

Arithmétique

Divisibilité, division euclidienne, congruence

(Magnard Ch.3 p 78)

I / Divisibilité et division euclidienne.

1°) *Théorèmes admis.*

Les axiomes d'arithmétique et de théorie des ensembles permettent de démontrer ces théorèmes :

- **Théorème du bon ordre** (équivalent à l'axiome du choix) de Zermelo (1871 – 1953)
Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.
- **Méthode de descente infinie** de P. de Fermat (1607 – 1665)
Toute suite d'entiers naturels strictement décroissante est nécessairement finie.
- **Principe des tiroirs** (*Pigeonhole principle* en anglais) de G. L. Dirichlet (1805 – 1859)
Si n chaussettes sont rangées dans m tiroirs et que $m < n$ alors il y a un tiroir qui contient au moins deux chaussettes.

2°) *Divisibilité dans $\mathbb{Z}$.*

Soit a et b deux entiers relatifs.

On dit que b divise a si et seulement s'il existe un entier relatif k tel que : $a = k b$.

Notation : On peut écrire $b \mid a$

Vocabulaire : On dit que b est un diviseur de a

On dit que a est un multiple de b

3°) *Propriétés élémentaires.*

Les nombres -1 et 1 divisent tout entier relatif.

Le nombre 0 est un multiple de tout entier relatif

Tout entier (et son opposé) est un diviseur et un multiple de lui-même.

Remarque : Les seuls diviseurs de 1 dans $\mathbb{Z}$ sont -1 et 1 .

4°) *Antisymétrie.*

Soit a et b deux entiers relatifs. Si $a \mid b$ et $b \mid a$ alors : $a = b$ ou $a = -b$.

5°) *Transitivité*

Soit a et b deux entiers relatifs. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

6°) *Combinaisons linéaires*

Soit a, b et c trois entiers relatifs.

- Pour tout entier relatif n : si $a \mid b$ alors $a \mid n b$.
- Si $a \mid b$ et $a \mid c$ alors $a \mid (b + c)$.
- Plus généralement, pour tous entiers relatifs n et p : Si $a \mid b$ et $a \mid c$ alors $a \mid (n b + p c)$.

7°) *Division euclidienne.*

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

Il existe un unique couple d'entiers relatifs $(q ; r)$ tel que : $a = b q + r$ et $0 \leq r < b$

Cette écriture est appelée : division euclidienne de a par b .

Vocabulaire : • On dit que a est le dividende

• On dit que b est le diviseur

• On dit que q est le quotient

• On dit que r est le reste

Remarque : b divise a si et seulement si $r = 0$.

II / Congruence.

1°) Définition et notation.

Soit n un entier naturel supérieur à 1, a et b deux entiers relatifs.

On dit que a est congru à b modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n .

On note alors : $a \equiv b [n]$ ou $a \equiv b (n)$ ou $a \equiv b \pmod{n}$ ou $a \equiv b \bmod n$.

2°) Relation d'équivalence.

La congruence définit une relation d'équivalence, c'est-à-dire qu'elle possède ces 3 propriétés :

- **Réflexivité** : Pour tout entier relatif a , $a \equiv a [n]$.
- **Symétrie** : Pour tous entiers relatifs a et b , si $a \equiv b [n]$ alors $b \equiv a [n]$.
- **Transitivité** : Pour tous entiers relatifs a , b et c , si $a \equiv b [n]$ et $b \equiv c [n]$ alors $a \equiv c [n]$.

3°) Définition équivalente

Soit n un entier naturel supérieur à 1, a et b deux entiers relatifs.

On dit que a est congru à b modulo n si et seulement si leur différence est divisible par n :

$$a \equiv b [n] \text{ équivaut à } 0 \mid a - b$$

4°) Compatibilité avec les opérations

Soit n un entier naturel supérieur à 1, a , b , c et d quatre entiers relatifs.

- **Somme** : Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a + c \equiv b + d [n]$
et donc en particulier, pour tout entier relatif k : Si $a \equiv b [n]$ alors $a + k \equiv b + k [n]$
- **Produit** : Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a c \equiv b d [n]$
et donc en particulier, pour tout entier relatif k : Si $a \equiv b [n]$ alors $k a \equiv k b [n]$
- **Puissance** : Pour tout entier naturel p : Si $a \equiv b [n]$ alors $a^p \equiv b^p [n]$

Attention : On peut aussi soustraire (ajouter l'opposé) mais on ne peut pas diviser...