Overview

• HW#1 Due Now & Pick up HW2 handout! Due in next week 9/18
• Last lecture: Sets Completed (keep coming back...)
  – Proof templates for sets: I and II
  – Set Operations: Union, Intersection, Difference, Sym Diff., Complement, Cartesian products
  – Set Identities, Proof by cases, Proof by using existing rules
  – Basic counting theorems
  – Principle of inclusion and exclusion
• Today’s lecture: General Proof Techniques
  – Proof by Exhaustion
  – Direct Proof
  – Proof by Counter Example
  – Proof by Contraposition
  – Proof by Contradiction
  – Proof Exercise by Various Methods
  – Mathematical Induction
  – Strong form of mathematical induction

Chapter 1.2 : Proof Techniques
Review some set proof templates

- \( x \in A \): show that \( x \) has all membership properties of \( A \)
- \( A \subseteq B \): show that every element of \( A \) is also in \( B \).
- \( A \subset B \): show \( A \subseteq B \) and also some element \( x \) of \( B \) is not in \( A \)
- \( A = B \): show that \( A \subseteq B \) and \( B \subseteq A \)
- \( A \neq B \): show that \( A \not\subseteq B \) or \( B \not\subseteq A \) by showing some element \( x \) of \( A \) or \( B \) is not in \( B \) or \( A \)
- \( A \rightarrow B \): suppose \( A \) is true then derive \( B \): “if \( A \), then \( B \)”
- \( A \leftrightarrow B \): show that \( A \rightarrow B \) and \( B \rightarrow A \)
- Proof by Cases: Make Membership Tables
- Proof by Using Existing Rules: Deductive Proof with Set Identities

Six general proof techniques

1) **Exhaustive Proof**: (to prove \( P \) is true),
   Show that all possible cases for \( P \) are true, (only for finite cases)
2) **Direct Proof**: to prove \( P \rightarrow Q \) is true (if \( P \) is true, then \( Q \) is true),
   Show that, suppose \( P \) is true, then **deduce** \( Q \). (deductive)
3) **Contraposition**: to prove \( P \rightarrow Q \) is true
   Show \( \neg Q \rightarrow \neg P \) (\( \neg Q \) implies \( \neg P \))
   (indirect proof)
4) **Contradiction**: to prove \( P \rightarrow Q \) is true,
   Show \( P \) and \( \neg Q \rightarrow \) (**contradiction**):
   Assume both the **hypothesis** (\( P \)) and the negation of the **conclusion** (\( \neg Q \)) are true, then try to deduce some contradiction from this assumption.
5) **Counterexample**: to disprove something

6) **Induction**: to prove that \( P(n) \) is true for all \( n \),
Use the principle of mathematical induction:

Base case: \( P(1) \) or \( P(0) \) is true
For all \( k \), \( [ P(k) \) true \( \rightarrow P(k+1) \) true \]
Conclusion: \( P(n) \) true, \( \forall n \)

---

**Proof by Exhaustion**: "**Proof by case**"

Example: Show that \( n! < 2^n \) for \( U = \{1, 2, 3\} \)
any positive integer \( n \leq 3 \) (U?)

Proof:

List all possible cases:

- \( n=1, \ 1! < 2^1 \rightarrow 1 < 2 \ \text{(true)} \)
- \( n=2, \ 2! < 2^2 \rightarrow 2 < 4 \ \text{(true)} \)
- \( n=3, \ 3! < 2^3 \rightarrow 6 < 8 \ \text{(true)} \)
Example: if an integer between 5 and 15 is divisible by 6, then it is also divisible by 3.

Proof:

List all possible cases:

- $n = 6$ is divisible by 6 and is divisible by 3.
- $n = 12$ is divisible by 6 and is divisible by 3.
- All other $n$ values are not divisible by 6.

Note: If the above problem is for all integers, then we cannot use exhaustive proof.

Direct Proof: (deductive)

Example: For all $x$, if $x$ is divisible by 6, then $x$ is divisible by 3.

Proof:

if $x$ is divisible by 6

$\rightarrow x = k \cdot 6$, for some integer $k$

$\rightarrow x = k \cdot 2 \cdot 3$

$\rightarrow x = (k \cdot 2) \cdot 3$

$\rightarrow x = k' \cdot 3$, where $k' = k \cdot 2$

since $k'$ is integer, $x$ is divisible by 3.
Example: Show that the product of two even integers is even.
Proof: Let \( x = 2m, y = 2n \) for some integer \( m, n \)
then \( xy = (2m)(2n) = 2(2mn) \), which is even
\[ \therefore 2mn \text{ is integer.} \]
\[ \because \text{be cause} \]

Example: Show that the sum of two odd integers is even
Proof: Let \( x = 2m+1, y = 2n+1 \) for some integer \( m,n \)
then \( x + y = 2m + 2n + 2 = 2(m+n+1) \),
where \( m+n+1 \) is an integer
\[ \therefore x+y \text{ is even.} \]

**Proof by Counterexample:**
Proving \( P \) to be false (disproof) is much easier than proving \( P \) to be true (proof)!

**PROOF:** must show all cases are true

**DISPROOF:** showing only one case that is not true suffices!

\[
B \cap C = A \cup (B \cap C) \\
A \cup B = (A \cup B) \cap (A \cup C)
\]

<table>
<thead>
<tr>
<th>A B C</th>
<th>B \cap C</th>
<th>A \cup (B \cap C)</th>
<th>A \cup B</th>
<th>A \cup C</th>
<th>(A \cup B) \cap (A \cup C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0 0 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0 1 0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0 1 1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1 0 0</td>
<td>0</td>
<td>( \times )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1 0 1</td>
<td>0</td>
<td>( \times )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1 1 0</td>
<td>0</td>
<td>( \times )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1 1 1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

10
**Proof by Counterexample:**

Proving $P$ to be false (disproof) is much easier than proving $P$ to be true (proof)!

**PROOF:** must show all cases are true  
**DISPROOF:** showing only one case that is not true suffices!

There are two (three) types of questions in proof
1) Prove/disprove a statement $P$.
2) Is a statement $P$ true?
3) Prove/disprove a statement $P$ by using $X$ technique

The second question requires you to see if the statement $P$ is true or not. So you must consider both cases of $P$ is true and $P$ is false.

---

**Examples for Proof by Counterexample:**

Example: Disprove that every integer less than 10 is bigger than 5.

To disprove (or prove the statement is not true), find a counterexample,

Let $n = 4 < 10$, but $n$ is not $> 5$.

Example: Is the sum of any three consecutive integers even?

Proof or Disproof?

To disprove the statement, give a counterexample: $2+3+4=9$
**Proof by Contraposition:**

Example: Prove that: If the square of an integer is odd, then the integer must be odd.

**note:** \( P \rightarrow Q \iff Q' \rightarrow P' \)

Prove: If \( n^2 \) is odd, then \( n \) is odd (initial statement)

Prove: If \( n \) is not odd, then \( n^2 \) is not odd (contraposition)

i.e. Prove: \( n \) is even \( \rightarrow \) \( n^2 \) is even

Let \( n = 2m \) for some integer \( m \)

\[
\rightarrow n^2 = n \times n = 2m \times 2m = 2(2m^2)
\]

\[
\rightarrow \text{since } 2m^2 \text{ is integer, } n^2 \text{ is even.}
\]

---

Example: Show that \( xy \) is odd if and only if both \( x \) and \( y \) are odd.

**Proof:**

\( \iff \) if \( x \) and \( y \) are odd, then \( xy \) is odd.

By direct proof:

Let \( x = 2m+1, y=2n+1 \) for some \( m, n \in \text{integers} \)

\[
\rightarrow xy = (2m+1)(2n+1) = 4mn + 2m + 2n +1 = 2(2mn+m+n) +1
\]

\[
\rightarrow \text{since } 2mn + m + n \text{ is an integer, } xy \text{ is odd.}
\]
(⇒) if xy is odd then x and y are odd.

By contraposition: if x is not odd or y is not odd, then xy is not odd

i.e. if x even or y even, then xy even

**case1** x even, y odd: Let x = 2m, y = 2n+1

xy = 2(2mn + m), which is even \( \therefore 2mn+m \in \mathbb{Z} \)

**case2** x odd, y even: similar to case1.

**case3** x even, y even: Let x = 2m, y = 2n

xy = 2(2mn), which is even \( \therefore 2mn \in \mathbb{Z} \)

---

**Proof by Contradiction**

- Prove/Show \( P \rightarrow Q \) by contradiction method
- Is equivalent to show that \( (P \wedge Q') \) deduces to a contradiction (violation of assumption)
- Logical proof of contradiction:
  - Let \( x' = (P \rightarrow Q)' = P \wedge Q' \), we assume \( x' \) and derive a contradiction \( y' \), i.e. \( x' \rightarrow y' \)
  - Where \( y' \) is false, i.e. \( y \) is true (or axiom)
  - By modus tollens: \( (x' \rightarrow y') \wedge y \rightarrow x \)
  - Therefore, conclude \( x = P \rightarrow Q \) is true
Proof by Contradiction:

Example: If a number added to itself gives itself, then the number is 0, i.e. if $x + x = x$, then $x = 0$.

Proof:
Assume $x + x = x$ and $x \neq 0$.

$\Rightarrow 2x = x$ and $x \neq 0$.

$\Rightarrow 2 = 1$, which is a contradiction.

$\therefore$ the assumption must be wrong.

$\therefore$ if $x + x = x$, then $x = 0$.

Example: Prove that if $x^2 + 2x - 3 = 0$, then $x \neq 2$.

1. by contradiction: $P \Rightarrow \neg Q$.

Suppose $x^2 + 2x - 3 = 0$ and $x = 2$,

$\Rightarrow 4 + 4 - 3 = 0$ or $5 = 0$, which is a contradiction.

2. by direct proof:

if $x^2 + 2x - 3 = 0 \Rightarrow (x + 3)(x - 1) = 0$

$\Rightarrow x = -3$ or $x = 1 \Rightarrow x \neq 2$.

3. by contraposition: $\neg Q \Rightarrow \neg P$.

show that if $x = 2$, then $x^2 + 2x - 3 \neq 0$.

$\Rightarrow x^2 + 2x - 3 = 5 \neq 0$. 
In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

a) Proof by contradiction

b) Proof by contraposition

c) Direct proof

In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

$\overline{P}$ \hspace{1cm} $\overline{Q}$

a) Proof by contradiction $P \land \lnot Q \Rightarrow \rightarrow \rightarrow \rightarrow \text{(contradiction)}$

b) Proof by contraposition $\lnot Q \rightarrow \rightarrow \rightarrow P'$

c) Direct proof $P \rightarrow \rightarrow \rightarrow Q$
In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

a) Proof by contradiction

- $3n+2$ is odd and $n$ is even
- $3n$ is even (product of odd and even is even)
- $n$ is even (product of even and odd is even)

$b)$ Proof by contraposition

If $n$ is even
- $n = 2m$ for some $m \in \mathbb{Z}$
- $3n+2 = 6m + 2 = 2(3m+1)$
- Even

$c)$ Direct proof

- $3n+2$ is odd
- $3n$ is odd (product of two odd numbers is odd)
- $n$ is odd (since $3n$ is even)

Mathematical Induction:

Proof by induction: to prove that the property $p(n)$ is true for all possible value of $n$

Idea: like playing the domino game.

Suppose dominos are placed correctly, then hitting the $1^{st}$ domino, when it falls, we know the rest of them will also fall.

(∵ In general, when the $k^{th}$ one falls, it implies the $(k+1)^{th}$ falls. Since $k$ is any arbitrary number, ∴ actually every domino falls.)
Mathematical Induction (template):

**Step 1:** (inductive base) or IB is to show that \( p(n_0) \) is true. Choose an \( n_0 \in \mathbb{N} \) appropriate to the problem.

Note: \( n_0 \) is usually a small number 0 or 1 unless a range is specified.

**Step 2:** (inductive hypothesis) or IH:

Assume \( p(k) \) is true for any \( k \geq n_0 \).

**Step 3:** (inductive step) or IS:

Show that \( p(k) \rightarrow p(k + 1) \), for all natural numbers \( k \) such that \( k \geq n_0 \).

(If \( p(k) \) is true then \( p(k+1) \) is also true; if a domino falls, the next domino also falls)

---

Example 1: show \( 1 + 3 + 5 + \ldots (2n-1) = n^2 \), for all \( n \geq 1 \)

**IB:** when \( n_0 = 1 \), \( \text{LHS} = 1 = 1^2 = \text{RHS} \)

**IH:** Assume \( 1 + 3 + 5 + \ldots (2k-1) = k^2 \) for \( n = k \geq n_0 \)

**IS:** Show \( 1 + 3 + 5 + \ldots (2k-1) + [2(k+1)-1] = (k+1)^2 \)

\[
\begin{align*}
\text{LHS}' &= 1 + 3 + 5 + \ldots (2k-1) + (2k + 1) \\
&= k^2 + 2k + 1 \quad \text{(by IH)} \\
&= (k + 1)^2 \\
&= \text{RHS}'
\end{align*}
\]

\( \therefore \) \( \text{LHS} = \text{RHS} \)
Example 2: Show \(1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}\), for all \(n \geq 1\)

**IB:** when \(n_o = 1\), LHS = \(1 = \frac{1(1+1)}{2} = \text{RHS}\)

**IH:** Assume \(1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}\) for \(n = n_o = 1\)

**IS:** Show \(1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}\)

\[
\text{LHS}' = 1 + 2 + 3 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)
\]

(by IH)

\[
= \frac{k(k+1) + 2(k+1)}{2} = \text{RHS}'
\]

by direct proof: Let \(x = 1 + 2 + 3 + \ldots + k\)

\[
+ \) \(x = k + k-1 + k-2 + \ldots + 1
\]

\[
2x = (k+1) + (k+1) + \ldots + (k+1) = kx(k+1)
\]

\[
\text{k of them}
\]

\[
\therefore x = \frac{k(k+1)}{2}
\]
Example 3: Show \( \sum_{i=1}^{n} 2^i - 1 = 2^{n+1} - 1 \), for all \( n \geq 1 \)

IB: when \( n_0 = 1 \), LHS = 1 + 2 = 3 = 2^2 - 1 = RHS

IH: Assume \( 1 + 2 + 2^2 + \ldots + 2^k = 2^{k+1} - 1 \) for \( n = k \geq n_0 \)

IS: Show \( 1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1 \) (\( n = k+1 \))

\[
\therefore \text{LHS}' = 1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} \quad \text{(by IH)}
\]
\[
= 2 \cdot 2^{k+1} - 1
\]
\[
= 2^{k+2} - 1
\]
\[
= \text{RHS}'
\]

Example 4: Show \( 2^{2n} - 1 \) is divisible by 3, for all \( n \geq 1 \)

IB: when \( n_0 = 1 \), \( 2^2 - 1 = 3 \) \( \therefore \) divisible by 3

IH: Assume \( 2^{2k} - 1 \) is divisible by 3

i.e. \( 2^{2k} - 1 = 3m \) for some integer \( m \) for \( n = k \geq n_0 \)

IS: show \( 2^{2(k+1)} - 1 \) is divisible by 3.

\[
2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1
\]
\[
= 2^2(3m+1) - 1 \quad (\because 2^{2k} - 1 = 3m)
\]
\[
= 2^2(3m + 1, \text{by IH})
\]
\[
= 12m + 3
\]
\[
= 3(4m + 1) \quad \text{where} \ 4m + 1 \ \text{is an integer}
\]

\( \therefore \) is divisible by 3
Example 5 (Fibonacci number property) Show that:

\[ F_1 + F_3 + \ldots + F_{2n-1} = F_{2n} - 1, \text{ for all } n \geq 1. \]

Note: \( F_0 = F_1 = 1 \) and \( F_k = F_{k-1} + F_{k-2} \) for all \( k > 2 \)

IB: when \( n_0 = 1 \), LHS = \( F_1 = 1 \), RHS = \( F_2 - 1 = 1 \)

IH: Assume \( F_1 + F_3 + \ldots + F_{2k-1} = F_{2k} - 1 \), for \( n = k \geq n_0 \)

IS: show \( F_1 + F_3 + \ldots + F_{2(k+1)-1} = F_{2(k+1)} - 1 \)

LHS’ = \( F_1 + F_3 + \ldots + F_{2k-1} + F_{2k+1} = F_{2k} - 1 + F_{2k+1} \)

(by Fibonacci number formula)

= \( F_{2k+2} - 1 \) (by IH)

= \( F_{2(k+1)} - 1 \)

= RHS’

Example 6 (Cardinality of a power set) : For any set \( X \) with \( |X| = n \), \( |P(X)| = 2^n \), for all \( n \geq 0 \).

IB: when \( n = 0 \), LHS = \( |P(\emptyset)| = 1 \), RHS = \( 2^0 = 1 \)

IH: Assume \( |X| = k \), \( |P(X)| = 2^k \) for \( n = k \geq 0 \)

IS: show \( |X| = k+1 \), \( |P(X)| = 2^{k+1} \)

Lemma: Let \( A \) be any set and let \( b \notin A \). If \( |P(A)| = m \), then \( |P(A \cup \{b\})| = 2m \).

Pick any element \( b \) from \( X \) in IS, \( |X\{b\}| = k \)

\( \rightarrow \) \( |P(X - \{b\})| = 2^k \) (by IH)

\( \rightarrow \) \( |P(X)| = 2 \times 2^k \) (by Lemma) = \( 2^{k+1} \)
In class exercise

Use induction to prove that:

\[ 2^n < n!, \text{ for all } n \geq 4 \]
Strong Form of Mathematical Induction (template):

Step1: \textit{(inductive base) or IB} is to show that \( p(n_o) \) is true. Choose an \( n_o \in \mathbb{N} \) appropriate to the problem.

Step2: \textit{(inductive hypothesis) or IH}:

Assume \( p(m) \) is true for all \( m: k \geq m \geq n_o \)

Step3: \textit{(inductive step) or IS} is to show that \( p(k) \rightarrow p(k + 1) \), for all \( k \) such that \( k \geq n_o \)

Example: Given \( a_0 = 0, a_1 = 2 \) and \( a_n = 4(a_{n-1} - a_{n-2}) \) for all \( n \geq 2 \). Show that: \( a_n = n \times 2^n \) for all \( n \)

IB: when \( n = 0 \), LHS = \( a_0 = 0 \), RHS = \( 0 \times 2^0 = 0 \)

\( n = 1 \), LHS = \( a_1 = 2 \), RHS = \( 1 \times 2^1 = 2 \)

\( n = 2 \), LHS = \( a_2 = 8 \), RHS = \( 2 \times 2^2 = 8 \)

IH: Assume \( a_k = k \times 2^k \) for all indices below \( k \)

IS: show \( a_{k+1} = (k+1) \times 2^{k+1} \)

LHS = \( 4(a_k - a_{k-1}) = 4(k \times 2^k - (k-1) \times 2^{k-1}) \) (by IH)

= \( 4(2k \times 2^{k-1} - k \times 2^{k-1} + 2^{k-1}) = 4(k+1)(2^{k-1}) \)

= \( (k+1) \times 2^{k+1} = \text{RHS} \)
Overview

• HW#1 Due Now & Pick up HW2 handout! Due in next week 9/18
• Last lecture: Sets Completed (keep coming back...)
  – Proof templates for sets: I and II
  – Set Operations: Union, Intersection, Difference, Sym Diff., Complement, Cartesian products
  – Set Identities, Proof by cases, Proof by using existing rules
  – Basic counting theorems
  – Principle of inclusion and exclusion
• Today’s lecture: General Proof Techniques
  – Proof by Exhaustion
  – Direct Proof
  – Proof by Counter Example
  – Proof by Contraposition
  – Proof by Contradiction
  – Proof Exercise by Various Methods
  – Mathematical Induction
  – Strong form of mathematical induction

Chapter 1.2 : Proof Techniques
Review some set proof templates

- \( x \in A \): show that \( x \) has all membership properties of \( A \)
- \( A \subseteq B \): show that every element of \( A \) is also in \( B \).
- \( A \subset B \): show \( A \subseteq B \) and also some element \( x \) of \( B \) is not in \( A \)
- \( A = B \): show that \( A \subseteq B \) and \( B \subseteq A \)
- \( A \neq B \): show that \( A \not\subseteq B \) or \( B \not\subseteq A \) by showing some element \( x \) of \( A \) or \( B \) is not in \( B \) or \( A \)
- \( A \rightarrow B \): suppose \( A \) is true then derive \( B \): “if \( A \), then \( B \)”
- \( A \leftrightarrow B \): show that \( A \rightarrow B \) and \( B \rightarrow A \)

- Proof by Cases: Make Membership Tables
- Proof by Using Existing Rules: Deductive Proof with Set Identities

Six general proof techniques

1) **Exhaustive Proof**: (to prove \( P \) is true),
Show that all possible cases for \( P \) are true, (only for finite cases)

2) **Direct Proof**: to prove \( P \rightarrow Q \) is true (if \( P \) is true, then \( Q \) is true),
Show that, suppose \( P \) is true, then **deduce** \( Q \).
(deductive)

3) **Contraposition**: to prove \( P \rightarrow Q \) is true
Show not-\( Q \rightarrow \) not-\( P \) (not-\( Q \) implies not-\( P \))
(indirect proof)

4) **Contradiction**: to prove \( P \rightarrow Q \) is true,
Show \( P \) and not-\( Q \rightarrow \) (contradiction):
Assume both the **hypothesis** \( (P) \) and the negation of the **conclusion** (not-\( Q \)) are true, then try to deduce some contradiction from this assumption.
5) **Counterexample**: to disprove something

6) **Induction**: to prove that $P(n)$ is true for all $n$,
Use the principle of mathematical induction:

Base case: $P(1)$ or $P(0)$ is true
For all $k$, $[ P(k) \text{ true} \implies P(k+1) \text{ true} ]$
Conclusion: $P(n) \text{ true, } \forall n$

---

**Proof by Exhaustion**: "Proof by case"

Example: Show that $n! < 2^n$ for $U = \{1, 2, 3\}$ any positive integer $n \leq 3$ (U?)

Proof:

List all possible cases:

- $n=1, \ 1! < 2^1 \implies 1 < 2 \ (\text{true})$
- $n=2, \ 2! < 2^2 \implies 2 < 4 \ (\text{true})$
- $n=3, \ 3! < 2^3 \implies 6 < 8 \ (\text{true})$

$\Box \ Q.E.D.$
Example: if an integer between 5 and 15 is divisible by 6, then it is also divisible by 3.
Proof:

List all possible cases:
- n = 6 is divisible by 6 and is divisible by 3
- n = 12 is divisible by 6 and is divisible by 3
- All other n values are not divisible by 6

Note: If the above problem is for all integers, then we cannot use exhaustive proof.

Direct Proof: (deductive)

Example: For all x, if x is divisible by 6, then x is divisible by 3.

Proof:
- if x is divisible by 6
  → x = k * 6, for some integer k
  → x = k * 2 * 3
  → x = (k * 2) * 3
  → x = k’ * 3, where k’ = k * 2
- since k’ is integer, x is divisible by 3
Example: Show that the product of two even integers is even.
Proof: Let \( x = 2m, y = 2n \) for some integer \( m, n \)
then \( xy = (2m)(2n) = 2(2mn) \), which is even
\( \therefore \) 2mn is integer.

Example: Show that the sum of two odd integers is even.
Proof: Let \( x = 2m+1, y = 2n+1 \) for some integer \( m,n \)
then \( x + y = 2m + 2n+ 2 = 2(m+n+1) \),
where \( m+n+1 \) is an integer
\( \therefore \) \( x+y \) is even.

Proof by Counterexample:
Proving \( P \) to be false (disproof) is much easier than proving \( P \) to be true (proof)!

PROOF: must show all cases are true
DISPROOF: showing only one case that is not true suffices!

\[
\begin{array}{c|c|c|c|c|c|c}
A & B & C & B \cap C & A \cup (B \cap C) & A \cup B & A \cup C & (A \cup B) \cap (A \cup C) \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
\end{array}
\]
**Proof by Counterexample:**

Proving $P$ to be false (disproof) is much easier than proving $P$ to be true (proof)!

- **PROOF:** must show all cases are true
- **DISPROOF:** showing only one case that is not true suffices!

There are two (three) types of questions in proof:

1) Prove/disprove a statement $P$.
2) Is a statement $P$ true?
3) Prove/disprove a statement $P$ by using X technique

The second question requires you to see if the statement $P$ is true or not. So you must consider both cases of $P$ is true and $P$ is false.

---

**Examples for Proof by Counterexample:**

Example: Disprove that every integer less than 10 is bigger than 5.

To disprove (or prove the statement is not true), find a counterexample,

Let $n = 4 < 10$, but $n$ is not $> 5$.

Example: Is the sum of any three consecutive integers even?

Proof or Disproof?

To disprove the statement, give a counterexample: $2+3+4 = 9$
Proof by Contraposition:

Example: Prove that: If the square of an integer is odd, then the integer must be odd.

\[ P \implies Q \iff Q' \implies P' \]

Prove: if \( n^2 \) is odd, then \( n \) is odd (initial statement)

Prove: if \( n \) is not odd, then \( n^2 \) is not odd (contraposition)

i.e. Prove: \( n \) is even \( \implies \) \( n^2 \) is even

Let \( n = 2m \) for some integer \( m \)

\[ \rightarrow n^2 = n \times n = 2m \times 2m = 2(2m^2) \]

\[ \rightarrow \text{since } 2m^2 \text{ is integer, } n^2 \text{ is even.} \]

Example: Show that \( xy \) is odd if and only if both \( x \) and \( y \) are odd.

\( \iff \) if \( x \) and \( y \) are odd, then \( xy \) is odd.

By direct proof:

Let \( x = 2m + 1, y = 2n + 1 \) for some \( m, n \in \text{integers} \)

\[ \rightarrow xy = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2(2mn+m+n) + 1 \]

\[ \rightarrow \text{since } 2mn + m + n \text{ is an integer, } xy \text{ is odd.} \]
(⇒) if \( xy \) is odd then \( x \) and \( y \) are odd.

**By contraposition:** if \( x \) is not odd or \( y \) is not odd, then \( xy \) is not odd

i.e. if \( x \) even or \( y \) even, then \( xy \) even

**case1**  \( x \) even, \( y \) odd: Let \( x = 2m, y = 2n+1 \)

\[ xy = 2(2mn + m), \text{ which is even } \therefore 2mn+m \in \mathbb{Z} \]

**case2**  \( x \) odd, \( y \) even: similar to case1.

**case3**  \( x \) even, \( y \) even: Let \( x = 2m, y = 2n \)

\[ xy = 2(2mn), \text{ which is even } \therefore 2mn \in \mathbb{Z} \]

---

**Proof by Contradiction**

- **Prove/Show** \( P \rightarrow Q \) **by contradiction method**
- **Is equivalent to show that** \( (P \land Q') \) **deduces to a contradiction** (violation of assumption)
- **Logical proof of contradiction:**
  - Let \( x' = (P \rightarrow Q)' = P \land Q' \), we assume \( x' \) and derive a contradiction \( y' \), i.e. \( x' \rightarrow y' \)
  - Where \( y' \) is false, i.e. \( y \) is true (or axiom)
  - By **modus tollens**: \( ((x' \rightarrow y') \land y) \rightarrow x \)
  - Therefore, conclude \( x = P \rightarrow Q \) is true
Proof by Contradiction:

Example: If a number added to itself gives itself, then the number is 0, i.e. if \( x + x = x \), then \( x = 0 \).

Proof:

Assume \( x + x = x \) and \( x \neq 0 \)

\[ \Rightarrow 2x = x \text{ and } x \neq 0 \]

\[ \Rightarrow 2 = 1, \text{ which is a contradiction} \]

\[ \therefore \text{ the assumption must be wrong} \]

\[ \therefore \text{ if } x + x = x, \text{ then } x = 0 \]

Example: Prove that if \( x^2 + 2x - 3 = 0 \), then \( x \neq 2 \).

1. by contradiction: \( P \land Q' \rightarrow \) Contradiction

   Suppose \( x^2 + 2x - 3 = 0 \) and \( x = 2 \),

   \[ \rightarrow 4 + 4 - 3 = 0 \text{ or } 5 = 0, \text{ which is a contradiction.} \]

2. by direct proof:

   if \( x^2 + 2x - 3 = 0 \rightarrow (x + 3)(x - 1) = 0 \)

   \[ \rightarrow x = -3 \text{ or } x = 1 \rightarrow x \neq 2 \]

3. by contraposition: \( Q' \rightarrow P' \)

   show that if \( x = 2 \), then \( x^2 + 2x - 3 \neq 0 \)

   \[ \rightarrow x^2 + 2x - 3 = 5 \neq 0 \]
In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

a) Proof by contradiction

b) Proof by contraposition

c) Direct proof
In class exercises

Show that if $3n+2$ is odd, then $n$ is odd.

a) Proof by contradiction
   \[ (P \land \overline{Q}) \rightarrow \text{contradiction} \]
   
   \[ 3n+2 \text{ is odd and } n \text{ is even} \]
   
   \[ 3n+2 \text{ is even (since even + 3 is odd, let } n \text{ be even}) \]
   
   \[ 3n+2 \text{ is even (sum of two even numbers is even, prove a proof!)} \]
   
   \[ \text{contradiction} \]

b) Proof by contraposition
   \[ \overline{Q} \rightarrow \overline{P} \]
   
   \[ n \text{ is even} \]
   
   \[ n \text{ is even} \]
   
   \[ 3n+2 = 6m+2 = 2(3m+1) \]
   
   \[ 3n+2 \text{ is even (sum of two odd numbers is even)} \]
   
   \[ 3n+2 \text{ is odd (contradiction)} \]

\[ \therefore \text{actually } x \text{ is odd.} \]

Mathematical Induction:

**Proof by induction:** to prove that the property $p(n)$ is true for all possible value of $n$

Idea: like playing the domino game.

Suppose dominos are placed correctly, then hitting the 1st domino, when it falls, we know the rest of them will also fall.

(∴ In general, when the $k$th one falls, it implies the $(k+1)$th falls. Since $k$ is any arbitrary number, ∴ actually every domino falls.)
Mathematical Induction (template):

**Step 1: (inductive base) or IB** is to show that \( p(n_0) \) is true. Choose an \( n_0 \in \mathbb{N} \) appropriate to the problem.

Note: \( n_0 \) is usually a small number 0 or 1 unless a range is specified.

**Step 2: (inductive hypothesis) or IH:**

Assume \( p(k) \) is true for any \( k \geq n_0 \).

**Step 3: (inductive step) or IS:**

Show that \( p(k) \rightarrow p(k + 1) \), for all natural numbers \( k \) such that \( k \geq n_0 \) (If \( p(k) \) is true then \( p(k+1) \) is also true; if a domino falls, the next domino also falls)

---

**Example 1:** show \( 1 + 3 + 5 + \ldots (2n-1) = n^2 \), for all \( n \geq 1 \)

**IB:** when \( n_0 = 1 \), \( \text{LHS} = 1 = 1^2 = \text{RHS} \)

**IH:** Assume \( 1 + 3 + 5 + \ldots (2k-1) = k^2 \) for \( n = k \geq n_0 \)

**IS:** Show \( 1 + 3 + 5 + \ldots (2k-1) + [2(k+1)-1] = (k+1)^2 \)

\[
\begin{align*}
\text{LHS} & = (k+1)^2 \\
& = \text{RHS} \\
\end{align*}
\]

\(: \text{LHS}' = 1 + 3 + 5 + \ldots (2k - 1) + (2k + 1) \quad = k^2 + 2k + 1 \quad \text{(by IH)}

\[
\begin{align*}
\text{LHS}' & = \text{RHS}' \\
\end{align*}
\]

\[
\begin{align*}
\text{Q.E.D.} & \quad \text{LHS} = \text{LHS}' = \text{RHS} = \text{RHS}'
\end{align*}
\]
Example 2: Show $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$, for all $n \geq 1$

IB: when $n_o = 1$, LHS = $1 = \frac{1(1+1)}{2} = \text{RHS}$

IH: Assume $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$ for $n = k \geq n_o = 1$

IS: Show $1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}$

\[ \begin{align*}
\text{LHS'} &= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} = \text{RHS'}
\end{align*} \]

by direct proof:

Let \( x = 1 + 2 + 3 + \ldots + k \)
\[ + \quad x = \quad \frac{k(k+1)}{2} + k - 1 + k - 2 + \ldots + 1 \]
\[ 2x = \frac{(k+1)(k+2) + \ldots + (k+1)}{k} = kx(k+1) \]
\[ \therefore \ x = \frac{k(k+1)}{2} \]
Example 3: Show \[ 1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1, \] for all \( n \geq 1 \)

- **IB**: when \( n_0 = 1 \), LHS = 1 + 2 = 3 = 2^2 - 1 = RHS

- **IH**: Assume \( 1 + 2 + 2^2 + ... + 2^k = 2^{k+1} - 1 \) for \( n=k \geq n_0 \)

- **IS**: Show \( 1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2^{k+2} - 1 \) (\( n=k+1 \))

\[ \therefore \text{LHS}' = 1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} \] (by IH)
\[ = 2 \times 2^{k+1} - 1 \]
\[ = 2^{k+2} - 1 \]
\[ = \text{RHS}' \]

Example 4: Show \( 2^{2n} - 1 \) is divisible by 3, for all \( n \geq 1 \)

- **IB**: when \( n_0 = 1 \), \( 2^2 - 1 = 3 \) \therefore divisible by 3

- **IH**: Assume \( 2^{2k} - 1 \) is divisible by 3

\[ \text{i.e. } 2^{2k} - 1 = 3m \text{ for some integer } m \text{ for } n=k \geq n_0 \]

- **IS**: show \( 2^{2(k+1)} - 1 \) is divisible by 3.

\[ 2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \times 2^{2k} - 1 \]
\[ = 2^2(3m+1) - 1 \] (\( \therefore 2^{2k} - 1 = 3m \)
\[ 2^{2k} = 3m + 1, \text{ by IH} \)
\[ = 12m + 3 \]
\[ = 3(4m + 1) \text{ where } 4m + 1 \text{ is an integer} \]

\[ \therefore \text{is divisible by 3} \]
Example 5 (Fibonacci number property) Show that:

\[ F_1 + F_3 + \ldots + F_{2n-1} = F_{2n} - 1, \text{ for all } n \geq 1. \]

Note: \( F_0 = F_1 = 1 \) and \( F_k = F_{k-1} + F_{k-2} \) for all \( k > 2 \)

IB: when \( n = 1 \), LHS = \( F_1 = 1 \), RHS = \( F_2 - 1 = 1 \)

IH: Assume \( F_1 + F_3 + \ldots + F_{2k-1} = F_{2k} - 1 \), for \( n = k \geq n_0 \)

IS: show \( F_1 + F_3 + \ldots + F_{2(k+1)-1} = F_{2(k+1)} - 1 \)

\[
\text{LHS'} = F_1 + F_3 + \ldots + F_{2k+1} = F_{2k} - 1 + F_{2k+1}
\]

(by Fibonacci number formula)

\[
= F_{2(k+1)} - 1
\]

(by IH)

\[
= \text{RHS'}
\]

Example 6 (Cardinality of a power set) : For any set \( X \) with \( |X| = n \), \( |P(X)| = 2^n \), for all \( n \geq 0 \).

IB: when \( n = 0 \), LHS = \( |P(\emptyset)| = 1 \), RHS = \( 2^0 = 1 \)

IH: Assume \( |X| = k \), \( |P(X)| = 2^k \) for \( n = k \geq 0 \)

IS: show \( |X| = k+1 \), \( |P(X)| = 2^{k+1} \)

Lemma: Let A be any set and let \( b \notin A \). If \( |P(A)| = m \), then \( |P(A \cup \{b\})| = 2m \).

Pick any element \( b \) from \( X \) in IS, \( |X - \{b\}| = k \)

\( \rightarrow |P(X - \{b\})| = 2^k \) (by IH)

\( \rightarrow |P(X)| = 2 \times 2^k \) (by Lemma) = \( 2^{k+1} \)
In class exercise

Use induction to prove that:
\[ 2^n < n! , \text{ for all } n \geq 4 \]
**Strong Form of Mathematical Induction (template):**

Step 1: *(inductive base) or IB* is to show that \( p(n_0) \) is true. Choose an \( n_0 \in \mathbb{N} \) appropriate to the problem.

Step 2: *(inductive hypothesis) or IH*:

Assume \( p(m) \) is true for all \( m : k \geq m \geq n_0 \)

Step 3: *(inductive step) or IS* is to show that \( p(k) \rightarrow p(k + 1) \), for all \( k \) such that \( k \geq n_0 \)

---

**Example:** Given \( a_0 = 0 \), \( a_1 = 2 \) and \( a_n = 4(a_{n-1} - a_{n-2}) \) for all \( n \geq 2 \). Show that: \( a_n = n \times 2^n \) for all \( n \)

IB: when \( n = 0 \), LHS = \( a_0 = 0 \), RHS = \( 0 \times 2^0 = 0 \)

\( n = 1 \), LHS = \( a_1 = 2 \), RHS = \( 1 \times 2^1 = 2 \)

\( n = 2 \), LHS = \( a_2 = 8 \), RHS = \( 2 \times 2^2 = 8 \)

IH: Assume \( a_k = k \times 2^k \) for all indices below \( k \)

IS: show \( a_{k+1} = (k+1) \times 2^{k+1} \)

LHS = \( 4(a_k - a_{k-1}) = 4(k \times 2^k - (k-1) \times 2^{k-1}) \) (by IH)

\[ = 4(2k \times 2^{k-1} - k \times 2^{k-1} + 2^{k-1}) = 4(k+1)(2^{k-1}) \]

\[ = (k+1) \times 2^{k+1} = \text{RHS} \]