Part I: basic techniques

1. **Direct proof**.

   The implication "$p \to q$" can be proven by showing that if p is true, then q must also be true. A proof of this kind is called a *direct proof*.

   Examples: (1) Prove that "If n is odd, then n^2 is odd"

   (2) Most of proofs we have seen in Chapters 1-3 use this techniuqe.

2. **Proof by contraposition**.

   Since the implication "$p \to q$" is logically equivalent to its contrapositive $\neg q \to \neg p$, i.e.,

   $$(p \to q) \equiv (\neg q \to \neg p)$$

   (verify by using the truth table!), the implication $p \to q$ can be proved by showing that its contrapositive $\neg q \to \neg p$ is true. This related implication is usually proved directly. An argument of this type is called a *proof by contraposition* or an *indirect proof*.

   Examples: (1) Prove that "if $3n + 2$ is odd, then n is odd".

   (2) Prove that if $n = ab$, where a and b are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

3. **Proof by contradiction**.

   By assuming that the hypothesis p is true and that the conclusion q is false, then using p and $\neg q$ as well as other axioms, definitions, and previously derived theorems, derives a contradiction. An argument of this type is called a *proof by contradiction*.

   Proof by contradiction can be justified by logical equivalence

   $$(p \to q) \equiv (p \wedge \neg q \to r \wedge \neg r)$$

   Examples: (1) Prove that $\sqrt{2}$ is irrational

   (2) Prove that for all real numbers x and y, if $x + y \ge 2$, then either $x \ge 1$ or $y \ge 1$.

4. **Equivalence proof** (or "if-and-only-if proof", necessary-and-sufficient proof")

   To prove $p \leftrightarrow q$, we use the the logical equivalence

   $$(p \leftrightarrow q) \equiv [(p \to q) \wedge (q \to p)]$$

   That is, the proposition " p if and only if q" can be proved if both the implication "if p, then q" and "if q, then p" are proved.

   Example: Prove that the integer n is odd if and only if n^2 is odd.

5. **Constructive existence proof**

   For example: Prove the quantification $\forall n\ \exists x\ (x + i$ is composite for $i = 1, 2, ..., n)$. That is, there are n consecutive composite positive integers for every positive integers n.[1]

6. **Proof by counterexample**.

   We can prove by counterexample to show that "$\forall x\ P(x)$ is false.

   Example: Show that the assertion "All primes are odd" is false.

[1] A positive integer that is greater than 1 and is not prime is called *composite*.

Part II

1. The proof technique "**Mathematical Induction**" is the most widely used to prove propositions of the form $\forall n\ P(n)$, where $n \in \mathbf{N} =$ the set of positive integers.

2. A proof by mathematical induction consists of two steps:

   (A) *Basis step*: show the proposition $P(1)$ is true.

   (B) *Inductive step*: show the implication $P(k) \to P(k+1)$ is true for every positive integer k, under the *inductive hypothesis* that $P(k)$ is true.

   When we complete both steps of a proof by mathematical induction, we have shown that $\forall n\ P(n)$ is true.

3. Expressed as propositional logic, mathematical induction proof technique can be stated as

$$\left[\underline{P(1)} \wedge \underline{\forall k(P(k) \to P(k+1))}\right] \to \forall n P(n)$$

4. Examples of proofs by Mathematical Induction:

   (a) Prove that the sum of the first n odd positive integers is n^2, i.e.,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

   (b) Show that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.

   (c) Show that the sum of geometric progression

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r-1}, \qquad \text{when} \quad r \neq 1.$$

   (d) Prove the inequality $n < 2^n$ for all positive integer n.

   (e) Prove that $2^n < n!$ for every positive integer n with $n \geq 4$.

   (f) Prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer.

   (g) Show that if S is a finite set with n elements, then S has 2^n subsets.

5. Why mathematical induction is a valid proof technique? (see the class website)

6. There is another form of mathematical induction, referred to as "the second principle of mathematical induction" or "strong induction". It can be summarize by the following two steps:

   (a) Basis step: the proposition $P(1)$ is shown to be true

   (b) Inductive step: It is shown that

$$[P(1) \wedge P(2) \wedge \cdots \wedge P(n)] \to P(n+1)$$

   is true for every positive integer n.

7. Example: Show that if n is an integer greater than 1, then n can be written as the product of primes.