The goal of today's lecture is to review mathematical induction, the well ordering principle of $\mathbb{N}$ and to prove that the two are equivalent.

\[
/N = \text{set of natural numbers, } \mathbb{Z} = \text{set of integers.}
\]

Well-ordering principle: Any nonempty subset of $\mathbb{N}$ has a smallest element.

Note: $\mathbb{Z}$ has no smallest element. The interval $(0,1)$ has no smallest element.

Principle of mathematical induction (P.M.I.)

Suppose $S \subseteq \mathbb{N}$ so that (1) $1 \in S$ and (2) if $n \in S$ then $n+1 \in S$.

Then: $S = \mathbb{N}$.

Another version:

P.M.I.2 Let $P_1, P_2, P_3, \ldots, P_n, \ldots$ be a collection of statements such that
1) $P_1$ is true
2) if $P_n$ is true then $P_{n+1}$ is true

Then: $P_n$ is true for all $n \in \mathbb{N}$.

Lemma 1.1 P.M.I. and P.M.I.2 are equivalent.

Proof (\(\Rightarrow\)) Assume P.M.I. Suppose \(P_1, P_1, \ldots, P_n, \ldots\) is a collection of statements with (1) $P_1$ true and

(2) $P_n$ true $\Rightarrow$ $P_{n+1}$ true.

Let $S = \{n \in \mathbb{N} \mid P_n \text{ is true}\}$
Then $1 \in S$ (since $P_1$ is true) 
And $n \in S \Rightarrow n+1 \in S$ (since $P_n$ true $\Rightarrow P_{n+1}$ true).

By PMI, $S = \mathbb{N}$, i.e. $P_n$ is true for all $n \in \mathbb{N}$.

$(\Leftarrow)$

Assume PMI 2. Suppose $S \subseteq \mathbb{N}$ with $1 \in S$ and $n \in S \Rightarrow n+1 \in S$.

Let $P_n$ be the statement: $n \in S$.

Then $1 \in S \Rightarrow P_1$ is true.

"$P_n$ is true" means "$n \in S$". So "$P_n$ is true" $\Rightarrow$ "$P_{n+1}$ is true".

PMI 2 $\Rightarrow$ "$P_n$ is true for all $n$", i.e. $n \in S \Rightarrow n \in S$.

But $S \subseteq \mathbb{N}$, i.e. $S = \mathbb{N}$.

Proposition 1.2 Well-ordering principle $\Rightarrow$ PMI.

Proof Assume well-ordering. Let $S \subseteq \mathbb{N}$ be a set with $1 \in S$ and "$n \in S$ $\Rightarrow$ $n+1 \in S$".

If $S \neq \mathbb{N}$, $\mathbb{N} \setminus S \neq \emptyset$.

By well-ordering, $\mathbb{N} \setminus S$ has a smallest element; call it $k$.

Since $1 \in S$ and $k \in S$, $k \neq 1$ $\Rightarrow$ $k > 1$.

$\Rightarrow$ $k-1 \in \mathbb{N}$, since $k-1 < k$ and $k = \min (\mathbb{N} \setminus S)$

$k-1 \notin \mathbb{N} \setminus S$ i.e. $k-1 \in S$.

But then $k = (k-1) + 1 \in S$. Contradiction.

Proposition 1.3 PMI $\Rightarrow$ Well-ordering.

Proof Suppose $\emptyset \neq S \subseteq \mathbb{N}$. We'd like to show $S$ has a smallest element. Suppose not.

Note 1 is the smallest natural number. So $1 \notin S$. 
Let $P_n$ be the statement "$1, 2, \ldots, n \notin S."

Then $P_1$ is true since $1 \notin S$.

Suppose $P_n$ is true: $1, \ldots, n \notin S$.

If $n+1 \in S$, then $n+1$ is the smallest element of $S$

(since $1, \ldots, n \notin S$)

But we assume $S$ has no smallest element. $\Rightarrow n+1 \notin S$.

$\Rightarrow P_{n+1}$ is true.

By PMI, $P_k$ is true for all $k$, i.e.

$\forall k \in \mathbb{N} \quad k \notin S$.

$\Rightarrow S = \emptyset$ (since $S \subseteq \mathbb{N}$).

Contradiction since we assumed $S \neq \emptyset$.

Conclusion: $S$ has a smallest element. $\blacksquare$

---

An Application of well-ordering principle: division "algorithm."

Recall

Definition An integer $b$ divides an integer $c$ if $\exists k \in \mathbb{Z}$

s.t. $c = b \cdot k$

Notation $b | c$

Example $3 | 6$, $3 \nmid 7$ ("3 does not divide 7")

Remark 1. From now on we assume well-ordering principle (and, equivalently, PMI, PMI2) as a property of $\mathbb{N}$

Remark 2 Any nonempty subset $S$ of $\mathbb{Z}_{\geq 0}$ also has a smallest element. Prove it!
Proposition 1.4 (division algorithm) For any two integers \(a\) and \(d\) with \(d \geq 1\), there exist unique integers \(q, r\) so that

1) \(a = q \cdot d + r\)
2) \(0 \leq r < d\)

Proof (existence)

Let \(S = \{ a - t \cdot d \mid t \in \mathbb{Z}, a - t \cdot d \geq 0 \}\)

Claim: \(S \neq \emptyset\)

Reason: If \(a \geq 0\), \(a = a - 0 \cdot d \in S\). If \(a < 0\), \(a - a \cdot d = a \cdot (1 - d) \geq 0\) since \(1 - d \geq 0\). \(\Rightarrow a - a \cdot d \in S\).

By well-ordering principle \(S\) has a smallest element \(r\):

\(r = \min \{ a - t \cdot d \mid t \in \mathbb{Z}, a - t \cdot d \geq 0 \}\)

\(\Rightarrow r \geq 0\) and \(r = a - q \cdot d\) for some \(q \in \mathbb{Z}\).

Remains to show: \(r < d\).

Suppose not: \(r \geq d\). Then

\[0 \leq r - d = (a - q \cdot d) - d = a - (q+1) \cdot d \in S\]

But \(r - d < r\) since \(d \geq 1\).

This contradicts \(r = \min S\).

\(\therefore r < d\).

(Uniqueness) Suppose \(r_1, r_2, r_1, r_2 \in \mathbb{Z}\) so \(a = q_1 \cdot d + r_1, q_1, r_1 \in \mathbb{Z}\).

We want to show: \(r_1 = r_2\) and \(q_1 = q_2\).

Take \(r_1 - r_2 = q_2 d - q_1 d = (q_2 - q_1) d\)

Now, \(r_1, r_2 \leq d \Rightarrow r_1 - r_2 < d\).

Suppose \(q_2 - q_1 \in \mathbb{Z}\)

\((q_2 - q_1) d \) in either \(\mathbb{Z}\) (since \(d\)'s 20) or 0.

\((q_2 - q_1) d \geq d\) contradicts \(r_1 - r_2 < d\).

\(\therefore 0 = (q_2 - q_1) d = r_1 - r_2\)

\(\Rightarrow r_1 = r_2\) and \(q_1 = q_2\). 
\(\square\)