The Jacobi Symbol

It's a little inconvenient that the Legendre symbol $\left(\frac{a}{p}\right)$ is only defined when the bottom is an odd prime. You can extend the definition to allow an *odd positive number* on the bottom using the Jacobi symbol. Most of the properties of Legendre symbols go through for Jacobi symbols, which makes Jacobi symbols very convenient for computation. We'll see, however, that there is a price to pay for the greater generality: Euler's formula no longer works, and we lose part of the connection between the value of a symbol and the solvability of the corresponding quadratic congruence.

Definition. Let $p, q \in \mathbb{Z}$, where $(p, q) = 1$ and q is a product of odd primes:

$$q = q_1 q_2 \cdots q_n.$$

(The q_i need not be distinct.) The **Jacobi symbol** $\left(\frac{p}{q}\right)$ is defined by

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_n}\right).$$

Note that the Jacobi symbol and the Legendre symbol coincide in the case where q is a single odd prime. That is why the same notation is used for both. It's clear from the definition that $\left(\frac{p}{q}\right) = \pm 1$.

Lemma. If q is a product of odd primes and a is a quadratic residue mod q, then $\left(\frac{a}{q}\right) = 1$.

Proof. Write $q = q_1 q_2 \cdots q_n$, where each q_i is an odd prime. Suppose a is a quadratic residue mod q. Then $(a, q) = 1$ and $x^2 = a \pmod{q}$ has solutions.

Since $q_i \mid q$, it follows that $(a, q_i) = 1$ and $x^2 = a \pmod{q_i}$ for $i = 1, \ldots n$. Hence, $\left(\frac{a}{q_i}\right) = 1$ for $i = 1, \ldots n$. Therefore,

$$\left(\frac{a}{q}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_n}\right) = 1 \cdot 1 \cdots 1 = 1. \quad \square$$

However, the converse is false: If $\left(\frac{p}{q}\right)$ is a Jacobi symbol and $\left(\frac{p}{q}\right) = 1$, it does not follow that p is a quadratic reside mod q.

Example. Show that $\left(\frac{2}{15}\right) = 1$, but 2 is not a quadratic residue mod 15.

Since 2 is not a square mod 3 or mod 5,

$$\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = -1.$$

Therefore,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

However, here is a table of squares mod 15:

x	0	1	2	3	4	5	6	7
$x^2 \pmod{15}$	0	1	4	9	1	10	6	4

x	8	9	10	11	12	13	14
$x^2 \pmod{15}$	4	6	10	1	9	4	1

The table shows that 2 is not a square mod 15. The quadratic residues mod 15 are 1 and 4, as those are the squares that are relatively prime to 15. □

The results that follow amount to saying that the algebraic properties of Legendre symbols hold for Jacobi symbols — and indeed, the proofs of these properties typically use those properties for Legendre symbols.

Theorem. Let q and q' be odd positive numbers, and suppose $(pp', qq') = 1$. Then:

(a) $\left(\frac{p}{q}\right)\left(\frac{p}{q'}\right) = \left(\frac{p}{qq'}\right)$.

(b) $\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right) = \left(\frac{pp'}{q}\right)$.

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

(d) $\left(\frac{p^2p'}{q^2q'}\right) = \left(\frac{p'}{q'}\right)$.

(e) If $p = p' \pmod{q}$, then $\left(\frac{p}{q}\right) = \left(\frac{p'}{q}\right)$.

Proof. (a) Write q and q' as products of odd primes:

$$q = q_1 q_2 \cdots q_m \quad \text{and} \quad q' = q_1' q_2' \cdots q_n'.$$

Then

$$\left(\frac{p}{q}\right)\left(\frac{p}{q'}\right) = \left(\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right)\right)\left(\left(\frac{p}{q_1'}\right)\left(\frac{p}{q_2'}\right)\cdots\left(\frac{p}{q_n'}\right)\right) = \left(\frac{p}{qq'}\right).$$

(b) Write q as a product of odd primes:

$$q = q_1 q_2 \cdots q_m.$$

Then

$$\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right) = \left(\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right)\right)\left(\left(\frac{p'}{q_1}\right)\left(\frac{p'}{q_2}\right)\cdots\left(\frac{p'}{q_m}\right)\right) =$$

$$\left(\left(\frac{p}{q_1}\right)\left(\frac{p'}{q_1}\right)\right)\left(\left(\frac{p}{q_2}\right)\left(\frac{p'}{q_2}\right)\right)\cdots\left(\left(\frac{p}{q_m}\right)\left(\frac{p'}{q_m}\right)\right) = \left(\frac{pp'}{q_1}\right)\left(\frac{pp'}{q_2}\right)\cdots\left(\frac{pp'}{q_m}\right) = \left(\frac{pp'}{q}\right).$$

(c) Write q as a product of odd primes:

$$q = q_1 q_2 \cdots q_m.$$

If q_k is an odd prime, then $\left(\frac{p^2}{q_k}\right) = 1$ (as a Legendre symbol). Hence,

$$\left(\frac{p^2}{q}\right) = \left(\frac{p^2}{q_1}\right)\left(\frac{p^2}{q_2}\right)\cdots\left(\frac{p^2}{q_m}\right) = 1 \cdot 1 \cdots 1 = 1.$$

Next, observe that if q_k is an odd prime, then

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

So

$$\left(\frac{p}{q^2}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right)\left(\frac{p}{q_m}\right) = 1\cdot 1\cdots 1 = 1.$$

(d)

$$\begin{aligned}\left(\frac{p^2p'}{q^2q'}\right) &= \left(\frac{p^2}{q^2q'}\right)\left(\frac{p'}{q^2q'}\right) && \text{(by (b))}\\ &= \left(\frac{p'}{q^2q'}\right) && \text{(by (c))}\\ &= \left(\frac{p'}{q^2}\right)\left(\frac{p'}{q'}\right) && \text{(by (a))}\\ &= \left(\frac{p'}{q'}\right) && \text{(by (c))}\end{aligned}$$

(e) Write q as a product of odd primes:

$$q = q_1q_2\cdots q_m.$$

Since $p = p' \pmod q$, I have $p = p' \pmod{q_k}$ for $k = 1,\ldots m$. Consequently, $\left(\frac{p}{q_k}\right) = \left(\frac{p'}{q_k}\right)$ (as Lengendre symbols). Therefore,

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_m}\right) = \left(\frac{p'}{q_1}\right)\left(\frac{p'}{q_2}\right)\cdots\left(\frac{p'}{q_m}\right) = \left(\frac{p'}{q}\right). \quad \square$$

Example. Show that if $(a,q) = 1$ and q is odd and positive, it does not follow that

$$\left(\frac{a}{q}\right) = a^{(q-1)/2} \pmod q.$$

(Thus, the analog of Euler's lemma does not hold for Jacobi symbols.)

Note that

$$\left(\frac{7}{15}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = (1)(-1) = -1.$$

But

$$7^{(15-1)/2} = 7^7 = 13 \pmod{15}. \quad \square$$

The next lemma will be used in the proofs of the formulas for $\left(\frac{-1}{q}\right)$ and $\left(\frac{2}{q}\right)$, as well as in the proof that Quadratic Reciprocity holds for Jacobi symbols.

Lemma. If m and n are odd, then

$$\frac{m-1}{2} + \frac{n-1}{2} = \frac{mn-1}{2} \pmod 2.$$

Proof. Since m and n are odd, I may write

$$m = 2a+1 \quad \text{and n = 2 b + 1} \quad \text{for} \quad a,b \in \mathbb{Z}.$$

Then

$$\frac{m-1}{2} + \frac{n-1}{2} = \frac{2a+1-1}{2} + \frac{2b+1-1}{2} = a+b.$$

On the other hand,

$$\begin{aligned} mn-1 &= (2a+1)(2b+1)-1 \\ mn-1 &= 4ab+2a+2b+1-1 \\ mn-1 &= 4ab+2a+2b \\ \frac{mn-1}{2} &= 2ab+a+b \\ \frac{mn-1}{2} &= 2ab+\frac{m-1}{2}+\frac{n-1}{2} \\ \frac{mn-1}{2} &= \frac{m-1}{2}+\frac{n-1}{2} \pmod 2 \end{aligned}$$

□

Corollary. If $m_1, m_2, \ldots m_n$ are odd, then

$$\frac{m_1-1}{2}+\frac{m_2-1}{2}+\cdots+\frac{m_n-1}{2} = \frac{m_1 m_2 \cdots m_n - 1}{2} \pmod 2 .$$

Proof. Use the previous lemma and induction. □

The way this corollary will be used in the following proof is the simple observation that if $s = t \pmod 2$, then $(-1)^2 = (-1)^t$.

Theorem. Let q be an odd positive number. Then

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

Proof. Write q as a product of odd primes:

$$q = q_1 q_2 \cdots q_m.$$

Then

$$\left(\frac{-1}{q}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right)\cdots\left(\frac{-1}{q_n}\right).$$

The terms on the right are Legendre symbols, for which I know

$$\left(\frac{-1}{q_k}\right) = (-1)^{(q_k-1)/2} \quad \text{for} \quad k = 1, \ldots n.$$

Thus,

$$\left(\frac{-1}{q}\right) = (-1)^{(q_1-1)/2}(-1)^{(q_2-1)/2}\cdots(-1)^{(q_n-1)/2} = (-1)^S, \quad \text{where} \quad S = \sum_{k=1}^{n}\frac{q_k-1}{2}.$$

Using the preceding corollary,

$$S = \sum_{k=1}^{n}\frac{q_k-1}{2} = \frac{\prod_{k=1}^{n} q_k - 1}{2} = \frac{q-1}{2} \pmod 2 .$$

Therefore,

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}. \quad \square$$

Theorem. (Quadratic Reciprocity) Suppose p and q are odd positive integers and $(p, q) = 1$. Then

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

Proof. I'll prove the equivalent statement

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{[(p-1)/2][(q-1)/2]}.$$

(To get from either this statement to the original one or vice versa, multiply both sides by $\left(\frac{q}{p}\right)$ and note that $\left(\frac{q}{p}\right)^2 = 1$.)

Write p and q as products of odd primes:

$$p = p_1 p_2 \cdot p_m \quad \text{and} \quad q = q_1 q_2 \cdots q_n.$$

Then

$$\left(\frac{p}{q}\right) = \prod_{i=1}^{m} \left(\frac{p_i}{q}\right) = \prod_{i=1}^{m} \prod_{j=1}^{n} \left(\frac{p_i}{q_j}\right).$$

Here's what the last double product looks like, multiplied out:

$$\begin{array}{c} \left(\frac{p_1}{q_1}\right)\ \left(\frac{p_2}{q_1}\right) \cdots \left(\frac{p_m}{q_1}\right) \cdot \\ \left(\frac{p_1}{q_2}\right)\ \left(\frac{p_2}{q_2}\right) \cdots \left(\frac{p_m}{q_2}\right) \cdot \\ \vdots \\ \left(\frac{p_1}{q_n}\right)\ \left(\frac{p_2}{q_n}\right) \cdots \left(\frac{p_m}{q_n}\right) \end{array}$$

By Quadratic Reciprocity for Legendre symbols,

$$\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right) (-1)^{[(p_i-1)/2][(q_j-1)/2]}.$$

Taking the product over i and j on both sides, I get

$$\left(\frac{p}{q}\right) = \prod_{i=1}^{m} \prod_{j=1}^{n} \left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{m} \prod_{j=1}^{n} \left(\frac{q_j}{p_i}\right) (-1)^{[(p_i-1)/2][(q_j-1)/2]} = \left(\frac{q}{p}\right) \cdot \prod_{i=1}^{m} \prod_{j=1}^{n} (-1)^{[(p_i-1)/2][(q_j-1)/2]}.$$

Taking the product of powers of -1 causes the powers to add. So

$$\prod_{j=1}^{n} (-1)^{[(p_i-1)/2][(q_j-1)/2]} = (-1)^S, \quad \text{where} \quad S = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2}.$$

By the preceding corollary,

$$\begin{aligned} \sum_{j=1}^{n} \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2} &= \sum_{i=1}^{m} \frac{p_i - 1}{2} \cdot \sum_{j=1}^{n} \frac{q_j - 1}{2} \\ &= \frac{p_1 p_2 \cdots p_m - 1}{2} \cdot \frac{q_1 q_2 \cdots q_n - 1}{2} \\ &= \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2 \end{aligned}$$

That is,

$$(-1)^S = (-1)^{[(p-1)/2][(q-1)/2]}.$$

Hence,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{[(p-1)/2][(q-1)/2]}. \quad \square$$

Remark. In computational terms, this version of reciprocity is like the one for Legendre symbols. Thus, suppose p and q are odd and relatively prime. If either p or q equals 1 mod 4, then

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

If both p and q equal 3 mod 4, then

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

Next, I'll derive a formula for $\left(\frac{2}{q}\right)$, where q is an odd prime. The proof is similar to the proof of the formula for $\left(\frac{-1}{q}\right)$, except that I have slightly different preliminary lemmas.

Lemma. If m and n are odd, then

$$\frac{m^2-1}{8} + \frac{n^2-1}{8} = \frac{m^2n^2-1}{8} \pmod 2.$$

Proof. Since m and n are odd, I may write

$$m = 2a+1 \quad \text{and n = 2 b + 1} \quad \text{for} \quad a, b \in \mathbb{Z}.$$

Then

$$m^2 = 4a^2+4a+1 \quad \text{and} \quad n^2 = 4b^2+4b+1$$
$$m^2-1 = 4a^2+4a \quad \text{and} \quad n^2-1 = 4b^2+4b$$

So

$$\frac{m^2-1}{8} + \frac{n^2-1}{8} = \frac{4a^2+4a}{8} + \frac{4b^2+4b}{8} = \frac{a^2+a}{2} + \frac{b^2+b}{2}.$$

(Note that a^2+a is even because it's the sum of two odd numbers, so $\frac{a^2+a}{2}$ is an integer. Likewise, $\frac{b^2+b}{2}$ is an integer.)

Now

$$m^2n^2 = (4a^2+4a+1)(4b^2+4b+1)$$
$$m^2n^2 = 16a^2b^2+16a^2b+16ab^2+16ab+4a^2+4b^2+4a+4b+1$$
$$m^2n^2-1 = 16a^2b^2+16a^2b+16ab^2+16ab+4a^2+4b^2+4a+4b$$
$$\frac{m^2n^2-1}{8} = \frac{16a^2b^2+16a^2b+16ab^2+16ab+4a^2+4b^2+4a+4b}{8}$$
$$\frac{m^2n^2-1}{8} = 2a^2b^2+2a^2b+2ab^2+2ab+\frac{a^2+a}{2}+\frac{b^2+b}{2}$$
$$\frac{m^2n^2-1}{8} = \frac{a^2+a}{2}+\frac{b^2+b}{2} \pmod 2$$
$$\frac{m^2n^2-1}{8} = \frac{m^2-1}{8}+\frac{n^2-1}{8} \pmod 2$$

$\square$

Corollary. If $m_1, m_2, \ldots m_n$ are odd, then

$$\frac{m_1^2-1}{8} + \frac{m_2^2-1}{8} + \cdots + \frac{m_n^2-1}{8} = \frac{m_1^2m_2^2\cdots m_n^2-1}{8} \pmod 2.$$

Proof. Use the previous lemma and induction. □

Theorem. Let q be an odd positive number. Then

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

Proof. Write q as a product of odd primes:

$$q = q_1 q_2 \cdots q_m.$$

Then

$$\left(\frac{2}{q}\right) = \left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right)\cdots\left(\frac{2}{q_n}\right).$$

The terms on the right are Legendre symbols, for which I know

$$\left(\frac{2}{q_k}\right) = (-1)^{(q_k^2-1)/8} \quad \text{for} \quad k = 1, \ldots n.$$

Thus,

$$\left(\frac{2}{q}\right) = (-1)^{(q_1^2-1)/8}(-1)^{(q_2^2-1)/8}\cdots(-1)^{(q_n^2-1)/8} = (-1)^S, \quad \text{where} \quad S = \sum_{k=1}^{n}\frac{q_k^2-1}{8}.$$

Using the preceding corollary,

$$S = \sum_{k=1}^{n}\frac{q_k^2-1}{8} = \frac{\prod_{k=1}^{n} q_k^2 - 1}{8} = \frac{q^2-1}{8} \pmod 2.$$

Therefore,

$$\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}. \quad \square$$

Example. Compute the Jacobi symbol $\left(\frac{71}{375}\right)$.

$$\left(\frac{71}{375}\right) = \left(\frac{71}{3\cdot 5^3}\right) = \left(\frac{71}{3\cdot 5}\right) = \left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1)(1) = -1. \quad \square$$

Example. Compute the Legendre symbol $\left(\frac{91}{103}\right)$.

Jacobi symbols can often be used to simplify the computation of Legendre symbols.

$$\left(\frac{91}{103}\right) = -\left(\frac{103}{91}\right) = -\left(\frac{12}{91}\right) = -\left(\frac{4\cdot 3}{91}\right) = -\left(\frac{3}{91}\right) = -\left(\frac{3}{7\cdot 13}\right) =$$

$$-\left(\frac{3}{7}\right)\left(\frac{3}{13}\right) = -(-1)\left(\frac{7}{3}\right)\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{3}\right) = 1\cdot 1 = 1. \quad \square$$
