1ZC3 Modular Arithmetic

$a = b \bmod p$ if $a = b + np$, $n \in \mathbb{Z}$

$a =_p b$

or $a \equiv b \bmod p$

} alternate notations

$a \equiv b \bmod p$ means a, b in same equivalence class

or congruence class

or residue class

act as "same number"

in "mod p" system $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}_p$

eg $2 + 6 = 8 \mod 7$

$= 1$

$2 + (-1) = 1$ $\quad (6 \equiv -1, \mod 7)$

eg Compute $48 \cdot 45 \mod 50$

$48 \equiv -2 \mod 50$, $45 \equiv -5 \mod 50$

$48 \cdot 45 \equiv (-2)(-5) \equiv 10 \mod 50$

Hill Cipher & Encryption

26 letters in english =>

A	B	C	....	M	....	X	Y	Z
1	2	3		13		24	25	0

use #, mod 26

Remember Inverses in "mod p"

a^{-1} exists if $a\,a^{-1} \equiv 1 \pmod{p}$.

a^{-1} only exists if $\gcd(a, p) = 1$

(ie no common factors).

For our calculations, mod 26, it's a very good idea to know our inverses

No even # or 13 has an inverse ($26 = 2 \cdot 13$)

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

$3 \cdot ? = 1 + n\,26$

$5 \cdot ? = 1 + n\,26 \rightarrow = 26+1$

$= 52+1$

$= 78+1$

$= 104+1 = 105$ ✓

$5 \cdot 21 = 105 \equiv 1 \pmod{26}$

$= 15 \cdot 7$

$25 = -1 \pmod p \quad (-1)^2 = 1 \Rightarrow 25^2 = 1 \pmod p$

$23 = -3 \pmod p \quad (-3)(-9) = 27 = 1 \pmod p$

$=$

d

$= 17 \pmod p$

Let's do the Hill Cipher

$A = 1, B = 2, \ldots Y = 25, Z = 0$ & write message as set of vectors.

eg. "Messages" $\Rightarrow$ "MESSAGES"

M E S S A G E S

13 5 19 19 1 7 5 19

$\Rightarrow \begin{bmatrix} 13 \\ 5 \end{bmatrix}, \begin{bmatrix} 19 \\ 19 \end{bmatrix} \begin{bmatrix} 1 \\ 7 \end{bmatrix} \begin{bmatrix} 5 \\ 19 \end{bmatrix}$

Now we need an encryption matrix, $\underline{\underline{M}}$, invertible mod 26

(det(M) invertible mod 26)

$M \cdot (\text{vector}) = (\text{new message}) \Rightarrow$ encrypts!

$M^{-1} \cdot (\text{new vector}) = (\text{old vector}) \Rightarrow$ decrypts!

Basic eg. Message "AH", Encryption matrix $M = \begin{bmatrix} 2 & 5 \\ 7 & 10 \end{bmatrix}$

So Let's apply this Hill Cipher, get new message.

then Find inverse matrix & decrypt!

Solution: "AH" ~ $\begin{bmatrix} A \\ H \end{bmatrix} \to \begin{bmatrix} 1 \\ 8 \end{bmatrix}$ } expressed as a "mod 26" vector

Apply cipher: $M \begin{bmatrix} A \\ H \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ 7 & 10 \end{bmatrix} \begin{bmatrix} 1 \\ 8 \end{bmatrix}$

$= \begin{bmatrix} 2 + 40 \\ 7 + 80 \end{bmatrix} = \begin{bmatrix} 42 \\ 87 \end{bmatrix} = \begin{bmatrix} 16 \\ 9 \end{bmatrix}$

$= \begin{bmatrix} P \\ I \end{bmatrix} = "PI"$

To decrypt! $M = \begin{bmatrix} 2 & 5 \\ 7 & 10 \end{bmatrix}$

$M^{-1} = \begin{bmatrix} 10 & -5 \\ -7 & 2 \end{bmatrix} \cdot (2 \cdot 10 - 7(5))^{-1}$

$= 11 \bmod 26$

$11^{-1} = 19 \bmod 26$

$= -7 \bmod 26$

(easier to use!)

$= \begin{bmatrix} -70 & 35 \\ 49 & -14 \end{bmatrix} = \begin{bmatrix} 8 & 9 \\ 23 & 12 \end{bmatrix} \bmod 26$

$-70 + 3 \cdot 26 = -70 + 78$

$= 8 \bmod 26$

or equivalently

$= \begin{bmatrix} 8 & 9 \\ -3 & 12 \end{bmatrix} \bmod 26.$

So decrypt "PI" = $\begin{bmatrix} 16 \\ 9 \end{bmatrix}$

$$M^{-1}\begin{bmatrix} P \\ I \end{bmatrix} = M^{-1}\begin{bmatrix} 16 \\ 9 \end{bmatrix} = \begin{bmatrix} 8 & 9 \\ -3 & 12 \end{bmatrix}\begin{bmatrix} 16 \\ 9 \end{bmatrix}$$

$$= \begin{bmatrix} 128 + 81 \\ 30 + 108 \end{bmatrix} = \begin{bmatrix} 1 \\ 8 \end{bmatrix} = \begin{bmatrix} A \\ H \end{bmatrix}$$

"AH"

$138 - 4 \cdot 26$

$= 34 - 26 = 8$ mod