The Jacobi Symbol

Carl Gustav Jacobi (1804-1851), a protegé of Gauss’, extended the definition of the Legendre symbol in a very satisfying way:

Let $m$ be any odd integer with prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Define the **Jacobi symbol** via the formula

$$
\left( \frac{a}{m} \right) = \left( \frac{a}{p_1} \right)^{e_1} \left( \frac{a}{p_2} \right)^{e_2} \cdots \left( \frac{a}{p_k} \right)^{e_k}
$$

where the symbols on the right are all Legendre symbols.

Note that when $m$ is prime, this corresponds exactly to the familiar Legendre symbol.

**Proposition** Let $a, b, m, n$ be integers with $m, n > 0$.

1. $a \equiv b \pmod{m} \Rightarrow \left( \frac{a}{m} \right) = \left( \frac{b}{m} \right)$

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

3. $\left( \frac{a}{mn} \right) = \left( \frac{a}{m} \right) \left( \frac{a}{n} \right)$
**Proof** Immediate. //

It is important to note that, unlike with the Legendre symbol, the Jacobi symbol $\left( \frac{a}{m} \right)$ does not directly determine whether $a$ is a quadratic residue mod $m$. For instance, it is easy to see that the only quadratic residues mod 15 that are prime to 15 are 1 and 4, but $\left( \frac{2}{15} \right) = \left( \frac{2}{3} \right) \left( \frac{2}{5} \right) = (-1)(-1) = 1$. However, if $a$ is a quadratic residue modulo each prime factor of $m$, then $\left( \frac{a}{m} \right) = 1$. This proves the

**Theorem** If $m > 0$ is odd, then $\left( \frac{a}{m} \right) = -1$ implies that $a$ is a quadratic nonresidue mod $m$. //

Still, because of its multiplicative properties, the Jacobi symbol is perfectly suited to help in the computation of Legendre symbols. The following analogous results are also useful.
**Theorem** Let $m$ and $n$ be odd, relatively prime integers. Then

(1) \( \left( \frac{-1}{m} \right) = 1 \iff m \equiv 1 \pmod{4} \)

(2) \( \left( \frac{2}{m} \right) = 1 \iff m \equiv \pm 1 \pmod{8} \)

(3) QRL for Jacobi Symbols: \( \left( \frac{m}{n} \right) \left( \frac{n}{m} \right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \).

**Proof** Let \( m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \) and \( n = q_1^{d_1} q_2^{d_2} \cdots q_l^{d_l} \) be the corresponding prime factorizations. Then

(1) \( \left( \frac{-1}{m} \right) = \left( \frac{-1}{p_1} \right)^{e_1} \left( \frac{-1}{p_2} \right)^{e_2} \cdots \left( \frac{-1}{p_k} \right)^{e_k} \), but we know that \( \left( \frac{-1}{p_i} \right) = 1 \iff p_i \equiv 1 \pmod{4} \). So \( \left( \frac{-1}{m} \right) = 1 \iff \) the prime factors that are congruent to $-1 \pmod{4}$ appear with even exponents in the factorization of $m$. Working mod 4, we see that this happens precisely when \( m \equiv 1 \pmod{4} \).

(2) \( \left( \frac{2}{m} \right) = \left( \frac{2}{p_1} \right)^{e_1} \left( \frac{2}{p_2} \right)^{e_2} \cdots \left( \frac{2}{p_k} \right)^{e_k} \), but we know that \( \left( \frac{2}{p_i} \right) = 1 \iff p_i \equiv \pm 1 \pmod{8} \). So \( \left( \frac{2}{m} \right) = 1 \iff \) the prime
factors that are congruent to $\pm 3 \mod 4$ appear with even exponents in the factorization of $m$. Working mod 8, we see that this happens precisely when $m \equiv \pm 1 \mod 8$.

(3) Let $u =$ the number of $p_i \equiv 3 \mod 4$, and let $v =$ the number of $q_j \equiv 3 \mod 4$. Then

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)^{e_i d_j}$$

but $\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right)$ unless $p_i \equiv q_j \equiv 3 \mod 4$, where this is true up to a sign change only, so we can make these substitutions in the product with exactly $uv$ changes of sign:

$$\left(\frac{m}{n}\right) = (-1)^{uv} \prod_{i,j} \left(\frac{q_j}{p_i}\right)^{e_i d_j} = (-1)^{uv} \left(\frac{n}{m}\right).$$

If either $u$ or $v$ is even, then respectively $m$ or $n$ is congruent to 1 mod 4 and $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$. Otherwise, both $u$ and $v$ are odd, both $m$ and $n$ are congruent to 3 mod 4, and $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, proving (3).  //