1) The numbers $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ form a complete residue system modulo 7.

Complete residue system modulo 7 = $\{0, 1, 2, 3, 4, 5, 6,\}$

0^2 mod 7 = 0. 1^2 mod 7 = 1 2^2 mod 7 = 4.

3^2 mod 7 = 2 4^2 mod 7 = 2 5^2 mod 7 = 4

6^2 mod 7 = 1.

we can observe that $4^2 \equiv 3^2$ mod 7 and no integer in the set $\equiv 5$ mod 7.

⇒ False . Justification : The complete residue system modulo 7 is the set of integers 0, 1, ... 6 . $0^2, 1^2 \ldots 6^2$ doesn't belong to the particular set. (1 Mark)

2) There exists an integer x such that

$3x \equiv 347$ mod 453 $a = 3$ $b = 347$ $n = 453$.

$(a, n) = (3, 453) = 3$.

$\Rightarrow \cancel{\frac{347}{3}}$

⇒ False . Justification :- Its a linear congruence relation. For x to exist, $\frac{b}{(a,n)}$. Here $\cancel{\frac{b}{(a,n)}}$. ∴ There is no x satisfying $3x \equiv 347$ mod 453. (1 Mark)

3) Find the number of +ve integers less than or equal to 1500 which are not divisible by 2, 3 & 5.

Ans : $1500 = 2^2 \times 3 \times 5^3$

2, 3 & 5 are the only prime factors of 1500.

Now the problem reduces to finding the $\phi(1500)$.

Because $\phi(1500)$ ~~contra~~ gives the no: of integers less than 1500 which are relatively prime to ~~ϕ~~ 1500.

∴ ~~The no: of intege~~ (the no: of)

∴ All the integers, which are not divisible by the prime factors of 1500 ~~500~~ can be computed by just computing $\phi(1500)$. (1 Mark)

$$\phi(1500) = 1500 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

(1 Mark)

$$= \underline{\underline{400}}$$

4) Find the least +ve residue of $2^{179} \bmod 89$

Ans: $a = 2 \quad n = 89$

$(a, n) = (2, 89) = 1.$

$\Rightarrow n$ is prime. [1 Mark for identifying application of fermat's theorem]

Apply Fermat's theorem

$$a^{p-1} \equiv 1 \bmod p.$$

$$2^{88} \equiv 1 \bmod 89.$$

$$2^{179} \bmod 89 = \left[(2^{88})^2 \times 2^3\right] \bmod 89.$$

$$= \left[(2^{88})^2 \bmod 89 \times 2^3 \bmod 89\right] \bmod 89$$

[1 Mark for calculation]

$$= \underline{\underline{8}}$$

5) If $a, n \in N$ and if there exists $k \in N$ such that $a^k \equiv 1 \bmod n$, then prove that $(a, n) = 1$. (2 Marks)

Ans: ~~Assume~~ Given $a^k \equiv 1 \bmod n$.

Assume $d = (a, n) > 1$.

$\Rightarrow a^k \equiv 1 \bmod n \Rightarrow a^k - 1 = nt$.

$a^k = nt + 1$.

$\Rightarrow d = (a, n)$ implies that $\frac{a}{d}$ & $\frac{n}{d}$.

$\Rightarrow$ Since $\frac{a}{d}$ then $\frac{a^k}{d}$

ie $\frac{nt+1}{d}$ $\Rightarrow$ For $nt+1$ to be divisible by d both nt & 1 should be divisible by d.

$\Rightarrow \frac{nt}{d}$ since $\frac{n}{d}$.

$\Rightarrow \cancel{\frac{1}{d}}$ since $d > 1$.

So if $\frac{a^k}{d}$, 1 should be divisible by d.

ie possible only if $(a, n) = 1$.

$\therefore$ If $a^k \equiv 1 \bmod n$ then gcd $(a, n) = 1$.

6) Solve the following simultaneous linear congruences.

$2x \equiv 1 \mod 5$ $\quad 3x \equiv 9 \mod 6$ $\quad 4x \equiv 1 \mod 7$.

Ans: Reduce the congruence relations to the form of simultaneous linear congruences.

(1) $2x \equiv 1 \mod 5$. , $(5,2)=1$. $\quad 5 = 2\times 2+1$
$2 = 2\times 1+0$.

$1 = 5 - 2\times 2$.

$x \equiv -2 \mod 5$. [Multiply with inverse of 2].

$\boxed{x \equiv 3 \mod 5.}$

(2) $3x \equiv 9 \mod 6$.

(÷) 3 $\quad x \equiv 3 \mod 2$.

$\boxed{x \equiv 1 \mod 2.}$

(3) $4x \equiv 1 \mod 7$ $\quad (7,4)$

$7 = 1\times 4+3$.

$4 = 1\times 3+1$

$3 = 3\times 1+0$.

$\boxed{x \equiv 2 \mod 7}$

$1 = 4 - 1\times 3$

$= 4 - 1[7 - 1\times 4]$

$= -1\times 7 + 2\times 4$.

1½ Marks

$b_1 = 3 \quad b_2 = 1 \quad b_3 = 2$.

$n_1 = 5 \quad n_2 = 2 \quad n_3 = 7$.

$N = n_1 \times n_2 \times n_3 = 70$.

$N_1 = \frac{N}{n_1} = 14$

$N_2 = \frac{N}{n_2} = 35$

$N_3 = \frac{N}{n_3} = 10.$

1 Mark.

$(N_1, n_1) \quad (14,5) \Rightarrow \quad 14 = 2 \times 5 + 4 \qquad 1 = 5 - 1 \times 4$

$5 = 1 \times 4 + 1 \qquad = 5 - 1\left[14 - 2 \times 5\right]$

$4 = 4 \times 1 + 0 \qquad = -1 \times 14 + 3 \times 5.$

$N_1^{-1} = -1$

$(N_2, n_2) \quad (35, 2) \Rightarrow \quad 35 = 17 \times 2 + 1 \qquad 1 = 35 - 17 \times 2.$

$2 = 2 \times 1 + 0.$

$N_2^{-1} = 1$

$(N_3, n_3) \quad (10, 7) \quad 10 = 1 \times 7 + 3 \qquad 1 = 7 - 2 \times 3$

$7 = 2 \times 3 + 1 \qquad = 7 - 2\left(10 - 1 \times 7\right]$

$3 = 3 \times 1 + 0 \qquad = -2 \times 10 + 2 \times 7.$

$N_3^{-1} = -2$

$x = \left[b_1 N_1 N_1^{-1} + b_2 N_2 N_2^{-1} + b_3 N_3 N_3^{-1}\right] \bmod N.$

$= \left[3 \times 14 \times -1 + 1 \times 35 \times 1 + 2 \times \overset{10}{\cancel{20}} \times -2\right] \bmod 70$

½ marks

$= \underline{\underline{23}}$

7) Find all natural numbers n such that $\phi(n) = n/3$ if any.

Ans: $n = p_1^{m_1} \, p_2^{m_2} \dots p_k^{m_k}$.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \dots \left(1-\frac{1}{p_k}\right)$$

$$= n \; p_1^{-1} \times p_2^{-1} \times \dots p_k^{-1} (p_1-1)(p_2-1)\dots(p_k-1)$$

Given $\phi(n) = n/3$.

$$\cancel{n} \; p_1^{-1} \times p_2^{-1} \times \dots p_k^{-1} (p_1-1)(p_2-1)\dots(p_k-1) = \frac{\cancel{n}}{3}$$

$$\therefore \; 3(p_1-1)(p_2-1)\dots(p_k-1) = p_1 \times p_2 \times \dots p_k$$

$\therefore$ One of the primes on ~~[illegible]~~ R.H.S should be 3.

Take $p_1 = 3$.

$$\therefore \Rightarrow \; 2(p_2-1)\dots(p_k-1) = p_2 \times p_3 \dots p_k .$$

$\therefore$ one of the primes on R.H.S should be 2.

Take $p_2 = 2$.

$$\Rightarrow \; (p_3-1)(p_4-1)\dots(p_k-1) = p_3 \dots p_k .$$

$(P_3-1)(P_4-1)\cdots(P_k-1) = P_3 \times P_4 \cdots P_K.$

L.H.S $\Rightarrow$ ~~odd~~ even

R.H.S $\Rightarrow$ odd.

$\therefore$ 2 & 3 are the only prime factors in

n, if $\phi(n) = n/3$.

$\therefore$ $n = 2^a 3^b$ where $a \geq 1$ & $b \geq 1$.