

IV Propriétés des congruences

Remarque : propriétés évidentes

Soient a et b 2 entiers relatifs soit $c \in \mathbb{Z}^*$

- $a \equiv a [c]$ • $a \equiv b [c] \Leftrightarrow b \equiv a [c]$
- $a \equiv b [c] \Leftrightarrow a \equiv b [-c]$ car c et $-c$ ont les même multiples
- a est un multiple de $c \Leftrightarrow a \equiv 0 [c]$
- $a \equiv b [c] \Leftrightarrow a$ s'écrit $a = kc + b$ $k \in \mathbb{Z}$
- [Si] R est le reste de la division euclidienne de a par c
[Alors] $a \equiv R [c]$

Attention la réciproque est vraie uniquement si $0 \leq R < c$

Dém: la division euclidienne s'écrit $a = kc + r$ $0 \leq r < c$
 $\Leftrightarrow a - r = kc$
 $\Leftrightarrow a \equiv r [c]$

Autre exemple pour la réciproque.

$$17 \equiv 27 [5] \text{ car } 27 - 17 = 10 = 2 \times 5$$

mais 17 n'est pas le reste de la division euclidienne par 5

prop 1: Transitivité

Soient a, a' et a'' des entiers relatifs, et $c \in \mathbb{Z}^*$

[si] $a \equiv a' [c]$ et $a' \equiv a'' [c]$

[Alors] $a \equiv a'' [c]$.

démonstration:

$$a \equiv a' [c] \Leftrightarrow \exists k \in \mathbb{Z} \text{ tel qm } a' - a = kc$$

$$a' \equiv a'' [c] \Leftrightarrow \exists k' \in \mathbb{Z} \text{ tel q } \underline{a'' - a' = k'c}$$

$$\Rightarrow \cancel{a' - a} + \cancel{a'' - a'} = kc + k'c$$

$$\Leftrightarrow a'' - a = c(k + k')$$

$$\Leftrightarrow a'' \equiv a [c]$$

Prop 2: Congruences et opérations

Soient a, b, a', b', k et c des entiers relatifs
tels que $c \neq 0$, $a \equiv b [c]$ et $a' \equiv b' [c]$

1°) $a+k \equiv b+k [c]$, on dit que l'addition est
 $a+a' \equiv b+b' [c]$ compatible avec les congruences

2°) $ka \equiv kb [c]$, la multiplication est compatible
 $aa' \equiv bb' [c]$ avec les congruences

3°) $a-a' \equiv b-b' [c]$

$a^n \equiv b^n [c] \quad \forall n \in \mathbb{N}$

Démonstration.

$$1^\circ) (a+k) - (b+k) = \cancel{a+k} - \cancel{b+k} = a-b$$

Or $a-b$ est un multiple de c car $a \equiv b [c]$

$$\text{donc } a+k \equiv b+k [c]$$

$$\begin{aligned} (a+a') - (b+b') &= a+a' - b-b' \\ &= (a-b) + (a'-b') \end{aligned}$$

$$\text{or } a \equiv b [c] \Leftrightarrow \exists q \in \mathbb{Z}, a = qc + b \Leftrightarrow a-b = qc$$

$$a' \equiv b' [c] \Leftrightarrow \exists q' \in \mathbb{Z}, a' = q'c + b' \Leftrightarrow a'-b' = q'c$$

$$\begin{aligned} \text{donc } (a+a') - (b+b') &= qc + q'c \\ &= c(q+q') \end{aligned}$$

$$\text{donc } a+a' \equiv b+b' [c]$$

$$2^\circ) ka - kb = k(a-b) = kqc = (kq)c$$

$$\text{donc } ka \equiv kb [c]$$

$$a = qc + b$$

$$a' = q'c + b'$$

$$aa' = (qc+b)(q'c+b') = qq'c^2 + b'qc + bq'c + bb'$$

$$\Leftrightarrow aa' = (qq'c + b'q + bq')c + bb'$$

$$\Leftrightarrow aa' - bb' = (qq'c + b'q + bq')c \quad \text{donc la congruence}$$

3°) Soustraction (idem qu pour l'addition)

- Par récurrence

Initialisation: au 1^{er} rang $n=0$

$$a^0 = 1 \text{ et } b^0 = 1$$

donc $a^0 \equiv b^0 [c]$ la propriété est vraie au 1^{er} rang

Hérédité:

→ H.R.: On suppose la propriété vraie à un rang n donné
 $a^n \equiv b^n [c]$

→ au rang suivant: on veut montrer que $a^{n+1} \equiv b^{n+1} [c]$

$$\text{D'après H.R. } \begin{cases} a^n \equiv b^n [c] \\ a \equiv b [c] \end{cases}$$

la multiplication est compatible avec les congruences donc

$$a^n \times a \equiv b^n \times b [c]$$

$$\Leftrightarrow a^{n+1} \equiv b^{n+1} [c]$$

la propriété est héréditaire

Conclusion: $\forall n \in \mathbb{N} \quad a^n \equiv b^n [c]$.

Attention: la division n'est pas compatible avec les congruences

en effet $6 \equiv 8 [2]$

$$\text{mais } \frac{6}{2} \not\equiv \frac{8}{2} [2] \quad \text{car } \frac{6}{2} = 3 \quad \text{et } \frac{8}{2} = 4$$

4-3 n'est pas un multiple de 2

↳ JAMAIS de division avec les congruences

II Complément sur la division euclidienne:

Cas où le diviseur est négatif

La division euclidienne reste semblable mais on doit avoir $0 \leq R < |b|$

exemple $-17 = 3 \times 5 + 2$ division euclidienne de
-17 par 5

$\Rightarrow -17 = -3 \times (-5) + 2$ division euclidienne
par (-5)
car $0 \leq 2 < |-5|$