Lecture - 2 Monday 1/8/2022

- $\gcd(a,b)$ is the least element of the set
  $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}$.

- If c is a common divisor of a and b, and $c<d$, where $d=\gcd(a,b)$, then $c\notin a\mathbb{Z}+b\mathbb{Z}$.
  Also, $c\,|\,(ax+by)$ $\forall\, x,y\in\mathbb{Z}$. Hence, $c\,|\,d$.

- Converse of Bezout's identity is not true in general.
  It is true when $\gcd(a,b)=1$.

<u>Theorem 1</u>: $\gcd(a,b)=1 \iff \exists\, x_0,y_0\in\mathbb{Z}$ such that
$$ax_0+by_0=1.$$

<u>Proof</u>: Let $\gcd(a,b)=1$. Then, by Bezout's identity, $\exists\, x_0,y_0\in\mathbb{Z}$ such that $ax_0+by_0=1$.

Conversely, suppose that $ax_0+by_0=1$ for some $x_0,y_0\in\mathbb{Z}$.

We know that, $\gcd(a,b)=$ smallest element of $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}$.

Since $1\in a\mathbb{Z}+b\mathbb{Z}$, so $\gcd(a,b)=1$.

#

<u>Theorem 2</u>: Given any non-zero integers $b_1,b_2,\dots,b_n$, there exist integers $x_1,x_2,\dots,x_n$ such that
$$\gcd(b_1,b_2,\dots,b_n)=\sum_{j=1}^{n} b_j x_j.$$

<u>Proof</u>: Extend the proof of Bezout's identity.

#

Theorem 3: For any positive integer m,

$$\gcd(ma, mb) = m \cdot \gcd(a, b).$$

Proof: $\gcd(ma, mb)$

$=$ least positive value of $ma \cdot x + mb \cdot y$, $x, y \in \mathbb{Z}$

$= m \cdot \{$least positive value of $ax + by$, $x, y \in \mathbb{Z}\}$

$= m \cdot \gcd(a, b)$.

#

Corollary: Let $c > 0$, and $c \mid a$ and $c \mid b$. Then,

$$\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}\gcd(a, b).$$

In particular, if $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: By Theorem 3, we have

$$\gcd(a, b) = \gcd\left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right) = c \cdot \gcd\left(\frac{a}{c}, \frac{b}{c}\right)$$

$$\Rightarrow \gcd\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}\gcd(a, b). \quad \#$$

If $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\gcd(a, b) = 1$.

#

Theorem 4: If $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.

Proof: By Bezout's identity, we have

$$ax_0 + my_0 = 1 = bx_1 + my_1 \quad \text{for some } x_0, y_0, x_1, y_1 \in \mathbb{Z}.$$

$$\Rightarrow ax_0 = 1 - my_0 \text{ and } bx_1 = 1 - my_1.$$

Now, $ax_0 \cdot bx_1 = (1 - my_0)(1 - my_1)$

$$= 1 - m(y_0 + y_1) + m^2 y_0 y_1$$

$$\Rightarrow ab \cdot x_0 x_1 + my_2 = 1, \text{ where } y_2 = y_0 + y_1 - my_0 y_1 \in \mathbb{Z}$$

By Theorem 1, $\gcd(ab, m) = 1$.

#

Theorem 5: For any integer x,

$$\gcd(a,b) = \gcd(b,a) = \gcd(a,-b) = \gcd(a, b+ax).$$

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

Clearly, $\gcd(a,b) = \gcd(b,a) = \gcd(a,-b)$.

Let $g = \gcd(a, b+ax)$.

Since $d = \gcd(a,b)$, so $\exists\, x_0, y_0 \in \mathbb{Z}$ such that

$$d = ax_0 + by_0.$$

Now,
$$\begin{aligned} d &= ax_0 + by_0 \\ &= ax_0 + by_0 + axy_0 - axy_0 \\ &= a(x_0 - xy_0) + (b+ax)y_0 \\ &\in a\mathbb{Z} + (b+ax)\mathbb{Z} = g\mathbb{Z} \end{aligned}$$

$\Rightarrow g \mid d$

Next, we prove that $d \mid g$.

$d \mid a$, $d \mid b$, so $d \mid (b+ax)$ for any $x \in \mathbb{Z}$

$\therefore$ d is a common divisor of a and $b+ax$

$\Rightarrow d \mid g$, where $g = \gcd(a, b+ax)$.

Since $d, g \geq 1$, and $g \mid d$ & $d \mid g$, so $d = g$.

#

Theorem 6: If $c|ab$ and $\gcd(b,c)=1$, then $c|a$.

Proof: $\gcd(ab, ac) = a \cdot \gcd(b,c) = a$.

Given that $c|ab$, and clearly $c|ac$.

$\therefore$ c is a common divisor of ab and ac.

$\Rightarrow c$ divides $\gcd(ab, ac) = a$.

#

Theorem 7: (Euclidean algorithm)

Given integers b and $a>0$, we make a repeated application of the division algorithm, to obtain a series of equations:

$$b = aq_1 + r_1, \quad 0 < r_1 < a$$

$$a = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$$

$$- \; - \; - \; - \; - \; - \; - \; - \; -$$

$$- \; - \; - \; - \; - \; - \; - \; - \; - \; - \; -$$

$$r_{j-2} = r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}$$

$$r_{j-1} = r_j q_{j+1}.$$

Then, $\gcd(a,b) = r_j$, the last non-zero remainder in the division process.

Proof: $a > r_1 > r_2 > \cdots > r_j$ is a strictly decreasing sequence of positive integers, so the process stops, and $r_{j+1} = 0$.

Now, $\gcd(a, b)$

$$= \gcd(a, b - aq_1)$$

$$= \gcd(a, r_1)$$

$$= \gcd(r_1, a - r_1 q_2)$$

$$= \gcd(r_1, r_2)$$

$$= \gcd(r_1 - r_2 q_3, r_2)$$

$$= \gcd(r_3, r_2)$$

$$= \cdots \quad \cdots$$

$$= \gcd(r_j, r_{j-1})$$

$$= \gcd(r_j, r_{j+1})$$

$$= \gcd(r_j, 0)$$

$$= r_j \qquad \#$$