190

Jacobi symbol (Extension of Legendre symbol)

If p is a positive odd integer with prime factorization

$$p = \prod_{i=1}^{r} p_i^{r_i}$$

Jacobi symbol

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{r_i}, \quad \text{where}$$

$\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \\ -1 & \\ 0 & \text{if } (a,p) > 1 \end{cases}$$

(191)

Theorem: If P and Q are odd positive integers, then

1. $\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) = \left(\frac{mn}{P}\right)$

2. $\left(\frac{n}{P}\right)\left(\frac{n}{Q}\right) = \left(\frac{n}{PQ}\right)$

3. $\left(\frac{m}{P}\right) = \left(\frac{n}{P}\right)$ iff $m \equiv n \pmod{P}$

4. $\left(\frac{a^2 n}{P}\right) = \left(\frac{n}{P}\right)$ whenever $(a, P) = 1$

192

Theorem: If p is an odd positive integer, we have

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

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof: Let $p = p_1 p_2 \cdots p_m = \prod_{i=1}^{m} p_i$ be the prime factorization of p not necessarily distinct.

$$p = \prod_{i=1}^{m} (1 + p_i - 1)$$

$$= 1 + \sum_{i=1}^{m} (p_i - 1) + \sum_{i \neq j} (p_i - 1)(p_j - 1) + \ldots$$

But each $p_i - 1$ is even

$$\therefore \; p \equiv 1 + \sum_{i=1}^{m} (p_i - 1) \pmod 4$$

193

$$\frac{1}{2}(P-1) = \sum_{i=1}^{m} \frac{1}{2}(p_i - 1)$$

$$\therefore \left(\frac{-1}{P}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right)$$

$$= \prod_{i=1}^{n} (-1)^{\frac{p_i-1}{2}}$$

$$= (-1)^{\sum_{i=1}^{m} \frac{1}{2}(p_i-1)}$$

$$= (-1)^{\frac{1}{2}(P-1)}$$

(2.) $$P^2 = \prod_{i=1}^{m} p_i^2$$

$$= \prod_{i=1}^{m} \left(1 + p_i^2 - 1\right)$$

$$= 1 + \sum_{i=1}^{m} (p_i^2 - 1) + \sum_{i \neq j}^{m} (p_i^2 - 1)(p_j^2 - 1) + \cdots$$

194

$$p^2 \equiv 1 + \sum_{i=1}^{m} \left(p_i^2 - 1\right) \pmod{64}$$

$$\left(\text{As} \quad p_i^2 - 1 \equiv 0 \pmod 8 \right)$$

$$\frac{1}{8}\left(p^2-1\right) \equiv \sum_{i=1}^{m} \frac{\left(p_i^2-1\right)}{8} \pmod 8$$

$$\left(\frac{2}{p}\right) = \prod_{i=1}^{m}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{m}(-1)^{\frac{p_i^2-1}{8}}$$

$$= (-1)^{\sum_{i=1}^{m} \frac{p_i^2-1}{8}}$$

$$= (-1)^{\frac{1}{8}\left(p^2-1\right)}$$

195

Reciprocity Law for Jacobi symbols

If P and Q are positive odd integers with $(P, Q) = 1$, then

$$(P|Q)(Q|P) = (-1)^{\frac{(P-1)(Q-1)}{4}}$$

Proof: $P = p_1 p_2 \dots p_m$

$Q = q_1 q_2 \dots q_n$,

p_i and q_j are primes, $i = 1, 2, \dots m$
$j = 1, 2, \dots n$

$$(P|Q)(Q|P) = \prod_{i=1}^{m} \prod_{j=1}^{n} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$$

$$= (-1)^{r}$$

$$r = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{1}{2}(p_i - 1)\frac{1}{2}(q_j - 1)$$

196

$$= \sum_{i=1}^{m} \frac{1}{2}(p_i - 1) \sum_{j=1}^{n} \frac{1}{2}(q_j - 1)$$

$$\sum_{i=1}^{m} \frac{(p_i - 1)}{2} \equiv \frac{1}{2}(P-1) \pmod 2$$

$$\sum_{j=1}^{n} \frac{(q_j - 1)}{2} \equiv \frac{1}{2}(Q-1) \pmod 2$$

$$\therefore \quad r = \frac{P-1}{2} \cdot \frac{Q-1}{2}$$

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

<u>Exc:</u> Determine whether 888 is a quadratic residue or non residue of the prime 1999

$$\left(\frac{888}{1999}\right) = \left(\frac{4}{1999}\right)\left(\frac{2}{1999}\right)\left(\frac{111}{1999}\right)$$

197

$$\left(\frac{4}{1999}\right) = 1$$

$$\left(\frac{2}{1499}\right) = 1 \quad \text{as} \quad 1999 \equiv 7 \pmod 8$$

$$\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right)$$

$$\left(\frac{3}{1999}\right) = \left(\frac{1999}{3}\right)(-1)^{\frac{3-1}{2}\,\frac{1999-1}{2}}$$

$$= \left(\frac{1999}{3}\right)(-1)(-1)$$

$$= \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{37}{1999}\right) = \left(\frac{1999}{37}\right)(-1)^{\frac{37-1}{2}\cdot\frac{1999-1}{2}}$$

$$= \left(\frac{1}{37}\right) \quad (1)(-1) = -1$$

QNR