MEM204-Number Theory

8th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 29/04/2020

University of Crete

The Jacobi Symbol

Definition

Let $n > 1$ be an odd integer and let

$$n = p_1^{n_1} \cdots p_k^{n_k}$$

be its prime factorization. Then, if $a \in \mathbb{Z}$ is such that $(a, n) = 1$, the Jacobi symbol (σύμβολο Jacobi) of a modulo n is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{n_1} \cdots \left(\frac{a}{p_k}\right)^{n_k},$$

where $\left(\frac{a}{p_i}\right)$ stands for the Legendre symbol of a modulo p_i ($i = 1, \ldots, k$).

Some facts

- Clearly, $\left(\frac{a}{n}\right) \in \{\pm 1\}$.
- If n is an odd prime, then the Jacobi symbol $\left(\frac{a}{n}\right)$ coincides with the Legendre symbol $\left(\frac{a}{n}\right)$. This means that the Jacobi symbol generalizes the Legendre symbol.
- As we will see today, the two symbols share even more properties.

Some facts

Remark

Some times in the literature, both the Legendre and the Jacobi symbols are defined without the restriction $(a, n) = 1$. *In this case, by definition,* $\left(\frac{a}{n}\right) = 0$.

Remark

As we will see in more detail in the upcoming exercise set, if $\left(\frac{a}{n}\right) = -1$, *then a is not a quadratic residue modulo n. However, the inverse is not true.*

Basic properties

Proposition

Let $m, n > 1$ be odd numbers and $a, b \in \mathbb{Z}$ be co-prime to both m and n. Then the following hold:

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
3. $a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
4. $\left(\frac{a^2}{n}\right) = 1$.

Proof

Assume that $n = p_1^{n_1} \cdots p_k^{n_k}$ and $m = p_1^{m_1} \cdots p_k^{m_k}$ ($n_i, m_i \geq 0$).

1. $\left(\frac{ab}{n}\right) = \left(\frac{ab}{p_1}\right)^{n_1} \cdots \left(\frac{ab}{p_k}\right)^{n_k} = \left(\frac{a}{p_1}\right)^{n_1} \cdots \left(\frac{a}{p_k}\right)^{n_k} \left(\frac{b}{p_1}\right)^{n_1} \cdots \left(\frac{b}{p_k}\right)^{n_k} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{p_1}\right)^{m_1+n_1} \cdots \left(\frac{a}{p_k}\right)^{m_k+n_k} = \left(\frac{a}{p_1}\right)^{m_1} \cdots \left(\frac{a}{p_k}\right)^{m_k} \left(\frac{a}{p_1}\right)^{n_1} \cdots \left(\frac{a}{p_k}\right)^{n_k} = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
3. Let $a \equiv b \pmod{n}$. Then, clearly, $a \equiv b \pmod{p_i}$ for every i. Hence $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{n_1} \cdots \left(\frac{a}{p_k}\right)^{n_k} = \left(\frac{b}{p_1}\right)^{n_1} \cdots \left(\frac{b}{p_k}\right)^{n_k} = \left(\frac{b}{n}\right)$.
4. $\left(\frac{a^2}{n}\right) = \left(\frac{a^2}{p_1}\right)^{n_1} \cdots \left(\frac{a^2}{p_k}\right)^{n_k} = 1$.

The Jacobi symbol of -1 and 2

Proposition

Let n be an odd number. Then

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

and

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

Proof

Assume that $n = p_1 \cdots p_k$, where the numbers $p_1, \ldots, p_k$ are (not necessarily distinct) odd primes. Then

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_k}\right) = (-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_k-1}{2}} = (-1)^P,$$

where $P = \sum_{i=1}^k \frac{p_i-1}{2}$. Thus it suffices to show that

$$P \equiv (n-1)/2 \pmod 2.$$

The above follows from the fact that, if p, q are odd primes,

$$(p-1)(q-1) \equiv 0 \pmod 4 \Rightarrow pq - 1 \equiv p + q - 2 \pmod 4,$$

that is,

$$\frac{pq-1}{2} \equiv \frac{p-1}{2} + \frac{q-1}{2} \pmod 2.$$

Proof (cont.)

Similarly,

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_k}\right) = (-1)^{\frac{p_1^2-1}{8}} \cdots (-1)^{\frac{p_k^2-1}{8}} = (-1)^Q,$$

where $Q = \sum_{i=1}^{k} \frac{p_i^2-1}{8}$. Thus it suffices to show that

$$Q \equiv (n^2-1)/8 \pmod 2.$$

The above follows from the fact that, if p, q are odd primes, then $p^2 \equiv q^2 \equiv 1 \pmod 8$, hence

$$(p^2-1)(q^2-1) \equiv 0 \pmod{64} \Rightarrow (pq)^2-1 \equiv p^2+q^2-2 \pmod{64},$$

that is,

$$\frac{(pq)^2-1}{8} \equiv \frac{p^2-1}{8} + \frac{q^2-1}{8} \pmod 8.$$

Theorem (The quadratic reciprocity law for the Jacobi symbol)

Let $m, n > 1$ be odd, co-prime numbers. Then

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

Proof.

Omitted. □

A few examples and applications

An interesting application

Theorem

Let $a \in \mathbb{Z}$. Then

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

for all odd primes p, if and only if $a = b^2$, for some $b \in \mathbb{Z}$.

Proof. If $a = b^2$, for some b, then clearly for every odd prime p, $\left(\frac{a}{p}\right) = \left(\frac{b^2}{p}\right) = 1$. Now assume that $a \neq b^2$, for all $b \in \mathbb{Z}$. It suffices to show that there exists some positive odd number P, such that $\left(\frac{a}{P}\right) = -1$, since, in this case, there exists a prime factor p of P, with $\left(\frac{a}{p}\right) = -1$. We distinguich three cases:

Proof (cont.)

If $a = \pm 2^k b$, where k, b are odd positive numbers. The Chinese Remainder Theorem implies that there exists some P, with

$$P \equiv 5 \pmod 8 \text{ and } P \equiv 1 \pmod b.$$

It follows that $4 \mid P - 1$, which combined with the fact that $b - 1$ is even, yields that $\frac{(P-1)(b-1)}{4}$ is even. Now the quadratic reciprocity law yields

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

Moreover, $P \equiv 5 \pmod 8$, implies $\left(\frac{-1}{P}\right) = 1$ and $\left(\frac{2}{P}\right) = -1$. Hence,

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

Proof (cont.)

If $a = \pm 2^{2h} q^k b$, where q is an odd prime and k, b are odd numbers and $q \nmid b$. The Chinese Remainder Theorem implies that there exists some P, with

$$P \equiv 1 \pmod 4, P \equiv 1 \pmod b \quad \text{and} \quad P \equiv c \pmod q,$$

where c is a non-quadratic residue modulo q. It follows that $4 \mid P - 1$, which combined with the fact that $b - 1$ is even, yields that $\frac{(P-1)(b-1)}{4}$ is even. Now the quadratic reciprocity law yields

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

Similarly, $\left(\frac{q^k}{P}\right) = \left(\frac{q}{P}\right) = \left(\frac{P}{q}\right) = \left(\frac{c}{q}\right) = -1$. Finally, we get that

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

Proof (cont.)

If $a = -b^2$, where $b \in \mathbb{Z}$. As before, let P be such that

$$P \equiv 3 \pmod 4 \text{ and } (P, b) = 1,$$

then

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

This concludes the proof.

An example

We will show that, if n is a positive odd number,

$$\left(\frac{6}{n}\right) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \text{ or } \pm 5 \pmod{24}, \\ -1, & \text{if } n \equiv \pm 7 \text{ or } \pm 11 \pmod{24}. \end{cases}$$

We have that

$$\left(\frac{6}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{3}{n}\right) = (-1)^{(n^2-1)/8}\left(\frac{3}{n}\right) = (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}\left(\frac{n}{3}\right).$$

The result follows from the facts

$$(-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}} = \begin{cases} 1, & \text{if } n \equiv 1 \text{ or } 3 \pmod{8}, \\ -1, & \text{if } n \equiv -1 \text{ or } -3 \pmod{8}, \end{cases}$$

$$\left(\frac{n}{3}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod{3}, \\ -1, & \text{if } n \equiv -1 \pmod{3}, \end{cases}$$

and the Chinese Remainder Theorem.

Stay home, stay safe!