Contrôle 2

Calculatrice et documents sont interdits.
Tous les résultats doivent être correctement rédigés et rigoureusement justifiés.
Le barème est donné à titre indicatif : 7 - 7 - 8.

Triplets pythagoriciens

Un triplet (a, b, c) d'entiers naturels est dit pythagoricien s'il satisfait l'égalité $a^2 + b^2 = c^2$. *(Le nom vient du fait qu'un tel triplet correspond à un triangle rectangle dont les côtés ont des longueurs entières.)*
L'objectif de ce problème est de caractériser ces triplets. On notera P leur ensemble :

$$P = \{(a, b, c) \in \mathbf{N}^3 \mid a^2 + b^2 = c^2\}$$

Les trois parties peuvent être traitées indépendamment.

Partie 1 : paramétrisation rationnelle du cercle unité

On définit les ensembles

$$A = \{(x, y) \in \mathbf{R}^2 \mid x^2 + y^2 = 1 \text{ et } x \neq -1\} \quad \text{et} \quad B = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \ ; \ t \in \mathbf{R} \right\}.$$

1. Soit $t \in \mathbf{R}$. Représenter sur une même figure l'ensemble A et la droite D_t d'équation $y = tx + t$.
2. Soit $(x, y) \in A \cap D_t$. Montrer : $x^2 - 1 + t^2(x+1)^2 = 0$.
3. En déduire l'expression de x puis de y en fonction de t.
   Factoriser l'expression précédente par $x + 1$ pour simplifier le calcul.
4. Montrer que $A = B$.
   Rédiger la preuve sans refaire les calculs déjà faits dans les questions précédentes. Ne pas oublier la condition « $x \neq -1$ ».
5. Représenter précisément sur votre figure les points obtenus pour $t \in \{-1, 0, \frac{1}{2}, 1, 2, 3\}$.

Partie 2 : congruences

On s'intéresse ici à des conditions de divisibilité des triplets pythagoriciens.

1. Montrer que si $(a, b, c) \in P$, alors a, b ou c est pair.
2. Dresser la table des carrés modulo 3.
3. En déduire que si $\bar{a}$, $\bar{b}$ et $\bar{c}$ sont non nuls dans $\mathbf{Z}/3\mathbf{Z}$, alors $a^2 + b^2 \neq c^2$.
   Conclure que si $(a, b, c) \in P$, alors l'un des trois entiers est divisible par 3.
4. Dresser de même la table des carrés dans $\mathbf{Z}/5\mathbf{Z}$ et en déduire que si $(a, b, c) \in P$, alors a, b ou c est divisible par 5.
5. Dresser enfin la table des carrés dans $\mathbf{Z}/8\mathbf{Z}$ et en déduire que si $(a, b, c) \in P$, alors a, b ou c est divisible par 4.

Partie 3 : paramétrisation des triplets pythagoriciens

L'objectif de cette partie est d'obtenir une paramétrisation de l'ensemble P et ainsi pouvoir déterminer tous les triplets pythagoriciens.
Dans toute cette partie, on considère un triplet $(a, b, c) \in P$ avec $c \neq 0$.

1. Montrer que $(\frac{a}{c}, \frac{b}{c})$ appartient à l'ensemble A défini dans la partie 1.

   On en déduit, d'après la partie 1, qu'il existe $t \in \mathbf{R}$ tel que $(\frac{a}{c}, \frac{b}{c}) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Et on admet que ce nombre t est nécessairement un nombre rationnel.

2. En déduire qu'il existe des entiers p et q tels que :

$$\frac{a}{c} = \frac{q^2 - p^2}{q^2 + p^2} \qquad \text{et} \qquad \frac{b}{c} = \frac{2pq}{q^2 + p^2}.$$

   On souhaiterait identifier les numérateurs et dénominateurs dans ces égalités. Pour que cela soit possible, il faut préciser nos hypothèses : on suppose que p et q sont premiers entre eux et on considère le cas où l'un est pair et l'autre impair.

3. Montrer que $q^2 + p^2$ est impair.
4. Démontrer : $\forall d \in \mathbf{N}, \quad [\ d|(q^2+p^2) \text{ et } d|(q^2-p^2)\ ] \implies [\ d|q^2 \text{ et } d|p^2\ ]$.
   En déduire que $q^2 + p^2$ et $q^2 - p^2$ sont premiers entre eux.

   On admet que de même, $2pq$ et $q^2 + p^2$ sont premiers entre eux.

5. Déduire de tout cela que si a et b sont premiers avec c, alors

$$a = q^2 - p^2, \qquad b = 2pq, \qquad c = q^2 + p^2.$$

6. Réciproquement, vérifier que pour tous entiers p et q tels que $q > p > 0$, le triplet ci-dessus est bien pythagoricien.
7. Donner ainsi trois exemples différents de triplets pythagoriciens (a, b, c), et constater que les conditions obtenues dans la partie 2 sont bien satisfaites.

La preuve ci-dessus est incomplète. En particulier, les triplets que nous avons réussi à paramétrer sont ceux pour lesquels a est impair et premier avec c. Pour conclure, il faudrait justifier les points admis et traiter le cas où p et q sont tous les deux impairs. Mais les idées principales sont bien là.