DIVISIBILITÉ ET CONGRUENCES

1) ENSEMBLES $\mathbb{N}$ et $\mathbb{Z}$

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 $\mathbb{Z}$.

Remarques :

- $\mathbb{N}$ est une partie de $\mathbb{Z}$: $\mathbb{N} \subset \mathbb{Z}$.
- 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.

Propriété : *admise*

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.

Exemples :

- Soit A = { 8 ; 12 ; 14 ; 21 } . A est une partie de $\mathbb{N}$. Le plus petit élément de A est 8.
- Soit B l'ensemble des entiers naturels impairs. B est une partie de $\mathbb{N}$. Le plus petit élément de B est 1.

2) DIVISIBILITÉ

Définition :

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)

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

Exemple :
De l'égalité $54 = 6 \times 9$, on peut déduire :

6 est un diviseur de 54 , 9 est un diviseur de 54 , 54 est un multiple de 6 , 54 est un multiple de 9.

Remarque :
L'ensemble des multiples de 3 est l'ensemble des nombres de la forme $3 \times k$ avec $k \in \mathbb{Z}$. Cet ensemble est noté $3\mathbb{Z}$.

Propriétés :

- Soit a et b deux 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.

On peut traduire la première propriété en termes de multiples :
Si n est un multiple non nul de p, alors $|n| \geq |p|$.

Preuve :

- Soit a et b deux entiers relatifs tels que a divise b et $b \neq 0$.
  Puisque a divise b, on peut écrire $b = ak$ avec $k \in \mathbb{Z}$, donc $|b| = |ak| = |a| \times |k|$
  Comme $b \neq 0$, on a $k \neq 0$, donc $|k| \geq 1$ et par conséquent $|b| \geq |a|$.

- Soit b un entier relatif non nul.
  Si a est un diviseur de b, on a vu que $|a| \leq |b|$, donc $-|b| \leq a \leq |b|$
  a peut donc prendre au maximum $2 \times |b| + 1$ valeurs et le nombre de diviseurs de b est fini (inférieur à $2 \times |b| + 1$)

Propriété :

Soit a, b et c trois entiers relatifs.
Si a divise b, alors a divise bc.

On peut traduire la propriété en termes de multiples :
Si b est un multiple de a, alors bc est un multiple de a.

Preuve :
Si a divise b, on peut écrire $b = a \times k$ avec $k \in \mathbb{Z}$.
On a donc $bc = (a \times k) \times c = a \times (kc)$
Or kc est un entier relatif que l'on peut noter k' .
On obtient $bc = a \times k'$ avec $k' \in \mathbb{Z}$. On en déduit que a divise bc.

Remarque :
Tout multiple d'un multiple de a est un multiple de a.

Propriété:

Soit a, b et c trois entiers relatifs.
Si a divise b et si a divise c alors a divise $b + c$ et a divise $b - c$.

Plus généralement, si a divise b et si a divise c alors a divise tout nombre de la forme $bu + cv$ où u et v sont des entiers relatifs.

On peut traduire la propriété en termes de multiples :
Si b et c sont des multiples de a, alors $bu + cv$ est un multiple de a.

Preuve :
Si a divise b, on peut écrire $b = a \times k$ avec $k \in \mathbb{Z}$.
Si a divise c, on peut écrire $c = a \times k'$ avec $k' \in \mathbb{Z}$.
Alors pour tous les entiers relatifs u et v, on peut écrire :

$$bu + cv = aku + ak'v = a\,(ku + k'v).$$

Comme $ku + k'v$ est un élément de $\mathbb{Z}$, on en déduit que a divise $bu + cv$.

- En prenant $u = 1$ et $v = 1$, on obtient que a divise $b + c$.
- En prenant $u = 1$ et $v = -1$, on obtient que a divise $b - c$.

Propriétés :

Soit a, b, c 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.

3) DIVISION EUCLIDIENNE

Propriété d'Archimède :

Soit b un entier naturel non nul.
Pour tout entier naturel a, il existe un entier naturel n tel que $a < nb$.

Preuve :
b étant un entier naturel non nul, on a $b \geq 1$, donc $(a + 1)b \geq a + 1 > a$.
Il suffit donc de prendre $n = a + 1$ pour que nb soit strictement supérieur à a .
Il existe donc un entier naturel n tel que $a < nb$

Remarque :
Cela revient à dire que l'ensemble des multiples de b ($b \neq 0$) n'est pas majoré par a, et ceci pour tout $a \in \mathbb{N}$.
On en déduit que l'ensemble des multiples de b ($b \neq 0$) n'est pas majoré.

Exemple :
$b = 3$; $a = 52$ pour $n \geq 18$, on $a < nb$.

Rappel : Technique de la division d'entiers naturels
On peut écrire $43 = 8 \times 5 + 3$.
43 s'appelle le **dividende**, 5 **le diviseur**, 8 **le quotient** et 3 **le reste**.

43	5
3	8

On a $3 < 5$.
Le reste doit toujours être strictement inférieur au diviseur.

Remarque :
Les multiples de 5 sont 0, 5, 10, 15, 20, 25, 30, 35, 40, 45 et on choisit $40 = 8 \times 5$ car $45 > 43$.
Pour chercher le quotient d'une division, on cherche en pratique les multiples du diviseur et on choisit celui qui précède immédiatement le multiple supérieur au dividende.

Division euclidienne dans $\mathbb{N}$:

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.

Preuve :
Soit a un entier naturel et b un entier naturel non nul.

- Existence du couple $(q\ ;\ r)$

Considérons l'ensemble E des entiers naturels n tels que $a < bn$. E = $\{n \in \mathbb{N} \ / \ a < bn\}$.
Puisque b est non nul, on sait d'après la propriété d'Archimède que l'ensemble E est non vide.
E est donc une partie non vide de $\mathbb{N}$, E a donc un plus petit élément.
Ce plus petit élément p n'est pas nul, car 0 n'appartient pas à E.
On a donc $p \geq 1$. Posons $q = p - 1$. Alors $q \in \mathbb{N}$.
D'autre part $q \notin$ E. (le plus petit élément de E est p et $q < p$)
Puisque $q \notin$ E, on a $bq \leq a$ et comme $p \in$ E, on a aussi $a < bp$ c'est-à-dire $a < b(q + 1)$.
On a donc trouvé un entier naturel q tel que $bq \leq a < b(q + 1)$.
Posons $r = a - bq$. On a $r \in \mathbb{N}$ et $a = bq + r$.
D'autre part : $bq \leq a < b(q + 1) \Leftrightarrow bq \leq a < bq + b \Leftrightarrow 0 \leq a - bq < b \Leftrightarrow 0 \leq r < b$.
Il existe donc un couple $(q\ ;\ r)$ d'entiers naturels tel que $a = bq + r$ et $r < b$.

- Unicité du couple $(q\ ;\ r)$

Supposons qu'il existe un deuxième couple $(q'\ ;\ r')$ vérifiant les mêmes conditions.
On a alors : $bq + r = bq' + r' \Leftrightarrow b(q - q') = r' - r$.
Or, on a : $0 \leq r < b \Leftrightarrow -b < -r \leq 0$
Et $0 \leq r' < b$
On en déduit que : $-b < r' - r < b \Leftrightarrow |r' - r| < b$

Par ailleurs on a vu que $r' - r = b(q - q')$, donc $r' - r$ est un multiple de b .
Si $r' - r$ était non nul, alors on aurait $|r' - r| \geq |b|$ c'est-à-dire $|r' - r| \geq b$ ce qui est en contradiction avec l'inégalité démontrée précédemment.
On a donc nécessairement $r' - r = 0$ et par conséquent $b(q' - q) = 0$, donc $q' - q = 0$
On obtient alors $r' = r$ et $q' = q$.
Le couple $(q\ ;\ r)$ est donc unique.

Remarques :

- 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 $k \in \mathbb{Z}$.

Exemple :
Division euclidienne de 31 par 7: $31 = 7 \times 4 + 3$

Remarque : Division euclidienne de 1715 par 71 avec une calculatrice ou un tableur.

La plupart des calculatrices permettent d'obtenir directement le quotient et le reste d'une division euclidienne.

- **Avec une TInspire:**

$\text{floor}\left(\frac{1715}{71}\right)$ 24

$\text{remain}(1715,71)$ 11

- **Avec un tableur :**

Le quotient est obtenu par ENT() (partie entière)
Le reste est obtenu par MOD(;)

	A	B	C	D
1			=ENT(A2/B2)	=MOD(A2;B2)
2	1715	71	24	11
3				

Division euclidienne d'un entier relatif :

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 $r < b$
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.

Preuve :
Soit a un entier relatif et b un entier naturel non nul.
Si a est un entier positif ou nul, la propriété a déjà été justifiée.

Considérons un entier a négatif.

- Existence du couple $(q ; r)$

a étant négatif, on considère son opposé $-a$ qui est un entier naturel.
D'après le résultat démontré sur les entiers naturels,
il existe un unique couple $(q ; r)$, $q \in \mathbb{N}$ et $r \in \mathbb{N}$ tel que : $-a = bq + r$ et $r < b$
Donc $a = -bq - r = b(-q) - r$.

- Si $r = 0$, alors $-r = 0$ donc $-r \in \mathbb{N}$, et le couple $(-q ; -r)$ répond à la question

- Si $r \neq 0$, le couple $(-q ; -r)$ ne répond pas à la question car $-r \in \mathbb{N}$.
  On peut alors écrire $a = b(-q - 1) + b - r$
  On pose $q' = -q - 1$ et $r' = b - r$
  $q' \in \mathbb{Z}$; vérifions que $r' \in \mathbb{N}$.
  b et r étant des entiers, $b - r$ est un entier, donc $b - r \in \mathbb{Z}$.
  De plus $r \neq 0$ et $0 \leq r < b$, donc :
  $$0 < r < b \Rightarrow -b < -r < 0 \Rightarrow b - b < b - r < b \Rightarrow 0 < b - r < b$$
  On a donc $b - r \in$ et $b - r <$ b . Le couple $(-q-1 ; b - r)$ répond donc à la question.

- Unicité du couple $(q ; r)$

L'unicité du couple se démontre exactement de le même façon que pour une division euclidienne dans $\mathbb{N}$.

Exemple :
La division euclidienne de -514 par 35 s'écrit : $-514 = 35 \times (-15) + 11$

Remarque :
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.

4) CONGRUENCES

Définition

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.

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

Remarques :

- $a \equiv b \ [p] \Leftrightarrow b \equiv a \ [p]$
- $a \equiv 0 \ [p]$ 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

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

Preuve :

- Supposons que $a \equiv b \ [p]$ alors a et b ont le même reste r dans la division euclidienne par p.
  On peut donc écrire $a = p \times k + r$ et $b = p \times k' + r$ avec $k \in \mathbb{Z}$, $k' \in \mathbb{Z}$, $r \in \mathbb{N}$ et $0 \leq r < p$
  Donc $b - a = p \times k' + r - (p \times k + r) = p \times k' - p \times k = p(k' - k)$
  $k' - k$ étant un entier relatif , on en déduit que $b - a$ est multiple de p.

  Réciproquement, Supposons que $b - a$ est multiple de p, on peut écrire $b - a = k \times p$ avec $k \in \mathbb{Z}$
  Notons q et r le quotient et le reste de la division euclidienne de b par p. On a donc :
  $$b = p \times q + r \Leftrightarrow b - a = p \times q + r - a \Leftrightarrow k \times p = p \times q + r - a \Leftrightarrow a = p \times q + r - kp \Leftrightarrow a = p(q - k) + r$$
  $q - k$ est un entier relatif et r un entier naturel tel que $0 \leq r < p$ (puisque r est le reste de la division euclidienne de b par p)
  On en déduit que r est le reste de la division euclidienne de a par p.
  Donc a et b ont le même reste dans la division euclidienne par p et par conséquent $a \equiv b \ [p]$

- Si $a \equiv b \ [p]$, alors a et b ont le même reste dans la division euclidienne par p.
  Si $b \equiv c \ [p]$, alors b et c ont le même reste dans la division euclidienne par p.
  On en déduit que a et c ont le même reste dans la division euclidienne par p et par conséquent $a \equiv c \ [p]$

- Si $a \equiv b \ [p]$ et si $a' \equiv b' \ [p]$, alors $b - a$ est un multiple de p et $b' - a'$ est un multiple de p.
  On en déduit, d'après les propriétés des multiples que :
  $(b - a) + (b' - a')$ et $(b - a) - (b' - a')$ sont des multiples de p
  C'est-à-dire $(b + b') - (a + a')$ et $(b - b') - (a - a')$ sont des multiples de p
  Donc $a + a' \equiv b + b' \ [p]$ et $a - a' \equiv b - b' \ [p]$

- Puisque $b - a$ est un multiple de p , $a'(b - a)$ est un multiple de p.
  Puisque $b' - a'$ est un multiple de p , $b(b' - a')$ est un multiple de p.
  On en déduit que $a'(b - a) + b(b' - a')$ est un multiple de p.
  C'est-à-dire $a'b - a'a + bb' - ba'$ est un multiple de p.
  On a alors $bb' - aa'$ est un multiple de p , c'est-à-dire $aa' \equiv bb' \ [p]$

- Soit la proposition $P(n)$: « $a^n \equiv b^n \ [p]$ », pour $n \in \mathbb{N}^*$

  Initialistion :

  Pour $n = 1$, on a $a^1 = a$ et $b^1 = b$ et on sait que $a \equiv b \ [p]$ donc P(1) est vraie

  Hérédité :

  Supposons P(n) vraie pour un entier $n \geq 1$ fixé, c'est à dire $a^n \equiv b^n \ [p]$ (HR)

  Montrons que P($n+1$) est vraie, c'est à dire $a^{n+1} \equiv b^{n+1} \ [p]$

  D'après (HR), on a $a^n \equiv b^n \ [p]$. Par ailleurs $a \equiv b \ [p]$. On en déduit que (d'après la propriété précédente) :

  $$a^n \times a \equiv b^n \times b \ [p] \Leftrightarrow a^{n+1} \equiv b^{n+1} \ [p]$$

  La proposition P($n+1$) est donc vraie.

  Conclusion :

  Donc $a^n \equiv b^n \ [p]$ pour tout $n \in \mathbb{N}^*$

- Si $a \equiv b \ [p]$ alors $b - a$ est un multiple de p.
  Or, on peut écrire $b - a = (b + c) - (a + c)$
  Donc $(b + c) - (a + c)$ est un multiple de p.
  On en déduit que $a + c \equiv b + c \ [p]$ pour tout $c \in \mathbb{Z}$

- De même on peut écrire $b - a = (b - c) - (a - c)$.
  Donc $a - c \equiv b - c \ [p]$ pour tout $c \in \mathbb{Z}$
  D'autre part, puisque $b - a$ est un multiple de p , pour tout $c \in \mathbb{Z}$, $c(b - a)$ est un multiple de p,
  c'est-à-dire que $bc - ac$ est un multiple de p donc $ac \equiv bc \ [p]$

Remarque :

La relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

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