CONGRUENCES

Définition

Soit p un entier naturel et a et b deux entiers relatifs.
On dit que a est congru à b modulo p, si a et b ont le même reste dans la division euclidienne par p.

On note : $a \equiv b$ [p] ou $a \equiv b$ (modulo p) ou $a \equiv b$ (p)

Remarques :

- $a \equiv b$ [p] $\Leftrightarrow$ $b \equiv a$ [p]
- $a \equiv 0$ [p] $\Leftrightarrow$ a est divisible par p
- Si $a \equiv r\ (b)$ et si $0 \leq r < b$, alors r est le reste de la division euclidienne de a par b

Propriétés

- $a \equiv b$ [p] $\Leftrightarrow$ $b - a$ est multiple de p
- Si $a \equiv b$ [p] et si $b \equiv c$ [p] alors $a \equiv c$ [p]
- Si $a \equiv b$ [p] et si $a' \equiv b'$ [p]

  alors $a + a' \equiv b + b'$ [p] ; $a - a' \equiv b - b'$ [p] ; $aa' \equiv bb'$ [p] ; $a^n \equiv b^n$ [p] $n \in \mathbb{N}^*$
- Si $a \equiv b$ [p] alors pour tout $c \in \mathbb{Z}$ $a + c \equiv b + c$ [p] ; $a - c \equiv b - c$ [p] ; $ac \equiv bc$ [p]

Preuve :

- Supposons que $a \equiv b$ [p] alors a et b ont le même reste r dans la division euclidienne par p.
  On peut donc écrire $a = p \times k + r$ et $b = p \times k' + r$ avec $k \in \mathbb{Z}$, $k' \in \mathbb{Z}$, $r \in \mathbb{N}$ et $0 \leq r < p$
  Donc $b - a = p \times k' + r - (p \times k + r) = p \times k' - p \times k = p(k' - k)$
  $k' - k$ étant un entier relatif , on en déduit que $b - a$ est multiple de p.

  Réciproquement, Supposons que $b - a$ est multiple de p, on peut écrire $b - a = k \times p$ avec $k \in \mathbb{Z}$
  Notons q et r le quotient et le reste de la division euclidienne de b par p. On a donc :
  $$b = p \times q + r \Leftrightarrow b - a = p \times q + r - a \Leftrightarrow k \times p = p \times q + r - a \Leftrightarrow a = p \times q + r - kp \Leftrightarrow a = p(q - k) + r$$
  $q - k$ est un entier relatif et r un entier naturel tel que $0 \leq r < p$ (puisque r est le reste de la division euclidienne de b par p)
  On en déduit que r est le reste de la division euclidienne de a par p.
  Donc a et b ont le même reste dans la division euclidienne par p et par conséquent $a \equiv b$ [p]

- Si $a \equiv b$ [p] , alors a et b ont le même reste dans la division euclidienne par p.
  Si $b \equiv c$ [p] , alors b et c ont le même reste dans la division euclidienne par p.
  On en déduit que a et c ont le même reste dans la division euclidienne par p et par conséquent $a \equiv c$ [p]

- - Si $a \equiv b$ [p] et si $a' \equiv b'$ [p] , alors $b - a$ est un multiple de p et $b' - a'$ est un multiple de p.
  On en déduit, d'après les propriétés des multiples que :
  $(b - a) + (b' - a')$ et $(b - a) - (b' - a')$ sont des multiples de p
  C'est-à-dire $(b + b') - (a + a')$ et $(b - b') - (a - a')$ sont des multiples de p
  Donc $a + a' \equiv b + b'$ [p] et $a - a' \equiv b - b'$ [p]

  - Puisque $b - a$ est un multiple de p , $a'(b - a)$ est un multiple de p.
  Puisque $b' - a'$ est un multiple de p , $b(b' - a')$ est un multiple de p.
  On en déduit que $a'(b - a) + b(b' - a')$ est un multiple de p.
  C'est-à-dire $a'b - a'a + bb' - ba'$ est un multiple de p.
  On a alors $bb' - aa'$ est un multiple de p , c'est-à-dire $aa' \equiv bb'$ [p]

  - Considérons pour $n \in \mathbb{N}^*$ la proposition $P(n)$: $a^n \equiv b^n$ [p]
    - Pour $n = 1$, on a $a^1 = a$ et $b^1 = b$ et on sait que $a \equiv b$ [p] donc P(1) est vraie

    - Supposons que la proposition P(n) est vraie pour un entier $n \geq 1$.
      On a $a^n \equiv b^n$ [p] et $a \equiv b$ [p] . On en déduit que (d'après la propriété précédente) :
      $$a^n \times a \equiv b^n \times b \text{ [p]} \Leftrightarrow a^{n+1} \equiv b^{n+1} \text{ [p]}$$
      La proposition P(n+1) est donc vraie.
      On a donc démontré par récurrence que P(n) est vraie pour tout entier $n \geq 1$

      Donc $a^n \equiv b^n$ [p] pour tout $n \in \mathbb{N}^*$

- - Si $a \equiv b$ [p] alors $b - a$ est un multiple de p.
  Or, on peut écrire $b - a = (b + c) - (a + c)$
  Donc $(b + c) - (a + c)$ est un multiple de p.
  On en déduit que $a + c \equiv b + c$ [p] pour tout $c \in \mathbb{Z}$

  - De même on peut écrire $b - a = (b - c) - (a - c)$.
  Donc $a - c \equiv b - c$ [p] pour tout $c \in \mathbb{Z}$
  D'autre part, puisque $b - a$ est un multiple de p , pour tout $c \in \mathbb{Z}$, $c(b - a)$ est un multiple de p,
  c'est-à-dire que $bc - ac$ est un multiple de p donc $ac \equiv bc$ [p]

Remarque :

La relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

Attention :

La relation de congruence n'est pas compatible avec la division ni avec la racine carrée.
Par exemple $44 \equiv 8$ [6] , mais on ne peut pas diviser par 4 pour affirmer que 11 est congru à 2 modulo 6.
ou encore $4 \equiv 16$ [12] , mais on ne peut pas prendre la racine carrée pour affirmer que 2 est congru à 4 modulo 12
On ne pourra en aucun cas simplifier dans une congruence comme on simplifie dans une égalité:
Une congruence du type $2x \equiv 2y$ [p] ne pourra pas être simplifiée par 2