166

Legendre Symbol: Let p be an odd prime and $\gcd(a, p) = 1$.

The Legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \in QR(p) \\ -1 & \text{if } a \in QNR(p) \end{cases}$$

QR : quadratic residue

QNR : quadratic non residue.

Exc: $p = 13$

$$(1/13) = (3/13) = (4/13) = (9/13)$$
$$= (10/13) = (12/13) = 1$$

$$(2/13) = (5/13) = (6/13) = (7/13) = (8/13)$$
$$= (11/13) = -1$$

167

Theorem: Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties

(a) If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$

(b) $(a^2/p) = 1$

(c) $(a/p) \equiv a^{p-1/2} \pmod{p}$

(d) $(ab/p) = (a/p)(b/p)$

(e) $(1/p) = 1$ and $(-1/p) = (-1)^{\frac{p-1}{2}}$

Proof: (a) If $a \equiv b \pmod{p}$,

then $x^2 \equiv a \pmod{p}$ & $x^2 \equiv b \pmod{p}$

(168)

have same solutions.

$\therefore$ $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$

are both solvable or neither one

has a solution.

$$\Rightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(b) $x^2 \equiv a^2 \pmod{p}$ has solution

$x = a$.

$$\Rightarrow \quad (a^2/p) = 1$$

(c) By Eulerian criterian

$$(a/p) = a^{p-1/2} \pmod{p}$$

(169)

(d) $$(ab/p) \equiv (ab)^{\frac{p-1}{2}}$$

$$\equiv a^{p-1/2} \cdot b^{p-1/2}$$

$$\equiv (a/p)(b/p) \pmod{p}$$

If $(ab/p) \neq (a/p)(b/p)$

$\Rightarrow \quad 1 \equiv -1 \pmod{p}$

$\Rightarrow \quad p \mid 2$, a contradiction as $p > 2$.

$$\Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(e) $\left(\frac{1}{p}\right) = 1$ as $x^2 \equiv 1 \pmod{p}$ has solution $x = 1$.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } -1 \in QR(p) \\ -1 & \text{if } -1 \in QNR(p) \end{cases}$$

170

$$(-1)^{p-1/2} = \begin{cases} 1 & \text{if } -1 \in QR(p) \\ -1 & \text{if } -1 \in QNR(p) \end{cases}$$

$$\Rightarrow \quad (-1/p) = (-1)^{p-1/2}$$

<u>Exc:</u> If p is an odd prime,

then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

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

If $p = 4k+1$ then $\frac{p-1}{2} = 2k$

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

If $p = 4k+3$ then $\frac{p-1}{2} = 2k+1$

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