Devoir maison n° 1
Triplets pythagoriciens

—

Arithmétique, groupe et géométrie

La clarté des raisonnements et la qualité de la rédaction interviendront pour une part importante dans l'appréciation des copies.

Il s'agit dans ce devoir de déterminer l'ensemble solution de l'équation diophantienne

$$x^2 + y^2 = z^2. \tag{1}$$

Un triplet $(a, b, c) \in \mathbb{N}^3$ solution de cette équation est appelé *triplet pythagoricien.*

1 Préliminaires

i) Soit $(a, b, c) \in \mathbb{N}^{*3}$ un triplet solution de (1). Montrer que l'on peut supposer a, b et c premiers entre eux, puis premiers deux à deux, ce que l'on supposera dans la suite de ce devoir.
Nous noterons $\mathcal{S}$ l'ensemble des solutions entières de (1) constituées de tels triplets.

ii) Montrer qu'il n'existe aucune solution de la forme $(a, b, 0)$ autre que $(0, 0, 0)$;

iii) Soit $\mathbb{S}^1$ le cercle unité. Établir une bijection entre $\mathcal{S} - \{(0, 0, 0)\}$ et l'ensemble des points à coordonnées rationnelles de $\mathbb{S}^1 - \{(0, \pm 1), (\pm 1, 0)\}$.

2 Géométrie : points rationnels du cercle

On se propose dans cette partie de déterminer l'ensemble des points du cercle à coordonnées rationnelles. Considérons la droite D_t passant par les points $(-1, 0)$ et $(0, t)$, ainsi que son second point d'intersection P_t avec le cercle unité $\mathbb{S}^1$.

i) Faire une figure ;

ii) Donner une équation de D_t sous forme paramétrique ainsi qu'une équation cartésienne de $\mathbb{S}^1$;

iii) En déduire les coordonnées du point $P_t = D_t \cap \mathbb{S}^1$ ainsi qu'une paramétrisation du cercle $\phi : \mathbb{R} \to \mathbb{S}^1$, $t \mapsto (x(t), y(t))$;

iv) Montrer que la paramétrisation précédente établit une bijection entre les paramètres $t \in \mathbb{Q}$ et les points à coordonnées rationnelles de $\mathbb{S}^1 - \{(-1, 0)\}$;

v) En déduire une bijection entre les points rationnels de $\mathbb{S}^1 - \{(\pm 1, 0), (0, \pm 1)\}$ et $\mathcal{S} - \{(0, 0, 0)\}$.

3 Loi de groupe sur $\mathbb{S}^1$

On se propose dans cette partie de munir l'ensemble solution $\mathcal{S}$ d'une structure de groupe abélien.

i) Posant $t = \tan(\theta/2)$ dans la paramétrisation ϕ précédente, donner une nouvelle paramétrisation de $\mathbb{S}^1$ en fonction de θ ;

ii) À partir de la question précédente, définir une loi de composition interne $\star$ sur les points de coordonnées rationnelles de $\mathbb{S}^1$. Pour P et Q deux points de $\mathbb{S}^1$, exprimer $P \star Q$;

iii) En déduire que $\mathcal{S}$ admet une structure de groupe abélien.

4 Arithmétique : solutions explicites

On se propose ici d'identifier la forme des solutions en utilisant le résultat de la première partie. Considérons un triplet $(a, b, c) \in \mathbb{N}^{*3}$ solution de (1).

i) Montrer que a et b sont de parité différente (on pourra raisonner sur la classe de congruence modulo 4 des solutions). On supposera par la suite que a est impaire ;

ii) En utilisant le résultat de la partie 2, montrer qu'il existe m et n entiers premiers entre eux tels que
$$\frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2} \qquad \frac{b}{c} = \frac{2nm}{n^2 + m^2};$$

iii) Expliquer pourquoi il existe $\lambda \in \mathbb{N}^*$ vérifiant
$$\begin{cases} \lambda a = n^2 - m^2 \\ \lambda b = 2nm \\ \lambda c = n^2 + m^2 \end{cases}$$

   (a) Montrer que si λ divise $n^2 - m^2$ et $n^2 + m^2$, alors $\lambda \in \{1, 2\}$;

   (b) Vérifier que si $\lambda = 2$, alors $n^2 - m^2 = 2$ [4] ;

   (c) En raisonnant sur les classes modula 4 de n et de m, en déduire que $\lambda = 1$.

iv) En déduire l'expression de (a, b, c) et vérifier que de telles expressions sont bien solutions de (1). Conclure.