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 :

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

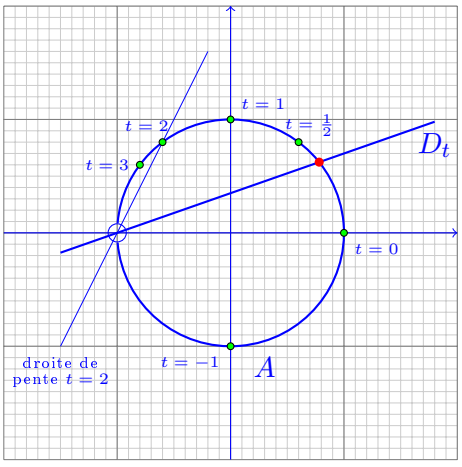
Les trois parties peuvent être traitées indépendamment.

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 : $x^2 - 1 + t^2(x + 1)^2 = 0$.

   Comme $(x, y) \in A$, $x \neq -1$ et $x^2 + y^2 = 1$. D'autre part, $(x, y) \in D_t$, donc $y = tx + t$. Ainsi $x^2 + (tx + t)^2 = 1$, donc $x^2 - 1 + t^2(x + 1)^2 = 0$.

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.

Factorisons par $x+1$: $x^2-1+t^2(x+1)^2 = (x+1)(x-1)+t^2(x+1)^2 = (x+1)(x-1+t^2(x+1)) = 0$. Or $x \neq -1$ et nous pouvons simplifier par $x+1$: $x-1+t^2x+t^2 = 0$, donc $x = \frac{1-t^2}{1+t^2}$.
Enfin $y = tx+t = \frac{t-t^3}{1+t^2}+t = \frac{2t}{1+t^2}$.

4. Montrer que $A = B$.
Rédiger la preuve sans refaire les calculs déjà faits dans les questions précédentes. Ne pas oublier la condition « $x \neq -1$ ».

Montrons que $B \subset A$: Soit $t \in \mathbf{R}$ et posons $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \in B$. Si $\frac{1-t^2}{1+t^2} = -1$, on déduit $1 = -1$. Donc $x \neq -1$.
De plus $x^2+y^2 = \frac{(1-t^2)^2}{(1+t^2)^2} + \frac{4t^2}{(1+t^2)^2} = \frac{t^4+2t^2+1}{(1+t^2)^2} = 1$. Donc $(x,y) \in A$.

Montrons que $A \subset B$: soit $(x,y) \in A$. Alors $x \neq -1$ et $x^2+y^2 = 1$. Posons $t = \frac{y}{x+1}$. Alors $y = tx+t$ et on retrouve les conditions des questions précédentes. Nous avons alors montré que $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Donc $(x,y) \in B$.

Remarque : nous aurions pu résoudre le système de la question 2 par équivalence et montrer rigoureusement l'équivalence :

$$(x,y) \in A \cap D_t \text{ ssi } (x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

Cela nous aurait permis d'éviter la vérification dans la partie « $B \subset A$ ».

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.

Soit $(a,b,c) \in \mathbf{N}^3$. Supposons que a, b et c sont tous les trois impairs. Alors a^2, b^2 et c^2 sont aussi impairs. Donc a^2+b^2 est pair. Ainsi $a^2+b^2 \neq c^2$. Par contraposée, cela démontre que si $a^2+b^2 = c^2$, alors a, b ou c est pair.

2. Dresser la table des carrés modulo 3.

Dans $\mathbf{Z}/3\mathbf{Z}$:

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{a}^2$	$\bar{0}$	$\bar{1}$	$\bar{1}$

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.

D'après le tableau, si $\bar{a} \neq \bar{0}$, alors $\bar{a}^2 = \bar{1}$. Il en est évidemment de même pour $\bar{b}$ et $\bar{c}$. Donc si les trois sont non nuls dans $\mathbf{Z}/3\mathbf{Z}$, alors $\bar{a}^2+\bar{b}^2 = \bar{2}$ et $\bar{c}^2 = \bar{1}$, donc $\bar{a}^2+\bar{b}^2 \neq \bar{c}^2$. Par contraposée, si $(a,b,c) \in P$, alors $a^2+b^2 = c^2$, donc dans $\mathbf{Z}/3\mathbf{Z}$, $\bar{a}^2+\bar{b}^2 = \bar{c}^2$ et donc $\bar{a}$, $\bar{b}$ ou $\bar{c}$ est nul. Cela signifie exactement que a, b ou c 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.

   Dans $\mathbf{Z}/5\mathbf{Z}$:

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{a}^2$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{1}$

   Si $\bar{a}$, $\bar{b}$ et $\bar{c}$ sont non nuls, alors d'après le tableau $\bar{a}^2+\bar{b}^2 \in \{\bar{1}+\bar{1}, \bar{1}+\bar{4}, \bar{4}+\bar{4}\} = \{\bar{2}, \bar{0}, \bar{3}\}$ et $\bar{c}^2 \in \{\bar{1}, \bar{4}\}$. Donc $\bar{a}^2+\bar{b}^2 \neq \bar{c}^2$. Le même raisonnement que précédemment permet de conclure 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.

   Dans $\mathbf{Z}/8\mathbf{Z}$:

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{a}^2$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$

   Les seuls carrés non nuls sont $\bar{1}$ et $\bar{4}$. Avec ces deux seuls nombres, il est impossible d'obtenir $\bar{a}^2+\bar{b}^2=\bar{c}^2$ car $\bar{1}+\bar{1}$, $\bar{1}+\bar{4}$ et $\bar{4}+\bar{4}$ ne sont égaux ni à $\bar{1}$, ni à $\bar{4}$. Donc si $(a,b,c) \in P$, alors l'un des trois carrés est nul modulo 8. D'après le tableau cela signifie que l'un des trois entiers est égal à 0 ou 4 modulo 8. Cela signifie exactement que cet entier 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.

   Comme $(a,b,c) \in P$, alors $a^2+b^2=c^2$. Donc $\frac{a^2}{c^2}+\frac{b^2}{c^2}=1$, *i.e.* $\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$. De plus, a et c sont positifs par hypothèse, donc $\frac{a}{c} \neq -1$. Par définition de A, on déduit que $(\frac{a}{c}, \frac{b}{c}) \in A$.

   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 :

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

   D'après la paramétrisation de A, on déduit en effet qu'il existe $t \in \mathbf{R}$ tel que $(\frac{a}{c}, \frac{b}{c}) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Plus précisément, on sait que le paramètre t est égal à « $\frac{y}{x+1}$ »= $\frac{b/c}{a/c+1}$.
   Comme a, b et c sont des entiers, on constate bien que t est un nombre rationnel.

   Récrivons-le sous la forme $t=\frac{p}{q}$ avec p et q entiers. Alors $\frac{a}{c} = \frac{1-t^2}{1+t^2} = \frac{1-\frac{p^2}{q^2}}{1+\frac{p^2}{q^2}} = \frac{q^2-p^2}{q^2+p^2}$ et $\frac{b}{c} = \frac{2\frac{p}{q}}{1+\frac{p^2}{q^2}} = \frac{2pq}{q^2+p^2}$.

   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.

   Remarque : lorsqu'on a posé $t=\frac{p}{q}$, nous pouvions parfaitement imposer à cette fraction d'être irréductible. Supposer que p et q sont premiers entre eux ne restreint donc en rien notre raisonnement. Cela implique en particulier que p et q ne peuvent pas être tous les deux pairs. Ils peuvent être tous les deux impairs ou de parité différente. C'est cette seconde hypothèse que nous imposons pour la suite.
   Dans ce cas p^2 et q^2 ayant les mêmes parités que p et q sont eux aussi de parité différente. Donc p^2+q^2 est impair.

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

   Soit $d \in \mathbf{N}$ et supposons que $d|(q^2+p^2)$ et $d|(q^2-p^2)$. Alors d divise leur somme, donc $d|2q^2$. Or q^2+p^2 est impair et divisible par d, donc d ne peut pas être pair. D'après le

lemme de Gauss, on déduit que $d|q^2$. De même, d divise aussi la différence de (q^2+p^2) et (q^2-p^2), donc $d|2p^2$. Le même raisonnement permet de conclure que $d|p^2$.
Or on sait que p et q sont premiers entre eux. Il en est donc de même pour p^2 et q^2 (cela se justifie en raisonnant sur les facteurs premiers de p et q). Le seul diviseur commun à p^2 et q^2 est donc 1, et d'après ce qui précède, il en est de même pour q^2+p^2 et q^2-p^2. Donc ces deux nombres sont premiers entre eux.

Pour $2pq$ et q^2+p^2, le raisonnement est analogue. Supposons par l'absurde qu'il existe un nombre premier d qui divise ces deux nombres. Comme q^2+p^2 est impair, $d \neq 2$. Donc $d|pq$ et d'après le lemme d'Euclide, $d|p$ ou $d|q$. Mais comme d divise aussi p^2+q^2, on peut en déduire que d divise p et q, ce qui est impossible par hypothèse. Donc $2pq$ et q^2+p^2 n'ont aucun facteur premier en commun et sont donc 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

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

Si a et c sont premiers entre eux, alors la fraction $\frac{a}{c}$ est irréductible. Et d'après la question précédente, $\frac{q^2-p^2}{q^2+p^2}$ est également irréductible. Comme ces deux fractions sont égales, on déduit $a = q^2 - p^2$ et $c = q^2 + p^2$. On raisonne de même avec $\frac{b}{c}$ et si b est premier avec c, on conclut que $b = 2pq$.

6. Réciproquement, vérifier que pour tous entiers p et q tels que $q>p>0$, le triplet ci-dessus est bien pythagoricien.

Soient p et q des entiers tels que $q > p > 0$, et posons $(a, b, c) = (q^2 - p^2, 2pq, q^2 + p^2)$. Alors

$$a^2 + b^2 = (q^2 - p^2) + (2pq)^2 = q^4 + 2p^2q^2 + p^4 = (q^2 + p^2)^2 = c^2.$$

Donc $(a, b, c) \in P$.

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.

Prenons des couples (p, q) d'entiers premiers entre eux et de parité différente.
Avec $(p, q) = (1, 2)$, on obtient $(a, b, c) = (3, 4, 5)$.
Avec $(p, q) = (1, 4)$, on obtient $(a, b, c) = (15, 8, 17)$.
Avec $(p, q) = (2, 3)$, on obtient $(a, b, c) = (5, 12, 13)$.
Avec $(p, q) = (3, 4)$, on obtient $(a, b, c) = (7, 24, 25)$.
On constate bien sur ces trois exemples qu'il y a à chaque fois un multiple de 3, un multiple de 4 et un multiple de 5 (ces conditions peuvent être satisfaites par un même nombre).

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.