DIVISIBILITÉ DANS Z.
DIVISION EUCLIDIENNE ET CONGRUENCE

1 Divisibilité dans $\mathbb{Z}$

$\mathbb{N}$ est l'ensemble des entiers naturels : $\mathbb{N} = \{0 ; 1 ; 2 ; 3 ; \dots\}$.
$\mathbb{Z}$ est l'ensemble des entiers relatifs : $\mathbb{Z} = \{\dots ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; \dots\}$.

Notation
b divise a se note $b | a$.

Définition 1 Soit a et b deux entiers relatifs.
- a est multiple de b s'il existe un entier relatif k tel que $a = kb$.
- Si $b \neq 0$, b est un diviseur de a si et seulement si a est un multiple de b.

Si b est diviseur de a, on dit aussi que b divise a et que a est divisible par b.

EXEMPLES
- 63 est multiple de -7 car $63 = (-7) \times (-9)$; -7 est un diviseur de 63.
- L'ensemble des multiples de 3 est $\{\dots ; -6 ; -3 ; 0 ; 3 ; 6 ; \dots\}$. On le note $3\mathbb{Z}$.
- Les diviseurs de 18 sont 1, 2, 3, 6, 9, 18 et leurs opposés.
Ceux de 12 sont 1, 2, 3, 4, 6, 12 et leurs opposés.
Les diviseurs communs à 12 et 18 sont 1, 2, 3, 6 et leurs opposés.

Vocabulaire
Un diviseur commun à a et b est un entier relatif qui divise à la fois a et b.

Remarques
- 0 est multiple de tout entier car $0 = 0 \times n$ pout tout entier n.
- Tout entier n non nul a pour diviseurs $1, -1, n$ et $-n$.
Il a un nombre fini de diviseurs tous compris entre $-n$ et n.
- Un entier non nul a une infinité de multiples.

Définition 2 Deux entiers relatifs sont premiers entre eux si leurs seuls diviseurs communs sont 1 et -1.

Propriété 1 Transitivité Soit a, b, c sont des entiers relatifs tels que $b \neq 0$ et $c \neq 0$.
Si c divise b et b divise a, alors c divise a.

On peut aussi énoncer que si a est multiple de b et b multiple de c, a est multiple de c.
Par exemple tout multiple de 8 est un multiple de 4.

Note
$ua + vb$, avec u et v entiers, est une combinaison linéaire entière de a et b.

Propriété 2 Combinaison linéaire Soit a, b, c des entiers relatifs tels que $c \neq 0$.
Si c est un diviseur commun à a et b, alors c divise $a + b$ et $a - b$.
Plus généralement, c divise $ua + vb$ pour tous entiers relatifs u et v.

EXEMPLE
Soit n un entier. Si c divise n et $n + 1$ alors c divise $n + 1 - n = 1$ donc $c = -1$ ou $c = 1$.
Les entiers consécutifs n et $n + 1$ sont premiers entre eux.

Démonstrations.

- **Propriété 1** Par hypothèse, il existe deux entiers relatifs k et k' tels que $b = kc$ et $a = k'b$.
Alors $a = kk'c$ où kk' est un entier relatif. Donc a est multiple de c, avec c non nul. Autrement dit c divise a.
- **Propriété 2** Il existe deux entiers relatifs a' et b' tels que $a = a'c$ et $b = b'c$.
Par conséquent pour u et v entiers relatifs quelconques,
$ua + vb = ua'c + vb'c = (ua' + vb')\,c$ où $ua' + vb'$ est un entier.
Donc $ua + vb$ est multiple de c, avec c non nul. C'est dire que c divise $ua + vb$.
En particulier pour $u = v = 1$, c divise $a + b$, et pour $u = 1$, $v = -1$, c divise $a - b$.

2 Division euclidienne

Note
Pour calculer q et r :
- Avec une calculatrice :
$q = E\left(\frac{a}{b}\right)$ et $r = a - bq$
- Avec Geogebra 5 :
Division[a, b] renvoie la liste $\{q, r\}$
- Avec un tableur, $r = \text{mod}(a, b)$
- Avec la TI-83 Premium : reste (a, b)

Théorème 1 et définition 3

Soit a et b deux entiers naturels avec $b \neq 0$.
Il existe un unique couple (q, r) d'entiers naturels tels que

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

On dit que a est le dividende, b le diviseur, q le quotient et r le reste dans la division euclidienne de a par b.

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

$a = bq + r$
$0 \leqslant r < b$

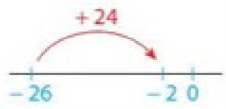
Attention ! Ne pas confondre deux significations du mot *diviseur* : dire que b est le diviseur dans la division euclidienne de a par b ne signifie pas que b est diviseur de a ; b est diviseur de a si le reste dans la division de a par b est nul.

Remarque
Il y a de multiples écritures de a sous la forme $bq + r$.
Pour $a = 103$ et $b = 13$ on a $103 = 13 \times 7 + 12 = 13 \times 6 + 25 = 13 \times 5 + 38$, etc.
Mais seule la 1re égalité, où $0 \leqslant r < b$, est la relation de la division euclidienne de a par b.

Interprétation graphique : on encadre a par deux multiples consécutifs de b.

Cette interprétation graphique permet de comprendre comment on étend la division euclidienne à $\mathbb{Z}$: si a et b sont des entiers relatifs, b non nul, il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ avec $0 \leqslant r < |b|$.

EXEMPLE
$-2 = 26 \times (-1) + 24$ est la relation de la division euclidienne de -2 par 26 avec pour quotient -1 et pour reste 24.



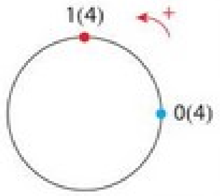
Propriété 3

Dans la division euclidienne de a par b, il y a b restes possibles : $0, 1, \ldots, b - 1$.

EXEMPLE
Tout entier a pour reste 0, 1, 2 ou 3 dans la division par 4 donc s'écrit sous la forme $4k$, $4k + 1$, $4k + 2$ ou $4k + 3$ avec k entier.

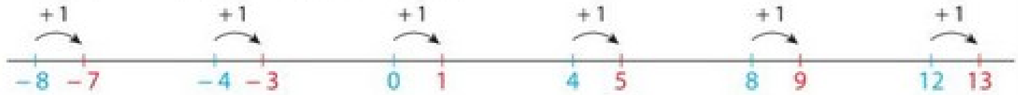
3 Congruences dans $\mathbb{Z}$

Note
Si l'on enroule la droite ci-contre sur un cercle de longueur 4, tous les nombres congrus à 1 modulo 4 sont représentés par un même point du cercle (en rouge).



Propriété 4 et définition 4 Soit c un entier naturel non nul. Deux entiers relatifs a et b ont même reste dans la division par c si et seulement si $a - b$ est un multiple de c.
Si c'est le cas, on dit que a et b sont congrus modulo c (ou que a est congru à b modulo c ou que b est congru à a modulo c).
a est congru à b modulo c se note $a \equiv b\ (c)$ ou $a \equiv b\ [c]$ ou $a \equiv b$ modulo c.

EXEMPLE
Sur la droite numérique, on a repéré en bleu des multiples de 4 et en en rouge des nombres ayant tous pour reste 1 dans la division par 4 ; ils sont tous congrus entre eux :
$5 \equiv 1\ (4)$; $9 \equiv 5\ (4)$; $13 \equiv 5\ (4)$; $-3 \equiv 9\ (4)$.



Remarques
Si a et b sont des entiers relatifs et c un entier naturel non nul :
- a est multiple de c si et seulement si $a \equiv 0\ (c)$;
- les nombres congrus à b modulo c sont les nombres $b + kc$, $k \in \mathbb{Z}$;
- r est le reste dans la division euclidienne de a par c si et seulement si $a \equiv r\ (c)$ ET $0 \leqslant r < c$;
- on peut aussi définir la congruence modulo c avec c entier, $c < 0$, mais les multiples de c et de $-c$ étant les mêmes, $a \equiv b\ (c)$ équivaut à $a \equiv b\ (-c)$. On prend donc $c > 0$ en général.

Propriété 5 Transitivité Soit a, a', a'' des entiers relatifs et c un entier naturel non nul.
Si $a \equiv a'\ (c)$ et $a' \equiv a''\ (c)$, alors $a \equiv a''\ (c)$.

Propriété 6 Congruences et opérations Soit a, b, a', b' des entiers relatifs et c un entier naturel non nul. Si $a \equiv b\ (c)$ et $a' \equiv b'\ (c)$ alors :
- $a + a' \equiv b + b'\ (c)$ et $a - a' \equiv b - b'\ (c)$.
- $aa' \equiv bb'\ (c)$ et pour tout n de $\mathbb{N}^*$, $a^n \equiv b^n\ (c)$.

En particulier, si $a \equiv b\ (c)$, pour tout entier relatif m, on a $ma \equiv mb\ (c)$.

Attention ! La réciproque est fausse. On ne peut pas simplifier une congruence comme une égalité : $22 \equiv 18\ (4)$ mais 11 et 9 ne sont pas congrus modulo 4.

Démonstrations.

- **Propriété 4** On écrit les relations de division euclidienne par c : $a = cq + r$, $0 \leqslant r < c$ et $b = cq' + r'$, $0 \leqslant r' < c$.
On en déduit que $a - b = c(q - q') + r - r'$ et que $-c < r - r' < c$.
  - Supposons que $r = r'$: alors $a - b = c(q - q')$ avec $q - q'$ entier, donc $a - b$ est multiple de c.
  - Réciproquement, si $a - b$ est multiple de c, alors $c | a - b$ et comme $c | c(q - q')$, par la propriété 2, $c | a - b - c(q - q')$, c'est-à-dire $c | r - r'$. Comme $-c < r - r' < c$, il faut que $r - r' = 0$ soit $r = r'$.
- **Propriété 6** Par hypothèse, il existe k et k' entiers tels que $a = b + kc$ et $a' = b' + k'c$.
  - $a + a' = b + b' + (k + k')\, c$ avec $k + k'$ entier, donc $a + a' \equiv b + b'\ (c)$. De même pour $a - a'$.
  - $aa' = bb' + (bk' + b'k + kk'c)\, c$ avec $bk' + b'k + kk'c$ entier, donc $aa' \equiv bb'(c)$.
On en déduit la propriété pour les puissances par un raisonnement par récurrence.