Devoir à rendre le 27 octobre

Le but principal de ce problème est de caractériser les entiers qui peuvent s'écrire comme somme de deux carrés *entiers*.
Dans la partie II, on montre, en utilisant un peu de géométrie et d'arithmétique, que le problème se ramène à obtenir une décomposition en somme de deux carrés *rationnels*.
La partie III permet de caractériser les nombres premiers qui s'écrivent comme somme de deux carrés entiers.
Enfin, dans la partie IV, on obtient une caractérisation pour tous les entiers.
La partie V concerne l'étude des sommes de quatre carrés. En particulier, on démontre, en généralisant les techniques de la partie III, que tout entier naturel est une somme de quatre carrés entiers (théorème de Lagrange).

I. Préliminaires

1. Soit $p = 2n + 1$ un nombre impair.
Établir que $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$) si et seulement si n est pair (resp. n est impair).

2. Montrer qu'un nombre de la forme $4m + 3$ ne peut pas s'écrire comme une somme de deux carrés entiers.

3. Soit $N_1 = a_1^2 + b_1^2$ et $N_2 = a_2^2 + b_2^2$ deux nombres qui admettent une décomposition en somme de deux carrés entiers. Montrer que le produit $N_1 N_2$ peut aussi s'écrire comme la somme de deux carrés entiers.
(Indication : écrire $a^2 + b^2 = |a + ib|^2$).

4. Montrer qu'il existe une infinité de nombres premiers de la forme $4m + 3$.
(Indication : si $p_1, p_2, \ldots, p_k$ sont les nombres premiers $\equiv 3 \pmod 4$, considérer le nombre $2p_1p_2 \ldots p_k + 1$).

II. Un peu de géométrie

Dans cette partie, on considère le plan affine euclidien $\mathbb{R}^2$ muni de sa distance usuelle. On désigne par $d(A, B)$ la distance entre les points A et B de $\mathbb{R}^2$. On dit qu'un point $A = (x, y)$ est un point entier (resp. rationnel) si ses coordonnées x et y sont toutes les deux entières (resp. rationnelles). Enfin N est un entier strictement positif.

1. Soit $A = (x, y)$ un point du plan $\mathbb{R}^2$, montrer qu'il existe un point entier $A' = (x', y')$ tel que $d(A, A') < 1$.

Soit $(\mathcal{C})$ le cercle d'équation $x^2 + y^2 = N$. On suppose qu'il existe un point rationnel mais pas entier $A_0 = (x_0, y_0)$ appartenant à $(\mathcal{C})$.

2. Montrer que l'on peut écrire A_0 sous la forme $A_0 = (\frac{m}{d}, \frac{n}{d})$ avec d, m et n entiers et $d \geq 2$.

3. Soit $B = (a, b)$ un point entier de $\mathbb{R}^2$ tel que $d(B, A_0) < 1$. Vérifier que l'équation paramétrique de la droite (D) passant par A_0 et B s'écrit :

$$\begin{cases} x &= a + t\left(\frac{m}{d} - a\right) \\ y &= b + t\left(\frac{n}{d} - b\right) \end{cases} \quad \text{avec } t \in \mathbb{R} \, .$$

4. En déduire que les points d'intersection de la droite (D) avec le cercle $(\mathcal{C})$ sont donnés pour les valeurs de t vérifiant l'équation suivante :

$$d(B, A_0)^2 t^2 + Qt + (a^2 + b^2 - N) = 0 \qquad (*) \ ,$$

où Q est un nombre rationnel à déterminer.

5. Montrer que l'équation $(*)$ est une équation de degré deux dont les solutions sont $t = 1$ et $t = \frac{M}{d(B,A_0)^2}$, où M est un entier que l'on déterminera.

6. Montrer que le nombre $d(A_0, B)^2$ est un nombre rationnel que l'on peut écrire sous la forme $\frac{d_1}{d}$ avec d_1 entier et $0 < d_1 < d$.

7. En déduire que le cercle $(\mathcal{C})$ contient un point rationnel A_1 qui s'écrit sous la forme $A_1 = (\frac{m_1}{d_1}, \frac{n_1}{d_1})$ avec $m_1, \ n_1 \in \mathbb{Z}$.

8. Déduire de ce qui précède que le cercle d'équation $x^2 + y^2 = N$ (qui contient un point rationnel) contient aussi par un point entier.

9. Conclure : si N peut s'écrire comme la somme de deux carrés rationnels, il peut s'écrire comme la somme de deux carrés entiers.

III. Arithmétique

1. Soit $p \geq 2$ un nombre premier, montrer que les propositions suivantes sont équivalentes :

(i) Le nombre p divise une somme de deux carrés entiers $a^2 + b^2$ avec $b = 1$

(ii) Le nombre p divise une somme de deux carrés entiers $a^2 + b^2$ avec a et b premiers entre eux.

(iii) Le nombre p divise une somme de deux carrés entiers $a^2 + b^2$ avec a et b non multiples de p.

2. Soit p un nombre premier de la forme $4m + 1$.
Montrer, en calculant $(4m)!$ (mod p) de deux façons différentes, que p vérifie la condition (i) de la question précédente.
(Indication : pour une des deux façons, on pourra regrouper, dans $(4m)!$, les termes x et $p - x$).

3. Ainsi, si p est un nombre premier de la forme $4m + 1$ alors -1 est un carré (mod p).

4. Soit $N = a^2 + b^2$ une somme de deux carrés entiers avec a et b premiers entre eux et soit p un nombre premier divisant N. Montrer que p est soit 2, soit de la forme $4m + 1$.
(Indication : par l'absurde, en supposant que N est divisible par un nombre premier de la forme $2n + 1$ avec n impair).

5. Soit p un nombre premier de la forme $4m + 3$, montrer que -1 n'est pas un carré modulo p.

6. Montrer qu'il existe une infinité de nombres premiers de la forme $4m + 1$.
(Indication : par l'absurde, si p_1, p_2 ... p_k sont les nombres premiers de la forme $4m + 1$, considérer le nombre $(2p_1p_2 \dots p_r)^2 + 1$ et utiliser la question 4).

7. Soit p un nombre premier de la forme $4m + 1$.

a. Montrer que p divise un nombre N de la forme $a^2 + b^2$ avec a et b premiers entre eux et $0 < N < p^2$.

b. Remarquer que N/p est un entier strictement plus petit que p. Que peut-on dire des diviseurs premiers de N/p ?

8. Montrer par récurrence sur p que tout nombre premier p de la forme $4m + 1$ peut s'écrire comme la somme de deux carrés entiers.
(Indication : montrer, en utilisant l'hypothèse de récurrence, que p peut s'écrire sous la forme $p = \frac{a^2+b^2}{x^2+y^2}$. Remarquer alors que l'on a $p = \frac{(a^2+b^2)(x^2+y^2)}{(x^2+y^2)^2}$. En déduire que p est une somme de deux carrés rationnels et utiliser la question 9 de la partie précédente).

IV. Généralisation

Soit $N > 0$ un nombre entier.

1. Montrer que N s'écrit de façon unique $N = C^2M$ où C et M sont des entiers et M est sans facteurs carrés.

2. Montrer que le nombre C de la question précédente est le plus grand (au sens de la division) carré divisant N.

3. Montrer que si aucun diviseur premier de M n'est de la forme $4m + 3$, alors N peut s'écrire comme la somme de deux carrés entiers.

4. Réciproquement, montrer que si N peut s'écrire comme la somme de deux carrés entiers alors les diviseurs premiers de M ne sont pas de la forme $4m + 3$.
(Indication : se ramener aux conditions de la question 4 de la partie précédente).

5. Déduire de ce qui précède que les assertions suivantes sont équivalentes :

(i) Le nombre N est somme de deux carrés entiers.

(ii) Dans la décomposition de N en produit de facteurs premiers, l'exposant de tout facteur premier de la forme $4m + 3$ est pair.

V. Somme de quatre carrés

Le but de cette partie est de démontrer un théorème de Lagrange : tout entier naturel N peut s'écrire comme une somme de quatre carrés entiers.

1. Soient $(x_j)_{j=1,\ldots,4}$ et $(y_j)_{j=1,\ldots,4}$ huit nombres entiers (resp. rationnels), montrer l'égalité suivante :

$$\begin{aligned}&(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\ &(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2+ \\ &(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned}$$

et en déduire que l'on peut restreindre le problème aux nombres premiers > 0.

2. Soit p un nombre premier impair. Montrer qu'il existe un entier m, $0 < m < p$ tel que mp est une somme de trois carrés entiers.
(Indication : considérer les deux ensembles $A = \{x^2, x = 0, 1, \ldots, (p-1)/2\}$ et $B = \{-1 - x^2, x = 0, 1, \ldots, (p-1)/2\}$).

3. En déduire, par récurrence, que tout nombre premier $p > 0$ s'écrit comme une somme de quatre carrés rationnels.

On considère l'espace euclidien $\mathbb{R}^4$ muni da sa distance euclidienne usuelle. On désigne par $d(A, B)$ la distance entre les points A et B de $\mathbb{R}^4$. On dit qu'un point $A = (x, y, z, t)$ est un point entier (resp. rationnel) si ses coordonnées x, y, z et t sont toutes entières (resp. rationnelles). Enfin N est un entier strictement positif.

4. Soit $A = (x, y, z, t)$ un point de $\mathbb{R}^4$, démontrer qu'il existe un point entier $A' = (x', y', z', t')$ tel que $d(A, A') \leq 1$.

5. À quelle condition sur A, ne peut-on pas avoir $d(A, A') < 1$? Dans ce cas, montrer qu'il existe 16 points entiers A' tels que $d(A, A') = 1$. Montrer alors qu'il existe des points entiers $A' = (x', y', z', t')$ et $A'' = (x'', y'', z'', t'')$ tels que $d(A, A') = 1$, $x'^2 + y'^2 + z'^2 + t'^2 \equiv 1 \pmod 2$, $d(A, A'') = 1$ et $x''^2 + y''^2 + z''^2 + t''^2 \equiv 0 \pmod 2$.

6. Montrer le théorème d'Aubry : si la sphère $\mathcal{S}$ d'équation $X^2 + Y^2 + Z^2 + T^2 = N$ contient un point rationnel, alors elle contient un point entier.
(Indication : soit $P = (a_1/d, a_2/d, a_3/d, a_4/d) \in \mathcal{S} \cap \mathbb{Q}^4$, la droite passant par P et par le point entier le plus proche de P coupe la sphère $\mathcal{S}$ en un autre point rationnel dont on pourra étudier le dénominateur...).

7. Conclure : démontrer le théorème de Lagrange.