

09/09/20.

Divisibilité:  $a/b \Leftrightarrow \exists k \in \mathbb{Z}, b \cdot q = k \cdot a$ .

Combinaison linéaire:

$a/b$  et  $a/c \Rightarrow \forall (\alpha; \beta) \in \mathbb{Z}^2$ , on a:

$$a / (\alpha b + \beta c).$$

Congruence:  $a \equiv b [n]$ .

$$\begin{cases} a = nq + r & 0 \leq r < n. \\ b = nq' + r & 0 \leq r < n. \end{cases}$$

$$8 \equiv 2 [3].$$

$$\begin{array}{r} \hat{8} \overline{) 3} \\ \underline{-6} \phantom{2} \\ \hline \boxed{2} \end{array}$$

$$\begin{array}{r} \hat{2} \overline{) 3} \\ \underline{-0} \phantom{0} \\ \hline \textcircled{2} \end{array}$$

$$8 \equiv 2 [3].$$

$$a \equiv b [n] \Leftrightarrow n / (a - b).$$

Démonstration:  $a \equiv b [n]$  donc on a:

$\Leftrightarrow$

$$\begin{aligned} \exists (q; r) \in \mathbb{Z}^2 \text{ t.q. } & \begin{cases} a = nq + r & \text{ou } 0 \leq r < n. \\ b = nq' + r & \text{ou } 0 \leq r < n. \end{cases} \end{aligned}$$

$$\Leftrightarrow a - b = nq + r - (nq' + r)$$

$$\Leftrightarrow (a - b) = nq + r - nq' - r.$$

$$\Leftrightarrow (a - b) = n(q - q'). \quad q \in \mathbb{Z} \quad q' \in \mathbb{Z} \text{ donc}$$

$$q - q' \in \mathbb{Z}.$$

$$\text{Soit } K = q - q'$$

$$\Leftrightarrow (a - b) = nK.$$

$$\Leftrightarrow n \mid (a - b)$$

Soleil est bleu  $\Leftrightarrow$  Soleil est bleu.

$$a \equiv b [n] \Leftrightarrow b \equiv a [n].$$

$$a = b \text{ et } b = c. \Rightarrow a = c. \quad 17 \equiv 1 \pmod{4}$$

Dém.

$$a \equiv b [n] \text{ et } b \equiv c [n].$$

$$\text{alors } a \equiv c [n].$$

$$\begin{cases} a = nq + r & \text{ou } 0 \leq r < n. \\ b = nq' + r & \text{ou } 0 \leq r < n. \end{cases}$$

$$\begin{cases} b = nq'' + r. \\ c = nq''' + r. \end{cases}$$

$$8 \equiv 2 [3]. \Leftrightarrow 3 \mid (8 - 2).$$

$$\begin{cases} a = nq + r. \\ c = nq'' + r. \end{cases} \quad \text{Done } a \equiv c [n].$$

$$a \equiv b [n] \Leftrightarrow a - b \equiv 0 [n].$$

$$a \equiv b [n] \Leftrightarrow n \mid (a - b)$$

$$\exists k \in \mathbb{Z} \text{ t.q. } a - b = nk + 0$$

$$0 = n \times 0 + \dots 0$$

Done

$$a - b \equiv 0 [n].$$


---

$$a \equiv b [n] \Leftrightarrow a - b \equiv 0 [n].$$

$$\begin{aligned} & a \equiv b [n] \\ * \Leftrightarrow & n \mid (a - b) \end{aligned}$$

$$a - b \equiv 0 [n].$$

$$n \mid (a - b - 0)$$

$$n \mid (a - b).$$


---

$$\nabla a = b$$

$$a + c = b + d.$$

$$a^m = b^m.$$

$$\nabla c = d.$$

$$a \times c = b \times d.$$

~~$$\frac{a}{c} = \frac{b}{d}.$$~~

$$* a \equiv b [m] \quad * c \equiv d [m].$$

Dém:  $* a + c \equiv b + d [m].$

- $a \equiv b [m] \Leftrightarrow m \mid (a-b)$   
 $\Leftrightarrow \exists k \in \mathbb{Z} \text{ t. q. } (a-b) = m k.$   
 $a - b = m k$

- $c \equiv d [m] \Leftrightarrow m \mid (c-d)$   
 $\Leftrightarrow \exists k' \in \mathbb{Z} \text{ t. q. } c - d = m k'.$

$$a - b + c - d = m k + m k'$$

$$(a+c) - (b+d) = m(k+k'). \quad k+k' \in \mathbb{Z}.$$

$$m \mid (a-b)$$

$$\Leftrightarrow a \equiv b [m].$$

$$m \mid ((a+c) - (b+d)).$$

$$a + c \equiv b + d [m].$$

$$* a \equiv b [m] \quad c \equiv d [m].$$

$\Leftrightarrow$

$$a c \equiv b d [m].$$

$$\exists k \in \mathbb{Z} \text{ t. q. } a - b = m k.$$

$$a = m k + b.$$

$$\exists k' \in \mathbb{Z} \text{ t. q. } c - d = m k'.$$

$$c = m k' + d.$$

$$axc = (mb + b) \times (mb' + d).$$

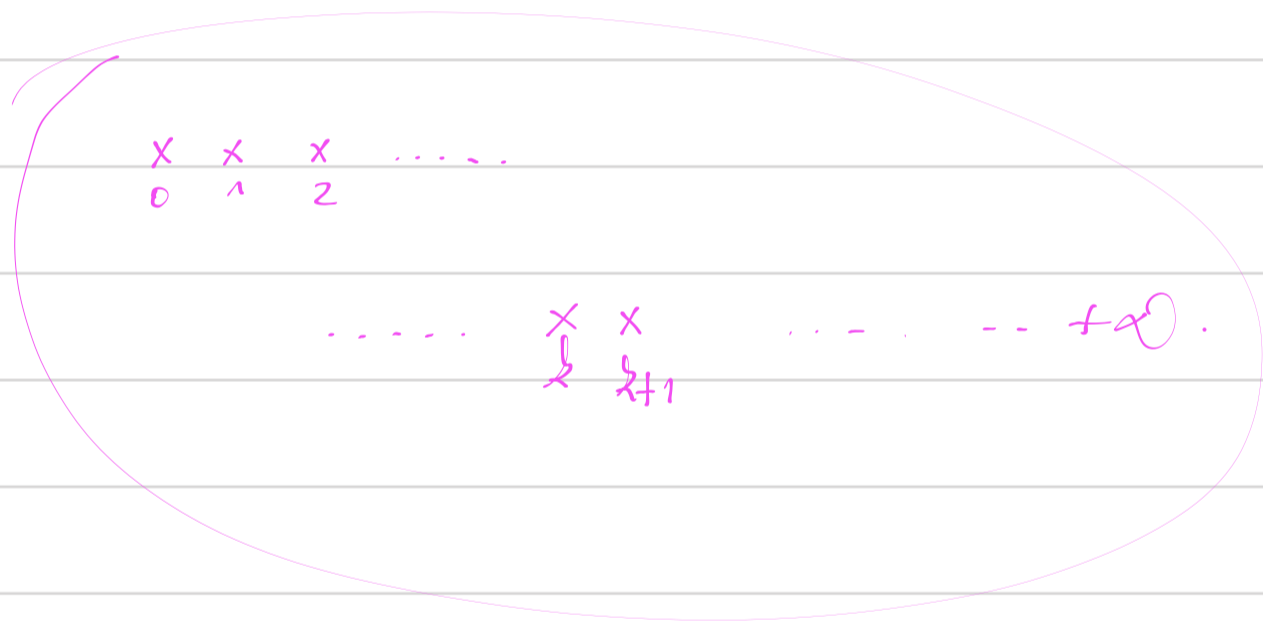
$$axc = m^2bb' + mbd + mb'b' + bcd.$$

$$ac - bd = \underbrace{m(mb'b' + bd + bb')}_{\in \mathbb{Z}}.$$

$$m \mid (ac - bd)$$

$$ac \equiv bd \pmod{m}.$$

$$* \quad a \equiv b \pmod{m} \quad \text{also} \quad \forall k \in \mathbb{N}, \text{ on } a: \quad a^k \equiv b^k \pmod{m}$$



$$1 + 2 + \dots + n = \frac{n(n+1)}{2}$$

$n$	1	2	3	...	$n$	$n+1$
$1 + \dots + n$	1	3	6		$1 + \dots + n$	$1 + \dots + n+1$
$\frac{n(n+1)}{2}$	1	3	6		$\frac{n(n+1)}{2}$	$\frac{(n+1)(n+2)}{2}$

Dém.  $a \equiv b [m] \Leftrightarrow \forall k \in \mathbb{N}, a^k \equiv b^k [m]$ .

Ini:  $k=0$ .  $a^0 = 1$   $b^0 = 1$ .

$$1 \equiv 1 [m].$$

Hérédité: Soit  $n \in \mathbb{N}$ , on suppose que:

$$a^k \equiv b^k [m].$$

$$\text{M. Q. : } a^{k+1} \equiv b^{k+1} [m].$$

$$* a^k \equiv b^k [m].$$

$$* a \equiv b [m].$$

$$a^{k+1} \equiv b^{k+1} [m].$$

$$\text{C.Q. : } \forall k \in \mathbb{N}, a^k \equiv b^k [m].$$

Pour le 16/09/20 faire les exercices à la fin  
du cours

