QUESTION

(i) Prove that if p is an odd prime, then $\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \text{ or } 3 \text{ mod } 8 \\ -1 & \text{if } p = 5 \text{ or } 7 \text{ mod } 8 \end{cases}$

(ii) Prove that if p is an odd prime> 3, then $\left(\frac{-}{p}\right) = \begin{cases} 1 & \text{if } p = 1 \text{ mod } 6 \\ -1 & \text{if } p = 5 \text{ mod } 6 \end{cases}$

(iii) Describe (in terms of congruence modulo a suitable n) all primes p for which $\left(\frac{3}{p}\right) = 1$.

ANSWER

(i) $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$.

We know $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ mod } 4 \\ -1 & \text{if } p \equiv 3 \text{ mod } 4 \end{cases}$ (th.1.7)

and $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ mod } 8 \\ -1 & \text{if } p \equiv \pm 3 \text{ mod } 8 \end{cases}$ (th.7.3).

Noting that $p \equiv 1$ mod $4 \Leftrightarrow p \equiv 1$ or 5 mod 8, i.e. $p \equiv 1$ or -3 mod 8, and that $p \equiv 3$ mod $4 \Leftrightarrow p \equiv 3$ or 7 mod 8, i.e. $p \equiv 3$ or -1 mod 8, we may put these together to deduce $\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \text{ or } 3 \text{ mod } 8 \\ -1 & \text{if } p \equiv -1 \text{ or } -3 \text{ mod } 8 \\ & \text{(i.e.7 or 5 mod 8)} \end{cases}$

(ii) $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$.

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

Thus if $p \equiv 1$ mod 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 $p \equiv 3$ mod 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 $p \equiv 3$ mod 4 and $3 \equiv 3$ mod 4. Thus in all cases $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

Thus $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ mod } 6 \\ -1 & \text{if } p \equiv 2 \text{ mod } 3 \end{cases}$ and as p is prime, and $p \neq 3$, we know $p \equiv 1$ or 5 mod 6, with the congruence class $p \equiv 1$ mod 6 covering all primes $\equiv 1$ mod 3, and the congruence class $p \equiv 5$ mod 6 covering all primes $\equiv 2$ mod 3.

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

(iii) By quadratic reciprocity, as $3 \equiv 3 \bmod 4$, $\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \bmod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \bmod 4 \end{cases}$

Now $\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 3 \\ -1 & \text{if } p \equiv 2 \bmod 3 \\ 0 & \text{if } p \equiv 3 \end{cases}$

Hence

$\left(\frac{3}{p}\right)$

$= \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \text{ and } p \equiv 1 \bmod 3 \text{ or } p \equiv 3 \bmod 4 \text{ and } p \equiv 2 \bmod 3 \\ -1 & \text{if } p \equiv 1 \bmod 4 \text{ and } p \equiv 2 \bmod 3 \text{ or } p \equiv 3 \bmod 4 \text{ and } p \equiv 1 \bmod 3 \end{cases}$

Now the Chinese Remainder Theorem tells us that the simultaneous congruences $p \equiv a \bmod 4$ and $p \equiv b \bmod 3$ have a unique solution mod 12. Thus expressing the results modulo 12 gives $\left(\frac{3}{p}\right) =$

$\begin{cases} 1 & \text{if } p \equiv 1 \bmod 12 \text{ or } p \equiv 11 \bmod 12 \\ -1 & \text{if } p \equiv 5 \bmod 12 \text{ or } p \equiv 7 \bmod 12 \end{cases}$ or $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$