

1.27 Theorem. (The Division Algorithm) (*continued from 1.26*)...Moreover (*uniqueness part*), if q, q' and r, r' are any integers that satisfy

$$\begin{aligned}m &= nq + r \\ &= nq' + r'\end{aligned}$$

with $0 \leq r, r' < n$, then $q = q'$ and $r = r'$.

Proof. Let

$$\begin{aligned}m &= nq + r \\ &= nq' + r'\end{aligned}$$

with $0 \leq r, r' < n$ be given.

$$\begin{aligned}nq + r &= nq' + r', \\ nq - nq' &= r' - r, \\ n(q - q') &= r' - r.\end{aligned}$$

Since $0 \leq r, r' < n$, this implies $-n < r' - r < n$. Substituting,

$$\begin{aligned}-n &< n(q - q') < n, \\ -1 &< q - q' < 1.\end{aligned}$$

Therefore $q - q' = 0$, and $q = q'$. From here its easy to see, using substitution

$$\begin{aligned}nq' + r &= nq' + r', \\ nq' - nq' + r &= r', \\ r &= r'.$$

Since $q = q'$ and $r = r'$, there is uniqueness. □