§ More Applications of Modular Arithmetic:

$\mathbb{Z}_{26} = \{0, 1, 2, \ldots\ldots, 25\}$ is important for enciphering or encrypting messages (called Plain text) using an enciphering fn

f_E : Plain text $\longrightarrow$ Cipher text

as follows:

A $\longleftrightarrow$ 0
B $\longleftrightarrow$ 1
C $\longleftrightarrow$ 2
⋮
Y $\longleftrightarrow$ 24
Z $\longleftrightarrow$ 25

Now Fix $a, b \in \mathbb{Z}_{26}$ & define

$$f_E : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$$
$$: x \longrightarrow ax + b.$$

Ex Encipher the Plaintext BABA By Applying the enciphering fn

$$f_E : x \longrightarrow 3x + 4$$

to 1-letter message units over the alphabet A = 0, B = 1, etc Z = 25

B = 1 A = 0 $\Rightarrow$

B: $f_E : 1 \longrightarrow 3(1) + 4 = 7$ so B → H

A: $f_E : 0 \longrightarrow 3(0) + 4 = 4$ so A → E

So The message BABA $\longrightarrow$ HEHE.

Ex : CAT = Plain text

& $f_E : x \longrightarrow 7x + 20$

C = 2 ; A = 0 ; T = 19

So : C = 2 so $f_E : 2 \longrightarrow 7(2) + 20 = 34 = 8 \leftrightarrow I$ in $\mathbb{Z}_{26}$

$(34 = 26(1) + 8)$

So C $\xrightarrow{f_E}$ I

A = 0 so $f_E : 0 \longrightarrow 7(0) + 20 = 20 \leftrightarrow U$

So A $\xrightarrow{f_E}$ U

T = 19 so $f_E : 19 \longrightarrow 7(19) + 20 = 133 + 20$
$= 153 = 23 \leftrightarrow X$

$(153 = 26(5) + 23)$

So T $\xrightarrow{f_E}$ X

ie the Plain text CAT $\longrightarrow$ IUX

IUX ↓ Cipher text

Note : To decipher we do the following :

$$f_E : x \longrightarrow 7x + 20 = y$$

$$\xleftarrow{\quad D_E \quad}$$

$$D_E : y \longrightarrow 7^{-1}(y - 20)$$

$$= 7^{-1}((7x + 20) - 20)$$

$$= 7^{-1}7x = x$$

ie $y \longrightarrow 15(y - 20)$

Because $15 = 7^{-1}$ in $\mathbb{Z}_{26}$

as $(15)(7) = 105 = 1$ in $\mathbb{Z}_{26}$

$(105 = (4)26 + 1)$

e.g in IUX ; $X \leftrightarrow 23 = y$

$23 \longrightarrow 15(23 - 20) = 45 = 19$ in $\mathbb{Z}_{26}$

$(45 = 26(1) + 19)$ $\quad \updownarrow$ T

So X get deciphered to T ✓

It was important that 7^{-1} existed

ie that $\gcd(7, 26) = 1$

So when choosing $a, b \in \mathbb{Z}_{26}$ for $f_E : x \longrightarrow ax + b$ want $\gcd(a, 26) = 1$

Ex: We can also use matrices with entries in $\mathbb{Z}_{26}$ to send messages 2 letters at a time as follows:

Encipher the Plain text BABA By applying the enciphering function

$$f_E : \begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 2 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 12 \\ 21 \end{pmatrix}$$

to 2-letter message units over the alphabet $A = 0$, $B = 1$, $\ldots$ $Z = 25$

$$\underbrace{BA}\ \widetilde{BA} \longleftrightarrow \underbrace{10}\ \widetilde{10}$$

$$f_E : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 2 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 12 \\ 21 \end{pmatrix}$$

$$= \begin{pmatrix} 3 \\ 1 \end{pmatrix} + \begin{pmatrix} 12 \\ 21 \end{pmatrix} = \begin{pmatrix} 15 \\ 22 \end{pmatrix} = \begin{pmatrix} P \\ W \end{pmatrix}$$

So BABA $\longrightarrow$ PWPW