CSci 2312
Discrete Structures II: Euclidean Algorithm

Poorvi L. Vora

In this module, we present the euclidean algorithm for finding $gcd(x, m)$.

Definition: The greatest common divisor of two positive integers m and n is the largest integer that divides both m and n. It is denoted (m, n) or $gcd(m, n)$.

In other words,

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

Here $a|b$ is notation for "a divides b". Recall that $a|b \Rightarrow b = ka$ for some $k \in \mathbb{Z}$.

Examples: $(6, 9) = 3$, $(12, 36) = 12$, $(5, 9) = 1$.

Definition: m and n are said to be relatively prime if $(m, n) = 1$.

The euclidean algorithm is as follows:

gcd(m, n) /* $m > n$ */

$(a, b) := (m, n)$ /* Initialize */

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

return(a)

Example Use the euclidean algorithm to determine $gcd(79, 551)$.

$$\begin{aligned} (a, b) &= (551, 79) \\ (a, b) &= (79, 77) \\ (a, b) &= (77, 2) \\ (a, b) &= (2, 1) \\ (a, b) &= (1, 0) \\ return(1) & \end{aligned}$$

Example Use the euclidean algorithm to determine $gcd(632, 5056)$.

$$\begin{aligned}
(a, b) &= (869, 632) \\
(a, b) &= (632, 237) \\
(a, b) &= (237, 158) \\
(a, b) &= (158, 79) \\
(a, b) &= (79, 0) \\
return(79) &
\end{aligned}$$

In each recursion, $gcd(a, b)$ stays the same while a and b change. Further, at each step, we decrease both a and b, and neither is ever negative. Hence the algorithm will end some time, in fact, in at most n steps. Finally, at the last but one recursion, because $a \ rem \ b$ is zero, a is a multiple of b and hence $gcd(a, b) = b$. 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).