Examen du 31 janvier : corrigé

Ex 1 : 1) Montrons par l'absurde qu'il n'existe aucun tels entiers : Si c'était le cas on aurait $7(15a+10b+6c) = 30$ et alors $7 \mid 30$ ce qui est absurde.

b) Soient $m, n \in \mathbb{Z}$ et δ leur pgcd. Il existe une relation de Bezout $am+bn=\delta$ avec $a, b \in \mathbb{Z}$. Si d est un diviseur commun à m et n, alors $d \mid am$ et $d \mid bn$ d'où $d \mid am+bn = \delta$. cqfd.

Ex 2 : 1) si $p=2$, $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$ et $1^2 = 1$ donc il y a 1 carré dans $(\mathbb{Z}/2\mathbb{Z})^*$.
Si $p>2$, l'ens des carrés (c'est un sous groupe en fait) de $(\mathbb{Z}/p\mathbb{Z})^*$ est l'image du morphisme $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $x \mapsto x^2$.

Par le th d'isomorphisme, $\mathrm{Im}\,\varphi \simeq (\mathbb{Z}/p\mathbb{Z})^* / \ker \varphi$.

Or $\ker \varphi = \{ x \in (\mathbb{Z}/p\mathbb{Z})^*,\ x^2 = 1 \}$

le pol $X^2 - 1 \in \mathbb{F}_p(X)$ admet 2 racines évidentes 1 et -1 (et elles sont distinctes car $p \neq 2$).

Donc comme il est de degré 2, ce sont toutes ses racines et on a $\ker \varphi = \{+1, -1\}$.

On en déduit qu'il y a $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

2) D'après le petit th de Fermat, $\forall a \in (\mathbb{Z}/p\mathbb{Z})^*$, $a^{p-1} = 1$.
De plus, si x est un carré, $\exists a$ tq $x = a^2$ et donc $x^{\frac{p-1}{2}} = (a^2)^{\frac{p-1}{2}} = 1$.
Le pol $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p(X)$ admet donc pour racines les $\frac{p-1}{2}$ carrés de $(\mathbb{Z}/p\mathbb{Z})^*$.
Pour des raisons de degré, ce sont toutes ses racines et on a donc.

$x^{\frac{p-1}{2}} = 1$ ssi x est un carré.

Comme $\left(x^{\frac{p-1}{2}}\right)^2 = 1$, $x^{\frac{p-1}{2}} \in \{+1, -1\}$ et on a donc $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.

3) On a donc $\left(\frac{-1}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{2}} & \text{si } p \neq 2 \\ 1 \text{ car } -1=1 & \text{si } p=2 \end{cases} = \begin{cases} -1 & \text{si } \frac{p-1}{2} \text{ est impair} \\ 1 & \text{si } \frac{p-1}{2} \text{ est pair} \\ 1 & \text{si } p=2 \end{cases}$.

$= \begin{cases} -1 & \text{si } p \equiv 3 (4) \\ 1 & \text{si } p \equiv 1 (4) \\ 1 & \text{si } p=2 \end{cases}$. D'où le résultat.

4) Pour $p=2$, $-2=0$ est un carré de $\mathbb{Z}/2\mathbb{Z}$.

Si p est impair, on a $\left(\frac{-2}{p}\right) = (-2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$.

$\left(\frac{-1}{p}\right)$ ne dépend que des valeurs de p modulo 4 (et donc a fortiori mod 8)

$\left(\frac{2}{p}\right)$ ——— 8.

Donc $\left(\frac{-2}{p}\right)$ ——— 8 et on a.

p mod 8	1	3	5	7
$\left(\frac{-1}{p}\right)$	1	-1	1	-1
$\left(\frac{2}{p}\right)$	1	-1	-1	1
$\left(\frac{-2}{p}\right)$	1	1	-1	-1

On en déduit que -2 est un carré mod p ssi $p=2$ ou si $p \equiv 1$ ou 3 mod 8.

Exercice 3 : Partie I

1) N s'étend à $\mathbb{C}$ en $\mathbb{C} \to \mathbb{R}_+$, $z \mapsto |z|^2$ qui est clairement multiplicative.

2) A est intègre comme sous-anneau de $\mathbb{C}$ qui l'est.

De plus, Mq $A^\times = \{+1, -1\}$

Soit $z_1 \in A^\times$, $\exists z_2 \in A$ tq $z_1 z_2 = 1$. d'où $N(z_1)N(z_2) = 1$ (dans $\mathbb{N}$).

D'où $N(z_1) = 1$. Si $z_1 = a + ib\sqrt{2}$, on a $a^2 + 2b^2 = 1$ d'où $b=0$ et $a = \pm 1$.

Réciproquement, si $N(z_1) = 1$, comme $N(z_1) = \underset{\in A}{z_1} \underset{\in A}{\overline{z_1}}$

on a que $\overline{z_1}$ est l'inverse de z_1 dans A.

3) Soient z_1 et $z_2 \neq 0$ des éléments de A.
Montrons qu'il existe $q, r \in A$ tq $z_1 = qz_2 + r$ avec $N(r) < N(z_2)$
(et $N(r) = 0 \Leftrightarrow r = 0$.)

Travaillons dans $\mathbb{Q}(i\sqrt{2}) = \mathrm{Frac}(\mathbb{Z}[i\sqrt{2}]) \subset \mathbb{C}$.

L'élément $\frac{z_1}{z_2}$ s'écrit $\alpha + i\beta\sqrt{2}$ avec $\alpha, \beta \in \mathbb{Q}$.

Soient a et b "les" entiers les plus proches de α et β (ils ne sont pas toujours uniques, mais on en choisit un !)

On a $|a - \alpha| \leq \frac{1}{2}$ et $|b - \beta| \leq \frac{1}{2}$.

On a alors $\left|\frac{z_1}{z_2} - (a + ib\sqrt{2})\right|^2 = |a-\alpha|^2 + 2|b-\beta|^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$.

... Posons alors $q = a + ib\sqrt{2}$ et $r = z_1 - z_2 q$.

Par construction, on a $N(r) = N(z_2) N\left(\frac{z_1}{z_2} - q\right) < \frac{3}{4} N(z_2)$.

D'où le résultat !

4) A est donc euclidien et toutes ses paires d'éléments admettent un pgcd qui se calcule avec l'algorithme d'Euclide.

$z_1 = 7 + 2i\sqrt{2}$ $\quad N(z_1) = 49 + 8 = 57$.

$z_2 = -5 + 4i\sqrt{2}$ $\quad N(z_2) = 25 + 32 = 57$

$$\frac{z_1}{z_2} = \frac{(7+2i\sqrt{2})(-5-4i\sqrt{2})}{57} = \frac{(-35+16) - 38i\sqrt{2}}{57} \approx -i\sqrt{2} = q.$$

$$\rightsquigarrow z_1 + i\sqrt{2} z_2 = -1 - 3i\sqrt{2}. \quad N(r) = 1 + 2 \cdot 9 = 19.$$

Donc $z_1 = -iz_2 - (1 + 3i\sqrt{2})$ est donc une div eucl de z_1 par z_2.

5) Soit $z \in A$ tq $N(z) \in \mathcal{P}$.

Si z se factorise sous la forme $z = z_1 z_2$ avec $z_1, z_2 \in A$.

on a $p = N(z) = N(z_1) N(z_2)$ et comme p est premier.

$N(z_1) = 1$ ou $N(z_2) = 1$ i.e $z_1 = \pm 1$.

Donc z est bien irréductible dans A.

II

6) Si $p \in \Sigma$, p s'écrit a^2+2b ie $p = (a+ib\sqrt{2})(a-ib\sqrt{2})$

Cette factorisation est non triviale dans A car $a \pm ib\sqrt{2} = \pm 1$

$\Rightarrow$: $a = \pm 1$, $b = 0$ et donc $p = a^2 = 1$ pas premier.

Donc p est réductible dans A.

Réciproquement, si $p = \beta_1 \beta_2$ dans A, avec $\beta_1, \beta_2 \neq \pm 1$.

alors $N(p) = p^2 = N(\beta_1) N(\beta_2)$ avec $N(\beta_1) \neq 1 \neq N(\beta_2)$.

D'où $N(\beta_1) = p = N(\beta_2)$. et donc si $\beta_1 = a_1 + ib_1\sqrt{2}$, $p = a_1^2 + 2b_1^2$.

7) Comme A est euclidien, "irréductible = premier"

p est irréductible ssi p est premier $\Leftrightarrow$ $A/(p)$ est intègre.

Or $A \simeq \mathbb{Z}[X]/(X^2+2)$ et donc $A/(p) \simeq \mathbb{F}_p[X]/(X^2+2)$

Cet anneau est intègre ssi X^2+2 ($\in \mathbb{F}_p[X]$) est irréductible,

comme il est de degré 2 cela revient à s'assurer qu'il n'a pas de racine dans $\mathbb{F}_p$ ie -2 n'est pas un carré !

8) Dans A, on a $2 = -(i\sqrt{2})^2$

$3 = (1+i\sqrt{2})(1-i\sqrt{2})$

$5 = 5$ est irréductible dans A car les carrés de $\mathbb{Z}/5\mathbb{Z}$ sont $0, 1, -1$.

III

9) si $n = a^2+2b^2$, $n = N(\underbrace{a+ib\sqrt{2}}_{\beta})$ et $m = a'^2+2b'^2$, $m = N(\underbrace{a'+ib'\sqrt{2}}_{\beta'})$ alors $nm = N(\beta\beta')$ est aussi dans Σ.

10) Soit $n \in \Sigma$ et $p \mid n$ avec p irréductible dans A.

$\exists a, b \in \mathbb{Z}$, $n = a^2+2b^2 = (a+ib\sqrt{2})(a-ib\sqrt{2})$.

Comme p est premier dans A, $p \mid a+ib\sqrt{2}$ ou $p \mid a-ib\sqrt{2}$.

et donc $p \mid a$ et $p \mid b$. Comme $n = a^2+2b^2$, on a alors $p^2 \mid n$

et $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + 2\left(\frac{b}{p}\right)^2 \in \Sigma$.

11) Montrons $\Sigma = \{ n \in \mathbb{N}$ tq tous les facteurs premiers tq -2 n'est pas un carré mod p apparaissent avec un exposant pair $\}$.

⊃ : Les puisque Σ est stable par $\times$, il suffit de montrer que n est produit d'éléments de Σ.
pour les facteurs premiers réductibles, c'est vrai d'après 6) dans A.
pour les facteurs premiers irréductibles dans A, ils apparaissent avec une multiplicité paire disons 2α,
et $p^{2\alpha} = (p^\alpha)^2 + 2 0^2 \in \Sigma$.

$\subset$ Réciproquement, d'après 10), si $n \in \Sigma$, tous les facteurs premiers p de n tq -2 n'est pas un carré mod p sont tq $p^2 | n$. et $\frac{n}{p^2} \in \Sigma$.
Ceci implique par une récurrence immédiate que l'exposant de p dans n est pair.

Rq : Dans l'exercice 2, on a explicité les premiers p tq -2 n'est pas un carré mod p, ce sont les $p \equiv 5$ ou $7 \bmod 8$.