Recall the <u>induction principle</u>: If $A \subseteq \mathbb{N}$ is such that $1 \in A$ and $S(A) \subseteq A$, then $A = \mathbb{N}$.

<u>Well-ordering principle</u>: Let $A \subseteq \mathbb{N}$ be a non-empty subset. There exists $n_0 \in A$ such that $\{m : m < n_0\} \cap A = \phi$. The element n_0 is called the minimum element of A.

<u>Proposition</u>: The axiom of induction implies the well-ordering principle.

<u>proof</u>: For $n \in \mathbb{N}$, let $I_n := \{K \in \mathbb{N} : K \leq n\}$.

Suppose for contradiction that there exists a set $A \subseteq \mathbb{N}$ which does not have a minimum element, with $A \neq \phi$.

Let $B = \{n \in \mathbb{N} \mid I_n \cap A = \phi\}$.

If $n \in B$, then $I_n \cap A = \phi$. This implies $n \notin A$. Therefore, $B \subseteq \mathbb{N} \setminus A$

Observe that $1 \notin A$, as 1 is the smallest element in $\mathbb{N}$.

This implies that $1 \in B$.

If $n \in B$, then $I_n \cap A = \phi$. As $I_{n+1} = I_n \cup \{n+1\}$ (because there is no element in between n and $n+1$),

we have two choices

- $n+1 \in A$, and hence $n+1 = \min(A)$, contradiction.
- $n+1 \notin A$, and hence $I_{n+1} \cap A = \phi$, where $n+1 \in B$.

Therefore, $n \in B \Rightarrow n+1 \in B \quad \forall n \in \mathbb{N}$.

We conclude that $B = \mathbb{N}$. As $B = \mathbb{N} \setminus A$, we have $A = \phi$, a contradiction. $\boxtimes$

<u>Proposition</u>: the well-ordering principle implies mathematical induction.

<u>proof</u>: Let $A \subseteq \mathbb{N}$ be such that $1 \in A$ and $S(A) \subseteq A$.

<u>Goal</u>: To show that $A = \mathbb{N}$.

Let $B = \{ k \in \mathbb{N} : k \notin A \}$. Suppose for contradiction that A is non-empty and let $n = \min B$. As $1 \in A$, we have $1 \notin B$. Then, $\exists\, r \in \mathbb{N}$ such that $n = s(r)$.

As $r < n$, by definition of minimum element we have $r \notin B$, and hence $r \in A$. But this imblies $s(r) \in A$, contradiction.

<u>Strong induction</u>: Let A be a set such that $1 \in A$.

Suppose that if $\{1, \ldots, k\} \subseteq A$, then $k+1 \in A$.

Then, $A = \mathbb{N}$.

<u>Proposition</u>: strong induction $\Rightarrow$ weak induction

<u>proof</u>: Let T be a set such that $1 \in S$ and $S(T) \subseteq T$

Note that if $\{1, 2, \ldots, k\} \subseteq T$, then $k \in T$ and hence $k+1 \in T$. By strong induction, we have $T = \mathbb{N}$.

<u>Proposition</u>: weak induction $\Rightarrow$ strong induction.

<u>proof</u>: Let A be a set such that $1 \in A$ and suppose that if $\{1, 2, \ldots, k\} \subseteq A$, then $k+1 \in A$.

Let $B = \{ k \in \mathbb{N} : \{1, 2, \ldots, k\} \subseteq A \}$.

Note that $1 \in B$ and $S(B) \subseteq B$. This implies $B = \mathbb{N}$ (by weak induction). As $B \subseteq A$, we have $A = \mathbb{N}$ $\blacksquare$

Now we do a brief pause on the axiomatic construction of the natural numbers. Next, we see some nice applications of induction.

Problem ① For $n \in \mathbb{N}$, define $H_n = 1 + \frac{1}{2} + \dots + \frac{1}{n}$.

Show that $H_{2^n} \geq 1 + \frac{n}{2}$ for every $n \in \mathbb{N}$.

Solution: Define $A = \{ n \in \mathbb{N} : H_{2^n} \geq 1 + \frac{n}{2} \}$.

Note that $1 \in A$. This is the basis of induction.

Induction step: Let $k \in A$. Our goal is to show that $k+1 \in A$.

Note that

$$H_{2^{k+1}} = H_{2^k} + \underbrace{\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^{k+1}}}_{\text{Each of these terms is } \geq \frac{1}{2^{k+1}}}$$

As the set $\{2^k+1, \dots, 2^{k+1}\}$ has $2^{k+1} - (2^k+1) + 1 = 2^k$ elements, it follows that

$$H_{2^{k+1}} \geq H_{2^k} + 2^k \cdot \frac{1}{2^{k+1}}.$$

As $k \in A$, we have $H_{2^k} \geq 1 + \frac{k}{2}$.

Therefore, it follows that

$$H_{2^{k+1}} \geq H_{2^k} + \frac{1}{2}$$

$$\overset{\text{I.H.}}{\geq} 1 + \frac{k}{2} + \frac{1}{2}$$

$$= 1 + \frac{k+1}{2}.$$

This implies that $k+1 \in A$.

By induction, we have $A = \mathbb{N}$ //

<u>Definition</u>: We say that a divides b, or b is divisible by a, if $\exists\, q \in \mathbb{N}$ such that $b = a \cdot q$. <u>Notation</u>: $a \mid b$.

<u>Problem</u>: Show that $3 \mid n^3 - n$ for all $n \in \mathbb{N}$.

<u>proof</u>: Let $A = \{ n \in \mathbb{N} : 3 \mid n^3 - n \}$.

Note that $1 \in A$, as $3 \mid 0$.

Let $k \in A$. Our goal is to show that $k+1 \in A$.

Note that

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1$$

$$= k^3 - k + 3(k^2 + k).$$

As $k \in A$, we have that $\exists\, q = q(k)$ such that $3 \cdot q(k) = k^3 - k$. Thus,

$$(k+1)^3 - (k+1) = 3q(k) + 3(k^2 + k)$$

$$= 3(q(k) + k^2 + k) \Rightarrow k+1 \in A.$$

We have shown that

① $1 \in A$.

② If $k \in A$, then $k+1 \in A$.

Together, ① and ② imply that $A = \mathbb{N}$.