Claim: All odd numbers greater than 1 are prime.

Proof by:

A primary school student:

- 3 is a prime.
- 5 is a prime.
- 7 is a prime.
- So all odd numbers greater than 1 are prime.

An experimental scientist:

- 3, 5, 7 are primes.
- 9 is an experimental error.
- 11, 13 are primes.
- 15 is an experimental error.
- 17, 19 are primes.
- So all odd numbers greater than 1 are prime.

Lecture 6
Part I

MATHEMATICAL INDUCTION

The principle of mathematical induction is used to prove countably infinitely many statements.

Usually these statements are indexed by $\mathbb{Z}^+$, but sometimes $\mathbb{Z}_{\geq k}$ for $k \in \mathbb{Z}$ can also be used to index the statements.

This principle relies on the following:

Theorem (Well-ordering Principle of $\mathbb{Z}^+$)

Every non-empty subset of $\mathbb{Z}^+$ has a minimal element.

Proof.

1. Let $\varnothing \neq S \subseteq \mathbb{Z}^+$.
2. Since $S \neq \varnothing$, there exists $s \in S$.
3. Run the following algorithm:
    1. $n := 1$;
    2. stop := false;
    3. while not stop do
        1. If $n \in S$ then stop := true;
        2. Else $n := n + 1$;
    4. enddo;
    5. return n;
4. The algorithm will stop, after at most s cycles, since $s \in S$.
5. The value returned is the minimal element of S.

$\square$

Theorem (Principle of Mathematical Induction)

For each $n \in \mathbb{Z}^+$, let $P(n)$ be a statement. Suppose that $P(1)$ is true and that $(P(n) \to P(n+1))$ is true for all $n \in \mathbb{Z}^+$. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof.

1. Let $S = \{n \in \mathbb{Z}^+ \mid {\sim}P(n)\}$.
2. $1 \notin S$ since $P(1)$ is true.
3. If $S \neq \varnothing$, then
   1. S has a minimal element m by well-ordering principle.
   2. $m \geq 2$ by (2), and so $m - 1 \in \mathbb{Z}^+$.
   3. $m - 1 \notin S$ by minimality of m.
   4. By (1), (3.2) and (3.3), $P(m-1)$ is true.
   5. Since $P(m-1) \to P(m)$ is assumed true, we have $P(m)$ (modus ponens).
   6. By (1) and (3.5), $m \notin S$, contradicting (3.1).
4. Thus $S = \varnothing$, and $P(n)$ is true for all $n \in \mathbb{Z}^+$.

$\square$

The set $\mathbb{Z}^+$ may be replaced by $\mathbb{Z}_{\geq k}$ ($k \in \mathbb{Z}$) in the well-ordering principle and mathematical induction, in which case the base case $P(1)$ should be replaced by $P(k)$.

How to Prove by Induction

To prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$:

1. Check that the base case $P(1)$ is true.
2. Prove the inductive step: Assume $P(n)$, and use this information to prove that $P(n+1)$ is true.

Example

Prove that $1^3 + 2^3 + \cdots + n^3 = \frac{n^2}{4}(n+1)^2$.

Solution:

1. Let $P(n) = (1^3 + 2^3 + \cdots + n^3 = \frac{n^2}{4}(n+1)^2)$.
2. $P(1) = (1^3 = \frac{1^2}{4}(1+1)^2)$, which is true.
3. Assume $P(n)$, i.e. $1^3 + 2^3 + \cdots + n^3 = \frac{n^2}{4}(n+1)^2$.

   $[P(n+1) = \big(1^3 + 2^3 + \cdots + (n+1)^3 = \frac{(n+1)^2}{4}((n+1)+1)^2\big).]$

4. Now,

$$\begin{aligned} 1^3 + 2^3 + \cdots + (n+1)^3 &= (1^3 + 2^3 + \cdots + n^3) + (n+1)^3 \\ &= \frac{n^2}{4}(n+1)^2 + (n+1)^3 \qquad \text{(applying } P(n)\text{)} \\ &= \frac{n^2+4(n+1)}{4}(n+1)^2 = \frac{(n+2)^2}{4}(n+1)^2. \end{aligned}$$

5. Thus $P(n+1)$ is true.
6. By MI, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Example

Prove that $1 + 3n < n^2$ for all positive integers $n \geq 4$.

Solution:

1. Let $P(n) = (1 + 3n < n^2)$.
2. $P(4) = (1 + 3(4) < 4^2)$, which is true.
3. Assume $P(n)$, i.e. $1 + 3n < n^2$.

   $[P(n+1) = \big(1 + 3(n+1) < (n+1)^2\big).]$

4. Now,

$$
\begin{aligned}
1 + 3(n+1) &= 1 + 3n + 3 \\
&< n^2 + 3 && \text{(applying } P(n)\text{)} \\
&= n^2 + 2 + 1 \\
&< n^2 + 2n + 1 && (1 < n) \\
&= (n+1)^2.
\end{aligned}
$$

5. Thus $P(n+1)$ is true.
6. By MI, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 4}$.

A 'Proof' that All Horses Have the Same Colour

1. Let $P(n) =$ 'in any collection of n horses, the horses have the same colour'.
2. $P(1)$ is clearly true.
3. Assume $P(n)$, i.e. any collection of n horses have the same colour.
4. Let $H = \{h_1, h_2, \ldots, h_{n+1}\}$ be a collection of $n+1$ horses (where each h_i denote a horse).
5. Then $H - \{h_{n+1}\}$ is a collection of n horses, so by $P(n)$, they have the same colour, say brown.
6. Also, $H - \{h_1\}$ is another collection of n horses, so by $P(n)$, they have the same colour.
7. $h_2 \in H - \{h_{n+1}\}$, so h_2 is brown.
8. $h_2, h_{n+1} \in H - \{h_1\}$, so h_{n+1} is also brown by (6).
9. Thus all the horses in H are brown by (5) and (9); in particular, all horses in H have the same colour.
10. Since H is an arbitrary collection of $n+1$ horses, $P(n+1)$ is true.
11. By MI, $P(n)$ is true for all $n \in \mathbb{Z}^+$.
12. Let N be the total number of horses in the world at this present moment. Then $P(N)$ is true, and so all horses have the same colour.

What went wrong?

Strong Mathematical Induction

Theorem

For each $n \in \mathbb{Z}^+$, let $P(n)$ be a statement. Suppose that $P(1)$ is true, and that $(P(1) \wedge P(2) \wedge \cdots \wedge P(n) \rightarrow P(n+1))$ is true for all $n \in \mathbb{Z}^+$. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof.

Exercise. $\square$

How to Prove by Strong Induction

To prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$:

1. Check that the base case $P(1)$ is true.
2. Prove the inductive step: Assume that $P(1), \ldots, P(n)$ is true, and use this information to prove that $P(n+1)$ is true.

Note

- Difference between proving by normal induction and by strong induction:
  1. For normal induction, only $P(n)$ is assumed when proving $P(n+1)$.
  2. For strong induction, we may assume $P(1), \ldots, P(n)$ when proving $P(n+1)$.

  Usually proving by strong induction is easier, since we can assume more information when trying to prove $P(n+1)$ in the inductive step.
- Statements that can be proved by normal induction can also be proved by strong induction, but not necessarily vice versa.

For the next theorem/example, we recall:

Let $n \in \mathbb{Z}^+$. Then n is **composite** if there exist $a, b \in \mathbb{Z}^+$ with $1 < a, b < n$ and $n = ab$.
Furthermore, n is **prime** if and only if $n \geq 2$ and n is not composite.

Existence of Prime Factorisation

Theorem

Every $n \in \mathbb{Z}_{\geq 2}$ can factorised into primes (i.e. $n = p_1 p_2 \cdots p_k$ where $p_1, p_2 \ldots, p_k$ are primes, and $k \in \mathbb{Z}^+$).

Proof.

1. For each $n \in \mathbb{Z}_{\geq 2}$, let $P(n) = (n$ can be factorised into primes).
2. $P(2) = (2$ can be factorised into primes), which is true since 2 is a prime.
3. Assume $P(2), P(3), \ldots, P(n)$.
4.
    1. Case 1: $n+1$ is prime. Then $P(n+1)$ is clearly true.
    2. Case 2: $n+1$ is composite. Then $n+1 = ab$ for some $a, b \in \mathbb{Z}^+$ with $1 < a, b < n+1$.
        1. $P(a)$ and $P(b)$ are true by (3). So $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_l$ for some primes $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$.
        2. Thus, $n+1 = ab = (p_1 p_2 \cdots p_k)(q_1 q_2 \cdots q_l)$.
        3. Hence $P(n+1)$ is true.
5. In all cases, $P(n+1)$ is true.
6. By SMI, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 2}$.

□

Other Forms of Mathematical Induction

Theorem

Let $k \in \mathbb{Z}^+$. For each $n \in \mathbb{Z}^+$, let $P(n)$ be a statement. Suppose that $P(1), P(2), \ldots, P(k)$ are true, and that $(P(n) \wedge P(n+1) \wedge \cdots \wedge P(n+k-1) \rightarrow P(n+k))$ is true for all $n \in \mathbb{Z}^+$. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proof.

Exercise. □

Note

This form of induction is particularly useful for proving results about recursively defined sequences.

Example

The **Fibonacci sequence** $a_0, a_1, \ldots, a_n, \ldots$ is defined by $a_0 = 0$, $a_1 = 1$, and $a_n = a_{n-1} + a_{n-2}$ for all $n \in \mathbb{Z}_{\geq 2}$. Prove that $a_n < 2^n$ for all $n \in \mathbb{Z}_{\geq 0}$.

Solution:

1. For each $n \in \mathbb{Z}_{\geq 0}$, let $P(n) = (a_n < 2^n)$.
2. $P(0) = (a_0 < 2^0)$, which is true.
3. $P(1) = (a_1 < 2^1)$, which is also true.
4. Assume $P(n)$ and $P(n+1)$, i.e. $a_n < 2^n$ and $a_{n+1} < 2^{n+1}$.
5. Note that $n \geq 0$, so that $n + 2 \geq 2$. Thus

$$\begin{aligned} a_{n+2} &= a_{n+1} + a_n && \text{(given recurrence relation)} \\ &< 2^{n+1} + 2^n && \text{(applying } P(n+1) \text{ and } P(n)\text{)} \\ &< 2^{n+1} + 2^{n+1} \\ &= 2(2^{n+1}) = 2^{n+2}. \end{aligned}$$

6. Thus $P(n+2)$ is true.
7. By MI, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 0}$.

Consider the following proof of the last example using strong induction:

1. For each $n \in \mathbb{Z}_{\geq 0}$, let $P(n) = (a_n < 2^n)$.
2. $P(0) = (a_0 < 2^0)$, which is true.
3. Assume $P(0), P(1), \ldots, P(n)$.
4. Then

$$\begin{aligned} a_{n+1} &= a_n + a_{n-1} && \text{(given recurrence relation)} \\ &< 2^n + 2^{n-1} && \text{(applying } P(n) \text{ and } P(n-1)\text{)} \\ &< 2^n + 2^n \\ &= 2(2^n) = 2^{n+1}. \end{aligned}$$

5. Thus $P(n+1)$ is true.
6. By SMI, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 0}$.

Is this proof valid? Why/Why not?

Limitations of Mathematical Induction

While mathematical induction is a good method to employ in many proofs, its limitation include:

- it cannot be used to prove uncountably infinitely many statements;
- it can only be used to verify an asserted statement, but does not offer any insight on how the asserted statement comes about;
- it cannot be used to find reasonable assertions which it can then verify;
- sometimes, assuming all preceding statements does not necessarily provide enough information to prove the succeeding statement.

Summary

We have covered:

- Well-ordering principle of $\mathbb{Z}^+$ (or $\mathbb{Z}_{\geq k}$)
- Principle of mathematical induction:
  - Usual induction
  - Strong induction
  - A variant useful for proving results about recursively defined sequences
- Existence of prime factorisation for $\mathbb{Z}_{\geq 2}$ (proved by strong induction)