§ 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

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

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: $x \equiv 4 \bmod 7$ — (i)
$x \equiv 3 \bmod 9$ --- (ii)

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

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

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

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

So $n \equiv (4)(8) \bmod 9$ $(28 = 9(3) + 1)$

$\Rightarrow n \equiv 5 \bmod 9$ $(32 = 9(3) + 5)$

$\Rightarrow n = 5 + 9m$

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

§ The Euler ϕ fn: (NOT on the Exam But Appears on Final HW sheet)

FOR $n > 1$, $n \in \mathbb{N}$:

$\phi(n) :=$ the number of elements $a \in \mathbb{Z}_n$ s.t. $\gcd(a, n) = 1$ (a & n are coprime)
= the number of elements $a \in \mathbb{Z}_n$ s.t. a^{-1} exists in $\mathbb{Z}_n$.

Fact: Write $n = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$ as a product of prime powers e.g. $n = 108 = 2^2 \cdot 3^2 \cdot 5$

Then $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$

e.g. $\phi(180) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 180\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$

$= 48$

(Explanation of the formula for $\phi(n)$

$\frac{\phi(n)}{n}$ = Probability or chances or odds of choosing a number in $\mathbb{Z}_n$ s.t. $\gcd(a, n) = 1$.

ie s.t. no prime dividing n (ie $p_1, \ldots, p_r$) also divides a

e.g $p_1 = 2$ every 2nd number is div by 2

so the Prob that $2 \mid a = \frac{1}{2}$

& the Prob that $2 \nmid a = 1 - \frac{1}{2}$

say $p_2 = 3$ every 3rd number is div by 3

so the Prob that $3 \mid a = \frac{1}{3}$

$\Rightarrow$ " " " $3 \nmid a = 1 - \frac{1}{3}$

etc

so $\frac{\phi(n)}{n} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$

& $\Rightarrow \phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$

Some Questions on the Sample 6th HW sheet.

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) $x \equiv 2 \bmod 7$ (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) $\Rightarrow x = 4 + 5n \equiv 2 \bmod 7$ (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 $x = 4 + 5(1 + m(7)) = 9 + m(5)(7)$ ✓

Q.4. If $n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_r^{s_r}$ is the prime power decomposition of n as a product of prime powers then

FACT: $\phi(n)$:= The number of elements a in $\mathbb{Z}_n$ s.t. $\gcd(a,n) = 1$ i.e. s.t. $a^{-1} \in \mathbb{Z}_n$ exists.

Then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

Ex: $n = 504 = 2^3 \cdot 3^2 \cdot 7$

$\therefore \phi(504) = 504\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right)$

$= 504 \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{6}{7}\right) = 144$

Q.5. $$A = \begin{pmatrix} 4 & 6 & 2 \\ 2 & 4 & 6 \\ 6 & 2 & 4 \end{pmatrix}$$

Then $$A^{-1} = \frac{1}{|A|}\left((-1)^{i+j} d_{ij}\right)^T$$

where d_{ij} = the determinant of the 2×2 matrix obtained from A by deleting the ith row & j-th col.

& $|A| = a_{11}d_{11} - a_{12}d_{12} + a_{13}d_{13}$