1.7 & 1.8

Methods of Proof

A **theorem** is a statement that can be shown to be true. We demonstrate that a theorem is true through a sequence of statements that form an argument, called **proof**. To construct proofs, methods are needed to derive new statements from old ones. The statements used in a proof can include **axioms** or **postulates**, which are underlying assumptions about mathematical structures, the hypotheses of the theorem and previously proved theorems. The **rules of inference**, which are the means used to draw conclusions from other assertions, tie together the steps of a proof. In this module, we discuss the various methods that are commonly used to prove theorems.
The methods of proof discussed in this module are not only important for their use to prove mathematical theorems but are also important for their many applications in computer science. These applications include verifying that computer programs are correct, establishing that operating systems are secure, making inferences in the area of artificial intelligence and so on.

We proved several theorems. We now examine the methodology of constructing proofs and describe how different types of statements are proved.

Vacuous Proof

Suppose that the hypothesis of the conditional $h \longrightarrow c$ is false. Then $h \longrightarrow c$ is true regardless of whether c is true or false. Thus, if the hypothesis h can be shown to be false, then the theorem $h \longrightarrow c$ is true. Such a proof is called a **Vacuous Proof**. (Vacuous proofs are rare and are necessary to handle the special cases).

Example: If $\mathbf{1} = \mathbf{2}$ then $\mathbf{3} = \mathbf{4}$
(A conditional with a false hypothesis is guaranteed to be true)

Example: Let $P(n)$ be the proposition "If n is an integer and $n > 1$, then $n^2 > n$". Show that the proposition $P(0)$ is true.

Solution: We have $P(0)$: If $0 > 1$,then $0^2 > 0$. Since the hypothesis is false, $P(0)$ is true by vacuous proof.

Trivial proof

Suppose that the conclusion c of the conditional $h \longrightarrow c$ is true. Then $h \longrightarrow c$ is true irrespective of the truth value of h. If the conclusion c can be shown to be true, then the theorem $h \longrightarrow c$ is true. Such a proof is called **trivial proof.**

Trivial proofs are often important to prove special cases of theorems and in mathematical induction.

Example 1:
Let $P(n)$ be the proposition "if a and b are positive integers with $a \geq b$ and n is an integer, then $a^n \geq b^n$. Show that the proposition $P(0)$ is true.

Solution: We have $P(0)$: If $a \geq b$, then $a^0 \geq b^0$. Since $a^0 = b^0 = 1$, the conclusion of $P(0)$ is true. Thus $P(0)$ is true trivially. Note that in this example of trivial proof we have not used the premise $a \geq b$.

Example 2:
Let $P(n)$: If x is a positive real number and n is any nonnegative integer, then $(1 + x)^n \geq 1 + nx$. Show that the proposition $P(0)$ is true.

Solution: We have $P(0)$:If x is a positive real number then $(1 + x)^0 \geq 1 + 0.x$. Since $(1 + x)^0 = 1 \geq 1 + 0.x$, the conclusion $P(0)$ is true. Thus $P(0)$ is true trivially. In this trivial proof, we have not used the premise $x > 0$.
Many theorems are conditionals $h_1 \wedge h_2 \wedge \ldots \wedge h_m \longrightarrow c$ .Proving such a theorem means verifying that the proposition $h_1 \wedge h_2 \wedge \ldots \wedge h_m \longrightarrow c$ is a tautology ($i.e.$, $h_1 \wedge h_2 \wedge \ldots \wedge h_m \Longrightarrow c$).Therefore the techniques for proving implications are important.

Direct Proof

The conditional $h \longrightarrow c$ can be proved by showing that if h is true, then c must also be true. (This shows that the combination h true and c false never occurs). A proof of this kind is called a **direct proof.**

In the direct proof of the theorem $h \longrightarrow c$, assume the given hypotheses in h are true .Using the laws of logic and previously known facts together with rules of inference prove the derived conclusion c as the final step of a chain of tautological implications: $h \Longrightarrow c_1,\ c_1 \Longrightarrow c_2, \ldots\ c_m \Longrightarrow c$. Then by repeated application of the hypothetical syllogism, it follows that $h \Longrightarrow c$.

Example 3:
Prove the following by the direct method of proof. The product of any two odd integers is an odd integer.

Solution: Let x and y be any two odd integers. Then it is known that there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$xy = (2m + 1)(2n + 1) = 2(2mn + m + n) + 1 = 2k + 1$$

where $k = 2mn + m + n$ is an integer, since m and n are integers. This shows that xy is an odd integer.

Note: We can rewrite the proof as a chain of tautological implications.

Indirect Proof

Direct proofs lead from the hypothesis h of a theorem to the conclusion c. They begin with the premises, continue with a sequence of logical deductions and end with the conclusion. Proofs that do not start with the hypothesis and end with conclusion are called ***Indirect Proofs***. There are two useful types of indirect proofs. They are (1) **Proof by contraposition** and (2) **Proof by contradiction**.

Proof by contraposition: This proof makes use of the fact that the conditional statement $h \longrightarrow c$ is equivalent to its contrapositive, $\sim c \longrightarrow \sim h$. That is, $h \longrightarrow c$ can be proved by showing its contrapositive $\sim c \longrightarrow \sim h$ is true. Therefore, we take $\sim c$ as hypothesis and using axioms, definitions and previously proven theorems, together with rules of inference we show that $\sim h$ follows. We normally look for a proof by contraposition when we cannot find a direct proof.

Example 4: Prove that if n is an integer and $3n + 2$ *i*s odd, then n is odd.

Solution: (To construct a direct proof, we assume that $3n + 2$ is an odd integer, i.e., $3n + 2 = 2k + 1$ for some integer k. We see that $3n = 2k - 1$ and a direct way to conclude that n is odd is not in sight. Therefore we look for a proof by contraposition).

Assume the negation of the conclusion. That is n is even. Therefore, $n = 2k$ for some integer k. Now $3n + 2 = 2(3k + 1)$. This shows that $3n + 2$ is even. That is, $3n + 2$ is not odd which is the negation of the hypothesis. Thus by the proof by contraposition, the given result is proved.

Proof by Contradiction: Suppose we want to prove that a proposition p is true. Further, suppose that we can find a contradiction q such that $\sim p \longrightarrow q$ is true. Since q is false, $\sim p$ is false. This means p is true.
Because the proposition $r \wedge \sim r$ is a contradiction whenever r is a proposition, we can prove p is true if we can show that $\sim p \longrightarrow (r \wedge \sim r)$ is true for some proposition r. Proofs of this type are called ***proofs by contradiction***. Since it does not prove a result directly, it is another type of indirect proof.

Example 5: Prove by contradiction: There is no largest prime number. That is, there are infinitely many prime numbers.

Solution: Notice that the theorem has no hypothesis. Suppose that the given conclusion is false; that is, there is a largest prime number say p. Therefore, we have the prime numbers $2,3,5,7, \ldots, p$. Assume that there are k such primes $p_1, p_2, p_3, \ldots, p_k$ i.e., $p_1 = 2\ , p_2 = 3, \ldots, p_k = p$.

Let $n = (2 \cdot 3 \cdot 5 \ldots p) + 1$. Clearly, $n > p$ and n is not divisible by any of these prime numbers $2,3,5, \ldots, p$. Who is n? n is either prime or n is composite. If n is prime then we have more than k primes. If n is composite then n is divisible by a prime, $q \neq p_i,\ 1 \leq i \leq k$. Thus we have more than k prime,a contradiction. Therefore, the result follows.

Proof by Contradiction to propositions $h \to c$:
Proof by contradiction can be used to prove conditional propositions $h \longrightarrow c$. In such proofs, we assume that the hypotheses h are true but the conclusion c is false. Then argue logically and reach a contradiction F_0.

Example 6: Give a proof by contradiction of the theorem: If $3n + 2$ is odd, then n is odd.

Solution: Let $h : 3n + 2$ is odd, $c : n$ is odd. Assume that h is true but c is false. Therefore, h and $\sim c$ is true. That is $3n + 2$ is odd and n is not odd. It follows that n is even and there by $3n + 2$ is even. Thus, $\sim h$ is true. This shows that h and $\sim h$ are true. This is a contradiction. By the proof by contradiction the theorem is proved.

Proof of Equivalence

To prove a theorem that is a biconditional proposition, $i.e.$, a proposition of the form $p \leftrightarrow q$, we show that $p \longrightarrow q$ and $q \longrightarrow p$ are both true. The validity is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow \big((p \longrightarrow q) \wedge (q \longrightarrow p)\big)$$

Example 7: Let n be a positive integer. Then n is odd if and only if n^2 is odd.

Solution: Let p: n is odd; q: n^2 is odd. This theorem is of the form: p if and only if q. To prove the theorem we show that $p \longrightarrow q$ is true and $q \longrightarrow p$ is true.
We use a direct proof to show that $p \to q$ is true .Suppose p is true .Then n is odd and so $n = 2k + 1$ for some integer k. Therefore, $n^2 = 2(2k^2 + 2k) + 1$.This shows that n^2 is also odd. Thus, $p \longrightarrow q$ is true.
To prove $q \longrightarrow p$ is true, we prove its contraposition. Assume that $\sim p$ is true. Therefore, n is even .Thus, $n = 2k$ for some integer k. Then $n^2 = 2(2k^2)$ is also even and $\sim q$ is true .This proves $\sim p \longrightarrow \sim q$ is true. By proof by contraposition $q \longrightarrow p$ is true. Thus, $p \leftrightarrow q$ is true.

Note: Some times a theorem states that several propositions $p_1, p_2, \dots, p_n$ are equivalent. This can be written as $p_1 \Leftrightarrow p_2 \Leftrightarrow p_3 \Leftrightarrow \cdots \Leftrightarrow p_n$ and it

states that all n propositions have the same truth values, and that consequently, $p_i \Leftrightarrow p_j$ for i and j with $1 \leq i, j \leq n$. One way to prove that these are mutually equivalent is to use the tautology

$$(p_1 \Leftrightarrow p_2 \Leftrightarrow p_3 \Leftrightarrow \cdots \Leftrightarrow p_n) \longrightarrow \big((p_1 \longrightarrow p_2) \wedge (p_2 \longrightarrow p_3) \wedge \ldots \wedge (p_n \longrightarrow p_1)\big)$$

This shows that if the conditional propositions $p_1 \longrightarrow p_2,\ p_2 \longrightarrow p_3,$ $\ldots, p_{n-1} \longrightarrow p_n, p_n \longrightarrow p_1$ are true, then the propositions $p_1, p_2, \ldots, p_n$ are all equivalent.

Example 8: Show that the statements about the integer n

p_1: n is even,

p_2: $n-1$ is odd,

p_3: n^2 is even

are equivalent.

Solution: We will show that these statements are equivalent by showing that the conditionals $p_1 \longrightarrow p_2,\ p_2 \longrightarrow p_3, p_3 \longrightarrow p_1$ are true.

We use a direct proof to show that $p_1 \longrightarrow p_2$ is true. Suppose n is even. Then $n = 2k$ for some integer k and $n - 1 = 2(k-1) + 1$. This shows that $n - 1$ is odd. Thus, $p_1 \longrightarrow p_2$ is true.

We use a direct proof to show $p_2 \longrightarrow p_3$ is true. Suppose that $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some integer k. Then $n = 2k + 2$ and $n^2 = 2[2(k+1)^2]$. This shows that n^2 is even. Thus, $p_2 \longrightarrow p_3$ is even.
To prove $p_3 \longrightarrow p_1$, we prove by contraposition. That is, if n is not even, then n^2 is not even. That is, if n is odd then n^2 is odd. This is true. (We have already proved). Thus, $p_3 \longrightarrow p_1$ is true. Therefore p_1, p_2, p_3 are equivalent.

Proofs by Cases

It is a method of proof that can be used to prove a theorem by considering different cases separately. To prove a conditional statement of the form

$$(h_1 \vee h_2 \vee \ldots \vee h_m) \longrightarrow c$$

the equivalence $(h_1 \vee h_2 \vee \ldots \vee h_m) \longrightarrow c \Leftrightarrow (h_1 \longrightarrow c) \wedge (h_2 \longrightarrow c) \wedge \ldots \wedge (h_m \longrightarrow c)$ can be used as a rule of inference.
This shows that the conditional statement with a hypothesis made up of a disjunction of the propositions $h_1, h_2, \ldots, h_m$ can be proved by proving each of the n conditional statements $h_i \longrightarrow c$, $1 \leq i \leq n$, is true individually. Such an argument is called a **proof by cases**.

Note: Some times to prove a conditional statement $h \longrightarrow c$ is true, it is convenient to use a disjunction $h_1 \vee h_2 \vee \ldots \vee h_m$ instead of h if h is equivalent $h_1 \vee h_2 \vee \ldots \vee h_m$.

Example 9: Prove that if n is an integer, then $n^2 \geq n$.

Solution: We prove the conclusion by considering three cases, when $n = 0, n \geq 1$ and $n \leq -1$.

Case (i): When $n = 0$, we have $n^2 \geq 0$, since $0^2 \geq 0$. The conclusion is true in this case.

Case (ii): When $n \geq 1$, we have $n^2 = n \cdot n \geq n \cdot 1 = n$. The conclusion is true in this case.

Case (iii): When $n \leq -1$, we have $n^2 \geq 0$.Thus $n^2 \geq n$. The conclusion is true in this case also.

Thus, the conclusion is true in all the three cases. Therefore $n^2 \geq n$, if n is an integer (by proof by cases).

Note: A proof by cases is considered if it is not possible to consider all cases of a proof at the same time.

Exhaustive proof: Some theorems can be proved by examining a relatively small number of particular cases. Such proofs are called **exhaustive proofs,** because these proofs exhaust all possibilities.

Note: An exhaustive proof is a special type of proof by cases where each case is a single particular case.

Example 10: Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: We use a proof by exhaustion. We need to check whether the inequality $(n+1)^3 \geq 3^n$ is true for $n = 1,2,3,4$.
For $n = 1$, we have $(n+1)^3 = 8 \geq 3^1 = 3^n$; for $n = 2$, we have $(n+1)^3 = 27 \geq 3^2 = 3^n$; finally for $n = 4$, we have $(n+1)^3 = 125 \geq 3^4 = 3^n$.
In each case the inequality is true. Thus, the result is true.

Note: We can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement.

Predicate

Declarative sentences involving variables such as $x > 3$; $x = y + 3$; $x + y = z$ and *computer x is functioning properly* are often found in mathematical assertions, in computer programs and in system specifications. These are neither true nor false when the values of the variables are not specified.
The declarative sentence "*x is greater than 3*" has two parts. The first part, the variable x, is the subject of the sentence. The second part, "is greater than", is the property of the subject and it is called the **predicate**. That is, the part of a declarative sentence that attributes a property to the subject is called the **predicate**. We denote the sentence "x is greater than 3" by $P(x)$ where P denotes the predicate "is greater than 3" and x is the variable. $P(x)$ is also said to be the value of the **propositional function P** at x. Once a value is assigned to x, the $P(x)$ becomes a proposition and has a truth value.
A declarative sentence of the form $P(x_1, x_2, \dots, x_n)$ is the value of the proposition function P at the n-tuple $(x_1, x_2, \dots, x_n)$ and P is also called an ***n*-ary predicate** or ***n*-place predicate**.
Propositional functions occur in computer programs.

Quantifiers

Quantification is a way to create a proposition from a proposition function and it expresses the extent to which a predicate is true over a range of elements. We deal with two types of quantification here: (i) *Universal quantification*, which says that a predicate is true for every element under consideration and (ii) *existential quantification*, which says that there is one or more elements under consideration for which the predicate is true. The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

The Universal quantifier: Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called **domain of discourse** or **universe of discourse** or often just referred as the **domain**. The universal quantification of $P(x)$ for a particular domain is the proposition that asserts that $P(x)$ is true for all x in this domain.

The universal quantification of $P(x)$ is the statement "$P(x)$ *for all* x *in the domain*". The notation $\forall x\ P(x)$ (read as for all $x\ \ P(x)$) denotes universal quantification of $P(x)$. Here $\forall$ is called **universal quantifier**. An element for which $P(x)$ is false is called a **counter example**.

Example 11: Let $P(x)$: $x + 1 > x$ and the domain is the set of real numbers. Since $P(x)$ is true for all real numbers x, the quantification is $\forall x\ P(x)$.

The existential quantifier: Many mathematical statements assert that there is an element with a certain property. Such statements are expressed using existential quantification .With existential quantification, we form a proposition that is true if and only if $P(x)$ is true for at least one value of x in the domain.

The *existential quantification* of $P(x)$ is the proposition "*There exists an element* x *in the domain such that* $P(x)$".The notation $\exists x\ P(x)$ (read as there exists $x\ P(x)$) is used for the existential quantification of $P(x)$. Here $\exists$ is called the **existential quantifier**.

Existence Proofs

Many theorems are assertions that elements of particular type exist. A theorem of this type is a proposition of the form $\exists x\, P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x\, P(x)$ is called an **existence proof**.

There are two kinds of existence proofs :(i) **the constructive existence proof** and (ii) **nonconstructive existence proof**.

Constructive existence proof: In this method of proof we find an element a such that $P(a)$ is true.

Example 12: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution: All that we need is to produce an element a that has the required properties. After considerable trying we find that

$$a = 1729 \text{ , since } 1729 = 1^3 + 12^3 = 9^3 + 10^3$$

Thus, the assertion is shown.

Nonconstructive existence proof: In this method we do not find an element a such that $P(a)$ is true but rather prove that $\exists x\, P(x)$ is true in some other way.

A method of a nonconstructive existence proof is to use a proof by contradiction and that the negation of the existential quantification leads to a contradiction.

Example 13: Show that there exist irrational numbers x and y such that x^y is rational.

Solution: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ such that x^y is rational. On the other hand, if $\sqrt{2}^{\sqrt{2}}$ is irrational then we have irrational numbers $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ such that $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$, a rational number.

Note that we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these pairs works.

Counter Example

To show that a statement of the form $\forall x P(x)$ is false, we need to find a *counter example*, i.e., an example x for which $P(x)$ is false.

If statement of the form $\forall x P(x)$, resisted all proof attempts and we believe it to be false then we look for a counter example.

Example 14: Is the statement "Every positive integer is the sum of the squares of three integers" true ?

Solution: We try to find a counter example. We observe the following:

$1 = 0^2 + 0^2 + 1$; $\quad 2 = 0^2 + 1^2 + 1^2$; $\quad 3 = 1^2 + 1^2 + 1^2$;

$4 = 0^2 + 0^2 + 2^2$; $\quad 5 = 0^2 + 1^2 + 2^2$; $\quad 6 = 1^2 + 1^2 + 2^2$;

Can we write 7 as the sum of three squares? We note that the only possible squares not exceeding 7 are $0, 1$ and 4 and no three of which add up to 7. Thus 7 is a counter example. Therefore, the statement is false.

Conjectures and Open Problems

A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence or the intuition (of an expert). When a proof of a conjecture is found, the conjecture becomes a theorem. Many conjectures are shown to be false.

Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are disproved, some are difficult to prove and others have remained open problems for many years.

It would be useful to have a function $f(n)$ such that $f(n)$ is prime for all the integers n. If we had such a function, we could find large primes for use of cryptography and other applications.
Number theorists dream of finding formulas that generate prime numbers. One such formula was given as a conjecture by the Swiss mathematician Leonard Euler, but his conjecture was disproved. The following is his conjecture.

"The formula $E(n) = n^2 - n + 41$ generates a prime number for every positive integer n"

Example 15: Is the statement "The formula $\boldsymbol{E(n) = n^2 - n + 41}$ generates a prime for every positive integer $\boldsymbol{n}$" true ?

Solution: Notice that it yields a prime for $n = 1, 2, 3, 4, \ldots, 40$ but for $n = 41$, we see that $E(41) = 41^2 - 41 + 41 = 41^2$ is not a prime. Therefore, 41 is a counter example and it disproves the claim.

Example 16: Fermat conjectured (in 1640) that numbers of the form $f(n) = 2^{2^n} + 1$ are prime numbers for all nonnegative integers n. Note that $f(0) = 3, f(1) = 5,\ f(2) = 17, f(3) = 257$ and $f(4) = 65,537$ are all primes. Euler established the falsity of Fermat's conjecture by producing a counter example. He showed that $f(5) = 2^{2^5} + 1 = 641 \times 67{,}00{,}417$, is a composite number.

Prime numbers of the form $2^{2^n} + 1$ are called ***Fermat primes***.

Many problems about primes still await ultimate resolution. A few of the most accessible and better known of these problems are given below:

Goldbach's Conjecture: The conjecture "Every even integer $n, n > 2$ is the sum of two primes" is known as Goldbach's conjecture.

We can check this conjecture for small even numbers. It was verified by hand calculations for numbers up to the millions prior to the advent of computers. The conjecture has been checked with computers for all even integers up to 2×10^{17} (This information is up to the year 2006).

Note: Although no proof of this conjecture has been found, most mathematicians believe it is true.

The Twin Prime Conjecture: Twin primes are primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19; $4{,}967$ and $4{,}969$ and so on. The twin prime conjecture asserts that: *there are infinitely many twin primes*. The world's record for twin primes, as early 2006, consists of the numbers

$$1{,}68{,}69{,}98{,}73{,}39{,}975 \times 2^{1{,}71{,}960} \pm 1$$

with $51{,}779$ digits.

Mathematical Induction

Mathematical induction is an important proof technique (method of proof) that can be used to prove theorems of the type $\forall n \ P(n)$, where P is a predicate and the domain of the predicate is the set of natural numbers. This method is used extensively to prove results about a large variety of discrete objects. (For example, it is used to prove results about the complexity of algorithms, the correctness of certain types of computer programs, theorems about graphs and trees, as well as a wide range of identities and inequalities).

In this section, we will describe how mathematical induction can be used and why it is a valid proof technique.

Note: Mathematical induction can be used only to prove results obtained in some other way. *It is not a tool for discovering formulae or theorems*.

Principle of Mathematical induction:

To prove that $P(n)$ is true for all natural numbers n, where $P(n)$ is a propositional function, we complete two steps.
***Basis step*:** we verify that $P(1)$ is true.
Inductive step: We show that the conditional statement $P(k) \longrightarrow P(k+1)$ is true for any arbitrary natural number k.

The assumption that $P(k)$ is true is called the **inductive hypothesis**. To complete the inductive step we assume that $P(k)$ is true for an arbitrary natural number k and show that $P(k+1)$ is also true.

Note: Some times we need to show that $P(n)$ is true for $n = a, a+1, a+2, \ldots$ where a is an integer other than 1. We can use mathematical induction to accomplish this as long as we change the basis step: Verify that $P(a)$ is true.

Example 17: Use mathematical induction to show that

a) $\mathbf{1+2+3+\cdots+n=\frac{n(n+1)}{2}}$ **, for all natural numbers**
b) $\mathbf{1+3+5+\cdots+(2n-1)=n^2}$ **, for all natural numbers**
c) $\mathbf{1+2+2^2+\cdots+2^n=2^{n+1}-1}$ **, for all non-negative integers**

Solution: *Left as exercise.*

Mathematical induction can be used to prove a variety of inequalities that hold for all natural numbers greater than a natural number.

Example 18: Use mathematical induction to prove that $2^n < n!$ for every natural number n with $n \geq 4$.

Solution: Let $P(n)$ be the proposition: $2^n < n!$. The domain of the propositional function is the set of natural numbers $n, n \geq 4$

Basis step: The basis step is $P(4)$.Note that $P(4)$ is true, since $2^4 = 16 < 24 = 4!$
Inductive step: We assume that $P(k)$ is true for the natural number k with $k \geq 4$. That is, $2^k < k!$ is true. Then

$$2^{k+1} = 2.2^k < 2.k! \text{ (by the inductive step)}$$

$$< (k+1).k! \text{ (since } 2 < k+1 \text{ when } k \geq 4)$$

$$= (k+1)!$$

Thus, $2^{k+1} < (k+1)!$. This shows that $P(k+1)$ is true when $P(k)$ is true. Therefore by the principle of mathematical induction $P(n)$ is true for all natural numbers n with $n \geq 4$. That is, $2^n < n!$ for all $n \in \boldsymbol{N}$, $n \geq 4$.

Mathematical induction can be used to the prove divisibility results about integers.

Example19: Use mathematical induction to prove that $n^3 - n$ is divisible by 3, when n is a natural number.

Solution: Let $P(n)$ be the proposition: $n^3 - n$ is divisible by 3. The domain of the propositional function is the set of natural numbers.
Basis step: Note that $1^3 - 1 = 0$ is divisible by 3. Therefore, $P(1)$ is true.
Inductive step: We assume that $P(k)$ is true. That is, $k^3 - k$ is divisible by 3. Therefore, $k^3 - k = 3m$ for some natural number m. Then

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k - k$$

$$= (k^3 - k) + 3(k^2 + k)$$

$$= 3m + 3(k^2 + k) \text{ (by inductive step)}$$

This shows that $(k+1)^3 - (k+1)$ is divisible by 3.Thus $P(k+1)$ is true when $P(k)$ is true.
By the principle of mathematical induction $P(n)$ is true for all natural numbers n. That is, $n^3 - n$ is divisible by 3 whenever n is a natural number.

Mathematical induction can be used to prove many results about sets.

Example 20: The number of subsets of a finite set

Use mathematical induction to show that if S is a finite set with n elements where n is a non negative integer, then S has 2^n subsets.

Solution: Let $P(n)$ be the proposition: *A set with n elements has 2^n subsets*.
The domain of the propositional function is the set of nonnegative integers.
Basis step: $P(0)$ is true, since a set with no elements , $i.e.$, the empty set, has exactly $1 = 2^0$ subset (namely itself).
Inductive step: Assume that $P(k)$ is true for an arbitrary nonnegative integer k, $i.e.$, every set with k elements has 2^k subsets. Let T be a set with $k+1$ elements. Then it is possible to write $T = S \cup \{a\}$, where a is one of the elements of T and $S = T - \{a\}$. Note that S has k elements and by induction hypothesis S has 2^k

subsets. The subsets of T can be obtained in the following way:
For each subset X of S there are exactly two subsets of T. They are X and $X \cup \{a\}$. These constitute all the subsets of T and they are all distinct. Since S has 2^k subsets of there are $2 \cdot 2^k = 2^{k+1}$ subsets of T, thus $P(k+1)$ is true when $P(k)$ is true. This proves the inductive step.

By the principle of mathematical induction $P(n)$ is true for all positive integers n. That is, a set with n elements has 2^n subsets, whenever n is a nonnegative integers n.

Validity of Mathematical Induction

The validity follows from an axiom, called **the well-ordering property**, for the set of natural numbers.

The well-ordering property*:* Every non empty subset of natural numbers has a least element.

Suppose that $P(1)$ is true and that the proposition $P(k) \longrightarrow P(k+1)$ is true for an arbitrary natural number k. To show that $P(n)$ is true for all natural numbers n , assume that there is atleast one natural number for which $P(n)$ is false. Let S be the set of all those natural numbers for which $P(n)$ is false. Clearly, S is non empty. By well-ordering property, S has a least element, say m. Note that $P(m)$ is false. Surely $m \neq 1$, since $P(1)$ is true. Therefore, $m > 1$ and $m-1$ is a natural number. Since $m-1 < m, m-1$ is not in S. Therefore , $P(m-1)$ must be true. Since the conditional proposition $P(m-1) \longrightarrow P(m)$ is true, it follows that $P(m)$ is true. This contradicts the choice of m. Therefore, (by proof by contradiction) $P(n)$ is true for every natural number n.This shows that the mathematical induction is a valid method of proof.

P1:

Give a direct proof of the theorem: If m and n are both perfect squares, then mn is also a perfect square.

Solution:

We recall a definition: An integer a is a perfect square if there is an integer b such that $a = b^2$. To produce a direct proof, we first assume the hypothesis of the conditional statement is true. That is , m and n are perfect squares. Therefore by definition, there are integers s and t such that $m = s^2$ and $n = t^2$. Now $mn = (st)^2$. This shows that mn is also a perfect square.

P2:

Prove by a proof by contraposition that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution:

We furnish a proof by contraposition. Assume that the conclusion of the conditional is false. That is, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ is false. Therefore, $a \leq \sqrt{n}$ is false and $b \leq \sqrt{n}$ is false. Thus, $a > \sqrt{n}$ and $b > \sqrt{n}$. From this it follows $ab > \sqrt{n} \cdot \sqrt{n} = n$. This shows that $n \neq ab$, which says that the hypothesis of the conditional is false. By the proof by contraposition the given conditional statement is true. Hence the result.

P3:

Prove by proof by contradiction that $\sqrt{2}$ is an irrational number.

Solution:

We prove it by a proof by contradiction. Let p be the proposition: $\sqrt{2}$ is a irrational number. To prove by the proof by contradiction, suppose that $\sim p$ is true. That is $\sqrt{2}$ is a rational number. We show that this leads to a contradiction. Thus, there exists integers a and b such that they have no common factors and $\sqrt{2} = \frac{a}{b}$ .Squaring both sides, it gives $2b^2 = a^2$. From this it follows that a^2 is even and there by a is even. Therefore, $a = 2c$ for some integer c. Thus $2b^2 = 4c^2$ and $b^2 = 2c^2$. From this it follows that b is even. This shows that a and b have common factor 2, a contradiction. Thus, the assumption $\sim p$ is true leads to a contradiction. Therefore, $\sim p$ is false and therefore p is true.

P4:

Using a proof by cases, show that $|xy| = |x||y|$, where x and y are real numbers.

Solution:

Let a be a real number. Recall that, $|a|$ denotes the absolute value of a and it is defined as

$$|a| = \begin{cases} a & if \quad a \geq 0 \\ -a & if \quad a < 0 \end{cases}$$

Since $|x|$ and $|y|$ occur in the formula to be proved, we consider the following four cases:

(i) x and y both non-negative, (ii) x is non-negative and y is negative,
(iii) x is negative and y is nonnegative, and (iv) x and y both negative.

Case (i) : If $x \geq 0$ and $y \geq 0$ then $xy \geq 0$. Therefore, $|xy| = xy = |x||y|$. The conclusion is true in this case.

Case (ii) : If $x \geq 0$ and $y < 0$ then $xy \leq 0$. Therefore,
$|xy| = -xy = x(-y) = |x||y|$. The conclusion is true in this case.

Case (iii) : If $x < 0$ and $y \geq 0$ then $xy \leq 0$. Therefore,
$|xy| = -xy = (-x)y = |x||y|$. The conclusion is true in this case.

Case (iv) : If $x < 0$ and $y < 0$ then $xy > 0$. Therefore
$|xy| = xy = (-x)(-y) = |x||y|$. The conclusion is true in this case also .
The result follows by the proof by cases.

P5:

Using a proof by exhaustion, show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.

Solution:

We can eliminate all but a few cases. An integer x is not a solution if $x^2 > 8$, $i.e.$, if $|x| \geq 3$ and an integer y is a solution if $3y^2 > 8$, $i.e.$, if $|y| \geq 2$. This leaves the case when x takes one of the values $-2, -1, 0, 1$, or 2 and y takes one of the values $-1, 0$, or 1 . For any of these values x^2 takes one of the values 0, 1, 4 and $3y^2$ takes one of the values 0,3. Note that the largest value for $x^2 + 3y^2$ is 7.Thus the equation $x^2 + 3y^2 = 8$ has no integer solutions for $x$and y.

P6:

Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Solution:

To show that the statement is false, we look for a counter example, i.e., an integer which is not the sum of the squares of two integers. Note that the only perfect squares not exceeding 3 are $0^2 = 0,\ 1^2 = 1$ and their sum is at most 1. Thus, there is no way to express 3 as the sum of the squares of two integers. Therefore, the given statement is false.

P7:

Use mathematical induction to show that $2n^3 + 3n^2 + n$ is divisible by 6 for every natural number n.

Solution:

Let $P(n)$ be the proposition: $2n^3 + 3n^2 + n$ is divisible by 6.The domain of the propositional function is the set of natural numbers.

Basis step: $P(1)$ is true, since $2.1^3 + 3.1^2 + 1 = 6$, which is divisible by 6.
Inductive step: Assume that $P(k)$ is true for an arbitrary natural number k, i.e., assume that $2k^3 + 3k^2 + k$ is divisible by 6.Therefore $2k^3 + 3k^2 + k = 6m$ for some natural number m. Then

$$2(k+1)^3 + 3(k+1)^2 + (k+1)$$

$$= (2k^3 + 3k^2 + k) + 6(k^2 + 2k + 1)$$

$$= 6m + 6(k^2 + 2k + 1) \quad \text{(By inductive hypothesis)}$$
$$= 6(m + k^2 + 2k + 1)$$

This shows that $P(k+1)$ is true when $P(k)$ is true. By the principle of mathematical induction, $P(n)$ is true for all natural number n, $i.e.$, $2n^3 + 3n^2 + n$ is divisible by 6 for every natural number n.

P8:

Use mathematical induction to prove the following generalization of De Morgan's law for propositions:

$$\sim(\boldsymbol{p_1} \wedge \boldsymbol{p_2} \wedge \ldots \wedge \boldsymbol{p_n}) \equiv \sim\boldsymbol{p_1} \vee \sim\boldsymbol{p_2} \vee \ldots \vee \sim\boldsymbol{p_n}$$

for all $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{n} \geq \boldsymbol{2}$.

Solution:

Let $P(n)$ be the indentity for n proposition.The domain of the propositional function is the set of natural numbers n, $n \geq 2$.

Basis step: $P(2)$ is true, since $\sim(p_1 \wedge p_2) \equiv \sim p_1 \vee \sim p_2$ by De Morgan's law.

Inductive step: We assume that $P(k)$ is true for an arbitrary natural number $k, k \geq 2$. That is $\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k) \equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k$.

Then,

$$\begin{aligned}
\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k \wedge p_{k+1}) &\equiv \sim\big((p_1 \vee p_2 \vee \ldots \vee p_k) \wedge p_{k+1}\big) \\
&\equiv \sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k) \vee \sim p_{k+1} \\
&\equiv (\sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k) \vee \sim p_{k+1} \\
&\equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k \vee \sim p_{k+1}
\end{aligned}$$

This, shows that $P(k+1)$ is true when $P(k)$ is true. By the principle of mathematical induction $P(n)$ is true for all $n \in \boldsymbol{N}$, $n \geq 2$. That is

$\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_n$, for all $n \in \boldsymbol{N}$, $n \geq 2$.

1.7. Methods of Proof

Exercise:

1. Prove by direct proof that, if an integer a is such that $a-2$ is divisible by 3, then a^2-1 is divisible by 3.

2. Prove by proof by contraposition that for any non-negative integers x, y, if $\sqrt{xy} \neq \frac{(x+y)}{2}$, then $x \neq y$.
3. Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.
4. Show that if n is an integer and n^3+5 is odd, then n is even ,using
   a. A proof by contraposition b. A proof by contradiction.

5. Use a proof by contradiction to show that there is no rational number r for which $r^3+r+1=0$. [Hint: Assume that $r=a/b$ is a root, where a and b are integers and a/b is in lowest terms. Obtain an equation involving integers by multiplying by b^3. Then look at whether a and b are each odd or even.]

6. Show that these statements about the integer x are equivalent:
   (a) $3x+2$ is even,(b) $x+5$ is odd, (c) x^2 is even.

7. Use the mathematical induction to prove that
$$1^2+3^2+5^2+\cdots+(2n+1)^2=\frac{(n+1)(2n+1)(2n+3)}{3}$$
   whenever n is a nonnegative integer.
8. Use the mathematical induction to prove that for every positive integer n,
$$1\cdot 2+2\cdot 3+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$$
9. Prove that 5 divides n^5-n whenever n is a nonnegative integer.
10. Prove that if $A_1, A_2, \ldots A_n$ are subsets of a universal set U, then
$$\left(\bigcup_{k=1}^{n} A_k\right)' = \bigcap_{k=1}^{n} (A_k)'$$
    Where A' denotes the complement of the set A