17. Jacobi Symbol

It is convenient to exend the definition of the Legendre symbol to the case that the term on the bottom is not prime.

Definition 17.1. *Let a and b be two integers where b is odd.*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)\cdots\left(\frac{a}{p_r}\right),$$

where $b = p_1p_2\dots p_r$ is the factorisation of b into primes.

The Jacobi symbol has all of the properties of the Legendre symbol, except one. Even if

$$\left(\frac{a}{b}\right) = 1$$

it is not clear that a is a quadratic residue modulo b.

Example 17.2. *Is 2 a square modulo 15?*

The answer is no. $15 = 3 \cdot 5$ and so if 2 is a square modulo 15 it is a square modulo 3. But 2 is not a square modulo 3. Let's compute the Jacobi symbol:

$$\begin{aligned}\left(\frac{2}{15}\right) &= \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\\ &= (-1)^2\\ &= 1.\end{aligned}$$

Note however if the Jacobi symbol is negative then a is not a quadratic residue modulo b, since there must be one prime factor of b for which the Legendre symbol is -1.

Theorem 17.3. *We have the following relations for the Jacobi symbol, whenever these symbols are defined:*

(1)
$$\left(\frac{a_1a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right).$$

(2)
$$\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

(3) *If* $a_1 \equiv a_2 \mod b$ *then*
$$\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right).$$

(4)
$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}.$$

(5)

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

(6) If $(a, b) = 1$ then

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

Example 17.4. *Is* 1001 *a quadratic residue modulo* 9907*?*

We already answered this type of question using Legendre symbols, let's now use Jacobi symbols.

$$\begin{aligned}
\left(\frac{1001}{9907}\right) &= \left(\frac{9907}{1001}\right) \\
&= \left(\frac{898}{1001}\right) \\
&= \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right) \\
&= \left(\frac{1001}{449}\right) \\
&= \left(\frac{103}{449}\right) \\
&= \left(\frac{449}{103}\right) \\
&= \left(\frac{37}{103}\right) \\
&= \left(\frac{103}{37}\right) \\
&= \left(\frac{29}{37}\right) \\
&= \left(\frac{37}{29}\right) \\
&= \left(\frac{8}{29}\right) \\
&= \left(\frac{2}{29}\right) \\
&= -1.
\end{aligned}$$

Thus 1001 is not a quadratic residue modulo 9907.

Proof of (17.3). We first prove (1). Suppose that $b = p_1 p_2 \dots p_r$ is the prime factorisation of b. We have

$$\begin{aligned}\left(\frac{a_1a_2}{b}\right) &= \left(\frac{a_1a_2}{p_1}\right)\left(\frac{a_1a_2}{p_2}\right)\dots\left(\frac{a_1a_2}{p_r}\right) \\ &= \left(\frac{a_1}{p_1}\right)\left(\frac{a_2}{p_1}\right)\left(\frac{a_1}{p_2}\right)\left(\frac{a_2}{p_2}\right)\dots\left(\frac{a_1}{p_r}\right)\left(\frac{a_2}{p_r}\right) \\ &= \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right).\end{aligned}$$

This is (1).

We now prove (2). Suppose that $b_1 = p_1 p_2 \dots p_r$ and $b_2 = q_1 q_2 \dots q_s$. We have

$$\begin{aligned}\left(\frac{a}{b_1b_2}\right) &= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right)\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\dots\left(\frac{a}{q_s}\right) \\ &= \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).\end{aligned}$$

This is (2).

We now prove (3). Suppose that $b = p_1 p_2 \dots p_r$ is the prime factorisation of b. We have

$$\begin{aligned}\left(\frac{a_1}{b}\right) &= \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_r}\right) \\ &= \left(\frac{a_2}{p_1}\right)\left(\frac{a_2}{p_2}\right)\dots\left(\frac{a_2}{p_r}\right) \\ &= \left(\frac{a_2}{b}\right).\end{aligned}$$

This is (3).

We now prove (4). Suppose that $b = p_1 p_2 \dots p_r$ is the prime factorisation of b. We have

$$\begin{aligned}\left(\frac{-1}{b}\right) &= \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) \\ &= \prod_{i=1}^{r}(-1)^{(p_i-1)/2} \\ &= (-1)^{1/2\sum_{i=1}^{r}(p_i-1)}.\end{aligned}$$

On the other hand, as m and n are odd, we have

$$\begin{aligned}(m-1)(n-1) &\equiv 0 \mod 4\\ mn-1 &\equiv (m-1)+(n-1) \mod 4\\ \frac{mn-1}{2} &\equiv m-12+\frac{n-1}{2} \mod 2.\end{aligned}$$

By induction on r it follows that

$$\begin{aligned}\sum_{i=1}^{r}\frac{p_i-1}{2} &= \frac{\prod_{i=1}^{r}p_i-1}{2} \mod 2\\ \frac{b-1}{2}.\end{aligned}$$

Thus is (4).

We now prove (5). Suppose that $b = p_1p_2\ldots p_r$ is the prime factorisation of b. We have

$$\begin{aligned}\left(\frac{2}{b}\right) &= \prod_{i=1}^{r}\left(\frac{2}{p_i}\right)\\ &= \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8}\\ &= (-1)^{1/8\sum_{i=1}^{r}(p_i^2-1)}.\end{aligned}$$

On the other hand, as m and n are odd, we have $m^2 \equiv 1 \mod 8$ so that

$$\begin{aligned}(m^2-1)(n^2-1) &\equiv 0 \mod 64\\ m^2n^2-1 &\equiv (m^2-1)+(n^2-1) \mod 64\\ \frac{m^2n^2-1}{8} &\equiv \frac{m^2-1}{8}+\frac{n^2-1}{8} \mod 8.\end{aligned}$$

By induction on r it follows that

$$\begin{aligned}\sum_{i=1}^{r}\frac{p_i^2-1}{8} &= \frac{\prod_{i=1}^{r}p_i^2-1}{8} \mod 8\\ &= \frac{b^2-1}{8}.\end{aligned}$$

Thus is (5).

We now prove (6). Suppose that $a = p_1p_2\dots p_r$ and $b = q_1q_2\dots q_s$. As $(a,b) = 1$, $p_i \neq q_j$ for all i and j. We have

$$\begin{aligned}
\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{r}\left(\frac{a}{q_i}\right)\prod_{j=1}^{s}\left(\frac{b}{p_j}\right)\\
&= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)\\
&= \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\\
&= \prod_{j=1}^{s}\prod_{i=1}^{r}(-1)^{\frac{p_j-1}{2}\frac{q_i-1}{2}}\\
&= (-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_j-1}{2}\frac{q_i-1}{2}}\\
&= (-1)^{\sum_{j=1}^{s}\frac{p_j-1}{2}\sum_{i=1}^{r}\frac{q_i-1}{2}}\\
&= (-1)^{\sum_{j=1}^{s}\frac{a-1}{2}\frac{b-1}{2}}. \qquad \square
\end{aligned}$$

We now use Jacobi symbols to give an ideal characterisation of when a number is a square, using only modular arithmetic.

Theorem 17.5. *An integer a is a square if and only if it is a square modulo every prime p.*

Proof. One direction is clear; if $a = b^2$ then $a \equiv b^2 \mod p$.

Now suppose that a is a square modulo every prime p. More precisely the equation

$$x^2 \equiv a \mod p,$$

has a solution for every prime p.

The proof divides into four cases. Consider the prime factorisation of a. The first two cases cover the case when some prime factor has odd exponent and the last two cases deal with the case when a is a square up to sign. More precisely

I The exponent of 2 is odd.
II The exonent of 2 is even but some odd prime factor has odd exponent.
III $-a$ is a square.
IV a is a square.

We show that we cannot be in cases (I), (II) or (III) by exhibiting an integer P with the property that the Jacobi symbol

$$\left(\frac{a}{P}\right) = -1.$$

In this case there must be a prime factor p of P with the propert that the Legendre symbol

$$\left(\frac{a}{p}\right) = -1.$$

Case I: We may write $a = \pm 2^k b$ where b and k are odd. Since b is odd, by the Chinese remainder theorem we may pick P such that

$$P \equiv 5 \mod 8P \qquad\qquad \equiv 1 \mod b.$$

We have

$$\left(\frac{2}{P}\right) = 1,$$

and so

$$\begin{aligned}\left(\frac{-2}{P}\right) &= \left(\frac{-1}{P}\right)\left(\frac{2}{P}\right)\\ &= \left(\frac{2}{P}\right)\\ &= -1.\end{aligned}$$

As k is odd, $k-1$ is even and so

$$\left(\frac{2^{k-1}}{P}\right) = 1.$$

Finally, since $P \equiv 5 \mod 8$ we have $P \equiv 1 \mod 4$ and so

$$\begin{aligned}\left(\frac{b}{P}\right) &= \left(\frac{P}{b}\right)\\ &= \left(\frac{1}{b}\right)\\ &= 1.\end{aligned}$$

It follows that

$$\begin{aligned}\left(\frac{a}{P}\right) &= \left(\frac{\pm 2}{P}\right)\left(\frac{2^{k-1}}{P}\right)\left(\frac{b}{P}\right)\\ &= -1 \cdot 1 \cdot 1\\ &= -1.\end{aligned}$$

Case II: We may write $a = \pm 2^{2h} q^k b$ where b and k are odd, q is an odd prime and $(q, b) = 1$. Pick an integer n which is not a quadratic residue modulo q. Since 4, b and q are pairwise coprime, by the Chinese remainder theorem we may pick P such that

$$\begin{aligned} P &\equiv 1 \mod 4 \\ P &\equiv 1 \mod b \\ P &\equiv n \mod q. \end{aligned}$$

We have

$$\left(\frac{\pm 1}{P}\right) = 1 \qquad \text{and} \qquad \left(\frac{2^{2h}}{P}\right) = 1.$$

Further, since $P \equiv 1 \mod 4$ we have

$$\begin{aligned} \left(\frac{b}{P}\right) &= \left(\frac{P}{b}\right) \\ &= \left(\frac{1}{b}\right) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} \left(\frac{q^k}{P}\right) &= \left(\frac{q}{P}\right) \\ &= \left(\frac{P}{q}\right) \\ &= \left(\frac{n}{q}\right) \\ &= -1. \end{aligned}$$

It follows that

$$\begin{aligned} \left(\frac{a}{P}\right) &= \left(\frac{\pm 1}{P}\right)\left(\frac{2^{2h}}{P}\right)\left(\frac{b}{P}\right)\left(\frac{q^k}{P}\right) \\ &= 1 \cdot 1 \cdot 1 \cdot -1 \\ &= -1. \end{aligned}$$

Case III: We may write $a = -b^2$. Pick $P \equiv 3 \mod 4$ such that P is coprime to b. We have

$$\begin{aligned} \left(\frac{a}{P}\right) &= \left(\frac{-b^2}{P}\right) \\ &= \left(\frac{-1}{P}\right)\left(\frac{b^2}{P}\right) \\ &= -1 \cdot 1 \\ &= -1. \end{aligned}$$

□