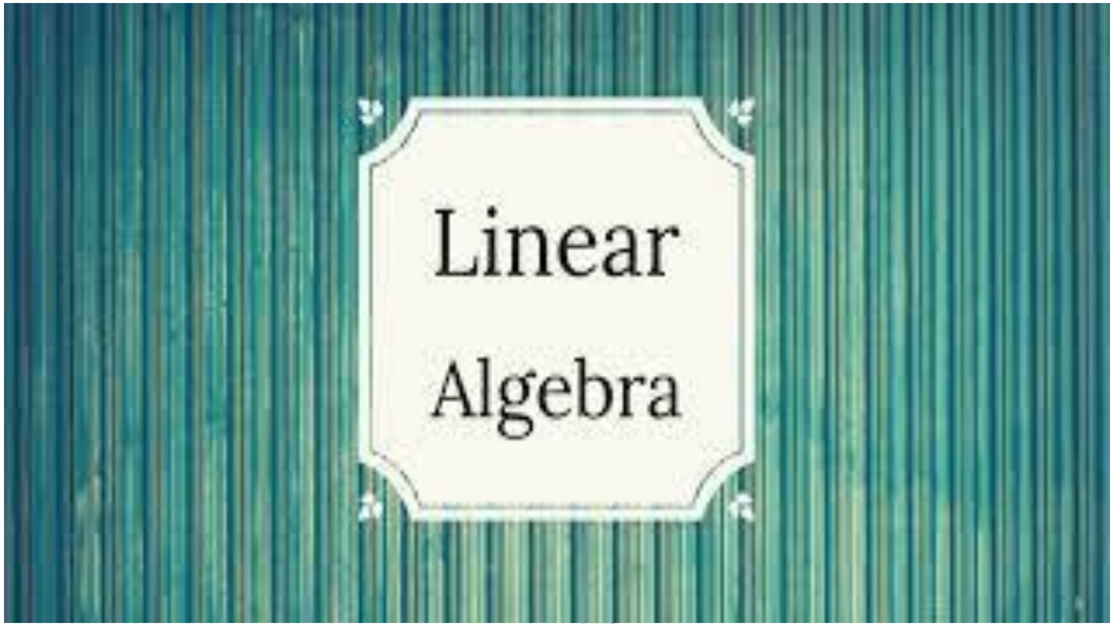


Lecture 8

Date: 19/09/2020

Note: These PPTs are for student’s reference, for detailed content(practice), students are advised to use text-books and reference books mentioned in the syllabus.

Topic: Solution of system of linear algebraic equations, by

Application of matrix to Encoding & Decoding

Introduction to find remainder using ‘modulo n’

Objectives

- Use matrices to encode and decode messages.

Cryptography

Cryptography

- Cryptography, is concerned with keeping communication private.
- Cryptography mainly consists of Encryption and Decryption.
- Encryption is the transformation of data into some unreadable form.
  - ❑ It is supposed to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.
- Decryption is the reverse of encryption.
  - ❑ It is the transformation of encrypted data back into some intelligible form.
- Encryption and Decryption require the use of some secret information, usually referred to as a key.

- Ciphers: In Cryptography, codes are called Ciphers.
- Ciphertext: The messages after coding are called as Ciphertext
- Substitution Ciphers: If each letter of alphabet is replaced by a different letter then it is called substitution Ciphers.

e.g.

A	B	C	………..	………..	Y	Z
C	D	E	………….	………..	A	B

One can observe that A is replaced by C, B is replaced by D and so on.

Hence the message "GOOD MORNING" will become "IQQF OQTPKPI"

The cipher was named in honor of Julius Caesar(Roman Dictator) who, used it to encrypt military and other official messages.

As the majority of Rome's enemies were illiterate at this time the cipher remained secure for a time.

Application of matrix to Cryptography

- One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message.
- The receiver of the message decodes it using the inverse of the matrix.
- This first matrix, used by the sender is called the encoding matrix and its inverse is called the decoding matrix, which is used by the receiver.

Modular Arithmetic

Quotient-Remainder theorem

If n is a positive integer and a, b are any integers, then we say that a is equivalent to b modulo n, which is written as $a \equiv b(mod\ n)$

i.e. n|(a-b) or (a-b)= k*n……… for k∈ Z

e.g. 25 ≡1(mod 6) ie when 25 is divided by 6, it leaves remainder 1

5 ≡2(mod 3) ie when 5 is divided by 3, it leaves remainder 2

65 ≡ 1(mod 8) ie when 65 is divided by 8, it leaves remainder 1

3 ≡3(mod 7) ie when 3 is divided by 7, it leaves remainder 3

For any modulo n it can be proved that every integer a is equivalent modulo n to exactly one of integers 0,1,2,……..,(n-1) which are called residue of a modulo n

i.e. The set Z_n={0,1,2,…..(n-1)} is called the set of residues under modulo n

e.g. Z_5={0,1,2,3,4} is set of residues under modulo 5

Exercise

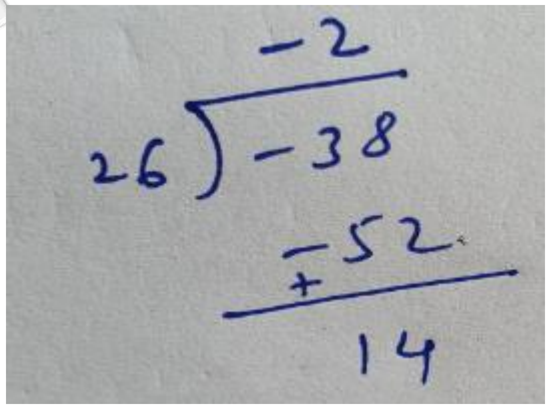
Find residues of 87, -38, -26 under mod 26

$$87 \equiv ?\,(mod\ 26)$$
$$-38 \equiv ?\,(mod\ 26)$$
$$-26 \equiv ?\,(mod\ 26)$$

Ans: $87 \equiv 9(mod\ 26)$

$-38 \equiv 14(mod\ 26)$

$-26 \equiv 0(mod\ 26)$



-2

26) -38

-52

+

14

Multiplicative Inverse of a modulo n

Definition: If g.c.d. of a & n is 1then we can find a^{-1} such that $a. a^{-1} \equiv 1(mod\ n)$, where a^{-1} is the multiplicative inverse of 'a' under modulo n.

e.g. under modulo 7, we can find, $1^{-1}, 2^{-1}, 3^{-1}, 4^{-1}, 5^{-1}, 6^{-1}$

$$1.1 \equiv 1(mod\ 7) \Rightarrow 1^{-1} = 1\ under (mod\ 7)$$

$$2.4 \equiv 1(mod\ 7) \Rightarrow 2^{-1} = 4\ under\ (mod\ 7)$$

$$3.5 \equiv 1(mod\ 7) \Rightarrow 3^{-1} = 5\ under\ (mod\ 7)$$

$$4.2 \equiv 1(mod\ 7) \Rightarrow 4^{-1} = 2\ under\ (mod\ 7)$$

$$5.3 \equiv 1(mod\ 7) \Rightarrow 5^{-1} = 3\ under\ (mod\ 7)$$

$$6.6 \equiv 1(mod\ 7) \Rightarrow 6^{-1} = 6\ under\ (mod\ 7)$$

Here, we can find multiplicative inverse of every non-zero element under modulo 7as 7 is a prime number.

Exercise

Find multiplicative inverse of all possible numbers under modulo 6

Note that only 1 and 5 are prime to 6

$$1.1 \equiv 1(mod\ 6) \Rightarrow 1^{-1} = 1\ under(mod\ 6)$$

$$5.5 \equiv 1(mod\ 6) \Rightarrow 5^{-1} = 5\ under(mod\ 6)$$

One can easily verify that $2^{-1}, 3^{-1}, 4^{-1}$ dose not exist

e.g. $2.1 \equiv 2(mod\ 6)$

$2.2 \equiv 4(mod\ 6)$

$2.3 \equiv 0(mod\ 6)$

$2.4 \equiv 2(mod\ 6)$

$2.5 \equiv 4(mod\ 6),$

Hence, $2^{-1}$is not possible under modulo 6

Exercise

Find multiplicative inverse of all possible numbers under modulo 26

First of all we will find all numbers prime to 26,

1,3,5,7,9,11,15,17,19,21,23,25

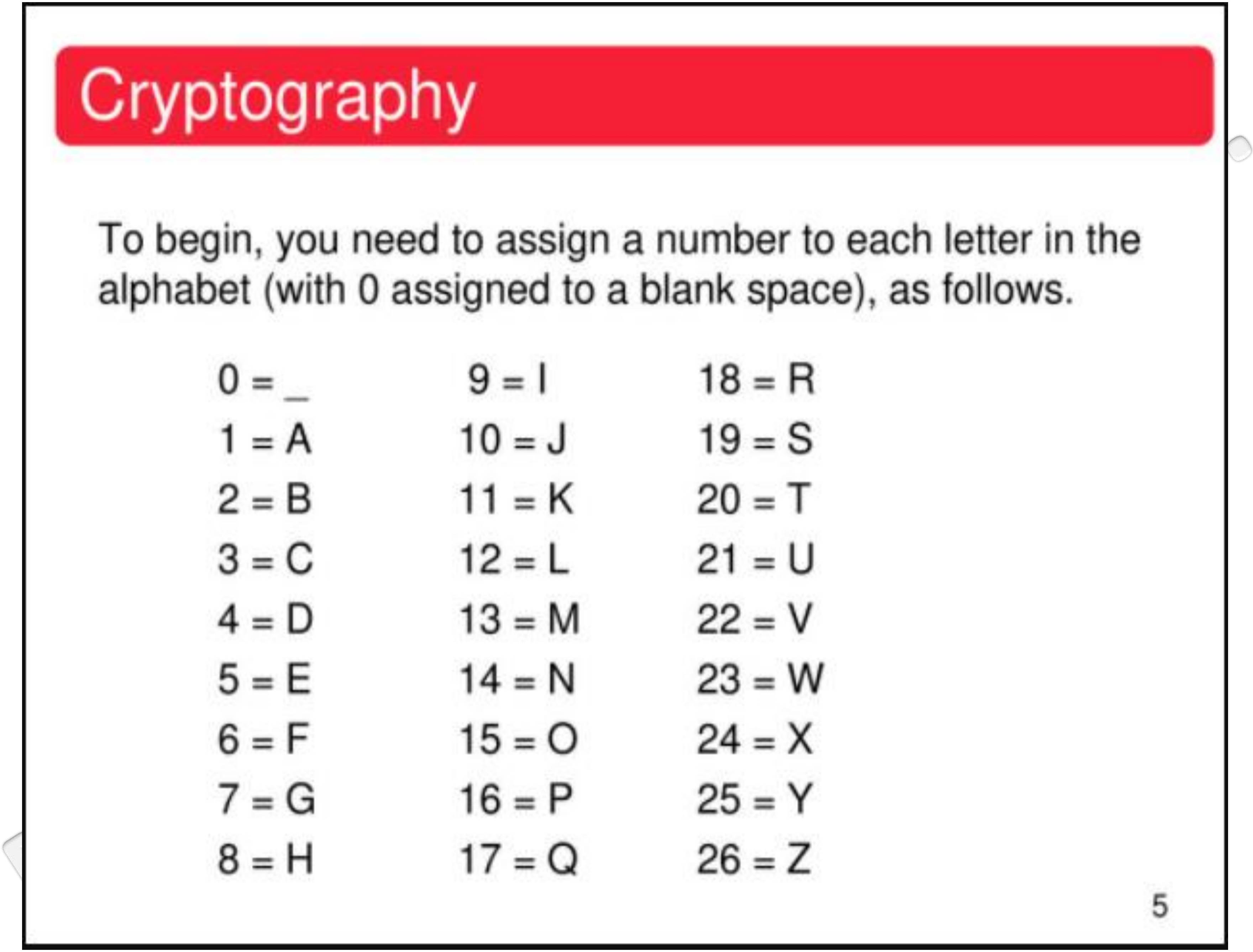
a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Exercise

Find multiplicative inverse of all possible numbers under modulo 27

Solution:

a	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25	26
a^{-1}	1	14	7	11	4	17	19	5	25	2	22	8	10	23	16	20	13	26



Cryptography

To begin, you need to assign a number to each letter in the alphabet (with 0 assigned to a blank space), as follows.

0 = _
1 = A
2 = B
3 = C
4 = D
5 = E
6 = F
7 = G
8 = H

9 = I
10 = J
11 = K
12 = L
13 = M
14 = N
15 = O
16 = P
17 = Q

18 = R
19 = S
20 = T
21 = U
22 = V
23 = W
24 = X
25 = Y
26 = Z