \geqslant 0$, par exemple en procédant comme suit.
Puisque a, b et c jouent des rôles symétriques, on suppose, sans perte de généralité, que $a \leqslant b \leqslant c$. On pose aussi $h : t \mapsto t^4-4t^2+3$, de sorte que $\mathbf{S}_4 = h(a)+h(b)+h(c)$. Puis

- ▷ si $b \geqslant 1$, on pose $x = b-1$ et $y = c-b$: on a donc $a = 1-2x-y$, $b = 1+x$ et $c = 1+x+y$, avec x et y positifs ou nuls ;
- ▷ si $b < 1$, on pose $x = b-1$ et $y = a-b$: on a donc $a = 1+x+y$, $b = 1+x$ et $c = 1-2x-y$, avec x et y négatifs ou nuls.

Dans les deux cas, on a donc

$$\mathbf{S}_4 = h(1+x+y) + h(1+x) + h(1-2x-y),$$

avec x et y de même signe.

On peut alors vérifier que

$$\mathbf{S}_4 = 12x^2(x-1)^2 + 6x^4 + 2(3x+y)^2y^2 + 3(3x+y)y(2x-1)^2 + (3x+y)y,$$

par exemple en développant les membres de gauche et de droite. Puisque le membre de droite est une somme de termes positifs, on en déduit bien que $\mathbf{S}_4 \geqslant 0$, et *a fortiori* que $\mathbf{S}_k \geqslant 0$ pour tout $k \geqslant 4$.

Par ailleurs, le lecteur désireux d'aller plus loin encore, et qui n'aura pas peur des expressions de la forme x^k où x et k sont deux *réels positifs* (pas forcément entiers) pourra en fait se réjouir de la caractérisation suivante, qui fait intervenir la constante

$$\sigma = \ln(9/2)/\ln(3/2) \approx 3.71 :$$

- ▷ si $k < \sigma$, et si $a = b = 3/2$ et $c = 0$, alors $\mathbf{S}_k < 0$;
- ▷ si $k = \sigma$, et si a, b et c sont trois réels positifs tels que $a+b+c = 3$, alors $\mathbf{S}_k \geqslant 0$, avec égalité si et seulement si $a = b = c = 1$ ou bien si (a,b,c) est égal à $(3/2, 3/2, 0)$, à l'ordre près des trois variables ;
- ▷ si $k > \sigma$, et si a, b et c sont trois réels positifs tels que $a+b+c = 3$, alors $\mathbf{S}_k \geqslant 0$, avec égalité si et seulement si $a = b = c = 1$.

Commentaire des correcteurs Même si cet exercice admet une solution relativement courte, il s'agit d'un exercice très difficile, sur lequel peu d'élèves ont obtenu des avancées majeures.

Certains ont voulu utiliser l'inégalité de Tchebychev pour démontrer que $ab+bc+ca \geqslant 3$, ce qui est faux dans le cas où $a = b = 0$ et $c = 3$: pour utiliser l'inégalité de Tchebychev, il faut s'assurer que les termes apparaissant dans le membre que l'on souhaite minorer sont dans le bon ordre !

Exercices Senior

Exercice 5. Soit $a_0, a_1, a_2, \ldots$ une suite d'entiers naturels telle que, pour tout entier $k \geqslant 0$, on ait à la fois $0 \leqslant a_k \leqslant k$ et

$$\binom{k}{a_0} + \binom{k}{a_1} + \ldots + \binom{k}{a_k} = 2^k.$$

Démontrer que tout entier naturel est égal à au moins un des termes $a_0, a_1, a_2, \ldots$

Solution de l'exercice 5 Nous allons en fait démontrer, par récurrence sur n, la propriété $\mathcal{P}_n$ suivante :

Il existe deux entiers k_n et ℓ_n tels que $0 \leqslant k_n \leqslant \ell_n$ et :

- ▷ pour tout entier $m \in \{0, \ldots, k_n - 1\}$, il existe exactement deux indices $i < j < n$ tels que $m = a_i = a_j$;
- ▷ pour tout entier $m \in \{k_n, \ldots, \ell_n - 1\}$, il existe exactement un indice $i < n$ tel que $m = a_i$;
- ▷ pour tout entier $m \geqslant \ell_n$, il n'existe aucun indice $i < n$ tel que $m = a_i$.

Une fois cette propriété acquise, notons que $n = k_n + \ell_n \leqslant 2\ell_n$. Ainsi, pour tout entier m on a bien $\ell_{2m} \geqslant m$: cela nous assure que m est égal à l'un des entiers $a_0, a_1, \ldots, a_{2m-1}$.

Démontrons maintenant la propriété $\mathcal{P}_n$. La propriété $\mathcal{P}_0$ est évidente. On suppose donc désormais que l'on dispose d'un entier $n \geqslant 0$ tel que $\mathcal{P}_n$ soit vraie. Alors

$$\begin{aligned}\binom{n}{a_n} &= 2^n - \sum_{0 \leqslant m < \ell_n} \binom{n}{m} - \sum_{0 \leqslant m < k_n} \binom{n}{m} = 2^n - \sum_{0 \leqslant m < \ell_n} \binom{n}{m} - \sum_{n-k_n < m \leqslant n} \binom{n}{m} \\ &= 2^n - \sum_{0 \leqslant m < \ell_n} \binom{n}{m} - \sum_{\ell_n < m \leqslant n} \binom{n}{m} = \binom{n}{\ell_n}.\end{aligned}$$

Les deux seuls entiers a tels que $0 \leqslant a \leqslant n$ et

$$\binom{n}{a} = \binom{n}{\ell_n}$$

sont $a = \ell_n$ et $a = n - \ell_n = k_n$. Il nous suffit alors de poser $k_{n+1} = k_n$ et $\ell_{n+1} = \ell_n + 1$ (dans le premier cas), ou bien $k_{n+1} = k_n + 1$ et $\ell_{n+1} = \ell_n$ (dans le second cas), pour constater que la propriété $\mathcal{P}_{n+1}$ est vérifiée, ce qui conclut.

Commentaire des correcteurs Cet exercice en apparence plutôt abordable était en fait assez compliqué. En effet, même si la majorité des élèves voyait qu'il fallait utiliser un raisonnement par récurrence et le binôme de Newton, peu sont ceux qui ont trouvé la bonne hypothèse de récurrence à utiliser.

Certains ont voulu montré que, parmi les entiers $a_0, \ldots, a_k$, et pour tout $i \leqslant k$, exactement deux étaient égaux à i ou à $k - i$, ou bien, de manière équivalente, que les $(n+1)$-uplets $(\binom{n}{k})_{0 \leqslant k \leqslant n}$ et $(\binom{n}{a_k})_{0 \leqslant k \leqslant n}$ étaient égaux à permutation près. Cette propriété, bien que vraie, était très difficile à démontrer directement par récurrence.

Sur un tel type d'exercice, il ne faut surtout pas hésiter à faire des petits cas, quitte à passer 30 minutes à regarder les possibilités pour les 10 premiers termes de la suite (a_k) et voir ce qu'il se passe : c'est ainsi que l'on peut se rendre compte que les premiers termes sont pris deux fois par la suite, puis une, puis zéro, et trouver une propriété qui aura des chances de pouvoir se démontrer aisément par récurrence.

Certains ont essayé de regarder les moments d'apparitions des entiers successifs, cela pouvait marcher, mais était souvent techniquement bien plus pénible que la preuve donnée par le corrigé.

Enfin, la notion d'ensemble n'était pas toujours comprise, et a souvent été confondue avec celle de multi-ensemble : dans un ensemble, il n'y a pas de répétition. Ainsi, les ensembles $\{\binom{2}{0}, \binom{2}{1}, \binom{2}{2}\}$ et $\{\binom{2}{0}, \binom{2}{1}\}$ sont égaux l'un à l'autre. Nombreux sont les élèves qui, souhaitant écrire que les $(n+1)$-uplets $(\binom{n}{k})_{0 \leqslant k \leqslant n}$ et $(\binom{n}{a_k})_{0 \leqslant k \leqslant n}$ étaient égaux à permutation près, ont en fait écrit que les ensembles $\{\binom{n}{k}) \colon 0 \leqslant k \leqslant n\}$ et $\{\binom{n}{a_k} \colon 0 \leqslant k \leqslant n\}$ étaient égaux, ce qui ne signifie pas du tout la même chose et pouvait facilement induire le correcteur en erreur.

Exercice 6. Trouver les triplets (a, b, c) d'entiers naturels non nuls tels que $\mathrm{PGCD}(a, b, c) = 1$ et que $a + b + c$ divise chacun des entiers

$$a^{12} + b^{12} + c^{12},\ a^{23} + b^{23} + c^{23} \text{ et } a^{11004} + b^{11004} + c^{11004}.$$

<u>*Solution de l'exercice 6*</u> Considérons un triplet d'entiers (a, b, c) premiers entre eux dans leur ensemble, et posons $\mathbf{S}_k = a^k + b^k + c^k$.

Tout d'abord, si $\mathbf{S}_1$ est pair, alors au moins l'un des entiers a, b et c est pair ; on suppose donc que c est pair. Mais alors, si a est pair, b l'est aussi, et réciproquement. Comme a, b et c ne peuvent pas être pairs tous les trois, c'est donc que a et b sont impairs. Dans ces conditions, on sait que

$$\mathbf{S}_{12} \equiv (a^2)^6 + (b^2)^6 + (c^2)^6 \equiv 1 + 1 + 0 \equiv 2 \pmod 4,$$

et donc que 4 ne divise pas $\mathbf{S}_1$. Ainsi, dans tous les cas, on sait que $v_2(\mathbf{S}_1) \leqslant 1$.

Supposons maintenant que l'on dispose d'un facteur premier p de $\mathbf{S}_1$. De nouveau, si p divise c, il ne peut pas diviser a ni b. Mais alors

$$\mathbf{S}_{12} \equiv a^{12} + (-a)^{12} \equiv 2a^{12} \pmod p,$$

ce qui est impossible. Ainsi, on sait que p ne divise ni a, ni b ni c.

On pose alors $\alpha \equiv a/c \pmod p$ et $\beta \equiv b/c \pmod p$, de sorte que p divise $\alpha^k + \beta^k + 1$ pour $k = 1$, 12, 23 et 11004. Avec ces notations, on constate que

$$\begin{aligned}\alpha^{24} &\equiv (\alpha^{12})^2 \equiv (-1 - \beta^{12})^2 \equiv 1 + 2\beta^{12} + \beta^{24} \\ &\equiv \alpha \times \alpha^{23} \equiv (-1 - \beta)(-1 - \beta^{23}) \equiv 1 + \beta + \beta^{23} + \beta^{24} \pmod p.\end{aligned}$$

et donc que p divise $(1 + \beta + \beta^{23} + \beta^{24}) - (1 + 2\beta^{12} + \beta^{24}) = \beta - 2\beta^{12} + \beta^{23} \equiv \beta(\beta^{11} - 1)^2$. Puisque p et β sont premiers entre eux, c'est donc que $\beta^{11} \equiv 1 \pmod p$.

On en déduit de même que $\alpha^{11} \equiv 1 \pmod p$, donc que $\mathbf{S}_{k+11} \equiv c^{11}\mathbf{S}_k \pmod p$ pour tout $k \geqslant 0$. Et, comme p divise $\mathbf{S}_{11004}$, il divise aussi $\mathbf{S}_4$. Ainsi, $\alpha^4 + \beta^4 + 1 \equiv 0 \pmod p$.

Comme précédemment, on en déduit que

$$\begin{aligned}1 + \beta^{12} &\equiv -\alpha^{12} \equiv (-\alpha^4)^3 \equiv (1 + \beta^4)^3 \equiv (1 + \beta^{12}) + 3\beta^4(1 + \beta^4) \\ &\equiv (1 + \beta^{12}) - 3\alpha^4\beta^4 \pmod p,\end{aligned}$$

et donc que p divise $3\alpha^4\beta^4$. Comme p est premier avec α et β, c'est donc que p divise 3, c'est-à-dire que $p = 3$.

Dans ces conditions, puisque a, b et c sont tous premiers avec 3, leur ordre modulo 9 divise $\varphi(9) = 6$, donc $\mathbf{S}_{12} \equiv (a^6)^2 + (b^6)^2 + (c^6)^2 \equiv 3 \pmod 9$. Cela signifie que 9 ne divise pas $\mathbf{S}_1$, et donc que $v_3(\mathbf{S}_1) \leqslant 1$.

On vient donc de montrer que $\mathbf{S}_1 \in \{1, 2, 3, 6\}$. Puis, quitte à réordonner a, b et c de sorte que $a \leqslant b \leqslant c$, il reste plusieurs cas à vérifier.

- ▷ Si $\mathbf{S}_1 = 3$, alors $(a, b, c) = 1$, et effectivement $\mathbf{S}_1 = \mathbf{S}_k$ pour tout $k \geqslant 1$.
- ▷ Si $\mathbf{S}_1 = 6$, alors $(a, b, c) = (1, 1, 4)$, $(1, 2, 3)$ ou $(2, 2, 2)$. Or, on a montré plus haut qu'aucun des entiers a, b et c n'est divisible par 3 ; de plus, ils sont premiers entre eux dans leur ensemble, donc pas tous pairs. Ainsi, on sait que $(a, b, c) = (1, 1, 4)$, et alors $\mathbf{S}_k \equiv 0 \pmod 2$ et $\mathbf{S}_k \equiv 0 \pmod 3$ pour tout $k \geqslant 1$, donc $\mathbf{S}_1$ divise $\mathbf{S}_k$.

En conclusion, les solutions recherchées sont $(1, 1, 1)$, $(1, 1, 4)$, $(1, 4, 1)$ et $(4, 1, 1)$.

Commentaire des correcteurs L'exercice était très difficile. Une bonne partie des élèves traite la divisibilité de S_1 par 2 et parvient à montrer que, si p est un diviseur impair de S_1, alors p ne divise aucun des entiers a, b et c.

Quelques élèves ont significativement avancé dans le problème, notemment pour montrer que le seul diviseur impair possible de S_1 était 3, grâce à d'astucieuses manipulations des congruences. Ainsi, plusieurs ont réussi à montrer que, si p est un diviseur impair de S_1, on avait $a^{11} \equiv b^{11} \equiv c^{11} \pmod{p}$.

Exercice 7. Soit f une fonction qui, à chaque droite d du plan, associe un point $f(d)$ appartenant à d. On suppose que, dès lors que trois droites d_1, d_2 et d_3 sont concourantes en un point X, les points $f(d_1)$, $f(d_2)$, $f(d_3)$ et X appartiennent à un même cercle.

a) Démontrer qu'il existe un point P tel que $f(d) = P$ pour toute droite d passant par P.

b) Démontrer qu'il existe bien une telle fonction f.

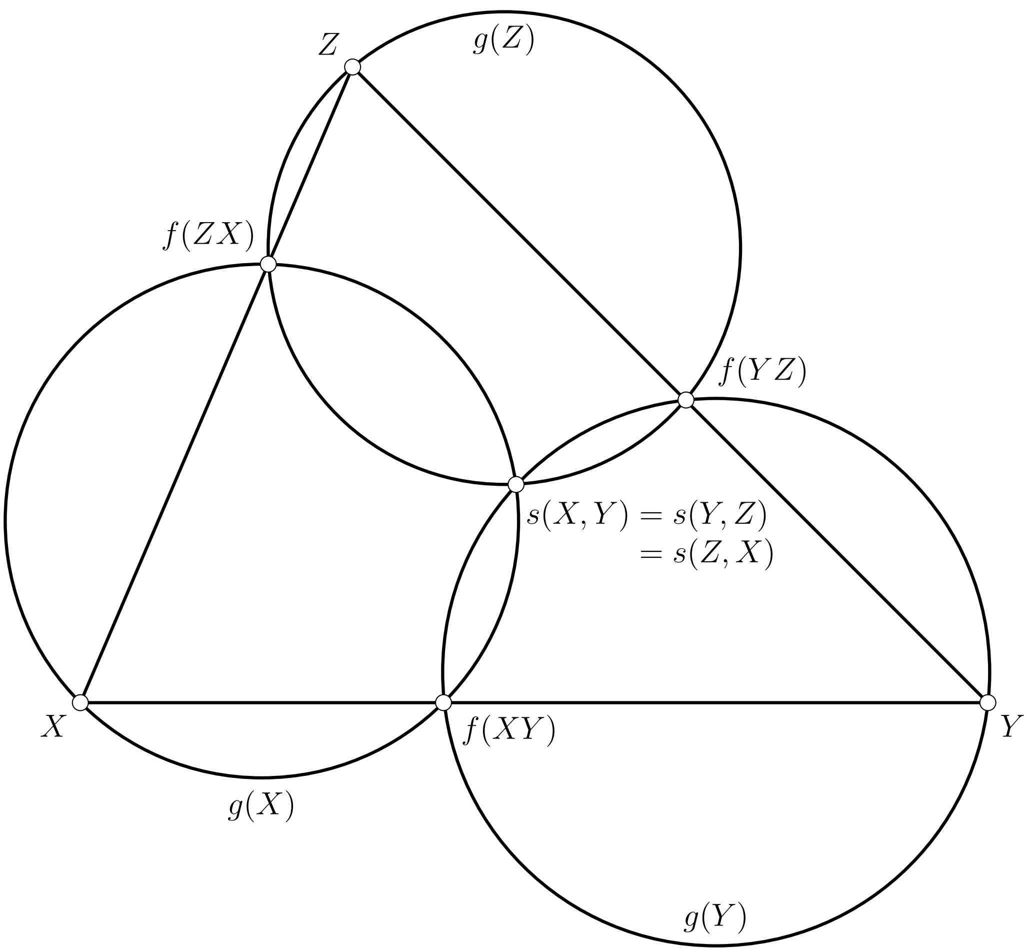
Solution de l'exercice 7 Pour tout point X du plan, il existe un cercle $g(X)$ tel que, dès lors qu'une droite d passe par X, le point $f(d)$ appartient à $g(X)$. En effet :

- ▷ s'il existe au plus une droite d passant par X et telle que $f(d) \neq X$, alors n'importe quel cercle $g(X)$ passant à la fois par X et par $f(d)$ convient ;
- ▷ sinon, soit d_1 et d_2 deux droites fixées, passant par X, et telles que $X \notin \{f(d_1), f(d_2)\}$, puis soit $\mathcal{C}$ le cercle circonscrit à X, $f(d_1)$ et $f(d_2)$; alors, pour toute droite d passant par X, le point $f(d)$ appartient nécessairement à $\mathcal{C}$, et le cercle $g(X) = \mathcal{C}$ convient donc.

D'autre part, pour tous les points X et Y, on sait que $f(XY)$ appartient à $g(X) \cap g(Y) \cap (XY)$. Ainsi, les deux cercles $g(X)$ et $g(Y)$ se rencontrent nécessairement en $f(XY)$. On note alors $s(X, Y)$ leur second point d'intersection, qui est confondu avec $f(XY)$ si et seulement si $g(X)$ et $g(Y)$ sont tangents l'un à l'autre, c'est-à-dire si et seulement si X, Y et $s(X, Y)$ sont alignés.

On remarque alors le lemme suivant, qui découle directement du théorème de Miquel, comme illustré ci-dessous :

> Soit X, Y et Z trois points non alignés et tels que $f(XY)$, $f(YZ)$ et $f(ZX)$ soient tous trois distincts de X, Y et Z. Alors $s(X, Y) = s(Y, Z) = s(Z, X)$.



Choisissons maintenant une droite d quelconque, ainsi que six points $X_1, \ldots, X_6$ de d, tous distincts de $f(d)$. Puis soit Y et Y' deux points qui n'appartiennent ni à d, ni à un des cercles $g(X_i)$. Quitte à réordonner nos points X_i, on peut supposer que $g(Y)$ ne contient aucun des points $X_1, \ldots, X_4$. Mais alors, pour tout $i \leqslant 4$, le point $f(X_iY)$ est distinct de X_i et de Y, et notre lemme ci-dessus indique que $s(X_i, X_j) = s(X_i, Y) = s(X_j, Y)$ pour tous $i, j \leqslant 4$: notons P ce point par lequel passent les cercles $g(Y)$, et $g(X_i)$ pour $i \leqslant 4$.

Notons dès à présent que, si $P \in d$, alors les points $f(d)$ et P sont nécessairement confondus. Il nous reste donc à démontrer que $f(d') = P$ pour toute droite $d' \neq d$ passant par P.

Pour ce faire, notons Y' un point de d' n'appartenant pas à d ni à un des cercles $g(X_i)$. En réappliquant la construction précédente, on constate qu'il existe deux points X_i et X_j, avec $i < j \leqslant 4$, tels que $P = s(X_i, X_j) = s(X_i, Y') = s(X_j, Y')$. Puisque $f(d')$ appartient à l'ensemble $d' \cap g(Y') = \{P, Y'\}$, ceci étant valable pour tout point Y', c'est donc que $f(d') = P$, ce qui conclut.

Enfin, on peut construire directement un exemple de telle fonction f. Il s'agit, par exemple, de la fonction qui, à chaque droite d, associe le projeté orthogonal du point O sur d, où O est un point fixé. En effet, dans ce cas, si trois droites d_1, d_2 et d_3 sont concourantes en un point X, alors les trois points $f(d_1)$, $f(d_2)$ et $f(d_3)$ appartiennent nécessairement au cercle de diamètre $[OX]$.

Commentaire des correcteurs Cet exercice était extraordinairement diffficile, au point qu'aucun élève ne l'a résolu entièrement. Néanmoins, plusieurs élèves ont identifié des propriétés remarquables, qui ont toutes été valorisées : l'existence du cercle $g(X)$, la surjectivité de la fonction f, la non-injectivité de f, ou encore la configuration du lemme.

En particulier, commencer par démontrer que f n'était pas injective était une excellente idée, qui pouvait effectivement mener à une solution (longue et chronophage, donc omise ci-dessus). En effet, l'énoncé nous assurait bien que f ne serait pas injective, et réciproquement, au vu des fonctions solutions plausibles, il y avait tout lieu de croire que le point P recherché serait le seul point du plan avec au moins deux antécédents par f.

Enfin, rappelons quelques évidences simples, qui auraient pu éviter à plusieurs élèves de perdre des points par ailleurs si durement acquis :

- ▷ trois points alignés ne sont pas nécessairement distincts ;
- ▷ deux droites parallèles ne sont pas concourantes, et une droite n'est pas un cercle ;
- ▷ quand quatre points A_1, A_2, A_3 et A_4 appartiennent à un même cercle, le fait que $A_1 = A_2 = A_3$ n'implique *pas* que $A_1 = A_4$; au contraire : tout point est situé sur un cercle qui passe aussi par $A_1 = A_2 = A_3$.

Exercices EGMO

Exercice 8. Noémie a écrit n nombres réels sur son cahier. Chacun est supérieur ou égal à 1, et la somme de ces n nombres est égale à $2n$. Démontrer que, pour tout réel r tel que $0 \leqslant r \leqslant 2n$, Noémie peut choisir un ensemble de nombres, parmi ceux qu'elle a écrits, et dont la somme appartient à l'intervalle $[r, r+2]$.

Solution de l'exercice 8 Soit $x_0, x_1, \ldots, x_{n-1}$ les nombres qu'a écrits Noémie, triés dans l'ordre croissant. On montre alors que, pour tout $k \leqslant n-1$, on a $x_k \leqslant k+2$. Supposons en effet qu'il existe un entier k tel que $x_k > k+2$. Alors

$$2n = x_0 + \ldots + x_{n-1} \geqslant kx_0 + (n-k)x_k > k + (n-k)(k+2) = 2n + k(n-k-1) \geqslant 2n,$$

ce qui est impossible.

Posons maintenant $s_k = x_0 + \ldots + x_{k-1}$, pour tout entier $k \leqslant n$. Nous allons démontrer, par récurrence sur k, la propriété $\mathcal{P}_k$ suivante :

> Pour tout réel r tel que $0 \leqslant r \leqslant s_k$, Noémie peut choisir un ensemble de nombres, parmi les nombres $x_0, \ldots, x_{k-1}$, et dont la somme appartient à l'intervalle $[r, r+2]$.

Puisque $s_0 = 0$, la propriété $\mathcal{P}_0$ est évidente. D'autre part, puisque $s_n = 2n$, l'énoncé nous demande en fait de montrer $\mathcal{P}_n$.

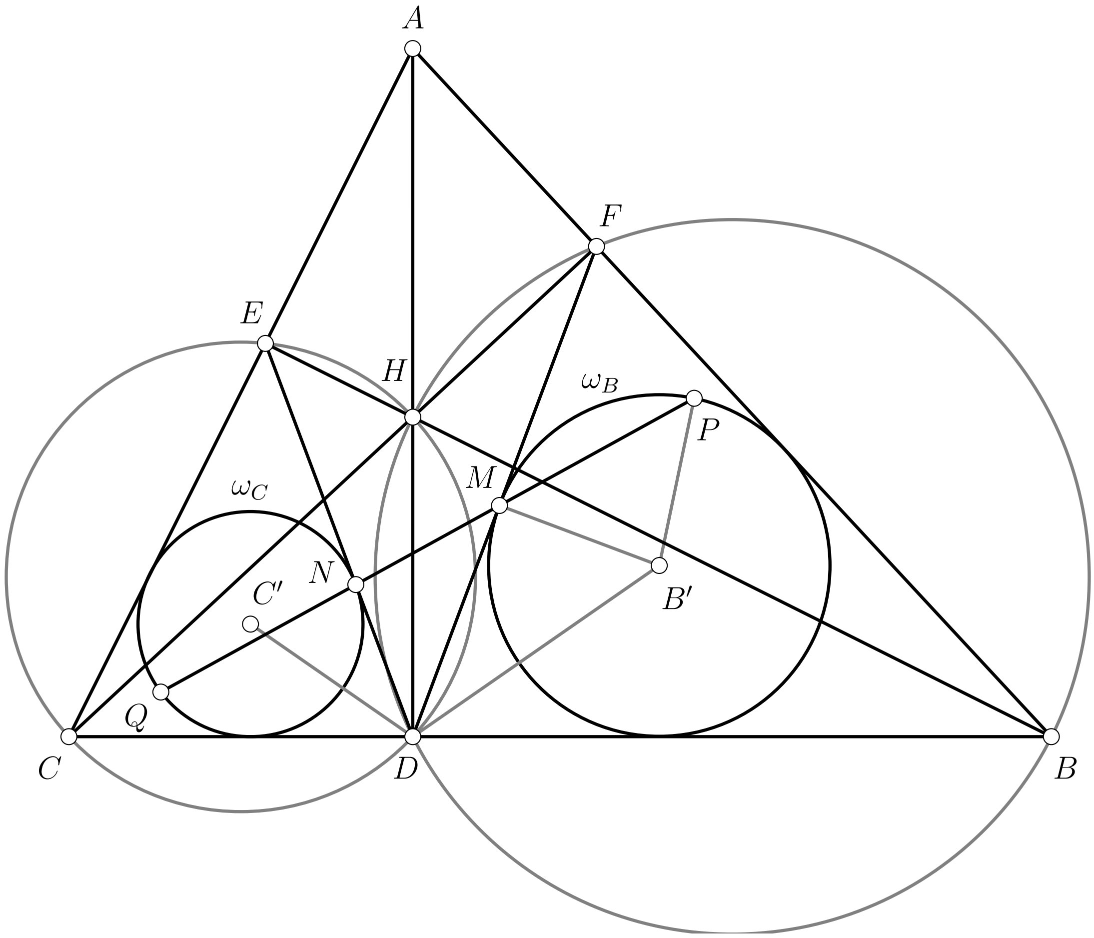
On considère donc un entier $k \geqslant 1$ tel que $\mathcal{P}_{k-1}$ soit vraie, puis un réel r tel que $0 \leqslant r \leqslant s_k$, et on distingue trois cas :

- Si $r \leqslant x_{k-1} - 2$, alors on sait même que $0 \leqslant r \leqslant k-1 \leqslant (k-1)x_0 \leqslant s_{k-1}$. La propriété $\mathcal{P}_{k-1}$ nous assure donc que Noémie peut choisir des nombres, parmi $x_0, \ldots, x_{k-2}$, dont la somme appartient à l'intervalle $[r, r+2]$.
- Si $x_{k-1} - 2 \leqslant r \leqslant x_{k-1}$, Noémie se contente de choisir le nombre x_{k-1}.
- Si $x_{k-1} < r \leqslant s_k$, posons $\delta = r - x_{k-1}$. Alors $0 \leqslant \delta \leqslant s_k - x_{k-1} = s_{k-1}$, et la propriété $\mathcal{P}_{k-1}$ nous assure que Noémie peut choisir des nombres, parmi $x_0, \ldots, x_{k-2}$, dont la somme appartient à l'intervalle $[\delta, \delta+2]$. Par conséquent, si elle choisit, outre ces nombres-là, le nombre x_k, elle obtiendra bien une somme appartenant à l'intervalle $[\delta + x_k, \delta + x_k + 2] = [r, r+2]$, ce qui conclut.

Commentaire des correcteurs Très peu d'élèves ont résolu ce problème ardu. Réussir à trouver une propriété que l'on pourrait démontrer par récurrence était la difficulté principale de cet exercice, mais de nombreuses élèves ont formulé des remarques qui auraient pu les aider à trouver une telle propriété, et qui ont donc été valorisées à hauteur de quelques points. Bravo à toutes les élèves qui ont réussi à avoir des idées sur cet exercice !

Exercice 9. Soit ABC un triangle dont tous les angles sont aigus. On note D, E et F les pieds respectifs des hauteurs issues de A, B et C. Soit ω_B le cercle inscrit dans le triangle BDF, et soit M le point de tangence entre ω_B et (DF). De même, soit ω_C le cercle inscrit dans le triangle CDE, et soit N le point de tangence entre ω_C et (DE). Enfin, soit P le point d'intersection, autre que M, entre (MN) et ω_B, et soit Q le point d'intersection, autre que N, entre (MN) et ω_C.
Démontrer que $MP = NQ$.

Solution de l'exercice 9 Commençons par tracer une figure, en prenant soin de faire apparaître l'orthocentre H du triangle ABC, ainsi que les centres respectifs B' et C' des cercles ω_B et ω_C.



Notons r_B et r_C les rayons respectifs des cercles ω_B et ω_C. Alors

$$MP = 2r_B \sin(\widehat{PB'M}/2) = 2r_B \sin(\widehat{PMF}) = 2r_B \sin(\widehat{DMN})$$

et, de même, $NQ = 2r_C \sin(\widehat{DNM})$. Or, la loi des sinus indique que $DM \sin(\widehat{DMN}) = DN \sin(\widehat{DNM})$. Il s'agit donc de démontrer que

$$MB' \times DN = r_B \times DN = r_C \times DM = NC' \times DM.$$

Afin de démontrer cette égalité, il suffit donc de montrer que les triangles rectangles $B'DM$ et $C'DN$ sont semblables, c'est-à-dire que $\widehat{B'DM} = \widehat{NDC'}$. Or, les points D et F sont tous les deux situés sur le cercle de diamètre $[BH]$, et les points D et E sont tous les deux situés sur le cercle de diamètre $[CH]$. On en déduit que

$$\begin{aligned} 2(B'D, DM) &= (BD, DM) = (BD, DF) = (BH, HF) \\ &= (EH, HC) = (ED, DC) = 2(ED, DC'), \end{aligned}$$

et donc que $\widehat{B'DM} \equiv \widehat{NDC'} \pmod{90°}$, ce qui conclut.

<u>*Commentaire des correcteurs*</u> Une seule élève a réussi l'exercice en entier mais plusieurs élèves ont réussi à avancer significativement. Il fallait noter que les triangles DCE et DFB sont semblables puis utiliser la loi des sinus, ce à quoi de nombreuses élèves ont pensé.

Exercice 10. 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 de l'exercice 10 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.

Commentaire des correcteurs Trois élèves ont résolu cet exercice difficile, mais beaucoup ont réussi à formuler des remarques utiles pour la suite, qui ont systématiquement été valorisées.

La difficulté principale de cet exercice consistait à trouver un cadre agréable pour exprimer la dynamique de notre système : ici, il s'agissait du fait que $a_0 = 2^\ell a_\ell$. Plusieurs élèves ont réussi à démontrer que le processus était injectif (ou réversible), de sorte qu'il se décomposerait nécessairement en un ou plusieurs cycles, mais très peu ont alors pensé à la notion d'ordre.

Enfin, plusieurs élèves ont entrepris de traiter à la main les 503 cas de départ possibles (réduits à 251 après symétrie), mais n'ont jamais abouti ; si de telles tentatives, bien que désespérées en apparence, permettaient bien sûr d'aboutir, elles n'ont en pratique jamais porté leurs fruits, car les élèves ont soit abandonné en cours de route, soit ont fait une erreur de calcul qui condamnait cette approche en l'absence de prise de recul par l'élève. Ainsi, et comme dans le cas de problèmes de géométrie que l'on traiterait en utilisant une approche analytique, ce genre de techniques purement calculatoires ne pouvait être valorisé que si l'élève en déduisait une propriété qui aurait un sens dans le cadre de l'exercice.