UNIVERSITÉ DE RENNES 1

Théorie des nombres

Correction du devoir surveillé

Durée 1h20. Documents et calculatrice autorisés.

Exercice 1.

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 $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{C}$, 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, $n \geq 0$.

   Solution. $|\alpha|^2 = (x + \frac{y}{2})^2 + (\frac{\sqrt{3}}{2}y)^2 = x^2 + xy + y^2 = q(x, y)$.
   Comme $|\alpha|^2 \geq 0$, *si* $n = q(x, y)$, $n \geq 0$.

2. Montrer que l'ensemble des entiers qui s'écrivent sous la forme $n = x^2 + xy + y^2$ est stable par produit.

   Solution. *Supposons que* $n = |\alpha|^2$, *et* $m = |\beta|^2$ *avec* $\alpha, \beta \in \Gamma$. *Alors* $nm = |\alpha\beta|^2$. *Il suffit donc de montrer que* Γ *est stable par multiplication. Mais puisque* $\omega^2 = \omega - 1 \in \Gamma$, *pour tout* $x, y, x', y' \in \mathbb{Z}$,

   $$(x + y\omega)(x' + y'\omega) = xx' + (xy' + x'y)\omega + yy'\omega^2 \in \Gamma$$

3. Les entiers 2 et 3 peuvent-ils s'écrire sous cette forme ?

   Solution. $3 = q(1, 1)$ *s'écrit bien sous cette forme. Par contre,* 2 *ne s'ecrit pas sous cette forme. En effet, si* $2 = q(x, y)$, *alors* $q(x, y) = 0[2]$. *Mais en essayant les 4 possibilités, on voit que la seule solution de* $q(x, y) = 0[2]$ *dans* $\mathbb{Z}/2\mathbb{Z}$ *est* $x = y = 0[2]$. *Mais ceci implique que* x^2, y^2, xy *sont multiples de* 4, *donc* $4|q(x, y)$, *donc* $q(x, y) \neq 2$.

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...)

   Solution. *Pour tout* $\bar{x}, \bar{y} \in \mathbb{Z}/p\mathbb{Z}$, *on a* $\bar{x}^2 + \bar{x}\bar{y} + \bar{y}^2 = (\bar{x} + \bar{y}/\bar{2})^2 - \bar{y}^2/\bar{4} + \bar{y}^2 = (\bar{x} + a\bar{y})^2 + (1 - \bar{a}^2)\bar{y}^2[p]$. *Donc si* $q(x, y) = p$, *on a* $(x + ay)^2 = (a^2 - 1)y^2 = 0[p]$. *Si* $y \neq 0[p]$, *on en deduit que* $(a^2 - 1) = (x + ay)^2 y^{-2}[p]$ *et que* $a^2 - 1$ *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$. *Mais si* $y = 0[p]$, *alors* $x = 0[p]$, *et* $p^2|q(x, y)$, *ce qui contredit* $q(x, y) = p$..

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.

Solution. $a^2-1=0[p]$ *ssi* $a^2=1[p]$ *ssi* $4a^2=4[p]$ *(car* $p\neq 2$ *donc* 4 *inversible) ssi* $1=4[p]$ *ssi* $3=0[p]$ *ssi* $p|3$. *Comme* $p\geq 5$, $a^2-1\neq 0[p]$.
Dans $\mathbb{Z}/p\mathbb{Z}$, $a^2-\bar{1}=(\bar{1}/\bar{2})^2-\bar{1}=\frac{-\bar{3}}{4}$. *Puisque* $4=2^2$ *est un carré,* a^2-1 *est un carré de* $\mathbb{Z}/p\mathbb{Z}$ *ssi* -3 *est un carré de* $\mathbb{Z}/p\mathbb{Z}$.

6. Quels sont les nombres premiers tels que -3 soit un carré modulo p ? -3 est-il un carré modulo le nombre premier 1201 ?

Solution. -3 *est un carré modulo* p *ssi* $\left(\frac{-3}{p}\right)=0$ *ou* $\left(\frac{-3}{p}\right)=1$. *Comme* p *est premier et* $p\geq 5$, *le premier cas n'est pas possible. Mais on a* $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$ *car* $3=-1 \pmod 4$, *ie* $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$. *Ainsi,* -3 *est un carré modulo* p *ssi* $p=0$ *ou* $p=1 \mod 3$, *la premiere eventualite n'etant pas possible si* $p\geq 5$.

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 $\alpha\in\Gamma'$, $|\alpha|^2=0 \pmod p$

Solution. *On a* $|alpha|^2=x^2+xy+y^2=((b-a)y)^2+y(b-a)y+y^2$. *Modulo* p, *on obtient* $|alpha|^2=y^2(b^2+a^2-2ab+b-a+1)=y^2(2a^2-2ab+b-a)[p]$ *puisque* $b^2=a^2-1$. *Comme* $2a=1$, *on obtient* $|alpha|^2=(a-b+b-a)=0[p]$.

8. Determiner le covolume de Γ'.

Solution. *Puisque* Γ *a pour base* $1,\omega$, *son covolume est*

$$Vol(\Gamma)=|\det\begin{pmatrix}1 & 1/2\\ 0 & \frac{\sqrt{3}}{2}\end{pmatrix}|=\frac{\sqrt{3}}{2}.$$

On a $\Gamma'=\ker\phi$, *avec* $\phi:\Gamma\to\mathbb{Z}/p\mathbb{Z}$ *definie par* $x+\omega y\mapsto\bar{x}+(a-b)\bar{y}$. ϕ *est clairement surjectif, donc* $[\Gamma:\Gamma']=p$, *et* $Vol(\Gamma')=pVol(\Gamma)$.
Autre méthode en trouvant une base de Γ' *:* $x+y\omega\in\Gamma'$ *ssi* $x=(b-a)y+kp$ *pour un certain* $k\in\mathbb{Z}$. *Donc* Γ' *est l'ensemble des* $[(b-a)y+kp]+y\omega=[(b-a)+\omega]y+kp$ *pour* $y,k\in\mathbb{Z}$. Γ' *est donc engendré par* p *et* $(b-a)+\omega$. *Comme cette famille est libre, c'est une base de* Γ'. *Ainsi,*

$$Vol(\Gamma')=|\det\begin{pmatrix}p & b-a+1/2\\ 0 & \frac{\sqrt{3}}{2}\end{pmatrix}|=p\frac{\sqrt{3}}{2}.$$

9. Montrer qu'il existe $\alpha\in\Gamma'\setminus\{0\}$ tel que $|\alpha|^2\leq p$.

Solution. *D'après le Th de Hermite, il existe* $\alpha\in\Gamma'\setminus\{0\}$ *tel que* $|\alpha|^2\leq(\frac{2}{\sqrt{3}})Vol(\Gamma')=p$.

10. Quels sont les nombres premiers p qui peuvent s'écrire sous la forme $n=x^2+xy+y^2$, avec $x,y\in\mathbb{Z}$?

Solution. *Pour* $p\geq 5$, *on a vu que si* p *s'ecrivait sous cette forme, alors* $p\equiv 1[3]$ *(questions 4,5,6). Réciproquement, si* $p\equiv 1[3]$, *la question* 9 *montre l'existence de* $x,y\in\mathbb{Z}$ *tel que* $q(x,y)\leq p$. *Or* $p|q(x,y)$ *d'apres 8, donc* $q(x,y)=p$, *et* p *s'ecrit bien sous la forme voulue. Pour* $p<5$, *on a vu que* 2 *ne pouvait pas s'ecrire sous cette forme, mais* 3 *oui.*
Conclusion : p *s'ecrit sous cette forme si et seulement si* $p\equiv 0$ *ou* $p\equiv 1[3]$.

11. Déterminer tous les entiers n qui peuvent s'écrire sous la forme $n = x^2 + xy + y^2$ avec $x, y \in \mathbb{Z}$.

Solution. *D'apres la question 2, l'ensemble E de ces entiers n est stable par produit. Or si n est un carré dans $\mathbb{Z}$, $n = x^2 = q(x, 0)$ donc $n \in E$. En particulier, si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec α_i pair dès que $p_i = -1 \mod 3$, alors $n \in E$.*

On a montré que l'ensemble F des entiers dont la décomposition en facteurs premiers est comme ci-dessus est contenu dans E Pour montrer l'inclusion reciproque supposons que $E \setminus F$ soit non vide, et soit n le plus petit element de $E \setminus F$. Puisque $n \notin F$, il y a un nombre premier tel que $n = p^k n'$ avec n' premier avec p, k impair, et $p = -1 \mod 3$. Puisque $n \in E$, ecrivons $n = q(x, y)$, et ecrivons $x = p^k x'$ et $y = p^l y'$ avec x', y' premiers avec p. Si $k \geq 1$ et $l \geq 1$, alors $p^2 | n$, et $\frac{n}{p^2} = q(\frac{x}{p}, \frac{y}{p})$, donc $\frac{n}{p^2} \in E$. Donc $\frac{n}{p^2} \in E \setminus F$ et ce qui contredit le choix de n minimal. Quitte a échanger les rôles de x et y, on peut supposer y premier avec p. Alors en regardant modulo p, on obtient comme dans la question 4 que $a^2 - 1$ est un carré modulo p, ce qui contredit que $p = -1 \mod 3$ d'apres les questions 5,6.

Exercice 2.

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 $N(\alpha) = \pm 1$.

Solution. *Pour $\alpha = x + y\sqrt{3}$, notons $\overline{\alpha} = x - \sqrt{3}y$. Un calcule elementaire montre que $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$. On a $N(\alpha) = \alpha\overline{\alpha}$, donc $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$.*

Si $\alpha \in R^\times$ d'inverse β, alors $N(\alpha), N(\beta) \in \mathbb{Z}$ verifient $N(\alpha)N(\beta) = 1$, donc $N(\alpha)$ inversible dans $\mathbb{Z}$ donc $N(\alpha) = \pm 1$.

Reciproquement, si $\alpha \in R$ est tel que $N(\alpha) = \pm 1$, alors $\alpha\overline{\alpha} = \pm 1$, donc $\pm\overline{\alpha}$ est un inverse de α dans R, donc $\alpha \in R^\times$.

2. Existe-t-il $\alpha \in R$ tel que $N(\alpha) = -1$?

Solution. *Non. En effet, si $x^2 - 3y^2 = -1$, alors $x^2 = -1 \pmod{]3}$ mais -1 n'est pas un carré dans $\mathbb{Z}/3\mathbb{Z}$.*

3. Montrer que R est euclidien pour la jauge euclidienne $|N(\alpha)|$.

Solution. *Soit $\alpha, \beta \in R$ avec $\beta \neq 0$. Soit $\tilde{q} = \alpha/\beta = \tilde{x} + \tilde{y}\sqrt{3} \in K$ avec $\tilde{x}, \tilde{y} \in \mathbb{Q}$. Soient $x, y \in \mathbb{Z}$ des entiers tels que $|x - \tilde{x}| \leq \frac{1}{2}$ et $|y - \tilde{y}| \leq \frac{1}{2}$. Soit $q = x + y\sqrt{3}$, et $r = \alpha - q\beta$. Pour montrer que q, r verifient bien la condition de division euclidienne pour la jauge $\alpha \mapsto |N(\alpha)|$, il faut verifier que $|N(r)| < |N(\beta)|$. Or $|N(r)| = |N(\alpha - q\beta)| = |N(\tilde{q}\beta - q\beta)| = |N(\beta)| \cdot |N(\tilde{q} - q)|$. Il suffit donc de verifier que $N(\tilde{q} - q) < 1$. Mais $N(\tilde{q} - q) = (\tilde{x} - x)^2 - 3(\tilde{y} - y)^2$. Ces deux quantites etant de signes opposes, on a*

$$-3/4 \leq -3(\tilde{y} - y)^2 \leq N(\tilde{q} - q) = (\tilde{x} - x)^2 - 3(\tilde{y} - y)^2 \leq (\tilde{x} - x)^2 \leq 1/4.$$

En particulier, $|N(\tilde{q} - q)| \leq 3/4 < 1$.