SECURITY GOALS

- Data Confidentiality
  - Keep data and communication secret
  - Privacy of personal financial/health records, etc.
  - Military and commercial relevance
- Data Integrity
  - Protect reliability of data against tampering
  - Can we be sure of the source and content of information?
- System Availability
  - Data/resources should be accessible when needed
  - Protection against denial of service attacks

Cryptographic Attacks

Accessing of data by unauthorized entity is called as attack

Passive Attacks

Active Attacks

Passive Attacks:

In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system.

Active Attacks:

An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks.

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

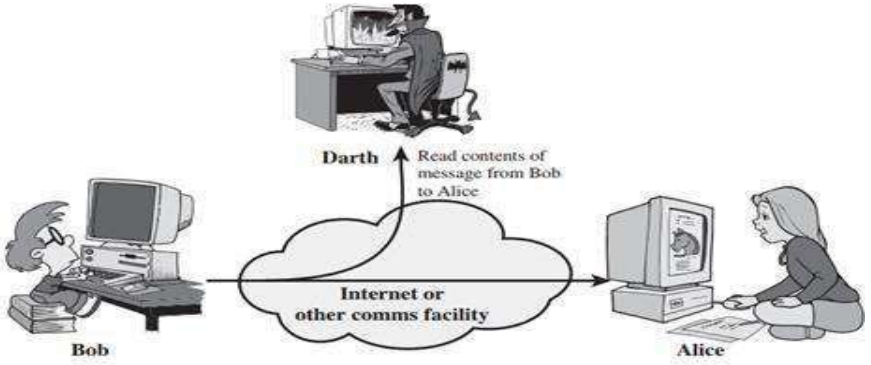
Passive Attacks

(a) Release of message content –

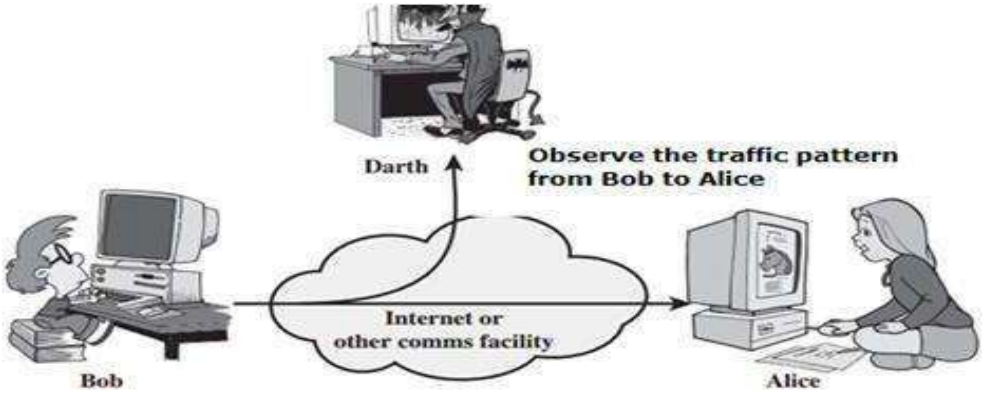
Capture and read the content transmissions.

(b) Traffic Analysis–

- can't read the information, but observe the pattern
- determine the location and identity of communicating parties
- observe frequency and length of communication



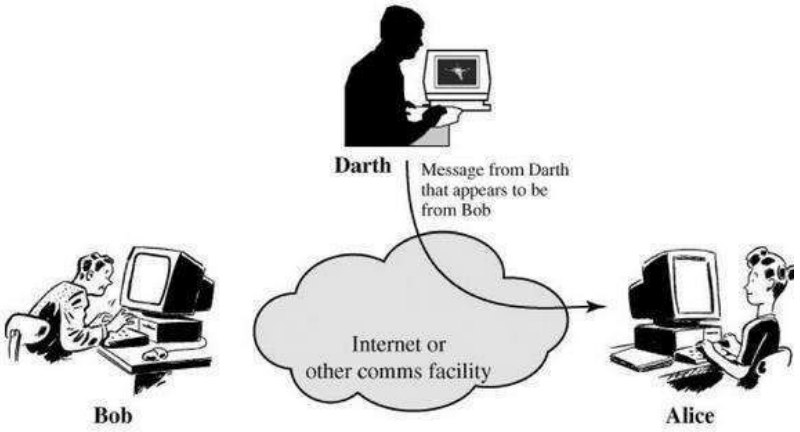
(a) Release of Message content



(b) Traffic Analysis

Active Attacks

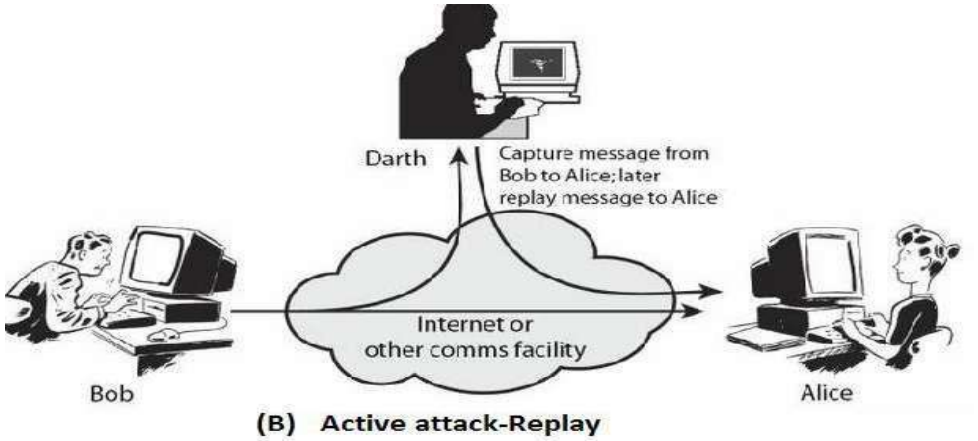
(a) Masquerading: Masquerading or snooping happens when the attacker impersonates somebody else.



Active Attack – Masquerade

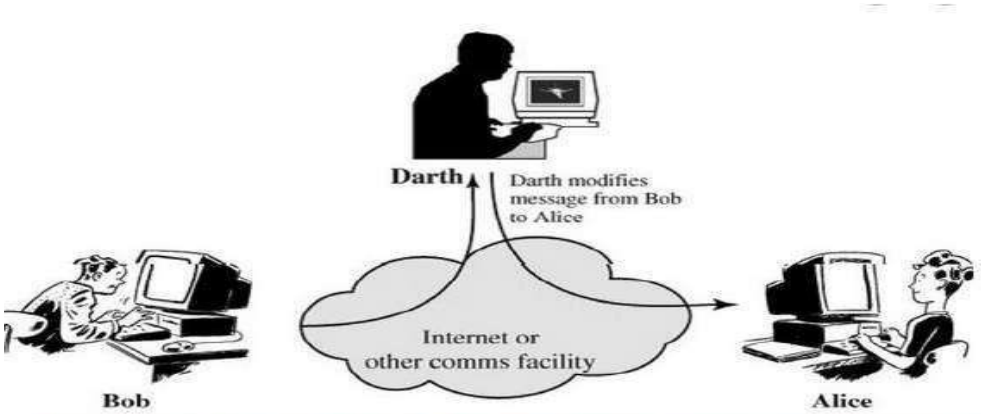
(b) Replay–

The attacker obtains a copy of a message sent by a user and later tries to replay it.



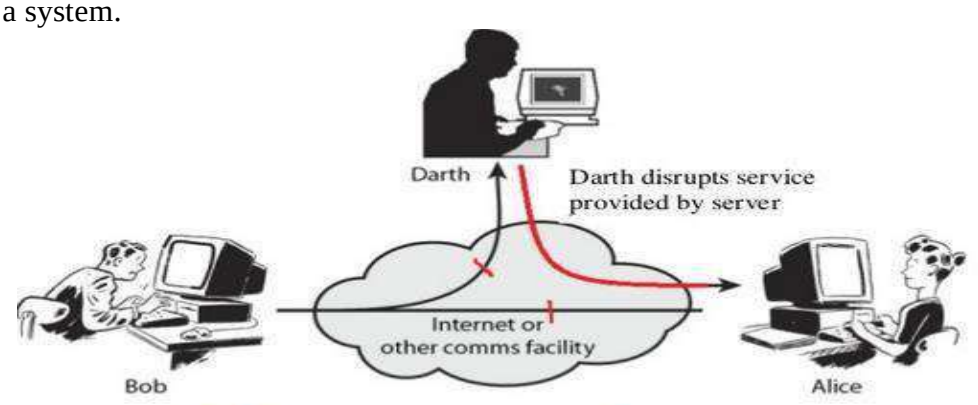
(B) Active attack-Replay

(c) Modification: After intercepting or accessing information, the attacker modifies the information then send to receiver.



Active Attack – Modification of messages

(d) Denial of service: Denial of service (Dos) is a very common attack.it may slow down or totally interrupt the service of a system.



(d) Active attack - Denial of Service

Cryptographic Attacks Categories

Cryptographic attacks can be broadly categorized into two distinct types:

- Cryptanalytic
- Non-Cryptanalytic

Cryptanalytic Attacks:

- These attacks are combinations of statistical and algebraic techniques aimed at discover the secret key of a cipher.

- The attacker thus guesses the key and looks for the distinguishing property. if the property is detected, the guess is correct otherwise the next guess is tried.

Non-Cryptanalytic Attacks:

- The other types of attacks are non-cryptanalytic attacks, which do not explain the mathematical weakness of the cryptographic algorithm.

SERVICES AND MECHANISM

Security Services

ITU-T (X .800) is provided by protocol layer of transmission that defines security services ensures security of the data transfer

- Data Confidentiality: It is designed to protect data from disclosure attack.. That is, it is designed to prevent snooping and traffic analysis attack.
- Data Integrity: It is designed to protect data from modification, insertion, deletion and replaying by an adversary
- Authentication: It provides the authentication of the party at the other end of the line.
- Non-repudiation: It protects against repudiation by either the sender or the receiver of the data.
- Access Control: It provides protection against unauthorized access to data

Security Mechanism:

ITU-T recommends Security mechanisms to provide the security services

- Encipherment:The use of mathematical algorithms to transform data into a form that is not readily understandable

- Data Integrity:A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- Digital Signature:A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
- Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.
- Routing Control:Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- Traffic Padding: Inserting bogus data to prevent traffic analysis.
- Notarization:The use of a trusted third party to assure certain properties of a data exchange.
- Access Control:A variety of mechanisms that enforce access rights to resources.

Relation Security Services and Mechanisms

➢ Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.

➢Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Services	Mechanisms
Confidentiality	Encryption, routing control
Integrity	Digital Signature, Encryption
Authentication	Encryption, Digital Signature
Non-repudiation	Digital Signature, Notarization
Access Control	Interactive Proofs, access control mechanisms and policies.

MATHEMATICS OF CRYPTOGRAPHY

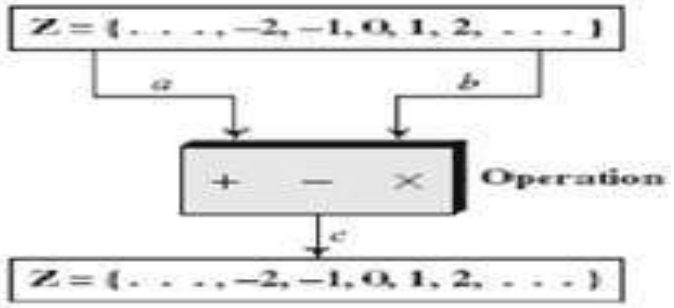
Integer Arithmetic: In Integer arithmetic, we are use a set and a few operations.

➢ Set of Integers: The set of Integers, denoted by z, contains all integral numbers (with no fraction) from negative infinity to positive infinity.

$$Z = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$$

Fig. 2.1 *The set of integers*

➢ Binary Operations: A Binary operation takes two inputs and creates one output. Three common binary operations defined for integers are addition, subtraction and multiplication.



- Examples:

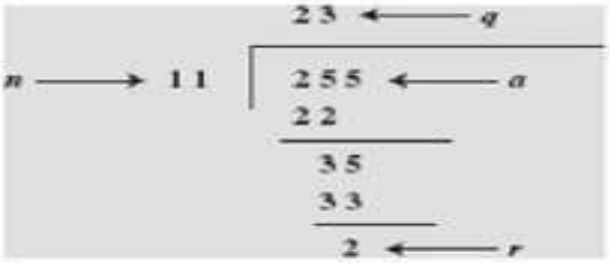
Add:	5+9=14	(-5)+9=4	5+(-9)=-4
Subtract:	5-9=-4	(-5)-9=14	5-(-9)=14
Multiply:	5x9=45	(-5)x9=-45	5x(-9)=45

Integer Division: if we divide a by n, we can get q and r. The relationship between these four integers can be shown as

a=q x n + r

a is dividend, n is the divisor, q is quotient , r is remainder

- Examples: Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm. We have shown in following

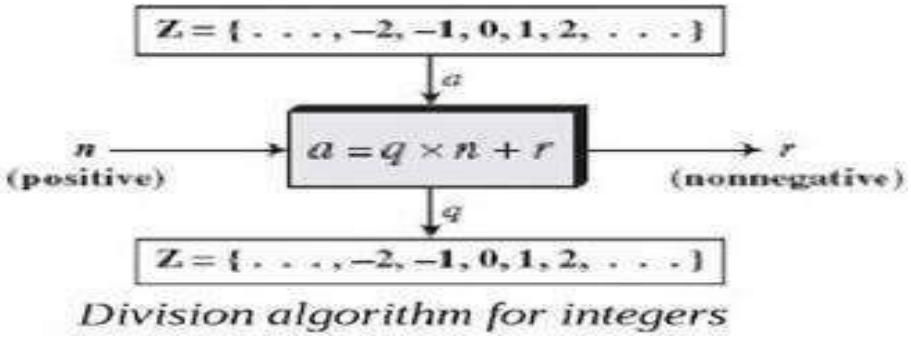


finding the quotient and the remainder

Two Restrictions:

- First, we require that the divisor be a positive integer (n > 0).
- Second, we require that the remainder be a non-negative integer (r ≥ 0).

Integer Division



Division algorithm for integers

Examples: Assume r and q are negative when 'a' is negative.

- To make r positive, decrement q by 1 and add value of n to r
- consider -255=(-23x 11) +(-2) ↔ -255=(-24x11)+9
- We have decremented -23 to -24 and added 11 to -2 to make 9.

The relation is still valid

Divisibility:

If a is not zero and we let r = 0 in the division relation, we get

a = q x n

We then say that n divides a (or n is a divisor of a). We can also say that a is divisible by n. The above is n | a .

If the remainder is not zero, then n does not divide a and we can write the relationship as a + n.

- Examples: The integer 4 divides the integer 32 because 32 = 8 x 4.
  We show this is as 4 |32
- The number 8 does not divide the number 42 because 42 = 5 x 8 + 2. There is a remainder, the number 2, in the equation.
  We show this as 8 + 42.

- Examples: The integer 4 divides the integer 32 because 32 = 8 x 4.
  We show this is as 4 |32
- The number 8 does not divide the number 42 because 42 = 5 x 8 + 2. There is a remainder, the number 2, in the equation.

We show this as 8 + 42.

Examples:

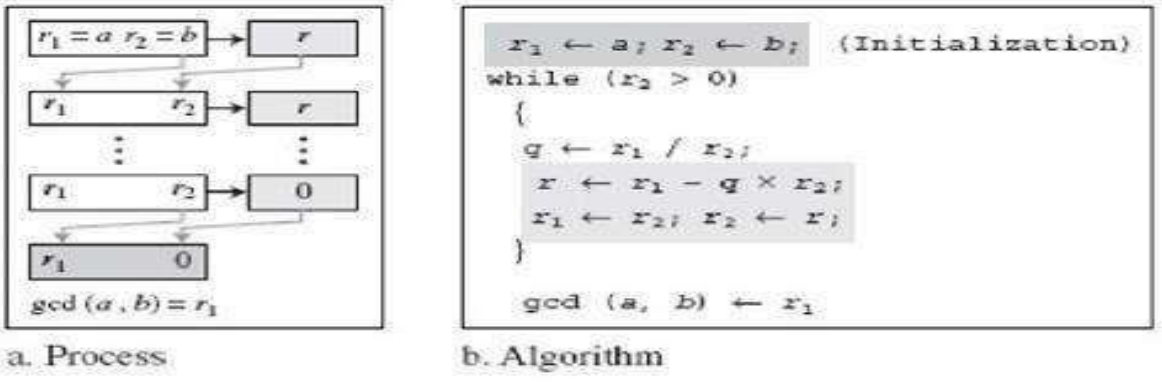
1) Since 3 | 15 and 15 | 45, according to third property, 3 |45
2) Since 3 | 15 and 3 | 9, according to the fourth property, 3 |(15 x 2 + 9 x 4), which means 3 | 66.

Greatest Common Divisor(GCD)

The greatest common divisor of two positive integers is the largest integer that can divide both integers we can write the relationship as a + n.

Examples: GCD of 15 and 20 is 2 because divisors of 15 are 3,5 and divisors of 20 are 2,4,5,10. The GCD is 5

- Euclidean Algorithm:
- Euclidean algorithm is used to finding the greatest common divisor (gcd) of two positive integers. The Euclidean algorithm is based on the following two facts
  - Fact 1: gcd (a, 0) = a
  - Fact 2: gcd (a, b) = gcd (b , r), where r is the remainder of dividing a by b
  - When gcd (a, b) = 1, we say that a and b are relatively prime.



a. Process b. Algorithm

Example: gcd (36, 10) = ?

```
gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2
```

Example: gcd (2740,1760) = ?

Solution: we initialize r_1 to 2740 and r_2 to 1760

Answer:

gcd (2740, 1760) = 20

.

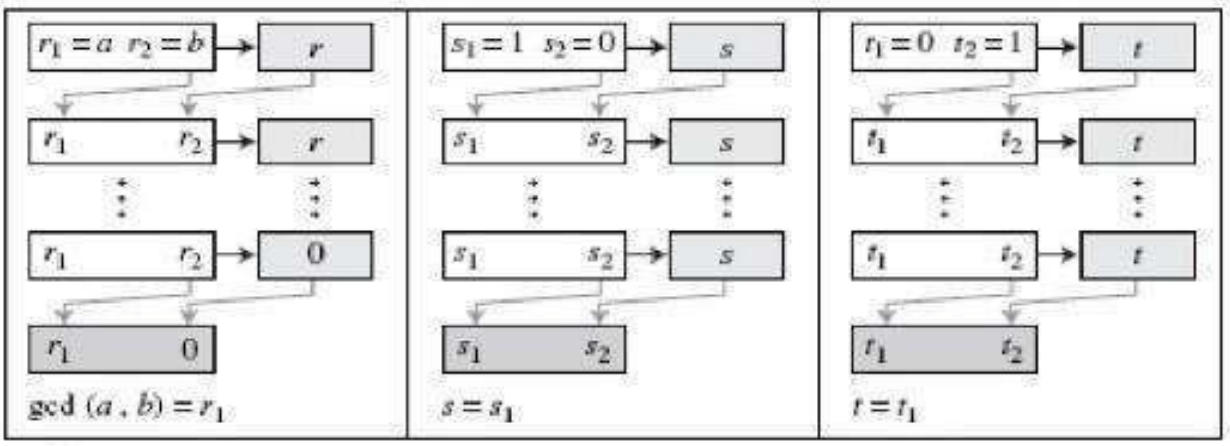
q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

Extended Euclidean Algorithm

- Given two integers a and b, we often need to find other two integers, s and t, such that

s x a + t x b = gcd (a,b)

- The Extended Euclidean Algorithm can calculate the gcd (a, b) and at the same time calculate the value if s and t.



a. Process

```
r1 ← a; r2 ← b;
s1 ← 1; s2 ← 0;                    (Initialization)
t1 ← 0; t2 ← 1;
while (r2 > 0)
{
  q ← r1 / r2;
  r ← r1 – q × r2;
  r1 ← r2;   r2 ← r;               (Updating r's)
  s ← s1 – q × s2;
  s1 ← s2;   s2 ← s;               (Updating s's)
  t ← t1 – q × t2;
  t1 ← t2;   t2 ← t;               (Updating t's)
}
gcd (a , b) ← r1;   s ← s1;   t ← t1
```

b. Algorithm

Example: Given a = 161 and b = 28,
Find gcd (a,b) and the values of s and t.
Solution:
$r = r_1 – q \times r_2$, $t = t_1 – q \times t_2$, $s = s_1 – q \times s_2$, We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	–5
1	28	21	7	0	1	–1	1	–5	6
3	21	7	0	1	–1	4	–5	6	–23
	7	0		–1	4		6	–23	

We get gcd (161,28) = 7, s=-1 and t = 6

Linear Diophantine Equations

An equation of type ax + by = c with variables is called as Linear Diophantine Equation.
The Extended Euclidean algorithm is used to find solutions to the Linear Diophantine Equations
This type of equation has either no solution or an infinite number of solutions. Let d = gcd(a,b).
if d + c, then the equation has no solution.
If d | c, then we have an infinite number of solutions. (one is particular and rest are general solutions).
Particular Solution: if d | c, a particular solution to the above equation can be found using the following steps:

- Reduce the equation to $a_1x + b_1y = c_1$ by dividing both sides of the equation by d. This is possible because d divides a, b, and c by the assumption.
- Solve for s and t in the relation $a_1s + b_1t = 1$ using the extended Euclidean algorithm.
- The particular solution: $x_0 = (c/d)s$ and $y_0 = (c/d)t$

General Solutions: after finding the particular solution, the general solutions can be found:
$x = x_0 + k (b/d)$ and
$y = y_0 – k (a/d)$ where k is an integer

Example: Find the particular and general solutions to the equation
21x + 14y = 35.

Given equation, 21x+14y = 35 that is written as ax+by = c
a=21, b=14, c=35

d = gcd(a,b) = gcd(21,14) [Apply Euclidean Algorithm]
= gcd (14,7) 1.gcd(a,0) = a
= gcd (7,0)=7 2.gcd(a,b) =gcd(b,r)
so, d=7 where 'r' remainder

Note: if d | c i.e 7|35 (7 divides 35), so one is Particular solution and infinity General solutions.

Particula Solution :-

$21x+14y=35$ ①

Divide both sides by 7 in ①, then

$3x+2y=5$ ②

using Extended Euclidean Algorithm , find "s" and "t"
such as 3s+2t = 1 Ref. (s x a + t x b = gcd (a,b))
Find gcd (3, 2) where r1 is 3 and r2 is 2 using Extended Euclidean Algorithm
r = r1 - r2 x q , s= s1 - s2 x q , t= t1 - t2 x q

q	r1	r2	r	s1	s2	s	t1	t2	t
1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
x	1	0	x	1	-2	x	-1	3	x

gcd(3,2)=r1=1 s=s1=1 t=t1=-1

as per particular solutions
$x_0 = (c/d)s$ and $y_0 = (c/d)t$
substitute values a=21,b=14 , c=35, d=7 for x_0 and y_0

$x_0 = (35/7)x\ 1 = 5$
$y_0 = (35/7)(-1) = -5$

General Solution:
$x = x_0 + k\ (b/d)$ and $y = y_0 – k\ (a/d)$ where k is an integer
x = 5+k(14/7) ; y = -5-k(21/7)
x = 5+2k y = -5-3k
here "k" is an integer ; k=0,1,2,3,4… then substitute k in above:
(5,-5), (7,-8),(9,-11), ... are solutions to given equation

Modular Arithmetic

The division relationship (a = q x n + r) has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are focused in only one of the outputs, the remainder r.

Modulo Operator:

- Modulo operator is shown as *mod*.
- The second input (n) is called the modulus.
- The output r is called the residue.

The below figure shows the division relation compared to the modulo operator

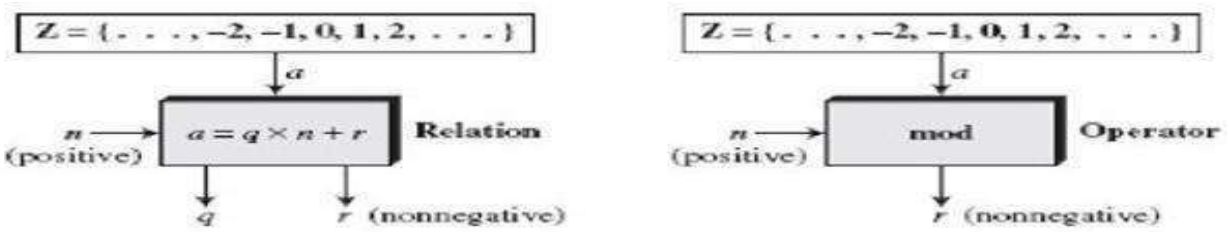


Fig. : *Division relation and modulo operator*

The modulo operator (mod) takes an integer (a) from the set Z and a positive modulus (n). The operator creates a non-negative residue (r).

a mod n = r

- Example

Find the results of the following operations:

a. 27 mod 5
b. 36 mod 12
c. −18 mod 14
d. −7 mod 10

SOLUTION We are looking for the residue *r*. We can divide the *a* by *n* and find *q* and *r*. We can then disregard *q* and keep *r*.

a. Dividing 27 by 5 results in *r* = 2. This means that 27 mod 5 = 2.
b. Dividing 36 by 12 results in *r* = 0. This means that 36 mod 12 = 0.
c. Dividing −18 by 14 results in *r* = −4. However, we need to add the modulus (14) to make it nonnegative. We have *r* = −4 + 14 = 10. This means that −18 mod 14 = 10.
d. Dividing −7 by 10 results in *r* = −7. After adding the modulus to −7, we have *r* = 3. This means that −7 mod 10 = 3.

SET OF RESIDUES: Z_n

The result of the modulo operation with modulus 'n' is always an integer between 0 and n-1.
In other words (a mod n) is always a non negative integer less than n
Modulus operation creates a set, that is called set of least residues modulo n or Z_n
We have one set of Z(integers), but we have infinite instances of the set o residues Z_n for each n.

$$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$$

$Z_2 = \{0, 1\}$ $Z_6 = \{0, 1, 2, 3, 4, 5\}$ $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Fig. *Some Z_n sets*

CONGRUENCE (≡)

If two numbers A and B have the property that their difference A-B is integrally divisible by a number C (i.e., (A-B)/C is an integer), then A and B are said to be "congruent modulo C." The number C is called the modulus , and the statement "A is congruent to B (modulo C)" is written mathematically as

$$A \equiv B \ (\text{mod } C)$$

This says that " A is congruent to B modulo C".

Examining the expression closer:

1. $\equiv$ is the symbol for congruence, which means the values A and B are in the same **equivalence class**.
2. $(\text{mod } C)$ tells us what **operation** we applied to A and B.
3. when we have both of these, we call "$\equiv$" **congruence modulo** C.

e.g. $26 \equiv 11 \ (\text{mod } 5)$

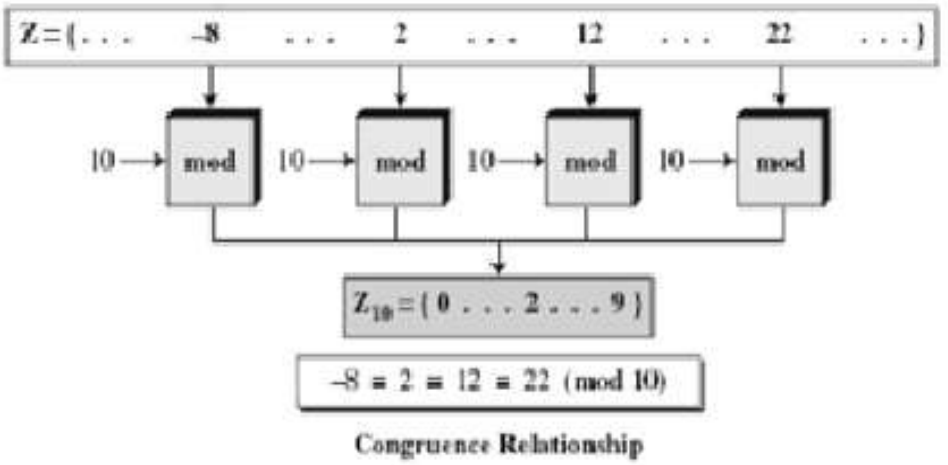
$26 \bmod 5 = 1$ so it is in the equivalence class for 1,

$11 \bmod 5 = 1$ so it is in the equivalence class for 1, as well.

So, 26 is congruent to 11 modulo 5

Example 2:

Assume, -8≡12(mod 10) 2≡12(mod 10) 12≡22(mod 10) 22≡32(mod 10)



Congruence Relationship

RESUDUE CLASSES

A residue class [a] is the set of integers congruent modulo n.
In other words it is the set of all integers such that x=a (mod n).
For example, if n=5, we have five sets [0], [1], [2], [3], [4] as shown below

[0]= { ...., -15 -10 ,-5, 0, 5, 10,15,...}
[1]= { ...., -16 -11 ,-6, 1, 6, 11,16,...}
[2]= { ...., -17 -12 ,-7, 2, 7, 12,17,...}
[3]= { ...., -18 -13 ,-8, 3, 8, 13,18,...}
[4]= { ...., -19 -14 ,-9, 4, 9, 14,19,...}

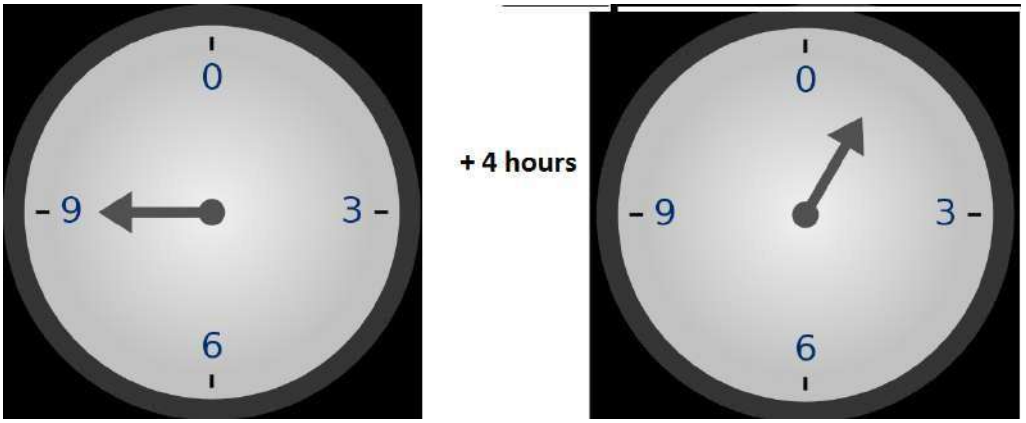
From each set there is one lease residue that
0 in [0], 1 in [1], 2 in [2], 3 in[3] and 4 in [4]..
The set of these residues are shown as

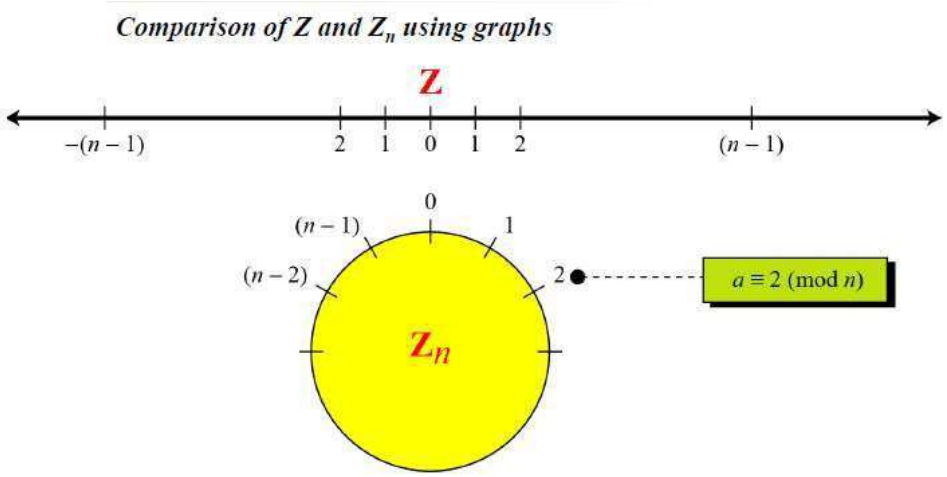
$Z_5 = \{0,1,2,3,4\}$

Applications:

We use a clock to measure time. Our clock system uses modulo 12 arithmetic. How ever instead of a 0 we the 12

.





Operations in Z_n

The three Binary operations (addition, subtraction and multiplication) are defined for the set Z_n.

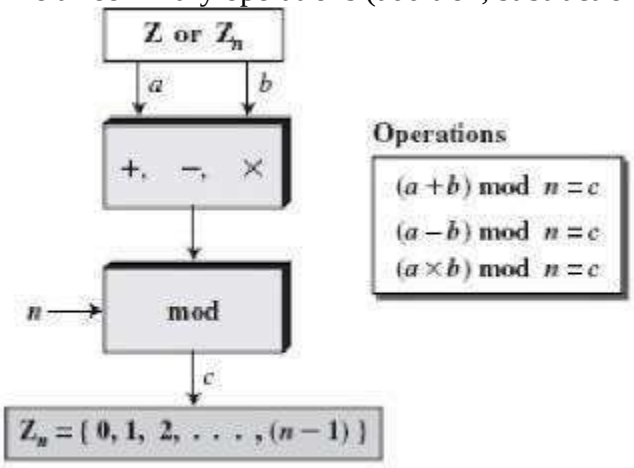


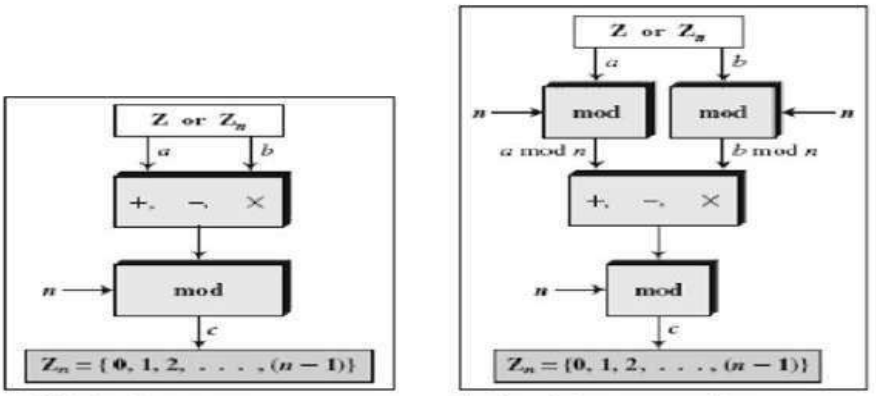
Fig. *Binary operations in Z_n*

Properties:

First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$



a. Original process b. Applying properties

EXAMPLE : Perform the following operations (the inputs come from Z_n):

a. Add 7 to 14 in Z_{15}.
b. Subtract 11 from 7 in Z_{13}.
c. Multiply 11 by 7 in Z_{20}.

Solution:

$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$

$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$

$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$

Example 2

Perform the following operation:

a. Add 17 to 27 in Z_{14}
   (17+27) mod 14 = (44) mod 14 = 2
b. Subtract 34 from 12 in Z_{13}

(12-34) mod 13 = (-22) mod 13 = - 9 = (-9+13) = 4

c. Multiply 123 by -10 in Z_{20}

(123*(-10)) mod 20 = (-1230) mod 20 = -10 =(-10+20) = 10

Property 1:

(a+b) mod n= [(a mod n) + (b mod n)] mod n

(4+5) mod 2 = [(4 mod 2) + (5 mod 2)] mod 2

9 mod 2 = [0 + 1] mod 2

1 = 1

Property 2:

(a-b) mod n= [(a mod n) - (b mod n)] mod n

(4 - 5) mod 2 = [(4 mod 2) - (5 mod 2)] mod 2

-1 mod 2 = [0 - 1] mod 2

-1 mod 2 = -1 mod 2

Property 3:

(axb) mod n= [(a mod n) x (b mod n)] mod n (4 x 5) mod 2 = [(4 mod 2) x (5 mod 2)] mod 2 20 mod 2 = [0 x 1] mod 2

0 = 0 mod 2

0 = 0

INVERSES

When we are working in modular arithmetic, we need to find inverse of a number relative to an operation. There are two types of inverses are used modular arithmetic.

- Additive inverse (relative to an addition operation).
- Multiplicative inverse (relative to a multiplication operation).

❑ ***Additive Inverse*** In $\mathbf{Z}_n$, two numbers a and b are additive inverses of each other if

$$a + b = 0 \pmod{n}$$

In $\mathbf{Z}_n$, the additive inverse of a can be calculated as $b = n - a$.

For example, the additive inverse of 4 in $\mathbf{Z}_{10}$ is $10 - 4 = 6$.

Note:In modular arithmetic, each integer has an additive inverse.

- The sum of an integer and its additive inverse is congruent to 0 modulo n

❑ ***Multiplicative Inverse*** In $\mathbf{Z}_n$, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

For example, if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have $(3 \times 7) \bmod 10 = 1$.

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the ! product of the integer and its multiplicative inverse is congruent to 1 modulo n.

It can be proved that 'a' has a multiplicative inverse in Zn iff gcd(n,a)=1. (In this case 'a' and n are said to **relatively prime**.

Example 1: Find multiplicative inverse of 8 in Z_{10}.

SOLUTION There is no multiplicative inverse because gcd (10, 8) = $2 \neq 1$. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Example 2: Find all multiplicative inverses in Z_{10}.

SOLUTION There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse. We can see that

$$(1 \times 1) \bmod 10 = 1 (3 \times 7) \bmod 10 = 1 (9 \times 9) \bmod 10 = 1$$

The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd $(n, b) = 1$. The multiplicative inverse of b is the value of t after being mapped to Z_n.

Example 3: Find all multiplicative inverses 23 in Z_{100}.

SOLUTION We use a table similar to the one we used before with $r_1 = 100$ and $r_2 = 23$. We are interested only in the value of t.

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	–4
2	23	8	7	1	–4	9
1	8	7	1	–4	9	–13
7	7	1	0	9	–13	100
	1	0		–13	100	

The gcd (100, 23) is 1, which means the inverse of 23 exists. The extended Euclidean algorithm gives $t_1 = -13$. The inverse is $(-13) \bmod 100 = 87$. In other words, 23 and 87 are multiplicative inverses in $\mathbf{Z}_{100}$. We can see that $(23 \times 87) \bmod 100 = 2001 \bmod 100 = 1$.

Addition and Multiplication Tables:

In addition table, each integer has an additive inverse. The inverse pairs can be found when the result of addition is zero. In Figure 2.16, we have (0,0), (1,9), (2,8), (3,7), (4,6), and (5,5).
In multiplication table, the pairs can be found whenever the result of multiplication is 1. In Figure, we have (1,1), (3,7) and (9,9).

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Addition Table in Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Multiplication Table in Z_{10}

Fig: Addition and multiplication tables in Z_{10}
Note: We need to use Z_n when additive inverses are needed; we need to use Z*n when multiplicative inverses are needed.

Two more Sets:

Cryptography often uses two more sets: Z_p and Z*p.

The set $\mathbf{Z}_p$ is the same as $\mathbf{Z}_n$ except that n is a prime. $\mathbf{Z}_p$ contains all integers from 0 to $p - 1$. Each member in $\mathbf{Z}_p$ has an additive inverse; each member except 0 has a multiplicative inverse.

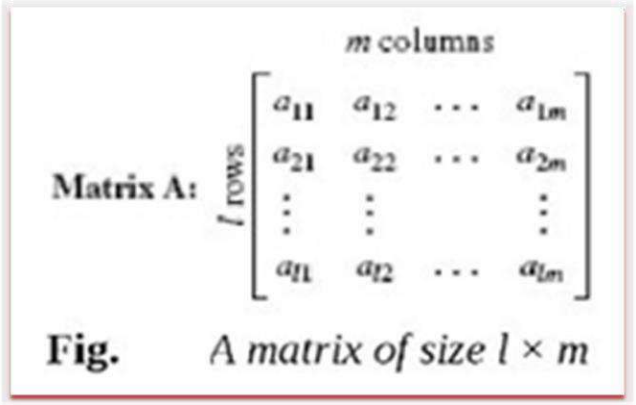
The set $\mathbf{Z}_{p^*}$ is the same as $\mathbf{Z}_{n^*}$ except that n is a prime. $\mathbf{Z}_{p^*}$ contains all integers from 1 to $p - 1$. Each member in $\mathbf{Z}_{p^*}$ has an additive and a multiplicative inverse. $\mathbf{Z}_{p^*}$ is a very good candidate when we need a set that supports both additive and multiplicative inverse.

The following shows these two sets when $p = 13$.

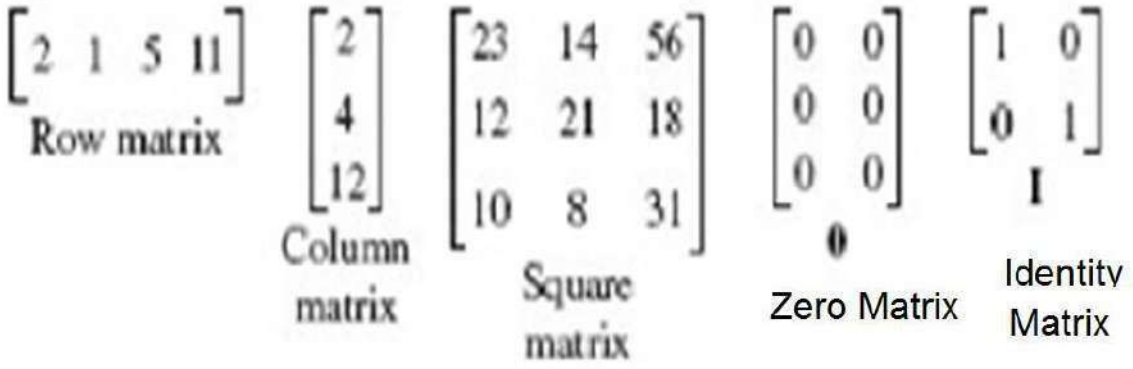
$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

MATRICES

A matrix is a rectangular array of *l x m* elements; in which
l is the number of rows and
m is the number of columns.
A matrix is normally denoted with an Uppercase Letter such as A.
The element a_{ij} is located in the ith row and jth column.



DIFFERENT TYPES OF MATRICES



OPERATIONS AND RELATIONS

Relation operation:

Equality:

If two matrices are equal sizde and content is same then they have equality

Four operations:

1. Addition
2. Subtraction
3. Multiplication
4. Scalar multiplication

Examples:

Addition : $C_{IJ}=A_{IJ}+ B_{IJ}$

$$\begin{bmatrix}12 & 4 & 4\\ 11 & 12 & 30\end{bmatrix} = \begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 10\end{bmatrix} + \begin{bmatrix}7 & 2 & 3\\ 8 & 10 & 20\end{bmatrix}$$

$$C = A + B$$

Subtraction: : $C_{IJ}=A_{IJ} - B_{IJ}$

$$\begin{bmatrix}-2 & 0 & -2\\ -5 & -8 & 10\end{bmatrix} = \begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 10\end{bmatrix} - \begin{bmatrix}7 & 2 & 3\\ 8 & 10 & 20\end{bmatrix}$$

$$D = A - B$$

Multiplication

If each element of matrix **A** is called a_{ij}, each element of matrix **B** is called bj_k, then each element of matrix **C**, c_{ik}, can be calculated as

$$c_{ik} = \Sigma\, a_{ij} \times b_{jk} = a_{i1} \times b_{1j} + a_{i2} \times b_{2j} + \cdots + a_{im} \times b_{mj}$$

Examples:

$$\underset{C}{\begin{bmatrix}53\end{bmatrix}} = \underset{A}{\begin{bmatrix}5 & 2 & 1\end{bmatrix}} \times \underset{B}{\begin{bmatrix}7\\ 8\\ 2\end{bmatrix}}$$

In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

$$\underset{C}{\begin{bmatrix}52 & 18 & 14 & 9\\ 41 & 21 & 22 & 7\end{bmatrix}} = \underset{A}{\begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 4\end{bmatrix}} \times \underset{B}{\begin{bmatrix}7 & 3 & 2 & 1\\ 8 & 0 & 0 & 2\\ 1 & 3 & 4 & 0\end{bmatrix}}$$

Scalar Multiplication We can also multiply a matrix by a number (called a **scalar**). If **A** is an $l \times m$ matrix and x is a scalar, $\mathbf{C} = x\mathbf{A}$ is a matrix of size $l \times m$, in which $c_{ij} = x \times a_{ij}$.

$$\begin{matrix} & \mathbf{B} & & & \mathbf{A} & \\ \begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{bmatrix} & = & 3 \times & \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix} \end{matrix}$$

Multiplication unit matrix with normal matrix gives the same matrix

A X I = I X A = A

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1X2 + 0X3 & 1X4 + 0X1 \\ 0X2 + 1X3 & 0X4 + 1X1 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$$

DETERMINANT

If A is square matrix of mxm then determinant of A is det(A)

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$
2. If $m > 1$, $\det(\mathbf{A}) = \sum_{i=1\ldots m} (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

Where A_{ij} is a matrix obtained from A by deleting the ith row and jth column.
Determinant is obtained for only square matrices

Det(2x2) matrix

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{i+1} \times 5 \times \det[4] + (-1)^{i+2} \times 2 \times \det[3]$$

=5x4-2x3=14

or $$\det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

Example : det(3x3) matrix

$$\det\begin{bmatrix}5 & 2 & 1\\ 3 & 0 & -4\\ 2 & 1 & 6\end{bmatrix} = (-1)^{1+1}\times 5\times \det\begin{bmatrix}0 & -4\\ 1 & 6\end{bmatrix} + (-1)^{1+2}\times 2\times \det\begin{bmatrix}3 & -4\\ 2 & 6\end{bmatrix}$$

$$+ (-1)^{1+3}\times 1\times \det\begin{bmatrix}3 & 0\\ 2 & 1\end{bmatrix}$$

$$= (+1)\times 5\times (+4) \quad + \quad (-1)\times 2\times (24)$$

$$+ \quad (+1)\times 1\times (3)$$

$$= -25$$

MATRICES-Inverses

Additive Inverse

The additive inverse of the matrix A is another matrix B such that A+B=0.

In other words $b_{ij}=-a_{ij}$

Generally additive inverse is of A=-A

Multiplicative Inverse:

The multiplicative Inverse of a square matrix A is a B such that A X B = I.

Normally Multiplicative inverse of A is defined by A^{-1}

Multiplicative inverse is defined for only square matrices

Residue Matrices

Cryptography uses residue matrices: matrices with all elements are in $\mathbf{Z}_n$. All operations on residue matrices are performed the same as for the integer matrices except that the operations are done in modular arithmetic. One interesting result is that a residue matrix has a multiplicative inverse if the determinant of the matrix has a multiplicative inverse in $\mathbf{Z}_n$. In other words, a residue matrix has a multiplicative inverse if gcd (det(**A**), n) = 1.

EXAMPLE Figure shows a residue matrix A in Z_{26} and its multiplicative inverse A^{-1}. We have det(A) = 21 which has the multiplicative inverse 5 in Z_{26}. Note that when we multiply the two matrices, the result is the multiplicative identity matrix in Z_{26}.

$$A = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad A^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$\det(A) = 21$ $\det(A^{-1}) = 5$

Fig. *A residue matrix and its multiplicative inverse*

Example : Find A^{-1} modulo value -

Problem:

if $A = \begin{pmatrix} 3 & 2 \\ 4 & 7 \end{pmatrix}$ mod 36; then A^{-1} mod 36 = ?

Solution:

$A = \begin{pmatrix} 3 & 2 \\ 4 & 7 \end{pmatrix} \Rightarrow \det(A) = 3x7 - 2x4 = 13$

$[\det(A)]^{-1} \bmod 36 = 13^{-1} \bmod 36 = ?$

$(13)^{-1} \bmod 36 = ? \Rightarrow$ use extended Euclidian Alg. to find $13^{-1} \bmod 36 = ?$

Calculate gcd (36, 13), 13 multiplicative inverse

$r = r_1 - q x\, r_2 \qquad t = t_1 - q \times t_2$

$r_1 = 36;\ r_2 = 13,\ t_1 = 0;\ t_2 = 1$

q	r_1	r_2	r	t_1	t_2	t
2	36	13	10	0	1	-2
1	13	10	3	1	-2	3
3	10	3	1	-2	3	-11
3	3	1	0	3	-11	36
X	1	0	X	-11	36	X

gcd(13,36)=1 "13" multiplicative inverse

$13^{-1} \bmod 36 = -11 \bmod 36$

$= (-11+36) \bmod 36 = 25 \bmod 36$

'13' multiplicative inverse in Z_{36} = 25

$\Rightarrow [\det(A)]^{-1} \bmod 36 = 13^{-1} \bmod 36 = 25$

$$A^{-1} = 25 \begin{bmatrix} 7 & -2 \\ -4 & 3 \end{bmatrix} \pmod{36}$$

$$= \begin{bmatrix} 175 & -50 \\ -100 & 75 \end{bmatrix} \pmod{36}$$

$$= \begin{bmatrix} 175 \bmod 36 & -50 \bmod 36 \\ -100 \bmod 36 & 75 \bmod 36 \end{bmatrix}$$

175 mod 36= 31
-50 mod 36=(72-50 mod 36) = 22
-100 mod 36=(108-100 mod 36)=8
75 mod 36=3

$$= \begin{bmatrix} 31 & 22 \\ 8 & 3 \end{bmatrix} \quad \text{so, } A^{-1} \bmod 36 = \begin{bmatrix} 31 & 22 \\ 8 & 3 \end{bmatrix}$$

Linear Congruence

Single variable Linear Equations:

Equations of the form ax ≡ b (mod n) might have no solution or a limited number of solutions

Assume that the gcd(a,n) = d.

If d + b (d not divides b), there is no solution.

If d | b (d divides b), there are d solutions.

If d | b, we use the following strategy to find the solutions:

- Reduce the equation by dividing both sides of the equation (including the modulus) by d.
- Multiply both sides of the reduced equation by the multiplicative inverse of 'a' to find the particular solution x_0.
- The General solutions are $x = x_0 + k (n / d)$ for k = 0, 1, 2, , (d-1).

Congruence-Example

Example 1: Solve the equation

10 x = 2(mod 15).

Solution :-

Given Linear equation 10x≡ 2(mod 15)

In basic form ax ≡ b(mod n)

a = 10 ; b = 2; n= 15

Now, find d = ?

d = gcd(a,n)= gcd (10,15)

= gcd (15,10) = gcd (10,5)

= gcd (5,0)

= 5

check if d+b (d not divides b), then no solution

5+2 means '5' not divides '2', so, The given equation has No solution.

Example 2: Solve the equation

14 x= 12 (mod 18)

Solution :- Given Linear equation

14x ≡ 12(mod 18)

In basic form ax ≡ b(mod n)

a = 14 ; b = 12; n= 18

d = gcd(a,n)= gcd (14,18) = gcd (18,14)

= gcd (14,4) = gcd (4,2)=gcd(2,0)=2

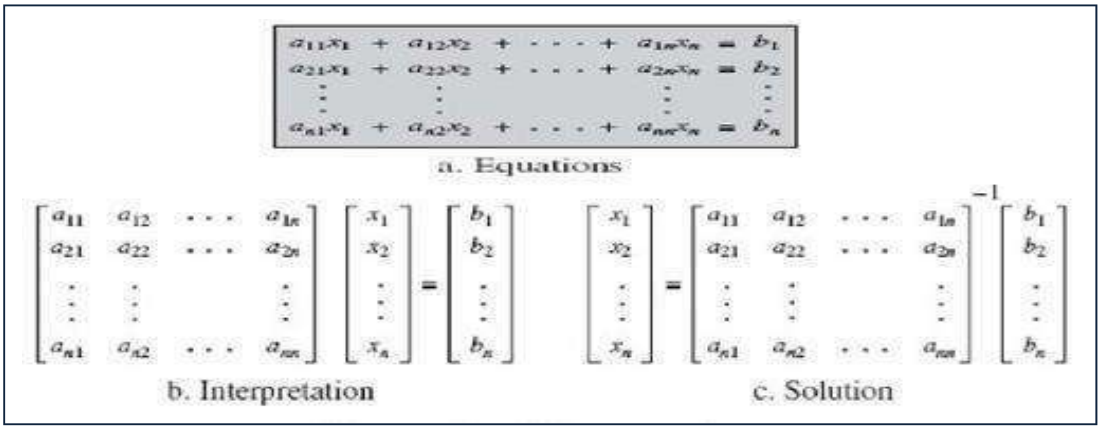
check, d b or d+ b

d | b → 2 | 12 means " 2 divides 12", so the given equation have "2 solutions".

Given equation 14 x 12 (mod 18)
divides 'd' on both sides of equation
7x 6 (mod 9)
multiply 7^{-1} on both sides of above to get particular solution 'x_0'.
7^{-1} x 7 * $x_0 \equiv 6 * 7^{-1} \pmod 9$
$x_0 \equiv 6x\ 7^{-1} \pmod 9$ i.e $7^{-1} \bmod 9 \equiv 4$
$x_0 \equiv 6 \times 4 \pmod 9$
$x_0 \equiv 24 \bmod 9$
$x_0 \equiv 6$
solutions are $x = x_0 + k\ (n/d)$ where k = 0,1
(d = 2)
if k = 0 $x = x_0 + 0\ (n/d)$
$x = 6 + 0\ (18/2) = 6$
$x = 6$
if k = 1 $x = x_0 + 1\ ((n/d) = 6+1\ (18/2)$
$x = 15$
'6' and '15' are solution to 14 x 12 (mod 18)

Set of Linear Equations:

Solve the set of linear equations with same modulus by forming three matrices using coefficients.
Matrix 1: square matrix made from coefficients
Matrix 2: Column matrix made from variables
Matrix 3: Column matrix made from values at right side of equations
Consider the matrix as



Example

Solve the following sets of Linear equations?
3x + 2y ≡ 5 (mod 7)
4x + 6y ≡ 4 (mod 7)

Solution:

Matrix format of above equations is

$$\begin{bmatrix}3 & 2\\ 4 & 6\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}5\\ 4\end{bmatrix} \pmod 7$$

$$\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}3 & 2\\ 4 & 6\end{bmatrix}^{-1}\begin{bmatrix}5\\ 4\end{bmatrix} \pmod 7$$

Let $A=\begin{bmatrix}3 & 2\\ 4 & 6\end{bmatrix}$ then $A^{-1}= \begin{bmatrix}3 & 2\\ 4 & 6\end{bmatrix}^{-1} = \frac{1}{10}\begin{bmatrix}6 & -2\\ -4 & 3\end{bmatrix}$

$$\begin{bmatrix}x\\ y\end{bmatrix} = \frac{1}{10}\begin{bmatrix}6 & -2\\ -4 & 3\end{bmatrix}\begin{bmatrix}5\\ 4\end{bmatrix} \pmod 7 = \frac{1}{10}\begin{bmatrix}30-8\\ -20+12\end{bmatrix} \pmod 7$$

$$= \frac{1}{10}\begin{bmatrix}22\\ -8\end{bmatrix} \pmod 7 = \begin{bmatrix}22/10\\ -8/10\end{bmatrix} \pmod 7$$

$x = 22/10 \pmod 7$

$y = -8/10 \pmod 7$

Check the answer by inserting values:

$3x + 2y = 5 \pmod 7$

$3(22/10) + 2(-8/10) = (66/10)-(16/10) = 5 \pmod 7$

$4x + 6y = 4 \pmod 7$

$4(22/10) + 6(-8/10) = (88/10)-(48/10) = 4 \pmod 7$

LINEAR DIOPHANTINE EQUATION

The equation of the form ax +by = c is called as **Linear Diophantine Equation.**

Example: 19x +13y = 20

We can solve the above equation using following steps:

Step1: check whether it has solution or not.

Perform gcd(a,b) and if gcd(a,b) divides c then it has solution

Step 2: Use Euclidian Algorithm and reverse Euclidian algorithms to find the Particular solution.. x_0, y_0

Step3: Find general solution

$x=x_0+b.n$ where n is any integer

$y=y_0-a.n$

Example 1:-

Find particular and General solutions to the following **Linear Diophantine Equation:**

25x+10y=15

Solution:

a=25, b=10 and c=15

Check whether we have solution or not by calculating GCD(25,10) using Euclidian Algorithm:

gcd(25,10)=gcd(10,5)=gcd(5,0)=5

since gcd(25,10)=5 that divides the 15, we have solutions.

Reverse Euclidian Algorithm is:

25 = 2 x 10 + **5** ---------Eq1

10 = 2 x 5 + 0

Since gcd is 5 , rewrite the Eq1 from write to left:

5= 25 – 2 x10

5= 1x25 – 2x10 (1x25 – 2x10 is similar to 25x + 10y)

Multiply both sides by 3 since in the given equation right hand side is 15

3x5=3(1x25)-3(2x10)

15 = 3 x 25 – 6 x 10 then it can be rewrite as

25x3 – 10x6 = 15

The above is similar to

25x + 10y = 15

So, the **particular solution** is

$x_0 = 3$ and $y_0 = -6$

Substitute the x0 and y0 in the above $25x_0 + 10y_0 = 25x3+10(-6)=75-60=15$

Now, find **General solution**:

$x=x_0+b.n$ (where n is any integer and a=25, b=10)
$y=y_0-a.n$

- **if n=1, then**
  x=3+10x1=13
  y=-6-25x1=-31

Substitute the x and y in the given equation to check result:
25x + 10y = 25x13+10(-31)=325-310=15

- **if n= -1, then**
  x=3+10x(-1)=3-10= -7
  y=-6-25x(-1)= -6 +25 = 19

Substitute the x and y in the given equation to check result:
25x + 10y = 25x(-7)+10(19)=-175+190=15
Finally, the x,y pairs are (-7,19), (3,-6), (13,-31),….

Example 2:

Find particular and General solutions to the following **Linear Diophantine Equation:**
19x+13y=20

Solution:
A=19, b=13 and c=20
Check whether we have solution or not by calculating GCD(19,13) using Euclidian Algorithm:
gcd(19,13)=gcd(13,6)=gcd(6,1)=gcd(1,0)=1
since gcd(19,13)=1 that divides the 20, we have solutions.
Reverse of Euclidian Algorithm is :
19= 1 x13+ 6----------**(Eq 1)**
13= 2 x 6 + **1**---------- **(Eq 2)**
6 = 6x1 + 0
So, gcd(19,13) is 1.

- Rewrite the Eq 2 from write to left:
  1 = 13 – 2 x 6 ----------**(Eq 3)**
- Rewrite the Eq 1 from write to left:
  6 = 19 – 1 x13 ----------**(Eq 4)**

Substitute the 6 equivalent in Eq 4 that is 19-1x13 in Eq 3
1= 13- 2 x (19-1x13)
1= 13-2x19 + 2 x13
1= 1x13-2x19 + 2 x13
1= 3x13-2x19
Multiply both sides by 20 since in the given equation right hand side is 20
20x1=60x13-40x19)
20 = 13x60 – 19 x 40 then it can be rewrite as
This can be rewrite as similar to the given equation 19x+13y=20
13x60-19x40 = 20
-19x40 + 13x 60 =20
19x(-40)+13x60=20
So, the **particular solution** is
x_0 = -40 and y_0 = 60
Substitute the x_0 and y_0 in the given equation to check the result
19x+13y = 19(-40) + 13x60 = -760+780 = 20
Now, find **General solution**:
$x=x_0+b.n$ (where n is any integer and a=19, b=13)
$y=y_0-a.n$

- **if n=1, then**

x=-40+13x1=-40+13= -27
y=60 –19x1=41

Substitute the x and y in the given equation to check result:

19x + 13y = 19(-27)+13(41)=-513+533=20

- **if n= -1, then**

x=-40+13x(-1)=-40-13= -53
y=60-19x(-1)= 60+19 = 79

Substitute the x and y in the given equation to check result:

19x + 13y = 19x(-53)+13(79)=-1007+1027=20

Finally, the x,y pairs are (-40,60), (-27,41), (-53,79),….

UNIT -II

Symmetric Encryption

Mathematics of Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers, Data Encryption Standard, Advanced Encryption Standard.

Mathematics of Symmetric Key Cryptography:

Cryptography ?

Cryptography is a technique of securing information and communications through use of codes. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

Cryptography Types

1) Symmetric Key Cryptography:

The sender and receiver of message use a single common key to encrypt and decrypt messages.

2) Asymmetric Key Cryptography:

A pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

3) Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered..

Mathematics of Symmetric Key Cryptography

Algebraic Structures:

Cryptography requires set of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an **algebraic structure**.

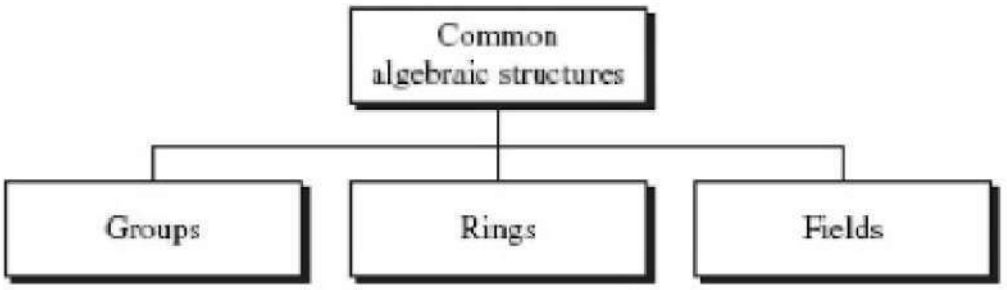


Fig. *Common algebraic structures*

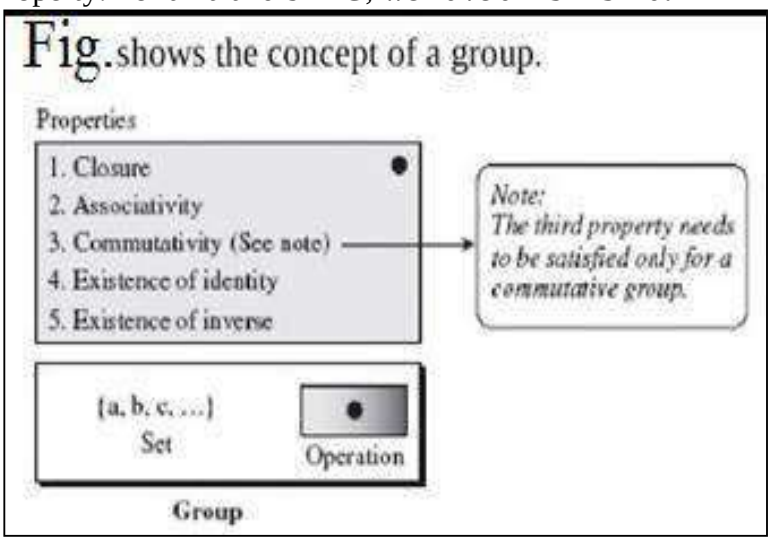
1. Groups

A **Group (G)** is a set elements with a binary operation "•" usually Addition or multiplication that satisfies four properties(Axioms).

• A **Commutative Group**, also called an **abelian group**, is a group in which the operator satisfies the four properties for groups plus an extra property, commutativity.

- Closure Property: if a and b are elements of G, then c = a • b is also an element of G.
- Associatively Property: if a, b, and c are elements of "G, then (a • b) • c = a • (b • c).
- Existence of Identity Property: For all a in G, there exists an element e, called the identity element, such that e • a = a • e = a

- Existence of Inverse Property: For each a in G, there exists an element a^1, called the inverse of a, such that $a \bullet a^1 = a^1 \bullet a = e$
- Commutativity Property: For all a and b in G, **we have a • b = b • a.**



EXAMPLE 1

The set of residue integers with the addition operator, G=< Z_n , + >, is a commutative group

1. Closure is satisfied. The result of adding two integers in Z_n is another integer in Zn

2.Associativity is satisfied. The result of 4+(3+2) is same as (4+3) + 2

3. Commutative is satisfied. we have 3+4=4+3

4.The identity element is 0. we have 3+0=0+3=3

5.Every element has an additive inverse. The inverse of 3 is 7 (3+7 mod 10 =0 mod 10 in Z_{10}) and inverse of 7 is 3(7+3 mod 10 =0 mod 10 in Z_{10}), so inverse property satisfied

EXAMPLE 2

The set Z_n* with multiplication operator, G=<Z_n*, x >, is also an abelian group. We can perform multiplication and divisions on the elements. We an identity element as 1.

Finite Group: A group is called a finite group if the set has a finite number of elements; otherwise, it is an infinite group.

Order of a Group: The order of group, **|G|**, is the number of elements in the group. If the group is not finite, its order is infinite; if the group is finite, the order is finite.

Subgroups: A subset **H** of a group **G** is a subgroup of G if H itself is a group with respect to the operation on **G**. In other words, if **G = <S, • >** is a group, **H = <T, • >** is a group under the same operation, and T is a non-empty subset of **S**, then **H** is a subgroup of **G**. The above definition implies that:

1.If a and b are members of both groups, then c=a • b is also a member of both groups
2.The group share the same identity element
3.If a is a member of both groups, the inverse of a is also a member of both groups
4.The group made with the identity element of G,H=<{e}, • >, is a sub group of G
5. Each group is a subgroup of itself

Cyclic Subgroup: If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

The term power means repeatedly applying the group operation to the element:

a^n -> a.a.a.a.....a (n times)

Example: The group G=< Z3, + > contains cyclic subgroups for 0,1 and 2:

If generated using 0:

0^0 mod 3 = 0, 0^1 mod 3 = 0, 0^2 mod 3 = 0. so, H1=<{0}, +>