Proof. $S \subset \mathbb{Z} \Rightarrow S = m\mathbb{Z}$

Since $S \neq \emptyset$, $\exists a \in S$

Since S is closed under $+$, $-$, $0 \in S$. We may assume that $S \neq \{0\}$. (if $S = \{0\}$, then $S = 0 \cdot \mathbb{Z}$)

Take any $n \in S$. Then $0 - n = -n \in S$. Thus we may also assume that S has a positive integer.

In all, WLOG[1], we may assume that S has a positive integer.

By WOP, S has a least positive integer m. We want to show that $S = m\mathbb{Z}$.

$A = B \Rightarrow A \subset B$ and $B \subset A$
$A \subset B \Rightarrow$ if $x \in A$ then $x \in B$

1. $m\mathbb{Z} \subset S$
   $m \in S$ and S is closed under $+$, $-$. So S must have all multiples of m.
2. $S \subset m\mathbb{Z}$
   Take any $a \in S$. By division algorithm, $\exists q, r \in \mathbb{Z}$ such that $a = qm + r$ where $0 \leq r < m$. Since $mq \in S$ and $a \in S$,
   $$r = a - mq \in S$$
   . Thus $r = 0$ by the minimality of m. Hence $a = mq \in m\mathbb{Z}$.
   Remains to show the uniqueness of m. Suppose $m\mathbb{Z} = S = m'\mathbb{Z}$. Then $m = \pm m'$. Since $m, m' > 0$, $m = m'$.

Theorem 1. *Let $d = (a, b)$. Then $d = ax + by$ for some $x, y \in \mathbb{Z}$ and $\{ax + by \mid x, y \in \mathbb{Z}\}$ is the set of all multiples of d. i. e. $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.*

Proof. We knew that $d = ax + by$ for some $x, y \in \mathbb{Z}$. (by the theorem in the last class)

Define $S := a\mathbb{Z} + b\mathbb{Z}$. Then $a\mathbb{Z} \subset S$ and $b\mathbb{Z} \subset S$. Since S is closed under $+$, $-$, it follows the previous theorem that

$$\exists m \geq 0 \in \mathbb{Z} \text{ such that } S = m\mathbb{Z}.$$

We want to show that $m = d$. Since $a, b \in S = m\mathbb{Z}$, $m \mid a$, $m \mid b$. If $e \mid a$ and $e \mid b$, then $e \mid m$. ($\because m + as + bt$ for some $s, t \in \mathbb{Z}$)

By the definition of GCD, $m = d$.

[1] Without loss of generality

Remark The GCD of a and b (not both 0) is the least positive integer that is a linear combination of a and b.

Theorem 2 (Euclidean Algorithm). *$a, b \in \mathbb{Z}$, $a \neq 0$. Using the division algorithm,*

$$b = aq_1 + r_1, \text{ where } 0 < r_1 < |a|.$$

If $r_1 = 0$, terminate process.

Repeating process,

$$\begin{aligned} a &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Then $(a, b) = r_n$.

Proof. Clearly, $r_n > 0$. Note that

$$\begin{aligned} r_n \mid r_{n-1}, r_n \mid r_n &\Rightarrow r_n \mid r_{n-2} \\ r_n \mid r_{n-2}, r_n \mid r_{n-1} &\Rightarrow r_n \mid r_{n-3} \\ &\vdots \\ r_n \mid r_1, r_n \mid r_2 &\Rightarrow r_n \mid a \\ r_n \mid a, r_n \mid r_1 &\Rightarrow r_n \mid b \end{aligned}$$

Note also that if

$$\begin{aligned} k \mid a, k \mid b &\Rightarrow k \mid r_1 \\ k \mid r_1, k \mid a &\Rightarrow k \mid r_2 \\ &\vdots \\ k \mid r_n, k \mid r_{n-1} &\Rightarrow k \mid r_n \end{aligned}$$

Hence we conclude that $r_n = (a, b)$.

Proof (Alternate proof).

$$b = aq + r \Rightarrow (a, b) = (a, r) \qquad r = a(-q) + b,\ b = aq + r$$

Note that $e \mid a, e \mid b$ iff $e \mid r, e \mid a$. Thus $(a, b) \mid (a, b)$ and $(a, k) \mid (a, b)$.

Hence $(a, b) = (a, r)$, since $(a, b) > 0$ and $(a, k) > 0$. Therefore we can see that

$$(a, b) = (a, r) = (r_1, r_2) = \cdots = (r_{n-1}, r_n).$$

Example

$$\begin{aligned}
(68, 710) &= 2 \\
710 &= 68 \cdot 10 + 30 \\
68 &= 30 \cdot 2 + 8 \\
30 &= 8 \cdot 3 + 6 \\
8 &= 6 \cdot 1 + 2 \\
6 &= 2 \cdot 3
\end{aligned}$$

$$\begin{aligned}
2 &= 8 - 6 \cdot 1 \\
&= 8 - (30 - 8 \cdot 3) \\
&= 8 \cdot 4 + 30 \cdot (-1) \\
&= (68 - 30 \cdot 2) \cdot 4 + 30 \cdot (-1) \\
&= 68 \cdot 4 + 30 \cdot (-1) \\
&= 68 \cdot 4 + (710 - 68 \cdot 10) \cdot (-9) \\
&= 68 \cdot 94 + 710 \cdot (-9)
\end{aligned}$$

Definition 1. *A **Diophantine equation** is a polynomial equation that allows two or more variables to take integer values only.*

e. g.

$$ax + by = c$$
$$x^n + y^n = z^n$$
$$x^2 - dy^2 = 1$$

Theorem 3. *$a \neq 0$, $b \neq 0$.*

1. *The equation $ax + by = c$ has integer solutions if and only if $(a, b) \mid c$.*
2. *Suppose that $(a, b) \mid c$. Then the general solution of the equation $ax + by = c$ has form the of*

$$\left\{ x_0 + \frac{b}{(a, b)} t, y_0 - \frac{a}{(a, b)} t \right\}$$

where $t \in \mathbb{Z}$ and (x_0, y_0) is an arbitrary solution of the equation.

General solution for
$y'' - 4y' + 3y = 0$?
$\Rightarrow c_1 e^x + c_2 e^{3x}$
– 2 bases