UPS. L3 Mathématiques Fondamentales. Algèbre. Devoire. 2009/2010

Sommes de deux carrés et entiers de Gauss.

Soit $Q \subset \mathbb{N}$ l'ensemble des entiers qui peuvent s'écrire comme somme de deux carrés $Q = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$.

---

1. Montrer que si $n \in Q$, alors $n \not\equiv 3 \mod 4$.

---

2. En utilisant $\mathbb{Z}[i]$, montrer que Q est stable par multiplication.

Par conséquent, on va essayer de répondre à la question : *Quels sont les nombres premiers qui s'écrivent comme somme de deux carrés ?* On a vu que si p est une somme de deux carrés, alors $p \not\equiv 3 \mod 4$, i.e. $p = 2$, ou $p \equiv 1 \mod 4$. On va démontrer la réciproque. Le chemin sera détourné, et fera de jolis détours par l'algèbre que vous venez d'apprendre.

Rappel : $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $d(a + bi) = a^2 + b^2$. Tout élément de $\mathbb{Z}[i]$ a donc une décomposition unique en produit de facteurs premiers dans $\mathbb{Z}[i]$. Mais attention, un nombre $p \in \mathbb{Z}$ qui est premier dans $\mathbb{Z}$ (5 par exemple) peut ne pas être premier dans $\mathbb{Z}[i]$ ($5 = (1 + 2i)(1 - 2i)$).

---

3. Montrer par contre que si $p \in \mathbb{Z}$ est premier dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}$.

---

4. Soit p un nombre premier de $\mathbb{Z}$. Montrer que si p n'est pas irreductible dans $\mathbb{Z}[i]$, alors p s'écrit $p = \pi\overline{\pi}$ avec π irréductible dans $\mathbb{Z}[i]$. *Indication :* soit π un facteur premier de p dans $\mathbb{Z}[i]$, et montrer que $\pi\overline{\pi}$ divise p. En déduire l'équivalence :
(i) p est une somme de deux carrés
(ii) p n'est pas premier dans $\mathbb{Z}[i]$

---

5. a. Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$ où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

b. En déduire que p est premier dans $\mathbb{Z}[i]$ si et seulement si $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$.

En déduire l'équivalence
(i) p est une somme de deux carrés
(ii) p n'est pas premier dans $\mathbb{Z}[i]$
(iii) -1 est un carré dans $\mathbb{F}_p$.

---

6. Soit G un groupe abélien fini d'ordre n. On note m l'exposant de G - le nombre minimal tel que $g^m = 1$ pour tout $g \in G$.

Rappel : D'après le théorème de structure, G est isomorphe au produit $(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_s\mathbb{Z})$ où $m_1|m_2|\ldots|m_s$.

a. Montrer que m divise n et que si $m = n$, alors G est cyclique (indication : utiliser le théorème de structure).

b. Montrer que le groupe $\mathbb{F}_p^*$ est cyclique (indication : combien de racine peut avoir le polynôm $X^m - 1$?)

---

7. On se demande donc pour quels nombres premier, -1 est un carré.

a. Quelle est la réponse pour $p = 3, 5, 7$?

b. On suppose p impair. Montrer que -1 est un carré dans $\mathbb{F}_p$ ssi le groupe $\mathbb{F}_p^*$ contient un élément d'ordre 4 (indication : montrer que -1 est le seul élément d'ordre 2 dans $\mathbb{F}_p^*$).

c. En utilisant le fait que $\mathbb{F}_p^*$ est un groupe *cyclique* d'ordre $p-1$, montrer que -1 est un carré mod p ssi $p = 2$ ou $p \equiv 1 \mod 4$.

En déduire l'équivalence
(i) p est une somme de deux carrés ;
(ii) p n'est pas premier dans $\mathbb{Z}[i]$;
(iii) -1 est un carré dans $\mathbb{F}_p$;
(iv) $p = 2$ ou $p \equiv 1 \mod 4$.

---

8. On retourne au problème initial. Soit $n \in \mathbb{N}$. Montrer que $n \in Q$ si et seulement si, dans sa décomposition en facteurs premiers (dans $\mathbb{Z}$) $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, les puissances des facteurs premiers égaux à $3 \mod 4$ sont paires.

En déduire que $4410 = 2{\times}9{\times}5{\times}49$ est une somme de deux carrés (lesquels ?), alors que $924 = 4 \times 3 \times 7 \times 11$ ne l'est pas.