Travail individuel de rédaction en temps libre
À rendre le jeudi 8 décembre

Exercice 1 *L'anneau* $\mathbb{Z}/n\mathbb{Z}$

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 $x \in \mathbb{Z}$, on note $\bar{x}$ la classe d'équivalence de x. On note alors

$$\mathbb{Z}/n\mathbb{Z} = \left\{ \bar{0}, \bar{1}, \dots, \overline{n-1} \right\}.$$

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

A1. On souhaite définir les lois $+$ et $\cdot$ par

$$\forall (x, y) \in \mathbb{Z}, \bar{x} + \bar{y} = \overline{x+y} \text{ et } \bar{x} \cdot \bar{y} = \overline{xy}.$$

Montrer que l'on définit bien ainsi deux lois de composition internes sur $\mathbb{Z}/n\mathbb{Z}$.

A2. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

A3. Écrire les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

A4. Parmi les anneaux précédents, déterminer ceux qui sont intègres. Déterminer ceux qui sont des corps.

A5. 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-ème de l'unité.

A6. On note S_3 l'ensemble des bijections de $[\![1, 3]\!]$ dans $[\![1, 3]\!]$. Les groupes $(\mathbb{Z}/6\mathbb{Z})$ et $(S_3, \circ)$ sont-ils isomorphes?

Partie B Éléments inversibles, diviseurs de $\bar{0}$

B1. Soit $x \in \mathbb{Z}$. Montrer que $\bar{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si x et n sont premiers entre eux.

B2. Déterminer, en le justifiant, l'inverse de $\overline{15}$ dans $\mathbb{Z}/98\mathbb{Z}$.

B3. Soit p un nombre premier et $\alpha \in \mathbb{N}^\star$. Déterminer le nombre d'éléments inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$.

B4. On dit que $\bar{x}$ est un diviseur de $\bar{0}$ s'il existe $\bar{y} \neq \bar{0}$ tel que $\bar{x} \cdot \bar{y} = \bar{0}$.

(a) Soit $x \in \mathbb{Z}$ tel que $x \not\equiv 0 \pmod{n}$. Montrer que $\bar{x}$ est un diviseur de $\bar{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si x et n ne sont pas premiers entre eux.

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

B5. Montrer que les assertions suivantes sont équivalentes

(i) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps.

(ii) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau intègre.

(iii) n est un nombre premier.

Partie C Théorème de Wilson

C1. Dans cette question, on suppose que n est un nombre premier.

- Résoudre dans $\mathbb{Z}/n\mathbb{Z}$ l'équation $\bar{x}^2 - \bar{1} = \bar{0}$.
- En déduire que les seuls éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont leur propre inverse sont $\bar{1}$ et $\overline{n-1}$.

C2. On suppose que n est un nombre premier et $n \geq 3$. Montrer que $\prod_{k=1}^{n-1} \bar{k} = \overline{n-1}$.

C3. Démontrer le théorème de Wilson

Soit $n \in \mathbb{N}$, $n \geq 2$. L'entier n est un nombre premier si, et seulement si n divise $1 + (n-1)!$.