UNIVERSITÉ DE RENNES 1

Théorie des nombres

Devoir surveillé
Corrigé

Exercice 1.

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

Par le théorème chinois, 19 est un carré modulo 505 ssi c'est un carré modulo 5 et modulo 101. $19 \equiv 4 \mod 5$ *est un carré mod 5.* $\left(\frac{19}{101}\right) = \left(\frac{101}{19}\right)$ *car* $101 \equiv 1 \mod 4$, $\left(\frac{101}{19}\right) = \left(\frac{6}{19}\right) = \left(\frac{25}{19}\right) = 1$ *puisque* 25 *est un carré. Donc 19 est un carré modulo* 101, *modulo* 5 *et donc modulo* 505.

---

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

Le discriminant de cette équation est $\Delta = 8^2 - 4 \times 3 \times 7 = -20$.

$$\left(\frac{-20}{113}\right) = \left(\frac{-5}{113}\right)\left(\frac{4}{113}\right) = \left(\frac{-5}{113}\right) = \left(\frac{5}{113}\right)$$

car $113 \equiv 1 \mod 4$. *On a donc*

$$\left(\frac{5}{113}\right) = \left(\frac{113}{5}\right) = \left(\frac{3}{5}\right) = -1$$

donc Δ *n'est pas un carré modulo 113.*
On en déduit que l'équation $3x^2-8x+7 = 0$ *n'a pas de solution dans* $\mathbb{Z}/113\mathbb{Z}$. *(En effet, si* x *était une solution de* $ax^2+bx+c = 0$ *avec* $a \neq 0$ *dans* $\mathbb{Z}/p\mathbb{Z}$ *avec* p *impair, on aurait* $(x+\frac{b}{2a})^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0$ *i.e.* $(x-\frac{b}{2a})^2 - \frac{b^2-4ac}{4a^2} = 0$ *donc* $\Delta = 4a^2(x-\frac{b}{2a})^2$ *serait un carré.)*

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 ?

La matrice de $\vec{u}, \vec{v}$ *dans la base canonique est* $\begin{pmatrix} 1 & 1+\sqrt{2} \\ 1 & 1-\sqrt{2} \end{pmatrix}$ *son déterminant est* $(1-\sqrt{2}) - (1+\sqrt{2}) = -2\sqrt{2}$, *donc le covolume de* L *est* $2\sqrt{2}$.

---

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

Il suffit de développer

$$||x\vec{u}+y\vec{v}||^2 = || \begin{pmatrix} x \\ x \end{pmatrix} + \begin{pmatrix} y(1+\sqrt{2}) \\ y(1-\sqrt{2}) \end{pmatrix} ||^2 = (x+y(1+\sqrt{2}))^2+(x+y(1-\sqrt{2}))^2 = 2x^2+6y^2+4xy = 2q(x,y)$$

---

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 $(\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}$?

Soit $(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}$ qui satisfait l'équation $q(x,y) = 0$. Si on avait $y = 0$, alors on aurait $x^2 = 0$, donc $(x,y) = (0,0)$, une contradiction. Donc $y \neq 0$. On écrit alors $0 = q(x,y) = (x+y)^2 + 2y^2$ donc $-2 = \frac{(x+y)^2}{y^2}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Réciproquement si $-2 = a^2$ est un carré modulo p, on pose $y = 1$, et $x = a - 1$, et on a bien $(x+y)^2 + 2y^2 = a^2 + 2 = 0$.

Maintenant, -2 est bien un carré modulo 2. Pour $p > 2$, on a $\left(\frac{-2}{p}\right) = (-1)^{p(p-1)/2}(-1)^{(p^2-1)/4}$. Ceci s'exprime comme un congruence modulo 8 : $p = 1$ ou $p = 3$ modulo 8.

---

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_α.

Soit $\phi : L \to \mathbb{Z}/p\mathbb{Z}$ définie par $(x,y) \mapsto x - \alpha y$, de sorte que $L_\alpha = \ker \phi$. Ce morphisme est surjectif, donc son image est de cardinal p, son noyau est d'indice p.donc $[L : L_\alpha] = p$ donc $Vol(L_\alpha) = pVol(L) = 2p\sqrt{2}$.

---

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

Le théorème de Hermite dit qu'il existe $\vec{w} \in L_\alpha \setminus \{0\}$ tq $||\vec{w}||^2 \leq \frac{2}{\sqrt{3}}.Vol(L_\alpha) = \frac{4p\sqrt{2}}{\sqrt{3}} < 4p$.

---

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

Soit p congru à 1 ou 3 modulo 8. Si $\vec{w} = x\vec{u} + y\vec{v} \in L_\alpha$, on a $x = \alpha y \pmod p$ donc $||\vec{w}||^2 = 2q(x,y) = 2(\alpha^2 + 2\alpha + 3)y^2 \pmod p$.

On veut donc que α satisfasse l'équation $\alpha^2 + 2\alpha + 3 = 0[p]$, ie $(\alpha+1)^2 + 2 = 0$. Cette equation a bien une solution parce que -2 est un carré modulo p puisque $p \equiv 1$ ou $p \equiv 3 \pmod 8$.

Soit L_α le réseau correspondant et $\vec{w} \in L_\alpha \setminus \{0\}$ tel que $||\vec{w}||^2 < 4p$. On a donc $0 < 2q(x,y) < 4p$, donc $0 < q(x,y) < 2p$, or $q(x,y) \equiv 0 \pmod p$, donc $q(x,y) = p$.

L'enoncé demandait en fait de montrer l'existence de (x,y) tel que $q(x,y) = 2p$. Un calcul direct montre que si $q(x,y) = p$, alors $q(y-x, y+x) = 2p$.

On peut aussi dire que $q(1,-1) = 2$, et que l'ensemble des valeurs prises par q est stable par multiplication. En effet, $q(x,y) = (x+y)^2 + 2y^2 = (x+y+iy\sqrt{2})(x+y-iy\sqrt{2}) = z\bar{z} = N(z)$ avec $z = x+y+iy\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Puisque $N(zz') = N(z)N(z')$, et que tous les elements de $\mathbb{Z}[\sqrt{2}]$ peuvent s'ecrivent $z = x + y + iy\sqrt{2}$ avec $x, y \in \mathbb{Z}$, l'ensemble des valeurs prises par q est stable par multiplication.

Une autre méthode, consiste a considerer L'_α comme les elements $x\vec{u}+y\vec{w} \in L_\alpha$ tels que $x = y \mod 2$. Il est d'indice $2p$ dans L, et ses elements $\vec{w}$ verifient $2q(x,y) = ||\vec{w}||^2 = 0[4p]$. On montre comme dans la question ci dessus qu'il existe $\vec{w}$ tq $||\vec{w}||^2 < 8p$, donc qu'il existe $\vec{w}$ tq $||\vec{w}||^2 = 4p$, donc il existe $x, y \in \mathbb{Z}$ tel que $q(x,y) = 2p$.

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 $a_5 = 5 + 11i$.

$73 \equiv 1 \mod 4$, *donc* 73 *n'est irréductible pas dans* $\mathbb{Z}[i]$. *Sa décomposition en produit d'irréductible est* $73 = 8^2 + 3^2 = (8 + 3i)(8 - 3i)$.

$75 = 3 * 5^2$, 3 *est irréductible dans* $\mathbb{Z}[i]$, *et* $5 = (1+2i)(1-2i)$. *Donc* $75 = 3(1+2i)^2(1-2i)^2$.

$77 = 11 * 7$ *est une décomposition en irréductibles puisque* 11 *et* 7 *sont congrus à* $-1 \mod 4$.

$N(4 + 5i) = 16 + 25 = 41$ *est un nombre premier, donc* $4 + 5i$ *est irréductible.*

$N(5 + 11i) = 25 + 121 = 146 = 2 * 73$. *Comme* $2 = (1 + i)(1 - i)$ *divise* $a_5\bar{a}_5$, $1 + i$ *divise* a_5 *ou* $\bar{a}_5$, *et comme* $1 + i$ *est associé à son conjugué* $1 - i$, *on a forcément que* $1 + i$ *divise* a_5. *D'ailleurs,* $\frac{5+11i}{1+i} = \frac{(5+11i)(1-i)}{2} = 8 + 3i$. $8 + 3i$ *est irréductible puisque sa norme est le nombre premier 73. Donc* $5 + 11i = (1 + i)(8 + 3i)$ *est la décomposition en produit d'irréductibles.*