UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°3 : Réseaux, formes quadratiques

TEST DE COMPRÉHENSION

Test 1.

a. Dessiner le réseau Γ de $\mathbb{R}^2$ engendré par $u = (1,0)$, $v = (\sqrt{3}/2, 1/2)$. Donner un vecteur non nul Γ, de longueur minimale. Quel est le covolume de Γ ?

b. Mêmes questions avec l'ensemble des éléments de $\mathbb{Z}^2$ tq $x + y = 0 \mod 3$. En donner une base.

c. Soit Γ le réseau de $\mathbb{R}^3$ engendré par $u = (1,2,0)$, $v = (1,-5,2)$, $w = (0,3,1)$. Déterminer l'indice de Γ dans $\mathbb{Z}^3$, et son covolume (pour le produit scalaire usuel).

Réponses : a. la longueur du vecteur le plus court est $\frac{1}{2}\sqrt{6 - 4\sqrt{3}} \simeq 0,5176$. Le covolume est $1/2$.

b. Covolume : 3. Base : $(3,0),(2,1)$. Longueur minimale : $\sqrt{2}$.

Test 2.

Soit Γ le réseau de $\mathbb{R}^3$ engendré par $u = (1, \sqrt{2}, 0)$, $v = (1, -5, \sqrt{2})$, $w = (0, -\sqrt{2}, 1)$.
Déterminer sa matrice de Gram, et le discriminant de Γ pour le produit scalaire usuel.

Test 3.

Considérons la forme quadratique q sur $\mathbb{R}^2$ définie par $q(x,y) = x^2 - xy + 2y^2$. Montrer que q est définie positive.

Considérons le réseau $\Gamma = \mathbb{Z}^2$, muni de sa base canonique. Donner la matrice de Gram de q dans cette base, et le discriminant de q relativement à Γ.

Réponse : q est définie positive, Matrice de Gram : $M = \begin{pmatrix} 1 & -1/2 \\ -1/2 & 2 \end{pmatrix}$. $disc(q) = 2-1/4 = 7/4$.

Avec la convention des formes quadratiques binaires, le discriminant de $q(x,y) = x^2-xy+2y^2$ est $1 - 4 \cdot 2 = -7$.

RÉSEAUX ET FORMES QUADRATIQUES

Exercice 4.

a. Écrire $2425 = 5^2 \cdot 97$ et $754 = 2 \cdot 13 \cdot 29$ comme sommes de deux carrés.

b. Tous les entiers naturels sont-ils sommes de trois carrés ?

c. Écrire l'identité qui exprime le fait que la norme du produit de deux quaternions est égale au produit de leurs normes.

d. Écrire $323 = 17 \cdot 19$ et $1265 = 5 \cdot 11 \cdot 23$ comme sommes de quatre carrés.

Exercice 5.

On cherche les nombres premiers p s'écrivant sous la forme $p = x^2 + 2y^2$.

a. Montrer que pour un tel p, -2 est un carré dans $\mathbb{F}_p$. Traduire cette condition en une condition de congruence sur p.

b. Supposons que -2 est un carré dans $\mathbb{F}_p$. Il existe donc un entier a tel que $a^2 = -2 \mod p$. En considérant le réseau $\mathcal{R}$ de $\mathbb{Z}^2$ engendré par $(a, 1)$ et $(p, 0)$ et l'ellipse définie pour un certain r par $x^2 + 2y^2 = r^2$ (le volume défini par une telle ellipse est $V_r = \frac{\pi r^2}{\sqrt{2}}$), montrer qu'il existe deux entiers x et y tels que $x^2 + 2y^2 = p$.

c. Écrire 323 sous la forme $n = x^2 + 2y^2$.

Exercice 6.

Soit p un nombre premier.

a. Montrer que s'il existe $(x, y) \in \mathbb{Z}^2$ tels que $p \mid (x^2 + 5y^2)$, alors p divise x ou -5 est un carré dans $\mathbb{F}_p$.

b. Montrer que si $p \neq 5$ et si -5 est un carré modulo p, alors il existe un couple d'entiers $(x, y) \in \mathbb{Z}^2$ tel que $x^2 + 5y^2 \in \{p, 2p\}$.

c. Trouver un nombre premier p qui s'écrive sous la forme $p = x^2 + 5y^2$, avec x et y entiers, et tel que $2p$ ne peut pas s'écrire sous cette forme.

d. Trouver un nombre premier p tel qu'il existe des entiers x et y vérifiant $2p = x^2 + 5y^2$, et tel que p ne s'écrive pas sous cette forme.

e. Montrer qu'il existe un couple $(x, y) \in \mathbb{Z}^2$ tel que $x^2 + 5y^2 \in \{p, 2p\}$ si et seulement si $p = 5$ ou $p \equiv 1, 3, 7 \text{ ou } 9 \pmod{20}$.

f. Montrer que, modulo 20, 3 et 7 ne peuvent pas s'ecrire sous la forme $x^2 + 5y^2 \mod 20$. En déduire que si $p = x^2 + 5y^2$, $p \equiv 1, 9 \pmod{20}$. Montrer de la même façon que que si $2p = x^2 + 5y^2$, $p \equiv 3, 7 \pmod{20}$. En deduire qu'un nombre premier $p \geq 7$ s'ecrit $x^2 + 5y^2$ si et seulement si $p = 1, 9 \pmod 2)0$.

Exercice 7.

On rappelle que $\mathbb{Z}[i]$ est euclidien, et que ses inversibles sont $\{\pm 1, \pm i\}$. Soit α un irréductible de $\mathbb{Z}[i]$.

a. Supposons que α a un associé dans $\mathbb{Z}$. Montrer que $|\alpha|$ est un nombre premier de $\mathbb{N}$ qui n'est pas somme de 2 carrés (ie $|\alpha| = -1 \mod 4$)

b. Supposons que α n'a pas d'associé dans $\mathbb{Z}$, et que $\alpha, \bar{\alpha}$ ne sont pas associés. Montrer que l'entier $p = |\alpha|^2$ est un nombre premier impair qui est somme de 2 carrés, ie $p = N(\alpha) = 1 \mod 4$.

c. Supposons que α n'a pas d'associé dans $\mathbb{Z}$, et que $\alpha, \bar{\alpha}$ sont associés. Montrer que $\alpha \sim (1 + i)$ et $|\alpha|^2 = 2$.

d. En deduire un nombre premier $p \in \mathbb{N}$ reste premier dans $\mathbb{Z}[i]$ ssi $p = -1 \mod 4$.

Exercice 8.

Soit $a, b \in \mathbb{Z}$. Montrer que si a et b sont premiers entre eux dans $\mathbb{Z}$, alors ils le sont aussi dans $\mathbb{Z}[i]$.

Exercice 9.

On rappelle que tout nombre premier congru à 1 modulo 4 est somme de deux carrés. On considère l'équation $(E) : x^2 + y^2 = pz^2$ où p est un nombre premier impair.

a. Vérifier qu'elle possède une solution dans $\mathbb{Q}^3 \setminus \{(0,0,0)\}$ si et seulement si elle en possède une dans $\mathbb{Z}^3 \setminus \{(0,0,0)\}$.

b. Montrer que si elle admet une solution dans $\mathbb{Z}^3 \smallsetminus \{(0,0,0)\}$, -1 est un carré dans $\mathbb{F}_p$ et donc p est congru à 1 modulo 4.

c. La réciproque est-elle vraie ?

d. Décrire l'ensemble des solution de E à partir de l'ensemble S_p des solutions rationnelles de l'équation $x^2 + y^2 = p$.

e. Montrer que l'ensemble des points (x, y) du cercle $x^2+y^2 = 1$ à coordonnées rationnelles est $S_1 = \{(-1, 0)\} \cup \{(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}), t \in \mathbb{Q}\}$.

f. En identifiant S_1 et S_p à des sous-ensembles de $\mathbb{Q}[i]$, décrire S_p sous une forme similaire à S_1 (lorsqu'il est non vide).

Exercice 10.

Réduire les formes quadratiques $q(x, y) = 5x^2+6xy+3y^2$, $2x^2-2xy+3y^2$, $10x^2+30xy+23y^2$.

Exercice 11.

Déterminer toutes les formes quadratiques definies positives (à coefficients entiers) réduites de discriminant -5 et -7.

A quelle condition sur $\delta \in \mathbb{Z}$ existe-t-il une forme quadratique à coefficients entiers de discriminant δ ? Definie positive ?

Exercice 12.

Considérons la forme quadratique $q(x, y) = 5x^2 + 5xy + 2y^2$. Pour $n = 109, 110, 111$, il s'agit de determiner si q représente n.

a. Montrer que q est definie positive, et donner son discriminant δ.

b. Determiner la forme réduite équivalente à q

c. Pour chacune des valeurs de n determiner si δ est un carré dans $\mathbb{Z}/4n\mathbb{Z}$. Lorsque c'est le cas, déterminer ses racines carrées.

d. Pour chacune des valeurs de n, déterminer un ensemble fini de formes quadratiques q_i de discriminant δ telles que $q_i(1, 0) = n$, telle que toute forme de discriminant δ représentant proprement n soit équivalente à l'une des q_i.

e. Les entiers $109, 110, 111$ sont-ils proprement représentés par q ?