Devoir à la Maison

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

À rendre le lundi 28 février 2011

* * *

Soit n un entier naturel supérieur ou égal à 2. On rappelle que la relation d'égalité modulo n est une relation d'équivalence. Pour tout $i \in [\![0, n-1]\!]$, on note $\overline{i}$ la classe d'équivalence de i. On note alors $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

1. Premier contact avec $\mathbb{Z}/n\mathbb{Z}$.

a) Écrire les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

b) Parmi les anneaux précédents, déterminer ceux qui sont intègres ? ceux qui sont des corps ?

2. Isomorphismes.

a) Montrer que le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est isomorphe au groupe $(\mathbb{U}_n, \cdot)$, où $\mathbb{U}_n$ désigne l'ensemble des racines n-èmes de l'unité.

b) Les groupes $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathfrak{S}_3, \circ)$ sont-ils isomorphes ?

3. Étude des éléments inversibles (pour la loi $\times$).

a) Soit $x \in \mathbb{Z}$. Montrer que x et n sont premiers entre eux si et seulement si $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

b) Déterminer, en justifiant votre réponse, l'inverse de $\overline{15}$ dans $\mathbb{Z}/98\mathbb{Z}$.

c) Soit p un nombre premier et $\alpha \in \mathbb{N}^\star$. Déterminer le nombre d'éléments inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$.

4. Étude des diviseurs de $\overline{0}$.

a) Soit $x \in \mathbb{Z}^\star$ tel que $x \not\equiv 0\ [n]$. Montrer que $\overline{x}$ est un diviseur de $\overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x et n ne sont pas premiers entre eux.

b) Déterminer les diviseurs de $\overline{0}$ dans $\mathbb{Z}/30\mathbb{Z}$.

5. Montrer que les assertions suivantes sont équivalentes.

1. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau intègre.
3. n est premier.

6. Dans cette question, n désigne un nombre premier.

a) Résoudre dans $\mathbb{Z}/n\mathbb{Z}$ l'équation $\overline{x}^2 - \overline{1} = \overline{0}$.

b) En déduire que les seuls éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont leur propre inverse sont $\overline{1}$ et $\overline{n-1}$.

7. Théorème de Wilson. n est un nombre premier si et seulement si n divise $1 + (n-1)!$.

a) Montrer ce résultat pour $n = 2$.

b) Soit $n \geq 3$ un nombre premier. Montrer que dans $\mathbb{Z}/n\mathbb{Z}$, on a $\displaystyle\prod_{k=1}^{n-1} \overline{k} = \overline{n-1}$.

c) En déduire le théorème de Wilson.