Chapitre 7
L'ensemble $\mathbb{Z}/_{n\mathbb{Z}}$ des entiers modulo n

1 Classes d'équivalences modulo n

Rappel : la relation de congruence modulo n est une relation d'équivalence dans $\mathbb{Z}$.

Définition 1.1 *Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On appelle* classe d'équivalence de a modulo n*, que l'on note $\dot{a}$, l'ensemble de tous les entiers congrus à a modulo n. Ainsi,*

$$\dot{a} = \{b \in \mathbb{Z} \,/\, b \equiv a \pmod n\} = \{b \in \mathbb{Z} \,/\, \exists\, k \in \mathbb{Z} \,/\, b = a + kn\} = \{a + kn \,/\, k \in \mathbb{Z}\}.$$

Exemples

1. Soit $a \in \mathbb{Z}$ et prenons $n = 2$. Alors soit a est pair, soit a est impair.
   Si a est pair, alors $a \equiv 0 \pmod 2$, donc $a \in \dot{0}$ puis $\dot{a} = \dot{0}$.
   Si a est impair, alors $a \equiv 1 \pmod 2$, donc $a \in \dot{1}$ puis $\dot{a} = \dot{1}$.
   Remarquons de plus que $\dot{0} \neq \dot{1}$ car par exemple $0 \in \dot{0}$ mais $0 \notin \dot{1}$. En fait, $\dot{0}$ et $\dot{1}$ sont des parties *disjointes* de $\mathbb{Z}$, cf. chapitre 4 sur les relations binaires.
2. Soit $n = 3$. Alors $\dot{0} = \{$ $\}$, $\dot{1} = \{$ $\}$, $\dot{2} = \{$ $\}$,
   $\dot{3} = \{$ $\} =$, $\dot{4} =$.

Proposition 1.2 *Soit $n \in \mathbb{N}^*$. Deux classes d'équivalence $\dot{a}$ et $\dot{b}$ modulo n sont égales si et seulement si $a \equiv b \pmod n$.*

Définition 1.3 *Étant donné un $n \in \mathbb{N}^*$, on appelle* ensemble des entiers modulo n*, que l'on note $\mathbb{Z}/_{n\mathbb{Z}}$, l'ensemble de toutes les classes d'équivalence d'entiers modulo n.*

Proposition 1.4 *Étant donné un $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/_{n\mathbb{Z}}$ possède exactement n éléments. Plus précisément,*

$$\mathbb{Z}/_{n\mathbb{Z}} = \left\{\dot{0}, \dot{1}, \ldots, \dot{\widehat{n-1}}\right\}.$$

Démonstration : Soit $a \in \mathbb{Z}$. $\dot{a} = \{b \in \mathbb{Z} \,/\, b \equiv a \pmod n\}$. Ainsi $\dot{a}$ est l'ensemble de tous les entiers qui ont même reste que a dans la division euclidienne par n.
Il y a donc autant de classes d'équivalence modulo n distinctes que de restes possibles dans cette division euclidienne, soit n (puisque le reste peut prendre toutes valeurs entières de 0 à $n-1$).

Remarque : pour désigner les éléments de $\mathbb{Z}/_{n\mathbb{Z}}$ on utilise les résidus possibles modulo n. Les entiers modulo n sont aussi appelés classes résiduelles modulo n.

Exemples

1. Soit $n = 2$. Alors $\mathbb{Z}/_{2\mathbb{Z}} = \{\dot{0}, \dot{1}\}$, comme on l'a d'ailleurs montré dans l'exemple 1. précédent.
2. Soit $n = 3$. Alors $\mathbb{Z}/_{3\mathbb{Z}} = \{\dot{0}, \dot{1}, \dot{2}\}$, avec $\dot{0} = \{3k \,/\, k \in \mathbb{Z}\}$, $\dot{1} = \{1 + 3k \,/\, k \in \mathbb{Z}\}$ et $\dot{2} = \{2 + 3k \,/\, k \in \mathbb{Z}\}$.

2 Opérations dans l'ensemble des entiers modulo n

Soit dans toute la suite $n \in \mathbb{N}^*$.

Définition 2.1 *On définit dans $\mathbb{Z}/_{n\mathbb{Z}}$*

- *une addition, notée $+$, via* $\dot{a} + \dot{b} = \dot{\widehat{a+b}}$,
- *une multiplication, notée $\times$ ou plus simplement $\cdot$, via* $\dot{a} \times \dot{b} = \dot{\widehat{ab}}$

pour tous $\dot{a}, \dot{b} \in \mathbb{Z}/_{n\mathbb{Z}}$.

Exemples dans $\mathbb{Z}/_{8\mathbb{Z}}$:

$$\dot{3} + \dot{4} = \dot{\widehat{7}}, \qquad \dot{3} + \dot{7} = \dot{\widehat{10}} = \dot{2} \text{ car } 10 \equiv 2 \pmod 8$$
$$\dot{3} \times \dot{2} = \dot{\widehat{6}}, \qquad \dot{3} \times \dot{4} = \dot{\widehat{12}} = \dot{4}$$

Proposition 2.2

1. *L'addition dans $\mathbb{Z}/_{n\mathbb{Z}}$ possède les propriétés suivantes :*
   - *$+$ est commutative : $\dot{a}+\dot{b}=\dot{b}+\dot{a}$,*
   - *$+$ est associative : $(\dot{a}+\dot{b})+\dot{c}=\dot{a}+(\dot{b}+\dot{c})$,*
   - *il existe un élément neutre, $\dot{0}$: $\dot{a}+\dot{0}=\dot{0}+\dot{a}=\dot{a}$,* *en effet : $\dot{a}+\dot{0}=\overset{\cdot}{\widehat{a+0}}=\dot{a}$*
   - *tout élément $\dot{a}$ possède un opposé noté $-\dot{a}$ défini par $-\dot{a}=\overset{\cdot}{\widehat{-a}}$* *en effet : $\dot{a}+\overset{\cdot}{\widehat{-a}}=\overset{\cdot}{\widehat{a+(-a)}}=\dot{0}$*

   pour tous $\dot{a},\dot{b},\dot{c}\in\mathbb{Z}/_{n\mathbb{Z}}$.
2. *La multiplication dans $\mathbb{Z}/_{n\mathbb{Z}}$ possède les propriétés suivantes :*
   - *$\times$ est commutative : $\dot{a}\times\dot{b}=\dot{b}\times\dot{a}$,*
   - *$\times$ est associative : $(\dot{a}\times\dot{b})\times\dot{c}=\dot{a}\times(\dot{b}\times\dot{c})$,*
   - *il existe un élément neutre, $\dot{1}$: $\dot{a}\times\dot{1}=\dot{1}\times\dot{a}=\dot{a}$,* *en effet : $\dot{a}\times\dot{1}=\overset{\cdot}{\widehat{a\times 1}}=\dot{a}$*

   pour tous $\dot{a},\dot{b},\dot{c}\in\mathbb{Z}/_{n\mathbb{Z}}$.
3. *La multiplication est distributive par rapport à l'addition : $\dot{a}\times(\dot{b}+\dot{c})=(\dot{a}\times\dot{b})+(\dot{a}\times\dot{c})$, pour tous $\dot{a},\dot{b},\dot{c}\in\mathbb{Z}/_{n\mathbb{Z}}$.*

Comme pour les nombres réels, on convient que la multiplication est prioritaire par rapport à l'addition et on renote toute expression du type $(\dot{a}\times\dot{b})+\dot{c}$ plus simplement $\dot{a}\cdot\dot{b}+\dot{c}$, ou encore $\dot{a}\dot{b}+\dot{c}$.

Tables d'addition dans $\mathbb{Z}/_{2\mathbb{Z}}$, $\mathbb{Z}/_{3\mathbb{Z}}$ et $\mathbb{Z}/_{4\mathbb{Z}}$. On notera à côté de chacune d'elles les opposés des éléments de $\mathbb{Z}/_{n\mathbb{Z}}$.

Soit $n=2$.

$+$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{1}$
$\dot{1}$	$\dot{1}$	$\dot{0}$

Soit $n=3$

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{0}$	$\dot{1}$

Soit $n=4$

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{0}$	$\dot{1}$	$\dot{2}$

On se pose la question suivante : les éléments non nuls de $\mathbb{Z}/_{n\mathbb{Z}}$ admettent-ils tous un inverse ?

Définition 2.3 *Un élément $\dot{a}\in\mathbb{Z}/_{n\mathbb{Z}}$ est dit* inversible *si et seulement si il existe $\dot{b}\in\mathbb{Z}/_{n\mathbb{Z}}$ tel que $\dot{a}\cdot\dot{b}=\dot{1}$.*
*Dans ce cas, on appelle $\dot{b}$ l'*inverse *de $\dot{a}$ et on note $\dot{b}=\dot{a}^{-1}$.*

Exemples dans $\mathbb{Z}/_{5\mathbb{Z}}$:

$\dot{1}\times\dot{1}=\dot{1}$ donc $\dot{1}^{-1}=\dot{1}$, $\dot{3}\times\dot{2}=\dot{6}=\dot{1}$ donc $\dot{3}^{-1}=\dot{2}$ et $\dot{2}^{-1}=\dot{3}$, $\dot{4}\times\dot{4}=\dot{16}=\dot{1}$ donc $\dot{4}^{-1}=\dot{4}$

Tables de multiplication dans $\mathbb{Z}/_{2\mathbb{Z}}$, $\mathbb{Z}/_{3\mathbb{Z}}$ et $\mathbb{Z}/_{4\mathbb{Z}}$. On notera à côté de chacune d'elles les inverses des éléments de $\mathbb{Z}/_{n\mathbb{Z}}$ s'ils existent.

Soit $n=2$.

$\times$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$

Soit $n=3$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{1}$

Soit $n=4$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$		$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	

Définition 2.4 *Un élément $\dot{a}\in\mathbb{Z}/_{n\mathbb{Z}}$ est dit un* diviseur de zéro *si et seulement si il existe $\dot{b}\in\mathbb{Z}/_{n\mathbb{Z}}-\{\dot{0}\}$ tel que $\dot{a}\cdot\dot{b}=\dot{0}$.*

Exemples

1. L'élément $\dot{0}$ est toujours diviseur de zéro puisque $\dot{0}\cdot\dot{1}=\dot{0}$.
2. Dans $\mathbb{Z}/_{3\mathbb{Z}}$, il n'y a pas de diviseur de zéro autre que $\dot{0}$; les éléments $\dot{1}$ et $\dot{2}$ sont inversibles et chacun des deux coïncide avec son inverse.
3. Dans $\mathbb{Z}/_{4\mathbb{Z}}$, $\dot{0}$ et $\dot{2}$ sont les diviseurs de zéro, tandis que $\dot{1}$ et $\dot{3}$ sont inversibles, chacun des deux coïncidant avec son inverse.

Théorème 2.5 *Soit $a \in \mathbb{Z}$. Alors $\dot{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ est inversible si et seulement si* $\operatorname{pgcd}(|a|, n) = 1$.
Autrement dit : $\dot{a} \in \mathbb{Z}/_{n\mathbb{Z}}$ est inversible si et seulement si a et n sont premiers entre eux.

Une conséquence importante de ce théorème est le corollaire suivant :

Corollaire 2.6 *Si n est premier alors tout élément $\dot{a} \neq \dot{0}$ de $\mathbb{Z}/_{n\mathbb{Z}}$ est inversible.*

Notation : L'ensemble des éléments inversibles de $\mathbb{Z}/_{n\mathbb{Z}}$ est noté $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$.

Exemples :

1. Si n est premier alors $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^* = \mathbb{Z}/_{n\mathbb{Z}} - \{\dot{0}\}$
2. $\left(\mathbb{Z}/_{4\mathbb{Z}}\right)^* = \{$.
3. $\left(\mathbb{Z}/_{15\mathbb{Z}}\right)^* = \{$.

Exercice : Résoudre dans $\mathbb{Z}$ la congruence $7x \equiv 5 \pmod{15}$.