THNO - Examen - 1e session - corrigé

Exercice 1

1-

$\mathbb{F}_p^\times$ est un groupe (cyclique) de cardinal $p-1$, et $3 \mid p-1$,
donc, par le lemme de Cauchy, $\mathbb{F}_p^\times$ a un élément d'ordre 3.

2-

Comme x est d'ordre 3, on a

$x^3 - 1 = 0$ donc $(x-1)(x^2+x+1) = 0$

$x \neq 1$ donc $x - 1 \neq 0$,

donc $x^2 + x + 1 = 0$.

On a donc $(2x+1)^2 = 4x^2 + 4x + 1$
$= 4(x^2+x+1) - 3$
$= -3$

3-

D'après la question précédente, -3 est un carré dans $\mathbb{F}_p$,
et $p \nmid -3$ car $p \equiv 1 \pmod 3$, donc $\left(\frac{-3}{p}\right) = 1$.

Exercice 2

On a : $\exists (x,y) \in \mathbb{Z}^2 \quad y^2 = 41x + 3 \iff \exists y \in \mathbb{Z} \quad y^2 \equiv 3 \pmod{41}$
$\iff \left(\frac{3}{41}\right) \in \{0, 1\}$ (41 est premier),

or $\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right)$ car $41 \equiv 1 \pmod 4$ (réciprocité quadratique)

$= \left(\frac{-1}{3}\right)$ car $41 \equiv -1 \pmod 3$

$= (-1)^{\frac{3-1}{2}}$

$= -1$,

donc l'équation diophantienne $y^2 = 41x + 3$ n'a pas de solution.

Exercice 3

1-

Soit $n = p_1 p_2 \cdots p_k$ la décomposition de n en produit de facteurs premiers,
avec $p_1, p_2, \ldots, p_k$ des nombres premiers (non nécessairement distincts).

Comme $n \equiv 3 \pmod 4$, n est impair, donc $2 \notin \{p_1, \ldots, p_k\}$,

donc $\forall i \in \{1, \ldots, k\} \quad p_i \equiv 1$ ou $3 \pmod 4$

Si $\forall i \in \{1, \ldots, k\} \quad p_i \equiv 1 \pmod 4$, on aurait $n \equiv p_1 \cdots p_k \equiv 1^k \equiv 1 \pmod 4$,

or $n \not\equiv 1 \pmod 4$, donc $\exists i \in \{1, \ldots, k\} \quad p_i \equiv 3 \pmod 4$.

Il existe donc un diviseur premier p de n tel que $p \equiv 3 \pmod 4$.

2-

Si x était pair, on aurait $x^3 \equiv 0 \pmod 8$,
donc en particulier $x^3 \equiv 0 \pmod 4$,
donc $y^2 \equiv x^3 + 7 \equiv 3 \pmod 4$,
or les carrés modulo 4 sont 0 et 1, donc c'est impossible.
Donc x est impair.

3-

On a : $(x+2)\left((x-1)^2+3\right) = (x+2)(x^2-2x+4)$

$= x^3 + 2x^2 - 2x^2 - 4x + 4x + 8$

$= x^3 + 8$

4-

Soit $(x,y) \in \mathbb{Z}^2$ tel que $y^2 = x^3 + 7$.
On a alors $y^2 = (x+2)\left((x-1)^2+3\right) - 1$ d'après la question 3.
Comme x est impair, on a $(x-1)^2 \equiv 0 \pmod 4$ donc $(x-1)^2 + 3 \equiv 3 \pmod 4$.
D'après la question 1, il y a donc un nombre premier p tel que $p \mid (x-1)^2+3$ et $p \equiv 3 \pmod 4$.
On a alors $y^2 \equiv (x+2)\left((x-1)^2+3\right) - 1 \equiv (x+2)\cdot 0 - 1 \equiv -1 \pmod p$,
donc $\left(\frac{-1}{p}\right) = 1$,
or $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$ car $p \equiv 3 \pmod 4$, donc c'est impossible.
L'équation diophantienne $y^2 = x^3 + 7$ n'a donc pas de solution.

Exercice 4

1-

Le discriminant de la base $1, \zeta, \zeta^2, \dots, \zeta^{p-2}$ de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$ est par définition le carré du déterminant de la matrice $\left(\sigma_j(\zeta^i)\right)_{\substack{0 \le i \le p-2 \\ 0 \le j \le p-2}}$,
où $\sigma_0, \sigma_1, \dots, \sigma_{p-2}$ sont les $p-1$ plongements de $\mathbb{Q}(\zeta)$ dans $\mathbb{C}$.

Comme $\zeta, \zeta^2, \dots, \zeta^{p-1}$ sont les $p-1$ racines distinctes de $X^{p-1} + X^{p-2} + \dots + 1 = \frac{X^p - 1}{X - 1}$ dans $\mathbb{C}$,
ces plongements sont donnés par $\sigma_j(\zeta) = \zeta^{j+1}$, et on a

$$\Delta = \begin{vmatrix} 1 & \zeta & \zeta^2 & \dots & \zeta^{p-2} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2(p-2)} \\ 1 & \zeta^3 & \zeta^6 & \dots & \zeta^{3(p-2)} \\ \vdots & \vdots & \vdots & & \\ 1 & \zeta^{p-1} & \zeta^{(p-1)2} & \dots & \zeta^{(p-1)(p-2)} \end{vmatrix}^2$$

$$= \left(\prod_{1 \le i < j \le p-1} (\zeta^j - \zeta^i) \right)^2 \qquad \text{(déterminant de Vandermonde)}$$

$$= (-1)^{(p-2)+(p-3)+\dots+1} \prod_{1 \le i < j \le p-1} (\zeta^i - \zeta^j) \cdot \prod_{1 \le i < j \le p-1} (\zeta^j - \zeta^i)$$

$$= (-1)^{\frac{(p-2)(p-1)}{2}} \prod_{\substack{1 \le i, j \le p-1 \\ i \ne j}} (\zeta^i - \zeta^j)$$

$$\Delta = (-1)^{\frac{p-1}{2}} \prod_{\substack{1 \le i, j \le p-1 \\ i \ne j}} (\zeta^i - \zeta^j) \qquad \text{car } p-2 \text{ est impair.}$$

2-

On a :

$$\Delta = (-1)^{\frac{p-1}{2}} \prod_{\substack{1 \le i,j \le p-1 \\ i \neq j}} (\zeta^i - \zeta^j) \qquad \text{d'après la question 1}$$

$$= (-1)^{\frac{p-1}{2}} \prod_{i=1}^{p-1} (\zeta^i)^{p-2} \prod_{\substack{1 \le i,j \le p-1 \\ i \neq j}} (1 - \zeta^{j-i})$$

$$= (-1)^{\frac{p-1}{2}} \zeta^{\frac{(p-1)p}{2}(p-2)} \left(\prod_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} (1 - \zeta^k) \right)^{p-2}$$

car chacun des facteurs $(1-\zeta^k)$ apparaît $p-2$ fois dans le produit $\prod_{\substack{i \neq j \\ 1 \le i,j \le p-1}} (1 - \zeta^{j-i})$

$$= (-1)^{\frac{p-1}{2}} \left(\prod_{k \in (\mathbb{Z}/p\mathbb{Z})^\times} (1 - \zeta^k) \right)^{p-2} \qquad \text{car } \tfrac{p-1}{2} \in \mathbb{Z},$$

3-

Or les $p-1$ racines (distinctes) de $X^{p-1} + X^{p-2} + \dots + 1$ sont $\zeta, \zeta^2, \dots, \zeta^{p-1}$,

donc $X^{p-1} + X^{p-2} + \dots + 1 = \prod_{k=1}^{p-1} (X - \zeta^k)$,

donc en particulier $p = \prod_{k=1}^{p-1} (1 - \zeta^k)$.

On trouve donc : $\Delta = (-1)^{\frac{p-1}{2}} p^{p-2}$.

4-

Pour $p = 3$, on trouve $\Delta = -3$, qui est sans facteur carré,

donc $(1, \zeta)$ est une base de $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$ formée d'entiers et dont le discriminant est sans facteur carré, donc c'est une base de l'anneau des entiers de $\mathbb{Q}(\zeta)$,

donc l'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$.

Notons que $\zeta = \frac{-1+\sqrt{-3}}{2}$ et $\mathbb{Z}[\zeta] = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$,

ce qui est cohérent avec les résultats connus sur les anneaux d'entiers des corps quadratiques ($-3 \equiv 1 \pmod 4$).

5-

Pour $p = 5$, on a $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^3) = -1$, car ζ et ζ^3 sont des racines du polynôme irréductible $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$,

donc $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\frac{1+\zeta+\zeta^3}{5}\right) = \frac{1}{5}\left(\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1) + \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) + \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^3)\right)$

$$= \frac{1}{5}(4 - 1 - 1)$$

$$= \frac{2}{5}$$

$$\notin \mathbb{Z},$$

donc $\frac{1+\zeta+\zeta^3}{5}$ n'est pas un entier algébrique.

Exercice 5

L'équation diophantienne $x^2 - 30y^2 = 1$ est une équation de Pell-Fermat. On utilise l'algorithme vu en cours pour trouver une unité fondamentale de $\mathbb{Z}[\sqrt{30}]$. Pour cela, on détermine le développement en fraction continue de $\sqrt{30}$.

$$\sqrt{30} = 5 + (\sqrt{30} - 5) = 5 + \frac{1}{\frac{\sqrt{30}+5}{5}}$$

$$\frac{5+\sqrt{30}}{5} = 2 + \left(\frac{\sqrt{30}-5}{5}\right) = 2 + \frac{1}{\sqrt{30}+5}$$

$$5+\sqrt{30} = 10 + \frac{1}{\frac{\sqrt{30}+5}{5}}, \text{ etc.}$$

On a donc $\sqrt{30} = 5 + \cfrac{1}{\left(2 + \cfrac{1}{10 + \cfrac{1}{\ddots}}\right)}$ (une période)

$5 + \frac{1}{2} = \frac{11}{2}$, et une unité fondamentale est $11 + 2\sqrt{30}$, associée à la solution $11^2 - 30 \cdot 2^2 = 1$. (La période est de longueur 2, qui est pair, donc il n'y a pas de solution à $x^2 - 30y^2 = -1$).

Les solutions de l'équation de Pell-Fermat $x^2 - 30y^2 = 1$ sont donc les couples $(x, y) = (\pm x_n, \pm y_n)$, où l'on a posé $x_n + y_n\sqrt{30} = (11 + 2\sqrt{30})^n$, $(x_n, y_n) \in \mathbb{Z}^2$, pour tout $n \in \mathbb{N}$.