Soit $a, b \in \mathbb{Z}$, avec $b > 0$. Montrons que l'on peut écrire

$$a = b \cdot q + r$$

avec $0 \leq r < b$ et $q \in \mathbb{Z}$, uniques.

preuve: On considère l'ensemble des éléments s de $\mathbb{N}$ tq. $s = a - bq$

Cet ensemble est une partie non vide de $\mathbb{N}$:

Si $a > 0$, on pose $q = 0$. Sinon, on pose $q = a$ $(s = a - b \cdot a = a \cdot (1 - b) \geq 0)$.

Soit $r \in \mathbb{N}$ le plus petit élément de cet ensemble. Par construction, $r = a - bq$ pour $q \in \mathbb{Z}$.

Si $r \geq b$, $\quad r - b \geq 0$

$$a - bq - b \geq 0$$

$$a - b(q+1) \geq 0$$

et donc $S = r - b$ est de la forme

$a - b \cdot q'$ et $r - b < r \Leftrightarrow S < r$

contredit le fait que r est minimum.

On a en fin de compte $r = a - b \cdot q$

$\Leftrightarrow a = b \cdot q + r$ avec $0 \leq r < b$

et l'existence est démontrée.

Reste à démontrer l'unicité.

Supposons que $a = b \cdot q + r$ et qu'il

existe également q' et r' tq. $a = bq' + r'$

avec $0 \leq r, r' < b$.

On soustrait les deux égalités et on obtient : $0 = bq + r - (bq' + r')$

$$\Leftrightarrow \quad 0 = bq + r - bq' - r'$$

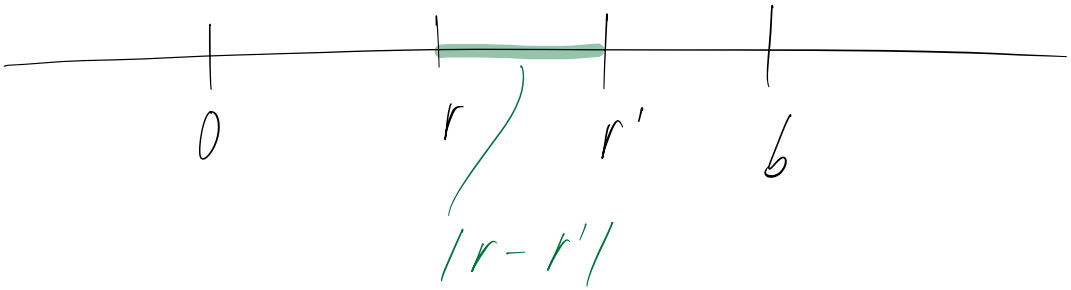
$$\Leftrightarrow \quad 0 = bq - bq' + r - r'$$

$$\Leftrightarrow \quad r - r' = bq' - bq$$

$$\Leftrightarrow \quad r - r' = b(q' - q) \qquad (*)$$

En d'autres termes, $b \mid (r - r')$.

De plus, on a $0 \leq r, r' < b$



Cela signifie que $|r-r'|<b$. Or on a vu que si $x|y$ avec $y \neq 0$,

alors $1 \leq |x| \leq |y|$.

Le fait que $b|(r-r')$ avec $|r-r'|<b$

implique donc que $r-r'=0 \Rightarrow r=r'$.

Dans ce cas, l'égalité (*) devient :

$$0 = b(q'-q) \quad \text{avec } b>0,$$

ce qui signifie que $q'-q=0 \Rightarrow q=q'$.

L'unicité est démontrée. □