Introduction to Proofs.

Proving Theorem

Many theorems have the form:

$$\forall x\ (P(x) \rightarrow Q(x))$$

To prove them, we can show that $P(c) \rightarrow Q(c)$ for an arbitrary element c of the domain, and apply the rule of universal generalization.

So, we must prove something of the form: $p \rightarrow q$.

Proving Conditional Statements: $p \rightarrow q$

Trivial Proof: If we know q is true, then $p \rightarrow q$ is true as well.

„If it's raining, then $1=1$."

Vacuous Proof: If we know p is false, then $p \rightarrow q$ is true as well.

„If I am both poor and rich, then $2+2=5$."

Proving Conditional Statements: $p \rightarrow q$

Direct Proof: Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

$p(n) \rightarrow q(n)$

Example: Prove that if $\overbrace{n \text{ is an odd integer}}^{p(n)}$, then $\underbrace{n^2 \text{ is odd}}_{q(n)}$.

$n = 2k+1$

Squaring both sides of the equation, we get:

$$\boxed{n^2} = \underbrace{(2k+1)^2 = \underbrace{4k^2+4k}+1 = 2(2k^2+2k)}+1 = \boxed{2r+1}$$

where $r = \underbrace{2k^2+2k}$, an integer. Therefore n^2 is odd integer.

$a+b=(2r+1)+(2s+1)=2r+2s+2$

$a=2r+1$

$$= 2\underbrace{(r+s+1)}_{k}$$

$b=2s+1$

$$=2k$$

Proving Conditional Statements: $p \to q$

Definition: The real number r is rational if there exist integers a and b where $b \neq 0$ such that $r = a/b$

Example: Prove that the sum of two rational numbers is rational.

$r = \frac{a}{b}$ where $b \neq 0$

$$r+s = \frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} = \frac{u}{v}, \text{ where } b, d \neq 0$$

$u = ad+bc$ and $v = bd$ are all integers. So the sum is also rational.

Proof by Contraposition: Assume $\neg q$ and then show $\neg p$ is true. This is sometimes called an indirect proof method. If we give a direct proof of $\neg q \to \neg p$ then we have a proof of $p \to q$.

Example: Prove that if $\underbrace{3n+2 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is odd for any integer } n}_{q}$.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Then

$$3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) = 2j$$

for $j = 3k+1$. Therefore we have $\underbrace{3n+2 \text{ is even}}_{\neg p}$