Chapter 11
Property of finite sets

**Theorem 1.** Let $f : X \to Y$ be a function. Assume $X, Y$ are two nonempty finite sets, with $|X| < |Y|$. Then $f$ is not a surjective.

**Theorem 2.** Let $f : X \to Y$ be a function. Assume $X, Y$ are two nonempty finite sets, with $|X| > |Y|$. Then $f$ is not an injective. That is, there exists $x_1 \neq x_2$ in $X$ such that $f(x_1) = f(x_2)$.

Theorem 2 is called ‘The pigeonhole principle’.

**Another formulation of ‘The pigeonhole principle’:** If more than $n$ objects are placed into $n$ drawers, then there is at least one drawer that contains two or more objects.

**Remark:** It is also called the ‘drawer principle’.

**Applications of the pigeonhole principle:**
1. Among 366 people, there are at least two people with birthdays at the same date of the year.
2. In any group of $n$ people, there are two who have an identical number of friends in the group.
3. (Putham 1958) Q: Let $S$ be a subset of $\{1, 2, 3, \ldots, 2n\}$ with $n + 1$ elements. Show that one can choose distinct elements $x, y \in S$ such that $x$ divides $y$.

**Proof:** Write $S = \{x_1, x_2, \ldots, x_{n+1}\}$
Write $x_1 = 2^{a_1}b_1$ where $a_1, b_1 \in \mathbb{Z}$ and $b_1$ is odd;
Write $x_2 = 2^{a_2}b_2$ where $a_2, b_2 \in \mathbb{Z}$ and $b_2$ is odd;
\[\cdots\]
Write $x_{n+1} = 2^{a_{n+1}}b_{n+1}$ where $a_{n+1}, b_{n+1} \in \mathbb{Z}$ and $b_{n+1}$ is odd;
Since each $b_i$ is odd and $1 \leq b_i \leq 2n$, so $b_i \in \{1, 3, 5, \ldots, 2n - 1\}$.

There are $n$ possibilities for $b_i$. There are, however, $n + 1$ many of $b_i$s. By the pigeonhole principle, there must be two $b_j, b_k, j \neq k$ such that $b_j = b_k$. Consider the corresponding $x_i$s:

\[x_j = 2^{a_j}b_j\]
\[x_k = 2^{a_k}b_k\]

Case 1: when $a_j < a_k \Rightarrow x_j$ divides $x_k$
Case 2: when $a_j > a_k \Rightarrow x_k$ divides $x_j$

**Theorem 3:** Suppose that $X$ and $Y$ are two nonempty finite set with $|X| = |Y|$, then a function $f : X \to Y$ is an injection if and only if it is a surjection.
Definition:
(1) Let \( A \) be a nonempty set of real numbers; \( A \subseteq \mathbb{R} \), \( b \) is called a minimum element of \( A \), if:
   (i) \( b \in A \) (ii) \( b \leq a \) for every \( a \in A \).
   Notation: \( b = \min(A) \)
(2) \( c \) is called a maximum element of \( A \) if:
   (i) \( c \in A \) (ii) \( c \geq a \) for every \( a \in A \)
   Notation: \( c = \max(A) \).

Eg. (1) \( A = \{ -1, 2, 9 \} \); then \( \min(A) = -1, \max(A) = 9 \).
(2) \( A = [0, 1] \), then \( \min(A) = 0, \max(A) = 1 \).
(3) \( A = (0, 1) \), then \( \min(A) \text{ DNE; } \max(A) \text{ DNE.} \)
(4) \( A = (0, 1] \), then \( \min(A) \text{ DNE; } \max(A) = 1 \).
(5) \( \max(\mathbb{Z}^+) \) DNE; \( \min(\mathbb{Z}^+) = 1 \)

Proposition: Let \( A \) be a finite nonempty set of real numbers, then \( A \) has a minimum element and a maximum element.
Proof: See page 139-140 in the textbook.

The greatest common divisor

Definition: Let \( d \in \mathbb{Z} \) and \( d \neq 0 \). We say \( d \) divides \( a \) if \( \frac{a}{d} \) is an integer. In this case, we say \( d \) is a divisor or a factor of \( a \); or \( a \) is a multiple of \( d \).
Notation: \( d \mid a \).

Remark: (1) Every non-zero integer divides 0.
(2) If \( a \neq 0 \), and \( d \mid a \), then \( |d| \leq |a| \).

Definition: Let \( a \in \mathbb{Z} \), we define: \( D(a) = \{ n \in \mathbb{Z} \mid n \mid a \} \).
Here \( D(a) \) is called the set of divisors of \( a \).

Definition: Let \( a, b \in \mathbb{Z} \), not both zero. The set of common divisors of \( a \) and \( b \) is defined by \( D(A) \cap D(b) = \{ n \in \mathbb{Z} \mid n \mid a \text{ and } n \mid b \} \).

Definition: Let \( a, b \in \mathbb{Z} \), not both zero. The greatest common divisor (or highest common factor) of \( a \) and \( b \) is defined as \( \max(D(a) \cap D(b)) \).
Notation: \( \gcd(a, b) \) or simply \( (a, b) \).

Definition: Let \( a, b \in \mathbb{Z} \), not both zero. They are called coprime (or relatively prime) when \( (a, b) = 1 \).
Remark: $(a,b) = 1 \iff D(a) \cap D(b) = \{-1, 1\}$.

Eg. Find $(30, 72)$

$D(30) = \{-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$;

$D(72) = \{-72, -36, -24, -18, -12, -9, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$

$D(30, 72) = \{-6, -3, -2, -1, 1, 2, 3\}$.

$\Rightarrow (30, 72) = 6.$