Worksheet - 3

(1) $$n \equiv r \pmod{p}$$

$$\Rightarrow \quad n = q(p-1) + r$$

By Fermat's theorem,

$$x^{p-1} \equiv 1 \pmod{p} \text{ if } x \not\equiv 0 \pmod{p}$$

$$\Rightarrow \quad x^n \equiv x^{q(p-1)+r} \equiv 1^q \cdot x^r \equiv x^r \pmod{p}$$

$$\Rightarrow \quad x^n \equiv x^r \pmod{p} \text{ if } x \not\equiv 0 \pmod{p}.$$

If $x \equiv 0 \pmod{p}$, It holds trivially.

(2) $$11 \equiv 3 \pmod{4}$$

$$8 \equiv 4 \equiv 0 \pmod{4}$$

$$5 \equiv 1 \pmod{4}$$

$$\Rightarrow \quad x^{11} + 2x^8 + x^5 + 3x^4 + 4x^3 + 1 \equiv x^3 + 2x^0 + x + 3x^0 + 4x^3 + 1 \pmod{5}$$

$$\equiv 5x^3 + x + 6 \pmod{5}$$

$$\equiv x + 1 \pmod{5}$$

(3) By Binomial Expension-

$$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}$$

We know- $$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$$

$$\Rightarrow \quad p! = k! \cdot (p-k)! \binom{p}{k}$$

$$\Rightarrow \quad p \mid k!\,(p-k)! \binom{p}{k}$$

Since p is a prime, so $p \mid k!$ or $p \mid (p-k)!$ or

$$p \mid \binom{p}{k}$$

Since $1 \le k \le p-1$

So, $\quad k < p$ and $p-k < p$

$\Rightarrow \quad p \nmid k!$ and $p \nmid (p-k)!$

$\Rightarrow \quad p \mid \binom{p}{k} \quad \forall \; 1 \le k \le p-1$

$\Rightarrow \quad \binom{p}{k} \equiv 0 \pmod p \quad \forall \; 1 \le k \le p-1$

Now, we need to find k such that

$$x = b_1 + km_1 \equiv b_2 \pmod{m_2}$$

or $\quad km_1 \equiv b_2 - b_1 \pmod{m_2} \quad$ — (3)

Since $d = \gcd(m_1, m_2)$, so $\exists$ $y, z \in \mathbb{Z}$ such that

$$ym_1 + zm_2 = d$$

or $\quad ym_1 \equiv d \pmod{m_2} \quad$ — (4)

Since $d \mid b_2 - b_1$

$\Rightarrow b_2 - b_1 = dl$, for some $l \in \mathbb{Z}$

multiply the both sides of eq^n (4) by $+l$.

$$+ ym_1 l \equiv + dl \pmod{m_2}$$

$$ym_1 l \equiv b_2 - b_1 \pmod{m_2}$$

So, choose $k = yl$, and then $x = b_1 + ylm_1$ will satisfy the given system.

Let x_1 and x_2 are two solutions of system of equations, then

$x_1 \equiv b_1 \pmod{m_1}$ & $x_2 \equiv b_1 \pmod{m_1}$

$x_1 \equiv b_2 \pmod{m_2}$ $x_2 \equiv b_2 \pmod{m_2}$

$\Rightarrow \quad m_1 \mid (x_1 - x_2)$ & $m_2 \mid (x_1 - x_2)$

$\Rightarrow \quad \operatorname{lcm}(m_1, m_2) \mid (x_1 - x_2)$

$\Rightarrow \quad x_1 \equiv x_2 \mod(\operatorname{lcm}(m_1, m_2))$

$\Rightarrow$ Sol^n of system is unique modulo $\operatorname{lcm}(m_1, m_2)$.

Ques-1:- (i) first we show-

If $(r_i, m) = 1$ then $(m - r_i, m) = 1$

Let if possible- $(m - r_i, m) = d$

$\Rightarrow d \mid m - r_i$ & $d \mid m$

$\Rightarrow d \mid m - (m - r_i)$ & $d \mid m$

$\Rightarrow d \mid r_i$ & $d \mid m$

$\Rightarrow d \mid (r_i, m)$

But $(r_i, m) = 1$.

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$

$\Rightarrow (m - r_i, m) = d = 1$

(ii) To show $\phi(m)$ is even for $n \geq 3$.

Case-1:- n is a power of 2. i.e. $n = 2^k$, $k \geq 2$

$\Rightarrow \phi(n) = 2^k - 2^{k-1} = 2^{k-1}$ -

which is even.

Case-2:- Prime factorization of n doesnot contain a power of 2. ~~Then~~ :

Let $n = p_1^{k_1} \cdots p_r^{k_r}$

$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$

$= p_1^{k_1 - 1} \cdots p_r^{k_r - 1} (p_1 - 1) \cdots (p_r - 1)$

$\Rightarrow \phi(n)$ is even. since $(p_i - 1)$ is even for all i.

Now come to the main problem.

Let $\{r_1, \dots r_{\phi(m)}\}$ be a reduced residue system modulo $m > 2$.

Since $(r_i, m) = 1 \Rightarrow (m - r_i, m) = 1$

So, we can make the pairs of reduced residue system such that

$$
\begin{aligned}
& r_1 + \dots r_{\phi(m)} \\
&= r_1 + \dots + r_{\phi(m)/2} + m - r_1 + \dots + m - r_{\phi(m)/2} \\
&= \frac{\phi(m)}{2} m \equiv 0 \pmod m
\end{aligned}
$$

(Since $\phi(m)$ is even for $m > 2$)