Deduction: GCD Invariant for Remainder

Let $m, nn \in \mathbb{N}^{\geq 1}$ such that $m > n$ and let q and r be the unique integers from the quotient remainder theorem, that is, they satisfy

$$m = q \cdot n + r \qquad \text{and} \qquad 0 \leq r < n$$

Then if $r > 0$ we have:

$$\gcd(m, n) = \gcd(n, r)$$

or if $r = 0$, then $n \mid m$ and $\gcd(m, n) = n$

Proof

- *If $r > 0$*
  - *Then the equivalent formulation:*

    $$m - q \cdot n = r$$

    shows us that if $d \mid m$ and $d \mid n$ then $d \mid r$
  - *Going the other direction would be assuming that d is a divisor of n and r, and showing that d also divides m. To show this prove that*

    $$(d \nmid m \wedge d \mid n) \Rightarrow (d \nmid m - qn)$$

    by doing so, it implies that if $d \nmid m$ then $d \nmid r$ which is a contradiction so d must divide m.
  - *Therefore we can conclude that*

    $$\gcd(m, n) = \gcd(n, r)$$

- *If $r = 0$ then we know that $m = q \cdot n$ which is the definition of $n \mid m$ and it's clear that $\gcd(m, n) = \gcd(q \cdot n, n) = n$*

■