Le cours – T° exp : Divisibilité et congruence

Divisibilité dans $\mathbb{Z}$

Soit a et b deux **entiers relatifs**.
a **divise** b s'il existe un entier relatif k tel que $b = ka$ $k \in \mathbb{Z}$.

On dit également :
a est un **diviseur** de b, b est **divisible** par a, b est un **multiple** de a.

La notation **a|b** signifie **a divise b**

Transitivité : Si a divise b et b divise c alors a divise c.

Combinaison linéaire : Si c divise a et b alors c divise $\alpha a + \beta b$ où α et β sont deux entiers relatifs.

Division euclidienne

Soit a un entier relatif et b entier naturel non nul.
Il existe un **unique** couple d'entiers $(q\ ;\ r)$ tel que $a = bq + r$ avec $0 \leq r < b$.

q est appelé le **quotient** de la division euclidienne de a par b.
r est appelé le **reste**.

Congruences

Soit n un **entier naturel** non nul.
Deux entiers a et b sont **congrus modulo n** lorsque $a - b$ est divisible par n.
On note $a \equiv b\ [n]$

Deux entiers a et b sont congrus modulo n, si et seulement si, la **division euclidienne de a par n a le même reste que la division euclidienne de b par n**.

La congruence est une **relation d'équivalence** :
- **Réflexivité** : $a \equiv a\ [n]$
- **Symétrie** : Si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$
- **Transitivité** : Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$

Soit a, b, a' et b' des nombres relatifs tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors on a :

$$a + a' \equiv b + b'\ [n]$$
$$a - a' \equiv b - b'\ [n]$$
$$a \times a' \equiv b \times b'\ [n]$$
$$a^p \equiv b^p\ [n] \qquad \text{avec } p \in \mathbb{N}$$

Les méthodes – T° exp : Divisibilité et congruence