Divisibilité et congruence

I] Divisibilité dans $\mathbb{Z}$:

1- Diviseurs d'un entier relatif :

Définition : Soient a et b deux entiers relatifs.
On dit que **a divise b** si et seulement si il existe un entier relatif k tel que $b = ka$.
On dit aussi que :

- a est un **diviseur** de b
- b est **divisible** par a.
- b est un **multiple** de a.

Notation : a divise b se note : $a \mid b$

Exemples :

- 42 est un multiple de – 7 car $42 = -7 \times (-6)$
- L'ensemble des multiples de 5 sont {… ; – 15 ; – 10 ; – 5 ; 0 ; 5 ; 10 ; …}. On note cet ensemble $5\mathbb{Z}$.
- L'ensemble des diviseurs de 6 sont {– 6 ; – 3 ; –2 ; –1 ; 1 ; 2 ; 3 ; 6}
- 0 possède une infinité de diviseurs : tous les entiers relatifs non nuls.

2- Propriétés de divisibilité :

Propriété (transitivité) : Soit a, b et c trois entiers relatifs.
Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

Démonstration :
Si a divise b et b divise c alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.
Donc : $c = k'ka$ et donc il existe un entier relatif $l = kk'$ tel que $c = la$.
Donc : a divise c.

Exemple : $3 \mid 12$ et $12 \mid 60$ **donc :** $3 \mid 60$.

Propriété : Soient a et b deux entiers relatifs.
Si **b ne divise pas a**, alors **aucun multiple de b ne peut diviser a**.

Exemple : Comme 2 ne divise pas 1 001, aucun nombre pair ne divise 1 001.
En effet, si par exemple 10 divisait 1 001 alors 2 diviserait 1 001.

Démonstration : (par l'absurde).
Soient a et b deux entiers tel que b ne divise pas a.
Supposons qu'il existe un entier k tel que kb divise a.
Or b divise kb, et puisque kb divise a, alors b divise a.
Impossible d'après les hypothèses.
Donc : si b ne divise pas a, alors aucun multiple de b ne peut diviser a.

Propriété : Soit a et b des entiers relatifs non nuls.
$a \mid b$ et $b \mid a$ **équivaut à** $a = b$ ou $a = -b$.

Démonstration :
Si $a \mid b$ et $b \mid a$ alors il existe deux entiers k et k' tels que $b = ka$ et $a = k'b$.
D'où : $ab = kk'ab$
Donc $kk' = 1$ car $ab \neq 0$.
k et k' sont ainsi des diviseurs de 1 ; ils sont donc égaux à 1 ou – 1
On a donc $a = b$ ou $a = -b$.

Réciproquement, si a = b ou a = – b, alors, par définition a | b et b | a.

Propriété (combinaisons linéaires) : Soit a, b et c des entiers relatifs non nuls et α et β deux entiers relatifs.

Si c | a et c | b, **alors c | (αa + βb)**

Démonstration :
Si c | a et c | b alors il existe deux entiers k et k' tels que a = kc et b =k'c.
αa + βb = αkc + βk'c = (αk + βk')c où (αk + βk') est un entier.
Donc : c | (αa + βb).

Attention : La réciproque est fausse : 2 | (3 × 2 + 4 × 3) mais 2 ne divise pas 3.

II] Division euclidienne :

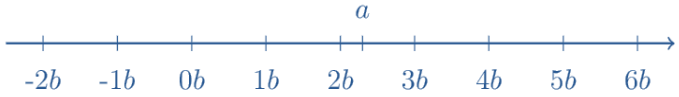
Propriété : Soit a un entier naturel et b entier naturel non nul.
Il existe un unique couple d'entiers (q ; r) tel que :

$$a = bq + r \text{ avec } 0 \leq r < b.$$

Cette écriture s'appelle la division euclidienne de a par b.
q est le quotient, r est le reste, a est le dividende et b est le diviseur de cette division euclidienne.

Exemple : Dans la division euclidienne de 392 par 13, on a : 392 = 13 × 30 + 2.

Démonstration :
Existence :
Soit $x$un réel. La partie entière de x est l'unique entier noté $E(x)$ tel que $E(x) \leq x < E(x) + 1$.



Posons $q = E\left(\frac{a}{b}\right)$. Alors $E\left(\frac{a}{b}\right) \leq \frac{a}{b} < E\left(\frac{a}{b}\right) + 1$, soit $q \leq \frac{a}{b} < q + 1$, donc $bq \leq a < bq + 1$, donc $0 \leq a - bq < b$.
En posant $r = a - bq$, on a bien $a = bq + r$ avec q et r des entiers et $0 \leq r < b$.

Unicité :
Supposons qu'il existe deux couples $(q\,;r)$ et $(q'\,;r')$vérifiant la propriété.
Alors on a $a = bq + r = bq' + r'$d'où $r' - r = b(q - q')$.
Or $0 \leq r < b$, soit $-b < -r < 0$, et comme on sait que $0 \leq r' < b$, on obtient par addition l'encadrement : $-b < r' - r < b$.
Or $r' - r = b(q - q')$ est un multiple de b strictement compris entre $-b$ et b, il ne peut donc s'agir que de 0.
Ainsi $r - r' = 0$ d'où $r = r'$.
D'autre part, $b(q - q') = 0$ donc $q = q'$.
Conclusion, le couple $(q\,;r)$vérifiant la propriété est unique.

Propriétés : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

- b divise a $\Leftrightarrow$ le reste dans la division euclidienne de a par b est 0.
- Dans la division euclidienne de a par b, il n'y a que b restes possibles : tous les entiers entre 0 et $b - 1$. Ainsi, tout entier s'écrit sous une, et une seule, de ces formes : bq, $bq + 1$, $bq + 2$, ..., $bq + (b - 1)$, avec $q \in \mathbb{Z}$.

III] Congruences :

1- Définition :

Définition : Soit n un entier naturel non nul.
Deux entiers **a et b sont dits congrus modulo n** si et seulement si ils **ont le même reste dans la division euclidienne par n**.
On le note : a ≡ b [n]

Remarques :

- On dit aussi que a est congru à b modulo n.
- Par définition, a ≡ b [n] ⟺ b ≡ a [n] et a ≡ a [n].
- Si r est le reste de la division euclidienne de a par n, alors a ≡ r [n] et r est l'unique entier tel que $0 \leqslant r < n$ et a ≡ r [n].

Exemples : $11 \equiv 5\ [3]$ (car $11 = 3 \times 3 + 2$ et $5 = 3 \times 1 + 2$)
$-4 \equiv 2\ [3]$ (car $-4 = 3 \times (-2) + 2$ et $2 = 3 \times 0 + 2$)

2- Propriété fondamentale :

Propriété : Soient n un entier naturel non nul et a et b deux entiers relatifs.
$\boldsymbol{a \equiv b[n]}$ si et seulement si **n divise $a - b$.**

Démonstration :
⇒ Si $a \equiv b[n]$, alors a et b ont le même reste r dans la division euclidienne par n, c'est-à-dire qu'il existe deux entiers relatifs q et q' tels que $a = nq + r$ et $b = nq' + r$.
Ainsi, $a - b = n(q - q')$, avec $q - q'$ entier, donc n divise $a - b$.

⇐ Réciproquement, si n divise $a - b$, alors il existe un entier k tel que $a - b = kn$, d'où $a = b + kn$.
La division euclidienne de a par n se traduit par l'existence de deux entiers q et r tels que $a = nq + r$ et $0 \leq r < n$.
Ainsi, $b + kn = nq + r$ donc $b = n(q - k) + r$ avec $q - k$ entier et $0 \leq r < n$.
On en déduit que r est aussi le reste de la division euclidienne de b par n, soit $a \equiv b[n]$.

Remarque : **a ≡ 0 [n]** si et seulement si **n divise a.**

3- Opérations sur les congruences :

Propriétés : Soit n un entier naturel non nul.
Soient a, a', b, b' et c des entiers relatifs.
Alors on a les relations suivantes :

1. Si $a \equiv b\ [n]$et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$(propriété de transitivité).
2. $a \equiv b\ [n] \iff a - b \equiv 0\ [n]$.
3. $a \equiv b\ [n] \iff a + c \equiv b + c\ [n]$.
4. Si $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$, alors $a + b \equiv a' + b'\ [n]$
   $a - b \equiv a' - b'\ [n]$
   $ab \equiv a'b'\ [n]$.
5. Si $a \equiv b\ [n]$, alors $ac \equiv bc\ [n]$.
6. Pour tout $m \in \mathbb{N}^*$, $a^m \equiv b^m\ [n]$.

Démonstration :

1. Si $a \equiv b[n]$, alors $n \mid (a - b)$, et si $b \equiv c[n]$, alors $n \mid (b - c)$.
   Ainsi, $n \mid (a + b) + (b - c)$, donc $n \mid (a - c)$ donc $a \equiv c[n]$.

2. $a \equiv b[n]$ si et seulement si $a - b$ est divisible par n, c'est-à-dire $a - b = 0$ divisible par n, d'où $a - b \equiv 0[n]$.
3. $a \equiv b[n] \iff n \mid a - b$
   $\iff n \mid (a + c) - (b + c)$ (car $(a + c) - (b + c) = a - b$)
   $\iff a + c \equiv b + c[n]$

4. Si $a \equiv a'[n]$ et $b \equiv b'[n]$, alors $a - a'$ et $b - b'$ sont des multiples de n, dont toute combinaison linéaire des deux est un multiple de n. Ainsi on a :
   $(a - a') + (b - b') = (a + b) - (a' + b')$ est un multiple de n, donc $a + b \equiv a' + b'[n]$.
   $(a - a') - (b - b') = (a - b) - (a' - b')$ est un multiple de n, donc $a - b \equiv a' - b'[n]$.
   $(a - a') \times b + (b' - b') \times a' = ab - a'b + a'b - a'b' = ab - a'b'$ est un multiple de n, donc $ab \equiv a'b'[n]$.

5. $a \equiv b[n]$ donc $a - b$ est divisible par n
   donc $c(a - b)$ est divisible par n
   donc $ca - cb$ est divisible par n
   donc $ca \equiv cb[n]$
   donc $ac \equiv bc[n]$.

6. **Initialisation** : La démonstration est triviale pour $p = 0$ ou $p = 1$.
   Hérédité :
   - Hypothèse de récurrence :
     Supposons qu'il existe un entier k tel que la propriété soit vraie :
     $$a^k \equiv b^k[n]$$
   - Démontrons que : La propriété est vraie au rang $k + 1$:
     $$a^{k+1} \equiv a^k \times a \equiv b^k \times b \equiv b^{k+1}[n]$$

   Conclusion : La propriété est vraie pour $p = 0$ et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel p.