

The Legendre symbol

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined whenever a is an integer and p is an **odd** prime number.

$$\left(\frac{a}{p}\right) = 0 \text{ if } p \mid a \text{ and } \left(\frac{a}{p}\right) = \pm 1 \text{ if } p \nmid a.$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ whenever } a \equiv b \pmod{p}.$$

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

$$\left(\frac{-1}{p}\right) = 1 \text{ if } p \equiv 1 \pmod{4} \text{ and } \left(\frac{-1}{p}\right) = -1 \text{ if } p \equiv 3 \pmod{4}.$$

$$\left(\frac{2}{p}\right) = 1 \text{ if } p \equiv \pm 1 \pmod{8} \text{ and } \left(\frac{2}{p}\right) = -1 \text{ if } p \equiv \pm 3 \pmod{8}.$$

If p and q are odd primes then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod{4}$ when $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

The Jacobi symbol

The Jacobi symbol $\left(\frac{a}{m}\right)$ is defined whenever a is an integer and m is a **positive odd** integer.

$\left(\frac{a}{m}\right) = 0$ if $\gcd(a, m) > 1$ and $\left(\frac{a}{m}\right) = \pm 1$ if $\gcd(a, m) = 1$.

$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ whenever $a \equiv b \pmod{m}$.

$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ and $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.

$\left(\frac{-1}{m}\right) = 1$ if $m \equiv 1 \pmod{4}$ and $\left(\frac{-1}{m}\right) = -1$ if $m \equiv 3 \pmod{4}$.

$\left(\frac{2}{m}\right) = 1$ if $m \equiv \pm 1 \pmod{8}$ and $\left(\frac{2}{m}\right) = -1$ if $m \equiv \pm 3 \pmod{8}$.

If m and n are odd positive integers then

$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless $m \equiv n \equiv 3 \pmod{4}$ when $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.