

# DEVOIR À LA MAISON N° : CORRIGÉ

## Problème 1 — Complexes et arithmétique

### Partie I – Quelques propriétés élémentaires

- Il suffit de montrer que  $\mathbb{Z}[i]$  est un sous-anneau de  $(\mathbb{C}, +, \times)$ . On vérifie donc que  $1 = 1 + 0i \in \mathbb{Z}[i]$  et que pour tout  $(z, z') \in \mathbb{Z}[i]^2$ ,  $z - z' \in \mathbb{Z}[i]$  et  $zz' \in \mathbb{Z}[i]$ .
- Soit  $u$  un inversible de  $\mathbb{Z}[i]$ . Il existe donc  $u' \in \mathbb{Z}[i]$  tel que  $uu' = 1$ . Soit alors  $z \in \mathbb{Z}[i]$ . On a  $z = uu'z = u(u'z)$  où  $u'z$  est un entier de Gauss. Donc  $u$  divise  $z$  dans  $\mathbb{Z}[i]$ .
- a. Soit  $(z, z') \in \mathbb{Z}[i]^2$ . Alors

$$N(zz') = zz'\overline{zz'} = z\bar{z}z'\overline{z'} = |z|^2|z'|^2 = N(z)N(z')$$

- Soit  $z$  un inversible de  $\mathbb{Z}[i]$ . Il existe donc  $z' \in \mathbb{Z}[i]$  tel que  $zz' = 1$ . Comme  $N$  est multiplicative,  $N(z)N(z') = N(zz') = N(1) = 1$ . Comme  $N$  est à valeurs dans  $\mathbb{N}$ ,  $N(z)$  est un diviseur positif de 1. Or le seul diviseur positif de 1 est 1. Ainsi  $N(z) = 1$ .  
Réciproquement, soit  $z \in \mathbb{Z}[i]$  tel que  $N(z) = 1$ . On a donc  $z\bar{z} = 1$ . Or  $\bar{z} \in \mathbb{Z}[i]$ , ce qui prouve que  $z$  est un inversible de  $\mathbb{Z}[i]$ .
- D'après la question précédente, les inversibles de  $\mathbb{Z}[i]$  sont les complexes de la forme  $a + ib$  avec  $a^2 + b^2 = 1$  et  $(a, b) \in \mathbb{Z}^2$ . Ce sont donc 1,  $-1$ ,  $i$  et  $-i$ .
- a.  $1 + 2i$  et  $1 - 2i$  conviennent puisque  $N(1 + 2i) = N(1 - 2i) = 5$ .  
On a également  $2 \pm i$ ,  $1 \pm 4i$ ,  $4 \pm i$ ,  $2 \pm 3i$ ,  $3 \pm 2i$ , ...  
b. Soit  $z \in \mathbb{Z}[i]$  tel que  $N(z)$  soit un nombre premier. D'abord,  $z$  est non inversible puisque  $N(z) \neq 1$ . Soit  $a \in \mathbb{Z}[i]$  un diviseur de  $z$  dans  $\mathbb{Z}[i]$ . Il existe donc  $b \in \mathbb{Z}[i]$  tel que  $z = ab$ . On a alors  $N(z) = N(a)N(b)$  mais comme  $N(z)$  est premier,  $N(a) = 1$  ou  $N(a) = N(z)$ .  
► Si  $N(a) = 1$ , alors  $a$  est inversible dans  $\mathbb{Z}[i]$  d'après **I.3.b**.  
► Si  $N(a) = N(z)$ , alors  $N(b) = 1$  et  $b$  est inversible dans  $\mathbb{Z}[i]$ . On a alors  $a = b^{-1}z$ .  $b^{-1}$  est également inversible dans  $\mathbb{Z}[i]$  et  $a$  est donc le produit de  $z$  par un inversible de  $\mathbb{Z}[i]$ .  
On en déduit que  $z$  est irréductible dans  $\mathbb{Z}[i]$ .
- 5 est premier mais non irréductible dans  $\mathbb{Z}[i]$  puisque  $5 = (1 - 2i)(1 + 2i)$  et que  $N(1 - 2i) = N(1 + 2i) = 5 \neq 1$ . Les nombres premiers 13, 17, ... conviennent également.

**REMARQUE.** On peut montrer que tous les nombres premiers congrus à 1 modulo 4 conviennent.

- a.  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$  puisque  $p = (a - ib)(a + ib)$  et que  $N(a - ib) = N(a + ib) = p \neq 1$ . Mais d'après la question **I.4.b**,  $a + ib$  et  $a - ib$  sont irréductibles dans  $\mathbb{Z}[i]$ .  
b. Soit  $p$  un nombre premier non irréductible dans  $\mathbb{Z}[i]$ . Il existe donc  $z$  et  $z'$  dans  $\mathbb{Z}[i]$  tels que  $p = zz'$ ,  $N(z) \neq 1$  et  $N(z') \neq 1$ . On a de plus  $N(z)N(z') = N(p) = p^2$ .  $p$  étant premier, les diviseurs de  $p^2$  sont 1,  $p$  et  $p^2$ . On a donc les possibilités suivantes :  
►  $N(z) = 1$  et  $N(z') = p^2$  ;  
►  $N(z) = p^2$  et  $N(z') = 1$  ;  
►  $N(z) = N(z') = p$ .  
Or  $N(z) \neq 1$  et  $N(z') \neq 1$  donc  $N(z) = N(z') = p$ . Ainsi  $p = \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2$  est bien la somme de deux carrés d'entiers naturels.

### Partie II – Décomposition en facteurs irréductibles dans $\mathbb{Z}[i]$

1. a. Soit  $z$  un entier de Gauss non nul et non inversible. L'ensemble  $\mathcal{D}$  des diviseurs non inversibles de  $z$  dans  $\mathbb{Z}[i]$  est non vide puisqu'il contient  $z$ . Comme la norme est à valeurs dans  $\mathbb{N}$ ,  $\mathcal{D}$  possède un élément  $w$  de norme minimale.  
Supposons  $w$  non irréductible. Il existe donc  $a, b \in \mathbb{Z}[i]$  tels que  $w = ab$ ,  $N(a) \neq 1$  et  $N(b) \neq 1$ .  $b$  ne peut être nul sinon  $z$  le serait également. Ainsi  $N(b) > 1$ . Par conséquent,  $N(a) < N(w)$  et  $a$  est un diviseur non inversible de  $w$  donc de  $z$ , ce qui contredit la définition de  $w$ .
- b. On définit l'hypothèse de récurrence suivante :

HR( $n$ ) : « tout entier de Gauss non nul et non inversible de norme inférieure ou égale à  $n$  peut s'écrire comme un produit d'entiers de Gauss irréductible. »

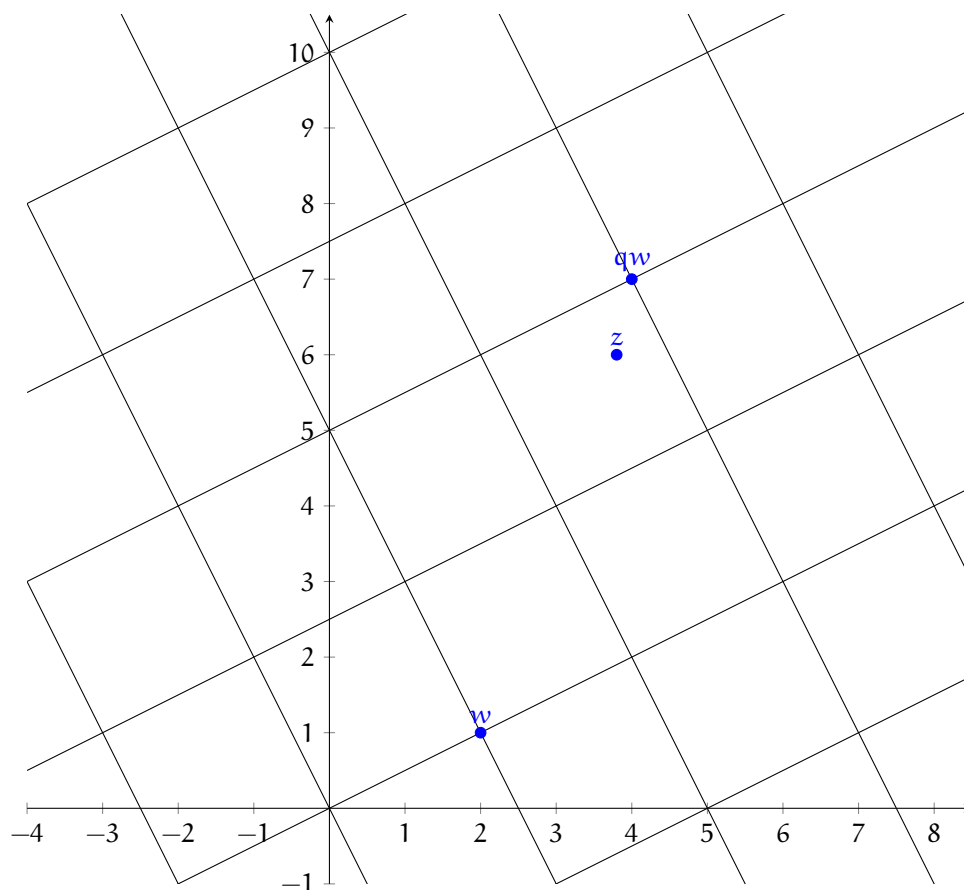
HR(1) est vraie puisque tous les entiers de Gauss de norme inférieure ou égale à 1 sont soit nuls (norme égale à 0) soit inversibles (norme égale à 1).

Supposons que HR( $n$ ) soit vraie pour un entier  $n \geq 1$ . Soit  $z$  un entier de Gauss de norme  $n + 1$ . Comme  $n + 1 \geq 2$ ,  $z$  n'est ni nul ni inversible. D'après la question précédente, il admet un diviseur irréductible  $w$ . Il existe donc  $d$  tel que  $z = dw$ .

Si  $d$  est inversible, on montre facilement que  $dw$  est irréductible et  $z$  s'écrit bien comme le « produit » d'un facteur irréductible.

Supposons maintenant  $d$  non inversible. On a  $d \neq 0$  puisque  $z \neq 0$ . On a  $N(w) > 1$  puisque  $w$  n'est ni nul ni irréductible. Ainsi  $N(d) < N(z)$  i.e.  $N(d) \leq n$ . On applique HR( $n$ ) à  $d$  qui s'écrit donc comme le produit de facteurs irréductibles. Comme  $z = dw$  avec  $w$  irréductible,  $z$  s'écrit également comme le produit de facteurs irréductibles.

2. Les complexes de la forme  $qw$  où  $q \in \mathbb{Z}[i]$  sont des entiers de Gauss dont les images dans le plan complexe sont les points du réseau représenté sur la figure suivante. Il s'agit donc de choisir un point  $qw$  de ce réseau suffisamment



proche de  $z$  pour que  $N(z - qw) < N(q)$ . Ceci est possible puisque pour tout point du plan, il existe un point du réseau à une distance inférieure à la demi-diagonale d'une maille du réseau  $|q| \frac{\sqrt{2}}{2}$ .

En effet, posons  $\frac{z}{w} = x + iy$  avec  $(x, y) \in \mathbb{R}^2$  (on a en fait  $(x, y) \in \mathbb{Q}^2$ ). Il existe des entiers  $a$  et  $b$  tels que  $|x - a| \leq \frac{1}{2}$  et  $|y - b| \leq \frac{1}{2}$  (si la partie fractionnaire de  $x$  est inférieure à  $\frac{1}{2}$ , on prend pour  $a$  la partie entière de  $x$ , sinon on

prend pour  $a$  la partie entière de  $x + 1$  ; on procède de même pour  $b$ ). On pose alors  $q = a + ib$  et  $r = z - qw$ . Alors

$$0 \leq N(r) = N(w) \left| \frac{z}{w} - q \right|^2 = N(w) (|x - a|^2 + |y - b|^2) \leq \frac{1}{2} N(w) < N(w)$$

On n'a pas unicité de  $q$  et  $r$ . Choisissons par exemple  $z = \frac{1}{2} + \frac{1}{2}i$  et  $w = 1$ . Les couples  $(q, r)$  suivants conviennent :

$$\left(0, \frac{1}{2} + \frac{1}{2}i\right), \left(1, -\frac{1}{2} + \frac{1}{2}i\right), \left(i, \frac{1}{2} - \frac{1}{2}i\right), \left(1 + i, -\frac{1}{2} - \frac{1}{2}i\right)$$

**3.** Soit  $(z, w) \in \mathbb{Z}[i]^2$ .

Supposons qu'il existe  $u, v \in \mathbb{Z}[i]$  tels que  $uz + vw = 1$ . Soit  $d$  un diviseur commun de  $z$  et  $w$  dans  $\mathbb{Z}[i]$ .  $d$  divise alors  $uz + vw = 1$ . Ainsi  $d$  est inversible (les inversibles sont exactement les diviseurs de 1).

Supposons maintenant que  $z$  et  $w$  sont premiers entre eux. Soit  $A = \{uz + vw \mid u, v \in \mathbb{Z}[i]\}$ .  $A \setminus \{0\}$  est non vide et possède donc un élément  $m$  de norme minimale.

Écrivons la « division euclidienne » de  $z$  par  $m$  : il existe  $q, r \in \mathbb{Z}[i]$  tels que  $z = mq + r$  et  $N(r) < N(m)$ . Comme  $m, z \in A$ ,  $r = z - mq \in A$ . Par minimalité de  $m$ ,  $r = 0$  et  $m$  divise  $z$ . On démontre de la même façon que  $m$  divise  $w$ . Ainsi  $m$  est un diviseur commun de  $z$  et  $w$  ; il est inversible.

Or  $m \in A$ , donc il existe  $u_0, v_0 \in \mathbb{Z}[i]$  tels que  $u_0 z + v_0 w = m$ . En posant  $u = m^{-1}u_0$  et  $v = v^{-1}v_0$ , on a bien  $uz + vw = 1$ .

**4.** Si  $c$  est inversible, alors  $c^3$  l'est également. On en déduit que  $a$  et  $b$  sont également inversibles puisque  $(c^3)^{-1}ab = 1$ . Or tous les inversibles de  $\mathbb{Z}[i]$  sont des cubes :  $1 = 1^3$ ,  $-1 = (-1)^3$ ,  $i = (-i)^3$  et  $-i = i^3$ .

Supposons maintenant  $c$  non inversible. On écrit une décomposition en facteurs premiers de  $c$ ,  $c = \prod_{i=1}^r p_i$ . Ainsi

$c^3 = \prod_{i=1}^r p_i^3$ . Comme  $a$  et  $b$  n'ont pas de diviseur premier commun, il existe une partition de  $\llbracket 1, r \rrbracket$  en deux parties

$I$  et  $J$  telles que pour  $i \in I$ ,  $p_i$  divise  $a$  et pour  $i \in J$ ,  $p_i$  divise  $b$ . D'après l'unicité de la décomposition en facteurs premiers et quitte à mettre tous les facteurs inversibles en facteur, il existe des inversibles  $u$  et  $v$  tels que  $a = u \prod_{i \in I} p_i^3$

et  $b = v \prod_{i \in J} p_i^3$  (si l'une des parties  $I$  et  $J$  est vide, on convient qu'un produit indexé sur l'ensemble vide vaut 1). On

a vu que tout inversible est un cube dans  $\mathbb{Z}[i]$ , c'est donc le cas de  $u$  et  $v$ , ce qui achève de prouver que  $a$  et  $b$  sont des cubes dans  $\mathbb{Z}[i]$ .

### Partie III – Résolution de l'équation $y^3 = x^2 + 1$

**1.** Si  $x$  est pair,  $x^2 + 1 \equiv 1[4]$ . Si  $x$  est impair,  $x^2 + 1 \equiv 2[4]$ .

Si  $y \equiv 0[4]$ ,  $y^3 \equiv 0[4]$ . Si  $y \equiv 1[4]$ ,  $y^3 \equiv 1[4]$ . Si  $y \equiv 2[4]$ ,  $y^3 \equiv 0[4]$ . Si  $y \equiv 3[4]$ ,  $y^3 \equiv 3[4]$ .

On n'a jamais  $y^3 \equiv 2[4]$  ; on en déduit que  $x$  ne peut qu'être pair.

**2.** Soit  $k \in \mathbb{N}$  tel que  $x = 2k$ . Soit  $d$  un diviseur commun de  $x + i$  et  $x - i$ . Comme  $(-i)(x + i) + i(x - i) = 2$ ,  $d$  divise 2 dans  $\mathbb{Z}[i]$ . Donc  $N(d)$  divise  $N(2) = 4$ . Par ailleurs,  $N(d)$  divise  $N(x + i) = 1 + 4k^2$ . Ainsi  $N(d)$  divise 1 i.e.  $N(d) = 1$ , ce qui prouve que  $d$  est inversible.

Les seuls diviseurs communs de  $x + i$  et  $x - i$  sont les inversibles de  $\mathbb{Z}[i]$  ;  $x + i$  et  $x - i$  sont premiers entre eux.

**3.** Tout d'abord  $x^2 + 1 > 0$  donc  $y \neq 0$ . Comme  $y^3 = (x + i)(x - i)$  et que  $x + i$  et  $x - i$  sont premiers entre eux,  $x + i$  et  $x - i$  sont des cubes d'éléments de  $\mathbb{Z}[i]$  d'après la question **II.4**.

**4.** D'après la question précédente, il existe  $a, b \in \mathbb{Z}$  tels que  $x + i = (a + ib)^3$ . En passant à la partie imaginaire, on a notamment  $b^2(3a - b) = 1$ . On a donc  $b = 3a - b = \pm 1$ . On ne peut avoir  $b = 1$ , sinon on aurait  $3a = 2$  avec  $a$  entier, ce qui est impossible. C'est donc que  $b = -1$  et  $a = 0$ . On a donc  $x = (a + ib)^3 - i = (-i)^3 - i = 0$ . Il vient alors  $y = 1$ .

L'unique couple de solutions entières de l'équation  $y^3 = x^2 + 1$  est donc le couple  $(x, y) = (0, 1)$ .