§ 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

↓

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

§ THE CHINESE REMAINDER THEOREM: This theorem says: FOR $n_1, n_2 \in \mathbb{N}$ & $n_1 \& n_2 > 1$ s.t. $\gcd(n_1, n_2) = 1$ (we say n_1 & n_2 are COPRIME) the simultaneous congruences

$$x \equiv a_1 \bmod n_1$$
& $$x \equiv a_2 \bmod n_2$$

have a unique solution modulo $n_1 \cdot n_2$

Ex: Solve the simultaneous congruences

$$x \equiv 4 \bmod 7$$
$$x \equiv 3 \bmod 9$$

METHOD 1: $x \equiv 4 \bmod 7 \Rightarrow$ x leaves a remainder 4 when divided by 7

$\Rightarrow$ x is of the form

$x = 4 + n7$ for some $n \in \mathbb{N}$

$\Rightarrow x \in \{4, 4+7, 4+(2)7, \text{etc}\}$ ie

ie $x \in \{4, 11, 18, 25, 32, \boxed{39}, 46, \cdots\}$

& $x \equiv 3 \bmod 9 \Rightarrow$ x leaves a remainder 3 when divided by 9

$\Rightarrow$ x is of the form

$x = 3 + m9$ for some $m \in \mathbb{N}$

$\Rightarrow x \in \{3, 3+9, 3+(2)9, 3+(3)9, \cdots \text{etc}\}$

ie $x \in \{3, 12, 21, 30, \boxed{39}, 48, \cdots\}$

So $39 = x$ lies in both sets & is the smallest soln.

So too does $x = 39 + s(7)(9)$ for $s \in \mathbb{N}$.

Method 2: $x \equiv 4 \mod 7$ ··— (i)
$x \equiv 3 \mod 9$ ··-- (ii)

By (i) we have that $x = 4 + 7n \equiv 3 \mod 9$ (By (ii))

So $7n \equiv (-4) + 3 \mod 9 \equiv -1 \mod 9$
$\equiv 8 \mod 9$

$\Rightarrow (7^{-1})(7)n \equiv (7^{-1})(8) \mod 9$

But $7^{-1} = 4$ in $\mathbb{Z}_9$ Because
$(4)(7) = 28 = 1$ in $\mathbb{Z}_9$

So $n \equiv (4)(8) \mod 9$ $(28 = 9(3) + \underline{1})$

$\Rightarrow n \equiv 5 \mod 9$ $(32 = 9(3) + \underline{5})$

$\Rightarrow n = 5 + 9m$

$\Rightarrow x = 4 + 7(5 + 9m) = \underline{39} + (7)(9)m$ ✓
for some $m \in \mathbb{N}$

Recall: How to Solve a Pair of Simultaneous congruences of the form

(i) $x \equiv 4 \bmod 5$ (x leaves Remainder 4 when divided by 5

(ii) $x \equiv 2 \bmod 7$ (R x leave remainder 2 when divided by 7

Method 1: (Easy)

i) $\Rightarrow x \in \{ 4, \boxed{9}, 14, 19, 24, 29, 34, 39, \ldots \}$

ii) $\Rightarrow x \in \{ 2, \boxed{9}, 16, \ldots \}$

So $x = 9$ & all other solns are of the form $9 + m(5)(7)$, $m \in \mathbb{N}$

ie 9 is the unique soln mod 35

Method 2: (i) $\Rightarrow x = 4 + n5 \equiv 2 \bmod 7$ (By (ii)

$\Rightarrow 5n \equiv -4+2 \bmod 7$

$\Rightarrow 5n \equiv -2 \bmod 7$

$\Rightarrow 5n \equiv 5 \bmod 7$

$\Rightarrow \underbrace{5^{-1}(5)}_{1}(n) \equiv 5^{-1}(5) \bmod 7$

$\Rightarrow n \equiv 3(5) \bmod 7$

(But $3(5) \overset{=15}{\equiv} 1 \bmod 7$
$\Rightarrow 5^{-1} = 3$ in $\mathbb{Z}_7$

$\Rightarrow n \equiv 1 \bmod 7$

$\Rightarrow n = 1 + m(7)$ $m \in \mathbb{N}$

So $x = 4 + 5(1 + m(7)) = 9 + m(5)(7)$ ✓