PMI can provide a powerful method for proving statements that are true for all natural numbers.

Suppose that $\mathrm{P}(n)$ is an open sentence concerning the natural numbers.

Proof of $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ by mathematical induction

Proof.

(i) **Basis Step**. Show that $\mathrm{P}(1)$ is true.

(ii) **Inductive Step**. Suppose that $\mathrm{P}(n)$ is true.

$\vdots$

Therefore, $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. $\square$

Example

Prove that for every natural number n,

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 .$$

Proof.

Let $\mathrm{P}(n)$ be the open sentence $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

1. $\mathrm{P}(1)$ is true since $1 = 1^2$.
2. Suppose that $\mathrm{P}(n)$ is true. Then

   $$1+3+5+\cdots+(2n-1)+(2n+1) = n^2+(2n+1) = (n+1)^2$$

   which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. $\square$

Example (De Moivre's formula)

Let θ be a real number. Prove that for every $n \in \mathbb{N}$,

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)\,.$$

Proof.

Let $\mathrm{P}(n)$ be the open sentence $(\cos\theta+i\sin\theta)^n = \cos(n\theta)+i\sin(n\theta)$.

1. Obviously $\mathrm{P}(1)$ is true.
2. Suppose that $\mathrm{P}(n)$ is true. Then

$$\begin{aligned}(\cos\theta + i\sin\theta)^{n+1} &= \big[\cos(n\theta) + i\sin(n\theta)\big]\cdot(\cos\theta + i\sin\theta)\\ &= \big[\cos(n\theta)\cos\theta - \sin(n\theta)\sin\theta\big]\\ &\quad + i\big[\cos(n\theta)\sin\theta + \sin(n\theta)\cos\theta\big]\\ &= \cos(n+1)\theta + i\sin(n+1)\theta\end{aligned}$$

which shows that $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. □

Example (Archimedean Principle for $\mathbb{N}$)

For any natural numbers a and b, there exists a natural number s such that $sb > a$.

Proof.

Let b be a fixed natural number, and $\mathrm{P}(a)$ be the open sentence

$$(\exists\, s \in \mathbb{N})(sb > a)\,.$$

1. If $a = 1$, then $2b > 1$; thus $\mathrm{P}(1)$ is true.
2. Suppose that $\mathrm{P}(n)$ is true. Then there exists $t \in \mathbb{N}$ such that $tb > n$. Then $(t+1)b = tb + b > n + 1$; thus $\mathrm{P}(n+1)$ is true.

Therefore, **PMI** ensures that $(\forall\, n \in \mathbb{N})\mathrm{P}(n)$ is true. $\square$

- **Generalized Principle of Mathematical Induction (GPMI)**:

If $S \subseteq \mathbb{Z}$ has the property that

1. $k \in S$, and
2. $n+1 \in S$ whenever $n \in S$,

then S contains all integers greater than or equal to k.

Reason: Let $T = \{n \in \mathbb{N} \mid k+n-1 \in S\}$. Then $T \subseteq \mathbb{N}$. Moreover,

1. $1 \in T$ since $k \in S$ if and only if $1 \in T$.
2. If $n \in T$, then $k+n-1 \in S$; thus $k+n \in S$ which implies that $n+1 \in T$.

Therefore, **PMI** ensures that $T = \mathbb{N}$ which shows that

$$S = \{n \in \mathbb{Z} \mid n \geqslant k\}.$$

Example

Prove by induction that $n^2 - n - 20 > 0$ for all natural number $n > 5$.

Proof.

Let $S = \{n \in \mathbb{N} \mid n^2 - n - 20 > 0\}$.

1. $6 \in S$ since $6^2 - 6 - 20 = 10 > 0$.
2. Suppose that $n \in S$. Then

$$\begin{aligned}(n+1)^2 - (n+1) - 20 &= n^2 + 2n + 1 - n - 1 - 20 \\ &> 2n > 0\,.\end{aligned}$$

Therefore, **GPMI** ensures that $S = \{n \in \mathbb{N} \mid n \geqslant 6\}$. □

There are two other versions of mathematical induction.

1. **Well-Ordering Principle (WOP)**:

   Every nonempty subset of $\mathbb{N}$ has a smallest element.

2. **Principle of Complete Induction (PCI)**:

   Suppose S is a subset of $\mathbb{N}$ with the property:

   for all natural number n, if $\{1, 2, \cdots, n-1\} \subseteq S$, then $n \in S$.

   Then $S = \mathbb{N}$.

We remark here that in the statement of **PCI** we treat $\{1, 2, \cdots, 0\}$ as $\varnothing$.

Remark:

Similar to **GPMI**, **PCI** can be extended to a more general case stated as follows:

> Suppose S is a subset of $\mathbb{N}$ with the property:
>
> there exists $k \in \mathbb{Z}$ such that for all natural number n, if $\{k, k+1, \cdots, k+n-2\} \subseteq S$, then $k+n-1 \in S$.
>
> Then $S = \{n \in \mathbb{Z} \mid n \geqslant k\}$.

The same as the case of **PCI**, here we treat $\{k, k+1, \cdots, k-1\}$ as the empty set.

In the following, we prove that **PMI** $\Rightarrow$ **WOP** $\Rightarrow$ **PCI** $\Rightarrow$ **PMI**.

Proof of PMI $\Rightarrow$ WOP.

Assume the contrary that there exists a **non-empty** set $S \subseteq \mathbb{N}$ such that S does not have the smallest element. Define $T = \mathbb{N} \setminus S$, and $T_0 = \{n \in \mathbb{N} \,|\, \{1, 2, \cdots, n\} \subseteq T\}$ (T 中從 1 開始數起不需跳號就可以數到的數字). Then we have $T_0 \subseteq T$. Also note that $1 \notin S$ for otherwise 1 is the smallest element in S, so $1 \in T$ (thus $1 \in T_0$).
Assume $k \in T_0$. Since $\{1, 2, \cdots, k\} \subseteq T$, $1, 2, \cdots k \notin S$. If $k+1 \in S$, then $k+1$ is the smallest element in S. Since we assume that S does not have the smallest element, $k+1 \notin S$; thus $k+1 \in T \Rightarrow k+1 \in T_0$.
Therefore, by **PMI** we conclude that $T_0 = \mathbb{N}$; thus $T = \mathbb{N}$ which further implies that $S = \varnothing$, a contradiction. $\square$

Proof of WOP $\Rightarrow$ PCI.

Assume the contrary that for some $S \neq \mathbb{N}$, S has the property

for all natural number n, if $\{1, 2, \cdots, n-1\} \subseteq S$, then $n \in S$. $(\star)$

Define $T = \mathbb{N} \backslash S$. Then T is a **non-empty** subset of $\mathbb{N}$; thus **WOP** implies that T has a smallest element k. Then $1, 2, \cdots, k-1 \notin T$ which is the same as saying that $\{1, 2, \cdots, k-1\} \subseteq S$. By property $(\star)$, $k \in S$ which implies that $k \notin T$, a contradiction. □

Proof of PCI $\Rightarrow$ PMI.

Let $S \subseteq \mathbb{N}$ has the property

(a) $1 \in S$, and (b) $n+1 \in S$ whenever $n \in S$.

We show that $S = \mathbb{N}$ by verifying that

for all natural number n, if $\{1, 2, \cdots, n-1\} \subseteq S$, then $n \in S$.

1. (a) implies $1 \in S$; thus the statement "$\{1, 2, \cdots, k-1\} = \varnothing \subseteq S \Rightarrow 1 \in S$" is true.
2. Suppose that $\{1, 2, \cdots, k-1\} \subseteq S$. Then $k-1 \in S$. Using (b) we find that $k \in S$; thus the statement "$\{1, 2, \cdots, k-1\} \subseteq S \Rightarrow k \in S$" is also true.

Therefore, S has property $(\star)$ and **PCI** implies that $S = \mathbb{N}$. □

Theorem (Fundamental Theorem of Arithmetic)

Every natural number greater than 1 is prime or can be expressed uniquely as a product of primes.

The meaning of the unique way to express a composite number as a product of primes:

Let m be a composite number. Then there is a unique way of writing m in the form

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \,,$$

where $p_1 < p_2 < \cdots < p_n$ are primes and $\alpha_1, \alpha_2, \cdots, \alpha_n$ are natural numbers.

Proof based on WOP.

We first show that every natural number greater than 1 is either a prime or a products of primes, then show that the prime factor decomposition, when it is not prime, is unique.

1. Suppose that there is at least one natural number that is greater than 1, not a prime, and cannot be written as a product of primes. Then the set S of such numbers is non-empty, so **WOP** implies that S has a smallest element m. Since m is not a prime, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. Both s and t are less than the smallest element of S, so they are not in S. Therefore, each of s and t is a prime or is the product of primes, which makes m a product of primes, a contradiction. □

Proof based on WOP (Cont'd).

2. Suppose that there exist natural numbers that can be expressed in two or more different ways as the product of primes, and let n be the smallest such number (the existence of such a number is guaranteed by **WOP**). Then
$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$
for some $k, m \in \mathbb{N}$, where each p_i, q_j is prime. Then p_1 divides $q_1 q_2 \cdots q_m$ which, with the help of Euclid's Lemma, implies that $p_1 = q_j$ for some $j \in \{1, \cdots, m\}$. Then $\frac{n}{p_1} = \frac{n}{q_j}$ is a natural number smaller than n that has two different prime factorizations, a contradiction. □

Alternative Proof of Fundamental Theorem of Arithmetic.

Let m be a natural number greater than 1. We note that 2 is a prime, so the statement is true when m is 2. Now assume that k is a prime or is a product of primes for all k such that $1 < k < m$. If m has no factors other than 1 and itself, then m is prime. Otherwise, $m = st$ for some natural numbers s and t that are greater than 1 and less than m. By the complete induction hypothesis, each of s and t either is prime or is a product of primes. Thus, $m = st$ is a product of primes, so the statement is true for m. Therefore, we conclude that every natural number greater than 1 is prime or is a product of primes by **PCI**. □

Theorem

Let a and b be nonzero integers. Then there is a smallest positive linear combination of a and b.

Proof.

Let a and b be nonzero integers, and S be the set of all positive linear combinations of a and b; that is,

$$S = \left\{ am + bn \,\middle|\, m, n \in \mathbb{Z}, am + bn > 0 \right\}.$$

Then $S \neq \varnothing$ since $a \cdot 1 + b \cdot 0 > 0$ or $a \cdot (-1) + b \cdot 0 > 0$. By **WOP**, S has a smallest element, which is the smallest positive linear combination of a and b. $\square$