Financière Sun Life

Solutions de l'OMC 2015

Problème 1. *Soit* $\mathbb{N} = \{1, 2, 3, \ldots\}$ *l'ensemble des entiers strictement positifs. Trouvez toutes les fonctions* f *définies sur* $\mathbb{N}$ *et prenant des valeurs dans* $\mathbb{N}$ *telles que* $(n-1)^2 < f(n)f(f(n)) < n^2 + n$ *pour tout entier* $n \in \mathbb{N}$.

Solution. La seule fonction qui satisfait la condition est $f(n) = n$. On va montrer que c'est bien le cas.

Méthode 1: Supposons que la fonction f satisfait la condition. On montrera par induction que $f(n) = n$ pour tout $n \in \mathbb{N}$. En remplaçant $n = 1$ on trouve que $0 < f(1)f(f(1)) < 2$, ce qui ne laisse que la possibilité $f(1) = 1$. Supposons maintenant que $f(k) = k$ pour toutes les valeurs $k < n$ et que $f(n) \neq n$.

D'un côté, si $f(n) \leq n-1$ alors $f(f(n)) = f(n)$ et $f(n)f(f(n)) = f(n)^2 \leq (n-1)^2$ ce qui est une contradiction. De l'autre côté, si $f(n) \geq n+1$ on peut procéder de plusieurs manières afin d'obtenir une contradiction.

Première variante: Supposons que $f(n) = M \geq n+1$. Alors $(n+1)f(M) \leq f(n)f(f(n)) < n^2 + n$. Ainsi, $f(M) < n$ et on a $f(f(M)) = f(M)$ et $f(M)f(f(M)) = f(M)^2 < n^2 \leq (M-1)^2$, ce qui est une contradiction. C'est ce qui complète l'étape d'induction. □

Deuxième variante: On remarque pour commencer que si $|a-b| > 1$, alors les intervalles $((a-1)^2, a^2+a)$ et $((b-1)^2, b^2+b)$ sont disjoints. Ceci nous assure que $f(a)$ et $f(b)$ ne peuvent être égaux.

En supposant que $f(n) \geq n+1$, on obtient que $f(f(n)) < \frac{n^2+n}{f(n)} \leq n$. Ceci implique que pour un certain $a \leq n-1$, $f(a) = f(f(n))$. C'est une contradiction puisque $|f(n) - a| \geq n + 1 - a \geq 2$. C'est ce qui complète l'étape d'induction. □

Méthode 2:
Étape 1: Supposons qu'il y a une autre fonction f qui satisfait la condition. Alors soit

$$f(n) > n \quad \text{pour un certain } n \in \mathbb{N}, \tag{1}$$

ou

$$f(n) < n \quad \text{pour un certain } n \in \mathbb{N}. \tag{2}$$

Étape 2: Supposons que la condition (1) est vraie et posons $k = f(n) > n$. Alors $f(n)f(f(n)) = kf(k) < n^2 + n$, donc $f(k) < (n^2+n)/k \leq (n^2+n)/(n+1) = n < k$. Ainsi, la condition (2) doit aussi être vraie.

Étape 3: Supposons que la condition (2) est vraie et posons $m = f(n) < n$. Alors $f(n)f(f(n)) = mf(m) > (n-1)^2$, donc $f(m) > (n-1)^2/m \geq (n-1)^2/(n-1) = n-1 \geq m$. De cette façon, la condition (1) doit aussi être vraie.

Étape 4: Nous avons montré jusqu'à présent que les conditions (1) et (2) sont équivalentes. Supposons que la condition (2) est vraie, soit que $m = f(n) < n$ pour un certain $n \in \mathbb{N}$. Le calcul fait à l'étape 3 nous montre que $f(m) > m$ et le calcul de l'étape 2 nous montre

Financière Sun Life

de son côté que $f(f(m)) < m < f(m)$. On définit la séquence $a_0, a_1, a_2, \dots$ par $a_0 = n$, et $a_l = f(a_{l-1})$ pour $l \geq 1$. Ainsi, nous avons $a_1 < a_0$ tandis que les étapes 2 et 3 montrent que si $a_{2i+1} < a_{2i}$, on a $a_{2i+3} < a_{2i+1} < a_{2i+2}$. L'induction montre que $a_{2i+1} < a_{2i}$ et $a_{2i+3} < a_{2i+1}$ pour tout $i \geq 0$. En particulier, on a

$$a_1 > a_3 > a_5 > \dots > a_{2l+1} > a_{2l+3} > \dots$$

Il s'agit d'une suite strictement décroissante d'entiers positifs, ce qui est impossible dans le contexte. Ceci implique qu'aucune des conditions (1) et (2) ne peut être vraie et ainsi que la seule fonction qui satisfait les critères demandés est $f(n) = n$. □

Problème 2. *Soit ABC un triangle aigu avec ses hauteurs AD, BE et CF. Soit H, l'orthocentre du triangle (le point de rencontre des hauteurs). Montrez que*

$$\frac{AB \cdot AC + BC \cdot BA + CA \cdot CB}{AH \cdot AD + BH \cdot BE + CH \cdot CF} \leq 2\,.$$

Solution. Méthode 1: On pose $AB = c$, $AC = b$ et $BC = a$ les longueurs des côtés du triangle.

Comme $\angle BFH = \angle BDH = 90°$, $FHDB$ est un quadrilatère inscriptible. Par le théorème de la puissance d'un point, $AH \cdot AD = AF \cdot AB$ (on peut trouver cette relation de plusieurs façons, voir par exemple la méthode 2 plus bas).

Puisque $AF = AC \cdot \cos\angle A$, on a que $AH \cdot AD = AC \cdot AB \cdot \cos\angle A = bc\cos\angle A$.

Par la loi des cosinus, $\cos\angle A = \dfrac{b^2+c^2-a^2}{2bc}$ qui implique que $AH \cdot AD = \dfrac{b^2+c^2-a^2}{2}$.

Par symétrie, on peut montrer que $BH \cdot BE = \dfrac{a^2+c^2-b^2}{2}$ et $CH \cdot CF = \dfrac{a^2+b^2-c^2}{2}$. Ainsi,

$$\begin{aligned} AH \cdot AD + BH \cdot BE + CH \cdot CF &= \frac{b^2+c^2-a^2}{2} + \frac{a^2+c^2-b^2}{2} + \frac{a^2+b^2-c^2}{2} \\ &= \frac{a^2+b^2+c^2}{2}. \end{aligned} \tag{3}$$

L'inégalité voulue, $\dfrac{AB \cdot AC + BC \cdot BA + CA \cdot CB}{AH \cdot AD + BH \cdot BE + CH \cdot CF} \leq 2$, est équivalente à l'inégalité $\dfrac{cb+ac+ba}{\frac{a^2+b^2+c^2}{2}} \leq 2$, qui peut être simplifiée à $2a^2 + 2b^2 + 2c^2 \geq 2ab + 2bc + 2ca$.

Mais cette dernière inégalité est facile à démontrer puisqu'elle est équivalente à $(a-b)^2 + (a-c)^2 + (b-c)^2 \geq 0$.

On a donc montré l'inégalité voulue. La preuve montre aussi que l'égalité survient seulement lorsque $a = b = c$, i.e. lorsque $\triangle ABC$ est équilatéral. □

Méthode 2: On remarque que

$$\frac{AE}{AH} = \cos(\angle HAE) = \frac{AD}{AC} \quad \text{et} \quad \frac{AF}{AH} = \cos(\angle HAF) = \frac{AD}{AB}.$$

Il suit alors que

$$AC \cdot AE = AH \cdot AD = AB \cdot AF\,.$$

Par symétrie, on a aussi

$$BC \cdot BD = BH \cdot BE = BF \cdot BA \quad \text{et} \quad CD \cdot CB = CH \cdot CF = CE \cdot CA\,.$$

Ainsi

$$\begin{aligned}
&2(AH \cdot AD + BH \cdot BE + CH \cdot CF)\\
&\quad = \; AB(AF + BF) \,+\, AC(AE + CE) \,+\, BC(BD + CD)\\
&\quad = \; AB^2 \,+\, AC^2 \,+\, BC^2.
\end{aligned}$$

Ceci montre l'équation (3) de la Méthode 1. Le reste de la preuve est semblable à celle de la Méthode 1 après l'équation (3). □

Problème 3. *Sur une grille carrée* $(4n+2) \times (4n+2)$*, une tortue se déplace entre les cases qui partagent un côté. La tortue débute dans un coin de la grille et visite chaque case exactement une fois avant de revenir à son point de départ. En fonction de* n*, quel est le plus grand entier positif* k *tel qu'il doit y avoir une rangée ou une colonne dans laquelle la tortue est entrée à au moins* k *reprises?*

Solution. Nous allons montrer que la réponse est $2n+2$. On numérote les rangées en ordre croissant du haut vers le bas. On fait de même pour les colonnes, de la gauche vers la droite. Par symétrie, on suppose que la tortue débute dans le coin supérieur droit de la grille.

Pour commencer, on montre qu'il doit y avoir une rangée ou une colonne dans laquelle la tortue est entrée au moins $2n+2$ fois. Soit $m = 4n+2$. On remarque tout d'abord qu'à chaque fois que la tortue bouge, elle entre soit dans une rangée ou dans une colonne. On pose r_i comme le nombre de fois que la tortue entre dans la rangée i et c_i comme le nombre de fois qu'elle entre dans la colonne i. Puisque la tortue bouge m^2 fois,

$$r_1 + r_2 + \cdots + r_m + c_1 + c_2 + \cdots + c_m = m^2.$$

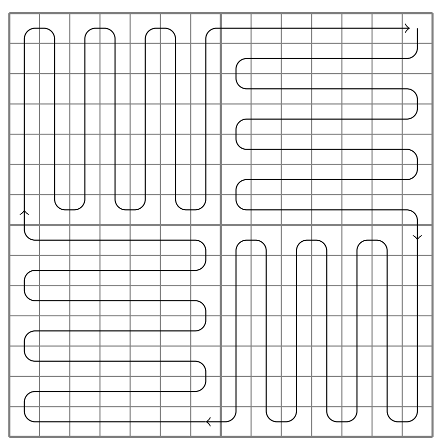
Mais à chaque fois que la tortue entre dans la colonne 1, la prochaine colonne dans laquelle elle entre est nécessairement la colonne 2. Ainsi, c_1 est aussi égal au nombre de fois que la tortue entre dans la colonne 2 à partir de la colonne 1. De plus, la tortue doit entrer au moins une fois dans la colonne 2 à partir de la colonne 3, ce qui implique que $c_2 > c_1$. Ainsi, puisque les $2m$ termes r_i et c_i ne sont pas tous égaux, un de ceux-ci doit être supérieur à $m^2/(2m) = 2n+1$ et donc au moins $2n+2$.

On doit ensuite trouver un exemple pour lequel la tortue est entrée au plus $2n+2$ fois dans chacune des lignes ou colonnes. On présente ici trois exemples possibles.

Exemple 1:

On sépare la grille en quatre quadrants de grosseur $(2n+1) \times (2n+1)$ qu'on nomme A, B,

C et D et qui contiennent respectivement le coin supérieur gauche, supérieur droit, inférieur gauche et inférieur droit. La tortue débute au coin supérieur droit de B, descend d'une case puis traverse vers la gauche sur toute la deuxième rangée de B. Elle descend ensuite d'une case puis traverse vers la droite sur toute la troisième rangée de B. La tortue continue à bouger de cette façon jusqu'à la ligne inférieure de B. Comme $2n+1$ est impair, la tortue termine au coin inférieur droit de B. La tortue descend ensuite d'une case pour arriver dans le quadrant D et traverse chaque colonne de D tour à tour en bougeant d'une case vers la gauche lorsqu'une colonne est terminée. Elle termine au coin inférieur gauche de D et se déplace vers la gauche dans le quadrant C. Elle parcourt ensuite les lignes de C en bougeant vers le haut à chaque fin de ligne pour finalement terminer au coin supérieur gauche de C. Elle entre dans le quadrant A et parcourt les colonnes de A en bougeant d'une case vers la droite lorsqu'une colonne est terminée. La tortue termine au coin supérieur droit de A où elle entre dans le quadrant B et parcourt la ligne supérieure de B pour retourner à son point de départ. Pour chaque ligne passant dans les quadrants A et B, la tortue est entrée au plus $2n+1$ fois dans A et au plus 1 fois dans B, pour un total d'au maximum $2n+2$. On peut adapter ce raisonnement à chaque ligne et colonne de la grille. Ainsi, la tortue est entrée au plus $2n+2$ fois dans chaque ligne ou colonne, comme la figure l'illustre.



Problème 3: Exemple 1 dans le cas $n = 3$

Exemple 2:
On écrit (a, b) pour identifier la case de la $a^{\text{ième}}$ colonne à partir de la droite et de la $b^{\text{ième}}$ rangée à partir du haut. La tortue part de la case $(1, 1)$ et descend tout droit vers la case $(1, 4n+2)$. Elle bouge ensuite vers la gauche vers la case $(2, 4n+2)$, vers le haut jusqu'à la case $(2, 2)$ et à gauche sur la case $(3, 2)$.

Pour i allant de 0 à $n-1$, voici la façon selon laquelle la tortue se déplace de la case $(4i+3, 2)$ à la case $(4i+6, 2)$:

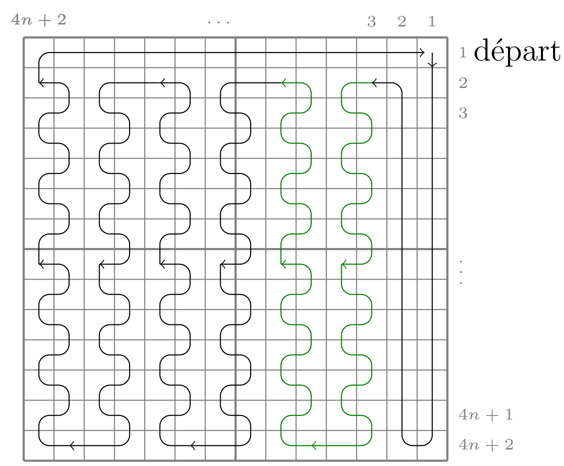
> En partant de la case $(4i+3, 2)$, la tortue se déplace d' *une case vers la gauche, d'une case vers le bas, d'une case vers la droite puis d'une case vers le bas* pour atteindre $(4i+3, 4)$. La tortue effectue cette séquence $2n$ fois pour terminer en $(4i+3, 4n+2)$.

La tortue bouge ensuite vers la gauche pour atteindre la case $(4i+6, 4n+2)$ et répète ensuite la séquence *une case vers le haut, une case vers la droite, une case vers le haut, une case vers la gauche* à $2n$ reprises pour terminer en $(4i+6, 2)$.

Si $4i+6 < 4n+2$, alors elle bouge d'une case vers la gauche sur $(4i+7, 2)$ et répète la procédure pour la valeur suivante de i (voir le chemin en vert pour $i=0$).

Lorsqu'elle atteint $(4n+2, 2)$, la tortue bouge vers le haut jusqu'à $(4n+2, 1)$ et ensuite vers la droite jusqu'à $(1, 1)$.

En suivant ce chemin, la tortue pénètre dans la rangée 1 une seule fois, dans la rangée 2 à $n+2$ reprises, dans chacune des rangées 3 à $(4n+1)$ à $2n+2$ reprises et dans la rangée $(4n+2)$ à $n+1$ reprises. On entre dans la colonne 1 une seule fois, dans la colonne 2 à deux reprises, dans chacune des colonnes 3 à $(4n+1)$ à $2n+2$ reprises et dans la colonne $(4n+2)$ à $2n+1$ reprises.



Problème 3: Exemple 2 dans le cas $n = 3$

Exemple 3:
On identifie les cases par (a, b) comme dans l'exemple 2. On va montrer que pour $n \geq 1$, il existe un chemin qui

(a) traverse chacune des $(4n+2)\times(4n+2)$ cases de la grille exactement une fois et revient à son point de départ;

(b) débute en $(1, 1)$ et fait son dernier pas de la case $(2, 1)$ vers $(1, 1)$;

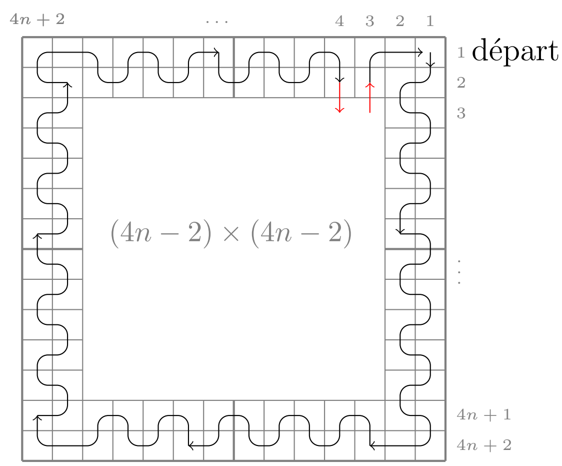
(c) entre dans chaque ligne ou colonne au plus $2n{+}2$ fois;

(d) entre dans la rangée 1 au plus $2n{+}1$ fois.

Pour la grille 6×6 $(n=1)$, on peut faire une des constructions décrites plus haut. Supposons qu'il existe un tel chemin pour la grille $(4n-2)\times(4n-2)$, pour une certaine valeur de $n \geq 2$.

Dans la grille $(4n+2) \times (4n+2)$, la tortue débute à la case $(1,1)$ et traverse les deux premières colonne, les deux lignes du bas, les deux colonnes de gauche et termine en traversant les deux lignes du haut comme indiqué dans la figure. Lorsqu'elle atteint la case $(4,2)$, elle descend pour entrer dans la grille $(4n-2) \times (4n-2)$ dont le coin supérieur droit est $(4,3)$. La tortue suit ensuite le chemin prévu pour la grille $(4n-2) \times (4n-2)$ dans la direction inverse (sans le dernier mouvement), et termine en $(3,3)$. La tortue termine son parours en traversant deux cases vers le haut et deux cases vers la droite pour revenir à son point de départ.

Ce parcours de la grille $(4n+2) \times (4n+2)$ satisfait les conditions (a) et (b) énoncées plus haut. La tortue entre dans la rangée 1 exactement $2n$ fois donc la condition (d) tient. La tortue entre dans la rangée 2 à $2n+2$ reprises. Le nombre de fois où la tortue entre dans la rangée 3 est exactement trois de plus que le nombre de fois où elle entre dans cette rangée dans la grille $(4n-2) \times (4n-2)$. Puisque le chemin utilisé dans la sous-grille satisfait à la condition (d) (avec n remplacé par $n-1$), la tortue entre dans la rangée 3 au plus $2n+2$ fois. De la même manière, le nombre de fois où la tortue entre dans chacune des rangées 4 à $4n$ et chacune des colonnes 3 à $4n$ est exactement 2 de plus que le nombre correspondant pour la grille $(4n-2) \times (4n-2)$. Ainsi, la tortue est entrée dans chacune de ces rangées et de ces colonnes au plus $2n+2$ fois. La tortue entre dans la rangée $(4n+1)$ exactement $2n+1$ fois; elle entre dans la rangée $(4n+2)$ exactement $2n$ fois; dans les colonnes 1 et $(4n+2)$ à $2n+1$ reprises chacune; dans les colonnes 2 à $(4n+1)$ à $2n+2$ reprises chacune. Ainsi, la condition (c) est satisfaite.



Problème 3: Exemple 3 dans le cas $n = 3$

$\square$

Problème 4. *Soit ABC un triangle aigu dont le centre du cercle circonscrit est O. Soit Γ un cercle dont le centre se trouve sur la hauteur issue de A dans ABC et qui passe par le sommet A ainsi que par les points P et Q sur les côtés AB et AC. Supposons que $BP \cdot CQ = AP \cdot AQ$. Montrez que Γ est tangent au cercle circonscrit du triangle BOC.*

Solution. **Méthode 1:** Soit ω le cercle circonscrit de BOC. On pose M le point diamétralement opposé à O sur ω et on pose que AM croise ω en M et K. Puisque O est le centre du cercle circonscrit de ABC, on sait que $OB = OC$ et donc que O est le point milieu de l'arc $\widehat{BOC}$ sur ω. Comme M est diamétralement opposé à O, M est le point milieu de l'arc $\widehat{BMC}$ de ω. Comme K est sur ω, ceci implique que KM est la bissectrice de $\angle BKC$. De la même façon on a $\angle BKM = \angle CKM$, i.e. KM est la bissectrice de $\angle BKC$.

Puisque O est le centre du cercle circonscrit de ABC, on sait que $\angle BOC = 2\angle BAC$. Comme B, K, O et C se trouvent tous sur ω, on en déduit que $\angle BKC = \angle BOC = 2\angle BAC$. Comme KM sépare en deux $\angle BKC$, on trouve que $\angle BKM = \angle CKM = \angle BAC$. Le fait que A, K et M se trouvent sur une même droite nous indique que $\angle AKB = \angle AKC = 180^\circ - \angle BAC$. On trouve ensuite que

$$\angle KBA = 180^\circ - \angle AKB - \angle KAB = \angle BAC - \angle KAB = \angle KAC.$$

Ceci implique que les triangles KBA et KAC sont semblables. En réarrangeant la condition dans l'énoncé du problème, on trouve $BP/AP = AQ/CQ$ qui, conjointement avec le fait que KBA et KAC sont semblables, implique que les triangles KPA et KQC sont semblables. Ainsi, $\angle KPA = \angle KQC = 180^\circ - \angle KQA$ ce qui implique que K est situé sur Γ.

Notons S le centre de Γ et T le centre de ω. On remarque que T est le point milieu du segment OM et que TM et AS, tous deux perpendiculaires à BC, sont parallèles. Ceci implique que $\angle KMT = \angle KAS$ puisque A, K et M sont colinéaires. De plus, comme KTM et KSA sont des triangles isocèles, on trouve que $\angle TKM = \angle KMT$ et $\angle SKA = \angle KSA$. Ainsi $\angle TKM = \angle SKA$ ce qui implique que S, T et K sont colinéaires. Donc Γ et ω se croisent au point K, situé sur ST. On sait donc que les cercles Γ et ω sont tangents en K. $\square$

Remarque: Une autre manière d'approcher la Méthode 1 est le concept du centre de la similarité spirale . Plus précisément, il existe un unique point K pour lequel il existe une similarité spirale (composition d'une rotation et d'une homothétie, tous deux de centre R) envoyant B sur A et envoyant A sur C. En particulier, les triangles BAK et ACK sont similaires. Il s'agit du K qui apparaît dans la méthode 1. Il faut ensuite montrer que K est sur Γ et sur Ω et que K est sur le segment ST.

Méthode 2: Soit α, β, et γ les angles de ABC en A, B et C respectivement. Sans perte de généralité, supposons que $\beta \geq \gamma$ et que le cercle circonscrit de ABC a un rayon de longueur 1. Soit x le rayon de Γ, X le centre de Γ et Y le cercle circonscrit du triangle BOC. Soit Z le point (outre A) où Γ croise la hauteur issue de A dans le triangle ABC.

On va montrer que $XY = x + OY$, ce qui implique que Γ est tangent au cercle circonscrit de BOC.

Puisque $\angle APZ = \angle AQZ = 90^\circ$, on a $AP = 2x\cos\angle PAZ = 2x\cos\left(\frac{\pi}{2} - \beta\right) = 2x\sin\beta$. De la même manière, $AQ = 2x\sin\gamma$. De $BP/AP = AQ/CQ$, on trouve que $BP/AB = AQ/AC$, et donc que $AP/AB + AQ/AC = 1$. Puisque le cercle circonscrit de ABC a rayon 1, la loi du Sinus nous donne

$$\frac{2x\sin\beta}{2\sin\gamma} + \frac{2x\sin\gamma}{2\sin\beta} \;=\; 1\,, \quad \text{ce qui implique que} \quad x \;=\; \frac{\sin\beta\,\sin\gamma}{\sin^2\beta + \sin^2\gamma}\,.$$

Comme $\angle YOC = \angle YCO = \frac{1}{2}\angle BOC = \alpha$, on a $\cos\alpha = (OC/2)/OY = 1/2OY$. De plus, $\angle XAO = \angle BAO - \angle PAZ = \frac{1}{2}(\pi - \angle AOB) - (\frac{\pi}{2} - \beta) = \beta - \gamma$. Ensuite, puisque $AZ \parallel OY$,

$$\begin{aligned} XY^2 &= (OY + AO\cos\angle XAO - x)^2 + (AO\sin\angle XAO)^2 \\ &= \left(\frac{1}{2\cos\alpha} + \cos(\beta-\gamma) - x\right)^2 + \sin^2(\beta-\gamma). \end{aligned}$$

Conséquemment, on a les équivalences suivantes:

$$\begin{aligned} & & x + OY &= XY \\ &\iff & \left(x + \frac{1}{2\cos\alpha}\right)^2 &= \left(\frac{1}{2\cos\alpha} + \cos(\beta-\gamma) - x\right)^2 + \sin^2(\beta-\gamma) \\ &\iff & x^2 + \frac{x}{\cos\alpha} + \frac{1}{4\cos^2\alpha} &= \frac{1}{4\cos^2\alpha} + \cos^2(\beta-\gamma) + x^2 + \sin^2(\beta-\gamma) \\ & & &\quad + 2\left(\frac{\cos(\beta-\gamma)}{2\cos\alpha} - x\cos(\beta-\gamma) - \frac{x}{2\cos\alpha}\right) \\ &\iff & \frac{2x}{\cos\alpha} &= 1 + \frac{\cos(\beta-\gamma)}{\cos\alpha} - 2x\cos(\beta-\gamma) \\ &\iff & 2x(1+\cos\alpha\cos(\beta-\gamma)) &= \cos\alpha + \cos(\beta-\gamma). \end{aligned}$$

Maintenant, comme $\alpha+\beta+\gamma = \pi$, on a

$$\cos\alpha + \cos(\beta-\gamma) = 2\cos\left(\frac{\alpha+\beta-\gamma}{2}\right)\cos\left(\frac{\alpha-\beta+\gamma}{2}\right) = 2\cos\left(\frac{\pi}{2}-\gamma\right)\cos\left(\frac{\pi}{2}-\beta\right).$$

En utilisant cette équation et notre valeur préalablement trouvée pour x, on obtient

$$\begin{aligned} & & x + OY &= XY \\ &\iff & \frac{2\sin\beta\,\sin\gamma}{\sin^2\beta + \sin^2\gamma}(1+\cos\alpha\,\cos(\beta-\gamma)) &= 2\sin\gamma\,\sin\beta \\ &\iff & 1+\cos\alpha\,\cos(\beta-\gamma) &= \sin^2\beta + \sin^2\gamma\,. \end{aligned}$$

Finalement,

$$\begin{aligned} 1+\cos\alpha\,\cos(\beta-\gamma) &= 1 + \frac{1}{2}(\cos(\alpha-\beta+\gamma) + \cos(\alpha+\beta-\gamma)) \\ &= 1 + \frac{1}{2}(\cos(\pi-2\beta) + \cos(\pi-2\gamma)) \\ &= 1 - \frac{1}{2}(\cos(2\beta) + \cos(2\gamma)) \\ &= 1 - \frac{1}{2}(1 - 2\sin^2\beta + 1 - 2\sin^2\gamma) \\ &= \sin^2\beta + \sin^2\gamma\,, \end{aligned}$$

ce qui démontre le résultat. □

Problème 5. *Soit p un nombre premier pour lequel $\frac{p-1}{2}$ est aussi premier et posons a, b, c des entiers qui ne sont pas divisibles par p. Montrez qu'il y a au plus $1+\sqrt{2p}$ entiers strictement positifs n tels que $n < p$ et que p divise $a^n + b^n + c^n$.*

Solution. Soit I l'ensemble $\{1, 2, \dots, p-1\}$. Pour chaque entier m qui n'est pas divisible par p, on écrit m^{-1} pour identifier l'unique entier d dans I tel que $md \equiv 1 \pmod{p}$.

Supposons premièrement que $b \equiv \pm a \pmod{p}$ et $c \equiv \pm b \pmod{p}$. Ainsi, pour tout n, on a que $a^n + b^n + c^n \equiv \pm a^n$ ou $\pm 3a^n \pmod{p}$. Donc $p \neq 3$ (puisque $\frac{3-1}{2}$ n'est pas premier) et $p \not| a$, alors $a^n + b^n + c^n \not\equiv 0 \pmod{p}$ et l'affirmation est triviale dans ce cas. Sinon, on suppose sans perte de généralité que $b \not\equiv \pm a \pmod{p}$. Ainsi, en définissant $w = ab^{-1}$, on voit que $w \not\equiv \pm 1 \pmod{p}$.

Posons maintenant $q = \frac{p-1}{2}$. Par le petit théorème de Fermat, on sait que l'ordre de w mod p divise $p - 1 = 2q$. Par contre, comme $w \not\equiv \pm 1 \pmod{p}$, l'ordre de w ne divise pas 2. Ainsi, l'ordre doit être q ou $2q$.

Soit $A \equiv ac^{-1} \pmod{p}$ et $B \equiv bc^{-1} \pmod{p}$. Alors $AB^{-1} \equiv w \pmod{p}$ et

$$a^n + b^n + c^n \equiv 0 \pmod{p} \Longleftrightarrow A^n + B^n + 1 \equiv 0 \pmod{p}.$$

Soit $S = \{n \in I \mid A^n + B^n + 1 \equiv 0 \pmod{p}\}$, et $k = |S|$. On veut obtenir une borne sur k en bornant $k^2 = |S \times S|$. Pour le faire, on fractionne $S \times S$ de la façon suivante. Pour chaque entier positif t inférieur à $2q = p - 1$, on pose

$$D_t \ = \ \{(i, j) \in S \times S \mid j - i \equiv t \pmod{2q}\}.$$

Ainsi, $S \times S$ est l'union des ensembles $D_0, D_1, \dots, D_{p-2}$. Pour chaque valeur de t, on a $|D_t| \leq k$ (puisque pour chaque $i \in I$, il y a exactement un $j \in I$ tel que $j - i \equiv t \pmod{2q}$). Par contre, on peut faire bien mieux pour plusieurs valeurs de t.

Lemme: Supposons que $1 \leq t \leq p-2$ et $t \neq q$. Alors l'ensemble D_t a une cardinalité d'au plus 2.

Preuve: Pour t comme demandé dans l'énoncé, prenons $(i, j) \in D_t$. Alors

$$A^i + B^i \equiv A^j + B^j \pmod{p}\,;$$
$$\therefore B^i(B^t - 1) \equiv A^i(1 - A^t) \pmod{p}.$$

(On a utilisé $x^{j-i} \equiv x^t \pmod{p}$ du petit théorème de Fermat.) Si $B^t \equiv 1 \pmod{p}$ alors on a aussi $A^t \equiv 1 \pmod{p}$ par la congruence donnée plus haut. Ainsi, $w^t = (AB^{-1})^t \equiv 1 \pmod{p}$. Par contre, l'ordre de w est q ou $2q$ et $q \not| t$, ce qui est impossible. Donc

$$w^i \ = \ A^i(B^{-1})^i \ \equiv \ \left(B^t - 1\right) \cdot \left(1 - A^t\right)^{-1} \pmod{p}.$$

Ainsi, t nous donne la valeur de $w^i \pmod{p}$. Puisque l'ordre de w est soit q ou $2q$, il y a au plus deux valeurs possibles pour i. Comme la valeur de j est déterminée par i et t, le Lemme est démontré. $\square$

À partir du Lemme et de la discussion qui le précède, on a

$$k^2 \;=\; |S \times S| \;=\; \sum_{t=0}^{p-2} |D_t| \;\leq\; k + k + 2(p-3)\,.$$

Il en suit que $(k-1)^2 \leq 2p-5$, et donc que $k \leq 1 + \sqrt{2p-5}$. $\square$