1ZC3 Engineering Math II-B (Linear Algebra I)

(WS 19 C03) Lecture 36

Last Time Hill 2-Ciphers & Counting Modulo 26

- "Plaintext" Message : e.g. GET OUT
- Convert to #s $\{1, \ldots, 25, 0\}$ ($A, \ldots, Y, Z$): 7 5 20 15 21 20
- Pair up into plaintext vectors: $\begin{bmatrix} 7 \\ 5 \end{bmatrix}, \begin{bmatrix} 20 \\ 15 \end{bmatrix}, \begin{bmatrix} 21 \\ 20 \end{bmatrix}$
- Apply matrix A: e.g. $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$: $\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 21 \\ 20 \end{bmatrix} = \begin{bmatrix} 63 \\ 41 \end{bmatrix}$
- Convert to ciphertext vectors mod 26 : $\begin{bmatrix} 11 \\ 11 \\ 15 \end{bmatrix}$ K K O
- Send corresponding letters ("ciphertext")

Multiplication mod 26

Examples
$$3 \times 4 = 12 = 12 \pmod{26}$$
$$5 \times 7 = 35 = 9 \pmod{26}$$
$$11 \times 19 = 209 = 1 \pmod{26}$$

Definition If $b \in \mathbb{Z}_m$ (i.e. $\{0, \ldots, m-1\}$), then if there is another # in $\mathbb{Z}_m$, call it b^{-1},

with $bb^{-1} = b^{-1}b = 1 \pmod{m}$, we call b^{-1} the reciprocal of b modulo m.

Example 11 is the reciprocal of 19 modulo 26

19 " " " " 11 " " .

Fact (about mod 26) $b \in \mathbb{Z}_{26}$ has a reciprocal exactly when it does NOT have EITHER 2 OR 13 as a divisor.

We get pairs

1	3	5	7	$\binom{9}{3}$	11	$\binom{15}{7}$	17	$\binom{19}{11}$	$\binom{21}{5}$	$\binom{23}{17}$	25
1	9	21	15		19		23				25

(Good idea to know this table.)

$3 \times 9 = 27 = 1 \pmod{26}$ ↖ $5 \times 21 = 105 = 1 \pmod{26}$

We can extend arithmetic ideas to matrices

Example $\begin{bmatrix} 0 & 5 \\ 7 & -3 \end{bmatrix}\begin{bmatrix} 10 & -12 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 15 \\ 64 & -93 \end{bmatrix} = \begin{bmatrix} 10 & 15 \\ 12 & 11 \end{bmatrix} \pmod{26}$

How to decode ciphertext?

$AP_i = C_i$

P_i: plaintext vector

C_i: ciphertext vector

We send $C_i \pmod{26}$

So we can't just use A^{-1} !!

We need an inverse modulo 26! i.e. "A^{-1}"

with $AA^{-1} = A^{-1}A = I \pmod{26}$ AND need

to stay inside $\mathbb{Z}_{26} = \{0, \ldots, 25\}$ i.e. all entries of "A^{-1}" should be in $\mathbb{Z}_{26}$.

To find the inverse of $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ modulo 26.

First find $A^{-1} = (\det(A))^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$(\det(A))^{-1}$ is the reciprocal of $\det(A) \pmod{26}$

2 Choices

Replace this with $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$

or not

Then multiply through by $(\det(A))^{-1}$ & convert all entries modulo 26.

This means the "rule" for choosing A for this Hill cipher process is that $\det(A) \pmod{26}$ has a reciprocal modulo 26. (So we cannot have that $\det(A) \pmod{26}$ is even or 13.)

Example Find the inverse of $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$ modulo 26.

Solution First find usual $A^{-1} = 3^{-1}\begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix}$

Here 3^{-1} does NOT mean $\frac{1}{3}$. It means the reciprocal of 3 modulo 26, i.e., 9.

$$= 9\begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix}$$

multiply through right away.

$$= \begin{bmatrix} 9 & 0 \\ -9 & 27 \end{bmatrix} = \begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \pmod{26}$$

Example Find the inverse of $A = \begin{bmatrix} 1 & 2 \\ 10 & 3 \end{bmatrix}$ modulo 26.

Solution First: $A^{-1} = (9)^{-1}\begin{bmatrix} 3 & -2 \\ -10 & 1 \end{bmatrix}$

$$\det(A) = 3 - 20 = -17 = (-17 + 26) \pmod{26} = 9 \pmod{26}$$

Reciprocal of 9: $(9)^{-1}$

Can also just do:

$$= 3\begin{bmatrix} 3 & -2 \\ -10 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & -6 \\ -30 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 20 \\ 22 & 3 \end{bmatrix} \pmod{26}$$

$$= 3\begin{bmatrix} 3 & 24 \\ 16 & 1 \end{bmatrix} \pmod{26}$$

Now multiply through

$$= \begin{bmatrix} 9 & 72 \\ 48 & 3 \end{bmatrix} \pmod{26}$$

Here the entries of the adjugate/adjoint matrix above replaced mod 26

$$= \begin{bmatrix} 9 & 20 \\ 22 & 3 \end{bmatrix} \pmod{26}$$

To decipher, same process as enciphering, but use the inverse of A modulo 26 in place of A.

Example Use $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$ to decode UL HI KO.

$\begin{bmatrix} 21 \\ 12 \end{bmatrix} \begin{bmatrix} 8 \\ 9 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix}$

We'll need $A^{-1} \bmod 26$

$= \begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}$ (from above)

$189 = (189-156) \pmod{26} = 33 \pmod{26}$
$= 7 \pmod{26}$

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 12 \end{bmatrix} = \begin{bmatrix} 189 \\ 369 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \end{bmatrix}$ G E

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 72 \\ 145 \end{bmatrix} = \begin{bmatrix} 20 \\ 15 \end{bmatrix}$ T O

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 99 \\ 202 \end{bmatrix} = \begin{bmatrix} 21 \\ 20 \end{bmatrix}$ U T

Try to check using division by 26 with remainder, or subtracts multiples of 26.

Example Decode HB CO GJ SJ using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$.

Solution

$\begin{bmatrix} 8 \\ 2 \end{bmatrix} \begin{bmatrix} 3 \\ 15 \end{bmatrix} \begin{bmatrix} 7 \\ 10 \end{bmatrix} \begin{bmatrix} 19 \\ 10 \end{bmatrix}$

$A^{-1} \bmod 26 = \begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}$

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 2 \end{bmatrix} = \begin{bmatrix} 72 \\ 138 \end{bmatrix} = \begin{bmatrix} 20 \\ 8 \end{bmatrix} \pmod{26}$ T H

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 27 \\ 66 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \pmod{26}$ A N

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 7 \\ 10 \end{bmatrix} = \begin{bmatrix} 63 \\ 129 \end{bmatrix} = \begin{bmatrix} 11 \\ 25 \end{bmatrix} \pmod{26}$ K Y

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix} \begin{bmatrix} 19 \\ 10 \end{bmatrix} = \begin{bmatrix} 171 \\ 339 \end{bmatrix} = \begin{bmatrix} 15 \\ 21 \end{bmatrix} \pmod{26}$ O U