III Congruences

Propriété.

Soit c un entier relatif non nul

Deux entiers a et b ont même reste dans la division euclidienne par c

$\boxed{\text{ssi}}$ $a-b$ est multiple de c

Exemple : $27 = 4\times 6 + 3$ même reste dans la division euclidienne par 6

$15 = 2\times 6 + 3$ on a bien $27 - 15 = 12 = 2\times 6$

Démonstration : Rq $\boxed{\text{ssi}}$ est une équivalence

On fait cette démonstration en 2 temps $\boxed{\text{dans le cas où } c \in \mathbb{N}^*}$

⊛ $\Rightarrow$) a et b ont même reste dans la division euclidienne par c

les divisions euclidienne s'écrivent.

$$\begin{cases} a = cq + R \\ b = cq' + R \end{cases} \qquad q, q' \in \mathbb{Z} \quad \text{et} \quad 0 \leq R < c$$

donc $a - b = (cq + R) - (cq' + R)$

$= cq + \cancel{R} - cq' - \cancel{R}$

$= cq - cq' = c(q - q')$

donc $a-b$ est un multiple de c

⊛ $\Leftarrow$) réciproquement

les divisions euclidiennes de a et b par c s'écrivent

$a = cq + R \qquad q, q' \in \mathbb{Z} \qquad 0 \leq R < c$

$b = cq' + R' \qquad\qquad 0 \leq R' < c.$

on veut montrer que $R = R'$

on $a-b$ est un multiple de c

$\Leftrightarrow c \mid a-b$

De plus on a $a - b = (cq + R) - (cq' + R')$

$a - b = c(q - q') + R - R'$

$\Leftrightarrow a - b - c(q - q') = R - R'$

$$\begin{cases} c \mid a-b \\ c \mid c(q-q') \end{cases} \Rightarrow c \mid (a-b) - c(q-q') \quad \text{combinaison linéaire}$$

$$\Rightarrow c \mid R - R'$$

$R - R'$ est donc un multiple de c

$$0 \leq R' < c$$

$$\Leftrightarrow 0 \geq -R' > -c$$

$$\Leftrightarrow -c < -R' \leq 0$$

De plus + $0 \leq R < c$

$$\Rightarrow -c < R - R' < c$$

Le seul multiple de c strictement compris entre $-c$ et c est 0 donc $R - R' = 0$

$$\Leftrightarrow R = R'$$

donc a et b ont même reste dans la division euclidienne par c

Définition : Soient a et b 2 entiers relatifs

Soit c un entier naturel non nul.

a et b sont congrus modulo c

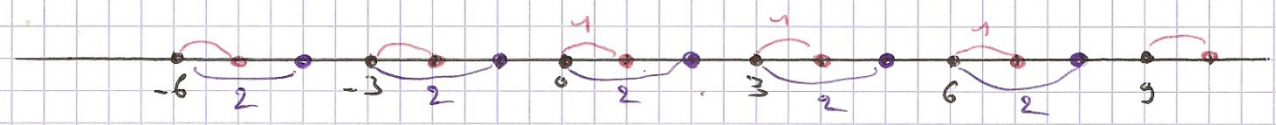
$\boxed{\text{ssi}}$ $a-b$ est un multiple de c

et on écrira $a \equiv b\ [c]$ qui se lit :

" a est congru à b modulo c "

Visualisation des congruences modulo 3

On représente $\mathbb{Z}$ à l'aide d'une droite



- entiers qui s'écrivent $3k$ (reste $= 0$)
- entiers qui s'écrivent $3k+1$ (reste $= 1$)
- entiers qui s'écrivent $3k+2$ (reste $= 2$)