DM 9 - Somme de deux carrés – Lemme de Fekete

1 Entiers de Gauss et sommes de deux carrés

Dans ce problème, on étudie l'anneau $\mathbb{Z}[i] = \left\{a + ib, (a, b) \in \mathbb{Z}^2\right\}$ 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 :
   $$\forall a \in \mathbb{Z}[i], \forall b \in \mathbb{Z}[i] - \left\{0\right\}, \exists (q, r) \in \mathbb{Z}[i]^2 : a = bq + r \text{ et } N(r) < N(b).$$
   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

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

6. Montrer qu'il existe $d \in I - \left\{0\right\}$ tel que $N(d) = \min\left\{N(z), z \in I - \{0\}\right\}$.
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 sait[1] 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 $\Sigma = \left\{n \geq 1 \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2+b^2\right\}$. 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.

[1] Par un exercice du TD ou par le dernier DM

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

2 Lemme de Fekete, avec une application

2.1 Lemme de Fekete

Soit $(x_n)_{n\geq 1}$ une suite réelle telle que, pour tous $n, p \in \mathbb{N}^*$, $x_{n+p} \leq x_n + x_p$. On pose

$$E = \left\{ \frac{x_n}{n}, n \in \mathbb{N}^* \right\}.$$

1. Soit $d \in \mathbb{N}^*$. Si $n \geq d$, on note $n = dq + r$, la division euclidienne de n par d.
   Montrer que, pour tout $n \geq d$, $x_n \leq q x_d + x_r$.
2. En déduire que $\forall n \geq d, \dfrac{x_n}{n} \leq \dfrac{x_d}{d} + 2\dfrac{X_d}{n}$, où $X_d = \max\Big(|x_1|, \dots, |x_d|\Big)$.
3. On suppose que E est minoré. Montrer que $\left(\dfrac{x_n}{n}\right)_{n\geq 1}$ tend vers $\inf(E)$.

2.2 Chemins auto-évitants dans $\mathbb{Z}^2$

Un pas dans $\mathbb{Z}^2$ est un élément de $\mathscr{P} = \big\{(1,0), (0,1), (-1,0), (0,-1)\big\}$. Un chemin de longueur $n \in \mathbb{N}$ dans $\mathbb{Z}^2$ est une $(n+1)$-liste $(s_0, \dots, s_n)$ d'éléments de $\mathbb{Z}^2$ telle que $s_0 = (0,0)$ et, telle que pour tout $k \in [\![0, n-1]\!]$, $s_{k+1} - s_k$ est un pas. Un tel chemin est auto-évitant si la liste est sans répétition. On note c_n le nombre de chemins de longueur n auto-évitants.

1. Illustrer ces définitions.
2. Déterminer c_n pour $n \in [\![0, 4]\!]$.
3. Montrer que pour tous $n, p \in \mathbb{N}$, $c_{n+p} \leq c_n c_p$.
4. En déduire que la suite $(\sqrt[n]{c_n})_{n\geq 1}$ converge vers un réel[3] $\mu \in [2, 3]$.

Une conjecture affirme qu'il existe deux constantes c et γ telles que $c_n \sim c\mu^n n^\gamma$.
On suppose dans la suite que cette conjecture est vraie.

5. Montrer que $\dfrac{c_{n+1}}{c_n}$ tend vers μ.
6. Interpréter la quantité $\dfrac{c_{2n}}{c_n^2}$ et en déterminer un équivalent.
7. En déduire une expression de la constante[4] γ comme la limite d'une suite ne dépendant que de c_n.
8. **Bonus.** Écrire un programme calculant c_n ; vérifier empiriquement les valeurs de μ et γ.

[3]La valeur exacte est inconnue. On sait cependant que $\mu \in [2{,}6; 2{,}7]$. Pour le problème analogue où on considère des chemins sur le réseau hexagonal (les pas sont les racines 6-èmes de l'unité), la constante μ vaut $\sqrt{2+\sqrt{2}}$, *Smirnov et Duminil-Copin, 2008.*

[4]Il est aussi conjecturé que $\gamma = \dfrac{11}{32}$.