Definitions and Theorems

Definition 1. *Let $a, b \in \mathbb{Z}$*

$$a = qb, \exists q \in \mathbb{Z} \iff a|b$$

Definition 2. *Let $a, b, d \in \mathbb{Z}$. If $d|a$ and $d|b$, d is a common divisor of a and b.*

Theorem 1. *Let $a, b \in \mathbb{Z}$ Let S be the set of all common divisors of a and b.*

$$\exists d_m \in S, \forall s \in S, s|d_m$$

Proof. $\{ma + nb|m, n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ with addition.

This subgroup can only be cyclic.

Let $g = xa + yb, \exists x, y \in \mathbb{Z}$ be the generator of this subgroup.

$g \in S$, since $g|1a + 0b$ and $g|0a + 1b$.

$\forall d \in S, d|a$ and $d|b \implies d|xa + yb = g$.

g is our desired d_m.

∎

Definition 3. *We pick the positive generator of $\{ma+nb|m, n \in \mathbb{Z}\}$ to be $gcd(a, b)$, and call it the greatest common divisor of a and b.*

Theorem 2. *Let $gcd(a, b) = 1$*

$$a|c, b|c \implies ab|c \tag{1}$$

$$a|bc \implies a|c \tag{2}$$

Proof. Pick α, β, such $\alpha a + \beta b = 1$

$\alpha ac + \beta bc = c$

To prove (1)

$b|c \implies \exists \gamma, \gamma b = c$, so $\alpha ac = \alpha a \gamma b$

$a|c \implies \exists \delta, \delta a = c$, so $\beta bc = \beta b \delta a$

$ab|(\alpha\gamma + \beta\delta)ab = c$

To prove (2)

$a|a \implies a|\alpha ac$

$a|bc \implies a|\beta bc$

$a|\alpha ac + \beta bc = c$

■

Theorem 3. *Let S be the set of all common multiples of a and b.*

$$\exists k \in S, \forall s \in S, k|s$$

Proof. Let $d = gcd(a, b)$

We claim $\frac{ab}{d}$ is our desired k.

$d|a$ and $d|b \implies b|\frac{ab}{d}$ and $a|\frac{ab}{d} \implies \frac{ab}{d} \in S$.

By Theorem 1, $\forall s \in S, ab|s \implies s = abq, \exists q \in \mathbb{Z} \implies \frac{ab}{d}|abq = s$.

■

Definition 4. *We pick $\frac{ab}{d}$ from above to be $lcm(a, b)$*

Corollary 3.1. $lcm(a, b)gcd(a, b) = ab$

Theorem 4. *Let $0 \neq a, b \in \mathbb{Z}$, and $gcd(a, b) = d$, and α, β are the Bezout's identity. The equation*

$$xa + yb = c$$

have solution

$$x = n\alpha + \frac{bm}{d}, y = n\beta - \frac{am}{d}, \forall m \in \mathbb{Z}$$

only when $c = nd, \exists n \in \mathbb{Z}$.

Proof. When $c = nd$

$xa + yb = n\alpha a + \frac{abm}{d} + n\beta b - \frac{abm}{d} = n(\alpha a + \beta b) = nd = c$

When $c = nd + r$, where $0 < r < d$

$c \notin \langle d \rangle = \{xa + yb | x, y \in \mathbb{Z}\}$

■

Exercises