■ ■ ■

On note i le nombre complexe tel que $i^2 = -1$ et

$$\mathbb{Z}[i] = \left\{a + ib,\, (a,b) \in \mathbb{Z}^2\right\}.$$

Pour tout $z = a + ib \in \mathbb{Z}[i]$, on pose $N(a+ib) = a^2 + b^2$.

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.
On dira qu'un nombre $z \in \mathbb{Z}[i]$ est inversible s'il existe un nombre $y \in \mathbb{Z}[i]$ tel que $zy = 1$.

2. Montrer que pour tous x, $y \in \mathbb{Z}[i]$, $N(xy) = N(x)N(y)$. En déduire l'ensemble des élements symétrisables de $\mathbb{Z}[i]$.

3. On dit qu'un élément $z \in \mathbb{Z}[i]$ est irréductible s'il n'est pas inversible et s'il ne peut pas se décomposer comme un produit d'éléments non inversibles de $\mathbb{Z}[i]$.

a) Soit $z \in \mathbb{Z}[i]$ tel que $N(z)$ soit un nombre premier. Montrer que z est irréductible.

b) Montrer qu'il existe $z \in \mathbb{Z}[i]$ tel que z soit irréductible et que $N(z)$ soit un nombre entier composé.

c) On dit que $x \in \mathbb{Z}[i]$ est un diviseur de $z \in \mathbb{Z}[i]$ s'il existe $y \in \mathbb{Z}[i]$ tel que $z = x \times y$. Déterminer l'ensemble des diviseurs de $1 + i$.

4. Dans cette question, nous définissons une division euclidienne sur $\mathbb{Z}[i]$. Soit $z \in \mathbb{Z}[i]$ et $y \in \mathbb{Z}[i]\backslash\{0\}$. On note $\frac{z}{y} = u + iv$, où u, $v \in \mathbb{Q}$.

a) Montrer qu'il existe $(u_0, v_0) \in \mathbb{Z}^2$ tels que $|u - u_0| \leqslant \frac{1}{2}$ et $|v - v_0| \leqslant \frac{1}{2}$.

b) Montrer que $z = (u_0 + iv_0)y + r$, où $r \in \mathbb{Z}[i]$ et $N(r) < N(y)$.

c) Cette décomposition est-elle unique ?

5. Autour de la décomposition d'un nombre comme somme de deux carrés.

a) Soit p un nombre premier (dans $\mathbb{Z}$). Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement s'il n'existe pas de couple $(a,b) \in \mathbb{N}^2$ tels que $p = a^2 + b^2$.

b) Soit $n \in \mathbb{N}$ et $\mathscr{C} = \{a^2 + b^2,\, (a,b) \in \mathbb{N}^2\}$. Montrer que $n \in \mathscr{C}$ si et seulement s'il existe $u \in \mathbb{Z}[i]$ tel que $N(u) = n$.

c) En déduire que si n, $n' \in \mathscr{C}$, alors $nn' \in \mathscr{C}$.