UNIVERSITÉ DE RENNES 1

Théorie des nombres

Devoir surveillé

Durée 1h. Documents et calculatrice autorisés. Téléphone interdit. Barème indicatif

Exercice 1. 14 points

On cherche à déterminer les entiers $n \in \mathbb{N}$ qui peuvent s'ecrire sous la forme $n = x^2 + xy + y^2$, avec $x, y \in \mathbb{Z}$.

On note $q(x, y) = x^2 + xy + y^2$. Soit $\omega = 1 + i\frac{\sqrt{3}}{2} \in \mathbb{C}$, et $\Gamma \subset \mathbb{C}$ le réseau engendré par $\{1, \omega\}$.

1. Pour $\alpha = x + \omega y \in \Gamma$, déterminer $|\alpha|^2$. Montrer que si n s'écrit sous la forme $n = x^2 + xy + y^2$, alors nécessairement, $n \geq 0$.
2. Montrer que l'ensemble des entiers qui s'écrivent sous la forme $n = x^2 + xy + y^2$ est stable par produit.
3. Les entiers 2 et 3 peuvent-ils s'écrire sous cette forme ?

On considère maintenant un nombre premier $p \geq 5$, et on cherche à savoir si p s'écrit sous la forme $p = q(x, y)$ avec $x, y \in \mathbb{Z}$.

4. Soit $a \in \mathbb{Z}/p\mathbb{Z}$ l'inverse de 2. Montrer que si $p = x^2 + xy + y^2$, alors $a^2 - 1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (on pourra écrire la forme quadratique $q(x, y)$ comme combinaison linéaire de carrés de formes linéaires...)
5. Montrer que $a^2 - 1 \neq 0 \pmod p$, et que $a^2 - 1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si -3 est un carré modulo p.
6. Quels sont les nombres premiers tels que -3 soit un carré modulo p ? -3 est-il un carré modulo le nombre premier 1201 ?

On suppose maintenant qu'il existe $b \in \mathbb{Z}$ tel que $b^2 = a^2 - 1 \pmod p$. Soit $\Gamma' \subset \Gamma$ défini par

$$\Gamma' = \{x + y\omega | x, y \in \mathbb{Z}, \text{ et } x + ay = by \pmod p\}.$$

7. Montrer que pour tout $\alpha \in \Gamma'$, $|\alpha|^2 = 0 \pmod p$
8. Determiner le covolume de Γ'.
9. Montrer qu'il existe $\alpha \in \Gamma' \setminus \{0\}$ tel que $|\alpha|^2 \leq p$.
10. Quels sont les nombres premiers p qui peuvent s'écrire sous la forme $n = x^2 + xy + y^2$, avec $x, y \in \mathbb{Z}$?
11. Déterminer tous les entiers n qui peuvent s'écrire sous la forme $n = x^2 + xy + y^2$ avec $x, y \in \mathbb{Z}$.

Exercice 2. 6 points

Soit $K = \mathbb{Q}[\sqrt{3}]$, et $R = \mathbb{Z}[\sqrt{3}]$. Pour $\alpha = x + \sqrt{3}y \in K$, on note $N(\alpha) = x^2 - 3y^2$.

1. Montrer que pour tout $\alpha, \beta \in K$, $N(\alpha\beta) = N(\alpha)N(\beta)$. Montrer que $\alpha \in R^\times$ si et seulement si $N(\alpha) = \pm 1$.
2. Existe-t-il $\alpha \in R$ tel que $N(\alpha) = -1$?
3. Montrer que R est euclidien pour la jauge euclidienne $|N(\alpha)|$.