UNIVERSITÉ DE RENNES 1

Théorie des nombres

Interrogation 2 : corrigé

Question 1

Soit p un nombre premier. Montrer que s'il existe $x, y \in \mathbb{Z}$ tels que $p \mid (x^2 + 6y^2)$, alors :

- si $p \mid y$, alors $p^2 \mid (x^2 + 6y^2)$;
- si $p \nmid y$, alors -6 est un carré dans $\mathbb{F}_p$.

Si $p \mid y$, alors $p \mid y^2$, or $p \mid (x^2 + 6y^2)$, donc $p \mid x^2$. Or p est premier, donc $p \mid x$. Comme $p \mid x$ et $p \mid y$, on a $p^2 \mid x^2$ et $p^2 \mid y^2$, donc $p^2 \mid (x^2 + 6y^2)$.
Si $p \nmid y$, alors y est non nul dans $\mathbb{F}_p$, or on a $x^2 + 6y^2 \equiv 0 \pmod{p}$, donc $(xy^{-1})^2 \equiv -6 \pmod{p}$, donc -6 est un carré dans $\mathbb{F}_p$.

Question 2

Montrer que -6 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 2$, $p = 3$ ou $p \equiv 1, 5, 7$ ou $11 \pmod{24}$.

Par définition du symbole de Legendre, -6 est un carré dans $\mathbb{F}_p$ si et seulement si $\left(\frac{-6}{p}\right) = 0$ ou 1.
On a $\left(\frac{-6}{p}\right) = 0$ si et seulement si $p \mid (-6)$, i.e. si et seulement si $p = 2$ ou $p = 3$.
Si $p \notin \{2, 3\}$, on a :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$
$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) \quad \text{par réciprocité quadratique,}$$

donc, par multiplicativité du symbole de Legendre,

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{3}\right)$$
$$= \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases} \times \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv -1 \pmod 3, \end{cases}$$

donc

$$\left(\frac{-6}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1,5,7 \text{ ou } 11 \pmod{24} \\ -1 & \text{si } p \equiv -1,-5,-7 \text{ ou } -11 \pmod{24}. \end{cases}$$

On trouve donc que -6 est un carré $\mathbb{F}_p$ si et seulement si $p = 2$, $p = 3$ ou $p \equiv 1,5,7$ ou $11 \pmod{24}$.

Question 3

Montrer que pour tout $p \in \{2,3\}$, il existe des entiers $x, y \in \mathbb{Z}$ tels que $x^2 + 6y^2 = 2p$.

Pour $p = 2$, on a $2^2 + 6 \cdot 0^2 = 2 \cdot 2$, donc $x = 2$ et $y = 0$ conviennent.
Pour $p = 3$, on a $0^2 + 6 \cdot 1^2 = 2 \cdot 3$, donc $x = 0$ et $y = 1$ conviennent.

Question 4

On suppose désormais que p est un nombre premier qui vérifie $p \equiv 1,5,7$ ou $11 \pmod{24}$. Énoncer le théorème de Minkowski et montrer qu'il existe des entiers $x, y \in \mathbb{Z}$ tels que $x^2 + 6y^2 \in \{p, 2p, 3p\}$.

Théorème (Minkowski) : Soit Λ un réseau de $\mathbb{R}^n$, de volume V_Λ, et soit S un convexe symétrique borné de $\mathbb{R}^n$, de volume V_S. Si $V_S > 2^n V_\Lambda$, alors $\Lambda \cap S$ n'est pas réduit à $\{0\}$.

Comme $p \equiv 1,5,7 \text{ ou } 11 \pmod{24}$, d'après la question 2 il existe un $\alpha \in \mathbb{Z}$ tel que $\alpha^2 \equiv -6 \pmod{p}$. Considérons

$$\Lambda = \left\{(x,y) \in \mathbb{Z}^2 / y \equiv \alpha x \pmod{p}\right\}.$$

C'est un $\mathbb{Z}$-module libre, de base $(1,\alpha)$, $(0,p)$ (car tout $(x,y) \in \Lambda$ s'écrit de manière unique sous la forme $x(1,\alpha) + k(0,p)$, avec $k = \frac{y-\alpha x}{p} \in \mathbb{Z}$). Comme

$$\begin{vmatrix} 1 & 0 \\ \alpha & p \end{vmatrix} = p \neq 0,$$

c'est un réseau de $\mathbb{R}^2$, de volume p. Posons

$$S = \left\{(x,y) \in \mathbb{R}^2 / x^2 + 6y^2 \leqslant A\right\},$$

pour une certaine constante $A > 0$ qui sera ajustée par la suite. L'aire de S est $\frac{\pi A}{\sqrt{6}}$ (par exemple en appliquant la transformation $(x,y) \mapsto (x, \frac{y}{\sqrt{6}})$ au disque de centre 0 et de rayon $\sqrt{A}$, dont l'aire est πA). Si l'on a $\frac{\pi A}{\sqrt{6}} > 4p$, alors d'après le théorème de Minkowski il existe $(x,y) \in \Lambda \cap S$ avec $(x,y) \neq (0,0)$.
Un tel couple (x,y) vérifie $y \equiv \alpha x \pmod{p}$ (car $(x,y) \in \Lambda$), donc $x^2 + 6y^2 \equiv 0 \pmod{p}$ puisque $\alpha^2 \equiv -6 \pmod{p}$. D'autre part, $x^2 + 6y^2 > 0$ puisque $(x,y) \neq (0,0)$, et $x^2 + 6y^2 \leqslant A$ puisque $(x,y) \in S$. Si $A < 4p$, alors $x^2 + 6y^2 \in \{p, 2p, 3p\}$.

Il suffit donc de montrer qu'il existe un réel $A > 0$ tel que $\frac{\pi A}{\sqrt{6}} > 4p$ et $A < 4p$, c'est-à-dire

$$4\frac{\sqrt{6}}{\pi}p < A < 4p.$$

Comme $\frac{\sqrt{6}}{\pi} < 1$ (puisque $6 < 3^2 < \pi^2$), il est effectivement possible de trouver un tel réel A.

Question 5

Montrer que si $x^2 + 6y^2 = p$ alors $p \equiv 1$ ou $7 \pmod{24}$. (Indication : on pourra réduire modulo 3).

Si $x^2 + 6y^2 = p$, alors $p \equiv x^2 \pmod 3$, donc p est un carré modulo 3, donc $p \equiv 0$ ou $1 \pmod 3$. Or, par hypothèse, on a $p \equiv 1, 5, 7$ ou $11 \pmod{24}$, donc $p \equiv 1$ ou $7 \pmod{24}$ (puisque $3 \mid 24$ et $5 \equiv 11 \equiv -1 \pmod 3$).

Question 6

Montrer que si $x^2 + 6y^2 = 2p$ alors $p \equiv 5$ ou $11 \pmod{24}$.

Si $x^2 + 6y^2 = 2p$, alors $-p \equiv x^2 \pmod 3$, donc $-p$ est un carré modulo 3, donc $p \equiv 0$ ou $-1 \pmod 3$. Or, par hypothèse, on a $p \equiv 1, 5, 7$ ou $11 \pmod{24}$, donc $p \equiv 5$ ou $11 \pmod{24}$ (puisque $3 \mid 24$ et $7 \equiv 1 \pmod 3$).

Question 7

Montrer que si $x^2 + 6y^2 = 3p$ alors $p \equiv 5$ ou $11 \pmod{24}$. (Indication : on pourra montrer que $x = 3a$ pour un certain $a \in \mathbb{Z}$, puis diviser par 3 et réduire modulo 3).

Si $x^2 + 6y^2 = 3p$, alors $x^2 \equiv 0 \pmod 3$, donc $3 \mid x$ (puisque 3 est premier). Soit $a = \frac{x}{3}$. On a $(3a)^2 + 6y^2 = 3p$, donc $3a^2 + 2y^2 = p$, donc $p \equiv -y^2 \pmod 3$, donc $p \equiv 0$ ou $-1 \pmod 3$. Comme $p \equiv 1, 5, 7$ ou $11 \pmod{24}$, on a donc $p \equiv 5$ ou $11 \pmod{24}$ dans ce cas aussi.

Question 8

Montrer que si $x^2 + 6y^2 = 3p$ alors il existe $a, b \in \mathbb{Z}$ tels que $3a^2 + 2b^2 = p$.

Si $x^2 + 6y^2 = 3p$, alors $x^2 \equiv 0 \pmod 3$, donc $3 \mid x$ (puisque 3 est premier). Soit $a = \frac{x}{3}$, alors $(3a)^2 + 6y^2 = 3p$, donc $3a^2 + 2y^2 = p$. On a donc bien $3a^2 + 2b^2 = p$, avec $a = \frac{x}{3} \in \mathbb{Z}$ et $b = y$.

Question 9

On suppose qu'il existe $a, b \in \mathbb{Z}$ tels que $3a^2 + 2b^2 = p$. Montrer qu'il existe $x', y' \in \mathbb{Z}$ tels que $x'^2 + 6y'^2 = 2p$.

Soient $a, b \in \mathbb{Z}$ tels que $3a^2 + 2b^2 = p$. On a alors $6a^2 + 4b^2 = 2p$, donc $x'^2 + 6y'^2 = 2p$ avec $x' = 2b \in \mathbb{Z}$ et $y' = a \in \mathbb{Z}$.

Question 10

En considérant un nombre premier p explicite tel que l'équation diophantienne $x^2 + 6y^2 = p$ n'ait pas de solution, montrer que l'anneau $\mathbb{Z}[\sqrt{-6}]$ n'est pas factoriel.

Soit $p > 3$ un nombre premier tel que $x^2 + 6y^2 = p$ n'ait pas de solution. D'après les questions précédentes (en particulier la question 5), cela équivaut à $p \equiv 5$ ou $11 \pmod{24}$. En particulier, $p = 5$ convient.

D'après les questions 4, 8 et 9, il existe des entiers $x, y \in \mathbb{Z}$ tels que $x^2 + 6y^2 = 2p$. On a alors

$$2p = (x + y\sqrt{-6})(x - y\sqrt{-6}).$$

Montrons que ce sont deux factorisations distinctes en produit d'irréductibles dans l'anneau $\mathbb{Z}[\sqrt{-6}]$.

Si 2 était réductible dans $\mathbb{Z}[\sqrt{-6}]$, alors il existerait $a, b \in \mathbb{Z}[\sqrt{-6}] \setminus \mathbb{Z}[\sqrt{-6}]^\times$ tels que $ab = 2$. On aurait alors $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a)\,\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(2) = 4$ par multiplicativité de la norme, $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) \geqslant 0$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) \geqslant 0$ car la norme $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}$ est toujours positive, et $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a), \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) \neq \pm 1$ car a et b ne sont pas inversibles. On aurait donc $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) = \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = 2$. Si $a = u + v\sqrt{-6}$, avec $u, v \in \mathbb{Z}$, alors $u^2 + 6v^2 = \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) = 2$, et c'est impossible car on aurait $6v^2 \leqslant 2$ donc $v = 0$, donc $u^2 = 2$, et 2 n'est pas un carré. Donc 2 est irréductible dans $\mathbb{Z}[\sqrt{-6}]$.

Si p était réductible dans $\mathbb{Z}[\sqrt{-6}]$, alors il existerait $a, b \in \mathbb{Z}[\sqrt{-6}] \setminus \mathbb{Z}[\sqrt{-6}]^\times$ tels que $ab = p$. On aurait alors $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a)\,\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = p^2$, et $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a), \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) > 1$ (comme dans le cas précédent), donc $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) = \mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = p$. Il existerait $u, v \in \mathbb{Z}$ tels que $a = u + v\sqrt{-6}$, et donc $u^2 + 6v^2 = p$. Or, p a été choisi de sorte qu'il n'existe pas d'entiers u, v vérifiant cette dernière égalité. Donc p est irréductible dans $\mathbb{Z}[\sqrt{-6}]$.

Si $x \pm y\sqrt{-6}$ était réductible dans $\mathbb{Z}[\sqrt{-6}]$, alors il existerait $a, b \in \mathbb{Z}[\sqrt{-6}] \setminus \mathbb{Z}[\sqrt{-6}]^\times$ tels que $ab = x \pm y\sqrt{-6}$. On aurait alors $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a)\,\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = x^2 + 6y^2 = 2p$, donc (comme ci-dessus) $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) = 2$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = p$, ou $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(a) = p$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}(b) = 2$. Or on a montré (dans les deux cas précédents) qu'il n'y a pas d'élément de norme 2 ou p dans $\mathbb{Z}[\sqrt{-6}]$. Donc $x \pm y\sqrt{-6}$ sont irréductible dans $\mathbb{Z}[\sqrt{-6}]$.

Finalement, $u + v\sqrt{-6} \in \mathbb{Z}[\sqrt{-6}]$ est inversible si et seulement si sa norme est ± 1, i.e. si et seulement si $u^2 + 6v^2 = 1$, donc $\mathbb{Z}[\sqrt{-6}]^\times = \{\pm 1\}$.

Supposons que 2 soit associé à l'un des irréductibles $x \pm y\sqrt{-6}$, alors on aurait $y = 0$ (puisque les éléments associés à 2 sont ± 2), donc $x^2 = 2p$. Comme on a pris $p \neq 2$, $2p$ n'est pas un carré donc c'est impossible. On a donc deux factorisations distinctes (même à permutation et multiplication par des inversibles près) en produit d'irréductibles pour l'élément $2p$ dans l'anneau $\mathbb{Z}[\sqrt{-6}]$. Cet anneau n'est donc pas factoriel.