Devoir Maison 2 - Structures algébriques

L'objectif de ce devoir est de démontrer le résultat suivant :

Théorème. *Un nombre entier $n \geqslant 2$ s'écrit comme la somme de deux nombres au carré si et seulement si pour tout nombre premier p congru à $3 \mod 4$, la valuation p-adique de n est paire.*

Dans la suite, on notera Σ l'ensemble des entiers sommes de deux carrés :

$$\Sigma := \{n \in \mathbb{N},\ n = a^2 + b^2,\ a, b \in \mathbb{N}\}.$$

Question 1 : En admettant le théorème, dire quels sont les entiers entre 2 et 10 qui sont des sommes de deux carrés et, lorsque c'est le cas, donner une décomposition en somme de deux carrés. Le cercle centré en $(0, 0)$ de rayon $\sqrt{7}$ rencontre-t-il des points de coordonnées entières ?

Il est naturel d'aborder cette question à travers les entiers de Gauss, puisque la norme d'un élément de cet anneau est justement un élément de Σ.

Définition 1 (Entiers de Gauss)**.** Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss. On le munit de la norme définie par $N(a + ib) = a^2 + b^2$.

Question 2 :

i) Justifier (rapidement) que l'application N est une norme, qu'elle est multiplicative (c'est-à-dire que $N(zz') = N(z)N(z')$) et que l'anneau $\mathbb{Z}[i]$ est intègre.

ii) Montrer que $\mathbb{Z}[i]$ est euclidien (donc principal) pour le stathme N.

iii) Décrire les inversibles de $\mathbb{Z}[i]$ puis en déduire qu'un nombre premier $p \in \mathbb{Z}$ n'est pas nécessairement un élément premier (= irréductible puisque l'anneau est euclidien) dans l'anneau $\mathbb{Z}[i]$.

Commençons par nous convaincre que l'anneau $\mathbb{Z}[i]$ est pertinent dans l'étude de notre problème :

Question 3 : En utilisant la norme N, montrer que l'ensemble Σ est stable par multiplication interne.

Attaquons la démonstration à proprement parler. Comme souvent en arithmétique, on va résoudre le problème en regardant ce qui se passe modulo un nombre premier.

Question 4 : Démontrer le **lemme** suivant : Soit $p \in \mathbb{N}$ un nombre premier. Alors

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

On cherche à montrer mieux :

Proposition 2. *Soit $p \in \mathbb{N}$ un nombre premier. Alors :*

$$p \in \Sigma \iff p = 2 \text{ ou } p = 1 \mod 4.$$

Question 5 : Montrer le sens direct.

Question 6 : Montrons le sens réciproque.

i) Justifier qu'il suffit de montrer que l'anneau quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre pour conclure.

ii) Justifier soigneusement qu'on a l'isomorphisme suivant :

$$\mathbb{Z}[i]/(p) \simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}.$$

iii) En déduire que $p \in \Sigma$ si et seulement si -1 est un carré modulo p et conclure à l'aide d'un résultat déjà connu sur les carrés modulo p.

Passons au cas général. Pour $n \in \mathbb{N}$ et $p \in \mathbb{N}$ premier, on note $\nu_p(n)$ la valutation p-adique de n. Le théorème se reformule donc :

Théorème. *Soit $n \geqslant 2$. Alors*

$$n \in \Sigma \iff \nu_p(n) \text{ pair pour tout } p \text{ premier avec } p = 3 \mod 4.$$

Question 7 : Démontrer le théorème. (Indication : pour le sens réciproque, on pourra raisonner par récurrence sur $\nu_p(n)$.)

Pour conclure, donnons à l'aide de ce théorème une caractérisation des éléments irréductibles de $\mathbb{Z}[i]$:

Proposition 3. *Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :*
- *les entiers $n \in \mathbb{N}$ congrus à $3 \mod 4$.*
- *les $a + ib$ tels que $a^2 + b^2$ soit un nombre premier.*

Question 8 : Démontrer ce résultat (pour les cas où $a + ib$ n'est pas un entier on pourra, une fois de plus, raisonner avec la norme).