



**Propriété.**

Soit  $a$  et  $b$  deux entiers relatifs avec  $b \neq 0$ . On a les implications suivantes :

- Si  $b$  divise  $a$  alors les **multiples** de  $a$  sont des **multiples** de  $b$ .
- Si  $b$  divise  $a$  alors les **diviseurs** de  $b$  sont des **diviseurs** de  $a$ .

**Notation** : l'ensemble des multiples d'un entier relatif  $b$  dans  $\mathbb{Z}$  est noté  $b\mathbb{Z}$  et l'ensemble des diviseurs de  $b$  est noté  $\mathcal{D}(b)$ .

**Exemple.** Les multiples de 6 sont aussi des multiples de 3 donc  $6\mathbb{Z} \subset 3\mathbb{Z}$ .



**Exercice 2.3.** Déterminer dans  $\mathbb{Z}$  la liste des diviseurs de 7 et en déduire les entiers relatifs  $n$  tels que  $4n + 1$  divise 7.

**Propriété.**

Soit  $a$  et  $b$  deux entiers relatifs avec  $b \neq 0$ .

$$b|a \iff -b|a \iff b|-a \iff -b|-a.$$

**Conséquence** :  $a$  et  $-a$  ont les mêmes diviseurs dans  $\mathbb{Z}$ . Les diviseurs de  $-a$  étant les opposés des diviseurs positifs de  $a$ , on restreindra souvent l'étude à la divisibilité dans  $\mathbb{N}$ .

**Propriété.**

Tout entier  $n$  non nul a pour **diviseurs** 1,  $-1$ ,  $n$  et  $-n$  et a un nombre fini de diviseurs tous compris entre  $n$  et  $-n$ .

**Remarque.** Un entier **non nul** a une infinité de multiples.

**3. Divisibilité et transitivité****Propriété.**

Soit  $a$ ,  $b$  et  $c$  des entiers relatifs tels que  $b \neq 0$  et  $c \neq 0$ .

**Si**  $c$  divise  $b$  et  $b$  divise  $a$ , alors  $c$  divise  $a$ .

**Démonstration**

Par hypothèse,  $c$  divise  $b$  donc il existe un entier relatif  $k$  tel que  $b =$  .  
 De même,  $b$  divise  $a$ , il existe donc un entier relatif  $k'$  tel que  $a =$  .  
 Ainsi  $a =$  où  $kk'$  est un entier relatif. Donc  $a$  est un multiple de  $c$ , avec  $c$  non nul, autrement dit  $c$  divise  $a$  ■

**4. Divisibilité et combinaison linéaire****Propriété.**

Soit  $a$ ,  $b$  et  $c$  des entiers relatifs tels que  $c \neq 0$ .

**Si**  $c$  est un **diviseur commun** à  $a$  et  $b$ , alors  $c$  divise  $ua + vb$  pour tous entiers relatifs  $u$  et  $v$ .

**Démonstration**

Si  $c$  est un diviseur commun de  $a$  et  $b$  alors 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,

$$\begin{aligned} ua + vb &= \\ &= \\ &= \end{aligned}$$

où \_\_\_\_\_ est un entier. Donc  $ua + vb$  est multiple de  $c$  avec  $c$  non nul, par conséquent  $c$  divise  $ua + vb$  ■



**Exercice 3.3.** Déterminer les entiers relatifs  $n$  tels que  $n + 2$  divise  $2n + 8$ .

## II. Division euclidienne

### Théorème

Soit  $a$  et  $b$  deux **entiers naturels** avec  $b \neq 0$ .

Il existe un unique couple  $(q, r)$  d'entiers naturels tels que :

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

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

dividende	diviseur
	quotient
reste	



Il y a de multiples écritures de  $a$  sous la forme  $bq + r$ . Prenons par exemple  $a = 103$  et  $b = 13$ .

On a  $103 = 13 \times 7 + 12$  ou  $103 = 13 \times 6 + 25$  ou encore  $103 = 13 \times 5 + 38$ , etc.

Mais seule la 1<sup>re</sup> égalité, où  $0 \leq r < b$ , est la **relation de la division euclidienne** de  $a$  par  $b$ .

### Propriété.

Dans la division euclidienne de  $a$  par  $b$ , il y a  $b$  restes possibles :

$$0, 1, 2, \dots, b - 1.$$

### Propriété.

Soit  $a$  un entier naturel et  $b$  un entier naturel non nul.

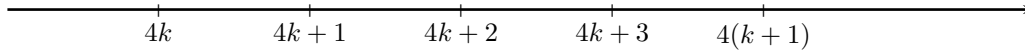
$b$  divise  $a$  si et seulement si le reste dans la division euclidienne de  $a$  par  $b$  est nul.


### Propriété.

Soit  $b$  un entier naturel supérieur ou égal à 2.

Tout **entier relatif** s'écrit sous l'une des formes suivantes :  $bq, bq + 1, bq + 2, \dots, bq + (b - 1)$  où  $q$  est un entier relatif.

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



 **Exercice 4.3.** En utilisant la méthode de disjonction des cas, démontrer que  $n^2 + 1$ ,  $n \in \mathbb{Z}$ , n'est jamais divisible par 3.

### III. Congruences dans $\mathbb{Z}$

#### 1. Propriété et définition

##### Propriété.

Soit  $n$  un entier naturel non nul.

*Deux entiers relatifs*  $a$  et  $b$  ont même reste dans la division euclidienne par  $n$  **si et seulement si**  $a - b$  est *multiple* de  $n$ .

##### Démonstration

On écrit les relations de division euclidienne par  $n$  :

$$a = nq + r, 0 \leq r < n \text{ et } b = nq' + r', 0 \leq r' < n.$$

On en déduit que  $a - b = n(q - q') + r - r'$  et que  $-n < r - r' < n$ .

- Supposons que  $r = r'$  alors  $a - b = n(q - q')$  avec  $q - q'$  entier, donc  $a - b$  multiple de  $n$ .
- Réciproquement, si  $a - b$  multiple de  $n$ , alors  $n | a - b$  et comme  $n | n(q - q')$  alors  $n | a - b - n(q - q')$  c'est-à-dire  $n | r - r'$ . Or  $-n < r - r' < n$ , il faut avoir  $r - r' = 0$  c'est-à-dire  $r = r'$  ■

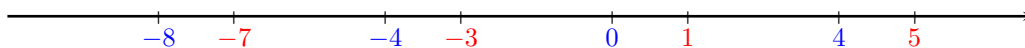
##### Définition.

Soit  $n$  un entier naturel non nul.

Si  $a$  et  $b$  ont *même reste* dans la division euclidienne par  $n$ , on dit que  $a$  et  $b$  sont *congrus modulo*  $n$  et on écrit :  $a \equiv b \pmod{n}$  ou  $a \equiv b \pmod{n}$  ou encore  $a \equiv b [n]$

**Exemple.** Sur la droite numérique, on a repéré en bleu des multiples de 4 et en rouge des nombres ayant tous pour reste 1 dans la division par 4 ; ils sont tous congrus entre eux.

$$5 \equiv 1(4), -7 \equiv 1(4), -3 \equiv 5(4) :$$



**Remarque :**  $a \equiv b [n] \iff b \equiv a [n]$ . On dit aussi que  $a$  et  $b$  sont *congrus modulo*  $n$ .

##### Propriétés.

Soit  $a$  et  $b$  deux entiers relatifs et  $n$  un entier naturel non nul.

- $a \equiv 0 [n]$  si et seulement si  $a$  est *divisible* par  $n$ .
- $a \equiv a [n]$ .
- $r$  est le reste de la division euclidienne de  $a$  par  $n$  **si et seulement si**  $a \equiv r [n]$  *et*  $0 \leq r < n$ .

## 2. Congruence et transitivité

### Propriété.

Soit  $a, b, c$  des entiers relatifs et  $n$  un entier naturel non nul.

Si  $a \equiv b (n)$  et  $b \equiv c (n)$  alors  $a \equiv c (n)$ .

### Idée de la démonstration

Par hypothèse, il existe  $k$  et  $k'$  entiers relatifs tels que  $a = b + kn$  et  $b = c + k'n$ ...

## 3. Compatibilité avec les opérations algébriques

### Propriété.

Soit  $a, b, c$  et  $d$  quatre entiers relatifs et  $n$  un entier naturel non nul.

Si  $a \equiv b [n]$  et  $c \equiv d [n]$  alors :

- $a + c \equiv b + d [n]$
- $a - c \equiv b - d [n]$
- $ac \equiv bd [n]$
- $a^p \equiv b^p [n]$  pour tout entier naturel  $p$ .

En particulier, si  $a \equiv b [n]$ , pour tout entier relatif  $m$ , on a :  $ma \equiv mb [n]$ .



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



### Exercice 5.3.

1. Résoudre dans  $\mathbb{Z}$  l'équation  $3x \equiv 2 [5]$ .
2. Montrer que pour tout entier naturel  $n$  non nul,  $2^{3n} - 1$  est multiple de 7.
3. Déterminer le reste dans la division euclidienne de  $11^{2020}$  par 3.