- DIVISIBILITÉ ET CONGRUENCES - MATH EXP chapitre 6 : L'ESSENTIEL DU COURS

Entiers et entiers naturels :
$\mathbb{N} \subset \mathbb{Z}$

L'ensemble $\{0;1;2;\ldots\}$ est appelé ensemble des **entiers naturels** . Il est noté $\mathbb{N}$.
L'ensemble $\{\ldots;-3;-2;-1;0;1;2;3;\ldots\}$ est appelé ensemble des **entiers relatifs (ou entiers)** . Il est noté $\mathbb{Z}$.

Propriétés :

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Une partie non vide de $\mathbb{Z}$ n'a pas nécessairement de plus petit élément.

- La somme et le produit de deux entiers naturels sont des entiers naturels.
- La somme et le produit de deux entiers relatifs sont des entiers relatifs.

Divisibilité :
Pour indiquer que a divise b, on note $a \mid b$.

Soit a et b deux entiers relatifs .
S'il existe un entier relatif k tel que $b = k \times a$, on dit que b est un **multiple** de a ou que a est un **diviseur** de b .
On dit aussi que b est **divisible** par a et que a **divise** b . (on ne dit jamais que b multiplie a)

Propriétés :

Soit a,b et c trois entiers relatifs

- Si a divise b et si $b \neq 0$, alors $|a| \leq |b|$.
- Tout entier relatif $b \neq 0$ a un nombre fini de diviseurs.
- Si a divise b, alors a divise bc.
- Si a divise b et si a divise c alors a divise toute combinaisons linéaires $bu + cv$ (donc $b+c$ et $b-c$) où u et v sont des entiers relatifs.
- 1, -1, a, $-a$ sont des diviseurs de a.
- Si a divise b alors $-a$ divise b , a divise $-b$ et $-a$ divise $-b$.
- Si a divise b et si b divise a , alors $a = b$ ou $a = -b$. (c'est-à-dire que $|a| = |b|$)
- Si a divise b et si b divise c, alors a divise c.
- Si a divise b alors pour tout entier relatif c, ac divise bc.

On peut traduire ces propriétés en termes de multiples . Par exemple : Si b est un multiple de a, alors bc est un multiple de a.

Division euclidienne d'un entier naturel:

Soit a un entier naturel et b un entier naturel non nul.
Il existe un unique couple $(q\,;r)$ d'entiers naturels tel que : $a = bq + r$ et $r < b$.
a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.
On dit que le couple unique $(q\,;r)$ est le résultat de la division euclidienne de a par b.

Remarque :

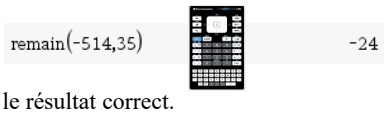
- Si $r = 0$, alors a est divisible par b.
- Le reste d'une division euclidienne par 2 est soit 0 soit 1.
- Tout nombre pair s'écrit sous la forme $2k$ avec $k \in \mathbb{Z}$.
- Tout nombre impair s'écrit sous la forme $2k+1$ avec $k \in \mathbb{Z}$.

Avec une TI-nspire

Division euclidienne d'un entier :

Soit a un entier relatif et b un entier naturel non nul.
Il existe un unique couple $(q\,;r)$, $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que : $a = bq + r$ et $r < b$

Attention :
Dans le cas d'entiers négatifs, les fonctions des calculatrices ne donnent pas toujours les résultats attendus, elles peuvent donner un reste négatif.
Il faudra donc faire preuve de vigilance dans leur utilisation et savoir rétablir le résultat correct.



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

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.

Remarque :

- $a \equiv b \ [p] \Leftrightarrow b \equiv a \ [p]$
- $a \equiv 0 \ [p]$ si et seulement si 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 :
La relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

- $a \equiv b \ [p] \Leftrightarrow b - a$ 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 $c \in \mathbb{Z}$ $a + c \equiv b + c \ [p]$; $a - c \equiv b - c \ [p]$; $ac \equiv bc \ [p]$

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