I. Find all solutions of the linear congruence $4x \equiv 10 \pmod 6$.

$6 \mid (4x-10) \Rightarrow \exists y \in \mathbb{Z}: \ 6y = 4x - 10$

$4x - 6y = 10$

$(4,6) = 2$; $2 \mid 10$; 2 classes of ~~solutions~~ solutions incongruent mod 6

$6 = 4 \times 1 + \boxed{2}$ $\Rightarrow 2 = 6 - 4 \times 1$

$4 = 2 \times 2 + 0$

$4(-1) - 6(-1) = 2 \mid \cdot 5$

$4(-5) - 6(-5) = 10 \Rightarrow \begin{cases} x_0 = -5 \\ y_0 = -5 \end{cases}$

$\begin{cases} x = -5 + 3k \\ y = -5 + 2k \end{cases}, k \in \mathbb{Z}$

$\Rightarrow x = -5 \equiv 1 \pmod 6$

$x \equiv -5 + 3 = -2 \equiv 4 \pmod 6$

are the two classes of solutions

II. Solve the system of linear congruences $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$

$(2,3) = (2,5) = (3,5) = 1 \Rightarrow$ we may apply the Chinese remainder t

- $M = 2 \times 3 \times 5 = 30$

$M_1 = \frac{30}{2} = 15$

$M_2 = \frac{30}{3} = 10$

$M_3 = \frac{30}{5} = 6$

- $M_1 y_1 \equiv 1 \pmod 2$

$\underbrace{15 y_1}_{y_1} \equiv 1 \pmod 2 \Rightarrow y_1 \equiv 1 \pmod 2$

- $M_2 y_2 \equiv 1 \pmod 3$

$10 y_2 \equiv 1 \pmod 3$

$y_2 \equiv 1 \pmod 3$

- $M_3 y_3 \equiv 1 \pmod 5$

$6 y_3 \equiv 1 \pmod 5$

$y_3 \equiv 1 \pmod 5$

$\Rightarrow x = 1 \times 15 \times 1 + 2 \times 10 \times 1 + 2 \times 6 \times 1 \pmod{30}$

$x \equiv 47 \equiv 17 \pmod{30}$

III. Prove that if $n = q_1 q_2 \cdots q_r$, $r > 2$ where q_i's are distinct primes such that $(q_i - 1) | (n - 1)$ for all i, then n is a Carmichael number.

- Let $b \in \mathbb{Z}^+$, $(b, n) = 1 \Rightarrow (b, q_j) = 1 \quad \forall j$.
- $b^{q_j - 1} \equiv 1 \pmod{q_j} \Rightarrow$
- $(q_j - 1) | (n-1) \Rightarrow \exists t_j \in \mathbb{Z} : (q_j - 1) t_j = n - 1 \Rightarrow$

$$\Rightarrow b^{n-1} = b^{(q_j - 1) t_j} = (\underbrace{b^{q_j - 1}}_{\equiv 1})^{t_j} \equiv 1 \pmod{q_j}$$

- $$\left.\begin{array}{l} b^{n-1} \equiv 1 \pmod{q_1} \\ \vdots \\ b^{n-1} \equiv 1 \pmod{q_r} \\ (q_j, q_i) = 1 \ \forall i \neq j \end{array}\right\} \Rightarrow b^{n-1} \equiv 1 \pmod{\underbrace{q_1 \cdots q_r}_{n}}$$

IV. Show that $1^p + 2^p + 3^p + \cdots (p-1)^p \equiv 0 \pmod{p}$, when p is an odd prime.

p prime
p odd $\Rightarrow p \geq 3$

$$\left.\begin{array}{l} (1,p)=1 \Rightarrow 1^p \equiv 1 \pmod{p} \\ (2,p)=1 \Rightarrow 2^p \equiv 2 \pmod{p} \\ \text{---} \cdot \text{---} \\ (p-1,p)=1 \Rightarrow (p-1)^p \equiv p-1 \pmod{p} \end{array}\right\} \Rightarrow$$

$$\Rightarrow 1^p + 2^p + \dots + (p-1)^p \equiv 1+2+\dots p-1 = \frac{(p-1)p}{2} \pmod{p}$$

But $p \geq 3 \Rightarrow p-1$ even $\Rightarrow p-1 = 2K,\ K \in \mathbb{Z}$
(p odd)

$$\Rightarrow 1^p + \dots + (p-1)^p \equiv Kp \pmod{p} \equiv 0 \pmod{p}$$

V. A. Find the last digit of 7^{5555}

We need $7^{5555} \pmod{10}$

$(7,10)=1 \Rightarrow 7^{\phi(10)} \equiv 1 \pmod{10}$ (Euler) $\Rightarrow 7^4 \equiv 1 \pmod{10}$

$7^{5555} = 7^{4\times 1388+3} = \underbrace{(7^4)}_{\equiv 1}{}^{1388} \cdot 7^3 \equiv 7^3 \pmod{10} =$

$= \underbrace{49}_{\equiv 9} \times 7 \pmod{10} = 9 \times 7 = 63 \equiv 3 \pmod{10}$

B. Show that, if a and b are relatively prime positive integers, then $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$

- $(a,b)=1 \Rightarrow a^{\phi(b)} \equiv 1 \pmod b$ (Euler) $\xrightarrow{+}$

  But $b^{\phi(a)} \equiv 0 \pmod b$

  $\Rightarrow \boxed{a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod b}$

- Similarly, $\left.\begin{array}{l} a^{\phi(b)} \equiv 0 \pmod a \\ b^{\phi(a)} \equiv 1 \pmod a \end{array}\right] \xrightarrow{+}$

  $\Rightarrow \boxed{a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod a}$

- Since $(a,b)=1$, then $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$