Lecture-1 July 29, 2022

- Well-ordering principle:
  Every non-empty subset of $\mathbb{N} \cup \{0\}$ has a smallest element.

- Division algorithm: Let $a, b \in \mathbb{Z}$ with $a \neq 0$.
  Then, $\exists$ unique integers q, r such that
  $$b = aq + r, \text{ where } 0 \leq r < |a|.$$

Proof: Let $a > 0$. Consider the arithmetic progression

$$\ldots, b-3a, b-2a, b-a, b, b+a, b+2a, \ldots$$

Let $S = \{b - ak \mid k \in \mathbb{Z}\}$

Since $a > 0$, so it is clear that S contains non-negative integers.

By well-ordering principle, S contains a smallest non-negative integer, say, r.

Since $r \in S$, so $r = b - aq$ for some $q \in \mathbb{Z}$

$\therefore b = aq + r$, where $r \geq 0$.

We now prove that $r < a$. Suppose that $r \geq a$.
Then, $r - a \geq 0$ and $r - a = b - a(1+q) \in S$
Since $0 \leq r - a < r$ and $r - a \in S$, this is a

contradiction to the fact that r is the smallest non-negative element of S.

$\therefore 0 \leq r < a$.

<u>Uniqueness:</u> Let $b = aq_1 + r_1$, $0 \leq r_1 < a$

& $b = aq_2 + r_2$, $0 \leq r_2 < a$.

Then, $a|q_1 - q_2| = |r_1 - r_2|$ and $0 \leq |r_1 - r_2| < a$.

$\Rightarrow 0 \leq |q_1 - q_2| < 1$

$\Rightarrow q_1 - q_2 = 0 \Rightarrow q_1 = q_2 \therefore r_1 = r_2$.

This completes the proof if $a > 0$.

If $a \neq 0$, then working with $|a|$, we have unique integers q and r such that

$b = |a|q + r$, where $0 \leq r < |a|$

$= aq_1 + r$, where $0 \leq r < |a|$.

Here $q_1 = \begin{cases} q & \text{if } a > 0 \\ -q & \text{if } a < 0. \end{cases}$

This completes the proof of division algorithm.

#

Lemma 1: Let $\phi \neq S \subseteq \mathbb{Z}$. Suppose that S satisfies the following properties:

(i) $u \in S \Rightarrow -u \in S$ (ii) $u, v \in S \Rightarrow u+v \in S$.

Then, either $S = \{0\}$ or $S = k\mathbb{Z}$, where k is the smallest positive integer in S.

Proof: Let S be a set satisfying (i) and (ii). Clearly, $0 \in S$. Suppose that S contains a non-zero integer u. Since $-u \in S$, so S contains a positive integer. Let k be the least positive integer in S (which exists by well-ordering principle)

Claim: $S = k \cdot \mathbb{Z} = \{ k \cdot n \mid n \in \mathbb{Z} \}$

Since $k \in S$, so $-k \in S$ (by property (i))

$\Rightarrow k\mathbb{Z} \subseteq S$. (by property (ii))

Now, let $x \in S$. By division algorithm,

$$x = k \cdot q + r, \text{ where } 0 \leq r < k$$

$$\Rightarrow r = x - k \cdot q \in S \quad \left(\because x \in S,\ -kq \in S \text{ so } x - kq \in S \right)$$

$$\Rightarrow r = 0 \quad \left(\because 0 \leq r < k \text{ and } k \text{ is the smallest positive integer in } S \right)$$

$$\therefore x = k \cdot q \in k\mathbb{Z} \Rightarrow S \subseteq k\mathbb{Z}.$$

Thus, $S = k \cdot \mathbb{Z}$ #

§ Greatest common divisor:

- $\gcd(0,0)$ is not defined.
- $\gcd(a,0) = |a|, \quad a \neq 0$
- $\gcd(a_1, \dots, a_n) = d$ if $d \geq 1$ is the largest such that $d \mid a_1, \dots, d \mid a_n$.

<u>Theorem</u> (Bezout identity):

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

$$d = ax_0 + by_0.$$

<u>Proof</u>: Let $S = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.

(i) $u \in S \Rightarrow -u \in S$

(ii) $u, v \in S \Rightarrow u + v \in S$

By Lemma 1, $S = d\mathbb{Z}$, where d is the smallest positive integer in S.

<u>Claim</u>: $d = \gcd(a,b)$.

We have
$$a = a\cdot 1 + b\cdot 0 \in S$$
$$b = a\cdot 0 + b\cdot 1 \in S$$

Since $S = d\mathbb{Z}$, so $a, b \in d\mathbb{Z} \Rightarrow d \mid a$ and $d \mid b$.

Let c be a common divisor of a and b.

Then, $a = c\cdot c_1$ and $b = c\cdot c_2$ for some $c_1, c_2 \in \mathbb{Z}$

Now, $d \in S \Rightarrow \quad d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$

$$\Rightarrow d = c \cdot c_1 x_0 + c \cdot c_2 y_0$$
$$= c(c_1 x_0 + c_2 y_0)$$
$$\Rightarrow c \mid d$$
$\therefore$ $d = \gcd(a, b)$.

Since $d \in S$, so $\exists\, x_0, y_0 \in \mathbb{Z}$ such that
$$d = a x_0 + b y_0.$$
This completes the proof.

#