Euclid's Algorithm

Dragan Marković

Euclid's algorithm, is an algorithms which finds greatest common divisor($\boldsymbol{GCD}$) of two numbers. $\boldsymbol{GCD(a,b)}$ for integers $\boldsymbol{a}$ and $\boldsymbol{b}$ is such number $\boldsymbol{d}$ that $\boldsymbol{d}$ divides both $\boldsymbol{a}$ and $\boldsymbol{b}$, and there isn't a greater number than $\boldsymbol{d}$ with the same property.

lemma. $\boldsymbol{GCD(a,b) = GCD(b, a\%b)}$, where $\boldsymbol{\%}$ is denotes modulo, that is $\boldsymbol{a\%b = a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b}$.

proof. Let $\boldsymbol{GCD(a,b) = p}$ and $\boldsymbol{GCD(b, a\%b) = q}$, then $\boldsymbol{a = b \cdot k + a\%b}$, since $\boldsymbol{p|a}$ and $\boldsymbol{p|b}$ it follows that $\boldsymbol{p|(a\%b)}$, likewise sine $\boldsymbol{q|b}$ and $\boldsymbol{q|(a\%b)}$ it follows that $\boldsymbol{q|a}$. We have that:

1. $\boldsymbol{q|a}$ and $\boldsymbol{q|b}$
2. $\boldsymbol{GCD(a,b) = p}$

From the definition of greatest common divisor and **1.)** and **2.)** it follows that $\boldsymbol{q \leq p}$, if $\boldsymbol{q > p}$ then $\boldsymbol{GCD(a,b) = q}$, which would be a contradiction. Analogical to that:

1. $\boldsymbol{p|b}$ and $\boldsymbol{p|(a\%b)}$
2. $\boldsymbol{GCD(b, a\%b) = q}$

We have that $\boldsymbol{p \leq q}$. Since $\boldsymbol{p \leq q}$ and $\boldsymbol{q \leq p}$, it must be that $\boldsymbol{p = q}$.

We can use this fact to come up with a recursive algorithm for finding greatest common divisor. Simply $\boldsymbol{GCD(a,b) = GCD(b, a\%b)}$, with the terminating condition that $\boldsymbol{GCD(a,0) = a}$. Although it is not at all trivial to prove this algorithm runs in $\boldsymbol{O(\log N)}$ time (worst possible input for this algorithm would be two successive Fibonacci numbers).

Least common multiple ($\boldsymbol{LCM}$), which represents the lowest possible number that is ***divisble*** by both $\boldsymbol{a}$ and $\boldsymbol{b}$, is simply $\boldsymbol{\frac{a \cdot b}{GCD(a,b)}}$.

A couple of examples:

1. $\boldsymbol{GCD(5,2) = GCD(2,1) = GCD(1,0) = 1}$
2. $\boldsymbol{GCD(15,6) = GCD(6,3) = GCD(3,0) = 3}$
3. $\boldsymbol{LCM(15,6) = \frac{15 \cdot 6}{GCD(15,6)} = \frac{90}{3} = 3}$