DEVOIR MAISON N°4

L'ANNEAU $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n, autrement dit :

$$\begin{aligned}\overline{x} &= \{y \in \mathbb{Z} \mid y \equiv x \quad [n]\} \\ &= \{x + kn \mid k \in \mathbb{Z}\} \\ &= x + n\mathbb{Z}\end{aligned}$$

1) Soit $a, b \in \mathbb{Z}$. Montrer que $\overline{a} = \overline{b}$ si et seulement si $a \equiv b \quad [n]$.

En particulier, il y a n classes d'équivalences (distinctes) pour cette relation, à savoir :

$$\overline{0}, \quad \overline{1}, \quad \overline{2}, \ldots, \quad \overline{n-1}$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble qui contient ces n classes. On munit cet ensemble des lois $+$ et $\cdot$ suivantes :

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z} \qquad \overline{x} + \overline{y} = \overline{x+y}$$

$$\forall \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z} \qquad \overline{x} \cdot \overline{y} = \overline{xy}$$

Par exemple, si $n = 4$,

$$\overline{2} + \overline{2} = \overline{4} = \overline{0} \qquad \text{et} \qquad \overline{3} \cdot \overline{2} = \overline{6} = \overline{2}$$

2) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif. *On admettra que $+$ et $\cdot$ sont des l.c.i. et des applications bien définies.*

3) Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Montrer que $\overline{a}$ est inversible si et seulement si $a \wedge n = 1$.

4) En déduire que si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. De plus, donner un contre-exemple lorsque $n = 14$.

5) Déduire de la question 3 que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier. De plus, lorsque $n = 7$, donner un inverse de tous les éléments inversibles de $\mathbb{Z}/7\mathbb{Z}$.

Un autre éclairage sur les équations de congruences

Pour $a, c \in \mathbb{Z}$, on cherche à résoudre $ax \equiv c \quad [n]$ lorsque $a \wedge n = 1$.

- Par la question 1, cela équivaut à $\overline{ax} = \overline{c}$, ce qu'on peut réécrire en $\overline{a} \cdot \overline{x} = \overline{c}$.
- Puis, comme $a \wedge n = 1$, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, il existe $\overline{b}$ tel que $\overline{b} \cdot \overline{a} = \overline{1}$.
- On multiplie $\overline{a} \cdot \overline{x} = \overline{c}$ par $\overline{b}$ à gauche et on obtient

$$\begin{aligned}&\overline{b} \cdot \overline{a} \cdot \overline{x} = \overline{b} \cdot \overline{c} \\ \iff &\overline{1} \cdot \overline{x} = \overline{bc} \\ \iff &\overline{x} = \overline{bc}\end{aligned}$$

- Et enfin, cette équation équivaut à $x \equiv bc \quad [n]$, à nouveau par la question 1.