1B03 – LINEAR ALGEBRA 1 (C01) WS19 Lecture 36

Last Time Hill 2-Ciphers & Counting Modulo 26

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

In $\mathbb{Z}_{26} = \{0, \ldots, 25\}$ every # a has a "reciprocal" if 2 and 13 do NOT divide a

e.g. 19 is the reciprocal of 11 modulo 26 since $19 \times 11 = 209 = 1 \bmod 26$

So we have 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
	11	11									
	27	105									

(Good idea to know these.)

We can extend arithmetic ideas to matrices

e.g. $\begin{bmatrix} 0 & 5 \\ 7 & -3 \end{bmatrix}\begin{bmatrix} 10 & -12 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 10 & 15 \\ 64 & -93 \end{bmatrix} =$

$\begin{bmatrix} 10 & 15 \\ 12 & 11 \end{bmatrix} \pmod{26}$

$64 = (64 - 52) \pmod{26} = 12 \pmod{26}$

$-93 = (-93 + 104) \pmod{26} = 11 \pmod{26}$

How to decode ciphertext?

$AP_i = C_i \Rightarrow C_i = A^{-1}P_i$? Not quite

P_i: plaintext, C_i: ciphertext

We don't send AP_i we send $AP_i \pmod{26}$

So we need an "inverse" to "undo" the addition/subtraction of multiples of 26.

We need to keep inside $\mathbb{Z}_{26} = \{0, \ldots, 25\}$

i.e. we want "A^{-1}" so that $AA^{-1} = A^{-1}A = I \pmod{26}$

& all entries in "A^{-1}" in $\mathbb{Z}_{26}$

So how?

We know, if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, that $A^{-1} = (\det A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

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

Replace adjoint of A with its equivalent modulo 26.

+ multiply through & make sure you have just a 2×2 matrix at the end with entries in $\mathbb{Z}_{26}$.

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

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

$\det(A) = 3$

Replace $(3)^{-1}$ with reciprocal of 3 in $\mathbb{Z}_{26}$ i.e. 9

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

$= \begin{bmatrix} 9 & 0 \\ -9 & 27 \end{bmatrix}$

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

Example $A = \begin{bmatrix} 1 & 2 \\ 10 & 3 \end{bmatrix}$. Find A^{-1} modulo 26.

Solution First find $\det(A) = 3 - 20 = -17$

$= (-17 + 26) \pmod{26}$

$= 9 \pmod{26}$

Now $(\det(A))^{-1}$ = reciprocal of 9 modulo 26

$= 3$

Then $A^{-1} = (\det(A))^{-1} \begin{bmatrix} 3 & -2 \\ -10 & 1 \end{bmatrix} = 3 \begin{bmatrix} 3 & -2 \\ -10 & 1 \end{bmatrix}$

Before multiplying through, you can convert this mod 26 here...

$= \begin{bmatrix} 9 & -6 \\ -30 & 3 \end{bmatrix} = \begin{bmatrix} 9 & 20 \\ 22 & 3 \end{bmatrix} \pmod{26}$ ...or not

$3 \begin{bmatrix} 3 & 24 \\ 16 & 1 \end{bmatrix} = \begin{bmatrix} 9 & 72 \\ 48 & 3 \end{bmatrix}$

Use $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$ to decode U L H I K O.

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

First find A^{-1} modulo 26 (see above): $\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}$

Pair up letters, convert to 2-tuples of #s, multiply by A^{-1} modulo 26 & convert back to letters.

In turn: $\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}\begin{bmatrix} 21 \\ 12 \end{bmatrix} = \begin{bmatrix} 189 \\ 369 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \end{bmatrix} \pmod{26}$ G E

Do check these!

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 72 \\ 145 \end{bmatrix} = \begin{bmatrix} 20 \\ 15 \end{bmatrix} \pmod{26}$ T O

$\begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}\begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 99 \\ 202 \end{bmatrix} = \begin{bmatrix} 21 \\ 20 \end{bmatrix} \pmod{26}$ U T

Now decode: HBCOGJSJ using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

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

$\left[\text{i.e. } A^{-1} = \begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}\right]$.

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

$138 - 104 = 34$
$= 34 - 26$

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

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

$A^{-1}\begin{bmatrix} 19 \\ 10 \end{bmatrix} = \begin{bmatrix} 9 & 0 \\ 17 & 1 \end{bmatrix}\begin{bmatrix} 19 \\ 10 \end{bmatrix} = \begin{bmatrix} 171 \\ 333 \end{bmatrix} = \begin{bmatrix} 15 \\ 21 \end{bmatrix} \pmod{26}$ O U

$333 - 208 = 125$
-104
21