Si a et b sont deux entiers, on dit que a divise b, ou que b est divisible par a, s'il existe un entier q tel que $b = a \times q$. On dit encore que a est un diviseur de b, ou que b est un multiple de a. On le note $a|b$.

Soient a et b deux entiers tel que $b \neq 0$, Effectuer une division euclidienne, c'est déterminer le quotient q et le reste r de la division de a par b.

I. Division euclidienne dans $\mathbb{N}$

Théorème : Existence et Unicité

Soient a et b deux entiers et positifs, (avec$b \neq 0$), il existe un couple unique (q, r) d'entiers positifs ou nuls tels que : $a = bq + r$ et $0 \leq r \prec b$

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

a) Démonstration : Existence du couple (q, r)

On distingue deux cas.

1) Si $a \prec b$. On prend $q = 0$ et $r = a$. Si $a = 0$, on prendra $q = r = 0$

2) Si $a \geq b$, On considère l'ensemble A des entiers naturels de la forme $a - mb$ pour m entier naturel. Cet ensemble est non vide puisqu'il contient a pour $m = 0$; il admet donc un plus petit élément tel que : $a – qb$. On $r \prec b$ sinon $a - (q + 1)\, b$ appartiendrait à A et serait plus petit que r. On a donc $0 \leq a - qb \prec b$. On a trouvé un couple d'entiers (q, r) répondant au problème.

$$\begin{cases} a = bq + r \\ 0 \leq r \prec b \end{cases}$$

b) Démonstration : Unicité du couple (q, r)

On suppose l'existence d'un deuxième couple (q', r') répondant au problème.

le $\begin{cases} a = bq' + r' \\ 0 \leq r' \prec b \end{cases}$

On en déduit $bq + r = bq' + r'$, soit $b\,(q - q') = (r' - r)$. Des inégalités$0 \leq r \prec b$, on déduit $-b \prec -r \leq 0$ et par addition respectivement avec les inégalités $0 \leq r' \prec b$, on déduit des inégalités strictes : $-b \prec r' - r \prec b$ et donc que $r' - r$ est strictement inférieur à b.

Comme b divise $r' - r$, il en résulte que $r' - r = 0$ et donc que $q = q'$.

Il y a donc unicité du couple (q, r).

II. Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers relatifs tels que : $b \neq 0$

Il existe un unique couple $(q; r)$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r \prec |b| \end{cases}$$

a) Démonstration : Existence du couple (q, r)

Soit A l'ensemble des entiers naturels de la forme : $a - bq$ avec $q \in Z$

$a + |ba|$ est element de A ; donc A est une partie non vide de N, qui admet un plus petit élément r.

r est élément de A ; donc $r \geq 0$ et $r = a - bq$ $(q \in Z)$

De plus, $r \prec |b|$ (sinon $r - |b| = a - bq - |b| = a - bq'$; donc $r - |b|$ serait un élément de A, plus petit que r ; c'est-à-dire que r ne serait plus le plus petit élément de A).

On déduit qu'il existe un couple $(q; r)$ de $Z \times N$ tel que $\begin{cases} a = bq + r \\ 0 \leq r \prec |b| \end{cases}$

b) Démonstration : unicité du couple (q, r)

Soient $(q; r)$ et $(q'; r')$ deux couples de $Z \times N$ tels que $\begin{cases} a = bq + r \\ a = bq' + r' \end{cases}$ et $\begin{cases} 0 \leq r \prec |b| \\ 0 \leq r' \prec |b| \end{cases}$.

On a : $0 = b\,(q' - q) + (r' - r)$; donc $|b|\,|q' - q| = |r' - r|$;

Or $-|b| \prec r' - r \prec |b|$; donc $|r' - r| \prec |b|$

On en déduit que $|q' - q| = 0$ (si $|q' - q| \geq 1$, on aurait $|b|\,|q' - q| \geq |q|$).

De plus $|r' - r| = |b|\,|q' - q|$; donc $q' = q$ et $r' = r$

On déduit qu'il existe un couple unique $(q; r)$ de $Z \times N$ tel que $\begin{cases} a = bq + r \\ 0 \leq r \prec |b| \end{cases}$