

DM 9 - Sommes de deux carrés – Ordres dans un groupe

Les parties 1.4 et 2.2 sont facultatives.

1 Entiers de Gauss et sommes de deux carrés

Dans ce problème, on étudie l'anneau $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ des entiers de Gauss. En guise d'application, on caractérise l'ensemble Σ des entiers naturels qui s'écrivent comme somme de deux carrés d'entiers. On adopte les définitions suivantes :

- Si a et b sont des éléments de $\mathbb{Z}[i]$, on dit que a divise b s'il existe $c \in \mathbb{Z}[i]$ tel que $b = ac$.
- Un élément $a \in \mathbb{Z}[i]$ est irréductible s'il n'est pas inversible et si, dans une décomposition $a = bc$, avec $b, c \in \mathbb{Z}[i]$, b ou c est un inversible de $\mathbb{Z}[i]$.

Pour tout $z \in \mathbb{Z}[i]$, on note $N(z) = |z|^2$.

1.1 $\mathbb{Z}[i]$ est un anneau euclidien.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} .
2. Montrer que $\forall z, z' \in \mathbb{Z}[i], N(zz') = N(z)N(z')$.
3. Soit $z \in \mathbb{Z}[i]$. Montrer que z est inversible dans $\mathbb{Z}[i]$ ssi $N(z) = 1$.
En déduire les inversibles de $\mathbb{Z}[i]$.
4. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien, de stathme N , au sens suivant :

$$\forall a \in \mathbb{Z}[i], \forall b \in \mathbb{Z}[i] - \{0\}, \exists (q, r) \in \mathbb{Z}[i]^2 : a = bq + r \text{ et } N(r) < N(b).$$

Considérer pour q un élément de $\mathbb{Z}[i]$ proche de $\frac{a}{b} \in \mathbb{C}$.

5. Y a-t-il unicité du couple (q, r) en général ?

1.2 Lemme d'Euclide dans $\mathbb{Z}[i]$

Soit a un irréductible de $\mathbb{Z}[i]$, soient $x, y \in \mathbb{Z}[i]$. On suppose que a divise xy et on cherche à montrer que a divise x ou a divise y . On suppose que a ne divise pas x et on note

$$I = a\mathbb{Z}[i] + x\mathbb{Z}[i] = \{au + xv, (u, v) \in \mathbb{Z}[i]^2\}.$$

6. Montrer qu'il existe $d \in I - \{0\}$ tel que $N(d) = \min \{N(z), z \in I - \{0\}\}$.
7. Montrer que d divise a ; en déduire que d est un inversible de $\mathbb{Z}[i]$, puis que a divise y .

1.3 Nombres premiers sommes de deux carrés

Dans cette partie, on montre qu'un nombre premier impair p est somme de deux carrés d'entiers ssi il est congru à 1 modulo 4.

8. On suppose que p est congru à 3 modulo 4. Montrer que p n'est pas somme de deux carrés d'entiers.

On suppose désormais que p est congru à 1 modulo 4. On sait¹ qu'on peut trouver $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 [p]$. Dans $\mathbb{Z}[i]$, on a la décomposition $x^2 + 1 = (x - i)(x + i)$.

9. Montrer que, dans $\mathbb{Z}[i]$, p divise $x^2 + 1$, mais qu'il ne divise ni $x + i$, ni $x - i$.
10. En déduire qu'il existe $b, c \in \mathbb{Z}[i]$, non inversibles, tels que $p = bc$.
11. Montrer que $N(b) = p$. En déduire que p est somme de deux carrés d'entiers.

1.4 Théorème de Fermat de Noël

Notons $\Sigma = \{n \geq 1 \mid \exists (a, b) \in \mathbb{N}^2 : n = a^2 + b^2\}$. Dans cette partie, on montre que pour tout entier $n \geq 1$, n appartient à Σ ssi pour tout premier p congru à 3 modulo 4, $v_p(n)$ est pair.²

12. Soit $n \geq 1$. Montrer que $n \in \Sigma$ ssi il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$.
13. En déduire que si $u, v \in \Sigma$, alors $uv \in \Sigma$.
14. En déduire que si pour tout premier p congru à 3 modulo 4, $v_p(n)$ est pair, alors $n \in \Sigma$.

Pour la réciproque, on fixe un nombre premier p congru à 3 modulo 4.

15. Soient u, v deux entiers. Montrer que $u^2 + v^2$ divise $u^{p-1} + v^{p-1}$.
16. En déduire que p divise $u^2 + v^2$ ssi p divise u et p divise v .
17. **Conclusion :** Soit $n \in \Sigma$. On écrit $n = a^2 + b^2$, avec $(a, b) \in \mathbb{N}^2$. On note

$$d = a \wedge b, a' = \frac{a}{d}, b' = \frac{b}{d}, n' = a'^2 + b'^2 = \frac{n}{d^2}.$$

Montrer que n' n'est divisible par aucun nombre premier congru à 3 modulo 4. Conclure.

¹Par un exercice du TD ou par le dernier DM

²Théorème énoncé par Girard en 1625. Dans une lettre à Mersenne datée du jour de Noël 1640, Fermat discute des outils nécessaires à sa résolution.