

Def: Soit  $n \in \mathbb{Z}_{>0}$ .

Soient  $a, b \in \mathbb{Z}$

On dit que  $a$  est congruent à  $b$  modulo  $n$   
et on écrit:

$$a \equiv b \pmod{n}$$

si  $n | a-b$ .

Le nombre  $n$  est appelé le module de la congruence.

### Exemple

1)  $n=1$

$3 \equiv 5 \pmod{1}$ ? Oui, car  $1 | 3-5$ .

On sait que  $\forall a \in \mathbb{Z} \quad 1 | a$ , donc modulo 1 il existe une seule classe d'équivalence:

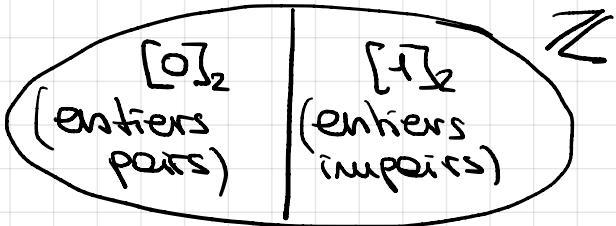
$$[0]_1 = \mathbb{Z}.$$

2)  $n=2$

$$a \equiv b \pmod{2} \iff 2 | [b-a]$$

$$\begin{aligned} [0]_2 &= \{a \in \mathbb{Z} : 2 | a-0\} = \{a \in \mathbb{Z} : 2 | a\} = \\ &= \{2k, k \in \mathbb{Z}\} = \{\text{entiers pairs}\} \end{aligned}$$

$$\begin{aligned} [1]_2 &= \{a \in \mathbb{Z} : 2 | a-1\} = \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tel que} \\ &\quad a-1 = 2k\} = \{2k+1, k \in \mathbb{Z}\} = \{\text{entiers impairs}\} \end{aligned}$$

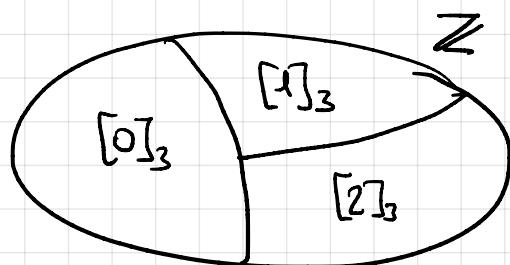


3)  $n=3$ . Modulo 3, il y a 3 classes d'équivalence

$$[0]_3 = \{3k, k \in \mathbb{Z}\}$$

$$[1]_3 = \{3k+1, k \in \mathbb{Z}\}$$

$$[2]_3 = \{3k+2, k \in \mathbb{Z}\}$$



Def: L'ensemble des classes d'équivalence pour la relation de congruence modulo  $n$  est noté  $\mathbb{Z}/n\mathbb{Z}$ .

Notation:  $n\mathbb{Z} := \{nk, k \in \mathbb{Z}\}$

Théorème: Soit  $n \in \mathbb{Z}_{>0}$ . Alors  $\mathbb{Z}/n\mathbb{Z}$  est l'ensemble des  $n$  classes d'équivalence :

$$[0]_n, [1]_n, \dots, [n-1]_n.$$

Ainsi, toute classe d'équivalence possède un représentant canonique compris entre 0 et  $n-1$ .

Démonstration

Soit  $a \in \mathbb{Z}$ . Alors, par division euclidienne,

$\exists q, r \in \mathbb{Z}$  avec  $0 \leq r < n$  tels que

$$a = nq + r$$



$$a - r = nq$$



$$n \mid a - r$$



$$a \equiv r \pmod{n}$$



$$[a]_n = [r]_n, \quad 0 \leq r < n$$

Donc  $r$  est un représentant de la classe de  $a$ , compris entre 0 et  $n-1$ .

On montre maintenant que si  $0 \leq a < b < n$  alors  $[a]_n \neq [b]_n$  (les classes sont distinctes).

Si, par l'absurde,  $[a]_n = [b]_n \Rightarrow b \equiv a \pmod{n} \Rightarrow n \mid b - a$ . Mais cela est impossible car  $1 \leq b - a < n$ .

Remarque : La démo du théorème nous dit aussi que  $\forall a \in \mathbb{Z}, [a]_n = [r]_n$  où  $r$  est le reste de la division euclidienne de  $a$  par  $n$ .

Exemples :  $n = 17$ .

$$[36]_{17} = [0]_{17} \quad (36 = 2 \cdot 17 + 0)$$

$$[58]_{17} = [7]_{17} \quad (58 = 3 \cdot 17 + 7)$$

$$[-1]_{17} = [16]_{17} \quad (-1 = -1 \cdot 17 + 16)$$

$$[-23]_{17} = [11]_{17} \quad (-23 = -2 \cdot 17 + 11)$$

Dans  $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$

On va définir deux opérations binaires sur  $\mathbb{Z}/n\mathbb{Z}$ :

- ADDITION :  $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$   
 $([a]_n, [b]_n) \longmapsto [a]_n + [b]_n := [a+b]_n$
- MULTIPLICATION :  $\circ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$   
 $([a]_n, [b]_n) \longmapsto [a]_n \cdot [b]_n := [a \cdot b]_n$

Quand on travaille avec des classes d'équivalences il faut montrer que ces opérations sont bien définies. Dans notre cas cela signifie que si  $a' \in [a]_n$  et  $b' \in [b]_n$  alors  $[a'+b']_n = [a+b]_n$  et  $[a' \cdot b']_n = [a \cdot b]_n$ .

Cela est conséquence du résultat suivant.

Proposition : Soient  $a, b, a', b' \in \mathbb{Z}$  et  $n \in \mathbb{Z}_{>0}$ .

Si  $a \equiv a' \pmod{n}$  et  $b \equiv b' \pmod{n}$ , alors :

- 1)  $a+b \equiv a'+b' \pmod{n}$ ,
- 2)  $a \cdot b \equiv a' \cdot b' \pmod{n}$ .

## Démo

Si  $a \equiv a' \pmod{n} \Rightarrow n | a-a' \Rightarrow \exists k_1 \in \mathbb{Z}$  tel que  $a-a'=nk_1$ .

Si  $b \equiv b' \pmod{n} \Rightarrow \exists k_2 \in \mathbb{Z}$  t.q.  $b-b'=nk_2$

1) Donc, en sommant, on a :

$$(a-a') + (b-b') = nk_1 + nk_2$$



$$(a+b) - (a'+b') = n(k_1 + k_2)$$



$$a+b \equiv a'+b' \pmod{n}$$

$$\begin{aligned} 2) a'b' &= \overbrace{(a-nk_1)(b-nk_2)}^{a' = a-nk_1} = ab - n(aK_2 - bK_1) + n^2K_1K_2 \\ &= ab + n \underbrace{(-aK_2 - bK_1 - nK_1K_2)}_{\in \mathbb{Z}} \end{aligned}$$

$$a' = a - nk_1$$

$$b' = b - nk_2$$

$$\Rightarrow a'b' \equiv ab \pmod{n}.$$

## Exemple

$$n = 17$$

$$[15]_{17} + [13]_{17} = [28]_{17} = [11]_{17}$$

$$[2]_{17} \cdot [13]_{17} = [26]_{17} = [9]_{17}$$

$$[11]_{17} + [6]_{17} = [17]_{17} = [0]_{17}$$

## Propriétés addition

1) Commutativité :  $\forall [a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$

$$[a]_n + [b]_n = [b]_n + [a]_n.$$

(conséquence de la commutat.  
de + dans  $\mathbb{Z}$ .)

2) associativité:  $\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ ,

$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$$

3)  $\exists$  élément neutre:  $[0]_n$

$$\forall [a]_n \in \mathbb{Z}/n\mathbb{Z}, [a]_n + [0]_n = [0]_n + [a]_n = [a]_n.$$

4)  $\exists$  élément opposé  $\forall [a]_n \in \mathbb{Z}/n\mathbb{Z}$ .

$\forall [a]_n \in \mathbb{Z}/n\mathbb{Z}, \exists [-a]_n \in \mathbb{Z}/n\mathbb{Z}$  t.q.

$$[a]_n + [-a]_n = [0]_n$$

Donc:  $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe abélien "commutatif"

### Propriétés de la multiplication

1) commutative

2) associative

3)  $\exists$  élément neutre:  $[1]_n$

en général

Attention: il n'existe pas d'inverse multiplicatif  
 $\forall [a]_n \in \mathbb{Z}/n\mathbb{Z} \setminus \{[0]_n\}$

exemple:  $n = 8, \mathbb{Z}/8\mathbb{Z}$

$$\bullet [7]_8 \cdot [7]_8 = [1]_8, \text{ donc}$$

$[7]_8$  a un inverse multi.  
(qui même)

$\bullet [2]_8$  n'a pas d'inverse

En plus :

- est distributive sur + :

$$\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z},$$

$$[a]_n ([b]_n + [c]_n) = [a]_n [b]_n + [a]_n [c]_n.$$

Donc  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un anneau commutatif unitaire.

Notation : lorsque le contexte est clair, on note la classe  $[a]_n$  simplement  $\bar{a}$  ou encore, pour abus de notation, juste  $a$ .

On peut donc écrire  $3 \in \mathbb{Z}/17\mathbb{Z}$  à la place de  $[3]_{17} \in \mathbb{Z}/17\mathbb{Z}$

Déf: Un élément  $a \in \mathbb{Z}/n\mathbb{Z}$  est inversible s'il existe  $b \in \mathbb{Z}/n\mathbb{Z}$  tel que  $ab \equiv 1 \pmod{n}$ .

Exemples : • 3 est inversible modulo 4, car  $3 \cdot 3 \equiv 1 \pmod{4}$ .  
• 3 n'est pas inversible modulo 6.

Remarque : c'est facile de voir que si  $a$  est inversible alors son inverse est unique et on le note  $a^{-1}$ .

Proposition : Un élément  $a \in \mathbb{Z}/n\mathbb{Z}$  est inversible si et seulement si  $\text{pgcd}(a, n) = 1$ .

Démo

$\Rightarrow)$  Supposons que  $a \in \mathbb{Z}/n\mathbb{Z}$  est inversible.

Alors  $\exists b \in \mathbb{Z}/n\mathbb{Z}$  tel que  $ab \equiv 1 \pmod{n}$

$\Rightarrow \exists k \in \mathbb{Z}$  tel que  $ab - 1 = nk$

$\Rightarrow ab - nk = 1 \Rightarrow \text{pgcd}(a, n) = 1.$

$\Leftarrow)$  Supposons que  $\text{pgcd}(a, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$  tel que  $au + nv = 1 \Rightarrow au - 1 = nv \Rightarrow$

$n \mid au - 1 \Rightarrow au \equiv 1 \pmod{n}$

Donc  $u$  est l'inverse de  $a$ .

La démonstration nous suggère aussi un algorithme d'inversion modulaire :

Algorithme :  $\text{InverseMod}(a, n)$

Entrée : Deux entiers  $a, n \neq 0$

Sortie : Un entier  $b$ ,  $0 < b < n$ , tel que  $ab \equiv 1 \pmod{n}$   
s'il existe, une erreur, sinon.

1.  $(d, u, v) \leftarrow \text{EuclideEtendu}(a, n)$
2. Si  $d \neq 1$ . Renvoyer une erreur «  $a$  n'est pas inversible modulo  $n$  »
3. Renvoyer  $u \pmod{n}$ .