	DAYANANDA SAGAR COLLEGE OF ENGINEERING *(An Autonomous Institute Affiliated to VTU, Belagavi)* Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078 **DEPARTMENT OF MATHEMATICS**

Course Material

COURSE	**MATHEMATICAL STRUCTURES**
COURSE CODE	**21MAT41A**
MODULE	**1**
MODULE NAME	**Set Theory and Number Theory**
FACULTY INCHARGE	**Dr. Rose Bindu Joseph P**

Objectives:

After studying this module, students will be able to

- Define Sets and Subsets
- Define Set Operations
- Understand the Laws of Set Theory,
- Understand Addition Principles
- Understand Concept of Number Theory-Simple Problems

Set

A set is a collection of well defined objects. The objects that constitute a set are called **elements** or **members** of the set.

Notation: Usually set is denoted by capital letters A, B, C, X, Y, Z …. And its elements are denoted by lower case letters a, b, c, x, y, z…….

For example, if A is any set having elements x_1, x_2, x_3 then we write $A = \{x_1, x_2, x_3\}$

If an element x is in the set A or belongs to the set A then it is denoted by $x \in A$, otherwise $x \notin A$.

If S be a set of odd integers, 3, 7, 11 $\in S$ but 4,6 $\notin S$.

Representation of a Set

i. **Tabular form of a set:** In this, the elements are enclosed in curly brackets after separating them by commas, e.g., the set of even positive integers less than 10 is written as $\boldsymbol{S = \{2, 4, 6, 8\}}$

ii. **Symbolic form of a set:** In this, the set is written as $\{x/p(x)\}$ where x is a typical element of the set and $P(x)$ is the property satisfied by this element. In symbolic form, the above set is given by
$S = \{x\ /x$ is an even positive integer less than 10$\}$

Empty set or null set: A set which has no elements is called an ***empty set*** or the ***null set*** usually denoted by ϕ.
Ex: { }

Finite and Infinite Sets: A set is said to be **finite** if it has a finite number of elements. Otherwise a set is said to be **infinite**.

The number of distinct elements in a finite set A is called its cardinality and is denoted by $|A|$.

Subset: Let A and B are two sets**.** If every element of the set A is also the element in B, then A is called a subset of B and this relationship is denoted by $A \subseteq$ B, and it means A is in B or A is equal to B. If A is not equal to B then A is called proper subset of B and it is denoted by $A \subset B$ which is read 'A is contained in B'.

Or

Another definition: If A and B are two sets such that $x \in A \Longrightarrow x \in B$ then A is called a subset of B.

Example: $X = set\ of\ natural\ numbers = \{x | x \in N\}$

Y= set of integers = $\{y | y \in Z\}$

then $X \subset Y$.

Example: $X = \{1,2,3,5,7,9\}$ and $Y = \{1,2,3,5,7,9,8\}$ then $X \subset Y$.

Equal sets: Two sets A and B are said to be equal if they have same elements and it is denoted by $A = B$.

In the other words, if A and B are two sets such that $A \subset B \quad and \quad B \supset A \iff A = B$

For example, $A = \{1,2,3\}$, $B = \{x \in N | 1 \leq x \leq 3\}$, then $A = B$.

Universal set: Universal set is that which has all the sets under investigation as its subsets. It is generally denoted by U.

Example:

- The set of all letters of English alphabet is a universal set
- The set of all integers Z= { ………..-3, -2, -1, 0, 1, 2, 3, …………………….}

Example: If A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$, then show that $A \subseteq C$

Solution: Let x be any element of A. Since $A \subseteq B$ i.e., all the elements of A belongs to B,

$x \in A \Longrightarrow x \in B$ (1)

Again as $B \subseteq C$ i.e., all the elements of B belongs to C,

$x \in B \Longrightarrow x \in C$ (2)

∴ It follows from (1) and (2) that $x \in A \Longrightarrow x \in C$, i.e., $A \subseteq C$.

Power set: Power set of A is the set of all subsets of A, called $P(A)$.

If a finite set A has n elements, then P(A), the power set of A has 2^n elements.
Ex: Let A = {a, b} then Ƥ(A) = {ø, {a}, {b}, {a, b}}

Note:
1. Every set is a subset of itself.
2. Two sets A and B are equal iff $A \subset B$ and $B \supset A$.
3. The null set Φ is a subset of every set A.
4. For any sets A, B, C if A=B and B=C, then A=C.

Set Operations:

Union of two sets:
Let A and B be two sets then the union of two sets A and B is denoted by $A \cup B$ is the set of elements which are in A or in B or in both, i.e.

$$A \cup B = \{x | x \in A \text{ or } x \in B\}$$

By use of Venn diagram, the union of two sets is given by the shaded portion in figure 1

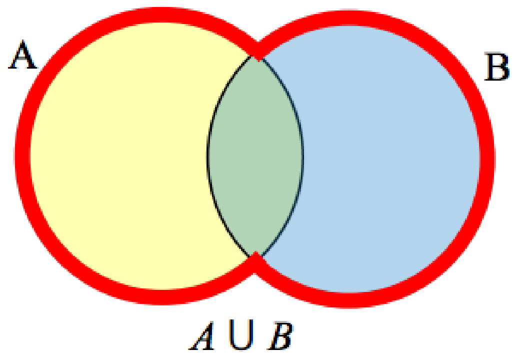

Figure 1

Example:

$A = \{1,2,3,4,5,6\}$

$B = \{5,7,4,3,9\}$

$A \cup B = \{1,2,3,4,5,6,7,9\}$

Intersection of two sets:
For two sets A and B the intersection fives a set having the elements in A as well as in B and is denoted by $A \cap B$.
i.e., $A \cap B = \{x | x \in A \text{ and } x \in B\}$
By Venn diagram $A \cap B$ is given by the following shaded portion in figure 2.

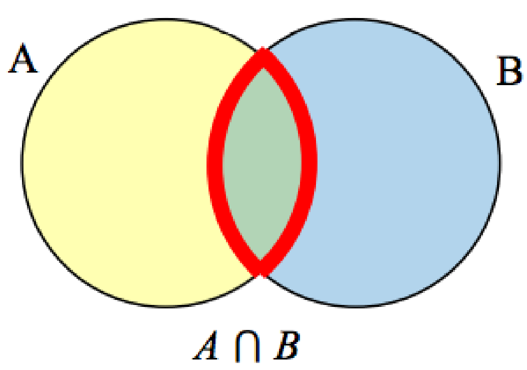

Figure 2

Example :

$A = \{1,2,3,4,5,6\}$

$B = \{5,7,4,3,9\}$

$A \cap B = \{3,4,5\}$

Disjoint Set: If for any two sets A and B, $A \cap B = \emptyset$ i.e., no element is common then A and B are called disjoint sets & by Venn diagram.

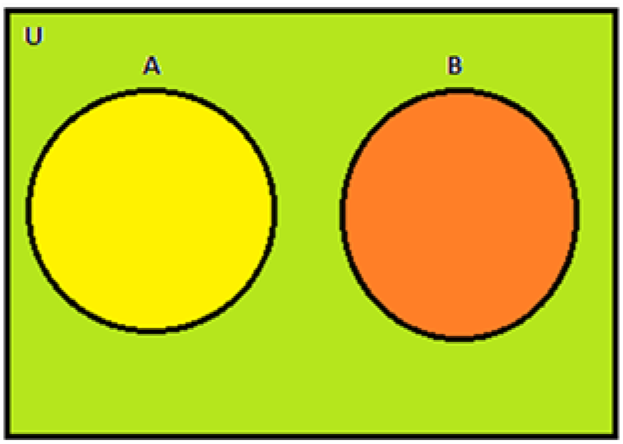

Figure 3

Example:

$A = \{1,2,3,4,5\}$

$B = \{10,11,12\}$

$A \cap B = \emptyset$

Complement of a set: The complement of a set A is the set of elements which belongs to U but not to A. It is denoted by A^c or A' or $\bar{A}$.

i.e., $A^c = \{x | x \in U, \ x \notin A\}$

By Venn diagram complement of the set is given by the shaded portion in figure 4.

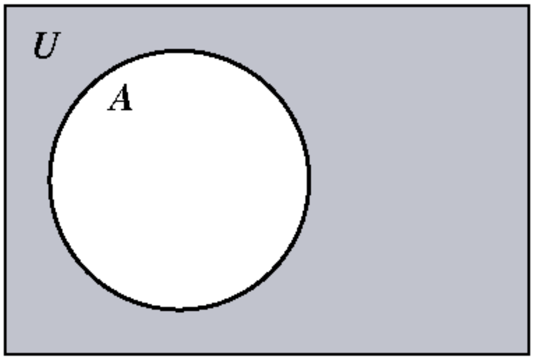

Figure 4

Relative Complement:

The relative complement of a set B with respect to a set A or simply, the difference of A and B is denoted by A$/$B or $A{\sim}B$ is the set of elements which belong to A but not to B.

i.e., A~B = $\{x|x \in A \; and \;\; x \notin B\}$

By Venn diagram A~B is given by the shaded portion in figure 5

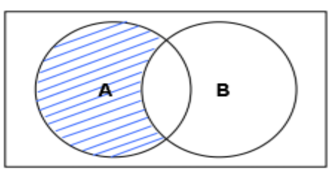

Figure 5

Example : If A={1,2,3,4}

B={3,4, 5, 6, 7}

A~B= {1.2}

Symmetric Difference:

The symmetric difference of the sets A and B is denoted by $A \oplus B$ consists of those elements which belongs to A or B but not both i.e.

$$A \oplus B = (A \cup B){\sim}(A \cap B)$$

$$= (A \sim B) \cup (B \sim A)$$

By Venn diagram the symmetric difference of two sets is given by the shaded portion, in figure 6.

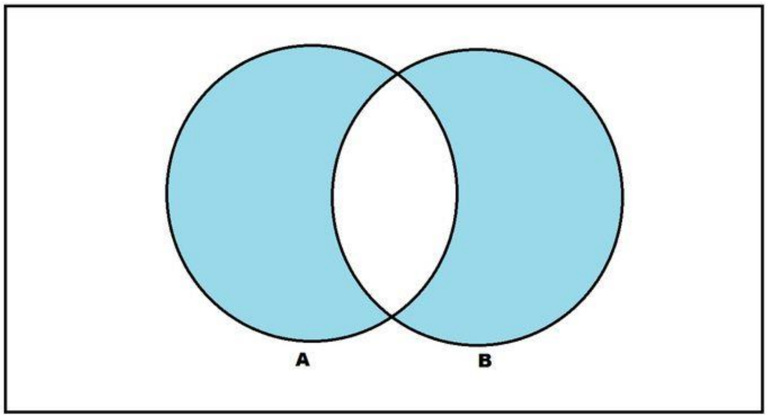

Figure 6

Example:

Let A={1, 2, 3, 4, 5, 6}

B={4, 5, 6, 7 ,8 , 9}

A~B = {1, 2, 3}

B ~ A= {7, 8, 9}

$A \oplus B = \{1, 2, 3, 7, 8, 9\}$

Algebra of sets:

Following are the properties which give the algebra of sets for the given sets A, B, and C.

1. $A \cup A = A$ **Idempotent laws**
   $A \cap A = A$

2. $(A \cup B) \cup C = A \cup (B \cup C)$ **Associative laws**
   $(A \cap B) \cap C = A \cap (B \cap C)$

3. $A \cup B = B \cup A$ **Commutative laws**
   $A \cap B = B \cap A$

4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ **Distributive laws**
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5. $A \cup \emptyset = A$ **Identity laws**
   $A \cap \emptyset = \emptyset$
   $A \cup U = U$

   $A \cap U = A$

Where $\emptyset$ is the empty set and U is the universal set.

6. $A \cup A^c = U$ **Complement laws**
   $A \cap A^c = \emptyset$ (A^c *is also denoted bt* $\bar{A}$)
   $(A^c)^c = A$
   $U^c = \emptyset$
   $\emptyset^c = U$

7. $(A \cup B)^c = A^c \cap B^c$ **De Morgan's law**
   $(A \cap B)^c = A^c \cup B^c$

8. $A \cup (A \cap B) = A$ **Absorption Laws**
   $A \cap (A \cup B) = A$

The results can be verified with the help of Venn diagrams.

Example: For any three sets A, B, C prove the following:

(i) $A \cup (B \cup C) = (A \cup B) \cup C$

Ans: Let $D = B \cup C$ *and* $E = A \cup B$. Take any $x \in A \cup (B \cup C)$.

Then $x \in A \cup D$ so that $x \in A$ *or* $x \in D$

so that $x \in A \quad or \quad x \in (B \cup C)$

so that $x \in A \quad or \quad (x \in B \quad or \quad x \in C)$

so that $(x \in A \quad or \quad x \in B) \quad or \quad x \in C$

so that $x \in A \cup B \quad or \quad x \in C$

so that $x \in E \quad or \quad x \in C$

so that $x \in E \cup C$

so that $x \in (A \cup B\ ) \cup C$

Hence the proof.

(ii) $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Ans: We have $\bar{A} \cup \bar{B} = \{\, x \mid x \in \bar{A} \ and \ x \in \bar{B}$

$= \{\, x \mid x \notin A \ and \ x \notin B$

$= \{\, x \mid x \notin A \cup B\}$

$= \overline{A \cup B}$

Hence the proof.

Dimension of a set / Cardinality of a set:

The total number of elements in a set A are called dimension of a set or cardinality of a set and is denoted by $n(A),\ card\ (A),\ |A|$.

Addition Principle (Principle of inclusion-exclusion)/ Fundamental Counting Principle:

Let A and B be two finite sets. Then the number of elements in $A \cup B$ is equal to the sum of the number of elements in A and the number of elements in B minus the number of elements that are common to A and B. That is,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

If A and B are finite ***disjoint sets*** that is $A \cap B = \emptyset$ then $|A \cup B| = |A| + |B|$

Theorem:

If A, B and C are finite sets then

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Example:

A computer company requires 30 programmers to handle systems programming jobs and 40 programmers for applications programming. If the company appoints 55 programmers to carry out these jobs, how many of these perform jobs of both types? How many handle only system programming jobs? How many handle only applications programming?

Solution:

Let A denote the set of programmers who handle systems programming job and B the set of programmers who handle applications programming. Then $A \cup B$ is the set of programmers appointed to carry out these jobs.

From the data given we have, $|A| = 30, \quad |B| = 40, \quad |A \cup B| = 55$

From Addition rule we have, $\quad |A \cup B| = |A| + |B| - |A \cap B|$

Then, $\quad |A \cap B| = |A| + |B| - |A \cup B| = 30 + 40 - 55 = 15$

Thus 15 programmers perform both types of jobs.

The number of programmers who handle only systems programming job is

$$|A - B| = |A| - |A \cap B| = 30 - 15 = 15$$

The number of programmers who handle only applications programming is

$$|B - A| = |B| - |A \cap B| = 40 - 15 = 25$$

Cartesian Product: Given two sets A and B, the Cartesian product $A \times B$ is defined by $A \times B = \{(a, b) | a \in A, \ \ b \in B\}$

i.e., $A \times B$ is a set of ordered pairs

Example: $A = \{1, 2, 3\}, \ B = \{a, b, c\}$

$$A \times B = \{(1, a); (1, b);\ (1, c); (2, a); (2, b); (2, c); (3, a); (3, b); (3, c)\}$$

It is to be noted that $A \times B$ may or may not be equal to $B \times A$.

What is $A \times A$?

The cartesian product of A itself.

Example: $A = \{1,2,3\}$

$$A \times A = \{(1,1); (1,2);\ (1,3); (2,1); (2,2); (2,3); (3,1); (3,2); (3,3)\}$$

Theorem1: For any two finite, non empty sets A and B, $|A \times B| = |A||B|$

i.e. $dimension\ \ A \times B = (dimension\ A)(dimension\ B)$

Proof: Let $|A| = m$ and $|B| = n$

The elements of $A \times B$ are ordered pairs in which first element belongs to the A and second element belongs to set B. e.g. $(x, y) \in A \times B$ where $x \in A\ and\ y \in B$.

There are n ways to chose $x \in A$ for the first position in ordered pair and m ways to choose $y \in A$ for second position in the ordered pair. So, by Multiplication principle there are $m \times n$ ways to form an order pair (a, b).

i.e. $|A \times B| = m\ n = |A||B|$

*Multiplication Principle: Suppose that two tasks $T_1\ and\ T_2$ are to be performed in sequence. If T_1 can be performed in n_1 ways and T_2 can be performed in n_2 ways then the sequence T_1T_2 can be performed in n_1n_2 ways.

Problem:

For any three sets A , B and C prove that

I. $\boldsymbol{A \times (B \cup C) = (A \times B) \cup (A \times C)}$
II. $\boldsymbol{A \times (B \cap C) = (A \times B) \cap (A \times C)}$

Solution:

I. Consider $A \times (B \cup C) = \{(x, y) | x \in A \text{ and } y \in (B \cup C)\}$

$$= \{(x, y) | x \in A \text{ and } (y \in B \text{ or } y \in C)\}$$

$$= \{(x, y) | (x \in A \text{ and } y \in B) \text{ or } (x \in A \text{ and } y \in C)\}$$

$$= (A \times B) \cup (A \times C)$$

$$\Longrightarrow A \times (B \cup C) = (A \times B) \cup (A \times C)$$

II. Consider $A \times (B \cap C) = \{(x, y) | x \in A \text{ and } y \in (B \cap C)\}$

$$= \{(x, y) | x \in A \text{ And } (y \in B \text{ and } y \in C)\}$$

$$= \{(x, y) | (x \in A \text{ And } y \in B) \text{ and } (x \in A \text{ And } y \in C)\}$$

$$= (A \times B) \cap (A \times C)$$

$$\Longrightarrow A \times (B \cap C) = (A \times B) \cap (A \times C)$$

<u>Number Theory</u>

Division Algorithm:

Theorem1.1: If $\boldsymbol{a}$ and $\boldsymbol{b}$ are integers with $\boldsymbol{b} > 0$, then there is a unique pair of integers $\boldsymbol{q}$ and $\boldsymbol{r}$ such that $\boldsymbol{a = qb + r}$ and $\boldsymbol{0 \leq r} < b$.

Example: If $a = 9$ and $b = 4$ then we have $9 = 2 \times 4 + 1$ with $0 \leq 1 < 4$, so $q = 2$ and $r = 1$; if $a = -9$ and $b = 4$ then $q = -3$ and $r = 3$.

In Theorem 1.1, we call q the quotient and r the remainder. By dividing by b, so that $\boldsymbol{\frac{a}{b} = q + \frac{r}{b}}$ **and** $\boldsymbol{0 \leq \frac{r}{b}} < 1$**,**

We see that q is the integer part $\lfloor a/b \rfloor$ of a/b, the greatest integer $i \leq a/b$. This makes it easy to calculate q, then to find $r = a - qb$.

We can now deal with the case $b < 0$; since $-b > 0$, Theorem 1.1 implies that there exist integers $q = -q^*$ we again have $a = qb + r$. Uniqueness is proved as before, so combining this with Theorem 1.1 we have:

Corollary: If a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.
(Note that when $b < 0$ we have $\frac{a}{b} = q + \frac{r}{b}$ and $0 \geq \frac{r}{b} > -1$, So that in this case q is $\lceil a/b \rceil$, the least integer $i \geq a/b$.)

To illustrate the Division Algorithm when b < 0, let us take b = -7. Then, for the choices of a = 1, -2, 61, and -59, we obtain the expressions

1=0(-7) + 1
-2 = 1(-7) + 5
61 = (-8)(-7)+5
-59 = 9(-7) + 4

- We wish to focus our attention on the applications of the Division Algorithm, and not so much on the algorithm itself.
- As a first illustration, note that with b = 2 the possible remainders are r = 0 and r = 1. When r = 0, the integer a has the form a = 2q and is called even; when r = 1, the integer a has the form a = 2q + 1 and is called odd.
- Now a^2 is either of the form $(2q)^2$ = 4k or $(2q+1)^2$= $4(q^2+q)$+1 = 4k+ 1.
- The point to be made is that the square of an integer leaves the remainder 0 or 1 upon division by 4.
- We also can show the following: the square of any odd integer is of the form 8k+ 1.
- For, by the Division Algorithm, any integer is representable as one of the four forms: 4q, 4q + 1, 4q + 2, 4q + 3.
- In this classification, only those integers of the forms 4q + 1 and 4q + 3 are odd. When the latter are squared, we find that
  $(4q+1)^2 = 8(2q^2+q)+1 = 8k+1$
  and similarly, $(4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1$

As examples, the square of the odd integer 7 is 7^2 = 49 = 8 · 6 + 1, and the square of 13 is 13^2 = 169 = 8 · 21 + 1.

As these remarks indicate, the advantage of the Division Algorithm is that it allows us to prove assertions about all the integers by considering only a finite number of cases. Let us illustrate this with one final example.
Example: We propose to show that the expression $a(a^2+2)/3$ is an integer for all $a \geq 1$. According to the Division Algorithm, every a is of the form $3q$, $3q+1$ or $3q+2$.

Assume the first of these cases. Then

$$\frac{a(a^2+2)}{3} = q(9q^2+2)$$

which clearly is an integer. Similarly, if $a = 3q + 1$, then

$$\frac{(3q+1)((3q+1)^2+2)}{3} = (3q+1)(3q^2+2q+1)$$

and $a(a^2+2)/3$ is an integer in this instance also. Finally, for $a = 3q + 2$, we obtain

$$\frac{(3q+2)((3q+2)^2+2)}{3} = (3q+2)(3q^2+4q+2)$$

an integer once more. Consequently, our result is established in all cases.

Example: Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Solution:

Let $A = \{x \in N|\ x\ \leq 2076$ and divisible by $4\}$ and $B = \{x \in N | x \leq 2076$ and divisible by $5\}$.

Then $|A \cup B| = |A| + |B| - |A \cap B|$

$$= \lfloor 2076/4 \rfloor + \lfloor 2076/5 \rfloor - \lfloor 2076/20 \rfloor$$

$$= 519 + 415 - 103 = 831$$

Thus, among the first 2076 positive integers, there are 2076-831=1245 integers not divisible by 4 or 5.

Example : Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7.

Solution: Let A, B and C denote the sets of positive integers ≤ 3000 and divisible by 3, 5, or 7.

By the inclusion-exclusion principle,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

$$= \lfloor 3000/3 \rfloor + \lfloor 3000/5 \rfloor + \lfloor 3000/7 \rfloor - \lfloor 3000/15 \rfloor - \lfloor 3000/35 \rfloor - \lfloor 3000/21 \rfloor + \lfloor 3000/105 \rfloor$$

=1000+600+428-200-85-142+28=1629

Base-b Representation:

The division algorithm can be used to convert a decimal integer to any other base. Furthermore, additions and multiplications can be carried out in any base, and subtraction can be accomplished using addition, as in base ten.

In everyday life, we use the decimal notation, base 10, to represent any real number.

For example, 234 = $2(10^2) + 3(10^1) + 4(10^0)$ which is the **decimal expansion** Of 234.

Likewise, 23.45 = $2(10^1) + 3(10^0) + 4(10^{-1}) + 5(10^{-2})$. Computers use base two (binary); very long binary numbers are often handled by human beings using base eight (**octal**) and base sixteen (**hexadecimal**).

Actually, any positive integer $b \geq 2$ is a valid choice for a base. This is a consequence of the following fundamental result, the proof of which is a bit long but straightforward.

Definition (**Base-b Representation): The expression $\boldsymbol{a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0}$ is the base-b expansion of the integer N. Accordingly $\boldsymbol{N = (a_k a_{k-1} \ldots a_1 a_0)_b}$ in case $\boldsymbol{b}$.**

- When the base is two, the expansion is called the **binary expansion**. When b = 2, each coefficient is 0 or 1; these two digits are called **bi**nary digi**ts** (or **bits**).

- The number system with base ten is the **decimal system**, from the Latin word *decem*, meaning ten. The decimal system employs the ten digits 0 through 9 to represent any number.
- The principal reason for this choice is undoubtedly that in earlier times men and women used their fingers for counting and computing, as some still do today.
- The base is omitted when it is ten. For example, 234_{ten}= 234 and $(10110)_{two} = 22$ (see the following example)
- When the base is greater than ten, we use the letters *A*,*B*,*C*, . . . to represent the *digits* ten, eleven, twelve, . . . respectively, to avoid any possible confusion. It is easy to find the decimal value of an integer from its base-*b* representation, as the next two examples illustrate.

Example: Express 10110_{two} in base ten.

Solution: $10110_{two} = 1(2^4) + 0(2^3) + 1(2^2) + 1(2^1) + 0(2^0)$

$$= 16 + 0 + 4 + 2 + 0 = 22$$

Example: Express $3ABC_{sixteen}$ in base ten.

Solution: Recall that A=10, B=11, and C=12. Therefore,

$$3ABC_{sixteen} = 3(16^3) + 10(16^2) + 11(16^1) + 12(16^0)$$

$$= 12{,}288 + 2560 + 176 + 12 = 15{,}036$$

Example: Express 3014 in base eight.

Solution:

The largest power of 8 that is contained in 3014 is 512. Apply the division algorithm with 3014 as the dividend and 512 as the divisor:

$$3014 = 5 \cdot 512+454$$

Now look at 454. It lies between 64 and 512. The largest power of 8 we can now use is 64:

$$454 = 7 \cdot 64+6$$

Continue like this until the remainder becomes less than 8:

$$6 = 6 \cdot 1+0$$

Thus, we have

$$\begin{aligned} 3014 &= 5(512) + 7(64) + 6 \\ &= 5(8^3) + 7(8^2) + 0(8^1) + 6(8^0) \\ &= 5706_{\text{eight}} \end{aligned}$$

Example: Represent 15,036 in the **hexadecimal system**, that is, in base sixteen.

Solution: We have

$$\begin{array}{rcrcrcr} \mathbf{15036} & = & \mathbf{939} & . & \mathbf{16} & + & \mathbf{12} \\ \mathbf{939} & = & \mathbf{58} & . & \mathbf{16} & + & \mathbf{11} \\ \mathbf{58} & = & \mathbf{3} & . & \mathbf{16} & + & \mathbf{10} \\ \mathbf{3} & = & \mathbf{0} & . & \mathbf{16} & + & \mathbf{3} \end{array} \qquad \begin{array}{c} \uparrow \\ \textbf{read up} \end{array}$$

Thus, 15,036 = $3ABC_{sixteen}$

Number Patterns:

Number patterns are fun for both amateurs and professionals. Often we would like to add one or two rows to the pattern, so we must be good at pattern recognition to succeed in the art of **inductive reasoning**. It takes both skill and ingenuity. In two of the following examples, mathematical proofs establish the validity of the patterns.

The following fascinating number pattern† was published in 1882 by the French mathematician François-Edouard-Anatole Lucas.

Example:

Study the following number pattern and add two more lines.

$$\begin{aligned} 1 \cdot 9 + 2 &= 11 \\ 12 \cdot 9 + 3 &= 111 \\ 123 \cdot 9 + 4 &= 1111 \end{aligned}$$

$$1234 \cdot 9 + 5 = 11111$$
$$12345 \cdot 9 + 6 = 111111$$
$$123456 \cdot 9 + 7 = 1111111$$

Solution:

Although the pattern here is very obvious, let us make a few observations, study them, look for a similar behavior, and apply the pattern to add two more lines:

- The LHS of each equation is a sum of two numbers. The first number is a product of the number 123 . . . *n* and 9.

- The value of *n* in the first equation is 1, in the second it is 2, in the third it is 3, and so on.

- Take a look at the second addends on the LHS: 2, 3, 4, 5, ... It is an increasing sequence beginning with 2, so the second addend in the *n*th equation is $n+1$.

- The RHS of each equation is a number made up of 1s, the *n*th equation containing $n + 1$ ones.

Thus, a pattern emerges and we are ready to state it explicitly: The first number in the *n*th line is 123 . . . *n*; the second number is always 9; the second addend is $n+1$; and the RHS is made up of $n+1$ ones.

So the next two lines are

$$1234567 \cdot 9 + 8 = 11111111$$
$$12345678 \cdot 9 + 9 = 111111111$$

The following pattern is equally charming.

Example:

Study the number pattern and add two more rows:

$$1 \cdot 8 + 1 = 9$$
$$12 \cdot 8 + 2 = 98$$
$$123 \cdot 8 + 3 = 987$$
$$1234 \cdot 8 + 4 = 9876$$
$$12345 \cdot 8 + 5 = 98765$$
$$123456 \cdot 8 + 6 = 987654$$

Solution:

A close look at the various rows reveals the following pattern: The first factor of the product on the LHS of the *n*th equation has the form 123 . . . *n*; the second factor is always 8. The second addend in the equation is *n*. The number on the RHS of the *n*th equation contains *n* digits, each begins with the digit 9, and the digits decrease by 1.

Thus the next two lines of the pattern are

$$1234567 \cdot 8 + 7 = 9876543$$
$$12345678 \cdot 8 + 8 = 98765432$$

Example: Establish the validity of the number pattern in Example 15.

Solution: We would like to prove that $123\ldots n \times 9 + (n+1) = \underbrace{11\ldots 11}_{\text{n+1 ones}}$

$$\text{LHS} = 123\ldots n \times 9 + (n+1)$$

$$= 9(1\,.\,10^{n-1} + 2\,.\,10^{n-2} + 3\,.\,10^{n-3} + \ldots + n) + (n+1)$$

$$= (10-1)(1\,.10^{n-1} + 2\,.\ 10^{n-2} + 3\,.10^{n-3} + \ldots + n\,) + (n+1)$$

$$= (\,10^{n} + 2\,.\ 10^{n-1} + \ldots + n\,.10) - (\,10^{n-1} + 2\,.\ 10^{n-2} + \ldots + n\,) + (n+1)$$

$$= (\,10^{n} + 10^{n-1} + 10^{n-2} \ldots + 10 + 1)$$

$$= \underbrace{11 \ldots 11}_{n+1\ \ ones}$$

$$= RHS$$

(It would be interesting to see if this result holds for any positive integer *n*; try it.)

Example:

Add two more rows to the following pattern, conjecture a formula for the *n*th row, and prove it:

9 · 9 + 7 = 88
98 · 9 + 6 = 888
987 · 9 + 5 = 8888
9876 · 9 + 4 = 88888
98765 · 9 + 3 = 888888

Solution:

- The next two rows of the pattern are

  987654 · 9 + 2 = 8888888
  9876543 · 9 + 1 = 88888888

- The general pattern seems to be

  $$987\ldots(10-n)\ .\ 9 + (8-n) = \underbrace{888 \ldots 888}_{n+1\ \ eights}\,, \qquad 1 \le n \le 8$$

- To provide the conjecture:

  LHS = $987\ldots(10-n)\ .\ 9 + (8-n)$

  $$= (10-1)[9\ .\ 10^{n-1} + 8\ .\ 10^{n-2} + 7\ .\ 10^{n-3} + \ldots + (11-n)10 + (10-n)] + (8-n)$$

$=[9\ .\ 10^n + 8\ .\ 10^{n-1} +\ \ldots + (11-n)10^2 + (10-n)10] -$
$[9\ .\ 10^{n-1} + 8\ .\ 10^{n-2} +\ 7\ .\ 10^{n-3} +\ \ldots + (11-n)10 + (10-n)] +$
$(8-n)$

$$= 9\ .\ 10^n - (10^{n-1} + 10^{n-2} + \cdots + 10) - (10-n) + (8-n)$$

$$= 9\ .\ 10^n - (10^{n-1} + 10^{n-2} + \cdots + 10 + 1) - 1$$

$$= 10\ .\ 10^n - (10^n + 10^{n-1} + \cdots + 10 + 1) - 1$$

$= 10^{n+1} - \frac{10^{n+1}-1}{9} - 1$, since $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1} (r \neq 1)$

$$= \frac{8(10^{n+1}-1)}{9}$$

But $10^{n+1} - 1 = \underbrace{99 \ldots 99}_{n+1\ nines}$

So $\frac{10^{n+1}-1}{9} = \underbrace{11 \ldots 11}_{n+1\ ones}$

Therefore, $LHS = \frac{8(10^{n+1}-1)}{9} = \underbrace{88 \ldots 88}_{n+1\ eights} = RHS$

<u>Prime and Composite Numbers</u>:

Prime numbers are the building blocks of positive integers. Two algorithms are often used to determine whether a given positive integer is a prime.

Some positive integers have exactly two positive factors and some have more than two. For example, 3 has exactly two positive factors: namely, 1 and 3; whereas 6 has four: 1, 2, 3, and 6. Accordingly, we make the following definition.

<u>Prime and Composite Numbers:</u>

A positive integer > 1 is a **prime number** (or simply a **prime**) if its only positive factors are 1 and itself. A positive integer > 1 that is not a prime is a **composite**

number (or simply a **composite**).

Notice that, by definition, 1 is neither a prime nor a composite. It is just the multiplicative identity or the **unit**.

The first ten primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29; the first ten composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16, and 18.

It follows from the definition that the set of positive integers can be partitioned into three disjoint classes: the set of primes, the set of composites, and $\{1\}$.

How many primes are there? Is there a systematic way to determine whether a positive integer is a prime?

To answer the first question, we need the following lemma, which we shall prove by induction. It can also be proved by contradiction .

Lemma: Every integer $n \geq 2$ has a prime factor.

Proof: (by strong Induction)

The given statement is clearly true when $n = 2$. Now assume it is true for every positive integer $n \leq k$, where $k \geq 2$. Consider the integer $k + 1$.

case 1 If k +1 is a prime, then k + 1 is a prime factor of itself.

case 2 If k + 1 is not a prime, k + 1 must be a composite, so it must have a factor $d \leq k$. Then, by the inductive hypothesis, d has a prime factor p. So p is a factor of k +1, by following Theorem .

Theorem2: Let a, b, c, α, and β be any integers.† Then
1. If $a|b$ and $b|c$, then $a|c$. (**transitive property**)
2. If $a|b$ and $a|c$, then $a|(\alpha b + \beta c)$.
3. If $a|b$, then $a|bc$.

The expression $\alpha b + \beta c$ is called a **linear combination** of b and c

Thus, by the strong version of induction, the statement is true for every integer ≥ 2; that is, every integer ≥ 2 has a prime factor. (Proved)

Example: Determine whether 1601 is a prime number.

Solution: First list all primes $\leq \lfloor\sqrt{1601}\rfloor$. They are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37. Since none of them is a factor of 1601 (verify), 1601 is a prime.

Theorem 3: Let $p_1, p_{2,} \dots p_t$ be the primes $\leq \sqrt{n}$. Then

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_{j} p_k} \right\rfloor + \cdots + (-1)^t \left\lfloor \frac{n}{p_1 p_2 \dots p_t} \right\rfloor$$

The following example illustrates this result.

Example: Using Theorem 3, find the number of primes ≤ 100.

Solution: Here $n = 100$. Then $\pi(\sqrt{n}) = \pi(\sqrt{100}) = \pi(10) = 4$ (see figure 2.25)

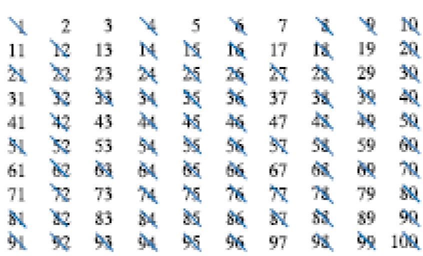

Figure 2.25

The four primes ≤ 10 are 2, 3, 5, and 7; call them $p_1, p_2,\ p_3, and\ \ p_4$, respectively. Then, by Theorem 3,

$$\pi(100) = 100 - 1 + 4 - \left(\left\lfloor\frac{100}{2}\right\rfloor + \left\lfloor\frac{100}{3}\right\rfloor + \left\lfloor\frac{100}{5}\right\rfloor + \left\lfloor\frac{100}{7}\right\rfloor\right)$$
$$+ \left(\left\lfloor\frac{100}{2.3}\right\rfloor + \left\lfloor\frac{100}{2.5}\right\rfloor + \left\lfloor\frac{100}{2.7}\right\rfloor + \left\lfloor\frac{100}{3.5}\right\rfloor + \left\lfloor\frac{100}{3.7}\right\rfloor + \left\lfloor\frac{100}{5.7}\right\rfloor\right)$$
$$- \left(\left\lfloor\frac{100}{2.3.5}\right\rfloor + \left\lfloor\frac{100}{2.3.7}\right\rfloor + \left\lfloor\frac{100}{2.5.7}\right\rfloor + \left\lfloor\frac{100}{3.5.7}\right\rfloor\right) + \left\lfloor\frac{100}{2.3.5.7}\right\rfloor$$

= 103−(50 +33+ 20+14) + (16 +10+7 +6+ 4+2)−(3 +2 +1+ 0) + 0
= 25

THEOREM 4: For every positive integer *n*, there are *n* consecutive integers that are composite numbers.

EXAMPLE: Find six consecutive integers that are composites.

Solution:

By Theorem 4, there are six consecutive integers beginning with (*n* + 1)! + 2 = (6 + 1)! + 2 = 5042, namely, 5042, 5043, 5044, 5045, 5046, and 5047. (You may notice from Figure 2.25 that the smallest consecutive chain of six composite numbers is 90, 91, 92, 93, 94, and 95.)

Example: Prove that there are at least $3\lfloor n/2\rfloor$ primes in the range *n* through *n*!, where $n \geq 4$.

Proof:

Notice that the statement is true for $4 \leq n \leq 9$. So assume $n \geq 10$.
case 1 Suppose n is even, say, n = 2k, where $k \geq 5$. Then
$n! = 1 \cdot 2 \cdot 3 \cdots (2k-2)(2k-1)n$
$= 2^k[1 \cdot 2 \cdot 3 \cdots (k-1)][1 \cdot 3 \cdot 5 \cdots (2k-1)]n$
$> 2^{k-1}(k-1)!\ 2^{k+2}n$
$\geq 2^{k-1}.\ 2^{k-1}.\ 2^{k+2}\ n,$ since $k \geq 5$

$= 2^{3k}n$

A repeated application of Bertrand's conjecture shows there are at least $3k$ = 3(n / 2) = $3\lfloor n/2 \rfloor$ primes in the range n through $2^{3k}n$, that is, between n and $n!$.

case 2 Suppose n is odd, say, $n = 2k + 1$, where $k \geq 5$. Then

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdot \cdot (2k-1)(2k)n$$
$$= 2^k k![1 \cdot 3 \cdot 5 \cdot \cdot \cdot (2k-1)]n$$
$$> 2^k . 2^k . 2^{k+2} n, \text{ since } k \geq 5$$
$$> 2^{3k}n$$

Thus, as before, there are at least 3k = 3[(n−1)/2)] = $3\lfloor n/2 \rfloor$ primes in the range n through $2^{3k}n$, that is, between n and $n!$.

Thus, in both cases, the result is true.

<u>Example:</u>

Find the primes such that the digits in their decimal values alternate between 0s and 1s, beginning with and ending in 1.

Solution:

Suppose N is a prime of the desired form and it contains n ones. Then

$$N = 10^{2n-2} + 10^{2n-4} + \cdots + 10^2 + 1$$

$= \frac{10^{2n}-1}{10^2-1}$ since $\sum_{i=0}^{n-1} r^i = \frac{r^n-1}{r-1}, r \neq 1$

$= \frac{(10^n-1)(10^n+1)}{99}$

If $n = 2$, then $N = \frac{(10^2-1)(10^2+1)}{99} = 101$ is a prime. If $n > 2$, $10^n - 1 > 99$ and $10^n + 1 > 99$. Then N has nontrivial factors, so N is composite. Thus, 101 is the only prime with the desired properties.