THNO 2010 - 2011 Examen 2e session (10 juin 2011) : corrigé.

Exercice 1

Si $P \in \mathbb{Z}[X]$ et $x \in \mathbb{Z}$, alors $3P(x) + 2 \equiv 2 \pmod 3$,
or 2 n'est pas un carré modulo 3 (par exemple car $0^2 \equiv 0 \pmod 3$ et $1^2 \equiv (-1)^2 \equiv 1 \pmod 3$),
donc l'équation $y^2 = 3P(x) + 2$ n'a pas de solution $y \in \mathbb{Z}$.
On a donc $\{ P \in \mathbb{Z}[X] \ / \ \exists (x,y) \in \mathbb{Z}^2 \quad y^2 = 3P(x) + 2 \} = \emptyset$.

Exercice 2

1-
Par définition de p, on a $x^2 - x + 1 \equiv 0 \pmod p$,
donc $4x^2 - 4x + 4 \equiv 0 \pmod p$,
donc $(2x-1)^2 + 3 \equiv 0 \pmod p$,
donc $(2x-1)^2 \equiv -3 \pmod p$,
donc -3 est un carré modulo p.

2-
Comme -3 est un carré modulo p, on a $\left(\frac{-3}{p}\right) \in \{0, 1\}$, en notant $\left(\frac{-3}{p}\right)$ le symbole de Legendre.
Comme x ou $x-1$ est pair, on a $x^2 - x + 1 = x(x-1) + 1 \equiv 1 \pmod 2$, donc $p \neq 2$.
On a donc

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) \quad \text{par réciprocité quadratique} \\
&= \left(\frac{p}{3}\right) \\
&= \begin{cases} 0 & \text{si } p = 3 \\ 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv 2 \pmod 3 \end{cases}
\end{aligned}$$

donc $p = 3$ ou $p \equiv 1 \pmod 3$.

Exercice 3

Plusieurs réponses de difficulté comparable étaient possibles pour cet exercice. Voici deux solutions possibles.

1e solution

1-
Soit $Q \in \mathbb{Z}[X]$ et soit p un nombre premier qui ne divise pas le coefficient dominant de Q. Si la réduction de Q modulo p est irréductible dans $\mathbb{F}_p[X]$, alors Q est irréductible dans $\mathbb{Q}[X]$. En particulier, si le coefficient dominant de Q est 1 alors l'irréductibilité de Q mod p dans $\mathbb{F}_p[X]$ entraîne l'irréductibilité de Q dans $\mathbb{Z}[X]$.

2-
On a vu qu'il existe un corps $\mathbb{F}_{2^{100}}$ (rappel : cela peut être démontré en considérant un corps de décomposition de $X^{2^{100}} - X$ sur $\mathbb{F}_2$). Par le théorème de l'élément primitif, il y a un $\alpha \in \mathbb{F}_{2^{100}}$ tel que $\mathbb{F}_{2^{100}} = \mathbb{F}_2(\alpha)$. Soit $\bar{Q} \in \mathbb{F}_2[X]$ le polynôme minimal de α sur $\mathbb{F}_2$. Comme $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_2[X]/(\bar{Q})$, on a $\deg \bar{Q} = 100$; d'autre part le coefficient dominant de $\bar{Q}$ est $1 \in \mathbb{F}_2$. Soit $Q \in \mathbb{Z}[X]$ tel que la réduction de Q modulo 2 soit $\bar{Q}$, avec $\deg Q = 100$ et tel que le coefficient dominant de Q soit 1. Par le critère énoncé au 1-, le polynôme Q est un polynôme irréductible. Les racines de Q (par exemple dans un corps de rupture de Q) sont alors des entiers algébriques de degré 100.

2e solution

1-
(Critère d'Eisenstein) Soit $Q(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$, et soit p un nombre premier. On suppose que :

- $a_0, a_1, \dots, a_{n-1}$ sont des multiples de p
- a_0 n'est pas un multiple de p^2.

Alors Q est irréductible dans $\mathbb{Z}[X]$.

2.

On considère le polynôme $X^{100} - 2$. Comme $2 \mid 2$, $2 \mid 0$, $4 \nmid 2$, le critère d'Eisenstein montre que ce polynôme est irréductible dans $\mathbb{Z}[X]$. Comme il est à coefficients entiers, de coefficient dominant 1, et irréductible, ses racines (par exemple dans un corps de rupture) sont des entiers algébriques de degré $\deg(X^{100} - 2) = 100$.

Exercice 4

Rappelons que :

- $\cos \frac{\pi}{3} = \frac{1}{2}$
- $\forall (a, b) \in \mathbb{R}^2 \quad \cos(a+b) = \cos a \cos b - \sin a \sin b$,
  donc en particulier $\forall \theta \in \mathbb{R} \quad \cos(2\theta) = \cos^2\theta - \sin^2\theta$
  $= 2\cos^2\theta - 1$.

On a donc $2\cos^2\frac{\pi}{6} - 1 = \frac{1}{2}$, i.e. $\cos\frac{\pi}{6}$ est racine de $4X^2 - 3$,

et $2\left(2\cos^2\frac{\pi}{12} - 1\right)^2 - 1 = \frac{1}{2}$ donc $\cos\frac{\pi}{12}$ est racine de $4(2X^2-1)^2 - 3 = 16X^4 - 16X^2 + 1$,

donc $\cos\frac{\pi}{12}$ est un nombre algébrique.

Montrons que le polynôme minimal de $\cos\frac{\pi}{12}$ est $16X^4 - 16X^2 + 1$, et donc que $\cos\frac{\pi}{12}$ n'est pas un entier algébrique. Pour cela, il suffit de montrer que $[\mathbb{Q}(\cos\frac{\pi}{12}) : \mathbb{Q}] = 4$.

Comme $2\cos^2\frac{\pi}{12} - 1 = \cos\frac{\pi}{6}$, on a $\mathbb{Q}(\cos\frac{\pi}{6}) \subset \mathbb{Q}(\cos\frac{\pi}{12})$, or $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$,

donc $[\mathbb{Q}(\cos\frac{\pi}{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, donc $2 \mid [\mathbb{Q}(\cos\frac{\pi}{12}) : \mathbb{Q}]$.

D'autre part, $[\mathbb{Q}(\cos\frac{\pi}{12}) : \mathbb{Q}] \leq 4$ puisque $\cos\frac{\pi}{12}$ est racine de $16X^4 - 16X^2 + 1$.

Il suffit donc de montrer que $[\mathbb{Q}(\cos\frac{\pi}{12}) : \mathbb{Q}] \neq 2$.

Si $[\mathbb{Q}(\cos\frac{\pi}{12}) : \mathbb{Q}] = 2$, le polynôme minimal de $\cos\frac{\pi}{12}$ sur $\mathbb{Q}$ donnerait un diviseur de $16X^4 - 16X^2 + 1$ de degré 2 à coefficients dans $\mathbb{Q}$. Or les **3** façons de regrouper les 4 racines de $16X^4 - 16X^2 + 1$ (dans $\overline{\mathbb{Q}}$) en deux facteurs de degré 2 sont :

$$16X^4 - 16X^2 + 1 = (4X^2 - 1)^2 - 8X^2 = (4X^2 - 2\sqrt{2}X - 1)(4X^2 + 2\sqrt{2}X - 1)$$
$$= (4X^2 + 1)^2 - 24X^2 = (4X^2 - 2\sqrt{6}X + 1)(4X^2 + 2\sqrt{6}X + 1)$$
$$= (4X^2 - 2)^2 - 3 = (4X^2 - 2 - \sqrt{3})(4X^2 - 2 + \sqrt{3})$$

et aucune de ces factorisations n'a ses coefficients tous dans $\mathbb{Q}$.

Le nombre algébrique $\cos\frac{\pi}{12}$ est donc de degré 4 sur $\mathbb{Q}$, son polynôme minimal est $16X^4 - 16X^2 + 1$, et ce n'est donc pas un entier algébrique.

Exercice 5

1-

Si $(x,y) \in \mathbb{N}^2$ vérifient $x^2+y^2 = p$,

on a $\begin{cases} x^2 \equiv 0 \text{ ou } 1 \pmod 4 \\ y^2 \equiv 0 \text{ ou } 1 \pmod 4 \end{cases}$,

donc $x^2+y^2 \equiv 0 \text{ ou } 1 \text{ ou } 2 \pmod 4$, donc $p \not\equiv 3 \pmod 4$.

Par contraposition, si $p \equiv 3 \pmod 4$, alors il n'existe pas d'entiers $x, y \in \mathbb{N}$ tels que $x^2+y^2 = p$.

2-

On a $(s^m)^{2^e} = s^{2^e m} = s^{p-1}$,

or $s \in \mathbb{F}_p^\times$ et le groupe $\mathbb{F}_p^\times$ est d'ordre $p-1$,

donc $s^{p-1} = 1$. L'entier $d = e \in \mathbb{N}$ convient donc.

3-

Si $x \in \mathbb{F}_p$, on a $x^2 = 1 \iff x^2 - 1 = 0$

$\iff (x-1)(x+1) = 0$

$\iff x-1 = 0 \text{ ou } x+1 = 0$ (car $\mathbb{F}_p$ est intègre)

$\iff x = 1 \text{ ou } x = -1$

donc les $x \in \mathbb{F}_p$ tels que $x^2 = 1$ sont 1 et -1.

4-

On note désormais d le plus petit entier naturel tel que $(s^m)^{2^d} = 1$.

Supposons $d \geq 2$, de sorte que $d-2 \geq 0$.

On a $(s^{2^{d-1}m})^2 = s^{2^d m} = 1$, et $s^{2^{d-1}m} \neq 1$ par minimalité de d,

donc $s^{2^{d-1}m} = -1$ d'après la question 3,

donc $(s^{2^{d-2}m})^2 = -1$, donc $(s^m)^{2^{d-2}}$ est une racine carrée de -1 dans $\mathbb{F}_p$.

5_

Si $d<2$, alors $d \in \{0,1\}$.

{ Si $d=0$, on a $s^m = 1$, donc $s^{2m}=1$.
Si $d=1$, on a $s^{2m}=1$.

Donc, si $d<2$, s est racine du polynôme $X^{2m}-1 \in \mathbb{F}_p[X]$.
Ce polynôme est de degré $2m$, donc il a au plus $2m$ racines dans $\mathbb{F}_p$.
Il y a donc au plus $2m$ éléments $s \in \mathbb{F}_p^\times$ tels que $d<2$.

6_

On considère l'application $\Phi : \begin{cases} \mathbb{Z}[i] \longrightarrow \mathbb{F}_p \\ a+ib \longmapsto a+\alpha b \end{cases}$. Comme $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module libre de base $(1,i)$, elle est bien définie.
On a :
- $\Phi(1) = \Phi(1+0i) = 1+0\alpha = 1$;
- si $a+ib$, $a'+ib' \in \mathbb{Z}[i]$, alors $\Phi\big((a+ib)+(a'+ib')\big) = \Phi\big((a+a')+i(b+b')\big)$
$= (a+a')+\alpha(b+b')$
$= (a+\alpha b)+(a'+\alpha b')$
$= \Phi(a+ib)+\Phi(a'+ib')$;
- si $a+ib$, $a'+ib' \in \mathbb{Z}[i]$, alors $\Phi\big((a+ib)(a'+ib')\big) = \Phi\big((aa'-bb')+i(ab'+a'b)\big)$
$= (aa'-bb')+\alpha(ab'+a'b)$
$= (a+\alpha b)(a'+\alpha b')$ car $\alpha^2=-1$
$= \Phi(a+ib)\,\Phi(a'+ib')$;

donc Φ est un morphisme d'anneaux.

7_

Comme Φ est un morphisme d'anneaux, $\ker\Phi$ est un idéal de $\mathbb{Z}[i]$.
On a $\Phi(p) = \Phi(p+0i) = p+0\alpha = 0$ dans $\mathbb{F}_p$,
et si $A \in \mathbb{Z}$ est un relèvement de $\alpha \in \mathbb{F}_p$, on a $\Phi(A-i) = \alpha - a = 0$,
donc $(p, A-i) \subseteq \ker\Phi$ (en notant $(p,A-i)$ l'idéal de $\mathbb{Z}[i]$ engendré par p et $A-i$).
Réciproquement, si $a+ib \in \ker\Phi$, alors $a+\alpha b = 0$ dans $\mathbb{F}_p$,
donc $a+Ab \equiv 0 \pmod p$, donc $a+ib = \underbrace{(a+Ab)}_{\in p\mathbb{Z}} - \underbrace{(A-i)b}_{\in (A-i)} \in (p, A-i)$,
donc $\ker\Phi \subseteq (p, A-i)$.
On a donc $\ker\Phi = (p, A-i)$.

8_

L'anneau $\mathbb{Z}[i]$ est euclidien, donc principal,
donc l'idéal $(p, A-i)$ est principal,
donc il existe un $g \in \mathbb{Z}[i]$ tel que $(p, A-i) = (g)$.

9_

1e solution

Comme $(g) = (p, A-i)$, on a $g \mid p$ dans $\mathbb{Z}[i]$,
donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) \mid N_{\mathbb{Q}(i)/\mathbb{Q}}(p)$ dans $\mathbb{Z}$, par multiplicativité de la norme,
c'est-à-dire $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) \mid p^2$. Comme $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) \geq 0$, on a donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) \in \{1, p, p^2\}$.
Si $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = 1$, alors g serait inversible dans $\mathbb{Z}[i]$, donc $\ker \Phi = (g) = \mathbb{Z}[i]$,
donc $\Phi = 0$, ce qui est faux puisque $\Phi(1) = 1 \neq 0$.
Si $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = p^2$, alors $N_{\mathbb{Q}(i)/\mathbb{Q}}\left(\frac{p}{g}\right) = 1$, donc $\frac{p}{g} \in \mathbb{Z}[i]^\times$, donc $(p) = (g)$,
or $A - i \in (g)$ donc $p \mid (A-i)$ dans $\mathbb{Z}[i]$,
donc $p \mid A$ et $p \mid (-1)$ dans $\mathbb{Z}$, or $p \nmid (-1)$ puisque p est premier.
On a donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = p$.

2e solution

Comme $\Phi|_{\mathbb{Z}}$ coïncide avec la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$,
le morphisme Φ est surjectif. Il induit donc un isomorphisme $\mathbb{Z}[i]/\ker\Phi \xrightarrow{\sim} \mathbb{F}_p$,
donc $\mathrm{Card}\left(\mathbb{Z}[i]/(g)\right) = p$.
Montrons que $\mathrm{Card}\left(\mathbb{Z}[i]/(g)\right) = \left|N_{\mathbb{Q}(i)/\mathbb{Q}}(g)\right|$. Comme $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module libre
de rang 2, et (g) en est un sous-$\mathbb{Z}$-module, il existe une base (e_0, e_1) de $\mathbb{Z}[i]$
et des entiers $d_0, d_1 \in \mathbb{Z}$ tels que $d_0 \mid d_1$ et $\mathbb{Z} d_0 e_0 + \mathbb{Z} d_1 e_1 = (g)$.
On a alors $\mathbb{Z}[i]/(g) \simeq \mathbb{Z}/d_0\mathbb{Z} \times \mathbb{Z}/d_1\mathbb{Z}$ comme $\mathbb{Z}$-modules,
donc $\mathrm{Card}\left(\mathbb{Z}[i]/(g)\right) = |d_0 d_1|$. En particulier, $d_1 \neq 0$, donc $(d_0 e_0, d_1 e_1)$ est une base
du $\mathbb{Z}$-module (g).
D'autre part, comme (e_0, e_1) est une base de $\mathbb{Z}[i]$, $(g e_0, g e_1)$ est une base de (g),
donc la matrice de passage de $(d_0 e_0, d_1 e_1)$ à $(g e_0, g e_1)$ est dans $GL_2(\mathbb{Z})$,
donc $\left|\det_{(d_0 e_0, d_1 e_1)}(g e_0, g e_1)\right| = 1$,
donc $\left|\det_{(e_0, e_1)}(g e_0, g e_1)\right| = \left|\begin{vmatrix} d_0 & 0 \\ 0 & d_1 \end{vmatrix} \cdot \det_{(d_0 e_0, d_1 e_1)}(g e_0, g e_1)\right| = |d_0 d_1|$,
or $\det_{(e_0, e_1)}(g e_0, g e_1)$ est le déterminant de l'endomorphisme de $\mathbb{Q}(i)$ donné par la
multiplication par g, c'est-à-dire $N_{\mathbb{Q}(i)/\mathbb{Q}}(g)$,
donc $\left|N_{\mathbb{Q}(i)/\mathbb{Q}}(g)\right| = |d_0 d_1| = \mathrm{Card}\left(\mathbb{Z}[i]/(g)\right) = p$.
Comme $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) \geq 0$, on a donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = p$.

10-

Si $g = a + ib$, avec $a, b \in \mathbb{Z}$,

alors $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = a^2 + b^2$, or $N_{\mathbb{Q}(i)/\mathbb{Q}}(g) = p$, donc $|a|^2 + |b|^2 = p$,

et $(|a|, |b|) \in \mathbb{N}^2$, donc le couple $(|a|, |b|)$ est une solution du problème des deux carrés.

11-

On a bien $97 \equiv 1 \pmod 4$. Plus précisément, $97 = 1 + 2^5 \cdot 3$,

donc $e = 5$ et $m = 3$ avec les notations de la question 2.

Prenons $s = 2 \in \mathbb{F}_{97}^\times$. On a bien $s^m = 8 \neq 1$ dans $\mathbb{F}_{97}$.

De plus, $8^2 \equiv 64 \equiv -33 \pmod{97}$

$8^4 \equiv 33^2 \equiv 1089 \equiv 22 \pmod{97}$

$8^8 \equiv 22^2 \equiv 484 \equiv -1 \pmod{97}$

$8^{16} \equiv (-1)^2 \equiv 1 \pmod{97}$,

donc $d = 4$ à la question 4, et 22 est une racine carrée de -1 dans $\mathbb{F}_{97}$.

On peut donc prendre $A = 22$ à la question 7.

On cherche maintenant un $g \in \mathbb{Z}[i]$ tel que $(97, 22 - i) = (g)$,

c'est-à-dire un PGCD de 97 et $22 - i$ dans $\mathbb{Z}[i]$.

L'anneau $\mathbb{Z}[i]$ étant euclidien, on peut utiliser l'algorithme d'Euclide.

$$\frac{97}{22-i} = \frac{97}{22^2+1}(22+i) = \frac{2134}{485} + \frac{97}{485}i = \frac{22}{5} + \frac{1}{5}i \qquad \frac{22}{5} = 4{,}4 \quad \frac{1}{5} = 0{,}2,$$

donc le quotient de 97 par $22 - i$ est 4, et le reste est $97 - 4 \cdot (22 - i) = 9 + 4i$.

$$\frac{22-i}{9+4i} = \frac{1}{9^2+4^2}(22-i)(9-4i) = \frac{1}{97}(196 - 97i) = 2 - i,$$

donc le quotient de $22 - i$ par $9 + 4i$ est $2 - i$ et le reste est 0.

Le PGCD de 97 et $22 - i$ est donc le dernier reste non nul obtenu,

c'est-à-dire $9 + 4i$.

On peut donc prendre $g = 9 + 4i$. D'après la question 10, une solution du problème des deux carrés est donc $(9, 4)$, et en effet on a bien $9^2 + 4^2 = 97$.