Définition : Soit n un entier naturel non nul.

Deux entiers a et b sont congrus modulo n signifie $a - b$ est divisible par n.

On note $\boldsymbol{a \equiv b[n]}$ ou $\boldsymbol{a \equiv b(n)}$ ou $\boldsymbol{a \equiv b(mod\ n\ )}$.

Cela revient à dire :

$$\boldsymbol{a \equiv b[n] \Leftrightarrow \textbf{il existe } k \in \mathbb{Z} \textbf{ tel que } a = nk + b}$$

Propriété : Soit n un entier naturel non nul.

Deux entiers a et b sont congrus modulo n

$\Leftrightarrow$ la division euclidienne de a par n a le même reste que la division euclidienne de b par n.

Démonstration :

$a = nq + r$ avec $0 \leq r < n$; $b = nq' + r'$ avec $0 \leq r' < n$

- Si $r = r'$:

$a - b = nq + r - nq' - r' = n(q - q')$ donc **$a - b$ est divisible par n** et donc $\boldsymbol{a \equiv b[n]}$.

- Si a et b sont congrus modulo n :

$a - b = nq + r - nq' - r' = n(q - q') + r - r'$

Donc $r - r' = a - b - n(q - q')$

Comme $a \equiv b[n]$, $a - b$ est divisible par n et donc $r - r'$ est divisible par n.

Par ailleurs, $0 \leq r < n$ et $0 \leq r' < n$

Donc $-n < -r \leq 0$ et $0 \leq r' < n$ donc $-n < r' - r \leq n$

$r - r'$ est un multiple de n compris entre $-n$ et n donc $r - r' = 0$, soit $r = r'$.

Exemple : On a vu que $21 \equiv 6[5]$.

Les égalités euclidiennes $21 = 4 \times 5 + 1$ et $6 = 1 \times 5 + 1$ montrent que le reste de la division de 21 par 5 est égal au reste de la division de 6 par 5.

Propriétés : **Soit n un entier naturel non nul.**

a) $a \equiv a[n]$ pour tout entier relatif a.

b) Si $a \equiv b[n]$ alors $b \equiv a[n]$

c) Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (Relation de transitivité)

d) Si r est le reste dans la division euclidienne de a par n,

alors $a \equiv r[n]$

Démonstration :

a) $a - a = 0$ est divisible par n.

c) $a \equiv b[n]$ et $b \equiv c[n]$ donc n divise $a - b$ et $b - c$

donc n divise $a - b + b - c = a - c$ donc $a \equiv c[n]$

Propriété (Opérations) : Soit n un entier naturel non nul.
Soit a, b, a' et b' des nombres relatifs tels que

si $\boldsymbol{a \equiv b[n]}$ et $\boldsymbol{a' \equiv b'[n]}$ alors on a :

$$\boldsymbol{a + a' \equiv b + b'[n]}$$

$$\boldsymbol{a - a' \equiv b - b'[n]}$$

$$\boldsymbol{a \times a' \equiv b \times b'[n]}$$

$$\boldsymbol{a^p \equiv b^p[n]} \text{ avec } p \in \mathbb{N}$$

Attention : on ne peut pas simplifier une congruence comme une égalité.
$2a \equiv 2b[n]$ n'implique pas $a \equiv b[n]$.
ex. $10 \equiv 6[4]$ soit $2 \times 5 \equiv 2 \times 3[4]$or $5 \equiv 1[4]$ et 5 n'est pas congru à 3 modulo 4
Les congruences sont compatibles avec les additions, soustractions, multiplications

mais pas les divisions.

Exercices

1) Résoudre dans $\mathbb{Z}$ les systèmes suivants :

a) $\begin{cases} x \equiv -2(5) \\ x > 0 \end{cases}$ b) $\begin{cases} x + 2 \equiv -1(7) \\ 100 \leq x < 125 \end{cases}$

2) Trouver les restes de la division euclidienne par 7 des nombres :
a) $351^{12} \times 85^{15}$ b) $16^{12} - 23^{12}$

3) Vérifier que $2^4 \equiv -1(17)$ et $6^2 \equiv 2(17)$.
Quel sont les restes de la division par 17 des nombres $1\,532^{20}$ et 346^{12} ?

4) Démontrer que pour tout entier naturel k, on a : $5^{4k} - 1$ divisible par 13.

5) a) Quels sont les restes possibles de la division de $3^n par\ 11$?
b) En déduire les entiers n pour lesquels $3^n + 7$ est divisible par 11.

6) Déterminer les entiers n tels que $2^n - 1$ est divisible par 9.

7) On pose $A_n = n^5 - n$ avec $n \in \mathbb{N}$
a) Montrer que A_n est pair.
b) Montrer que A_n est divisible par 3.
c) En utilisant les congruences modulo 5, démontrer que A_n est divisible par 5.
d) Pourquoi A_n est-il divisible par 30 ?

8) Déterminer le reste dans la division euclidienne de 11^{2011} par 7.