On note $A = \{x + iy\sqrt{2} \mid x, y \in \mathbb{Z}\}$. Si $\alpha = x + iy\sqrt{2} \in A$, on note $N(\alpha) = x^2 + 2y^2$.

1. Montrer que si α, β sont des éléments de A alors $\alpha + \beta$ et $\alpha\beta$ aussi.

Si α, β sont des éléments de A, on dit que α **divise** β si il existe $\gamma \in A$ tel que $\beta = \alpha\gamma$. On note $\alpha|\beta$.

2. a. Montrer que $\forall \alpha, \beta \in A$, on a $N(\alpha\beta) = N(\alpha)N(\beta)$.

b. Montrer que si $\alpha|\beta$ dans A alors $N(\alpha)|N(\beta)$ dans $\mathbb{N}$. La réciproque est-elle exacte ?

c. Quels sont les éléments inversibles (pour la multiplication) de A.

On dit que α et β appartenant à A sont **associés** s'il existe $u \in A$ inversible dans A tel que $\alpha = \beta u$.

d. Déterminer tous les diviseurs dans A de $1 + i\sqrt{2}$ et $5 + 9i\sqrt{2}$.

3. a. Montrer que $\forall z \in \mathbb{C}$, $\exists \alpha \in A$ tel que $|z - \alpha| < 1$.

b. En déduire que $\forall \alpha \in A$, $\forall \beta \in A^*$, $\exists \gamma, \rho \in A$ tels que
(i) $\alpha = \beta\gamma + \rho$;
(ii) $N(\rho) < N(\beta)$.

On dit qu'un élément λ de A^* est **premier** dans A s'il n'est pas inversible et si ses seuls diviseurs sont les éléments qui lui sont associés et les éléments inversibles.

4. a. Soit $\alpha \in A$. Montrer que si $N(\alpha)$ est premier dans $\mathbb{N}$ alors α est premier dans A. Montrer que la réciproque est fausse.

b. Déterminer si les éléments suivants sont premiers ou pas dans A : 2, 3, $3 + i\sqrt{2}$.

On dit que deux éléments α et β de A sont **premiers entre eux** si leurs seuls diviseurs communs sont les éléments inversibles.

5. a. Montrer que deux éléments α, β de A sont premiers entre eux, si, et seulement si, il existe u, v dans A tels que $\alpha u + \beta v = 1$.

b. En déduire : $\forall \alpha, \beta, \gamma \in A$, si $\alpha|\beta\gamma$ et si α est premier avec β alors α divise γ.

c. En déduire que si $\lambda \in A$ est premier dans A et si λ divise $\alpha\beta$ alors $\lambda|\alpha$ ou $\lambda|\beta$.

d. Décomposer en facteurs premiers $-13 + 14i\sqrt{2}$. (On ne demande pas de prouver l'unicité de cette décomposition ni l'existence d'une telle décomposition pour tous les éléments non-nuls de A).

6. a. Montrer que tout élément λ premier dans A divise un et un seul nombre premier p de $\mathbb{N}$.

b. Soit p un nombre premier de $\mathbb{N}$. Montrer que si p n'est pas premier dans A, il existe λ premier dans A tel que $p = N(\lambda)$.

c. Montrer que si p est un nombre premier dans $\mathbb{N}$, $p \equiv -1 \mod 8$ ou $p \equiv -3 \mod 8$ alors p est premier dans A.