5.7: Jacobi Symbol

In this section, we define the Jacobi symbol which is a generalization of the Legendre symbol. The Legendre symbol was defined in terms of primes, while Jacobi symbol will be generalized for any odd integers and it will be given in terms of Legendre symbol.

Let $n$ be an odd positive integer with prime factorization

$$n = p_1^{a_1}p_2^{a_2}...p_m^{a_m}$$

and let $a$ be an integer relatively prime to $n$, then

$$\left(\frac{a}{n}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right)^{c_i}.$$  

Notice that from the prime factorization of 45, we get that

$$\left(\frac{2}{55}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{11}\right) = (-1)(-1) = 1$$

We now prove some properties for Jacobi symbol that are similar to the properties of Legendre symbol.

properties for Jacobi symbol

Let $n$ be an odd positive integer and let $(a)$ and $(b)$ be integers such that $(a,n)=1$ and $(b,n)=1$. Then

1. if $n \mid (a-b)$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

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

Proofs
Proof of 1

Note that if \((p)\) is in the prime factorization of \(\left(\frac{n}{\text{prime}}\right)\), then we have that \((p)\mid (a-b)\). Hence by Theorem 70, we get that

\[
\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).
\]

As a result, we have

\[
\left(\frac{a}{n}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i} = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{c_i}
\]

Proof of 2

Note that by Theorem 71, we have \(\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)\) for any prime \((p)\) appearing in the prime factorization of \(\left(\frac{n}{\text{prime}}\right)\). As a result, we have

\[
\begin{aligned}
\left(\frac{ab}{n}\right) &= \prod_{i=1}^{m} \left(\frac{ab}{p_i}\right)^{c_i} \\
&= \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i} \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{c_i} \\
&= \left(\frac{a}{n}\right) \left(\frac{b}{n}\right).
\end{aligned}
\]

In the following theorem, we determine \(\left(\frac{-1}{n}\right)\) and \(\left(\frac{2}{n}\right)\).

Note

Let \((n)\) be an odd positive integer. Then

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

Proofs

Proof of 1

If \((p)\) is in the prime factorization of \(\left(\frac{n}{\text{prime}}\right)\), then by Corollary 3, we see that \(\left(\frac{a}{p}\right) \left(\frac{b}{p}\right)\). Thus

\[
\begin{aligned}
\left(\frac{a}{n}\right) &= \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i} \\
&= (-1)^{\sum_{i=1}^{m} c_i (p_i-1)/2}.
\end{aligned}
\]

Notice that since \((p)\) is even, we have

\[
[p_i^{c_i} = (1+(p_i-1))^{c_i} \equiv 1 + c_i (p_i-1) (mod 4)]
\]

and hence we get

\[
[n=\prod_{i=1}^{m} p_i^{c_i} \equiv 1 + \sum_{i=1}^{m} c_i (p_i-1) (mod 4)]
\]

As a result, we have \(((n-1)/2) \equiv \sum_{i=1}^{m} c_i (p_i-1) / 2 (mod 2)\)
Proof of 2

If \( p \) is a prime, then by Theorem 72 we have
\[
\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.
\]
Hence \[
\left(\frac{2}{n}\right) = (-1)^{\sum_{i=1}^mc_i(p_i^2-1)/8}.
\]
Because \( 8 \mid p_i^2-1 \), we see similarly that
\[
[(1+(p_i^2-1))^{c_i} \equiv 1+c_i(p_i^2-1)(mod \ 64)]
\]
and thus \[
[n^2 \equiv \sum_{i=1}^mc_i(p_i^2-1) (mod \ 64),]
\]
which implies that
\[
[(n^2-1)/8 \equiv \sum_{i=1}^mc_i(p_i^2-1)/8 (mod \ 8).]
\]

We now show that the reciprocity law holds for Jacobi symbol.

Let \((a,b)=1\) be odd positive integers. Then
\[
\left(\frac{b}{a}\right) \left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}.
\]
Notice that since \(a=\prod_{j=1}^mp_j^{c_j}\) and \(b=\prod_{i=1}^nq_i^{d_i}\) we get
\[
\left(\frac{b}{a}\right) \left(\frac{a}{b}\right) = \prod_{i=1}^n\prod_{j=1}^m\left(\frac{p_j}{q_i}\right) \left(\frac{q_i}{p_j}\right)^{c_jd_i}.
\]
By the law of quadratic reciprocity, we get
\[
\left(\frac{b}{a}\right) \left(\frac{a}{b}\right) = (-1)^{\sum_{i=1}^n\sum_{j=1}^mc_j \left(\frac{p_j-1}{2}\right) d_i \left(\frac{q_i-1}{2}\right)}.
\]
As in the proof of part 1 of Theorem 75, we see that
\[
\sum_{j=1}^mc_j \left(\frac{p_j-1}{2}\right) \equiv \frac{a-1}{2} (mod 2).
\]
and
\[
\sum_{i=1}^nd_i \left(\frac{q_i-1}{2}\right) \equiv \frac{b-1}{2} (mod 2).
\]
Thus we conclude that
\[
\sum_{j=1}^mc_j \left(\frac{p_j-1}{2}\right) \sum_{i=1}^nd_i \left(\frac{q_i-1}{2}\right) \equiv \frac{a-1}{2} \cdot \frac{b-1}{2} (mod 2).
\]

Exercises

1. Evaluate \(\left(\frac{258}{4520}\right)\).
2. Evaluate \(\left(\frac{1008}{2307}\right)\).

3. For which positive integers \(n\) that are relatively prime to 15 does the Jacobi symbol \(\left(\frac{15}{n}\right)\) equal 1?

4. Let \(\left(\frac{n}{a}\right)\) be an odd square free positive integer. Show that there is an integer \(a\) such that \(\left(\frac{a}{n}\right) = 1\) and \(\left(\frac{a}{n}\right) = -1\).

---

**Contributors and Attributions**

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.