1. Sets and Numbers

1.1 Introduction

1.2 Sets, Subsets and Elements

1.2.1 Sets
1.2.2 Notation
1.2.3 Equality of sets
1.2.4 Universal set
1.2.5 Empty set
1.2.6 Subsets
1.2.7 Disjoint sets
1.2.8 Sets of numbers

1.3 Venn Diagrams

1.4 Set Operations

1.4.1 Union
1.4.2 Intersection
1.4.3 Difference
1.4.4 Complement

1.5 Algebra of Sets

1.6 Application of Venn Diagrams in Counting

1.7 Mathematical Induction

1.7.1 Introduction
1.7.2 Mathematical induction

1.8 Modular Arithmetic

1.8.1 Introduction
1.8.2 Definition
1.8.3 Applications of integer modular in computer science

1.9 Reference

1. Sets and Numbers

1.1 Introduction

Sets are used to group objects together. Often, the objects in a set have similar properties. For example, all the students who are studying in this college make up a set. All students who are studying in this course also make up a set.

Set is a fundamental discrete structure on which all other discrete structures are built such as graphs, combinations etc. (Here discrete means consisting of distinct or unconnected elements.) Discrete structures are used in modelling and problem solving. There are many applications on the use of discrete structures in data storage, data communication and manipulation of data.

1.2 Sets, Subsets and Elements

1.2.1 Sets

A set is a collection of objects called "elements" or "members" of the set.

We usually use capital letters, A, B, C, ..., to denote sets and lowercase letters, a, b, c, ..., to denote elements of sets.

Example 1.2 - 1 $A = \{a, e, i, o, u\}$ is a set and a list of all its elements is given.

Example 1.2 - 2 $B = \{x : x \text{ is an integer}, x > 0\}$

Consider the set $C = \{1, 3, 5, 7, 9\}$. We write $3 \in C$ to mean that 3 belongs to the set C, and $-5 \notin C$ to mean that -5 does not belong to C.

1.2.2 Notation

There are two ways to specify a particular set:

1) To list all its elements if it is possible as given in example 1. It is read as "A is the set whose elements are the letters a, e, i, o and u". Note that elements are separated by commas and enclosed in braces { }.

2) To state the property which characterises the elements in the set as given in example 2. It is read as "B is the set of x such that x is an integer and x is greater than 0". A letter, usually x, is used to denote a typical members of the set, the colon is read as "such that" and the comma as "and".

Even if we can list the elements of a set, it may not be practical to do so. For example, we would not list the members of the set of people born in the world during the year 1990 although theoretically it is possible to compile such a list. That is, we describe a set by listing its elements only if the set contains a few elements, otherwise we describe a set by the property which characterises its elements.

1.2.3 Equality of Sets

Two sets are equal if and only if they have exactly the same elements. i.e. if every element which belongs to A also belongs to B and if every element which belongs to B also belongs to A.

Example 1.2-3 Let $A = \{a, e, i, o, u\}$, $B = \{u, o, i, e, a\}$ and $C = \{a, a, e, i, i, o, u\}$

then $A = B = C$

1.2.4 Universal Set

A universal set U is a set that contains all the objects under consideration.

Example 1.2 - 4
A = {all students in this campus}
B = {all full-time students in this campus}
C = {all students in this lecture theatre}

1.2.5 Empty Set

A set which contains no elements is called the empty set or null set and is denoted by ∅.

Example 1.2 - 5 Let $X = \{y : y^2 = 4,\ y \text{ is odd}\}$

then X is the empty set or $X = \varnothing$.

1.2.6 Subsets

The set A is said to be a subset of B if every element of A is also an element of a set B. It is denoted by

$A \subset B$ read as "A is a subset of B" or
$B \supset A$ read as "B contains A".

If A is not a subset of B then it is denoted by $A \not\subset B$.

Example 1.2 - 6 Let $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 4, 5\}$

then $A \subset B$ *or* $B \not\subset A$

1.2.7 Disjoint Sets

If sets A and B have no elements in common, then we say that A and B are disjoint. i.e. no element of A is in B and no element of B is in A.

Example 1.2 - 7 Let $A = \{1, 3, 5, 7\}$ and $B = \{2, 4, 6, 7\}$

then A and B are not disjoint since 7 is in both sets.
i.e. $7 \in A$ and $7 \in B$.

1.2.8 Sets of Numbers

Some sets of numbers occur very often and special symbols are use for them.

$\boldsymbol{Z}$ = set of all integers
e.g. $\{ 0, -2, 5, 3, -6, 12, \ldots\ldots \}$

$\boldsymbol{Z}^+$ = set of positive integers (or natural numbers)
= $\{x : x \in \boldsymbol{Z} \text{ and } x > 0\}$
e.g. $\{ 1, 3, 5, 7, 9, \ldots\ldots \}$

$\boldsymbol{N}$ = set of non-negative integers
= $\{x : x \in \boldsymbol{Z} \text{ and } x \geq 0\}$
e.g. $\{ 0, 1, 2, 3, 4, \ldots\ldots \}$

$\boldsymbol{Q}$ = set of rational numbers
= $\{x / y : x, y \in \boldsymbol{Z} \text{ and } y \neq 0\}$
e.g. $\{ 1/3, 7/4, -5/9, \ldots\ldots \}$

$\boldsymbol{R}$ = set of real numbers
e.g. $\{ -2/3, -4, 0, 5, 4/9, \ldots\ldots \}$

The above sets are related as follows:

$$\boldsymbol{Z}^+ \subset \boldsymbol{N} \subset \boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R}$$

1.3 Venn Diagrams

A Venn diagram is a pictorial representation of sets by sets of points in the plane. The universal set ***U*** is represented by the interior of a rectangle, and the other sets are represented by disks lying within the rectangle.

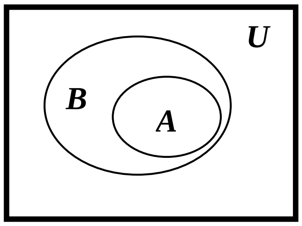


Figure 1

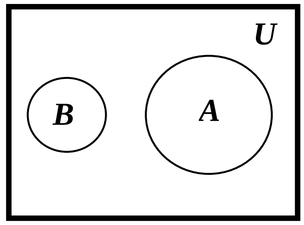


Figure 2

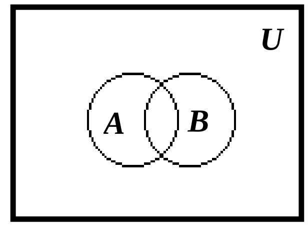


Figure 3

Figure 1 represents $A \subset B$ and $A \neq B$.
Figure 2 represents A and B are disjoint.
Figure 3 represents A and B are not disjoint.

1.4 Set Operations

1.4.1 Union, ∪

The union of two sets *A* and *B*, denoted by $A \cup B$, is the set of all elements which belong to *A* or to *B* or to both. i.e.

$$A \cup B = \{x : x \in A \ \ or \ \ x \in B\}$$

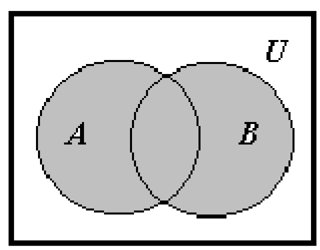


Figure 4 $A \cup B$ is shaded.

Example 1.4 - 1 Let $A = \{ a, b, c \}$, $B = \{ 1, 2, 3 \}$ and $C = \{ a, c, e, 1, 3, 5 \}$,

then $A \cup B = \{ a, b, c, 1, 2, 3 \}$

$B \cup C = \{ 1, 2, 3, 1, c, e, 5 \}$

$C \cup A = \{ a, c, e, 1, 3, 5, b \}$

1.4.2 Intersection, $\cap$

The intersection of two sets *A* and *B*, denoted by $A \cap B$, is the set of elements, which are common to both *A* and *B*. i.e.

$$A \cap B = \{ x : x \in A \text{ and } x \in B \}$$

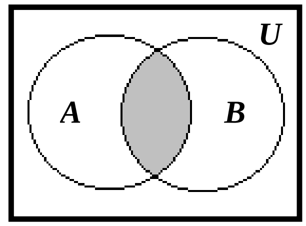


Figure 5 $A \cap B$ is shaded.

Note : If $A \cap B = \varnothing$ then *A* and *B* are disjoint.

Example 1.4-2 Let $A = \{ a, b, c, d, e \}$, $B = \{ c, d, e, f, g \}$ and $C = \{ a, e, i, o, u \}$,

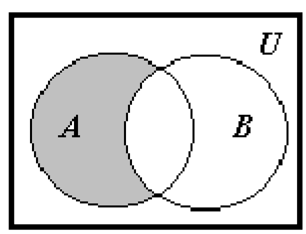
then $A \cap B = \{ c, d, e \}$

$B \cap C = \{ e \}$

$C \cap A = \{ a, e \}$

1.4.3 Difference \

The difference of set *A* and *B*, denoted by $A \setminus B$ is the set of elements which belong to *A* but which do not belong to *B*. i.e.



$$A \setminus B = \{ x : x \in A, \ x \notin B \}$$

Figure 6 $A \setminus B$ is shaded.

Example 1.4 - 3 Let $S = \{ a, b, c, d \}$ and $T = \{ c, d, e, f \}$,

then $S \setminus T = \{ a, b \}$

$T \setminus S = \{ e, f \}$

1.4.4 Complement, $\overline{A}$

The complement of a set A, denoted by $\overline{A}$, is the set of elements which do not belong to A, that is the difference of the universal set U and A. i.e.

$\overline{A} = \{ x : x \in U, x \notin A \}$

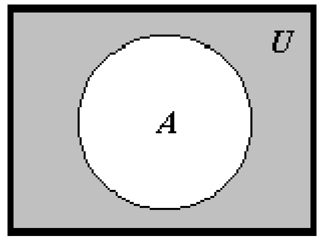


Figure 7 $\overline{A}$ is shaded.

Example 1.4-4 Let the universal set U be the English alphabet and $A = \{ a, b, c, x, y, z \}$

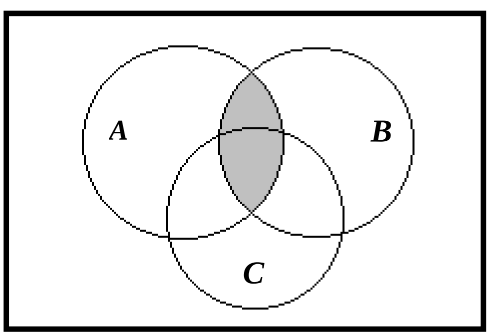
then $\overline{A} = \{ d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w \}$

Example 1.4 - 5 Use Venn diagrams to represent the following set expressions.

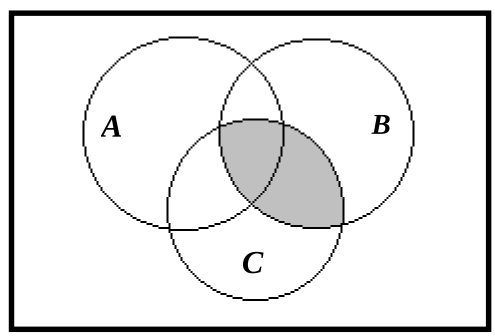
(a) $(A \cap B) \cup (B \cap C)$

(b) $A \cap (B \cup C) \cap (\overline{A} \cup \overline{B} \cup \overline{C})$

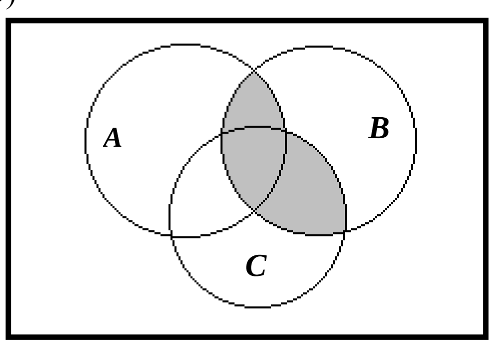
(a)



$(A \cap B)$

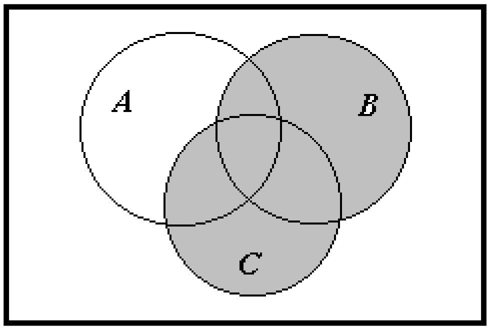


$(B \cap C)$

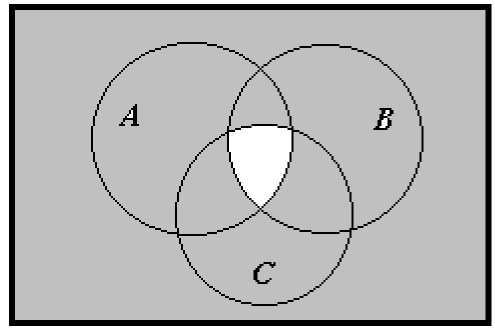


$(A \cap B) \cup (B \cap C)$

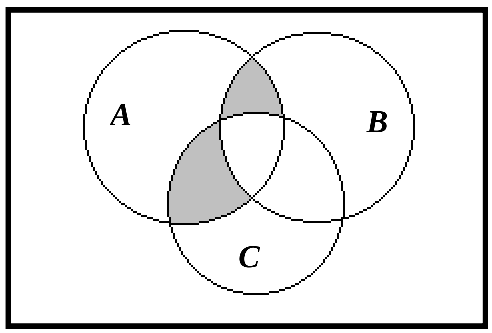
(b)



$(B \cup C)$



$(\overline{A} \cup \overline{B} \cup \overline{C})$



$A \cap (B \cup C) \cap (\overline{A} \cup \overline{B} \cup \overline{C})$

1.5 Algebra of Sets

Sets, under the operations of union, intersection and complement, satisfy the laws listed in the following table. We can use these laws of algebra of sets to simplify complicated set expressions. The following identities can be verified by drawing Venn diagrams.

Set identities

Identity laws	$A \cup \varnothing = A$	$A \cap U = A$
Idempotent laws	$A \cup A = A$	$A \cap A = A$
Inverse laws	$A \cup \overline{A} = U$	$A \cap \overline{A} = \varnothing$
Complementation laws	$\overline{(\overline{A})} = A$	
Domination laws	$A \cup U = U$	$A \cap \varnothing = \varnothing$
Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative laws	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$

Example 1.5 - 1 Let A, B and C be sets. Use laws of algebra of sets to simplify the following set expressions.

(a) $(A \cap B) \cup (B \cap C)$

(b) $(A \cap B) \cup (A \cap B \cap \overline{C} \cap D) \cup (\overline{A} \cap B)$

(a) $(A \cap B) \cup (B \cap C)$

$= (A \cap B) \cup (C \cap B)$ Commutative law

$= (A \cup C) \cap B$ Distributive law

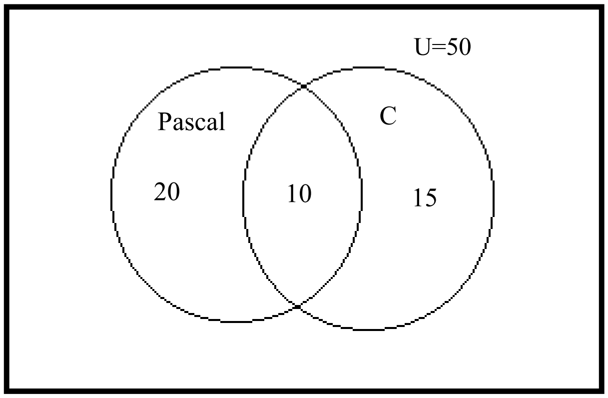
Now only two operators are needed.

(b) $(A \cap B) \cup (A \cap B \cap \overline{C} \cap D) \cup (\overline{A} \cap B)$

$= (A \cap B) \cup (\overline{A} \cap B) \cup (A \cap B \cap \overline{C} \cap D)$	Commutative law
$= (\ (A \cup \overline{A}) \cap B)\ ) \cup (A \cap B \cap \overline{C} \cap D)$	Distributive law
$= (U \cap B) \cup (A \cap B \cap \overline{C} \cap D)$	Inverse law
$= B \cup (A \cap B \cap \overline{C} \cap D)$	Domination law
$= B$	Absorption law

1.6 Application of Venn Diagrams in Counting

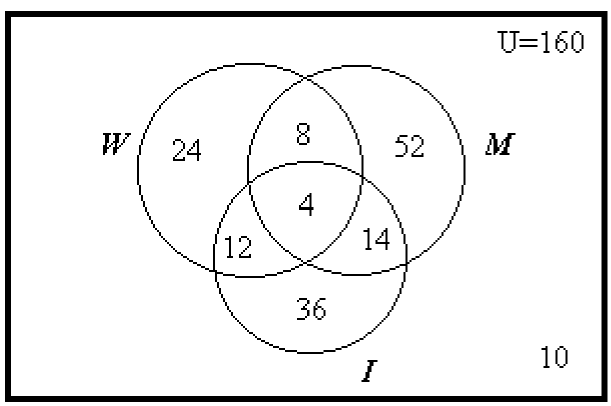
Example 1.6 - 1 In a class of 50 college students, 30 are studying Pascal, 25 are studying C and 10 are studying both computer languages. How many students do not study computer language ?



No. of students do not study computer language are
50 – 20 – 10 – 15 = 5 students

Example 1.6 - 2 In a survey of 160 passengers, an airline found that 48 preferred wine with their meals, 78 preferred mixed drinks, and 66 preferred ice tea. In addition, 12 enjoyed wine and mixed drinks, 18 enjoyed mixed drinks and ice tea, and 16 enjoyed ice tea and wine, and 4 passengers enjoyed them all.

a) How many passengers want only iced tea with their meals?
b) How many passengers do not like any of them?



a) The required number of passengers is 36

b) The required number of passengers is
160 – 24 – 52 – 36 – 12 – 8 – 14 – 4 = 10

1.7 Mathematical Induction

1.7.1 Introduction

Mathematical induction is an extremely important proof technique. It can be used to prove results about the complexity of algorithms, the correctness of certain types of computer programs, the mathematical theorems, a wide range of identities and inequalities and so on.

It is important to note that mathematical induction can be used only to prove results obtained in some other ways. It is not a tool for discovering formulae or theorems.

Consider the sum of the first n positive odd integers:

n	S_n		
1	1	= 1	$= 1^2$
2	1 + 3	= 4	$= 2^2$
3	1 + 3 + 5	= 9	$= 3^2$
4	1 + 3 + 5 + 7	= 16	$= 4^2$
5	……		

What is a formula for the sum of the first n positive odd integers?

From these values it is reasonable to guess that the sum of the first n positive odd integers is n^2. However, we need a method to prove whether or not this guess is correct.

1.7.2 Principle of Mathematical Induction

Many formulae like $1+2+......+n=\dfrac{n(n+1)}{2}$ can be proved to hold for every positive integer n by using mathematical induction which states that

> Suppose $P(n)$ is a statement in n for each positive integer n.
>
> If (step 1) $P(1)$ is true, and
>
> (step 2) for all positive integers $k \ge 1$, the assumption that $P(k)$ is true implies that $P(k+1)$ is true,
>
> then $P(n)$ is true for all positive integers n.

Example 1.7 - 1 Show that for every positive odd integer n,

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

Solution: Let $P(n)=1+3+5+......+(2n-1)=n^2$

When n = 1, L.H.S. of $P(1)=1$, R.H.S. of $P(1)=1$. $\therefore$ $P(1)$ is true.

Assume that $P(k)$ is true when $n = k$,

i.e. $P(k)=1+3+5+......+(2k-1)=k^2$

When $n = k+1$,

L.H.S. of $P(k+1)=1+3+5+......+(2k-1)+(2k+1)$

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

R.H.S. of $P(k+1)=(k+1)^2$ $\therefore$ $P(k+1)$ is true.

Since $P(n)$ holds for $n = k + 1$ whenever it holds for $n = k$. Therefore, the original formula holds for every positive odd integer n.

Example 1.7 - 2 Show that for every positive integer n,

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

Solution: Let $P(n)=1+2+3+......+n=\dfrac{n(n+1)}{2}$

When n = 1, L.H.S. of $P(1)=1$, R.H.S. of $P(1)=1$. $\therefore$ $P(1)$ is true.

Assume that $P(n)$ is true when $n = k$,

i.e. $P(k)=1+2+3+......+k=\dfrac{k(k+1)}{2}$

When $n = k+1$,

L.H.S. of $P(k+1)=1+2+3+......+k+(k+1)$

$$=\frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)+2(k+1)}{2}$$

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

R.H.S. of $P(k+1)=\dfrac{(k+1)(k+2)}{2}$ $\therefore$ $P(k+1)$ is true.

Since $P(n)$ holds for $n = k + 1$ whenever it holds for $n = k$, Therefore, the original formula holds for every positive n.

Example 1.7 - 3 Suppose we have stamps of two different denominations, 3 cents and 5 cents. Prove that it is possible to make up exactly any postage of 8 cents or more using stamps of these two denominations.

Solution: Let $P(n)$ be the statement that it is possible to make up exactly postage of n cents using stamps of these two denominations; where n is a positive integer greater than or equal to 8.

When $n = 8$,

$\because$ 8 cents = 3 cents + 5 cents

$\therefore$ $P(8)$ is true.

Assume that $P(k)$ is true for some positive integer $k \geq 8$,

i.e. it is possible to make up exactly a postage of k cents using 3-cent and 5-cent stamps.

For a postage of $k + 1$

We examine two cases:

Case 1

Suppose we make up a postage of k cents using at least one 5-cent stamp. Replacing a 5-cent stamp by two 3-cent stamps will yield a way to make up a postage of $k + 1$ cents.

Case 2

Suppose we make up a postage of k cents using 3-cent stamps only. Since $k \geq 8$, there must be at least three 3-cent stamps. Replacing three 3-cent stamps by two 5-cent stamps will yield a way to make up a postage of $k + 1$ cents.

Since $P(n)$ holds for $n = k + 1$ whenever it holds for $n = k$. Therefore, the original formula holds for every positive integer $n \geq 8$.

1.8 Modular Arithmetic

1.8.1 Introduction

In some situations we care only about the remainder of an integer when it is divided by some specified integer.

1.8.2 Definition

Let a be an integer and m be a positive integer, we use ***a* mod *m*** to denote the remainder when a is divided by m.

It follows from the definition that a mod m is the integer r such that

$a = qm + r$ and $0 \le r \le m$ i.e. r and m are positive.

Example 1.8 - 1

32 mod 5 = 2 i.e. $32 = 6 \times 5 + 2$

1997 mod 150 = 47 i.e. $1997 = 13 \times 150 + 47$

-64 mod 6 = 2 i.e. $-64 = -11 \times 6 + 2$

However, it is invalid if $-64 = (-10)(6) + (-4)$ because $r\,(-4)$ is not a positive number.

1.8.3 Applications of Integer Modular in Computer Science

1.8.3.1 Using Hashing Function to Assign Memory Locations to Computer Files.

One of the most common hashing function is

$h(k) = k$ mod m

where k is the key (reference) of a file and m is the number of available memory locations.

Because more than one file may be assigned to the same memory, when this happens, we say that a **collision** occurs. One way to resolve a collision is to assign the first free location following the occupied memory location. There are many sophisticated ways to resolve collisions that are more efficient than the simple method we have described.

Example 1.8 - 2 Assign a memory location to each of the following student numbers when m = 1024. Solve the problem if collisions occur.

Name	*Student number*	*Memory Location*
Peter	1234567	647
Michael	1352467	787
John	1347347	788

$h(1234567) = 1234567 \bmod 1024 = 647$
$h(1352467) = 1352467 \bmod 1024 = 787$
$h(1347347) = 1347347 \bmod 1024 = 787$

1.8.3.2 Pseudorandom Number Generator

Many computer software have the capability of generating random numbers for needs such as computer simulations and random sampling in statistics. Because numbers generated by systematic methods are not truly random, they are called pseudorandom numbers.

The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**. i.e.

$$x_{n+1} = (ax_n + c) \bmod m$$

where $2 \le a < m, 0 \le c < m \; and \; 0 \le x_0 < m$.

Example 1.8 - 3 The sequence of pseudorandom numbers generated by choosing $m = 9$, $a = 7$, $c = 4$ and $x_0 = 3$, can be found as follows:

$x_1 = 7x_0 + 4 = (7)(3) + 4 = 25 \text{mod} 9 = 7$

$x_2 = 7x_1 + 4 = (7)(7) + 4 = 53 \text{mod} 9 = 8$

$x_3 = 7x_2 + 4 = (7)(8) + 4 = 60 \text{mod} 9 = 6$

$x_4 = 7x_3 + 4 = (7)(6) + 4 = 46 \text{mod} 9 = 1$

$x_5 = 7x_4 + 4 = (7)(1) + 4 = 11 \text{mod} 9 = 2$

$x_6 = 7x_5 + 4 = (7)(2) + 4 = 18 \text{mod} 9 = 0$

$x_7 = 7x_6 + 4 = (7)(0) + 4 = 4 \text{mod} 9 = 4$

$x_8 = 7x_7 + 4 = (7)(4) + 4 = 32 \text{mod} 9 = 5$

$x_9 = 7x_8 + 4 = (7)(5) + 4 = 39 \text{mod} 9 = 3$

$x_{10} = 7x_9 + 4 = (7)(3) + 4 = 25 \text{mod} 9 = 7$

Since $x_9 = x_0$ and because each term depends only on the previous term, thus, this sequence contains nine different numbers before repeating.
The following sequence of numbers will be generated if we continue the process.

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, ...

1.8.3.3 Cryptology

One of the most important applications of modular arithmetic involves cryptology, which is the study of secret messages. One of the earliest known methods is the Caesar method. With this method messages are made secret by shifting each letter by k in the alphabet. For instance, using this scheme with $k = 3$, the letter C is sent to F and the Y is sent to B. This is an example of encryption, that is, the process of making a message secret.

Generalised Caesar's cipher process:

1. Choose a value of k where k is the number of letters to be shifted forward in the alphabet.
2. Replace each letter of the message by an integer p where $0 \le p \le 25$ based on its position in the alphabet.
3. Replace each number p by the following shift cipher function
$$f(p) = (p + k) \bmod 26$$
4. Translate the new number $f(p)$ back to letter based on its position in the alphabet.

Example 1.8 - 4 Find the secret message to represent the message "MEET YOU IN THE PARK" using Caesar cipher with $k = 3$.

Step 1:	$k = 3$				
Step 2:	12-4-4-19	24-14-20	8-13	19-7-4	15-0-17-10
Step 3:	15-7-7-22	1-17-23	11-16	22-10-7	18-3-20-13
Step 4:	"PHHW BRX LQ WKH SDUN"				

To recover the original message from a secret message encrypted by the Caesar cipher, the inverse function $f^{-1}(p) = (p - k) \bmod 26$ is used. The process of determining the original message from the encrypted message is called decryption.

Example 1.8 - 5 Find the original message of "FXAT QJZM" using Caesar cipher with $k = 9$.

Step 1: $k = 9$

Step 2: 5-23-0-19 16-9-26-12

Step 3: e.g. $5 - 9 = -4 \bmod 26 = 22 \Rightarrow W$ since

V	W	X	Y	Z	A	B
21	22	23	24	25	0	1

22, 14, 17, 10 7, 0, 17, 3

Step 4: "WORK HARD"

1.9 Reference

1.9.1 Discrete mathematics and its applications - Kenneth H. Rosen
McGraw-Hill international editions

1.9.2 Essential computer mathematics – Seymour Lipschutz
Schaum's outline series, McGraw-Hill international editions

1.9.3 http://www.CS.NMSU.Edu/~complog/sets/

1.9.4 http://www.cis.syr.edu/~sanchis/setory.html

1.9.5 http://www.csci.csusb.edu/dick/maths/intro_sets.html

1.9.6 http://www.math.ufl.edu/~jal/set_theory.html