Math 406 Section 11.3: The Jacobi Symbol

1. **Introduction:** The Jacobi symbol is a generalization of the Legendre symbol for when the denominator is odd but not necessarily prime. It preserves many of the same useful properties and almost the same meaning.

2. **Definition:** Let n be an odd positive integer with prime factorization $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ and let $a \in \mathbb{Z}$ be coprime to n. Define:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} ... \left(\frac{a}{p_k}\right)^{\alpha_n}$$

   Thus the Jacobi symbol is defined in terms of the Legendre symbol.

   Example: We have:

$$\left(\frac{109}{385}\right) = \left(\frac{109}{5}\right)\left(\frac{109}{7}\right)\left(\frac{109}{11}\right) = \left(\frac{4}{5}\right)\left(\frac{4}{7}\right)\left(\frac{10}{11}\right) = (1)(1)\left(\frac{-1}{11}\right) = -1$$

   Where the final equality is by the -1 rule.

3. **Theorem (Properties):** Let n be an odd positive integer and $a, b \in \mathbb{Z}$ be coprime to n. Then we have:

   (a) If $a \equiv b \bmod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

   (b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

   (c) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$

   (d) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1 & \text{if } n \equiv 1, 7 \bmod 8 \\ -1 & \text{if } n \equiv 3, 5 \bmod 8 \end{cases}$

   (e) If m is another odd positive integer coprime to n then

$$\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right) & \text{if } m \equiv 1 \bmod 4 \text{ or } n \equiv 1 \bmod 4 \\ -\left(\frac{n}{m}\right) & \text{if } m \equiv 3 \bmod 4 \text{ and } n \equiv 3 \bmod 4 \end{cases}$$

   Proof: Omitted. These proofs are mostly grunt work based on the definition of the Jacobi symbol. $\mathcal{QED}$

4. **Theorem (Relationship to Quadratic Residues):** Suppose n is a modulus and $\gcd(a, n) = 1$, then:

   (a) If $x^2 \equiv a \bmod n$ has solutions then $\left(\frac{a}{n}\right) = 1$.

   (b) If $\left(\frac{a}{n}\right) = 1$ we cannot conclude that $x^2 \equiv a \bmod m$ has solutions.

   Proof: If $x^2 \equiv a \bmod n$ has solutions then $n \mid (x^2 - a)$ and so for every p in the prime factorization of n we have $p \mid (x^2 - a)$ and so $x^2 \equiv a \bmod p$ which then tells us that $\left(\frac{a}{p}\right) = 1$. It follows that $\left(\frac{a}{n}\right) = 1$ because $\left(\frac{a}{n}\right)$ is simply a product of 1s.

   The reverse cannot be guaranteed, for example $x^2 \equiv 2 \bmod 15$ has no solution (this can be verified by trial and error). However $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{2}{5}\right) = -1$ and so $\left(\frac{2}{15}\right) = (-1)(-1) = 1$. $\mathcal{QED}$

5. **Calculation:** We can then calculate Jacobi symbols essentially like we did Legendre symbols. The biggest thing to watch out for is making sure that we carefully obey the rules at all stages of the calculation.

   Example: Let's calculate $\left(\frac{1009}{2307}\right)$. We have:

$$\begin{aligned}
\left(\frac{1009}{2307}\right) &= \left(\frac{2307}{1009}\right) \text{ LoQR because } 1009 \equiv 1 \bmod 4 \\
&= \left(\frac{289}{1009}\right) \text{ Reducing} \\
&= \left(\frac{1009}{289}\right) \text{ LoQR because } 1009 \equiv 1 \bmod 4 \\
&= \left(\frac{142}{289}\right) \text{ Reducing} \\
&= \left(\frac{2}{289}\right)\left(\frac{71}{289}\right) \text{ Splitting}
\end{aligned}$$

   Now then, $\left(\frac{2}{289}\right) = 1$ by the 2 rule because $289 \equiv 1 \bmod 8$. For the other part we continue:

$$\begin{aligned}
\left(\frac{71}{289}\right) &= \left(\frac{289}{71}\right) \text{ LoQR because } 289 \equiv 1 \bmod 4 \\
&= \left(\frac{5}{71}\right) \text{ Reducing} \\
&= \left(\frac{71}{5}\right) \text{ LoQR because } 5 \equiv 1 \bmod 4 \\
&= \left(\frac{1}{5}\right) \text{ Reducing}
\end{aligned}$$

   Thus $\left(\frac{1009}{2307}\right) = 1$. We cannot conclude if 1009 is a QR or a QNR mod 2307.

Example: Let's calculate $\left(\frac{1999}{2315}\right)$. We have: We have:

$$\begin{aligned}
\left(\frac{1999}{2315}\right) &= -\left(\frac{2315}{1999}\right) \text{ LoQR because } 1999 \equiv 3 \bmod 4 \text{ and } 2315 \equiv 1 \bmod 4 \\
&= -\left(\frac{316}{1999}\right) \text{ Reducing} \\
&= -\left(\frac{2}{1999}\right)^2 \left(\frac{79}{1999}\right) \text{ Splitting} \\
&= -\left(\frac{79}{1999}\right) \\
&= -\left(-\left(\frac{1999}{79}\right)\right) \text{ LoQR because } 1999 \equiv 3 \bmod 4 \text{ and } 79 \equiv 3 \bmod 4 \\
&= \left(\frac{24}{79}\right) \text{ Reducing} \\
&= \left(\frac{2}{79}\right)^3 \left(\frac{3}{79}\right) \text{ Splitting}
\end{aligned}$$

Now then, $\left(\frac{2}{79}\right) = 1$ by the 2 rule because $79 \equiv 7 \bmod 8$. For the other part we continue:

$$\begin{aligned}
\left(\frac{3}{79}\right) &= -\left(\frac{79}{3}\right) \text{ LoQR because } 3 \equiv 3 \bmod 4 \text{ and } 79 \equiv 3 \bmod 4 \\
&= -\left(\frac{1}{3}\right) \text{ Reducing} \\
&= -1
\end{aligned}$$

Thus $\left(\frac{1999}{2315}\right) = -1$. We can conclude that 1999 is a QNR mod 2315.