

CSCI 124/224

Discrete Structures II: Correctness of Euclidean Algorithm

Poorvi L. Vora

Recall the definition of the gcd of m and n , denoted (m, n) :

In other words,

$$g = (m, n) \Leftrightarrow \begin{cases} g|m, g|n \\ x|m, x|n \Rightarrow x|g \end{cases}$$

Recall the euclidean algorithm for the gcd:

$gcd(m, n) \text{ /* } m > n \text{ */}$

$(a, b) := (m, n) \text{ /* Initialize */}$

$\text{while } (b \neq 0) (a, b) := (b, a \text{ rem } b)$

$\text{return}(a)$

In order to show it is correct, we need two results.

Lemma: $b|a \Rightarrow (a, b) = b$

Proof: $b|a \Rightarrow b|a$ and $b|b$

Further, trivially, if $x|a$ and $x|b$ then $x|b$ and $b = (a, b)$ by the definition.

Lemma: $(m, n) = (n, m \text{ rem } n)$

Proof: Let $g = (m, n)$, and $r = m \text{ rem } n$, then

$$m = r + q_m n, q_m \in \mathbb{Z} \tag{1}$$

Because $g = (m, n)$, the following are known:

$$g|m, g|n \tag{2}$$

$$x|m, x|n \Rightarrow x|g \tag{3}$$

$$(1), (2) \Rightarrow g|r \tag{4}$$

$$y|r, y|n \Rightarrow y|m \text{ (from (1))} \Rightarrow y|g \text{ (from (3))} \tag{5}$$

$$(4), (5) \Rightarrow g = (n, r)$$

Now we can argue for the correctness of the euclidean algorithm. Because the gcd of (a, b) is that of $(b, a \text{ rem } b)$ when $b \neq 0$, in each recursion, $gcd(a, b)$ stays the same while a and b change. At the last recursion, $(a, b) = (b, 0)$ and the returned value a is the correct gcd (it is the value of b from the previous recursion).