1 Mathematical Induction

We assume that the set $\mathbb{Z}$ of integers are well defined, and we are familiar with the addition, subtraction, multiplication, and division. In particular, we assume the following axiom for subsets of integers bounded below.

Well-Ordering Principle. For every nonempty subset of integers, if it is bounded below, then it has a unique minimum number.

Example 1.1. The set $A = \{x \mid x \text{ integers}, x \geq \pi^2\}$ is a subset of $\mathbb{Z}$ and is bounded below. Find the minimum number in A. (The minimum number is 10.)

Example 1.2. The set $A = \left\{\frac{1}{n} \mid n \in \mathbb{P}\right\}$ is a bounded subset of $\mathbb{Q}$, the set of rational numbers, and also a bounded subset of $\mathbb{R}$. What is the minimum number inside A? (There is no minimum number inside A.)

Proposition 1.1. *For every nonempty subset of integers, if it is bounded above, then it has a unique maximum number.*

Proof. Let A be a nonempty subset of $\mathbb{Z}$, bounded above. Define the set

$$B = \{-n \in \mathbb{Z} \mid n \in A\}.$$

Obviously, B is a nonempty subset of $\mathbb{Z}$ and bounded below. By the Well-Ordering Principle, there is a minimum number m in B. Then $-m$ is the maximum number in A. $\square$

Theorem 1.2. *Let S be a subset of $\mathbb{P}$ satisfying the conditions:*

(a) $1 \in S$,

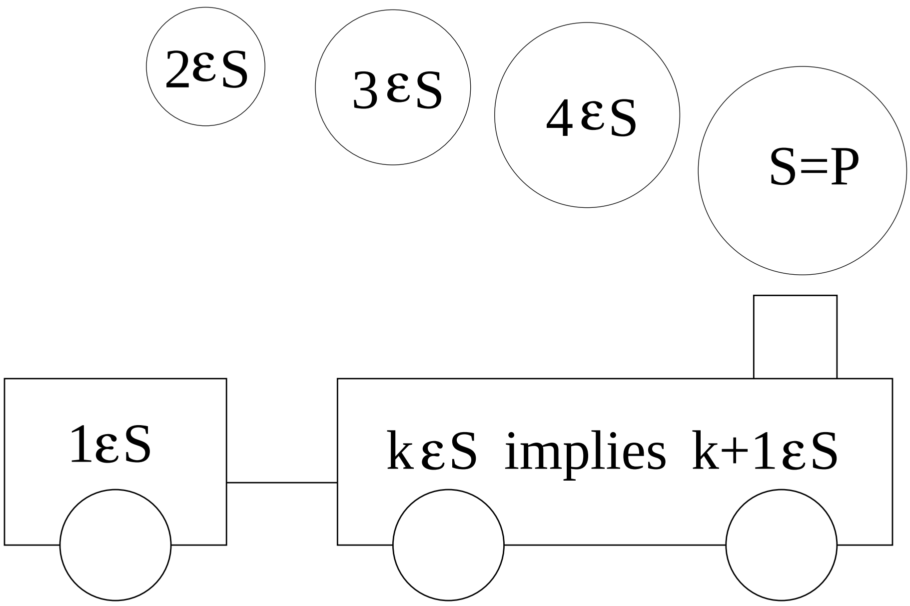
(b) for each $k \in \mathbb{P}$, *if* $k \in S$ *then* $k + 1 \in S$.

Then it follows that $S = \mathbb{P}$.

Proof. Suppose the conclusion is false, i.e., $S \neq \mathbb{P}$. Then the complement $\bar{S}$, defined by

$$\bar{S} = \{r \in \mathbb{P} \mid r \notin S\},$$

is nonempty. By the Well-Ordering Principle, $\bar{S}$ has a minimum integer m. Since $1 \in S$, $m \neq 1$. It follows that $m - 1$ is a positive integer; so $m - 1 \in \mathbb{P}$. Since m is the minimum in $\bar{S}$, $m - 1$ belongs to S. Putting $k = m - 1$ in Condition (b), we conclude that $m \in S$, which is contradictory to $m \in \bar{S}$. This means that $S \neq \mathbb{P}$ leads to a contradiction. So we must have $S = \mathbb{P}$. □



Mathematical Induction or MI. Let $P(n)$ be a family of problems indexed by the set $\mathbb{P}$ of positive integers. If,

(a) (Induction Basis or IB) the problem for $n = 1$ is true,

(b) (Induction Hypothesis or IH) if $P(n)$ is true then $P(n+1)$ is true;

then the whole problem $P(n)$ is true for all $n \in \mathbb{P}$.

Note. In the Induction Hypothesis, the symbol n is arbitrarily fixed and required $n \geq 1$, but there is only one assumption, i.e., $P(n)$ is true. This information will be used in the process of proving $P(n+1)$ to be true.

Example 1.3. The integer sequence x_n is defined recursively by

$$x_1 = 2, \quad x_n = x_{n-1} + 2n \quad (n \geq 2).$$

Show that $x_n = n(n+1)$ for all $n \in \mathbb{P}$.

Proof. For $n = 1$, $n(n+1) = 1 \cdot (1+1) = 2 = x_1$, it is true. (Induction Basis)

Suppose it is true for n, i.e., $x_n = n(n+1)$. We need to show $x_{n+1} = (n+1)((n+1)+1)$. In fact,

$$\begin{aligned} x_{n+1} &= x_n + 2(n+1) \quad \text{(By Recursive Definition)} \\ &= n(n+1) + 2(n+1) \quad \text{(By Induction Hypothesis)} \\ &= n^2 + 3n + 2 \\ &= (n+1)(n+2) = (n+1)((n+1)+1). \end{aligned}$$

So the formula is true for $n+1$. By MI, it is true for all $n \in \mathbb{P}$. □

Example 1.4. A wrong MI proof for the following statement.

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}\left(2n^3 - 11n^2 + 23n - 12\right).$$

"Proof:" Let $S_n = \frac{1}{2}\left(2n^3 - 11n^2 + 23n - 12\right)$.

For $n = 1$, $S_1 = (2 - 11 + 23 - 12)/2 = 1$; it is true.

For $n = 2$, $S_2 = (16 - 44 + 46 - 12)/2 = 3$; it is true.

For $n = 3$, $S_3 = (54 - 99 + 69 - 12)/2 = 6$; it is true.

So the statement is true for all positive integers. What is wrong with the proof? (Induction Hypothesis is not applied.)

Example 1.5. Another wrong MI proof for the following statement

$$S_n = \sum_{k=1}^{n} (2k + 1) = (n + 1)^2, \quad n \geq 1.$$

"Proof:" Suppose it is true for n, i.e., $S_n = (n + 1)^2$. Then, for $n + 1$,

$$\begin{aligned} S_{n+1} &= S_n + (2(n + 1) + 1) \\ &= (n + 1)^2 + (2n + 3) \\ &= n^2 + 4n + 4 \\ &= (n + 2)^2 = ((n + 1) + 1)^2. \end{aligned}$$

Thus, by MI, the statement is true for all $n \geq 1$. What is wrong with the proof? (Induction Basis is not verified.)

Example 1.6. Let $f : X \to X$ be an invertible function. Using MI to prove $f^k \circ f^{-k} = f^0$, where $k \in \mathbb{Z}$, $f^0 = \mathrm{id}_X$.

The conclusion can be stated into two statements:
(1) $f^k \circ f^{-k} = f^0$ for all $k \geq 1$;
(2) $f^{-k} \circ f^k = f^0$ for all $k \geq 0$.
MI Proof: We only prove statement (1).

Proof. For $k = 1$, $f^1 \circ f^{-1} = f^0$, it is true. (by definition of invertibility)

Suppose it is true for $k \geq 1$ and consider the case $k + 1$.

$$
\begin{aligned}
f^{k+1} \circ f^{-(k+1)} &= \underbrace{f \circ \cdots \circ f}_{k} \circ f \circ f^{-1} \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k} \\
&= \underbrace{f \circ \cdots \circ f}_{k} \circ f^0 \circ \underbrace{f^{-1} \circ \cdots \circ f^{-1}}_{k} \\
&= f^k \circ f^0 \circ f^{-k} \\
&= f^k \circ f^{-k} = f^0. \quad \text{(By Induction Hypothesis)}
\end{aligned}
$$

It is true for $k+1$. By MI, it is true for all integers $k \geq 1$. □

The MI may be stated as follows: For problems $P(n)$, where n are integers and $n \geq m$. If,

(a) (Induction Basis or IB) the problem for $n = m$ is true,

(b) (Induction Hypothesis or IH) if the problem is true for case n then it is true for the case $n + 1$;

then $P(n)$ is true for all integers $n \geq m$.

Note. In the Induction Hypothesis, the symbol n is required $n \geq m$ in the process of proving $P(n + 1)$ to be true.

Example 1.7. Try to show that $n! \geq 2^n$ for $n \geq 0$ by MI.

For $n = 0$, $0! = 1 \geq 1$, it is OK. Suppose it is true for case n; consider the case $n+1$. Then

$$(n+1)! = (n+1) \cdot n! \geq 2 \cdot n! \geq 2 \cdot 2^n = 2^{n+1}.$$

Thus by MI, we proved that $n! \geq 2^n$ for all $n \geq 0$. Anything wrong? (The inequality $n + 1 \geq 2$ is wrong when $n = 0$.)

So $n! \geq 2^n$ is not true for $n \geq 0$. However, $n! \geq 2^n$ is true for $n \geq 4$.

2 Second Form of Mathematical Induction

Second Form of MI. Let $P(n)$ be a family of problems indexed by the set $\mathbb{P}$ of positive integers. If,

(a) (Induction Basis or IB) the problem for $n = 1$ is true,

(b) (Induction Hypothesis or IH) if $P(1), P(2), \ldots, P(n)$ are true then $P(n+1)$ is true;

then $P(n)$ is true for all $n \in \mathbb{P}$.

Example 2.1. Let S_n be a sequence defined by

$$S_1 = 1; \quad S_n = S_1 + S_2 + \cdots + S_{n-1}, \quad n \geq 2.$$

Show that $S_n = 2^{n-2}$ for $n \geq 2$.

Proof. For $n = 2$, $S_2 = S_1 = 1 = 2^{2-2}$; it is true. Assume that it is true for $k = 2, 3, \ldots, n$; that is,

$$S_k = 2^{k-2}, \quad k = 2, 3, \ldots, n.$$

Consider the case $n+1$.

$$\begin{aligned} S_{n+1} &= S_1 + S_2 \cdots + S_n \\ &= 1 + \sum_{k=2}^{n} 2^{k-2} \\ &= 1 + (1 + 2 + 2^2 + \cdots + 2^{n-2}) \\ &\quad \left[\text{by } 1 + x + \cdots + x^m = \tfrac{x^{m+1}-1}{x-1}\right] \\ &= 1 + \frac{2^{n-1}-1}{2-1} = 2^{(n+1)-2}. \end{aligned}$$

So it is true for $n+1$. By MI, it is true for all integers $n \geq 2$. □

$$\begin{aligned} &(x-1)(1 + x + x^2 + \cdots + x^n) \\ &= (x + x^2 + \cdots + x^{n+1}) - (1 + x + \cdots + x^n) \\ &= x^{n+1} - 1. \end{aligned}$$

Then

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}, \quad x \neq 1.$$

Summary of MI

1. Do the basis step, say, for $n = 1$.
2. Write "Let n be a fixed but arbitrary integer ≥ 1, assume $P(n)$ is true, try to prove $P(n+1)$."
3. Express the job $P(n+1)$.
4. Prove $P(n+1)$.
5. Write "Therefore the induction step is proved, and by MI, $P(n)$ is true for all positive integers n."