CS 173 Lecture 3c: GCD and Euclid's Algorithm

Given integers a & b, an integer c is a common divisor of a and b, if $c \mid a$ and $c \mid b$.

The greatest common divisor is denoted by $\gcd(a,b)$.

$\gcd(192, 256) = 64$. $192 = 3 \cdot 64$ $256 = 4 \cdot 64$

$\gcd(-5, 5) = 5$ $-5 = -1 \cdot 5$ $5 = 1 \cdot 5$

$\gcd(0, a) = |a|$ for all non-zero integers a.

$\gcd(0,0)$ is undefined

$\gcd(a,b) > 0$ if $a \neq 0$ or $b \neq 0$.

Definition: Integers a & b are <u>coprime</u> if $\gcd(a,b) = 1$.

Application: cryptography: it's useful to find numbers that are coprime.

Problem: find a fast way to compute $\gcd(a,b)$

One way: compare prime factorizations

Insight:

Theorem: Let a, b, q, r be integers such that <u>$a = bq + r$</u>, then $\gcd(a,b) = \gcd(b,r)$.

Proof: We will show that the common divisors of a & b are the same as the common divisors of b & r

proving $p \leftrightarrow q$ means proving $p \to q$ & $q \to p$

$\forall n \in \mathbb{Z}$, n is a common divisor of a & b $\leftrightarrow$ n is a common divisor of b & r.

Let n be an integer.

Suppose n divides both a & b.

Goal: show $n \mid r$

Since n divides b, n divides $-bq$.

$a \mid b$ & $a \mid c$ $\to a \mid (b+c)$

So, n divides $a - bq = r$.

$a \mid b \to a \mid bc \; \forall c$

$\to a \mid (b+c)$

So, n divides $a - bq = r$.

$a \mid b$
$\to a \mid bc$ $\forall c$

Suppose n divides b & r.

Goal: $n \mid a$

Since n divides b, n divides bq,
so n divides $bq + r = a$.

This immediately implies that $\gcd(a,b) = \gcd(b,r)$. $\square$