# 5 Classes de congruence

Soit $m \in \mathbb{N}$.

On appelle **classe de congruence** de $a$ modulo $m$ l'ensemble de tous les entiers qui sont congrus à $a$ modulo $m$ ; on la note $\overline{a}_m$ ou simplement $\overline{a}$ s'il n'y a aucune ambiguïté sur $m$.

$$\overline{a}_m = \{b \in \mathbb{Z} : a \equiv b \mod m\} = \{a + k\,m : k \in \mathbb{Z}\}$$

Un élément d'une classe de congruence s'appelle **représentant** de cette classe.

On peut désigner une classe de congruence par n'importe quel représentant de cette classe. Cependant, il est souvent utile de la désigner par son plus petit représentant non négatif.

On note $\mathbb{Z}/m\mathbb{Z}$ l'ensemble de toutes les classes modulo $m$ :

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}_m\,;\overline{1}_m\,;\ldots\,;\overline{(m-1)}_m\}$$

On définit une addition et une multiplication dans $\mathbb{Z}/m\mathbb{Z}$ :

$$\overline{a}_m + \overline{b}_m = \overline{a+b}_m \qquad \overline{a}_m \cdot \overline{b}_m = \overline{a\,b}_m$$

L'exercice 2.9 garantit que ces définitions ont un sens, c'est-à-dire que le résultat ne dépend pas du choix des représentants de ces classes.

Ces opérations vérifient les propriétés suivantes :

1) $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$
2) $\overline{a}+\overline{0} = \overline{a}$
3) $\overline{a}+\overline{(-a)} = \overline{0}$
4) $\overline{a}+\overline{b} = \overline{b}+\overline{a}$
5) $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$
6) $\overline{a}\cdot\overline{1} = \overline{a}$
7) $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$
8) $\overline{a}\cdot\overline{b} = \overline{b}\cdot\overline{a}$

Les propriétés 1) à 4) signifient que $\mathbb{Z}/m\mathbb{Z}$ forme un *groupe commutatif*.

Les propriétés 1) à 8) signifient que $\mathbb{Z}/m\mathbb{Z}$ constitue un *anneau commutatif*.

Un ensemble d'entiers $\{r_1\,;r_2\,;\ldots\,;r_m\}$ constitue un **ensemble complet de représentants** de $\mathbb{Z}/m\mathbb{Z}$ si $\mathbb{Z}/m\mathbb{Z} = \{\overline{r_1}\,;\overline{r_2}\,;\ldots\,;\overline{r_m}\}$.

**5.1** Lesquels des ensembles suivants sont-ils des ensembles complets de représentants de $\mathbb{Z}/7\mathbb{Z}$ :

1) $\{1\,;3\,;5\,;7\,;9\,;11\,;13\}$
2) $\{1\,;4\,;9\,;16\,;25\,;36\,;49\}$
3) $\{1\,;8\,;27\,;64\,;125\,;216\,;343\}$
4) $\{0\,;1\,;3\,;9\,;27\,;81\,;243\}$
5) $\{0\,;1\,;4\,;16\,;128\,;512\,;2048\}$

**5.2** Montrer que $\{0\,;2\,;2^2\,;2^3\,;\ldots\,;2^{11}\,;2^{12}\}$ est un ensemble complet de représentants de $\mathbb{Z}/13\mathbb{Z}$.

Un élément $\overline{a}$ de $\mathbb{Z}/m\mathbb{Z}$ est dit **inversible** s'il existe $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tel que $\overline{a}\cdot\overline{b} = \overline{1}$. L'élément $\overline{b}$, s'il existe, s'appelle **inverse** de $\overline{a}$.

**5.3** Montrer que si $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ est inversible, son inverse est unique.

**Indication :** si $\overline{b}$ et $\overline{c}$ sont deux inverses de $\overline{a}$, calculer $\overline{c}\cdot(\overline{a}\cdot\overline{b})$ et $(\overline{c}\cdot\overline{a})\cdot\overline{b}$.

**5.4** Dans $\mathbb{Z}/13\mathbb{Z}$, trouver les inverses de $\overline{2}$, $\overline{4}$, $\overline{5}$ et $\overline{7}$.

**5.5** Dans $\mathbb{Z}/25\mathbb{Z}$, trouver les inverses de $\overline{3}$, $\overline{11}$ et $\overline{23}$.

On appelle **unité** de $\mathbb{Z}/m\mathbb{Z}$ tout élément inversible de $\mathbb{Z}/m\mathbb{Z}$.

La proposition de la page 5.1 implique que $\overline{a}$ est une unité de $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $a$ et $m$ sont premiers entre eux.

**5.6** Dans $\mathbb{Z}/12\mathbb{Z}$, trouver les éléments qui ont un inverse et, pour chacun des éléments trouvés, calculer l'inverse.

**5.7** Mêmes questions avec $\mathbb{Z}/14\mathbb{Z}$.

**5.8** Mêmes questions avec $\mathbb{Z}/20\mathbb{Z}$.

## La fonction indicatrice $\varphi$ d'Euler

Le nombre d'unités de $\mathbb{Z}/m\mathbb{Z}$ se note $\varphi(m)$.
La fonction $\varphi$ s'appelle la **fonction indicatrice d'Euler**.
Ainsi, $\varphi(m)$ est le nombre d'entiers $a$ tels que $1 \leqslant a \leqslant m$ et $\text{pgcd}(a, m) = 1$.

**5.9** À l'aide des exercices 5.6, 5.7 et 5.8, calculer $\varphi(12)$, $\varphi(14)$ et $\varphi(20)$.

**5.10** Soit $p$ un nombre premier. Que vaut $\varphi(p)$ ?

**5.11** Soient $p$ un nombre premier et $k \in \mathbb{N}$.

1) Soit $a$ un entier. Montrer l'équivalence suivante :
   $a$ et $p^k$ ne sont pas premiers entre eux $\iff$ $a$ est un multiple de $p$.
2) Combien d'éléments contient $\{a \in \mathbb{Z} : 1 \leqslant a \leqslant p^k \text{ et } \text{pgcd}(a, p^k) \neq 1\}$ ?
3) En déduire que $\boxed{\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)}$.

**5.12** Calculer $\varphi(125)$ et $\varphi(121)$.

**5.13** Soient $m$ et $n$ des entiers positifs premiers entre eux.

Le but de cet exercice est de prouver que $\varphi(mn) = \varphi(m)\,\varphi(n)$.

On désigne respectivement par $(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{r}_1\,;\overline{r}_2\,;\ldots\,;\overline{r}_{\varphi(m)}\}$ et $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{s}_1\,;\overline{s}_2\,;\ldots\,;\overline{s}_{\varphi(n)}\}$ l'ensemble des unités de $\mathbb{Z}/m\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

1) Justifier que l'on puisse définir une application *injective*

$$\begin{array}{ccc}(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (\overline{r}_i\,;\overline{s}_j) & \longmapsto & \overline{a}_{ij}\end{array}$$

telle que $\begin{cases} a_{ij} \equiv r_i \mod m \\ a_{ij} \equiv s_j \mod n \end{cases}$ pour tous $1 \leqslant i \leqslant \varphi(m)$ et $1 \leqslant j \leqslant \varphi(n)$.

2) Soient $1 \leqslant i \leqslant \varphi(m)$ et $1 \leqslant j \leqslant \varphi(n)$.

   (a) À l'aide de l'exercice 3.2, montrer que $\operatorname{pgcd}(a_{ij}, m) = \operatorname{pgcd}(r_i, m)$ et en déduire que $a_{ij}$ et $m$ sont premiers entre eux.

   (b) Montrer de même que $a_{ij}$ et $n$ sont premiers entre eux.

   (c) En conclure que $a_{ij}$ et $mn$ sont premiers entre eux, c'est-à-dire que $\overline{a}_{ij}$ est une unité de $\mathbb{Z}/mn\mathbb{Z}$.

3) Soit $\overline{a} \in \mathbb{Z}/mn\mathbb{Z}$ avec $\overline{a} \neq \overline{a}_{ij}$ pour tous $1 \leqslant i \leqslant \varphi(m)$ et $1 \leqslant j \leqslant \varphi(n)$.

   (a) Posons $r \equiv a \mod m$ et $s \equiv a \mod n$.
   Montrer que $r \notin (\mathbb{Z}/m\mathbb{Z})^*$ ou que $s \notin (\mathbb{Z}/n\mathbb{Z})^*$.

   (b) Supposons que $r \notin (\mathbb{Z}/m\mathbb{Z})^*$, c'est-à-dire que $\operatorname{pgcd}(r, m) > 1$.
   Montrer, grâce à l'exercice 3.2, que $\operatorname{pgcd}(a, m) > 1$.
   En tirer que $\overline{a}$ n'est pas une unité de $\mathbb{Z}/mn\mathbb{Z}$.

   (c) Prouver que si $s \notin (\mathbb{Z}/n\mathbb{Z})^*$, alors $\overline{a}$ n'est pas une unité de $\mathbb{Z}/mn\mathbb{Z}$.

4) Conclure que $\left\{\overline{a}_{ij} : 1 \leqslant i \leqslant \varphi(m) \text{ et } 1 \leqslant j \leqslant \varphi(n)\right\}$ constitue l'ensemble des unités de $\mathbb{Z}/mn\mathbb{Z}$. En déduire la formule $\varphi(mn) = \varphi(m)\,\varphi(n)$.

**5.14** Soit $n$ un entier dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1}\,p_2^{\alpha_2}\,\ldots\,p_k^{\alpha_k}$. Montrer que

$$\boxed{\varphi(n) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\ldots\left(1 - \tfrac{1}{p_k}\right)}$$

**5.15** Calculer :

1) $\varphi(100)$ 2) $\varphi(720)$ 3) $\varphi(1001)$ 4) $\varphi(10!)$

**5.16** Montrer que $\varphi(5186) = \varphi(5187) = \varphi(5188)$.

## Réponses

**5.1** 1) et 4)

**5.4** $\overline{7}$, $\overline{10}$, $\overline{8}$ et $\overline{2}$

**5.5** $\overline{17}$, $\overline{16}$ et $\overline{12}$

**5.6** Sont inversibles $\overline{1}$, $\overline{5}$, $\overline{7}$ et $\overline{11}$.
Ce sont leurs propres inverses.

**5.7** Sont inversibles $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{9}$, $\overline{11}$ et $\overline{13}$.
Leurs inverses respectifs sont $\overline{1}$, $\overline{5}$, $\overline{3}$, $\overline{11}$, $\overline{9}$ et $\overline{13}$.

**5.8** Sont inversibles $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$, $\overline{11}$, $\overline{13}$, $\overline{17}$ et $\overline{19}$.
Leurs inverses respectifs sont $\overline{1}$, $\overline{7}$, $\overline{3}$, $\overline{9}$, $\overline{11}$, $\overline{17}$, $\overline{13}$, $\overline{19}$.

**5.9** $\varphi(12) = 4$ $\varphi(14) = 6$ $\varphi(20) = 8$

**5.10** $\varphi(p) = p - 1$

**5.12** $\varphi(125) = 100$ et $\varphi(121) = 110$

**5.15** 1) 40 2) 192 3) 720 4) 829440

**5.16** $\varphi(5186) = \varphi(5187) = \varphi(5188) = 2592$