# Index



## Fiche en chantier....

Divisibilité, multiples de …, division euclidienne, congruences, … sont inséparables ….

### *Divisibilité :*

**Où** : dans les entiers (ensemble $\mathbb{Z}$) :
**Définition** : un entier $a$ divise un entier $b$ non nul si et seulement si, il existe un entier $q$ tel que $b = aq$.

***Conséquences immédiates et importantes*** :
0 ne peut pas être un diviseur de $b$ non nul puisque $0 \times q = 0$.
1 et $b$ sont toujours des diviseurs de 1 et $b$.
Si $a$ est un diviseur de $b$ alors $b$ est un multiple de $a$.
Si $b$ est un multiple de $a$ alors $a$ est un diviseur de $b$.

(On considère l'un ou l'autre point de vue suivant le contexte …).

**Lien avec la division euclidienne :**
***Définition de la division euclidienne :***
La division euclidienne de $b$ (dividende) par $a$ (diviseur) est la recherche du couple d'entiers $(q ; r)$ (quotient ; reste) où $0 \leqslant r < a$ tel que $b = aq + r$.

Il en résulte que $a$ divise $b$ si et seulement si le reste dans la division euclidienne est égal à 0.

**Notions associées :**
- Liste de diviseurs d'un entier ….
La décomposition en un produit de facteurs premiers est utile dans ce cas …

- Quand on a deux entiers $a$ et $b$, il est très utile de déterminer les diviseurs communs aux deux entiers $a$ et $b$. (et/ou les multiples communs).
Les diviseurs communs sont ceux de leur PGCD.
Les multiples communs sont ceux de leur PPCM.

- ***Propriété très importante :***
Si $d$ est un diviseur commun à $a$ et $b$ alors $d$ divise $ax + by$ où $x$ et $y$ sont des entiers.

### *Congruences.*

**Définition :**

Deux entiers $a$ et $b$ sont congrus modulo $n$ si dans la division euclidienne par $n$ de $a$ et $b$, les restes sont égaux.

Autrement dit : Si on écrit $a = n \times k + r$ avec $0 \leqslant r < n$ et $b = n \times k' + r'$ avec $0 \leqslant r' < n$

$a \equiv b$ (modulo $n$) si et seulement si $r = r'$.

ou encore :
$a - b$ est un multiple de $n$. (Puisque le reste de $a - b$ dans la division par $n$ sera nul).

*(C'est la même définition avec les angles modulo $2\pi$,*
*deux angles sont " égaux " modulo $2\pi$ lorsque leur différence est un multiple de $2\pi$ ($\alpha = \beta + 2k\pi$ ; $k \in \mathbb{Z}$) )*

les congruences sont très efficaces car elles sont " compatibles " avec
- l'addition
- la soustraction
- la multiplication (et les puissances)

Le seul problème est avec la division … ça ne marche pas … comme dans $\mathbb{R}$, mais, il y a un " truc " …
Il suffit de comprendre qu'en multipliant chacun des membres par le même nombre, on va pouvoir réduire surtout lorsque le produit donne 1.

Le " truc " :
on veut trouver $x$ tel que $ax \equiv b$ (modulo $n$).
On cherche $k$ tel que $ka \equiv 1$ (modulo $n$)
Et on aura : $kax \equiv kb$ (modulo $n$), d'où, $x \equiv kb$ (modulo $n$).
Pour cela, il faut que dans les congruences modulo $n$, $a$ possède un " inverse "
et c'est là qu'on retrouvera Bézout : si $a$ et $n$ sont premiers entre eux, on aura :
$au + nv = 1$ ce qui équivaut à : $au \equiv 1$ (modulo $n$)

*(Comme dans les matrices : $AX = B$ où $A$, $X$, $B$ sont des matrices, si on connaît $C$ tel que $CA = I$ (matrice identité), on aura : $X = CB$.*
*Pour cela, il faut que $A$ soit inversible et $C$ est la matrice inverse de $B$)*

***Un exemple :***

On veut chercher tous les entiers $x$ tels que $15x \equiv 17$ (23)

15 et 23 sont premiers entre eux, donc, on sait qu'on peut trouver des entiers $u$ et $v$ tels que $15u + 23v = 1$
Si on remarque que $15\times3 = 45$ et $23\times2 = 26$, on a : $-3\times15 + 2\times23 = 1$
soit : $-3\times15 \equiv 1$ (23)
Il suffit donc de multiplier les deux membres de la congruence par $-3$, ce qui donne :
$15x \equiv 17$ (23) implique $-3\times15x \equiv -3\times17$ (23)
$x \equiv -51$ (23)
Les entiers $x$ sont de la forme : $x = -51 + 23k$, $k \in \mathbb{Z}$.
(*On peut présenter autrement en " réduisant " $-51$ par un nombre qui lui est congru modulo 23 (par exemple : $-5$ (puisque $-51 + 2\times23 = -5$) ou par 18 ...))*