Division Algorithm

<u>Theorem</u>

Let $m, n \in \mathbb{Z}$ and $n >= 0$. There exists unique integers q and r such that:

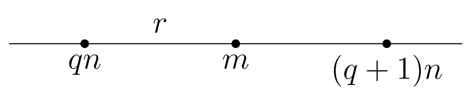
$$m = qn + r$$

where $0 \leq r < n$.

q is called the *quotient* and r is called the *remainder*.

m is called the *dividend* and n is called the *divisor*.

This can be demonstrated graphically by partitioning the real number line into segments of length n and then placing m on the line:



<u>Proof</u>

Let $S = \{m - kn \mid k \in \mathbb{Z}\}$
Let $T = \{s \in S \mid s \geq 0\}$
Note that $T \neq \emptyset$, since $m >= kn$ for some suitable $k \leq 0$
Thus, by the well-ordering principle, T has a minimum
Let $r = m - qn$ be that minimum for some $q \in \mathbb{Z}$
By construction, $r > 0$
ABC: $r \geq n$
$r > r - n \geq 0$
$r > (m - qn) - n \geq 0$
$r > m - (q+1)n = ge0$
But $m - (q+1)n \in T$
CONTRADICTION (of the minimality of r)!
$\therefore m = qn + r$ and $0 \leq r < n$

Now, assume $m = q_1 n + r_1$ and $m = q_2 n + r_2$ with $0 \leq r_1, r_2 < n$
$q_1 n + r_1 = q_2 n + r_2$
$(q_1 - q_2)n = (r_2 - r_1)$
$0 \leq r_1 < n$
$-n < -r_1 \leq 0$
$0 \leq r_2 < n$
$-n < r_2 - r_1 < n$
$-n < (q_1 - q_2)n < n$
$-1 < q_1 - q_2 < 1$

But, by closure, $q_1 - q_2 \in \mathbb{Z}$
So $q_1 - q_2 = 0$
$\therefore q_1 = q_2 = q$
$0n = r_2 - r_1 = 0$
$\therefore r_1 = r_2 = r$

$\therefore$ there exists unique $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < n$.

Given m and n, the greatest integer function can be used to calculate q and r:

$$q = \left\lfloor \frac{m}{n} \right\rfloor$$

$$r = m - nq$$

Example

Let $m = 123$ and $n = 10$:

$$q = \left\lfloor \frac{123}{10} \right\rfloor = 12$$

$$r = 123 - 12 \cdot 10 = 123 - 120 = 3$$

$$123 = 12 \cdot 10 + 3$$

$$0 \leq 3 < 10$$

Let $m = -123$ and $n = 10$:

$$q = \left\lfloor \frac{-123}{10} \right\rfloor = -13$$

$$r = -123 - (-13) \cdot 10 = -123 + 130 = 7$$

$$-123 = -13 \cdot 10 + 7$$

$$0 \leq 7 < 10$$