

# LEÇON N° 10 :

## Division euclidienne dans $\mathbb{Z}$ , unicité du quotient et du reste. Applications. L'exposé pourra être illustré par un ou des exemples faisant appel à l'utilisation d'une calculatrice.

### Pré-requis :

- $\mathbb{Z}$  est bien ordonné et archimédien ;
- Toute partie non vide et minorée (respectivement majorée) de  $\mathbb{Z}$  possède un plus petit (respectivement grand) élément ;
- Notions de groupes, sous-groupes (les sous-groupes de  $\mathbb{Z}$  sont les  $n\mathbb{Z}$ ) ;
- $b$  divise  $a$  ( $a, b \in \mathbb{Z}$ ) s'il existe  $c$  tel que  $a = bc$  (on note  $b|a$ ).

### 10.1 Division euclidienne dans $\mathbb{Z}$

**Théorème 1 (fondamental) :** Soient  $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que  $a = bq + r$ , avec  $0 \leq r < |b|$ .

#### démonstration :

**Unicité :** Si  $a = bq + r = bq' + r'$ , alors  $b(q - q') = r' - r \Rightarrow |b| |q' - q| = |r' - r| < |b| \Rightarrow 0 \leq |q - q'| < 1 \Rightarrow q = q'$  car  $q, q' \in \mathbb{Z}$  et par suite,  $r = r'$ .

**Existence :** Supposons  $b > 0$ . Soit  $A = \{n \in \mathbb{Z} \mid nb \leq a\}$ .  $A$  n'est pas vide (en effet, si  $a \leq 0$ ,  $0 \in A$  et si  $a < 0$ , alors  $a \in A$ ), et majoré par  $\max(0, a)$  (car  $n \leq a/b \leq \frac{1}{b} \max(0, a) \leq \max(0, a)$ ), donc  $A$  admet un plus grand élément que l'on note  $q_A$ . Soit  $r = a - q_A b$ .  $q_A \in A$  ce qui implique que  $q_A b \leq a$ , d'où  $r \geq 0$  et  $q_A + 1$  n'appartient pas à  $A$ . On en déduit que  $(q_A + 1)b > a \Leftrightarrow q_A b + b > a \Leftrightarrow b > a - q_A b \Leftrightarrow r < b = |b|$ , donc  $0 \leq r < |b|$  et l'on a bien  $a = q_A b + r$ . Si  $b \geq 0$ , partir de  $(a, -b)$ .

Ainsi s'achève la démonstration. ■

**Définition 1 :** Déterminer  $q$  et  $r$ , c'est effectuer la division euclidienne de  $a$  par  $b$ . Dans cette division,  $a$ ,  $b$ ,  $q$  et  $r$  sont respectivement appelés *dividende*, *diviseur*, *quotient* et *reste*.

#### Remarques 1 :

1. Si  $r = 0$ , alors  $b$  divise  $a$ .

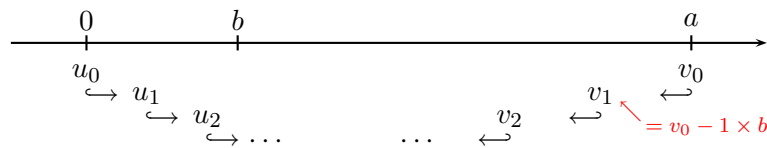
2.  $bq$  n'est pas nécessairement le multiple de  $b$  le plus proche de  $a$ .

Exemple :  $14 = 2 \times 5 + 4$  ( $a = 14, b = 5$ ). Or 15 est un multiple de  $b$  plus proche de  $a$  que  $2b = 10$ .

**Corollaire 1 :** Soit  $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{N}^2$  tel que  $a = bq + r$ , avec  $r < b$ .

*démonstration :* Si  $a < b, q = 0$ . Sinon,  $a - r = bq > 0$ , donc  $q \in \mathbb{N}$ . ■

## Descente de Fermat



$(u_n, v_n) = (q, r)$ , où  $v_n$  est le premier des  $v_i$  construits tels que  $v_n < b$ . L'algorithme se termine car  $v_n = a - nb \Leftrightarrow a \leq (n+1)b$ , et  $\mathbb{Z}$  est archimédien (donc  $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} \mid cb \geq a$ ).

## 10.2 Sous-groupes de $\mathbb{Z}$ et algorithme d'Euclide

**Théorème 2 :** Pour tout sous-groupe  $G$  de  $\mathbb{Z}$ , il existe un unique  $a \in \mathbb{N}$  tel que  $G = a\mathbb{Z}$ .

*démonstration :* Supposons  $G \neq \{0\}$ . Soit  $P = G \cap \mathbb{N}^*$ .  $P$  possède un plus petit élément  $a > 0$ . Par récurrence,  $a\mathbb{Z} \subset G$ . Soit alors  $b \in G$ . Par division euclidienne,  $b = aq + r$  avec  $0 \leq r < a$ .  $G$  étant un groupe,  $r = b - aq \in G$ , et donc  $r \in P \cup \{0\}$  car  $r \geq 0$ . Mais par définition de  $a$ , et comme  $r < a$ ,  $r$  ne peut appartenir à  $P$ , donc  $r = 0$  et par suite,  $b = aq$ . Il vient que  $G \subset a\mathbb{Z}$ . ■

**Proposition 1 :** Soit  $(a, b) \in \mathbb{Z}^2$ .  $G_{ab} = a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid (u, v) \in \mathbb{Z}^2\}$  est un sous-groupe de  $\mathbb{Z}$  et il existe un unique  $d \in \mathbb{N}$  tel que  $G_{ab} = d\mathbb{Z}$ .

*démonstration :*  $0 \in G_{ab}$ , et  $x = au + bv, y = au' + bv' \Rightarrow x - y = a(u - u') + b(v - v') \in G_{ab}$ , donc  $G_{ab}$  est un sous-groupe de  $\mathbb{Z}$ . Le théorème précédent assure l'existence de  $d$  tel que  $G_{ab} = d\mathbb{Z}$ . ■

**Proposition 2 :** Soit  $(a, b) \in \mathbb{Z}^2$ .  $d$  est l'unique entier naturel tel que :

- (i)  $d \mid a$  et  $d \mid b$ ;
- (ii)  $(c \mid a \text{ et } c \mid b) \Rightarrow c \mid d$ .

**démonstration** :  $d$  divise tous les éléments de  $d\mathbb{Z} = G_{ab}$ , donc en particulier  $a$  et  $b$ . Si  $c$  divise  $a$  et  $b$ , alors  $c$  divise  $au + bv$ , donc  $c$  divise  $d$ . ■

**Définition 2** :  $d$  est appelé **Plus Grand Commun Diviseur de  $a$  et  $b$** , noté **PGCD( $a, b$ )** ou  **$a \wedge b$** .

### Algorithme d'Euclide

Soit  $(a, b) \in (\mathbb{N}^*)^2$ , avec  $a \geq b$ . Si  $b|a$ ,  $a \wedge b = b$ . Sinon,  $a = bq_1 + r_1$ , et  $a \wedge b = b \wedge r_1$ <sup>1</sup>. On réitère le procédé :  $r_0 = b$  et  $r_{k-1} = r_k q_{k-1} + r_{k+1}$  ( $k \geq 1$ ) jusqu'à trouver un dernier reste non nul  $r_n$ , diviseur de  $r_{n-1}$  ( $r_{n+1} = 0$ ). Le procédé s'arrête parce que  $r_0 > r_1 > r_2 > \dots > 0$ . Au final,  $a \wedge b = r_n$ .

Exemple : Déterminons  $145 \wedge 7$ .

$$\begin{aligned} 145 &= 7 \times 20 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + \boxed{1} \leftarrow \text{dernier reste non nul} \\ 2 &= 1 \times 2 + 0. \end{aligned}$$

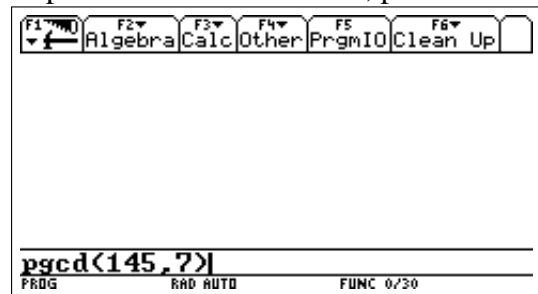
Conclusion :  $145 \wedge 7 = 1$ . On dit que 145 et 7 sont premiers entre eux. Cet algorithme peut facilement être implanté dans une calculatrice :

```

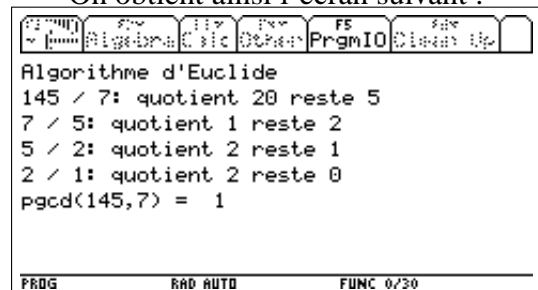
:pgcd(a,b)
:Prgm
:Local t,ta,tb,q
:If b<a Then: b->t: a->b: t->a
:EndIf
:ClrIO
:Disp "Algorithme d'Euclide"
:a->ta: b->tb
:Loop
:Disp string(tb)&" / "&string(ta)&": quo
tient "&string(int(tb/ta))&" reste "&st
ring(tb-ta*int(tb/ta))
:ta->t
:tb-ta*int(tb/ta)->ta
:t->tb
:If ta=0 Then
:Exit
:EndIf
:EndLoop
:Disp "pgcd("&string(b)&","&string(a)&")
= "&string(tb)
:EndPrgm

```

On tape ceci sur l'écran Home, puis on valide :



On obtient ainsi l'écran suivant :



<sup>1</sup> : Démontrons cette égalité :  $a = bq_1 + r_1$ . Soient  $d = a \wedge b$  et  $d_1 = b \wedge r_1$ .  $d_1|r_1$  et  $d_1|b$ , donc  $d_1|bq_1$ . Il vient que  $d_1|bq_1 + r_1 \Leftrightarrow d_1|a$ , et comme  $d_1|b$ ,  $d_1|d$  (d'après le point (ii) de la proposition 2). Or  $d|a$  et  $b$ , donc  $d|bq_1 - a \Leftrightarrow d|r_1 \Rightarrow d|d_1$ . Au final,  $d = d_1$ .

## 10.3 Applications

### 10.3.1 Congruences dans $\mathbb{Z}$

**Définition 3 :** Soit  $n \in \mathbb{N}^*$ . Deux nombres entiers  $a, b \in \mathbb{Z}$  sont dits *congrus modulo  $n$*  si  $a - b$  est divisible par  $n$ . On note alors  $a \equiv b [n]$ .

**Propriétés :** La relation de congruence est *réflexive*, *symétrique* et *transitive* : c'est une relation d'équivalence.

Par division euclidienne de  $a$  par  $n$ , on a  $a = qn + r$ , donc  $a \equiv r [n]$ , avec  $0 \leq r < n$ .  $r$  est le seul nombre congru à  $a$  modulo  $n$  vérifiant  $0 \leq r < n$ . La classe  $\bar{a}$  de  $a$  possède donc un élément unique dans  $\llbracket 0, n - 1 \rrbracket$ .

Réciproquement, pour tout  $r \in \llbracket 0, n - 1 \rrbracket$ ,  $\bar{r} = \{r + kn, k \in \mathbb{Z}\}$ .

L'ensemble  $\mathbb{Z}$  quotienté par  $\equiv$  sera noté  $\mathbb{Z}/n\mathbb{Z}$ , et possède  $n$  éléments :  $\bar{0}, \dots, \overline{n-1}$ . Enfin,

$$\begin{cases} x \equiv x' [n] \\ y \equiv y' [n] \end{cases} \Rightarrow \begin{cases} x + y \equiv x' + y' [n] \\ xy \equiv x'y' [n], \end{cases}$$

donc on peut munir canoniquement  $\mathbb{Z}/n\mathbb{Z}$  de deux lois de composition interne :

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{et} \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}.$$

Muni de ces deux lois,  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est l'anneau des classes résiduelles modulo  $n$ .

### 10.3.2 Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

**Proposition 3 :**  $\bar{a}$  est inversible (dans  $\mathbb{Z}/n\mathbb{Z}$ ) si et seulement si  $a \wedge n = 1$  (dans  $\mathbb{Z}$ ). L'ensemble des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$  forme un groupe.

**démonstration :**  $\bar{a}$  inversible  $\Leftrightarrow \exists \bar{a}' \mid \bar{a}\bar{a}' = \bar{1} \Leftrightarrow aa' - kn = 1 \stackrel{\text{Bézout}}{\Leftrightarrow} a \wedge n = 1$ . ■

Remarque 2 :

Si  $ab \equiv ac [n]$  et  $a \wedge n = 1$ , alors  $\bar{a}$  admet un inverse  $\bar{a}'$  dans  $\mathbb{Z}/n\mathbb{Z}$ , d'où  $\bar{a}'\bar{a}\bar{b} = \bar{a}'\bar{a}\bar{c} \Leftrightarrow \bar{b} = \bar{c} \Leftrightarrow b \equiv c [n]$ . On peut donc « simplifier » une congruence par tout nombre premier avec  $n$ .

**Corollaire 2 :**  $\mathbb{Z}/n\mathbb{Z}$  est un corps si et seulement si  $n$  est un nombre premier.

**démonstration :**  $\mathbb{Z}/n\mathbb{Z}$  corps  $\Leftrightarrow \bar{1}, \dots, \overline{n-1}$  sont inversibles  $\Leftrightarrow 1, \dots, n-1$  premiers avec  $n \Leftrightarrow n$  est premier. ■

### 10.3.3 Écriture d'un entier naturel en base $b$ ( $b \in \mathbb{N}$ et $b \geq 2$ )

Soit  $a \in \mathbb{N}$ . Alors il existe un unique  $x_0 \in \mathbb{N}$  tel que  $a = bq_0 + x_0$  ( $0 \leq x_0 < b$ ,  $q_0 < a$ ).

Il existe ensuite un unique  $x_1 \in \mathbb{N}$  tel que  $q_0 = bq_1 + x_1$  ( $0 \leq x_1 < b$ ,  $q_1 < q_0$ ), d'où

$$a = b^2 q_1 + bx_1 + x_0.$$

En allant plus loin, il existe un unique  $x_2 \in \mathbb{N}$  tel que  $q_1 = bq_2 + x_2$  ( $0 \leq x_2 < b$ ,  $q_2 < q_1$ ), d'où

$$a = b^3 q_2 + b^2 x_2 + bx_1 + x_0.$$

Itérant cet algorithme (qui se termine car  $(q_n)$  est strictement décroissante), on voit qu'il existe une unique suite finie  $x_0, \dots, x_n$  telle que

$$a = x_n b^n + x_{n-1} b^{n-1} + \dots + x_2 b^2 + x_1 b + x_0,$$

avec  $x_n \neq 0$ , et où pour tout  $i$ ,  $x_i \in \llbracket 0, b-1 \rrbracket$  : c'est l'écriture de  $a$  dans la base  $b$ .

### 10.3.4 Critère de divisibilité en base 10

Soit  $a \in \mathbb{N}$  d'écriture  $a = 10^n x_n + 10^{n-1} x_{n-1} + \dots + 10 x_1 + x_0$ .

- ◇ Un entier naturel est divisible par 2 (resp. 5) si et seulement si son chiffre des unités est divisible par 2 (resp. 5).

**démonstration** : 2 et 5 divisent 10, donc  $10^k$  (pour tout  $k$ ) :  $10^k \equiv 0 \pmod{2/5}$ , d'où  $a \equiv x_0 \pmod{2/5}$ . ■

- ◇ Un entier naturel est divisible par 3 (resp. 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. 9).

**démonstration** : 3 et 9 divisent  $10 - 1$ , donc  $10 \equiv 1 \pmod{3/9}$  (pour tout  $k$ ) :  $10^k \equiv 1 \pmod{3/9}$ , d'où  $a \equiv \sum_{i=0}^n x_i \pmod{3/9}$ . ■

- ◇ Un entier naturel est divisible par 11 si et seulement si la différence entre ses chiffres d'indice pair et la somme de ses chiffres d'indice impair est divisible par 11.

**démonstration** :  $10 \equiv -1 \pmod{11} \Rightarrow 10^k \equiv (-1)^k \pmod{11}$ , et donc  $a \equiv \sum_{i=0}^n (-1)^i x_i \pmod{11}$ . ■