Math 406 Section 11.2: Quadratic Reciprocity and Calculation Examples

1. **Introduction:** The Law of Quadratic reciprocity establishes that for primes p and q there is a connection between when p is quadratic residue mod q and when q is a quadratic residue mod p.

2. **Theorem (Law of Quadratic Reciprocity):** Suppose p and q are distinct odd primes, then:

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

   Note: In terms of practical computational application this can be better stated as:

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

   Note: Both the numerator and denominator must be prime in order to use this.

   Proof: Omitted due to length. $\mathcal{QED}$

3. **Calculation:** If we combine this along with a few facts from before:

   (a) For simple values we can just trial-and-error.

   (b) If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. This states that we can reduce the numerator mod the denominator. Call this "reducing".

   (c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ Call this "splitting".

   (d) $\left(\frac{a^2}{p}\right) = 1$ Call this the "square rule".

   (e) If p is an odd prime then:

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

   Call this the "-1 rule".

   (f) If p is an odd prime then:

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

   Call this the "2 rule".

We can then go on to calculate a fairly large number of Legendre symbols:

Example: Let's calculate $\left(\frac{48}{29}\right)$:

$\left(\frac{48}{19}\right) = \left(\frac{19}{29}\right)$ by reducing.
$\left(\frac{19}{29}\right) = \left(\frac{29}{19}\right)$ by the LoQR since $29 \equiv 1 \bmod 4$.
$\left(\frac{29}{19}\right) = \left(\frac{10}{19}\right)$ by reducing.
$\left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right)$ by splitting.

We then do these separately. First:

$\left(\frac{2}{19}\right) = -1$ by the 2 rule because $19 \equiv 3 \bmod 8$.

Second:

$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right)$ by the LoQR since $5 \equiv 1 \bmod 4$.
$\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right)$ by reducing.
$\left(\frac{4}{5}\right) = 1$ by the square rule.

Thus $\left(\frac{48}{29}\right) = (-1)(1) = -1$.

Example: Let's calculate $\left(\frac{105}{1009}\right)$. Note that 105 is not prime so we cannot use the LoQR immediately.

$\left(\frac{105}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{7}{1009}\right)$ by splitting.

We then do these separately. First:

$\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right)$ by LoQR since $1009 \equiv 1 \bmod 4$.
$\left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right)$ by reducing.
$\left(\frac{1}{3}\right) = 1$

Second:

$\left(\frac{5}{1009}\right) = \left(\frac{1009}{5}\right)$ by LoQR since $1009 \equiv 1 \bmod 4$.
$\left(\frac{1009}{5}\right) = \left(\frac{4}{5}\right)$ by reducing.
$\left(\frac{4}{5}\right) = 1$ by the square rule.

Third:

$\left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right)$ by LoQR since $1009 \equiv 1 \bmod 4$.
$\left(\frac{1009}{7}\right) = \left(\frac{1}{7}\right)$ by reducing.
$\left(\frac{1}{7}\right) = 1$

Thus $\left(\frac{105}{1009}\right) = (1)(1)(1) = 1$.