	PARUL UNIVERSITY **FACULTY OF ENGINEERING & TECHNOLOGY** **Department of Applied Sciences & Humanities** **Third Semester B. Tech (CSE, IT)** **Discrete Mathematics (303191202)** **Unit 2 - Principles of Mathematical Induction** **Academic Year: 2025-26**

Well Ordering Principle:

The well-ordering principle states that every non-empty set of non-negative integers has a least element.

Principle of Mathematical Induction: Mathematical induction is one of the most important and powerful techniques for verifying mathematical statements. Many complicated mathematical theorems about integers can be proved easily by mathematical induction. An analogy of the principle of mathematical induction is the **game of dominoes**. Suppose the dominoes are lined up properly, so that when one falls, the successive one will also fall. Now by pushing the first domino, the second will fall; when the second falls, the third will fall; and so on. We can see that all dominoes will ultimately fall.

Theorem 1. (Weak Mathematical Induction): For each positive integer n, let $P(n)$ be a statement. Suppose

(1) $P(1)$ is true (**Base Case**) ;

(2) if $P(k)$ is true for some positive integer k (this is called the **Inductive Hypothesis**), then $P(k+1)$ is also true. **(Inductive Step)**

Then $P(n)$ is true for all positive integers n.

Proof: Assume, to the contrary, that the theorem is false. Then there exists some positive integers n for which $P(n)$ is false. Let

$$S = \{n \in \mathbb{N} : P(n) \; is \; false\}.$$

Since S is a non-empty subset of $\mathbb{N}$, it follows by the **Well Ordering Principle** that S contains a least element s. Since $P(1)$ is true, $1 \notin S$. Thus $s \geq 2$ and $s-1 \in \mathbb{N}$. Therefore, $s-1 \notin S$ and so $P(s-1)$ is a true statement. By condition (2), $P(s)$ is also true and so $s \notin S$ which contradicts our initial assumption that $s \in S$. Hence $S = \emptyset$.

Remark: More generally, you have the following variation of Theorem 1.

Theorem 2. Suppose some statement $P(n)$ is defined for all $n \geq n_0$ where n_0 is a non-negative integer. Let

(1) $P(n_0)$ is true ;

(2) for any $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is also true.

Then $P(n)$ is true for all positive integers $n \geq n_0$.

Applications:

Example 1. Prove $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Proof: Let P(n) be the statement $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Base case: For P(1), L.H.S = 1 = $\frac{1}{2} \times 1 \times (1 + 1)$ = R.H.S. Hence P(1) is true.

Inductive step: Assume P(k) is true for some positive integer k, that is, $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$.

For P(k+1),

$$1 + 2 + 3 + \cdots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1) = \frac{1}{2}(k + 1)\,(k + 2) = \frac{1}{2}(k + 1)\,[(k + 1) + 1]$$

Thus P(k+1) is true. Therefore, by Theorem 1, P(n) is true for all positive integers n.

Example 2. Use the Principle of Mathematical Induction to verify that, $6^n - 1$ is divisible by 5 for any positive integer n.

Proof: For any $n \geq 1$, let P(n) be the statement that $6^n - 1$ is divisible by 5.

Base case: The statement P(1) says that $6^1 - 1 = 5$ which is divisible by 5. So P(1) is true.

Inductive step: Assume P(k) is true for some positive integer k, that is, $6^k - 1$ is divisible by 5.

For P(k+1),

$$6^{k+1} - 1 = 6 \cdot 6^k - 6 + 5 = 6(6^k - 1) - 5.$$

From our inductive hypothesis it follows that the first term $6(6^k - 1)$ is divisible by 5 and the second term is clearly divisible by 5. Therefore P(k+1) holds.

Thus, by Theorem 1, P(n) holds for all positive integers n.

Example 3. Prove that $n\,! > 3^n$ for $n \geq 7$.

Proof: For any $n \geq 7$, let P(n) be the statement that $n\,! > 3^n$.

Base case: The statement P(7) says that 7 ! = 5040 > 3^7 = 2187, which is true.

Inductive step: Assume P(k) is true for some positive integer $k \geq 7$, that is, $k\,! > 3^k$.

For P(k+1),

$$(k + 1)\,! = (k + 1)\,k\,! > (k + 1)\,3^k \geq (7 + 1)\,3^k = 8 \times 3^k > 3 \times 3^k = 3^{k+1}.$$

Therefore P(k+1) holds. Thus by Theorem 2, P(n) is true for all $n \geq 7$.

Practice Examples:

(1) Prove: $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \in \mathbb{N}$.

(2) Prove: $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$ for all $n \in \mathbb{N}$.

(3) Prove that $2^{2n} - 1$ is divisible by 3 for all $n \in \mathbb{N}$.

(4) Prove that $9^n - 2^n$ is divisible by 7 for all $n \in \mathbb{N}$.

Theorem 3. (Strong Mathematical Induction): For each positive integer n, let $P(n)$ be a statement. Let

(1) $P(1)$ is true (**Base Case**) ;

(2) if $P(1), P(2), \ldots, P(k)$ are all true for some positive integer k (this is called the **Inductive Hypothesis**), then $P(k+1)$ is also true. **(Inductive Step)**

Then $P(n)$ is true for all positive integers n.

Remarks: (i) To better understand the Strong Induction, consider an **Infinite Ladder**. Strong induction tells us that we can reach all steps of the ladder if

1. We can reach the first step, and

2. For every positive integer k, if we can reach all the first k steps, then we can reach the $(k+1)$th step.

(ii) We can have a variation of Theorem 3 similar to that of Theorem 2. The details are omitted as of now.

Motivation: The following three examples will serve as a motivation for Theorem 3 since you can't solve them using Theorem 1 or Theorem 2.

Example 4. Prove that every positive integer $n \geq 2$ can be written as a product of primes.

Proof: For any $n \geq 2$, let P(n) be the statement that n can be written as a product of primes.

Base case: The statement P(2) is true since 2 is itself a prime.

Inductive step: Suppose every integer $2, 3, \ldots, k$ can be written as a product of primes (the **Inductive Hypothesis**). For P(k+1), either $k+1$ is a prime or it isn't. If it's a prime, then we are done. Otherwise

$$k + 1 = a \cdot b \ \ with \ \ 2 \leq a \leq k \ \ \ and \ \ 2 \leq k \leq b.$$

By the Inductive Hypothesis, it follows a and b are each products of primes, and therefore k + 1 is also a product of primes.

Finally, by Theorem 3 (truly speaking, a variation of Theorem 3), P(n) holds for all positive integers $n \geq 2$.

Example 5. Define a sequence recursively by:

$$a_n = \begin{cases} a_1 = 1 \\ a_2 = 4 \\ a_n = 2a_{n-1} - a_{n-2} \quad for\ n \geq 3. \end{cases}$$

Prove that $a_n = 3n - 2$ for all $n \geq 1$.

Proof: For any $n \geq 1$, let P(n) be the statement that $a_n = 3n - 2$.

Base case: The statements P(1) and P(2) are true since $a_1 = 1 = 3 \cdot 1 - 2$ and $a_2 = 4 = 3 \cdot 2 - 2$.

Inductive step: Assume that $a_i = 3i - 2$ for $i = 1, 2, 3, \dots, k$. For P(k+1), observe that

$$a_{k+1} = 2a_k - a_{k-1} = 2(3k - 2) - [3(k - 1) - 2] = 6k - 4 - 3k + 3 + 2 = 3k + 1 = 3(k + 1) - 2.$$

Therefore, we are done.

Example 6. Prove that every integer $n \geq 12$ can be written as $n = 4a + 5b$ for some non-negative integers a, b.

Proof: For any $n \geq 12$, let P(n) be the statement that $n = 4a + 5b$ for some non-negative integers a, b.

Base case: The statements P(12), P(13), P(14) and P(15) are true. (Exercise)

Inductive step: Suppose every $12 \leq i \leq k$ can be written as $i = 4a + 5b$. We want to show $k + 1$ can also be written this way for $k + 1 \geq 16$.

For P(k+1), observe that $k + 1 = (k - 3) + 4$. By the inductive hypothesis, $k - 3 = 4a + 5b$ for some a, b since $k - 3 \geq 12$ which implies $k + 1 = 4(a + 1) + 5b$.

Hence, we are done (by a variation of Theorem 3).

Recursive Definitions:

Sometimes it is difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called **recursion**.

Recursively Defined Functions:

We use two steps to define a function with the set of nonnegative integers as its domain:

Basis Step: Specify the value of the function at zero.

Recursive Step: Give a rule for finding its value at an integer from its values at smaller integers. Such a definition is called a **recursive** or **inductive.**

Example: Suppose that f is defined recursively by

$$f(0) = 3,$$
$$f(n+1) = 2f(n) + 3$$

Find $f(1), f(2), f(3) \& f(4)$.

Solution: From the recursive definition it follows that

$f(1) = 2f(0) + 3 = 2 \bullet 3 + 3 = 9$
$f(2) = 2f(1) + 3 = 2 \bullet 9 + 3 = 21$
$f(3) = 2f(2) + 3 = 2 \bullet 21 + 3 = 45$
$f(4) = 2f(3) + 3 = 2 \bullet 45 + 3 = 93$

Example: Give a recursive definition of a^n, where a is a nonzero real number and n is a nonnegative integer.

Solution: The recursive definition contains two parts.

(1) a^0 is specified, namely, $a^0 = 1$.

(2) The rule for finding a^{n+1} from a^n, namely, $a^{n+1} = a^n \bullet a$, for n = 0, 1 , 2, 3 , . . . , is given.

The above two conditions uniquely define a^n for all nonnegative integers n.

The Division Algorithm:

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

Proof: The proof is by **Well Ordering Principle**. Let S be the set of non-negative integers of the form $a - dq$, where q is an integer. This set is non-empty because $-dq$ can be made as large as desired (taking q to be a negative integer with large absolute value). By the well-ordering property, S has a least element $r = a - dq_0$.

The integer r is non-negative. It is also the case that r < d. If it were not, then there would be a smaller non-negative element in S, namely, $a - d(q_0 + 1)$. To see this, suppose that $r \ge d$. Because $a = dq_0 + r$, it follows that $a - d(q_0 + 1) = (a - dq_0) - d = r - d \ge 0$. Consequently, there are integers q and r with $0 \le r < d$.

Definition: In the equality given in the division algorithm, d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder. The following notations are used to express the quotient and remainder :

$$q = a \operatorname{div} d, \quad r = a \bmod d$$

Example: What are the quotient and remainder when 101 is divided by 11 ?

Solution: We have $101 = 11 \bullet 9 + 2$

Hence, the quotient when 101 is divided by 11 is 9 = 101 div 11, and the remainder is 2 =101 mod 11.

Example: What are the quotient and remainder when - 11 is divided by 3 ?

Solution: We have $-11 = 3 \bullet (-4) + 1$. Hence, the quotient when - 11 is divided by 3 is - 4 = - 11 div 3, and the remainder is 1 = - 11 mod 3. Note that the remainder cannot be negative. Hence, the remainder is not -2, even though $-11 = 3 \bullet (-3) - 2$ because r = - 2 does not satisfy $0 \le r < 3$.

Primes:

A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p itself. A positive integer that is greater than 1 and also not prime is called composite.

Example: The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

Proof: The proof is by **Well Ordering Principle**. Let C be the set of all integers greater than 1 that cannot be factored as a product of primes. We assume C is not empty and derive a contradiction.

If $C \neq \emptyset$, there is a least element, $n \in C$, by well ordering property. Then n can't be a prime. So n must be a product of two integers a and b where $1 < \text{a}, \text{b} < \text{n}$. Since a and b are smaller than n, we have

$$a = p_1 \, p_2 \ldots p_k$$
$$b = q_1 \, q_2 \ldots q_l$$

for primes $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$. Therefore

$$n = p_1 \, p_2 \ldots p_k \, q_1 \, q_2 \ldots q_l$$

contradicting the claim that $n \in C$. Therefore $C = \emptyset$.

Example: The prime factorizations of 100, 641, 999, and 1024 are given by

$100 = 2 \bullet 2 \bullet 5 \bullet 5 = 2^2 \bullet 5^2$

$641 = 641$

$999 = 3 \bullet 3 \bullet 3 \bullet 37 = 3^3 \bullet 37$

$1024 = 2^{10}$

Remark: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Example: Show that 101 is prime.

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3 , 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

Greatest Common Divisor

Let a and b be integers, not both zero. The largest integer d such that $d \mid a \& d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a,b)$.

Example: What is the greatest common divisor of 24 and 36 ?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd (24, 36) = 12.

Example: What is the greatest common divisor of 17 and 22 ?

Solution: The integers 17 and 22 have no positive common divisors other than 1, so that gcd (17, 22) = 1.

Euclidean Algorithm:

Next, we will give a more efficient method of finding the greatest common divisor, called the Euclidean algorithm.

Example: Find gcd (91,287) using Euclidean algorithm.

Solution: First, divide 287, the larger of the two integers, by 91, the smaller one, 287 = 91 x 3 + 14 . Any divisor of 91 and 287 must also be a divisor of 287 - 91 x 3 = 14. Also, any divisor of 91 and 14 must also be a divisor of 287 = 91 x 3 + 14.

Hence, the greatest common divisor of 91 and 287 is the same as the greatest common divisor of 91 and 14. This means that the problem of finding gcd (91 , 287) has been reduced to the problem of finding gcd (91 , 14).

Next, divide 91 by 14 to obtain 91 = 14 x 6 + 7. Because any common divisor of 91 and 14 also divides 91 - 14 x 6 = 7 and any common divisor of 14 and 7 divides 91. Therefore gcd (91 ,14) = gcd (14, 7).

Continue by dividing 14 by 7, to obtain 14 = 7 x 2. Because 7 divides 14, it follows that gcd(14, 7) = 7.

Furthermore, because gcd (287, 91) = gcd (91 , 14) = gcd (14, 7) = 7.

Example: Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

662 = 414 x 1 + 248
414 = 248 x 1 + 166
248 = 166 x 1 + 82
166 = 82 x 2 + 2
82 = 2 x 41.

Hence, gcd (414, 662) = 2, because 2 is the last non-zero remainder.

Basic Counting Principles:

Product Rule: Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Sum Rule: If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Example: A new company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees ?

Solution: The procedure of assigning offices to these two employees consists of assigning an office to Sanchez, which can be done in 12 ways, then assigning an office to Patel different from the office assigned to Sanchez, which can be done in 11 ways. By the product rule, there are 12 x 11 = 132 ways to assign offices to these two employees.

Example: The chairs of an auditorium are to be labeled with a letter and a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently ?

Solution: The procedure of labeling a chair consists of two tasks, namely, assigning one of the 26 letters and then assigning one of the 100 possible integers to the seat. The product rule shows that there are 26 x 100 = 2600 different ways that a chair can be labeled. Therefore, the largest number of chairs that can be labeled differently is 2600.

Example: There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a microcomputer in the center are there ?

Solution: The procedure of choosing a port consists of two tasks, first picking a microcomputer and then picking a port on this microcomputer. Because there are 32 ways to choose the microcomputer and 24 ways to choose the port no matter which microcomputer has been selected, the product rule shows that there are 32 x 24 = 768 ports.

Example: Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student ?

Solution: There are 37 ways to choose a member of the mathematics faculty and there are 83 ways to choose a student who is a mathematics major. Choosing a member of the mathematics faculty is never the same as choosing a student who is a mathematics major because no one is both a faculty member and a student. By the sum rule it follows that there are 37 + 83 = 120 possible ways to pick this representative.

Example: A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from ?

Solution: The student can choose a project by selecting a project from the first list, the second list, or the third list. Because no project is on more than one list, by the sum rule there are 23 + 15 + 19 = 57 ways to choose a project.

Inclusion-Exclusion Principle:

To correctly count the number of ways to do the two tasks, we add the number of ways to do it in one way and the number of ways to do it in the other way, and then subtract the number of ways to do the task in a way that is both among the set of n_1 ways and the set of n_2 ways. This technique is called the principle of **inclusion-exclusion**. Sometimes, it is also called the **subtraction principle** for counting.

Example: How many bit strings of length eight either start with a 1 bit or end with the two bits 00 ?

Solution: We can construct a bit string of length eight that start with 1 in 2^7=128 ways. This follows by the product rule, because the first bit can be chosen in only one way and each of the other seven bits can be chosen in two ways. Next we construct bit string of length eight that end with 00 in 2^6=64 ways. This follows by the product rule, because the first 6 bits can be chosen in two ways and the last two bits can be chosen in only one way. We construct a bit string of length eight that start with 1 and end with 00 in 2^5=32 ways. which equals the number of ways to construct a bit string of length eight that begin with a 1 or that ends with 00, equals 128 + 64 - 32 = 160 ways.

Example: A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these people majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business ?

Solution: To find the number of these applicants who majored neither in computer science nor in business, we can subtract the number of students who majored either in computer science or in business (or both) from the total number of applicants.

Let A_1 be the set of students who majored in computer science and A_2 the set of students who majored in business. Then $A_1 \cup A_2$ is the set of students who majored in computer science or business (or both), and $A_1 \cap A_2$ is the set of students who majored both in computer science and in business.

By the principle of inclusion-exclusion, the number of students who majored either in computer science or in business (or both) equals $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ = 220 + 147 - 51 = 316.

We conclude that 350 - 316 = 34 of the applicants majored neither in computer science nor in business.

The Pigeonhole Principle:

If n items are put into m boxes, with n > m, then at least one box must contain more than one item.

Remark: A function f from a set with k + 1 or more elements to a set with k elements is not one-to-one.

Example: Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

Example: In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

Permutations:

A **permutation** of a set of distinct objects is an ordered arrangement of these objects. We also are interested in ordered arrangements of some of the elements of a set. An ordered arrangement of r elements of a set is called an **r-permutation**.

$$P(n,r) = \frac{n!}{(n-r)!}$$

Combinations:

A **combination** of these n objects taken r at a time is any selection of r of the objects where order does not count. In other words, **r-combination** of a set of n objects is any subset of r elements.

$$C(n,r) = \frac{n!}{r!(n-r)!}$$

Example: How many bit strings of length n contain exactly r 1's ?

Solution: The positions of r 1's in a bit string of length n form an r-combination of the set { 1 , 2 , 3 , . . . , n}. Hence, there are C (n, r) bit strings of length n that contain exactly r 1's.

Example: Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty members from the mathematics department and four from the computer science department ?

Solution: By the product rule, the answer is the product of the number of 3-combinations of a set with nine elements and the number of 4-combinations of a set with 11 elements. By Theorem 2, the number of ways to select the committee is $C(9, 3) \cdot C(11, 4) = \frac{9!}{3!6!} \cdot \frac{11!}{4!7!} = 84 \cdot 330 = 27{,}720$.

Example: Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities ?

Solution: The number of possible paths between the cities is the number of permutations of seven elements, because the first city is determined, but the remaining seven can be ordered arbitrarily. Consequently, there are $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ ways for the saleswoman to choose her tour. If, for instance, the saleswoman wishes to find the path between the cities with minimum distance, and she computes the total distance for each possible path, she must consider a total of 5040 paths.

Example: How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 100 different people who have entered a contest ?

Solution: Because it matters which person wins which prize, the number of ways to pick the three prize winners is the number of ordered selections of three elements from a set of 100 elements, that is, the number of 3-permutations of a set of 100 elements. Consequently, the answer is $P(100, 3) = 100 \cdot 99 \cdot 98 = 970{,}200$.

Example: A group of 30 people have been trained as astronauts to go on the first mission to Mars. How many ways are there to select a crew of six people to go on this mission (assuming that all crew members have the same job) ?

Solution: The number of ways to select a crew of six from the pool of 30 people is the number of 6-combinations of a set with 30 elements, because the order in which these people are chosen does not matter. By Theorem 2, the number of such combinations is $C(30, 6) = \frac{30!}{6!\ 24!} = (30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25) / (6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1) = 593{,}775$.