• **Cadre.** n est un entier naturel non nul.

1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes d'équivalence modulo n

Rappels : classes de congruences modulo n

• *Relation d'équivalence.* La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.
• *Classes d'équivalences.* Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe d'équivalence de x : $\overline{x} = \{x + kn \,;\, k \in \mathbb{Z}\}$.
• *Retenir :* Par construction, pour tous $x, y \in \mathbb{Z}$: $\boxed{\overline{x} = \overline{y} \iff x \equiv y \ [n]}$

Définition 1

On note $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ l'ensemble des classes d'équivalences pour la relation de congruences modulo n : $\boxed{\dfrac{\mathbb{Z}}{n\mathbb{Z}} \underset{\text{déf.}}{=} \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}}$

• **Remarque.** $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un ensemble fini de cardinal n

2 Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 — Soient $x, x', y, y' \in \mathbb{Z}$. Montrer que si $\overline{x} = \overline{y}$ et $\overline{x'} = \overline{y'}$, alors : $\overline{x + x'} = \overline{y + y'}$ et $\overline{xx'} = \overline{yy'}$

Le résultat de l'exercice qui précède permet [1] de définir deux lois de compositions internes sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$:

Définition 2

Pour tous $x, y \in \mathbb{Z}$ on pose : $\overline{x} + \overline{y} \underset{\text{déf.}}{=} \overline{x+y}$ et $\overline{x} \times \overline{y} \underset{\text{déf.}}{=} \overline{x \times y}$.

Théorème 1

$\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ est un anneau commutatif, d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.

• **Reformulation du petit théorème de Fermat dans $\mathbb{Z}/p\mathbb{Z}$.**

Pour tout $p \in \mathbb{P}$ et tout $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$: • $x^p = x$ • Si $x \neq \overline{0}$, alors : $x^{p-1} = \overline{1}$.

Exercice 2 — Montrer que $f : x \mapsto \overline{x}$ est un morphisme d'anneau de $\mathbb{Z}$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Exemple 1 — On suppose que $n \geq 2$ n'est pas premier. Montrer que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas un anneau intègre.

3 Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 2 : Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Pour tout $a \in \mathbb{Z}$: $a \in U\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right) \iff a \wedge n = 1$

En pratique : pour inverser a modulo n

Il suffit de trouver une relation de Bézout entre a et n : si on trouve $u, v \in \mathbb{Z}$ tels que $au + bn = 1$ alors $\overline{u} = \overline{a}^{-1}$.

Exemple 2 — Résoudre l'équation : $\overline{2}x = \overline{3}$ d'inconnue $x \in \dfrac{\mathbb{Z}}{37\mathbb{Z}}$.

Théorème 3

On suppose $n \geq 2$. $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps si et seulement si n est premier.

Exemple 3 — Soit p un nombre premier.

1. Soit $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$, non nul. Montrer que : $x = x^{-1}$ si et seulement si $x = \overline{1}$ ou $x = -\overline{1}$.
2. Démontrer le théorème de Wilson : $(p-1)! \equiv -1 \ [p]$. *Indication : Multiplier tous les éléments non nuls de* $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$

1. Les égalités $\overline{x + x'} = \overline{y + y'}$ et $\overline{xx'} = \overline{yy'}$ sont cruciales pour définir l'addition et la multiplication sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Par exemple il est naturel de définir dans $\mathbb{Z}/7\mathbb{Z}$ la somme $\overline{2} + \overline{4}$ par : $\overline{2} + \overline{4} \underset{\text{déf.}}{=} \overline{2+4} = \overline{6}$. Cependant, vu que $\overline{2} = \overline{9}$, il convient de s'assurer que $\overline{9+4}$ et $\overline{2+4}$ sont égaux.

Exercice 1 — Supposons que $\overline{x}=\overline{y}$ et $\overline{x'}=\overline{y'}$.
On sait donc que : $x\equiv y\ [n]$ et $x'\equiv y'\ [n]$.
Ainsi : $x+x'\equiv y+y'\ [n]$ et $xx'\equiv yy'\ [n]$
Dit autrement : $\overline{x+x'}=\overline{y+y'}$ et $\overline{xx'}=\overline{yy'}$.

Démonstration du théorème 1.
Il s'agit de montrer que :

i) $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ est un groupe commutatif, d'élément neutre $\overline{0}$.

ii) La loi $\times$:
- est associative et commutative [2]
- possède $\overline{1}$ pour élément neutre.

iii) $\times$ est distributive sur $+$.

Détaillons le point *i)*. On sait déjà que $+$ est une loi de composition interne sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Soient $x,y,z\in\mathbb{Z}$:
- *Commutativité de* $+$. $\overline{x}+\overline{y}=\overline{x+y}=\overline{y+x}=\overline{y}+\overline{x}$.
- *Associativité de* $+$.

$$\left(\overline{x}+\overline{y}\right)+\overline{z}=\overline{x+y}+\overline{z}=\overline{(x+y)+z}$$
$$=\overline{x+(y+z)}=\overline{x}+\overline{y+z}=\overline{x}+\left(\overline{y}+\overline{z}\right)$$

- *Element neutre pour* $+$.
$$\overline{x}+\overline{0}=\overline{x+0}=\overline{x}\quad\text{et}\quad\overline{0}+\overline{x}=\overline{0+x}=\overline{x}$$
- *« inverse » de* x *pour* $+$.
Montrons que $\overline{x}$ est inversible dans $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+\right)$, d'inverse $\overline{-x}$. Pour cela on calcule :
$$\overline{x}+\overline{-x}=\overline{x+(-x)}=\overline{0}\quad\text{et}\quad\overline{-x}+\overline{x}=\overline{(-x)+x}=\overline{0}$$

Exercice 2 —
- Par définition de f : $f(1)=\overline{1}$ (qui est bien l'élément neutre de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $\times$).
- Soient $x,y\in\mathbb{Z}$, par définition de f et des deux opérations $\times$ et $+$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$:
$$f(x+y)\underset{\text{déf. de }f}{=}\overline{x+y}\underset{\text{déf. de }+}{=}\overline{x}+\overline{y}\underset{\text{déf. de }f}{=}f(x)+f(y)$$
et
$$f(x\times y)\underset{\text{déf. de }f}{=}\overline{x\times y}\underset{\text{déf. de }\times}{=}\overline{x}\times\overline{y}\underset{\text{déf. de }f}{=}f(x)\times f(y)$$

Exemple 1 — Par hypothèse, il existe deux entiers $d,q\in[\![2,n-1]\!]$ tels que : $n=dq$.
Ainsi : $\overline{d}\times\overline{q}=0$ alors que : $\overline{d}\neq 0$ et $\overline{q}\neq 0$

Démonstration du théorème 2. Soit $a\in\mathbb{Z}$.
$$a\in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\iff\exists u\in\mathbb{Z}\mid\overline{a}\times\overline{u}=\overline{u}\times\overline{a}=\overline{1}$$
$$\iff\exists u\in\mathbb{Z}\mid\overline{au}=\overline{1}$$
$$\iff\exists u\in\mathbb{Z}\mid au\equiv 1\ [n]$$
$$\iff\exists u,v\in\mathbb{Z}\mid au+nv=1$$
$$\underset{\text{Bézout}}{\iff}a\wedge n=1$$

Exemple 2 —
$\overline{2}$ est inversible dans $\dfrac{\mathbb{Z}}{37\mathbb{Z}}$ car $2\wedge 37=1$.
De plus : $\overline{2}^{-1}=\overline{19}$. En effet :
- *Première possibilité* On constate directement que
$$2\times 19=38\equiv 1\ [37]$$
- *Deuxième possibilité* On détermine une relation de Bézout entre 2 et 37, ici : $2\times 19-1\times 37=1$

Soit $x\in\dfrac{\mathbb{Z}}{37\mathbb{Z}}$:
$$\overline{2}\times x=\overline{3}\iff x=\overline{2}^{-1}\times\overline{3}\iff x=\overline{19}\times\overline{3}=\overline{57}=\overline{20}$$
L'équation possède $\overline{20}$ comme unique solution.

Démonstration du théorème 3.
On a déjà vu que si n n'est pas premier, alors $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas intègre, en particulier, ce n'est pas un corps [3].
Supposons que n est un nombre premier.
Montrons que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps.
On sait déjà que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un anneau commutatif.
Il reste à montrer que tout élément autre que $\overline{0}$ est inversible.
Soit $\overline{x}\in\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, tel que : $\overline{x}\neq\overline{0}$ *i.e.* : $x\neq 0\ [n]$.
Ainsi n ne divise pas x.
Puisque n est premier : $n\wedge x=1$.
D'après le théorème 2, $\overline{x}$ est inversible.

Exemple 3 —
1. On procède par équivalence.
$$x=x^{-1}\iff x^2=\overline{1}\iff(x-\overline{1})(x+\overline{1})=0$$
Puisque $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, c'est un anneau intègre [a] donc, finalement :
$$x=x^{-1}\iff x=\overline{1}\quad\text{ou}\quad x=-\overline{1}$$
2. Posons $P=\displaystyle\prod_{\substack{x\in\mathbb{Z}/p\mathbb{Z}\\ x\neq\overline{0}}}x$.
Calculons P de deux façons :
- *Première façon.*
$$P=\prod_{k=1}^{p-1}\overline{k}=\overline{(p-1)!}$$
- *Deuxième façon.* Dans le produit P, tout facteur x autre que $\overline{1}$ et $-\overline{1}$ peut être regroupé avec son inverse $\overline{x}^{-1}$ et le résultat vaut $\overline{x}\times\overline{x}^{-1}=\overline{1}$ qui est neutre pour $\times$, le produit se réduit donc au seuls facteurs $\overline{1}$ et $-\overline{1}$ et vaut :
$$P=\overline{1}\times(-\overline{1})=-\overline{1}$$
En conséquence : $\overline{(p-1)!}=-\overline{1}$.
Autrement dit : $(p-1)!\equiv -1\ [p]$.

a. Le vérifier à titre d'exercice

2. Rappel : l'anneau est ici commutatif si $\times$ l'est, dans la définition d'un anneau la loi $+$ est toujours commutative

3. Si $d,q\in\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont deux éléments non nuls tels que $d\times q=\overline{0}$, alors ils ne sont pas non plus inversibles (en effet, si l'on suppose par l'absurde que d est inversible, alors en multipliant l'égalité $d\times q=\overline{0}$ par d^{-1}, on obtient $q=\overline{0}$ ce qui est faux)