The Division Theorem

Division Theorem: For all natural numbers n and d, there are unique non-negative integers q and r such that:

1) $n = q \cdot d + r$
2) $0 \leq r \leq d-1$

To find q and r, we can use long division.

Example: If $n = 199$ and $d = 7$,

$$\begin{array}{r} 28 \\ 7\overline{)199} \\ -14 \\ \hline 59 \\ -56 \\ \hline 3 \end{array}$$

$q = 28$ and $r = 3$

Q: How can we prove that q and r exist and are unique?

The Division Theorem

Division Theorem: $\forall n, d \in \mathbb{N}, \exists! q, r \in \mathbb{N} \cup \{0\} (n = qd + r \wedge 0 \leq r \leq d-1)$

Proof:

Existence:

Choose $q, r \in \mathbb{N} \cup \{0\}$ so that $n = q \cdot d + r$ and r is minimized.

Note: We have at least one choice as $n = 0 \cdot d + n$.

Claim: $0 \leq r \leq d-1$.

Proof: Assume $r \geq d$. Then $n = q \cdot d + r = (q+1) \cdot d + (r-d)$ so taking $q' = q+1$ and $r' = r-d$, $q', r' \in \mathbb{N} \cup \{0\}$, $n = q' \cdot d + r'$, and $r' < r$, which contradicts the minimality of r.

Uniqueness: Assume $q, r, q', r' \in \mathbb{N} \cup \{0\}$, $n = q \cdot d + r = q' \cdot d + r'$, $0 \leq r \leq d-1$, and $0 \leq r' \leq d-1$.

$r = n - q \cdot d$ and $r' = n - q' \cdot d$, so $r' - r = (q - q') \cdot d$ is divisible by d.
However, $|r' - r| \leq d-1$ so $r' - r = 0$ and thus $r' = r$.
$q \cdot d = n - r$ and $q' \cdot d = n - r$ so $q' \cdot d - q \cdot d = (q' - q) \cdot d = 0$ and thus $q' = q$.