**DM de MPSI2**

# Devoir non surveillé

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

Le but de ce problème est d'introduire les anneaux $\mathbb{Z}/n\mathbb{Z}$, fondamentaux en arithmétique.

Pour tout $n$ entier naturel $\geqslant 2$, on définit la *relation de congruence modulo $n$* sur $\mathbb{Z}$, par :

$$\forall\, x, y \in \mathbb{Z}, \quad (y \equiv x\,[n]) \Leftrightarrow (\exists k \in \mathbb{Z}, \quad y = x + kn)$$

(autrement dit, $y - x$ est un multiple entier de $n$, ou encore $n$ divise $y - x$).

On rappelle que relation de congruence modulo $n$ est une relation réflexive, symétrique, transitive (on dit que c'est une *relation d'équivalence*).

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

Pout tout entier relatif $x$, on note $\bar{x}$ la *classe d'équivalence de $x$* pour la relation de congruence modulo $n$, *i.e.* :

$$\bar{x} = \{y \in \mathbb{Z}, \quad y \equiv x[n]\}$$

**A.1** Montrer que si $x \equiv x'[n]$, alors $\bar{x} = \bar{x}'$. Montrer que l'ensemble $\{\bar{x}, x \in \mathbb{Z}\}$ est fini, de cardinal $n$. On note cet ensemble $\mathbb{Z}/n\mathbb{Z}$.

**A.2** On définit des lois d'addition et de multiplication sur $\mathbb{Z}/n\mathbb{Z}$ :

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

et

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

Montrer que ces opérations sont effectivement bien définies (il s'agit de prouver que la définition ne dépend pas des représentants $x$ et $y$ choisis pour les classes d'équivalence $\bar{x}$ et $\bar{y}$), puis qu'elles confèrent à $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau commutatif.

**A.3** Montrer que si $n$ est composé (*i.e.* n'est pas premier), l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

**A.4** Montrer que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si $n$ est premier.

**A.5** *Petit théorème de Fermat :* soit $a \in \mathbb{Z}$, et $p$ un nombre premier. Montrer que $a^p \equiv a\,[p]$.

**Indication :** utiliser la question précédente, et un exercice de la feuille de TD sur les structures algébriques.

### Partie B – Carrés dans $\mathbb{Z}/p\mathbb{Z}$

**B.1** Soit $a \in \mathbb{Z}$, et $p$ un nombre premier *impair*. On dit que $a$ est un *carré modulo $p$* (ou que $a$ ou $\bar{a}$ est un *carré* dans $(\mathbb{Z}/p\mathbb{Z})$) s'il existe $x \in \mathbb{Z}$ tel que

$$a \equiv x^2\,[p]$$

Montrer que dans $\mathbb{Z}/p\mathbb{Z}$ il y a $\frac{p+1}{2}$ carrés.

**Indication :** utiliser le morphisme carré sur $(\mathbb{Z}/p\mathbb{Z})^*$, pour montrer qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

**B.2** Montrer que $x \in \mathbb{Z}$ tel que $\bar{x} \neq \bar{0}$ est un carré modulo $p$ si et seulement si $x^{\frac{p-1}{2}} \equiv 1\,[p]$.

**B.3** Montrer que $-1$ est un carré modulo $p$ si et seulement si $p \equiv 1\,[4]$.