The Greatest Common Divisor

Definition: a) An integer d is called a common divisor of two integers m and n if $d|m$ and $d|n$.

b) The greatest common divisor (gcd) of m and n is the largest among the common divisors of m and n.

Notation: $d = \gcd(m, n)$. (Note: $d > 0$.)

Theorem 1: a) The Euclidean algorithm calculates the greatest common divisor $\gcd(m, n)$ of m and n.

b) If d is any common divisor of m and n, then $d|\gcd(m, n)$.

c) If $g = \gcd(m, n)$, then $\gcd\left(\frac{m}{g}, \frac{n}{g}\right) = 1$.

Properties of the gcd:

G0 $\gcd(\pm m, \pm n) = \gcd(m, n) = \gcd(n, m)$.

G1 $\gcd(m, m) = m$, if $m > 0$.

G2 $\gcd(m - n, n) = \gcd(m, n)$.

G2′ $\gcd(m - nx, n) = \gcd(m, n)$, for all $x \in \mathbb{Z}$.

Corollary. $m|m', n|n' \Rightarrow \gcd(m, n) \mid \gcd(m', n')$.