I. Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'anneau des *entiers de Gauss*.

(a) Soit $w = 1{,}8 + 2{,}6\,i$. Trouver un $q = a + ib \in \mathbb{Z}[i]$ avec $|w - q| < 1$.

(b) Soit $z = x + iy \in \mathbb{C}$. Expliquer comment on peut trouver un $q = a + ib \in \mathbb{Z}[i]$ avec $|z - q| < 1$.

(c) Soit $w_0 = \frac{7+i}{2-i}$. Trouver un $q = a + ib \in \mathbb{Z}[i]$ avec $|w_0 - q| < 1$. Existe-t-il un $r \in \mathbb{Z}[i]$ avec $7 + i = (2 - i)q + r$ et $|r| < |2 + i|$?

(d) Soit $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Démontrer que qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = vq + r$ et $|r| < |v|$.

(e) Quel est le plus grand diviseur commun de $7 + i$ et de $2 - i$ dans $\mathbb{Z}[i]$?

(f) Quel est le plus grand diviseur commun de $9 + 17i$ et de $10 + 4i$ dans $\mathbb{Z}[i]$?

II. La *norme* de d'un entier de Gauss $u = a+ib \in \mathbb{Z}[i]$ est $N(u) = u\overline{u} = |u|^2 = a^2+b^2 \in \mathbb{N}$.

(a) Démontrer qu'on a $N(uv) = N(u)N(v)$.

(b) Démontrer que si u divise w dans $\mathbb{Z}[i]$, alors $N(u)$ divise $N(w)$ dans $\mathbb{N}$.

(c) $N(2 - i) = 5$ divise $N(7 + i) = 50$ dans $\mathbb{N}$, mais $2 - i$ divise-t-il $7 + i$ dans $\mathbb{Z}[i]$?

(d) Pourquoi $1 + i$, $2 + i$, $3 + 2i$, $1 + 4i$ sont-ils irréductibles dans $\mathbb{Z}[i]$?

(e) Pour a, b entiers, quelles sont les valeurs possibles de $a^2 + b^2$ modulo 4 ?
Expliquer pourquoi 3, 7, 11 et 19 et les premiers de Mersenne $2^{13} - 1 = 8191$ et $2^{17} - 1 = 131071$ sont irréductibles dans $\mathbb{Z}[i]$.

(f) Factoriser $N(7 + 4i)$ dans $\mathbb{Z}$. Calculer le pgcd de $7 + 4i$ avec chaque facteur. En déduire une factorisation de $7 + 4i$ en irréductibles de $\mathbb{Z}[i]$.

III. (a) Quels sont les inversibles de $\mathbb{Z}[i]$?

(b) Deux éléments a, b d'un anneau commutatif A sont dits *associés* s'il existe un inversible $u \in A^\times$ tel qu'on ait $a = bu$.
Quels sont les associés de $2 + 3i$ dans $\mathbb{Z}[i]$? Quels sont les associés de $a + bi$?

(c) Déterminer les $w = a + bi$ tel que w et $\overline{w}$ sont associés.

IV. Soit A un anneau commutatif. Exhiber un morphisme d'anneaux $\varphi\colon \mathbb{Z} \to A$. Est-il unique ?

V. (a) Quel est le noyau du morphisme $\varphi\colon \mathbb{Z} \to \frac{\mathbb{Z}[i]}{(10+9i)\mathbb{Z}[i]}$?

(b) Trouver un multiple de $10 + 9i$ de la forme $M + 2i$ avec $M \in \mathbb{Z}$.
Trouver un autre de la forme $M + 3i$.

(c) Les classes $\overline{5 + 2i}$ et $\overline{7 + 3i} \in \frac{\mathbb{Z}[i]}{(10+9i)\mathbb{Z}[i]}$ sont-ils dans l'image du morphisme φ du (a) ?

(d) Soit $a, b \in \mathbb{Z}$ deux entiers premiers entre eux. Quel est le noyau du morphisme $\psi\colon \mathbb{Z} \to \frac{\mathbb{Z}[i]}{(a+bi)\mathbb{Z}[i]}$? Son image ?

VI. (a) Trouver $u, v \in \mathbb{Z}[i]$ tel qu'on ait $(2 + 3i)u + (10 + 3i)v = 1$.

(b) Quel est l'inverse de la classe $\overline{2 + 3i} \in \frac{\mathbb{Z}[i]}{(7+10i)\mathbb{Z}[i]}$?

(c) Expliquer pourquoi $\frac{\mathbb{Z}[i]}{(7+10i)\mathbb{Z}[i]}$ est un corps. Quel est son cardinal ?

(d) Expliquer pourquoi $\frac{\mathbb{Z}[i]}{3\mathbb{Z}[i]}$, $\frac{\mathbb{Z}[i]}{7\mathbb{Z}[i]}$ et $\frac{\mathbb{Z}[i]}{11\mathbb{Z}[i]}$ sont des corps. Quels sont leurs cardinaux ?

(e) Expliquer pourquoi $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$ et $\frac{\mathbb{Z}[i]}{5\mathbb{Z}[i]}$ ne sont pas des corps.