UNIVERSITÉ DE RENNES 1

Théorie des nombres

Devoir surveillé

Durée 1h. Documents et calculatrice autorisés.

Exercice 1.

a. 19 est-il un carré modulo $505 = 5 \times 101$?

b. L'équation $3x^2 - 8x + 7 = 0$ a-t-elle une solution dans $\mathbb{Z}/113\mathbb{Z}$?

Exercice 2.

Dans $\mathbb{R}^2$ muni de son produit scalaire usuel, on considère L le réseau de base $\vec{u}, \vec{v}$ avec $\vec{u} = (1,1)$, $\vec{v} = (1+\sqrt{2}, 1-\sqrt{2})$. On note $q(x,y) = x^2 + 2xy + 3y^2$.

a. Quel est le covolume de L ?

b. Verifier que $||x\vec{u} + y\vec{v}||^2 = 2q(x,y)$.

c. Soit p un nombre premier, et considérons l'équation $q(x,y) = 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Pour quelles valeurs de p cette équation a-t-elle une solution dans $(\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}$?

d. Fixons p un nombre premier et $\alpha \in \mathbb{Z}/p\mathbb{Z}$. Soit $L_\alpha \subset L$ le sous-réseau defini par

$$L_\alpha = \{x\vec{u} + y\vec{v} \mid x - \alpha y = 0 \bmod p,\ (x,y) \in \mathbb{Z}^2\}$$

Determiner le covolume de L'.

e. Montrer que L_α possede un $\vec{w} \neq 0$ tq $||\vec{w}||^2 < 4p$.

f. Montrer que pour tout nombre premier p congru à 1 ou 3 modulo 8, il existe $(x,y) \in \mathbb{Z}^2$ tq $q(x,y) = 2p$. (On pourra utiliser un réseau L_α bien choisi).

Exercice 3.

On se place dans l'anneau $\mathbb{Z}[i]$.

Décomposer en produit d'irréductibles de $\mathbb{Z}[i]$ les éléments $a_1 = 73$, $a_2 = 75$, $a_3 = 77$, $a_4 = 4 + 5i$ et $a_5 = 5 + 11i$.