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 $g = \alpha a + \beta b, \exists \alpha, \beta \in \mathbb{Z}$ be the generator of this subgroup.

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

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

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 $a, b \in \mathbb{Z}^+$, and $d = gcd(a, b)$*

$$gcd(\frac{a}{d}, \frac{b}{d}) = 1$$

Proof. Assume $\exists n > 1 \in \mathbb{Z}^+, n|\frac{a}{d}$ and $n|\frac{b}{d}$

We immediately see that $nd|a$ and $nd|b$, where $d|nd$ and $d < nd$ CaC

■

Theorem 4. *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 $a|\frac{ab}{d} \implies \frac{ab}{d} \in S$

Let $s \in S$

$\exists \alpha, \beta \in \mathbb{Z}, d = gcd(a, b) = \alpha a + \beta b$

$\forall s \in S, b|s \implies ab|s\alpha a$

$\forall s \in S, a|s \implies ab|s\beta b$

$ab|s\alpha a + s\beta b = s(\alpha a + \beta b) = sd \implies \frac{ab}{d}|s$

■

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

Corollary 4.1. $lcm(a, b)gcd(a, b) = ab$

Theorem 5. *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

1.11

Proof. $7 = gcd(1092, 1155, 2002) = (-1710)1092 + (1615)1155 + 2002$ ■

1.13

Proof. $lcm(1745, 1485) = \frac{(1745)1485}{5 = gcd(1745,1485)}$ ■

1.15

Proof.

$$y = 297m + 120, x = -(349m + 141)$$

■

1.16

Proof. We claim only when $gcd(a_1, \ldots, a_k)|c$ there exists some solution.

Again, $S = \{\sum_{i=1}^{k} x_i a_i | x_I \in \mathbb{Z}\}$ is a group.

We see $gcd(a_1, \ldots, a_k)$ is its generator, since $\forall s \in S, gcd(a_1, \ldots, a_k)|s$

So, $gcd(a_1, \ldots, a_k) = \sum_{i=1}^{k} \alpha_i a_i, \exists \alpha_I$

If $c = (q)gcd(a_1, \ldots, a_k)$, $c = \sum_{i=1}^{k} q\alpha_i a_i$

If $c = (q)gcd(a_1, \ldots, a_k) + r$, $c \notin \langle gcd(a_1, \ldots, a_k) \rangle = S$

■

1.25

Proof.

$$gcd(a,b)=1 \implies 1=\alpha a+\beta b, \exists \alpha,\beta \in \mathbb{Z}$$

Let $c = ab + m, \exists m \in \mathbb{Z}^+$

$\forall n \in \mathbb{Z}, c = c\alpha a + c\beta b = (c\alpha)a + (c\beta)b = (\alpha(ab+m))a + (\beta(ab+m))b = (\alpha(ab+m))a + (\beta(ab+m))b + nba - nba = (\alpha(ab+m) - nb)a + (\beta(ab+m) + na)b = (b(\alpha a - n) + \alpha m)a + (a(\beta b + n) + \beta m)b$

So $c = (b(\alpha a - n) + \alpha m)a + (a(\beta b + n) + \beta m)b$

After gaining the equation above, we see now if $\exists n, b(\alpha a - n) + \alpha m \geq 0$ and $a(\beta b + n) + \beta m \geq 0$, OPID

Recall $c = ab + m, \exists m \in \mathbb{Z}^+$. We now divide the situation into two cases.

case: $m = 0$

$m = 0 \implies b(\alpha a - n) + \alpha m = b(\alpha a - n)$ and $a(\beta b + n) + \beta m = a(\beta b + n)$

$b(\alpha a - n) \geq 0 \iff \alpha a - n \geq 0 \iff \alpha a \geq n$

$a(\beta b + n) \geq 0 \iff \beta b + n \geq 0 \iff n \geq -\beta b$

$1 = \alpha a + \beta b \iff -\beta b = \alpha a - 1$

So, we check if $\exists n \in \mathbb{Z}, \alpha a \geq n \geq \alpha a - 1$

This is clearly true.

case: $m \in \mathbb{Z}^+$

Transform $b(\alpha a - n) + \alpha m = b[\alpha(a + \frac{m}{b}) - n]$ and $a(\beta b + n) + \beta m = a[\beta(b + \frac{m}{a}) + n]$

$b(\alpha a - n) + \alpha m \geq 0 \iff b[\alpha(a + \frac{m}{b}) - n] \geq 0 \iff \alpha(a + \frac{m}{b}) - n \geq 0 \iff \alpha a + \frac{\alpha m}{b} \geq n$

$a(\beta b+n)+\beta m \geq 0 \iff a[\beta(b+\frac{m}{a})+n] \geq 0 \iff \beta(b+\frac{m}{a})+n \geq 0 \iff n \geq -\beta b - \frac{\beta m}{a} = \alpha a - 1 - \frac{\beta m}{a}$

So the required condition to finish the proof is to show $\exists n \in \mathbb{Z}, \alpha a + \frac{\alpha m}{b} \geq n \geq \alpha a - 1 - \frac{\beta m}{a}$

Notice $\frac{\alpha m}{b} + \frac{\beta m}{a} = \frac{\alpha a m + b\beta m}{ab} = \frac{(\alpha a+\beta b)m}{ab} = \frac{m}{ab} \geq 0$

So $\frac{\alpha m}{b} \geq -\frac{\beta m}{a}$

So $\alpha a + \frac{\alpha m}{b} \geq (\alpha - 1 - \frac{\beta m}{a}) + 1$

Then n clearly exists.

$\blacksquare$