

DM 9 - Somme de deux carrés – Lemme de Fekete – Corrigé

1 Entiers de Gauss et sommes de deux carrés**1.1 $\mathbb{Z}[i]$ est un anneau euclidien.**

- Soient $z, z' \in \mathbb{Z}[i]$. On note $z = a + ib$ et $z' = c + id$ avec $a, b, c, d \in \mathbb{Z}$. Alors $z - z' = (a - c) + i(d - c)$ donc $z - z' \in \mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est non vide (il contient 0), c'est un sous-groupe de $(\mathbb{C}, +)$. De plus, $1 \in \mathbb{Z}[i]$ et $zz' = (ac - bd) + i(ad + bc)$; donc $\mathbb{Z}[i]$ est stable par produit et contient l'élément neutre pour la multiplication. Donc $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} .
- Soient $z, z' \in \mathbb{Z}[i]$. On a

$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

- Soit $z = a + ib \in \mathbb{Z}[i]$. On a $N(z) = a^2 + b^2 \in \mathbb{N}$. Si z est inversible, il existe $z' \in \mathbb{Z}[i] : zz' = 1$. Par la question précédente, $N(z)N(z') = 1$. Comme $N(z)$ et $N(z')$ sont des entiers naturels, les deux valent 1. Donc $N(z) = 1$.
- Réiproquement, si $N(z) = 1$, on a $z\bar{z} = |z|^2 = 1$. Comme $\bar{z} \in \mathbb{Z}[i]$, z est inversible, d'inverse \bar{z} .

- Soient $a \in \mathbb{Z}[i]$, $b \in \mathbb{Z}[i] - \{0\}$. On écrit $\frac{a}{b} = x + iy$, avec x et y réels. On peut trouver des entiers x' et y' tels que $|x - x'| \leq 1/2$ et $|y - y'| \leq 1/2$. Notons $q = x' + iy' \in \mathbb{Z}[i]$. On a donc :

$$\left| \frac{a}{b} - q \right| \leq \sqrt{(1/2)^2 + (1/2)^2} = \frac{1}{\sqrt{2}}.$$

On multiplie par $|b|$ et on prend le carré :

$$|a - qb|^2 \leq \frac{1}{2}|b|^2.$$

Donc $N(a - qb) < N(b)$ (car $b \neq 0$). En posant $r = a - qb$, on a bien

$$a = bq + r \text{ et } N(r) < N(b).$$

- On considère $a = 1 + i$ et $b = 2$. Alors $1 + i = 2 \times 0 + (1 + i)$ et $1 + i = 2 \times +(-1 + i)$. Et $N(1 + i) = N(-1 + i) < N(2)$. Il n'y a donc pas unicité.

Cela n'a rien de surprenant. Déjà dans \mathbb{Z} , la division euclidienne n'est unique que si on décide de façon (arbitraire) de prendre un reste positif. Si on demande seulement que $|r| < |b|$, il y aura en général deux choix possibles (avec deux quotients différant de 1).

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

6. Notons X l'ensemble $\{N(z), z \in I - \{0\}\}$. On a vu que N est à valeurs dans \mathbb{N} . Donc X est une partie de \mathbb{N} , évidemment non vide. Elle admet donc un plus petit élément. Cet élément est donc de la forme $N(d)$, pour un $d \in I - \{0\}$.
7. On écrit une division euclidienne de a par d : $a = qd + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(d)$. Comme d est dans I , il est de la forme $d = au + xv$, avec $u, v \in \mathbb{Z}[i]$. Ainsi,

$$r = a - qd = a(1 - qu) + x(-qv).$$

Donc, $r \in I$. Comme $N(r) < N(d)$, on a nécessairement $r = 0$, par construction de d . Donc d divise a . Comme $d = au + xv$, on a aussi que d divise x .

On écrit donc $a = dd'$, avec $d' \in \mathbb{Z}[i]$. Comme a est irréductible, d ou d' est inversible. Mais si d' était inversible, on aurait que a divise d et que d divise x , ce qui est contraire à l'hypothèse. Donc, c'est d qui est inversible.

En multipliant $d = au + xv$ par l'inverse de d , on obtient une relation $1 = au' + xv'$, avec $u', v' \in \mathbb{Z}[i]$. On multiplie par y : $y = ayu' + xyv'$. Comme a divise ay et xy (par hypothèse), il divise le membre de droite. Donc a divise y (le membre de gauche). Le lemme d'Euclide est démontré.

1.3 Nombres premiers somme de deux carrés

8. Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\bar{0}^2 = \bar{2}^2 = \bar{0}$ et $\bar{1}^2 = \bar{3}^2 = \bar{1}$. Donc 0 et 1 sont les seuls carrés modulo 4. Ainsi, si $p = x^2 + y^2$, p vaut $0 + 0 = 1$ ou $1 + 0 = 0 + 1 = 1$ ou $1 + 1 = 2$ modulo 4. En particulier, un nombre premier p congru à 3 modulo 4 n'est pas somme de deux carrés.
9. Comme $x^2 \equiv 1 [p]$, p divise $x^2 + 1$ dans \mathbb{Z} , donc aussi dans $\mathbb{Z}[i]$. Si p divisait $x + i$, on aurait l'existence de $a, b \in \mathbb{Z}$ tels que $p(a + ib) = x + i$, d'où $ap = x$ et $bp = 1$. La deuxième égalité est absurde. Donc p ne divise pas $x + i$; de même il ne divise pas $x - i$.
10. Si p était irréductible dans $\mathbb{Z}[i]$, comme il divise $x^2 + 1$, le lemme d'Euclide impliquerait qu'il divise $x + i$ ou $x - i$, ce qui n'est pas. Donc p n'est pas irréductible ; il existe donc une décomposition $p = bc$, avec b et c dans $\mathbb{Z}[i]$ non inversibles.
11. On prend la norme dans l'égalité précédente : $N(p) = N(b)N(c)$. Or $N(p) = p^2$ et $N(b)$ et $N(c)$ sont des entiers naturels. De plus, $N(b)$ et $N(c)$ sont différents de 1 car b et c ne sont pas inversibles. Nécessairement, $N(b) = N(c) = p$.

On écrit $b = u + iv$, avec $u, v \in \mathbb{Z}$. Alors,

$$p = N(b) = u^2 + v^2$$

est une somme de deux carrés d'entiers.

1.4 Théorème de Fermat de Noël

12. Soit $n \geq 1$. On a les équivalences suivantes :

$$\begin{aligned} n \in \Sigma &\iff \exists a, b \in \mathbb{Z} : n = a^2 + b^2 \\ &\iff \exists a, b \in \mathbb{Z} : n = N(a + ib) \\ &\iff \exists z \in \mathbb{Z}[i] : n = N(z). \end{aligned}$$

13. Soient $u, v \in \Sigma$. On peut donc trouver $z, z' \in \mathbb{Z}[i]$ tels que $N(z) = u$ et $N(z') = v$. Alors $uv = N(zz')$. Donc $uv \in \Sigma$.

En pratique, cela donne un éclairage par les complexes à

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

qu'on appelle l'identité de Diophante, ou de Lagrange.

14. Soit n un entier dont toutes les valuations $v_p(n)$ sont paires, si p est congru à 3 modulo 4. Alors, n est le produit d'un certain nombre de facteurs 2, d'un certain nombre de facteurs p_i , avec p_i congru à 1 modulo 4, et d'un certain nombre de facteurs q_j^2 , avec q_j congru à 3 modulo 4.

Or $2 = 1^2 + 1^2$ est dans Σ . Les p_i congrus à 1 modulo 4 sont dans Σ d'après la partie précédente. Les q_j^2 , pour q_j congru à 3 modulo 4, vérifient $q_j^2 = q_j^2 + 0^2$, donc sont dans Σ .

Une récurrence immédiate utilisant la question précédente montre qu'un produit d'un nombre quelconque de facteurs dans Σ est encore dans Σ . Donc, n est dans Σ .

15. On écrit $u^{p-1} + v^{p-1} = (u^2)^{\frac{p-1}{2}} + (v^2)^{\frac{p-1}{2}} = (u^2)^{\frac{p-1}{2}} - (-v^2)^{\frac{p-1}{2}}$. La première égalité vient de ce que $p-1$ est pair, la deuxième du fait que $\frac{p-1}{2}$ est impair (car $p \equiv 3 [4]$). Par l'identité de Bernoulli, on a donc :

$$u^{p-1} + v^{p-1} = (u^2 + v^2) \sum_{k=0}^{\frac{p-1}{2}-1} (u^2)^k (-v^2)^{\frac{p-1}{2}-k}.$$

Donc $u^2 + v^2$ divise $u^{p-1} + v^{p-1}$.

16. Supposons que p divise $u^2 + v^2$. D'après la question précédente, on a donc $u^{p-1} + v^{p-1} \equiv 0 [p]$. Or, par le petit théorème de Fermat, $u^{p-1} \equiv 1 [p]$ (si $u \wedge p = 1$) ou $u^{p-1} \equiv 0 [p]$ (si $p \mid u$) ; de même pour v . Donc si p ne divise pas u ou v , on trouve $u^{p-1} + v^{p-1} \equiv 1$ ou $2 [p]$. Comme $p \geq 3$, c'est absurde. Donc, p divise u et p divise v .

La réciproque est évidente.

17. **Conclusion :** Supposons par l'absurde que n' soit divisible par un nombre premier p congru à 3 modulo 4. Comme $n' = a'^2 + b'^2$, on a alors, d'après la question précédente, que n divise a' et b' . Comme a' et b' sont premiers entre eux, c'est absurde. Donc n' n'est divisible par aucun nombre premier congru à 3 modulo 4.

Or, $n = n'd^2$. Si p est congru à 3 modulo 4, on a donc $v_p(n) = v_p(n') + 2v_p(d) = 2v_p(d)$. Donc, toutes les valuations $v_p(n)$ sont paires, si p est congru à 3 modulo 4.

Ceci conclut la réciproque.

2 Lemme de Fekete, avec une application

2.1 Lemme de Fekete

- Soient n, d deux entiers tels que $n \geq d$. La propriété vérifiée par (x_n) donne $x_{2n} \leq x_n + x_n = 2x_n$, puis $x_{3n} \leq x_{2n} + x_n \leq 3x_n$, etc. Par récurrence immédiate, on en déduit que

$$x_{qd} \leq qx_d.$$

Comme $x_n = x_{qd+r} \leq x_{qd} + x_r$, on en déduit $x_n \leq qx_d + x_r$.

- On divise l'inégalité précédente par n :

$$\frac{x_n}{n} \leq \frac{q}{n}x_d + \frac{1}{n}x_r.$$

Comme $n = qd + r$, on a $\frac{q}{n} = \frac{n-r}{n} \frac{1}{d}$. D'où :

$$\frac{x_n}{n} \leq \frac{x_d}{d} - \frac{1}{n} \frac{r}{d} x_d + \frac{1}{n} x_r.$$

Comme $r \leq d$, $-\frac{r}{d} x_d \leq X_d$ (attention, x_d peut être négatif!). De plus, $x_r \leq X_d$. On en déduit que :

$$\frac{x_n}{n} \leq \frac{x_d}{d} + 2 \frac{X_d}{n}.$$

- Notons $\ell = \inf(E)$. Soit $\varepsilon > 0$. On peut trouver $d \in \mathbb{N}^*$ tel que $\frac{x_d}{d} \leq \ell + \frac{\varepsilon}{2}$. Soit $n \geq d$. D'après la question précédente, on a

$$\frac{x_n}{n} \leq \frac{x_d}{d} + 2 \frac{X_d}{n},$$

où $X_d = \max(|x_1|, \dots, |x_d|)$. La suite $\left(2 \frac{X_d}{n}\right)_n$ tend vers 0 ; il existe donc $N \in \mathbb{N}$ tel que, pour tout $n \geq N$, $2 \frac{X_d}{n} \leq \frac{\varepsilon}{2}$. Alors, pour tout $n \geq \max(d, N)$, on a :

$$\frac{x_n}{n} \leq \ell + \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \ell + \varepsilon.$$

De plus, on a $\frac{x_n}{n} \geq \ell$ car $\frac{x_n}{n}$ est un élément de E , minoré par ℓ . Ainsi,

$$\forall n \geq \max(d, N), \left| \frac{x_n}{n} - \ell \right| \leq \varepsilon.$$

On en déduit que la suite $\left(\frac{x_n}{n}\right)$ tend vers ℓ .

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

- On trouve de jolies illustrations sur la page Wikipedia : chemin auto-évitant.

2. On a $c_0 = 1$ et $c_1 = 4$. La seule restriction pour les chemins de longueur 2 est que le deuxième pas ne soit pas opposé au précédent. Donc $c_2 = 4 \times 3 = 12$. De même, étant donné un chemin quelconque de longueur 2, on peut le prolonger de 3 façons différentes en un chemin de longueur 3 (on ne peut pas revenir en le sommet d'origine). Donc $c_3 = 4 \times 3 \times 3 = 36$. Même raisonnement pour les chemins de longueur 4, mais il faut aussi retirer les 4 chemins qui reviennent au sommet d'origine en un cycle de longueur 4 ; il y a 8 tels chemins. Donc $c_4 = 36 \times 3 - 8 = 100$.
3. Notons \mathcal{C}_n l'ensemble des chemins de longueur n . Un élément de \mathcal{C}_n s'écrit donc (s_0, \dots, s_n) . Soient $n, p \in \mathbb{N}^*$. On définit une application Φ de \mathcal{C}_{n+p} dans $\mathcal{C}_n \times \mathcal{C}_p$ par

$$\Phi(s_0, \dots, s_{n+p}) = \left((s_0, \dots, s_n), (s_0, s_{n+1} - s_n, s_{n+2} - s_n, \dots, s_{n+p} - s_n) \right).$$

On a donc découpé un chemin auto-évitant en deux sous-chemins, et translaté le deuxième pour le faire démarrer à l'origine.

On vérifie que Φ est bien définie et qu'elle est injective. En effet, si (s_0, \dots, s_{n+p}) et (s'_0, \dots, s'_{n+p}) , on a déjà $(s_0, \dots, s_n) = (s'_0, \dots, s'_n)$. Puis, pour tout $k \in \llbracket 1, p \rrbracket$, $s_{n+k} - s_n = s'_{n+k} - s'_n$, ce qui implique $s_{n+k} = s'_{n+k}$, puisqu'on sait déjà que $s_n = s'_n$. Ainsi

$$c_{n+p} \leq c_n c_p.$$

4. Soit $n \in \mathbb{N}^*$. Les chemins de longueur n dont les pas sont $(1, 0)$ et $(0, 1)$ sont auto-évitants. On en déduit que $c_n \geq 2^n$. On en déduit que la suite $(\frac{\ln c_n}{n})$ est minorée par $\ln 2$. Par la question précédente, elle vérifie la condition du lemme de Fekete, donc elle converge vers un réel $\geq \ln 2$. Alors, $\sqrt[n]{c_n} = \exp\left(\frac{\ln c_n}{n}\right)$ converge vers un réel $\mu \geq 2$.

La majoration $\mu \leq 3$ vient de ce que, pour tout entier $n \geq 2$, $c_n \leq 4 \times 3^{n-1}$ (car un pas ne peut pas être égal à l'opposé du pas précédent). En passant à la racine n -ème et à la limite, on en déduit $\mu \leq 3$.

5. On a $c_n \sim c\mu^n n^\gamma$. Donc, $c_{n+1} \sim c\mu^{n+1} (n+1)^\gamma$. Par quotient d'équivalents :

$$\frac{c_{n+1}}{c_n} \sim \frac{c\mu^{n+1} (n+1)^\gamma}{c\mu^n n^\gamma} = \mu\left(1 + \frac{1}{n}\right)^\gamma \sim \mu.$$

Donc $\frac{c_{n+1}}{c_n}$ tend vers μ .

6. Étant donnés deux chemins auto-évitants de longueur n , on peut les concaténer (en opérant une translation du deuxième chemin pour qu'il démarre à la fin du premier) pour obtenir un chemin de longueur $2n$. Ce chemin ne sera pas nécessairement auto-évitant. La quantité $\frac{c_{2n}}{c_n^2}$ s'interprète comme la probabilité pour que la concaténation de deux chemins auto-évitants de longueur n , donne un chemin auto-évitant de longueur $2n$.

On a $c_{2n} \sim c\mu^{2n} (2n)^\gamma$ et $c_n^2 \sim c^2 \mu^{2n} n^{2\gamma}$. Donc, par quotient d'équivalents :

$$\frac{c_{2n}}{c_n^2} \sim \frac{c\mu^{2n} (2n)^\gamma}{c^2 \mu^{2n} n^{2\gamma}} = \frac{2^\gamma}{c} n^{-\gamma}.$$

7. La constante γ doit être positive ou nulle. Sinon l'équivalent précédent montrerait que $\frac{c_{2n}}{c_n^2}$ tend vers $+\infty$, ce qui est absurde (on sait que la fraction est inférieure à 1). Supposons que $\gamma > 0$. Alors, dans l'équivalent précédent, les suites tendent vers 0. D'après le cours, on peut passer au logarithme dans ces équivalents et on a donc :

$$\ln\left(\frac{c_{2n}}{c_n^2}\right) \sim \gamma \ln 2 - \ln c - \gamma \ln n \sim -\gamma \ln n.$$

On en déduit que

$$\gamma = \lim_n \frac{2 \ln c_n - \ln c_{2n}}{\ln n}.$$

8. *Non corrigé.*