Deduction: GCD Invariant for Remainder

Let $m, n \in \mathbb{N}^{\geq 1}$ 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. This is clear from the original equation:*

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

  - *Therefore if we consider all the divisors of n and m each one of them also divides r, so the set of divisors of m and n is*

    $$\mathcal{D} = \{d \in \mathbb{N} : d \mid n \wedge d \mid m \wedge d \mid r\}$$

  - *We also consider all the divisors d of n and r, from our previous observations d also divides m so the set of divisors is also $\mathcal{D}$, therefore the maximum element from both of these sets is the same and we have :*

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

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

■