Method for finding gcd and lcm without factorization. (Euclidean Algorithm)

Theorem (7.3.1) If $a, b, q, r \in \mathbf{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Other conditions for gcd

Assume $a, b \neq 0$ and $d > 0$

The following conditions are equivalent to $d = \gcd(a,b)$:

1. d is a common divisor of a,b and for all common divisors c of $a,b,\quad c \mid d$ (i.e. the usual definition).

2. (7.4.2) d is the smallest positive integer of the form $ax + by,\ x, y \in \mathbf{Z}$.

3. (7.2.18) d is a common divisor of a,b and for all common divisors c of $a,b,\quad c \leq d$.

Relatively prime pairs of integers

$a, b \in \mathbf{Z}$ are *relatively prime* if $\gcd(a,b) = 1$.

Equivalently, for some $x, y \in \mathbf{Z},\quad ax + by = 1$.

Theorem (7.4.4)

1. If a,b are relatively prime and $a \mid bc$, then $a \mid c$.

2 If a,b are relatively prime and $a \mid c$ and $b \mid c$, then $ab \mid c$.

MATHS 255 Class Notes
¶ 7.2

gcd, lcm

Suppose $a, b, d, m \in \mathbf{Z}$, $a, b \neq 0$.

d is a *common divisor* of a,b if and only if $d \mid a$ and $d \mid b$.

m is a *common multiple* of a,b if and only if $a \mid m$ and $b \mid m$.

d is a *greatest common divisor* of a,b if and only if d is largest (with respect to the partial ordering |) in the set of positive common divisors of a,b. I.e. if c is any common divisor of a,b then $c \mid d$.

m is a *least common multiple* of a,b if and only if m is smallest (with respect to the partial ordering |) in the set of positive common multiples of a,b. I.e. if n is any common multiple of a,b then $m \mid n$.

Theorem.(7.2.16)
Any two non-zero integers have a unique gcd.

Proof:
Existence.

Uniqueness.