More on proofs.

Part I: $A=B$.

Let A and B be sets. To say $A=B$ is to say

$A \subseteq B$ and $B \subseteq A$

which is to say

$x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$

which is to say

$$x \in A \Leftrightarrow x \in B.$$

So an $A=B$ proof is a kind of $P \Leftrightarrow Q$ proof.

Template:

Theorem.

$$A=B.$$

Proof.

1) Let $x \in A$. [Do stuff to get to:] Therefore, $x \in B$. So $A \subseteq B$.

2) Next, let $x \in B$. [Do stuff to get to:] Therefore, $x \in A$. So $B \subseteq A$.

So $B = A$. $\square$

Example:

Theorem.

For any sets X, Y, and Z,

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

<u>Proof.</u>

Let X, Y, and Z be sets.

1) Assume $x \in X \cap (Y \cup Z)$. Then, by defintion of intersection, $x \in X$ and $x \in Y \cup Z$. So by definition of union, $x \in Y$ or $x \in Z$.
We consider two cases:

(a) $x \in X$ and $x \in Y$. Then, by definition of intersection, $x \in X \cap Y$. But then, by defintion of union, $x \in (X \cap Y) \cup (X \cap Z)$.

(b) $x \in X$ and $x \in Z$. Then, by definition of intersection, $x \in X \cap Z$. But then, by defintion of union, $x \in (X \cap Y) \cup (X \cap Z)$.

In either case, $x \in (X \cap Y) \cup (X \cap Z)$. So $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)$.

2) Assume $x \in (X \cap Y) \cup (X \cap Z)$. Then, by definition of union, $x \in X \cap Y$ or $x \in X \cap Z$.
We consider two cases.
(a) $x \in X \cap Y$. Then $x \in X$ and $x \in Y$ by def'n of intersection. But $x \in Y \Rightarrow x \in Y \cup Z$, by def'n of union. So $x \in X$ and $x \in Y \cup Z$, so $x \in X \cap (Y \cup Z)$, by def'n of intersection.
(b) $x \in X \cap Z$. By the same argument as in (a), but with Y and Z switched, we see (since $Z \cap Y = Y \cap Z$) that $x \in X \cap (Y \cap Z)$.

In either case, we have $x \in X \cap (Y \cup Z)$.
So $(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cap Z)$.

Therefore, $(X \cap Y) \cup (X \cap Z) = X \cap (Y \cup Z)$. $\square$

Part II: Disproof; counterexamples.

To say a statement P is true is to say it's true no matter what. So to disprove P, it's enough to give a counterexample.

Examples:

1) Are all prime numbers odd?

No: 2 is prime but not odd.

2) Is the following true?

Proposition.
For all sets A, B, and C,
$$A - (B \cap C) = (A - B) \cap (A - C).$$

Solution:
This is false. Counterexample:

$A = \mathbb{Z}$, $B = 1 + 3\mathbb{Z}$; $C = 2 + 3\mathbb{Z}$.

Then $B \cap C = \emptyset$. (See p.4 of S-POP, or Fact 1.5, p. 30 of T-BOP, on the division algorithm.)

So $A - (B \cap C) = A = \mathbb{Z}$.

But

$$A - B = 3\mathbb{Z} \cup 2+3\mathbb{Z} \quad \text{and}$$
$$A - C = 3\mathbb{Z} \cup 1+3\mathbb{Z}, \text{ so}$$

$$(A-B) \cap (A-C) = 3\mathbb{Z} \neq A - (B \cap C).$$