Eléments irréductibles et premiers

Exercice 1. — **Anneaux $\mathbf{Z}[\sqrt{d}]$**
Soit $d \in \mathbf{Z}$ un entier non carré et $A = \mathbf{Z}[\sqrt{d}]$ l'anneau associé (pour $d < 0$, on pose $\sqrt{d} := \imath\sqrt{-d}$). Pour tout élément $\alpha = a + b\sqrt{d}$, on pose $\overline{\alpha} := a - b\sqrt{d}$.

a) Montrer qu'un entier $n \in \mathbf{Z} \subset A$ divise $\alpha := a + b\sqrt{d}$ dans A ssi n divise a et b dans $\mathbf{Z}$.
En déduire que dans ce cas n divise aussi $\overline{\alpha}$.

b) Soit $N : A \to \mathbf{Z}$, $\alpha \mapsto \alpha\overline{\alpha}$ ("la norme").
Vérifier que N est bien à valeurs dans $\mathbf{Z}$ et montrer que pour $\alpha, \beta \in A$ on a $N(\alpha\beta) = N(\alpha)N(\beta)$.

c) Montrer que $\alpha \in A$ est inversible ssi $N(\alpha) = \pm 1$.

d) Soit $\alpha \in A$ tel que $N(\alpha)$ soit premier dans $\mathbf{Z}$. Montrer que α est irréductible dans A.

e) Montrer que les anneaux suivants sont euclidiens pour la fonction $x \mapsto |N(x)|$:

i) $\mathbf{Z}[\imath]$ **ii)** $\mathbf{Z}[\imath\sqrt{2}]$ **iii)** $\mathbf{Z}[\sqrt{2}]$

[**Indication:** La division euclidienne de $a + b\sqrt{d}$ par $e + f\sqrt{d}$ revient à trouver un $\alpha \in \mathbf{Z}[\sqrt{d}]$ proche de $\frac{a+b\sqrt{d}}{e+f\sqrt{d}}$.]
A-t-on unicité de la division euclidienne ?

Exercice 2. — Trouver le pgcd des éléments de $\mathbf{Z}[\imath]$ suivants :

a) $4 + 6\imath$ et $5 + 7\imath$.
b) $19 - 3\imath$ et $5 - 5\imath$.
c) $1 + 3\imath$ et 10.
d) 13 et $2 + 3\imath$.

Exercice 3. — Montrer que deux entiers premiers entre eux dans $\mathbf{Z}$ le restent dans $\mathbf{Z}[\imath]$.
[**Indication:** On a un algorithme pour tester si deux entiers sont premiers entre eux...]

Exercice 4. — **Triplets pythagoriciens**
Soit $(x, y, z) \in \mathbf{Z}^3$ un triplet d'entiers *premiers entre eux* tels que
$$x^2 + y^2 = z^2.$$

a) Donner un exemple non trivial de tel triplet. Pourquoi "pythagoricien" ? Remarquer que si (x, y, z) est un tel triplet, alors $(\pm x, \pm y, \pm z)$ et $(\pm y, \pm x, \pm z)$ le sont aussi.

b) Montrer que z est impair et que parmi x et y, il y en a exactement un pair et un impair.
[**Indication:** Réduire modulo 4.]

c) Montrer que $x + \imath y$ et $x - \imath y$ sont premiers entre eux dans $\mathbf{Z}[\imath]$.
[**Indication:** Commencer par montrer que leur pgcd doit diviser 2.]

d) Montrer que $x + \imath y$ est, à une unité près, un carré de $\mathbf{Z}[\imath]$.

e) En déduire, qu'aux symétries de ***a)*** près, les triplets pythagoriciens sont exactement ceux de la forme :
$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$
avec u, v des entiers premiers entre eux, pas tous deux impairs et $u > v > 0$.

Exercice 5. — Dans l'anneau $A = \mathbf{Z}[\imath\sqrt{3}]$ on a l'égalité :
$$2 \cdot 2 = (1 + \imath\sqrt{3}) \cdot (1 - \imath\sqrt{3}).$$

a) Montrer que les éléments $2, 1 + \imath\sqrt{3}$ et $1 - \imath\sqrt{3}$ sont irréductibles non associés dans A et qu'ils ne sont pas premiers.
[**Indication:** Utiliser l'exercice ***1-d)***.]

b) L'anneau A est-il euclidien ? principal ?

c) Montrer que 2 (resp. $(1 + \imath\sqrt{3})$) est un diviseur commun à 4 et $2 \cdot (1 + \imath\sqrt{3})$ dans A et qu'il est maximal (c'est-à-dire que tout diviseur commun qu'il divise lui est associé).
En déduire que ces deux éléments n'ont pas de pgcd dans A.

d) L'idéal $(4) + (2 \cdot (1 + \imath\sqrt{3}))$ est-il principal ? Et $(2) + (1 + \imath\sqrt{3})$?