

Euclidian Division In \mathbb{Z}

Definition : -----

for $a, b \in \mathbb{Z}^+ \times \mathbb{Z}_+^*$ we say that b devid a in the euclidian sense :

$$\exists q, r \in \mathbb{Z}^+ , \quad a = q*b + r \quad \text{with } q = \left\lfloor \frac{a}{b} \right\rfloor \text{ and } 0 \leq r < b$$

q : is the quotion

r : is the reminder

$\left\lfloor \frac{a}{b} \right\rfloor$ is the floor function meaning the largest integer smaller then $\frac{a}{b}$

Proof :

$$\begin{aligned} \text{we know that } \left\lfloor \frac{a}{b} \right\rfloor &\leq \frac{a}{b} < \left\lfloor \frac{a}{b} \right\rfloor + 1 \implies b * \left\lfloor \frac{a}{b} \right\rfloor \leq b * \frac{a}{b} < b * \left(\left\lfloor \frac{a}{b} \right\rfloor + 1 \right) \\ \implies b * q &\leq a < b * q + b \implies 0 \leq a - b * q < b \implies 0 \leq r < b \end{aligned}$$
