Jacobi symbols

Definition. *Let m be an odd positive integer.*

- *If $m = 1$, the Jacobi symbol $\left(\frac{\cdot}{1}\right) : \mathbb{Z} \to \mathbb{C}$ is the constant function* 1.
- *If $m > 1$, it has a decomposition as a product of (not necessarily distinct) primes $m = p_1 \cdots p_r$. The Jacobi symbol $\left(\frac{\cdot}{m}\right) : \mathbb{Z} \to \mathbb{C}$ is given by*

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

Note: The Jacobi symbol does not necessarily distinguish between quadratic residues and nonresidues. That is, we could have $\left(\frac{a}{m}\right) = 1$ just because two of the factors happen to be -1. For instance,

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

but 2 is not a square modulo 15. The following properties of the Jacobi symbol are direct consequences of its definition.

Proposition 1. *Let m, n be positive odd integers and $a, b \in \mathbb{Z}$. Then*

(i) $\left(\frac{1}{m}\right) = 1;$

(ii) $\left(\frac{a}{m}\right) = 0 \iff (a, m) > 1;$

(iii) $a \equiv b \pmod{m} \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right);$

(iv) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right);$

(v) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right);$

(vi) $(a,m)=1 \implies \left(\frac{a^2b}{m}\right) = \left(\frac{b}{m}\right).$

Proof. Exercise. □

Theorem 2. *Let m, n be positive odd integers. Then*

(i) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}};$

(ii) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}};$

(iii) $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right).$

Proof. The first two formulas are trivially true when $m = 1$ and so is the third if $m = 1$ or $n = 1$ or if $(m, n) > 1$. We assume that $m, n > 1$ and $(m, n) = 1$.
Thus $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ for some primes p_i and q_j and $p_i \neq q_j$ for all $1 \leq i \leq r, 1 \leq j \leq s$. Then

$$m = \prod_{i=1}^{r} p_i = \prod_{i=1}^{r} (1 + (p_i - 1)) = 1 + \sum_{i=1}^{r}(p_i - 1) + \sum_{1\leq i_1<i_2\leq r} (p_{i_1} - 1)(p_{i_2} - 1) +$$
$$\ldots \text{ products of } 3, 4 \text{ and so on factors } \ldots$$

Since m is odd, so are the primes p_i. Therefore $p_i - 1 \equiv 0 \pmod 2$ and $(p_{i_1} - 1)(p_{i_2} - 1) \equiv 0 \pmod 4$. Therefore all the terms in the above sum that are implicit are also divisible by 4. Hence

$$m \equiv 1 + \sum_{i=1}^{r}(p_i - 1) \pmod 4,$$

which is to say

$$m - 1 \equiv \sum_{i=1}^{r}(p_i - 1) \pmod 4.$$

Since m and the p_i's are odd, it follows that $m - 1 \equiv 0 \pmod 2$ and $p_1 - 1 \equiv 0 \pmod 2, 1 \leq i \leq r$. Thus we can divide each term above by 2 and still get integers. It follows that

$$\frac{m-1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2} \pmod 2, \tag{1}$$

so

$$(-1)^{\frac{m-1}{2}} = (-1)^{\sum_{i=1}^{r} \frac{p_i-1}{2}} = \prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}} = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \left(\frac{-1}{m}\right).$$

Similarly,

$$m^2 = \prod_{i=1}^{r} p_i^2 = \prod_{i=1}^{r} \bigl(1 + (p_i^2 - 1)\bigr) = 1 + \sum_{i=1}^{r} (p_i^2 - 1) + \sum_{1 \le i_1 < i_2 \le r} (p_{i_1}^2 - 1)(p_{i_2}^2 - 1) + \ldots \text{ products of } 3, 4 \text{ and so on factors } \ldots$$

We use again the fact that both m and the p_i are odd. That means that $m^2 - 1 = (m-1)(m+1)$ is the product of two consecutive even integers, so one of them is divisible by 4. Thus $m^2 - 1 \equiv 0 \pmod 8$ and likewise $p_i^2 - 1 \equiv 0 \pmod 8), 1 \le i \le r$. It follows that the product of two or more factors in the above summation is divisible by 64, hence

$$m^2 - 1 \equiv \sum_{i=1}^{r} (p_i^2 - 1) \pmod{64}.$$

Moreover each term is divisible by 8, so

$$\frac{m^2 - 1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2 - 1}{8} \pmod 8,$$

as integers. It follows that

$$(-1)^{\frac{m^2-1}{8}} = (-1)^{\sum_{i=1}^{r} \frac{p_i^2-1}{8}} = \prod_{i=1}^{r} (-1)^{\frac{p_i^2-1}{8}} = \prod_{i=1}^{r} \left(\frac{2}{p_i}\right) = \left(\frac{2}{m}\right).$$

The last part of the theorem, in the case $m, n > 1$ and $(m, n) = 1$, is equivalent to

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

But

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = (-1)^t$$

where

$$t = \sum_{\substack{1 \le i \le r \\ 1 \le j \le s}} \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2} = \sum_{1 \le i \le r} \frac{p_i - 1}{2} \sum_{1 \le j \le s} \frac{q_j - 1}{2}.$$

By (1), we have $t \equiv \dfrac{m-1}{2} \cdot \dfrac{n-1}{2} \pmod 2$ and the quadratic reciprocity law follows.

□

Jacobi symbols have many applications. The following result is an example of how they can be used in the study of certain Diophantine equations.

Proposition 3. *The Diophantine equation*

$$y^2 = x^3 + k$$

has no solution if $k = (4n-1)^3 - 4m^2$ *and no prime* $p \equiv 3 \pmod 4$ *divides* m.

Proof. We argue by contradiction. Assume that (x, y) is a solution. Since $k \equiv -1 \pmod 4$, it follows that

$$y^2 \equiv x^3 - 1 \pmod 4.$$

But $y^2 \equiv 0, 1 \pmod 4$, so x cannot be even and $x \not\equiv -1 \pmod 4$. Therefore $x \equiv 1 \pmod 4$.

Let $a = 4n - 1$. Then $a \equiv -1 \pmod 4$ and $k = a^3 - 4m^2$. We have

$$y^2 = x^3 + k = x^3 + a^3 - 4m^2,$$

so

$$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2). \tag{2}$$

Given that $x \equiv 1 \pmod 4$ and $a \equiv -1 \pmod 4$, we have that the last factor

$$x^2 - ax + a^2 \equiv 3 \pmod 4.$$

Thus $x^2 - ax + a^2$ is odd and it must have some prime divisor $p \equiv 3 \pmod 4$. But (2) implies that $p \mid y^2 + 4m^2$, i.e. $-4m^2 \equiv y^2 \pmod p$ so

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

On the other hand, since $p \equiv 3 \pmod 4$, we have that $p \nmid m$ and therefore

$$\left(\frac{-4m^2}{p}\right) = \left(\frac{-1}{p}\right) = -1 \text{ (contradiction!)}$$

□

Proposition 4. *If* m, n *are positive odd integers and is an integer with* $D \equiv 0, 1 \pmod 4$ *such that* $m \equiv n \pmod D$, *then*

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

Proof. First we treat the case when $D \equiv 1 \pmod 4$.

If $D > 0$, then

$$\left(\frac{D}{m}\right) = (-1)^{\frac{m-1}{2}\frac{D-1}{2}}\left(\frac{m}{D}\right).$$

But $\frac{D-1}{2}$ is even, hence $\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right)$. The argument holds for any positive odd integer m, and it can therefore be applied just as well to n. The result follows immediately since $m \equiv n \pmod D$.

If $D < 0$, set $d = -D$. Then $d > 0$ and $d \equiv 3 \pmod 4$, so $\frac{d+1}{2}$ is even. We have

$$\left(\frac{D}{m}\right) = \left(\frac{-d}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{m-1}{2}\frac{d-1}{2}}\left(\frac{m}{d}\right) = (-1)^{\frac{m-1}{2}\frac{d+1}{2}}\left(\frac{m}{d}\right) = \left(\frac{m}{d}\right).$$

Since the same holds for n, the result follows from the fact that $m \equiv n \pmod d$.

Now consider the other case, $D \equiv 0 \pmod 4$. It follows that $D = 2^a b$ for some positive odd integer b and $a \geq 2$.

If $D > 0$, then

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

Similarly,

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

The result would follow if we showed that

$$\frac{m^2-1}{8}a \equiv \frac{n^2-1}{8}a \pmod 2 \tag{3}$$

and

$$\frac{m-1}{2}\frac{b-1}{2} \equiv \frac{n-1}{2}\frac{b-1}{2} \pmod 2. \tag{4}$$

We have

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

and this is even since $4 \mid m-n$. Thus (4) is proved. For the other relation, we have

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

Now $2 \mid m+n$ and $2^a \mid m-n$. Thus $m^2-n^2 \equiv 0 \pmod{16}$ when $a \geq 3$ and (3) follows in this case. On the other hand, if $a = 2$, then $\frac{m^2-n^2}{8}a$ is again even and we are done. (We used the fact that $\frac{m^2-n^2}{8} \in \mathbb{Z}$.)

If $D < 0$, set $d = -D$. Then $d > 0$ and $d \equiv 0 \pmod 4$. From above it follows that

$$\left(\frac{d}{m}\right) = \left(\frac{d}{n}\right).$$

We also have

$$\left(\frac{D}{m}\right) = \left(\frac{-d}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{d}{m}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{d}{m}\right)$$

and, similarly,

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{d}{n}\right).$$

The result follows from the fact that

$$\frac{m-1}{2} \equiv \frac{n-1}{2} \pmod 2 \iff 2 \mid \frac{m-n}{2} \iff 4 \mid m-n \Leftarrow \begin{cases} m \equiv n \pmod D \\ D \equiv 0 \pmod 4). \end{cases}$$

□

Theorem 5. *Let $D \equiv 0, 1 \pmod 4$ be a nonzero integer. Then there exists a* unique *group homomorphism $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ such that*

$$\chi_D([p]) = \left(\frac{D}{p}\right) \text{ (the Legendre symbol modulo } p\text{) for all odd primes } p \nmid D.$$

Furthermore,

$$\chi_D([-1]) = \begin{cases} 1 & \text{if } D > 0; \\ -1 & \text{if } D < 0. \end{cases}$$

Proof. First we show existence. Let

$$\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\},\ \chi([a]) = \left(\frac{D}{m}\right) \text{ where } m \equiv a \pmod D \text{ is an odd positive integer.}$$

We need to show that this is a well-defined map, and for that we need to prove the following two facts.

Claim 1 For any $(a, D) = 1$ there exists a positive odd integer $m \equiv a \pmod D$.
Claim 2 If m, n are positive odd integers and $m \equiv n \pmod D$, then

$$\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right).$$

The second claim is an immediate consequence of Proposition 4. The first one, is also easy. There exists some integer k for which $a + kD > 0$. If D is even, then a has to be odd and $a + kD$ is odd and positive. If D is odd, then either $a + kD$ or $a + kD + |D|$ is both odd and positive.
The map χ is clearly a group homomorphism since the Jacobi symbol is completely multiplicative. The condition on primes is just as clear.

Now we have to prove uniqueness. Assume that $f : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ is a group homomorphism with $f([p]) = \left(\frac{D}{p}\right)$ for any odd prime $p \nmid D$. Clearly $f(m) = 1$. Also, for any odd integer $m > 1$, we have $m = p_1 \cdots p_r$ for some odd primes $p_1, \ldots, p_r$. Then

$$f([m]) = f([p_1]) \cdots f([p_r]) = \left(\frac{D}{p_1}\right) \cdots \left(\frac{D}{p_r}\right) = \left(\frac{D}{m}\right) = \chi([m]).$$

Since we have shown that every class $[a] \in (\mathbb{Z}/D\mathbb{Z})^\times$ contains a positive odd integer m, it follows that $f([a]) = \chi([a])$ for all $[a] \in (\mathbb{Z}/D\mathbb{Z})^\times$.
The proof for the expression of $\chi_D([-1])$ is left as an exercise.

$\square$