NUMBER THEORY AND ALGEBRA
QUADRATIC EQUATION

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

By Gauss Lemma, $\left(\frac{-2}{p}\right) = (-1)^m$
$S = \{1\cdot(-2), 2(-2), 3(-2), \ldots \left(\frac{p-1}{2}\right)\cdot(-2)\}$

$m = \frac{p-1}{2} - $ (No. of residues which are less than $\frac{p}{2}$)
Total number of elements in set 'S'.

$\Rightarrow m = \frac{p-1}{2} - $ (No. of residues of type $-2k < \frac{p}{2}$)
$\Rightarrow m = \frac{p-1}{2} + \left[\frac{p}{4}\right]$

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

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

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

$m = \frac{8k+1-1}{2} + 2k$
$m = 6k$

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

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

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

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

$m = \frac{8k+3-1}{2} + 2k$
$m = 6k+1$

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

$p \equiv -1 \pmod 8$

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

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

$= 2k+1$

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

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

$= 6k+4$

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

$p \equiv -3 \pmod 8$

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

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

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

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

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

$= 6k+3$

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

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

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

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 $p \equiv 1 \pmod 3$

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 $p = -1 \pmod 3$ that is $p \equiv -1 \pmod{12}$

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

On the otherhand, $\left(\frac{3}{p}\right)$ is equal to -1 precisely when exactly 1 of the factors is +ve and other is -ve.

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

$$p \equiv 1 \equiv 5 \pmod 4$$
$$p \equiv 2 \equiv 5 \pmod 3$$

Hence the Chinese Remainder Theorem yields

$p \equiv 5 \pmod{12}$

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

then $\quad p \equiv 3 \equiv -5 \pmod 4$

$\quad\quad p \equiv 1 = -5 \pmod 3$

Hence, the Chinese Remainder Theorem yields

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

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

③ 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

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

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 $\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$ $\quad p \equiv$ prime

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

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

Let x be a primitive root of p

$x, x^2, \ldots, x^{\phi(p) = p-1}$ are $\equiv (1, 2, \ldots, p-1)$ in some order ; mod p

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

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

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

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

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

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

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

$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{x}{p}\right)^k = \sum_{k=1}^{p-1} (-1)^k = 0$

5) A) $2^{41-1/2} \pmod{41}$

$2^{35} \pmod{41}$

$1 \pmod{41}$

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

B) $(-2)^{71-1/2}$ (mod 71)

$(-2)^{35}$ (mod 71)

(-1) (mod 71)

$\therefore$ The congruence doesn't have a solution

c) $2^{73-1/2}$ (mod 73)

2^{36} (mod 73)

1 (mod 73)

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

D) $(-2)^{73-1/2}$ (mod 73)

$(-2)^{36}$ (mod 73)

1 (mod 73)

Have a solution.