

II. Congruences modulo n

Introduction :

On cherche à ranger les nombres (à les catégoriser) par rapport à leur reste dans la division euclidienne par n .

Par exemple, on range les nombres selon leur reste dans la division euclidienne par 3.

On a 3 restes possibles : 0 (les multiples), 1 et 2.

Reste 0	Reste 1	Reste 2
0	1	2
3	4	5
6	7	8
9	10	11
12	13	14
...	...	...
Multiples de 3		
Forme $3k$	Forme $3k + 1$	Forme $3k + 2$
$x \equiv 0 [3]$	$x \equiv 1 [3]$	$x \equiv 2 [3]$
x congrue à 0 modulo 3	x congrue à 1 modulo 3	x congrue à 2 modulo 3

Faites le lien avec les angles sur le cercle trigonométrique : ils sont définis « à 2π près », c'est-à-dire qu'on retrouve le même point si on parcourt le cercle k fois (angle $+2k\pi$)

Par ex : $\frac{13\pi}{3} = \frac{\pi}{3} + 2 \times 2\pi$

Ou aussi $\frac{13\pi}{3} \equiv \frac{\pi}{3} [2\pi]$

Si on connaît la division euclidienne, on trouve la congruence

Exemples : $75 = 3 \times 24 + 3$ on en déduit $75 \equiv 3 [3]$ ou d'ailleurs $75 \equiv 0 [3]$

a. Définitions

1^{ère} définition

Pour un entier $a \in \mathbb{Z}$ et un entier naturel $n \in \mathbb{N}$

Si a a pour reste r dans la division euclidienne par n , on dit que a congrue à r modulo n

Notations : $a \equiv r [n]$ ou $a \equiv r \text{ mod } (n)$

Conséquences : il existe un réel k tel que $a = r + kn$. Par ex, si $x \equiv 3 [7]$, il existe k tel que $x = 7k + 3$

Exemples : **a.** $19 \equiv \dots [3]$ **b.** $27 \equiv \dots [8]$ **c.** $157 \equiv \dots [10]$ **d.** $846 \equiv \dots [2]$

Réponses : **a.** $19 \equiv 1 [3]$ **b.** $27 \equiv 3 [8]$ **c.** $157 \equiv 7 [10]$ **d.** $846 \equiv 0 [2]$

Les modulus 2, 10 et 5 sont très faciles (pairs ou impairs pour 2, chiffre des unités pour 10...)

Dans un modulo 3, ou 9, le nombre a le même reste que la somme de ses chiffres (et ça se démontre)

Propriété $a \equiv 0 [n] \Leftrightarrow a$ est un multiple de $n \Leftrightarrow$ Il existe $k \in \mathbb{Z}$ tel que $a = kn$

2^{ème} définition

Soient deux entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et un entier naturel $n \in \mathbb{N}$

a congrue à b modulo n si et seulement si **a et b ont le même reste** dans la division euclidienne par n

Autrement dit : $a \equiv b [n] \Leftrightarrow a \equiv r [n] \text{ et } b \equiv r [n]$

Propriété

a congrue à b modulo n si et seulement si **n divise $a - b$** (ou $a - b$ est un multiple de n)

$a \equiv b [n] \Leftrightarrow a - b \equiv 0 [n] \Leftrightarrow$ Il existe $k \in \mathbb{Z}$ tel que **$a - b = kn$**

Remarque : on a toujours $a \equiv a [n]$ et $a \equiv 0 [1]$

Exemples : 136 et 41 sont-ils congrus modulo 5 ?

Réponses : **a. Méthode 1** On calcule la différence : $136 - 41 = 95$ qui est bien un multiple de 5, donc ils sont congrus modulo 5

b. Méthode 2 $136 \equiv 1 [5]$ et $41 \equiv 1 [5]$: même reste, ils sont congrus modulo 5

On peut faire des « chaînes » de congruences en rajoutant ou en enlevant n autant de fois qu'on veut

Ex : $35 \equiv 3 [8] \equiv 11 [8] \equiv 19 [8]$ ou $35 \equiv -5 [8] \equiv -13 [8]$ etc...

Ce qui permet de trouver le b dans l'intervalle qu'on veut

b. Opérations

Règles d'opérations

Si $a \equiv b [n]$ on a :

- $a + c \equiv b + c [n]$
- $a \times c \equiv b \times c [n]$
- $a^p \equiv b^p [n]$

Si $a \equiv r [n]$ et $b \equiv s [n]$ on a :

- $a + b \equiv r + s [n]$
- $ab \equiv rs [n]$

Attention !!

Les congruences **ne marchent pas avec la division** (nombres entiers obligent)

Exemples :

$75 \equiv 5 [7]$ et $44 \equiv 2 [7] \Rightarrow$ Addition $75 + 44 \equiv 5 + 2 [7] \Leftrightarrow 119 \equiv 7 [7] \equiv 0 [7]$ (multiple de 7)

Multiplication $75 \times 44 \equiv 5 \times 2 [7] \Leftrightarrow 3300 \equiv 10 [7] \equiv 3 [7]$

Puissance $44^3 \equiv 2^3 [7] \equiv 8 [7] \equiv 1 [7]$

On peut faire des tableaux de congruence, où on range les opérations selon les restes :

Tableau de congruences de $x + 11$ modulo 3

$x \equiv \dots [3]$	0	1	2
$x + 11$	11	12	13
$x + 11 \equiv \dots [3]$	2	0	1

Tableau de congruences de $7x$ modulo 5

$x \equiv \dots [5]$	0	1	2	3	4
$7x$	0	7	14	21	28
$7x \equiv \dots [5]$	0	2	4	1	3

Quels sont les nombres x tels que $x + 11$ soit un multiple de 3 ?

$\Rightarrow$ **Les nombres $x = 3k + 1$ avec $k \in \mathbb{Z}$**

Dire, sans calculer le produit, si $7 \times 126 \equiv 2 [5]$

$\Rightarrow 126 \equiv 1 [5]$ donc $7 \times 126 \equiv 2 [5]$