Examen du 31 janvier 2023

1 heure 30

La correction tiendra grandement compte de la clarté et de la concision de la rédaction.
L'utilisation de calculatrice, de téléphone portable et autre gadget est interdite.

Exercice 1. — Les questions de cet exercice sont indépendantes entre elles.

1) **[MG2012]** Soient $a, b, c, d \in \mathbf{Z}$. On pose $A = (a, b) \in \mathbf{Z}^2$ et $B = (c, d) \in \mathbf{Z}^2$. On note $[A, B]$ le segment de $\mathbf{R}^2$ d'extrémités A et B. Démontrer que

$$\mathrm{Card}\left([A, B] \cap \mathbf{Z}^2\right) = \mathrm{pgcd}(c - a, d - b) + 1$$

2) Soient $m, n > 1$ deux entiers *premiers entre eux* et $a \in \mathbf{Z}$.
Montrer que a est un carré dans $\mathbf{Z}/mn\mathbf{Z}$ ssi (a est un carré de $\mathbf{Z}/m\mathbf{Z}$ **et** a est un carré de $\mathbf{Z}/n\mathbf{Z}$).
Que dire lorsque m et n ne sont pas premiers entre eux ?

* *
*

Exercice 2 **(Agreg Docteur 2021).** — On se donne P et Q dans $\mathbf{Z}[X]$ premiers entre eux dans $\mathbf{Q}[X]$ et on pose, pour tout $n \in \mathbf{N}$,

$$u_n = \mathrm{pgcd}(P(n); Q(n)).$$

Le but de l'exercice est de montrer que $(u_n)_{n\in\mathbf{N}}$ est périodique.

1) Montrer qu'il existe $d \in \mathbf{N}^*$ tel que pour tout $n \in \mathbf{N}$, u_n divise d.
[**Indication:** On pourra utiliser le théorème de Bézout.]

2) Montrer, pour tous $R \in \mathbf{Z}[X]$ et $n \in \mathbf{N}$, que $R(n + d) - R(n)$ est divisible par d.

3) Conclure.

Exercice 3. — On note $\mathbf{Z}[i] := \{a + ib,\ a, b \in \mathbf{Z}\}$ l'anneau des entiers de Gauss et on note $N : \mathbf{Z}[i] \to \mathbf{N}; z \mapsto |z|^2$.

1) Montrer que $\mathbf{Z}[i]$ est un anneau principal.

2) Déterminer l'ensemble des éléments inversibles de $\mathbf{Z}[i]$.

3) Montrer que les éléments $1 + 2i$ et $1 - 2i$ sont deux irréductibles non associés de $\mathbf{Z}[i]$.

4) Montrer que l'élément 3 est irréductible dans $\mathbf{Z}[i]$.

Pour $n \in \mathbf{N}$, on note $\mathcal{C}(n)$ le nombre de façons d'écrire n comme somme de deux carrés dans $\mathbf{Z}$. Autrement dit :

$$\mathcal{C}(n) := \mathrm{Card}\{a, b \in \mathbf{Z}^2,\ n = a^2 + b^2\}.$$

5) Pour $k \geqslant 1$, déterminer $\mathcal{C}(5^k)$.

6) En déduire que la fonction $\mathcal{C}$ n'est pas bornée.

Pour $\gamma \in \mathbf{Z}[i]$, on note $\widetilde{\mathcal{C}}(\gamma)$ le nombre de façons d'écrire γ comme somme de deux carrés dans $\mathbf{Z}[i]$. Autrement dit :

$$\widetilde{\mathcal{C}}(\gamma) := \mathrm{Card}\{\alpha, \beta \in \mathbf{Z}[i]^2,\ \gamma = \alpha^2 + \beta^2\}.$$

7) Calculer $\widetilde{\mathcal{C}}(3)$ et $\widetilde{\mathcal{C}}(2 + i)$