THNO - interrogation 3 - corrigé

Exercice 1

1-

Supposons qu'il existe un couple $(x,y) \in \mathbb{Z}^2$ tel que $p \mid (x^2+5y^2)$

On a alors $x^2+5y^2 = 0$ dans $\mathbb{F}_p$.

Si $y = 0$ dans $\mathbb{F}_p$, alors $x = 0$ dans $\mathbb{F}_p$ donc $p \mid x$.

Si $y \in \mathbb{F}_p^\times$, alors $(xy^{-1})^2 = -5$ donc -5 est un carré dans $\mathbb{F}_p$.

2-

Supposons $p \neq 5$ et que -5 est un carré modulo p.

Soit $\alpha \in \mathbb{Z}$ tel que $\alpha^2 \equiv -5 \pmod p$.

On considère $\Lambda = \{ (x,y) \in \mathbb{Z}^2 \ / \ x - \alpha y \equiv 0 \pmod p \}$. C'est un sous-réseau de $\mathbb{Z}^2$,

dont une base est $\big((\alpha,1),(p,0)\big)$, donc son volume est $\left|\left| \begin{pmatrix} \alpha & p \\ 1 & 0 \end{pmatrix} \right|\right| = |-p| = p$.

Considérons maintenant l'ellipse $E = \{ (x,y) \in \mathbb{R}^2 \ / \ x^2+5y^2 \leq B \}$, pour un réel $B > 0$.

Son aire est $\pi \frac{B}{\sqrt{5}}$. D'après le théorème de Minkowski, si $\pi \frac{B}{\sqrt{5}} > 4p$, alors

$E \cap \Lambda$ contient un point autre que $(0,0)$.

Si $(x,y) \in (E \cap \Lambda) \setminus \{0\}$, on a $x^2+5y^2 \in]0, B]$,

et d'autre part $x - \alpha y \equiv 0 \pmod p$ donc $x^2 - \alpha^2 y^2 \equiv 0 \pmod p$,

donc $x^2+5y^2 \equiv 0 \pmod p$ donc $x^2+5y^2 \in p\mathbb{Z} \cap]0, B]$.

Si $B < 3p$, on aura alors $x^2+5y^2 \in \{p, 2p\}$.

On cherche donc un $B \in \mathbb{R}$ tel que $\pi \frac{B}{\sqrt{5}} > 4p$ et $B < 3p$,

c'est-à-dire $\frac{4\sqrt{5}}{\pi} p < B < 3p$. Un tel B existe si et seulement si $\frac{4\sqrt{5}}{\pi} < 3$,

or $80 < 81$ donc $4\sqrt{5} < 9$, et $3 < \pi$ donc $4\sqrt{5} < 3\pi$, donc $\frac{4\sqrt{5}}{\pi} < 3$.

Il existe donc un couple $(x,y) \in \mathbb{Z}^2$ tel que $x^2+5y^2 \in \{p, 2p\}$.

4

Montrons que $p = 2$ convient :

- $2p = 4 = 2^2 + 5 \cdot 0^2$
- si $2 = x^2+5y^2$ pour $(x,y) \in \mathbb{Z}^2$, on aurait $y^2 \leq \frac{2}{5}$ et $y^2 \in \mathbb{N}$ donc $y^2 = 0$,
  donc $x^2 = 2$, donc $|x| \leq \sqrt{2}$, donc $|x| \leq 1$ puisque $|x| \in \mathbb{N}$, donc $x^2 \leq 1$, d'où une contradiction.

3.

Montrons que $p = 5$ convient :

- $p = 5 = 0^2 + 5 \cdot 1^2$
- si $2p = 10 = x^2+5y^2$ pour $(x,y) \in \mathbb{Z}^2$, on aurait $y^2 \leq \frac{10}{5} = 2$ donc $|y| \leq \sqrt{2}$ donc $|y| \leq 1$,
  donc $y^2 \in \{0,1\}$; si $y^2 = 1$ on aurait $x^2 = 5$ et $\sqrt{5} \notin \mathbb{Z}$, si $y^2 = 0$ on aurait $x^2 = 10$
  et $\sqrt{10} \notin \mathbb{Z}$.

5_

Supposons qu'il existe un couple $(x,y) \in \mathbb{Z}^2$ tel que $x^2+5y^2 \in \{p, 2p\}$.

D'après la question 1_, on a alors $p=5$ ou $\left(\frac{-5}{p}\right)=1$,

or $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$

$= (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right)$ si $p \neq 2$

$= (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)$ si $p \neq 2$, car $5 \equiv 1 \pmod 4$ (réciprocité quadratique)

$= (-1)^{\frac{p-1}{2}} \cdot \begin{cases} 1 & \text{si } p \equiv 1 \text{ ou } 4 \pmod 5 \\ -1 & \text{si } p \equiv 2 \text{ ou } 3 \pmod 5 \end{cases}$ si $p \neq 2$

$= \begin{cases} 1 & \text{si } p \equiv 1, 3, 7 \text{ ou } 9 \pmod{20} \\ -1 & \text{si } p \equiv 11, 13, 17 \text{ ou } 19 \pmod{20} \end{cases}$

donc $p \in \{2,5\}$ ou $p \equiv 1, 3, 7$ ou $9 \pmod{20}$.

Réciproquement,

- si $p=2$, on a $2p = 2^2 + 5 \cdot 0^2$ (cf. question 4)
- si $p=5$, on a $p = 0^2 + 5 \cdot 1^2$ (cf. question 3)
- si $p \equiv 1, 3, 7$ ou $9 \pmod{20}$, on a $p \neq 5$ et $\left(\frac{-5}{p}\right) = 1$, donc $\exists (x,y) \in \mathbb{Z}^2$ $x^2+5y^2 \in \{p, 2p\}$ d'après la question 2.

Il existe donc un couple $(x,y) \in \mathbb{Z}^2$ tel que $x^2+5y^2 \in \{p, 2p\}$ si et seulement si $p \in \{2,5\}$ ou $p \equiv 1, 3, 7$ ou $9 \pmod{20}$.

(Il y avait une erreur dans l'énoncé : le cas $p=2$ était omis).

Il peut être intéressant de comparer ce sujet à celui de l'interrogation 1. Ici, l'anneau d'entiers à considérer est $\mathbb{Z}[\sqrt{-5}]$, et la norme est donnée par $N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(x+y\sqrt{-5}) = x^2+5y^2$. Le fait qu'il existe des nombres premiers $p \neq 2$ tels que $2p$ s'écrive sous la forme x^2+5y^2 mais pas p (question 4) montre que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel : on a $2p = (x-y\sqrt{-5})(x+y\sqrt{-5})$, et 2, p, $x-y\sqrt{-5}$, $x+y\sqrt{-5}$ sont irréductibles (considérer leur norme, et les normes possibles pour un diviseur). Si $y \neq 0$ (i.e. $p \neq 2$), on trouve deux factorisations distinctes pour le même élément. Par exemple, pour $p=3$, on trouve $2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$ (exemple vu en cours).