QUADRATIC RESIDUE

NAME:- MANBENDRA SATPATHY
ROLL:- CB.EN.U4CYS21039
BRANCH:- B.Tech CSE (Cybersecurity)

Q.1. $\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv \pm 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \end{cases}$

A- $p \equiv -1 \pmod 8 \Rightarrow p \equiv 7 \pmod 8$
$p \equiv -3 \pmod 8 \Rightarrow p \equiv 5 \pmod 8$

By Gauss's lemma,

$$\left(\frac{-2}{p}\right) = (-1)^n$$

$$S = \left\{ 1.(-2),\ 2.(-2),\ 3.(-2), \ldots \left(\frac{p-1}{2}\right).-2 \right\}$$

$n = \frac{p-1}{2} - (\text{no. of residues which are less than } \frac{p}{2})$

$\hookrightarrow$ total number of elements in set 'S'

$\Rightarrow n = \frac{p-1}{2} - (\text{no. of residues of type } -2k < \frac{p}{2})$ $\nearrow$ an integer

$\Rightarrow n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$ ([ ] $\rightarrow$ stands for greatest integer function)

$$n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$$

$p \equiv \pm 1 \pmod 8$

(i) $p \equiv 1 \pmod 8$

$p = 8k + 1$

$\left[\frac{p}{4}\right] = \left[\frac{8k+1}{4}\right]$

$p \equiv \pm 3 \pmod 8$

(ii) $p \equiv 3 \pmod 8$

$p = 8k + 3$

$\left[\frac{p}{4}\right] = \left[\frac{8k+3}{4}\right] = \left[2k + \frac{3}{4}\right]$

$$\left[\frac{p}{4}\right] = \left[2k + \frac{1}{4}\right]$$

$$\Rightarrow \left[\frac{p}{4}\right] = 2k$$

$$n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$$

$$\Rightarrow n = \frac{8k+1-1}{2} + 2k$$

$$\Rightarrow n = \frac{8k}{2} + 2k$$

$$\Rightarrow n = 4k + 2k$$

$$\Rightarrow n = 6k$$

$$\left(\frac{-2}{p}\right) = (-1)^n = 1$$

(ii) $p \equiv -1 \pmod 8$

$p = 8k+7,\ 8k-1$

$$\left[\frac{p}{4}\right] = \left[\frac{8k+7}{4}\right] = \left[2k + \frac{7}{4}\right]$$

$$\Rightarrow \left[\frac{p}{4}\right] = \left[2k + 1 + \frac{3}{4}\right]$$

$$\Rightarrow \left[\frac{p}{4}\right] = 2k + 1$$

$$n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$$

$$\Rightarrow n = \frac{8k+7-1}{2} + 2k + 1$$

$$\Rightarrow n = 4k + 3 + 2k + 1$$

$$\Rightarrow n = 6k + 4$$

$$\left(\frac{-2}{p}\right) = (-1)^n = 1$$

$$\left[\frac{p}{4}\right] = 2k$$

$$n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$$

$$\Rightarrow n = \frac{8k+3-1}{2} + 2k$$

$$\Rightarrow n = 4k + 1 + 2k$$

$$\Rightarrow n = 6k + 1$$

$$\left(\frac{-2}{p}\right) = (-1)^n = -1$$

(iii) $p \equiv -3 \pmod 8$

$p = 8k-3,\ 8k+5$

$$\left[\frac{p}{4}\right] = \left[\frac{8k+5}{4}\right] = \left[2k + 1 + \frac{1}{4}\right]$$

$$\Rightarrow \left[\frac{p}{4}\right] = 2k + 1$$

$$n = \frac{p-1}{2} + \left[\frac{p}{4}\right]$$

$$\Rightarrow n = \frac{8k+5-1}{2} + 2k + 1$$

$$\Rightarrow n = 4k + 2 + 2k + 1$$

$$\Rightarrow n = 6k + 3$$

$$\left(\frac{-2}{p}\right) = (-1)^n = -1$$

Hence, $\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv \pm 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \end{cases}$ as required.

Q.2: $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

A- We have $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p \equiv 1 \pmod 4$

and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p \equiv -1 \pmod 4$

So if $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = 1$ exactly when $p \equiv 1 \pmod 3$

And if $p \equiv -1 \pmod 4$, then $\left(\frac{3}{p}\right) = 1$ exactly when $p \equiv -1 \pmod 3$

So, $\left(\frac{3}{p}\right) = 1$ when either $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$

that is $p \equiv 1 \pmod{12}$. When $p \equiv -1 \pmod 4$ and $p \equiv -1 \pmod 3$, that is $p \equiv -1 \pmod{12}$.

So, $\left(\frac{3}{p}\right) = 1$ exactly when $p \equiv \pm 1 \pmod{12}$.

On the other hand, $\left(\frac{3}{p}\right)$ is equal to -1 precisely when exactly one of the factors is positive and the other is negative.

If $(-1)^{(p-1)/2} = 1$ and $\left(\frac{p}{3}\right) = -1$, then

$$p \equiv 1 \equiv 5 \pmod 4$$

and

$$p \equiv 2 \equiv 5 \pmod 3.$$

Hence, the Chinese Remainder Theorem yields,

$$p \equiv 5 \pmod{12}.$$

On the other hand, if $(-1)^{(p-1)/2} = -1$ and $\left(\frac{p}{3}\right) = 1$, then

$$p \equiv 3 \equiv -5 \bmod 4$$

and $$p \equiv 1 \equiv -5 \bmod 3$$

Hence, the Chinese Remainder Theorem yields,

$$p \equiv -5 \pmod{12}$$

In summary, $\left(\frac{3}{p}\right) = -1$ precisely when $p \equiv \pm 5 \pmod{12}$

Q.3. $$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

A- As before $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$

Thus if $p \equiv 1 \pmod 4$, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$.

$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity and if

$p \equiv 3 \pmod 4$, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{3}{p}\right) = -1 \cdot \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$

again by quadratic reciprocity as here $p \equiv 3 \pmod 4$ and $3 \equiv 3 \pmod 4$.

Thus in all cases, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

Thus $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$ and as p is prime and $p \neq 3$.

We know $p \equiv 1$ or $5 \pmod 6$, with the congruence class $p \equiv 1 \pmod 6$ covering all primes $\equiv 1 \pmod 3$ and the congruence class $p \equiv 5 \pmod 6$ covering all primes $\equiv 2 \pmod 3$.

Hence $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$ as required.

Q.4. $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$

A- Let 'r' be a primitive root of p.
$r^1, r^2, \ldots\ldots, r^{\phi(p) = p-1}$ are congruent to $1, 2, \ldots, p-1$ in some order; mod p

$i \in \{1, 2, \ldots\ldots, p-1\}$

$r^k \equiv i \pmod p$ where $1 \leq k \leq p-1$

Using $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$$\left(\frac{i}{p}\right) = \left(\frac{r^k}{p}\right) = (r^k)^{\frac{p-1}{2}} = \left(r^{\frac{p-1}{2}}\right)^k \equiv (-1)^k \pmod p$$

r is a primitive root
$r^{p-1} \equiv 1 \pmod p$
$r^{\frac{p-1}{2}} \equiv -1 \pmod p$

$$\left(\frac{i}{p}\right) = \left(\frac{r^k}{p}\right) \equiv (-1)^k \pmod p$$

If k is even, then $\left(\frac{i}{p}\right) = 1$

If k is odd, then $\left(\frac{i}{p}\right) = -1$

$$\therefore \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{r^k}{p}\right) = \sum_{k=1}^{\underbrace{p-1}_{\text{even}}} (-1)^k = 0$$

$\therefore$ Hence, $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$

Q.5. A. $x^2 \equiv 2 \pmod{71}$

A- $2^{\frac{71-1}{2}} \pmod{71}$
$= 2^{70/2} \pmod{71}$
$= 2^{35} \pmod{71}$
$= 1 \pmod{71}$

$\therefore$ The given quadratic congruence does have a solution.

Q.5. B. $x^2 \equiv -2 \pmod{71}$

A- $(-2)^{\frac{71-1}{2}} \pmod{71}$
$= (-2)^{70/2} \pmod{71}$
$= (-2)^{35} \pmod{71}$
$= 70 \pmod{71} = -1 \pmod{71}$

$\therefore$ The given quadratic congruence doesn't have a solution.

Q.5. C. $x^2 \equiv 2 \pmod{73}$

A- $2^{\frac{73-1}{2}} \pmod{73}$
$= 2^{36} \pmod{73}$
$= 1 \pmod{73}$

$\therefore$ The given quadratic congruence does have a solution

Q.5. D. $x^2 \equiv -2 \pmod{73}$

$A = (-2)^{\frac{73-1}{2}} \pmod{73}$

$= (-2)^{36} \pmod{73}$

$= 1 \pmod{73}$

$\therefore$ The given quadratic congruence does have a solution.