Division euclidienne dans $\mathbb{Z}$

72.1 **Pté** Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Il existe un unique couple $(q,r) \in \mathbb{Z} \times [0..b[$
tel que $a = bq + r$

Preuve On considère $X = \{k \in \mathbb{Z} / bk \leq a\}$

- si $a \geq 0$ – $0 \in X$ car $b \times 0 = 0 \leq a$
  – puisque $b \geq 1$, $bk \leq a \Rightarrow k \leq a$. Donc a majore X.
- si $a < 0$ – $a \in X$ car $b \geq 1$ donc $ab \leq a$
  – $bk \leq a \Rightarrow bk \leq 0 \Rightarrow k \leq 0$ donc 0 majore X.

Dans les deux cas X est une partie non vide et majorée de $\mathbb{Z}$.
Elle admet donc un plus grand élément, que l'on note q. $(q \in X \subset \mathbb{Z})$
$q+1 \notin X$ donc $b(q+1) > a$ soit $b > a - bq$.
On pose $r = a - bq$. puisque $q \in X$ $bq \leq a$ donc $r \geq 0$, et $r < b$.
D'où l'existence de $q \in \mathbb{Z}$, et $r \in [0..b[$ tel que $a = bq + r$.

- Montrons l'unicité.
Supposons que $(q,q') \in \mathbb{Z}^2$ et $(r,r') \in [0..b[^2$ tels que $a = bq + r = bq' + r'$
$bq + r = bq' + r'$ donc $b(q-q') = r' - r$.
Or $r - r' \in [0-(b-1) .. (b-1)-0] = [1-b .. b-1]$
Et le seul multiple de b dans cet intervalle est 0.
Donc $b(q-q') = 0$ et $r' - r = 0$
Puisque $b \neq 0$ on en déduit $q = q'$ et $r' = r$. D'où l'unicité

72.2 **Déf** Sous ces notations $a = bq + r$ s'appelle la
division euclidienne de a par b.
q est le quotient de cette division, et r le reste.