Soit $a, b \in \mathbb{Z}$ avec $b > 0$.

Si $b \mid a$, $\exists z \in \mathbb{Z}$ tq. $a = b \cdot z$

$\Rightarrow a = b \cdot z + 0$ avec $0 \leq 0 < b$

Or, on sait qu'il existe $q, r \in \mathbb{Z}$, uniques, avec $0 \leq r < b$ tq.

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

$$a = b \cdot z + 0$$

Les deux lignes ci-dessus et l'unicité de q et r impliquent directement que $q = z$ et $r = 0$.

On a bien que $a \bmod b = 0$ □

Supposons réciproquement que

$a \bmod b = 0$

Le reste de la division de a par b

est donc $r = 0$.

On a $a = b \cdot q + r = b \cdot q + 0 = b \cdot q$

Vu que $q \in \mathbb{Z}$, $b \mid a$.

□