$\mathbb{N}$ désigne l'ensemble des nombres entiers naturels.
$\mathbb{Z}$ désigne l'ensemble des nombres entiers relatifs.

## I. Divisibilité dans $\mathbb{Z}$

Définition : Soit *a* et *b* deux entiers relatifs.

***a* divise *b* s'il existe un entier relatif *k* tel que *b* = *ka*.**
**$\Leftrightarrow$ *a* est un diviseur de *b*,**
**$\Leftrightarrow$ *b* est divisible par *a*,**
**$\Leftrightarrow$ *b* est un multiple de *a*.**

Exemples :

- 54 est un multiple de $-9$ car 54 = $-6 \times (-9)$
- L'ensemble des multiples de 5 sont $\{\ldots ; -15 ; -10 ; -5 ; 0 ; 5 ; 10 ; \ldots\}$.
- 0 est divisible par tout entier relatif ou tout nombre entier relatif $a$ divise 0 ; en effet $0 = a \times 0 \; et \; 0 \in \mathbb{Z}$.

Propriété (transitivité) : Soit *a*, *b* et *c* trois entiers relatifs.
Si *a* divise *b* et *b* divise *c* alors *a* divise *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 ;* on a alors $c = k' \times k \times a$
Donc il existe un entier relatif *l* = *kk*' tel que *c* = *la.*
Donc *a* divise *c*.
Exemple : 3 divise 12 et 12 divise 36 donc 3 divise 36.

Propriété (combinaisons linéaires) :
Soit *a*, *b* et *c* trois entiers relatifs.
Si $c$ divise $a$ et $b$, alors $c$ divise $a + b$ et $a - b$.
Si *c* divise *a* et *b,* alors *c* divise *ma* + *nb* où *m* et *n* sont deux entiers relatifs.
On peut dire que c divise **toutes combinaisons linéaires de $a$ et $b$**.

Démonstration :
Si *c* divise *a* et *b* alors il existe deux entiers relatifs *k* et *k'* tels que *a* = *kc* et *b* = *k'c ;*
on a alors $ma + nb = mkc + nk'c = (mk + nk')c$.
Donc il existe un entier relatif *l* = *mk* + *nk*' tel que *ma* + *nb* = *lc.*

Exemple :
Soit un entier relatif *N* qui divise les entiers relatifs *n* et *n* + 1.
Alors *N* divise $n + 1 - n = 1$.
Donc $N = -1$ ou *N* = 1.

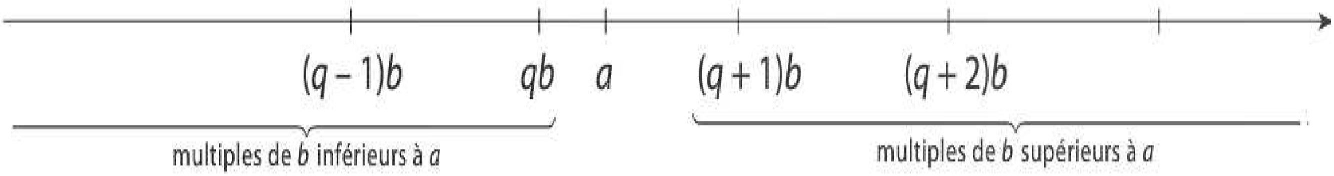
## II. Division euclidienne

Propriété :
Soit *a* un entier naturel et *b* entier naturel non nul.
Il existe un unique couple (*q* ; *r*) tel que *a* = *bq* + *r* avec $0 \leq r < b$.

Définition :
*q* est appelé le quotient de la division euclidienne de *a* par *b*,
*r* est appelé le reste.

Exemple :
Dans la division euclidienne de 412 par 15,
on a : 412 = $15 \times 27 + 7$

Démonstration :
**Existence du couple $(q\,;r\,)$ :**
La suite des multiples de $b$ est : ... ; $-kb$ ; ... ; $-2b$ ; $-b$ ; 0 ; $2b$ ; ... ; $kb$ ; ... avec $k \in \mathbb{N}$
1er cas : $a$ est un multiple de $b$, alors $a$ est un terme de la suite ci-dessus et il existe un entier relatif $q$ tel que $a = bq$.
2ième cas : $a$ n'est pas un multiple de $b$ ; alors il existe des multiples de $b$ inférieurs à $a$ et d'autres supérieurs à $a$.
Ainsi $bq < a < b(q+1)$ où $b(q+1)$ désigne le plus petit multiple de $b$ supérieur à $a$




Conclusion : dans les deux cas ci-dessus, il existe un entier relatif $q$ tel que $bq \leq a < b(q+1)$, c'est-à-dire
$0 \leq a - bq < b$.
On pose $r = a - bq$ et on obtient
$a = bq + r$ avec $0 \leq r < b$.

**Unicité :** on suppose qu'il existe deux couples (*q* ; *r*) et (*q'* ; *r'*).
Donc $a = bq + r = bq' + r'$ et donc : $b(q - q') = r' - r$.
Comme *q* – *q'* est entier, *r'* – *r* est un multiple de *b*.
On sait que $0 \leq r < b$ et $0 \leq r' < b$
donc $-b < -r \leq 0$ et $0 \leq r' < b$
donc par addition $-b < r' - r < b$.
Le seul multiple de *b* compris strictement entre –*b* et *b* est 0, donc *r'* – *r* = 0 et donc *r'* = *r* d'où *q* = *q*'.
On peut étendre la définition au cas où $a$ et $b$ est des entiers relatifs.

Déf. $a$ et $b$ sont deux entiers relatifs avec $b$ non nul.
Il existe un unique couple $(q\,;r)$ avec $q$ entier relatif et $r$ entier naturel tel que $a = bq + r$ et $0 \leq r < |b|$

Ex. $-50 = -3 \times 16 - 2 = -3 \times 16 - 2 + 3 - 3 = -3 \times 17 + 1$