Proof Methods

We assume that we have a proof system that has **axioms** and **inference rules**. A proof $p, q \vdash r$ means that we can establish r from the assumptions p, q using the axioms and the rules of the system. Below are some proof techniques.

1. Direct Proof

In a direct proof, the conclusion is established by logically combining the axioms, definitions, and earlier theorems.

Note In general, the direct proofs use the transitivity of $\vdash$. In the math books these proofs are listed as trivial, obvious, or exercise.

Example: Show that the sum of two even numbers is even.
Proof: Let m and n be even. From the definition of the even numbers, there are integers p and q such that $m = 2p$ and $n = 2q$. Then

$m + n = 2p + 2q$ by assumption
$= 2(p + q)$ $\cdot$ distributes over $+$

Since $m+n = 2(p+q)$, $m+n$ is even by the definition of an even number.

2. Mathematical Induction

In general the induction works on a set of term defined inductively.
For example, the induction on the whole numbers works as follows:
The property P holds for all whole numbers n if
1. $P(0)$ is true, and
2. for all n, if $P(n)$ is true, so is $P(n + 1)$.

This method was derived from the inductive definition of the whole numbers:
1. 0 is a whole number
2. if n is a natural number, so is $n + 1$
3. nothing else is a whole number

Example: Show that $n^3 - n$ is divisible by 3.
Proof:
1. Basis: $n = 0$. Then $n^3 - n = 0$ and 0 is divisible by 3 because $0 = 3 \cdot 0$.

2. Inductive step: assume that $n^3 - n$ is divisible by 3 and we have to show that $(n+1)^3 - (n+1)$ is divisible by 3. Since $n^3 - n$ is divisible by 3, there is a number m such that $n^3 - n = 3m$. Then,

$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1$ by the binomial formula

$= (n^3 - n) + 3(n^2 + n)$ by grouping the terms

$= 3m + 3(n^2 + n)$ because $n^3 - n$ is divisible by 3

$= 3(m + n^2 + n)$ by distributivity

The last expression is divisible by 3, so $(n+1)^3 - (n+1)$ is divisible by 3.

Notes 1. The induction methods are verification methods.

2. The induction axiom $\forall P((P(0) \wedge \forall n(P(n) \longrightarrow P(n+1))) \longrightarrow \forall n P(n))$ is a second order axiom.

3. Proof by Contradiction

We prove $p \vdash q$ by showing that $\{p, \neg q\}$ is inconsistent.

Example: Show that the set of prime numbers is infinite.
Proof: Assume, on the contrary, that the set if finite. Then let $p_1, p_2, \ldots, p_n$ be the set of prime numbers. Let $m = p_1 \cdot p_2 \ldots \cdot p_n + 1$. Then, m must be divisible by a prime (that prime could be itself). But m is not divisible by any of the primes $p_1, p_2, \ldots, p_n$. This contradicts the fact that the set of primes numbers is finite.

Note This is one of the most popular method of proof in mathematics, and the most popular with the beginners.

4. Proof by Exhaustion

We divide the conclusion into a finite number of cases and prove each case separately.

This corresponds to the rule if $p \vdash r$ and $q \vdash r$, then $p \vee q \vdash r$.

Example: Show that the square of any integer is divisible by 4 or has remainder 1 when divided by 4.

Proof: Let n be an integer.

Case 1: n is even. Then $n = 2m$ and $n^2 = 4m^2$, so n^2 is divisible by 4.

Case 2: n is odd. Then $n = 2m + 1$ and $n^2 = 4m^2 + 4m + 1$. Since $4m^2 + 4m + 1 = 4(m^2 + m) + 1$, n^2 has remainder 1 when divided by 4.

Note This is the proof by cases method.

5. Combinatorial Proof

Here we count the items of a set in two different ways.

Example: Let us show that in a full binary tree the number of leaves is equal to 1 plus the number of branches. We recall that in a full binary tree each branch has 2 children.

Proof: Let n be the number of leaves and m be the number of branches. The tree has $m+n$ nodes. Now every node except the root is the child of a branch. Different branches produce different children, so the number of nodes in the tree is $2m + 1$, 1 being the root. From the equality $m + n = 2m + 1$ we get $n = m + 1$.

Note: The combinatorial proofs allow us to discover new identities, but they may be tricky to find.

6. Proof by Transposition

We prove $p \vdash q$ by showing $\neg q \vdash \neg p$. This method utilizes the axiom $\vdash (p \longrightarrow q) \longleftrightarrow (\neg q \longrightarrow \neg p)$

Example: Let us show that whenever n^2 is even, so is n.
Proof: We use the transposition and show that if n is not even, then n^2 is not even. So, let n ne odd, i.e. $n = 2m + 1$. then $n^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$. So, n^2 is odd.

7. Proof by Infinite Descent

We show that for every whole number that has property P, there is a smaller whole number that also satisfies P.

Example: Show that $\sqrt{2}$ is irrational.

Proof: Assume that $\sqrt{2}$ is rational, i.e. $\sqrt{2} = m/n$ for some numbers whole numbers m and n.

We square both sides of the equation and get $m^2 = 2n^2$. 2 must divide m^2, so it must divide m. Hence $m = 2p$. We replace m by $2p$ in $m^2 = 2n^2$ and get $2p^2 = n^2$. So, 2 must divide n, i.e. $n = 2q$.

We replace m and n in $m^2 = 2n^2$ and, after simplification, we have $p^2 = 2n^2$, i.e. $\sqrt{2} = p/q$ and $p < m$.

Note This is a contradiction method that uses the fact that the set of whole number is noetherian, i.e. there in no infinitely descending chain. However, it used so often in logic and algebra that it has its own category.

General Note There are some other techniques, like the use of invariants, probabilistic proofs, or constructive proofs that are used in the existence proofs. We will not discuss them here.