Legendre Symbol Computations

The quadratic reciprocity theorem shows how $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are related. The theorem was guessed by Euler and Legendre years before it was first proved by Gauss. It's statement was arrived at by observation.

Theorem : Quadratic Reciprocity Theorem (11.4)

If p and q are odd primes and $p \equiv q \equiv 3 \mod 4$, then

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

If p and q are odd primes and $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

Example

Determine if $x^2 \equiv 85 \mod 97$ has a solution.

From Theorem 11.3 and Theorem 11.4, we have that

$$\begin{aligned}
\left(\frac{85}{97}\right) &= \left(\frac{17 \cdot 5}{97}\right) \\
&= \left(\frac{17}{97}\right) \cdot \left(\frac{5}{97}\right) && \text{by Theorem 11.3 (C)} \\
&= \left(\frac{97}{17}\right) \cdot \left(\frac{97}{5}\right) && \text{by Theorem 11.4} \\
&= \left(\frac{12}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{17}\right) \cdot \left(\frac{3}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (C)} \\
&= \left(\frac{3}{17}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (B)} \\
&= \left(\frac{17}{3}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.4} \\
&= \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) && \text{by Theorem 11.3 (A)} \\
&= (-1) \cdot (-1) && \text{by inspection} \\
&= 1
\end{aligned}$$

Therefore, $x^2 \equiv 85 \mod 97$ does have a solution.

Theorem : (11.5)

If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 4$$

$$\left(\frac{-1}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 4$$

Proof. If $p \equiv 1 \mod 4$, then $\frac{p-1}{2}$ is even, and Euler's Criterion gives that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \equiv 1 \mod p$$

If $p \equiv 3 \mod 4$, then $\frac{p-1}{2}$ is odd, and Euler's Criterion gives that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p \equiv -1 \mod p$$

□

Example

Determine if $x^2 \equiv 85 \mod 97$ has a solution.

From Theorem 11.3, Theorem 11.4, and Theorem 11.5, we have that

$$\begin{aligned}
\left(\frac{85}{97}\right) &= \left(\frac{-12}{97}\right) \\
&= \left(\frac{-1}{97}\right) \cdot \left(\frac{4}{97}\right) \cdot \left(\frac{3}{97}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot 1 \cdot \left(\frac{97}{3}\right) && \text{by Theorems 11.5, 11.3 (B), and 11.4} \\
&= \left(\frac{1}{3}\right) && \text{by Theorem 11.3 (A)} \\
&= 1
\end{aligned}$$

Example

Evaluate $\left(\frac{6}{7}\right)$ and $\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right)$.

From Theorem 11.3 and Theorem 11.5, we have that

$$\begin{aligned}\left(\frac{6}{7}\right) &= \left(\frac{-1}{7}\right) \qquad \text{Theorem 11.3 (A)}\\ &= -1 \qquad \text{by Theorem 11.5}\end{aligned}$$

From Theorem 11.5, we have that

$$\begin{aligned}\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right) &= \left(\frac{22}{23}\right) \qquad \text{by Theorem 11.3 (C)}\\ &= \left(-\frac{1}{23}\right) \qquad \text{by Theorem 11.3 (A)}\\ &= -1 \qquad \text{by Theorem 11.5}\end{aligned}$$

Theorem : (11.6)

If p is an odd prime, then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1 \mod 8 \quad \text{or} \quad p \equiv 7 \mod 8$$

$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3 \mod 8 \quad \text{or} \quad p \equiv 5 \mod 8$$

Example

Evaluate $\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right)$.

From Theorem 11.5, we have that

$$\begin{aligned}\left(\frac{2}{23}\right) \cdot \left(\frac{11}{23}\right) &= -1 \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{23}{11}\right) \qquad \text{by Theorem 11.4}\\ &= -1 \cdot \left(\frac{2}{23}\right) \cdot \left(\frac{1}{11}\right) \qquad \text{by Theorem 11.3 (A)}\\ &= -1 \cdot 1 \cdot 1 \qquad \text{by Theorem 11.6}\\ &= -1\end{aligned}$$

Example

Calculate $\left(\frac{1234}{4567}\right)$.

From Theorem 11.5, we have that

$$\begin{aligned}
\left(\frac{1234}{4567}\right) &= \left(\frac{2}{4567}\right) \cdot \left(\frac{617}{4567}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot \left(\frac{4567}{617}\right) && \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{248}{617}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{617}\right) \cdot \left(\frac{2}{617}\right) \cdot \left(\frac{31}{617}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot 1 \cdot \left(\frac{617}{31}\right) && \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{28}{31}\right) && \text{by Theorem 11.3 (A)} \\
&= \left(\frac{4}{31}\right) \cdot \left(\frac{7}{31}\right) && \text{by Theorem 11.3 (C)} \\
&= 1 \cdot -1 \cdot \left(\frac{31}{7}\right) && \text{by Theorem 11.3 (B) and Theorem 11.4} \\
&= -1 \cdot \left(\frac{3}{7}\right) \\
&= 1 && \text{by Theorem 11.4}
\end{aligned}$$

Example

Does $x^2 \equiv 211 \mod 159$ have a solution?

By the Chinese Remainder Theorem, there is a solution if and only if both of the following quadratic congruences have a solution.

$$x^2 \equiv 52 \mod 3 \equiv 1 \mod 3$$

$$x^2 \equiv 52 \mod 53 \equiv -1 \mod 53$$

By Theorem 11.4 (B), $x^2 \equiv 1 \mod 3$ has a solution. By Theorem 11.5, $x^2 \equiv -1 \mod 53$ has a solution.