Statements and Proofs.

I. The statement $P \Rightarrow Q$.

Read "if P then Q;" "P implies Q."

Meaning: whenever P is true, Q must follow.

Methods of proof:

A) Direct proof. Such a proof looks like this:

Theorem. $P \Rightarrow Q$.

Proof.

Assume P. [Now do what's necessary to conclude:] Therefore, Q.

So $P \Rightarrow Q$. $\square$

direct proof "template"

Example 1: prove

Theorem 1.

If n is an odd integer, then n^2-1 is divisible by 4.

Proof

Assume n is an odd integer: then $n = 2k+1$ for some integer k. So

$$n^2-1 = (2k+1)^2-1 = 4k^2+4k+1-1 = 4k^2+4k$$
$$= 4(k^2+k).$$

So n^2-1 is divisible by 4.

"divides"

So $n \in \mathbb{Z}$ is odd $\Rightarrow 4 \mid (n^2-1)$. $\square$

the set of integers

"not P" (the negation of P)

B) Contrapositive proof.

FACT: the statement $P \Rightarrow Q$ is always logically equivalent to its contrapositive $\sim Q \Rightarrow \sim P$.

So a contrapositive proof looks like:

contrapositive proof "template"

> Theorem. $P \Rightarrow Q$.
>
> Proof.
>
> Assume $\sim Q$. [Then do what's necessary to conclude:] Therefore, $\sim P$.
>
> So $P \Rightarrow Q$. $\square$

Example 2: prove

Theorem 2.

$n \in \mathbb{Z}$ is odd $\Rightarrow 4 \mid (n^2-1)$.

Proof.

Assume $4 \nmid (n^2-1)$. "does not divide"

Write

$n = 2k+r$ where $r=0$ (if n is even) or $r=1$ (if n is odd). Then

$$n^2-1 = (2k+r)^2-1 = 4k^2+4kr+r^2-1$$
$$= 4(k^2+kr)+(r^2-1).$$

Since $4 \nmid (n^2-1)$, we see that $r^2-1 \neq 0$, so $r \neq 1$, so $r=0$. So n is even (and therefore not odd).

So $n \in \mathbb{Z}$ is odd $\Rightarrow 4 \mid (n^2-1)$. $\square$

II) Proof by contradiction.

The idea: to prove a statement T, assume $\sim T$. Show this leads to an absurdity*. Then $\sim T$ must be false, so T is true.

*often, this will be of the form "V and $\sim V$," for some other statement V.

Like this:

<u>Theorem</u>. T.
<u>Proof</u>
Assume ~T. [Then do stuff to conclude:]
Therefore, V. [Then do more stuff to conclude:]
Therefore, ~V. Contradiction.

Therefore, T. □

Contradiction proof "template."

Example 3: prove

<u>Theorem 3.</u>

(by definition, these are positive.)

There are infinitely many prime numbers.
(the statement T)

(this is ~T)

<u>Proof</u>. Assume there are only finitely many prime numbers:
call them $p_1, p_2, p_3, \ldots, p_k$.
Define
$$M = p_1 p_2 p_3 \cdots p_k + 1,$$
and let p be any prime divisor of M.
Then:
(a) The only primes are $p_1, p_2, \ldots, p_k$, so p equals one of these primes, so p divides their product is
$$N = p_1 p_2 \cdots p_k.$$
Since p divides M and N, p divides their difference, so $p \mid (M-N)$.

(b) By the definitions of M and N, $M-N=1$, which is not divisible by any prime, so $p \nmid (M-N)$.

So $p \mid (M-N)$ and $p \nmid (M-N)$.
Contradiction. So $\exists$ infinitely many primes. $\square$