Qualification de l'Olympiade mathématique du Canada Repêchage 2026

Un concours de la Société mathématique du Canada.

Solutions officielles

25 février 2026

1. [10 points] Existe-t-il quatre droites dans un même plan, telles qu'aucune trois sont concourantes et aucune deux sont parallèles et telles que quatre particules puissent se déplacer le long de ces droites à des vitesses constantes non nulles (possiblement différentes) de sorte qu'à tout instant, les positions des quatre particules soient cocycliques ?

Solution : La réponse est oui. Une construction possible consiste à choisir un point O et une droite ℓ_1 ne contenant pas O. On définit les droites ℓ_2, ℓ_3 et ℓ_4 comme étant des rotations de ℓ_1 autour de O de sorte qu'aucune paire ne soit parallèle ; il est alors clair qu'aucune triple n'est concourante non plus. Des particules placées initialement en un point arbitraire de ℓ_1, ainsi que leurs images par rotation sur ℓ_2, ℓ_3 et ℓ_4, et se déplaçant à vitesse constante, restent à distance égale de O en tout temps. $\square$

2. [10 points] Existe-t-il des nombres réels positifs a, b, c, non tous égaux, tels que $a^b = b^c = c^a$?

Solution : La réponse est non. Supposons, par contradiction, que de tels a, b et c existent, et que la valeur commune de $a^b = b^c = c^a$ est x. Posons $f(z) = x^{1/z}$. Alors $f(a) = c$, $f(c) = b$ et $f(b) = a$.

Si $x < 1$, alors $f(z)$ est une fonction croissante, ce qui mène à une contradiction : par exemple, si $a < b$, alors on doit avoir $f(a) < f(b)$ et donc $c < a$, et par conséquent $b < c$, et un raisonnement similaire vaut pour $a > b$.

De plus, si $x > 1$, alors $f(z)$ est une fonction décroissante, donc $f(f(z))$ est une fonction croissante, et l'on peut appliquer le même argument que ci-dessus. $\square$

> **3. [10 points]** Soit un point P situé à l'extérieur du cercle Γ. Les tangentes issues de P au cercle Γ touchent Γ en A et B. Une troisième droite passant par P coupe Γ en C et D, avec C situé entre P et D. Un point Q est situé sur la corde CD tel que $\angle DAQ = \angle PBC$. Montrez que $\angle DBQ = \angle PAC$.

Solution : On constate que les angles CAD et CBD sont supplémentaires, de sorte que l'égalité d'angles donnée implique que les angles CAQ et PBD sont également supplémentaires. Posons $\angle DAQ = \angle PBC = \theta$, et $\angle CAQ = \pi - \angle PBD = \alpha$. On tente alors d'utiliser la loi des sinus afin de déterminer CQ/DQ en fonction d'objets ne faisant pas intervenir Q.

On remarque que $CQ = \frac{AC \sin\alpha}{\sin\angle AQC}$ et $DQ = \frac{AD\sin\theta}{\sin\angle AQC}$.

Notre objectif est maintenant d'écrire ce rapport en fonction d'une expression symétrique en A et B. À cette fin, on écrit $\sin\alpha = \frac{PD}{PB}\sin\angle CDB$ et $\sin\theta = \frac{PC}{PB}\sin\angle DCB$, d'où

$$\frac{CQ}{DQ} = \frac{AC \cdot PD \cdot \sin\angle CDB}{AD \cdot PC \cdot \sin\angle DCB} = \frac{AC \cdot PD \cdot CB}{AD \cdot PC \cdot BD}.$$

Cette expression est symétrique en A et B ; ainsi, si l'on choisit un point Q' tel que $\angle PAC = \angle DBQ'$, alors $CQ'/DQ' = CQ/DQ$, d'où $Q = Q'$, comme désiré. $\square$

> **4. [15 points]** Soit p un nombre premier fixe et soient k et n des entiers naturels tels que $k \geq n$. On choisit k vecteurs $v_1, \ldots, v_k$ de manière uniforme au hasard (avec répétition possible) dans l'ensemble $\{(x_1, \ldots, x_n) | x_i \in \{0, 1, \ldots, p-1\}\}$. De plus, pour $1 \leq i \leq n$, soit v_{k+i} le vecteur ayant la valeur p sur la i-ième coordonnée et 0 ailleurs.
> On dit que ces $k+n$ vecteurs *engendrent* $\mathbb{Z}^n$ si, pour tout vecteur à composantes entières $v = (y_1, \ldots, y_n)$, il existe des entiers $c_1, \ldots, c_{k+n}$ tels que $v = \sum_{i=1}^{k+n} c_i v_i$. On note $P(p,n,k)$ la probabilité que ces $k+n$ vecteurs engendrent $\mathbb{Z}^n$.
> Alors il existe une constante c, qui dépend de p et de n, telle que $p^k(1 - P(p,n,k)) - c \to 0$ lorsque $k \to \infty$. Déterminez c en fonction de p et de n.

Solution : La réponse est $\frac{p^n-1}{p-1} = p^{n-1} + \cdots + 1$. Comme le suggère l'énoncé, il est plus facile de compter le complément.

Pour un vecteur $v \in \mathbb{Z}^n$ dont les coordonnées ne sont pas toutes des multiples de p, on définit $v^\perp$ par

$$\left\{ w \in \mathbb{Z}^n \mid \sum_{i=1}^n w_i v_i \equiv 0 \pmod{p} \right\}.$$

On remarque que $v^\perp$ ne dépend que de la classe de résidus de v modulo p, et que $v^\perp = (cv)^\perp$ pour $c \in \{1, 2, \ldots, p-1\}$; il y a donc $\frac{p^n-1}{p-1}$ ensembles distincts de ce type $v^\perp$.

La donnée clé est le lemme d'algèbre linéaire suivant : si les $k+n$ vecteurs n'engendrent pas $\mathbb{Z}^n$, alors il existe un certain v pour lequel ils appartiennent tous à $v^\perp$. Reportons la preuve de ce lemme à la fin de cette solution. En admettant ce lemme, on peut conclure par le principe d'inclusion-exclusion. On obtient

$$1 - P(p,n,k) = \sum_w \mathbb{P}(v_1, \ldots, v_k \in w^\perp) - \sum_{w_1 \neq cw_2} \mathbb{P}(v_1, \ldots, v_k \in w_1^\perp \cap w_2^\perp) + \ldots$$

$$+(-1)^{m-1} \sum_{\substack{w_1,\ldots,w_m \\ \text{distinct jusqu'à la mise à l'échelle}}} \mathbb{P}(v_i \in w_j^\perp\ \forall i,j) - \ldots,$$

où cette somme est finie puisqu'il n'y a que $\frac{p^n-1}{p-1}$ possibilités distinctes pour $v^\perp$ jusqu'à la mise à l'échelle.

On note également que le premier terme dans la probabilité ci-dessus vaut
$\mathbb{P}(v_1,\ldots,v_k \in w^\perp) = \frac{1}{p^k}$, et que les termes d'ordre supérieur vérifient
$\mathbb{P}(v_1,\ldots,v_k \in w_1^\perp, w_2^\perp,\ldots,w_m^\perp) \leq \mathbb{P}(v_1,\ldots,v_k \in w_1^\perp, w_2^\perp) = \frac{1}{p^{2k}}$, d'où
$p^k(1-P(p,n,k)) = \frac{p^n-1}{p-1} + O(p^{-k})$, où la constante implicite dépend de n. Cela permet de conclure que $c = \frac{p^n-1}{p-1}$.

Preuve du lemme : Nous démontrons maintenant le lemme ci-dessus. L'idée principale est de construire un *sous-ensemble générateur* des vecteurs $v_1,\ldots,v_k$. Pour $1 \leq \ell \leq k$, soit T_ℓ l'ensemble engendré par $v_1,\ldots,v_\ell,v_{k+1},\ldots,v_n$. On dit que v_ℓ est un vecteur générateur si $T_\ell \neq T_{\ell-1}$ (de sorte que v_1 est toujours un vecteur générateur).

De plus, on définit la *taille* de T_ℓ comme le nombre de classes de résidus dans $\mathbb{Z}^n$ qu'il rencontre. On dispose alors du fait suivant : si v_ℓ est le m-ième vecteur générateur, alors la taille de T_ℓ est p^m. En admettant ce fait, on voit qu'il y a au plus $n-1$ vecteurs générateurs. Notons-les $x_1,\ldots,x_h$. On peut alors trouver un vecteur v tel que $x_1,\ldots,x_h \in v^\perp$, puisque cela revient à résoudre un système de h équations à n variables. □

5. [15 points] Déterminez s'il existe une fonction surjective $f : (0, \infty) \to \mathbb{N}$, telle que, pour tous réels positifs $a < b$, l'image de l'intervalle ouvert (a, b) par f soit un ensemble de la forme $\{1, 2, \ldots, N\}$, où N est un certain entier positif fini.

On rappelle qu'une fonction $f : (0, \infty) \to \mathbb{N}$ est dite *surjective* si, pour tout entier naturel M, il existe un réel strictement positif r tel que $f(r) = M$.

Solution : La réponse est oui. Nous donnons ci-dessous une construction explicite. Pour tout nombre de la forme $m/2^k$, où m et k sont des entiers positifs, soit $d(m)$ le nombre de 1 dans l'écriture binaire de m. On remarque que cela est indépendant de la représentation de m. On définit alors

$$f\left(\frac{m}{2^k}\right) = \max\left(1, \left\lfloor \log_2 \frac{m}{2^k} \right\rfloor + 1 - d(m)\right).$$

Pour tout réel r tel qu'il n'existe aucun entier positif k pour lequel $2^k r$ soit un entier, on pose $f(r) = 1$.

On peut maintenant vérifier que cette fonction est surjective ; en effet, $f(2^n) = n$ pour tout entier positif n. De plus, supposons qu'un intervalle ouvert (a, b) contienne un certain r tel que $f(r) = c$. Alors, si $c > 1$, en ajoutant une puissance de deux suffisamment petite à r, on obtient un certain $r + \frac{1}{2^m} \in (a, b)$ tel que $f(r + \frac{1}{2^m}) = c - 1$. Nous avons ainsi montré que si un entier positif c appartient à l'image de (a, b) par f, alors $c - 1$ y appartient aussi. De plus, on voit que $f(r) \leq \max(1, \log_2 r)$ par définition, donc f est bornée sur tout intervalle (a, b), et par conséquent l'image est de la forme $\{1, 2, \ldots, N\}$ pour un certain N, comme désiré. $\square$

6. [20 points] Un ensemble T d'entiers positifs est donné. Pour un entier positif n, Alice et Bob jouent à un jeu qui commence avec un tas initial de n pierres. À tour de rôle, ils retirent m pierres du tas, où $m \in T$ et $m \leq n$. Le joueur qui prend la dernière pierre gagne. Si, à un moment donné, le nombre de pierres dans le tas est strictement inférieur à $\min T$, alors la partie est déclarée nulle. On dit qu'un entier n est *bon* si Alice peut garantir une victoire, *mauvais* si Bob peut garantir une victoire, et *neutre* si ni Alice ni Bob ne peuvent garantir une victoire.

Par exemple, si T est l'ensemble des nombres premiers, alors $n = 4$ est neutre et $n = 5$ est bon : dans la première partie, Alice peut garantir un match nul en retirant 3 pierres à son premier coup, et elle ne peut pas faire mieux, tandis que dans la seconde partie, elle peut retirer toutes les pierres à son premier coup et gagner.

(a) Montrez que si T est fini, alors l'ensemble des entiers bons est ultimement périodique : c'est-à-dire qu'il existe des entiers positifs N et p tels que, pour tout entier positif $n > N$, n est bon si et seulement si $n + p$ est bon.

(b) Construisez un ensemble infini T tel que l'ensemble des entiers bons ne soit pas périodique : c'est-à-dire que, pour toute paire d'entiers positifs N et p, il existe un entier $n > N$ tel que exactement l'un des deux entiers n et $n + p$ soit bon.

Solution :

(a) Soit $M = \max T$. On voit que le statut de n ne dépend que des statuts de $n - M, n - M + 1, \ldots, n - 1$. Il y a un nombre fini de tels états, donc, par le principe des tiroirs, il existe $n_1 < n_2$ tels que les statuts de $n_1 - c$ et $n_2 - c$ soient identiques pour $c = M, M - 1, \ldots, 1$. Alors, par récurrence, ils sont aussi égaux pour $c \leq 0$, de sorte que l'on peut choisir $N = n_1$ et $p = n_2 - n_1$.

(b) On choisit T de sorte que $1, 2 \notin T$, $3, 4, 5 \in T$, et que, pour tout $n \in \mathbb{N}$, au moins un des entiers $n, n+1, n+2$ appartienne à T. L'assertion principale pour un tel ensemble T est qu'un entier positif $n \geq 5$ est bon si et seulement si $n \in T$, et que tous les entiers qui ne sont pas bons sont neutres.

On voit d'abord que si $n \in T$, alors Alice peut prendre toutes les pierres et gagner. De même, si $n \notin T$, alors soit $n - 1 \in T$, soit $n - 2 \in T$. Alice peut prendre ce nombre de pierres, mettant fin à la partie par une nulle, de sorte que tous les $n \notin T$ sont soit neutres soit bons. De plus, après le coup d'Alice, si elle enlève moins de $n - 3$ pierres, alors Bob se retrouvera dans la même situation et pourra forcer au pire une nulle. Ainsi, les $n \notin T$ ne peuvent pas être bons : ils doivent être neutres.

Il suffit maintenant de construire un tel ensemble T qui ne soit pas non plus éventuellement périodique. On peut par exemple choisir $T = \mathbb{N} \setminus \{n! \mid n \in \mathbb{N}\}$.

□

7. [**20 points**] Déterminez le plus petit entier positif qui n'est pas un carré parfait et qui peut s'écrire sous la forme $\frac{a^2+b^2}{ab+1}$ pour certains nombres rationnels a et b tels que $ab \neq -1$.

Solution : La réponse est 10. On voit que la paire $(a,b) = \left(\frac{13}{2}, \frac{1}{2}\right)$ donne $\frac{a^2+b^2}{ab+1} = 10$. Il reste à montrer que, pour les entiers positifs $k \in \{2,3,5,6,7,8\}$, il est impossible d'obtenir $\frac{a^2+b^2}{ab+1} = k$ avec des nombres rationnels a et b.

Tout d'abord, on remarque que si $a = 0$ ou $b = 0$, on obtient un carré parfait ; on peut donc supposer que a, b sont tous deux non nuls.

Pour un nombre premier p et un rationnel non nul r, on définit $v_p(r)$ comme étant le nombre de facteurs premiers p dans la factorisation de r. Il est clair par définition que $v_p(rs) = v_p(r) + v_p(s)$ pour tous r, s, et l'on voit aussi que $v_p(r+s) \geq \min(v_p(r), v_p(s))$, avec l'égalité vérifiée sauf si éventuellement $v_p(r) = v_p(s)$.

On voit maintenant que si $p \equiv 3 \pmod 4$, $p \mid k$, et $p \nmid k^2$, alors $v_p(a^2+b^2) = 2\min(v_p(a), v_p(b))$. Ainsi, $v_p(ab+1)$ doit être impair, et donc $v_p(a) + v_p(b) = 0$. Mais alors $v_p(a^2+b^2) \leq 0$ et $v_p(k(ab+1)) > 0$, ce qui est une contradiction. Cela élimine les cas $k = 3, 6, 7$.

Maintenant, pour $k = 5, 8$, on considère l'équation $(a-b)^2 = (k-2)ab + k$. Si $v_2(ab) \geq 0$, on obtient une contradiction puisque le membre de droite est $2 \pmod 3$. Sinon, $v_2(ab)$ doit être impair, puisque $v_2((k-2)ab)$ doit être un entier pair non positif. Cela implique que $v_2(a) \neq v_2(b)$. Supposons que $v_2(a) < v_2(b)$. Alors $v_2((a-b)^2) = 2v_2(a)$ et $v_2((k-2)ab+k) = 1 + v_2(a) + v_2(b)$, ce qui donne une contradiction.

Enfin, pour $k = 2$, notre équation devient $(a-b)^2 = 2$, qui n'admet pas de solutions rationnelles.

Remarque : Par le théorème de Hasse–Minkowski, on peut voir que si, pour un certain k qu'aucun a, b rationnel ne satisfait $\frac{a^2+b^2}{ab+1} = k$, il existera toujours un argument considérant v_p modulo un certain nombre premier qui mettra en évidence la contradiction, comme ci-dessus. $\square$

