Application of inverse of a Matrix to a Coding theory

- Coding theory is concerned with successfully transmitting data through noisy channel and corresponding errors in corrupted messages.

- The study of Encoding and decoding a secret messages id known as **Cryptography**

- In Cryptography codes are known as **Ciphers**

- The messages are called **Plain Text**

- The messages after coding are called **Cipher text**

- The process of converting Plaintext into Ciphertext is called **Enciphering or Encoding**

- The process of converting ciphertext to plain text is called **Deciphering or Decoding**

Methods for Encoding and decoding

(1) Number Encoding(Alpha Numeric code)

In this method, each alphabet is encoded with numbers as shown in following table

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Sp
14	15	16	17	18	19	20	21	22	23	24	25	26	0

In this method , the resulting encoded matrix might contains a numbers higher that 26 or a negative number after matrix multiplication,which is not feasible while decoding the message.

(2) Different type of coding

A	B	C	D	E	F	G	H	I	J	K	L
1	(-1)	2	(-2)	3	(-3)	4	(-4)	5	(-5)	6	(-6)

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Sp
7	(-7)	8	(-8)	9	(-9)	10	(-10)	11	(-11)	12	(-12)	13	(-13)	0

(3) Modular Mathematics

Concept: CODING

- If n is positive integer and a and b are any integers , then a is equivalent to b *modulo* n if (ab) is an integer multipe of n and is denoted by $a = b(modn)$

- For any modulus n , every integer a is equivalent to $modulon$ to exactly one of the integer $0, 1, 2, ..., (n-1)$. This integer is known as **Residue** of modulo n.

- If a is non negative integer greater than n , then its residue modulo n is simply the remainder that results when, a is divided by n.

- For any integer a and $modulusn$, let R be the remainder of $\frac{|a|}{n}$, then the Residue r of *modulo* n is given by

$$r = \begin{cases} R, & if a < 0 \ and \ R = 0 \\ n - R, & if a < 0 \ and \ R \neq 0 \\ 0, & if a < 0 \ and \ R = 0 \end{cases}$$

For greater security, for decoding the message alphabets must be decoded into numbers between 1to 26, and to do so we need to apply $Modulo$ 26 or $Modulo$ 27 arithmetic and modular Arithmetic keeps all the result within desired range.

Mathematically when we have integers greater that $26(or27)$ we replace it by remainder that results when integer is divided by $26(or27)$
e.g. Find Residues of $87,_{-}38),(-26), undermodulo26$

Based on above theorem,

(i) Dividing $|87| = 87$ by 26 ,we get remainder $R = 9$, hence $r = 9$

$\therefore 87 = 9(mod\ 26)$

(ii) Dividing $|-38| = 38$ by 26 ,we get remainder $R = 12$, hence $r = 26 - 12 = 14$

$\therefore (-38) = 14(mod\ 26)$

(iii) Dividing $|-26| = 26$ by 26 ,we get remainder $R = 0$, hence $r = 0$

$\therefore (-26) = 0(mod\ 26)$

Concept: DECODING

- In ordinary arithmetic , every nonzero number a has a reciprocal or multiplicative inverse , denoted by a^{-1}, such that $a.a^{-1} = a^{-1}.a = 1$

- Similarly in Modular Mathematics , If a is number in Z_n, then number a^{-1} in Z_n is called a **reciprocal or multiplicative inverse of** a $modulo$ n if $a.a^{-1} = a^{-1}.a = 1(mod\ n)$

e.g.(1) Find the reciprocal of 9 *modulo* 26

Here number 9 has a reciprocal modulo 26 because 9 and 26 have no common prime factors.

To obtain this reciprocal , we find number x that satisfies modular equation $9x = 1(mod\ 26)$

Trying possible solutions from , 0 to 25 , one at a time , we find $x = 3$ satisfies $9.3 = 27 = 1(mod\ 26)$

Thus $9^{-1} = 3(mod\ 26)$

(2) Find the reciprocal of 11 *modulo* 27

Here number 11 has a reciprocal modulo 27 because 11 and 27 have no common prime factors.

To obtain this reciprocal , we find number x that satisfies modular equation $11x = 1(mod\ 27)$

Trying possible solutions from , 0 to 26 , one at a time , we find $x = 5$ satisfies $11.5 = 55 = 1(mod\ 27)$

Thus $11^{-1} = 5(mod\ 27)$

In Modular mathematics, we use Hill Cipher concept for Coding and Decoding.

In Hill Cipher Alphabets are assigned a number. If we do not consider "space" as a character then we use modulo 26 for coding and decoding and if we consider "space" as a character ,we use modulo 27 for coding and decoding where number 0 is assigned to "space"

The following tables are useful with Hill Cipher coding and Decoding

Table 1: Table for Hill Cipher Modulo 26

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Table 2: Table for inverse under Modulo 26

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

Table 3: Table for Hill Cipher Modulo 27

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	Sp
15	16	17	18	19	20	21	22	23	24	25	26	0

Table 4: Table for inverse under Modulo 27

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

Some results for Hill Enciphering and Deciphering

- A square Matrix A with entries in $Z_n$is invertible modulo n if and only if the residue of $|A|$ modulo n has a reciprocal (inverse) modulo n

- A square matrix A with entries in Z_n is invertible modulo n if and only if n and the residue of $|A|$ modulo n have no common prime factors.

Working Rule Algorithm for Hill Enciphering and Deciphering

Encipherment with Hill Cipher

- Suppose we are given 26 alphabets and a space and integer $n > 1$ Then a Hill n- cipher is given by an N by n matrix A with entries in Z_{27}.
- This matrix prescribe the key for cipher. For such given key matrix A, Hill Cipher algorithm to Encipher (Encode) given Pain text(message) is as follows:

  Step I: Seperate the plain text from left to right into some number k of groups (polygraphs) of n letter each. If you run out of letters when forming a final group , take space as many times as needed to fill out that fina group of n letters.

  Step II: Replace each etter by the corresponding number of its position (from 1 to 27 and space by 0) in the alphabets to get k groups of n integers each.

  Step III: Reshape each of the k groups of integers into an n-row column vectors and in turn multiply A by each of those k column vector modulo 27.

Step IV: After arranging all k of the resulting product n row column vectors in order into a single $(k.n)$ -vector(with entries in Z_{27}, replace each of these $k.n$ entries with the corresponding letter of the alphabet.

The result is the **Ciphertext** corresponding to the original plain text.

Decipherment with Hill Cipher

The transformation from ciphertext to plaintext is just the inverse of the original transformation from plain text to ciphertext.

i.e. ***If Hill cipher has key Matrix*** A ***under modulo*** 27***, then inverse transformation is the Hill cipher whose key matrix is*** A^{-1} ***under modulo*** 27

Hill Cipher coding and decoding

- Consider that the matrix A as a key matrix under modulo 27 and the matrix B is the message matrix, then encoded message is given by $= AB(mod\ 27)$ where Matrix B is formed as per order of keymatrix so that Matrix multiplication exists.

- Decoding message can be done using $B = A^{-1}C(mod\ 27)$

EXAMPLES

1. Find inverse if$A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ under (i) modulo 26 and (ii) modulo 27

   Solution(i) : For a given key matrix $A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \Rightarrow |A| = 15 - 12 = 3$

   here 3 and 26 has no common prime factors , so inverse of A under modulo 26 exists
   $\therefore 3^{-1} = 9(\text{mod } 26)$

$$\begin{aligned}
\therefore A^{-1} &= 9 \begin{pmatrix} 3 & -6 \\ -2 & 5 \end{pmatrix} (\text{mod } 26) \\
&= \begin{pmatrix} 27 & -54 \\ -18 & 45 \end{pmatrix} (\text{mod } 26) \\
&= \begin{pmatrix} 1 & 24 \\ 8 & 9 \end{pmatrix} (\text{mod } 26)
\end{aligned}$$

   is the required inverse under mod 26

   Solution(ii) : For a given key matrix $A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \Rightarrow |A| = 15 - 12 = 3$

   here 3 and 27 has common prime factors , so inverse of A under modulo 27 does not exist

2. Encode and Decode "THE PROFESSOR IS GOOD" using $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ under (i)modulo 26 and (ii)modulo 27

3. Encode "SECRET CODE" using $A = \begin{pmatrix} 1 & 1 \\ 2 & 6 \end{pmatrix}$ under (i)modulo 26 and (ii)modulo 27