JacobiSymbol

Notations

Traditional name

Jacobi symbol

Traditional notation

$$\left(\frac{n}{m}\right)$$

Mathematica StandardForm notation

`JacobiSymbol[n, m]`

Primary definition

13.08.02.0001.01

$$\left(\frac{n}{m}\right) = \prod_{k=1}^{j} \left(\frac{n}{p_k}\right) /;$$

$$\frac{m-1}{2} \in \mathbb{N} \bigwedge \text{factors}(m) = \{\{p_1, 1\}, \{p_2, 1\}, \ldots, \{p_j, 1\}\} \bigwedge \left(\left(\frac{n}{p}\right) = \left(1 - \delta_{\frac{n}{p} - \left\lfloor \frac{n}{p} \right\rfloor, 0}\right) \left(2 \operatorname{sgn}\left(\sum_{j=1}^{p} \delta_{j^2 \bmod p, n \bmod p}\right) - 1\right) /; p \in \mathbb{P}\right)$$

For positive integer n and nonnegative odd m the Jacobi symbol $\left(\frac{n}{m}\right)$ can be defined by above formula and can get only three values: -1, 0 or 1.

Examples: $\left(\frac{0}{m}\right) = 0 /; \frac{m-3}{2} \in \mathbb{N}$, $\left(\frac{-1}{m}\right) = -1 /; \frac{m-3}{4} \in \mathbb{N}$, $\left(\frac{-1}{m}\right) = 1 /; \frac{m-1}{4} \in \mathbb{N}$.

Specific values

Specialized values

For fixed *n*

13.08.03.0001.01

$$\left(\frac{n}{1}\right) = 1$$

13.08.03.0002.01

$$\left(\frac{n}{p}\right) = 0 /; \frac{n}{p} \in \mathbb{Z} \bigwedge p \in \mathbb{P} \bigwedge p > 2$$

13.08.03.0003.01

$$\left(\frac{n}{p}\right) = 1 /; \exists_{k \in \mathbb{Z} \land k > 0} k^2 \bmod p = n \bigwedge p \in \mathbb{P} \bigwedge p > 2$$

13.08.03.0004.01

$$\left(\frac{n}{p}\right) = -1 /; \neg \left(\exists_{k \in \mathbb{Z} \land k > 0} k^2 \bmod p = n \bigwedge p \in \mathbb{P} \bigwedge p > 2\right)$$

13.08.03.0005.01

$$\left(\frac{n}{p}\right) = (-1)^{\sum_{j=1}^{\left\lfloor \frac{p}{2} \right\rfloor} (2 n j) \bmod p} /; p \in \mathbb{P} \land p > 2$$

For fixed *m*

13.08.03.0006.01

$$\left(\frac{0}{m}\right) = 0 /; \frac{m-3}{2} \in \mathbb{N}$$

13.08.03.0007.01

$$\left(\frac{1}{m}\right) = 1 /; \frac{m-1}{2} \in \mathbb{N}$$

13.08.03.0008.01

$$\left(\frac{-1}{m}\right) = 1 /; \frac{m-1}{4} \in \mathbb{N}$$

13.08.03.0009.01

$$\left(\frac{-1}{m}\right) = -1 /; \frac{m-3}{4} \in \mathbb{N}$$

Values at fixed points

13.08.03.0010.01

$$\left(\frac{0}{1}\right) = 1$$

13.08.03.0011.01

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

13.08.03.0012.01

$$\left(\frac{-4}{3}\right) = -1$$

13.08.03.0013.01

$$\left(\frac{-3}{3}\right) = 0$$

13.08.03.0014.01

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

13.08.03.0015.01

$$\left(\frac{-1}{3}\right) = -1$$

13.08.03.0016.01

$$\left(\frac{0}{3}\right) == 0$$

13.08.03.0017.01

$$\left(\frac{1}{3}\right) == 1$$

13.08.03.0018.01

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

13.08.03.0019.01

$$\left(\frac{3}{3}\right) == 0$$

13.08.03.0020.01

$$\left(\frac{4}{3}\right) == 1$$

13.08.03.0021.01

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

13.08.03.0022.01

$$\left(\frac{6}{3}\right) == 0$$

13.08.03.0023.01

$$\left(\frac{7}{3}\right) == 1$$

13.08.03.0024.01

$$\left(\frac{8}{3}\right) == -1$$

13.08.03.0025.01

$$\left(\frac{9}{3}\right) == 0$$

13.08.03.0026.01

$$\left(\frac{10}{3}\right) == 1$$

13.08.03.0027.01

$$\left(\frac{-5}{5}\right) == 0$$

13.08.03.0028.01

$$\left(\frac{-4}{5}\right) == 1$$

13.08.03.0029.01

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

13.08.03.0030.01

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

13.08.03.0031.01

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

13.08.03.0032.01

$$\left(\frac{0}{5}\right) = 0$$

13.08.03.0033.01

$$\left(\frac{1}{5}\right) = 1$$

13.08.03.0034.01

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

13.08.03.0035.01

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

13.08.03.0036.01

$$\left(\frac{4}{5}\right) = 1$$

13.08.03.0037.01

$$\left(\frac{5}{5}\right) = 0$$

13.08.03.0038.01

$$\left(\frac{6}{5}\right) = 1$$

13.08.03.0039.01

$$\left(\frac{7}{5}\right) = -1$$

13.08.03.0040.01

$$\left(\frac{8}{5}\right) = -1$$

13.08.03.0041.01

$$\left(\frac{9}{5}\right) = 1$$

13.08.03.0042.01

$$\left(\frac{10}{5}\right) = 0$$

13.08.03.0043.01

$$\left(\frac{-5}{7}\right) = 1$$

13.08.03.0044.01

$$\left(\frac{-4}{7}\right) == -1$$

13.08.03.0045.01

$$\left(\frac{-3}{7}\right) == 1$$

13.08.03.0046.01

$$\left(\frac{-2}{7}\right) == -1$$

13.08.03.0047.01

$$\left(\frac{-1}{7}\right) == -1$$

13.08.03.0048.01

$$\left(\frac{0}{7}\right) == 0$$

13.08.03.0049.01

$$\left(\frac{1}{7}\right) == 1$$

13.08.03.0050.01

$$\left(\frac{2}{7}\right) == 1$$

13.08.03.0051.01

$$\left(\frac{3}{7}\right) == -1$$

13.08.03.0052.01

$$\left(\frac{4}{7}\right) == 1$$

13.08.03.0053.01

$$\left(\frac{5}{7}\right) == -1$$

13.08.03.0054.01

$$\left(\frac{6}{7}\right) == -1$$

13.08.03.0055.01

$$\left(\frac{7}{7}\right) == 0$$

13.08.03.0056.01

$$\left(\frac{8}{7}\right) == 1$$

13.08.03.0057.01

$$\left(\frac{9}{7}\right) == 1$$

13.08.03.0058.01

$$\left(\frac{10}{7}\right) == -1$$

13.08.03.0059.01

$$\left(\frac{10}{7}\right) == -1$$

13.08.03.0060.01

$$\left(\frac{-4}{9}\right) == 1$$

13.08.03.0061.01

$$\left(\frac{-3}{9}\right) == 0$$

13.08.03.0062.01

$$\left(\frac{-2}{9}\right) == 1$$

13.08.03.0063.01

$$\left(\frac{-1}{9}\right) == 1$$

13.08.03.0064.01

$$\left(\frac{0}{9}\right) == 0$$

13.08.03.0065.01

$$\left(\frac{1}{9}\right) == 1$$

13.08.03.0066.01

$$\left(\frac{2}{9}\right) == 1$$

13.08.03.0067.01

$$\left(\frac{3}{9}\right) == 0$$

13.08.03.0068.01

$$\left(\frac{4}{9}\right) == 1$$

13.08.03.0069.01

$$\left(\frac{5}{9}\right) == 1$$

13.08.03.0070.01

$$\left(\frac{6}{9}\right) == 0$$

13.08.03.0071.01

$$\left(\frac{7}{9}\right) == 1$$

13.08.03.0072.01

$$\left(\frac{8}{9}\right) == 1$$

13.08.03.0073.01

$$\left(\frac{9}{9}\right) == 0$$

13.08.03.0074.01

$$\left(\frac{10}{9}\right) == 1$$

General characteristics

Domain and analyticity

$\left(\frac{n}{m}\right)$ is a nonanalytical function of n and m which is defined for $n \in \mathbb{Z}$ and nonnegative odd m.

13.08.04.0001.01

$$(n * m) \longrightarrow \left(\frac{n}{m}\right) :: (\mathbb{Z} \otimes \mathbb{Z}) \longrightarrow \{-1, 0, 1\}$$

Symmetries and periodicities

Quasi-permutation symmetry

13.08.04.0002.01

$$\left(\frac{n}{m}\right) == -\left(\frac{m}{n}\right) /; \frac{m-3}{4} \in \mathbb{N} \bigwedge \frac{n-3}{4} \in \mathbb{N}$$

13.08.04.0003.01

$$\left(\frac{n}{m}\right) == \left(\frac{m}{n}\right) /; \neg\left(\frac{m-3}{4} \in \mathbb{N} \bigwedge \frac{n-3}{4} \in \mathbb{N}\right)$$

Periodicity

No periodicity

Series representations

Other series representations

13.08.06.0001.01

$$\left(\frac{n}{p}\right) == \frac{1}{i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}} \left(\sum_{k=0}^{p} \delta_{\gcd(k,p)-1} \exp\left(\frac{2 n \pi i k^2}{p}\right) + 1\right) /; \gcd(n, p) == 1 \land p \in \mathbb{P} \land p > 3 \land n-3 \in \mathbb{N}^+$$

Transformations

Multiple arguments

13.08.16.0001.01

$$\left(\frac{n}{k\,m}\right) == \left(\frac{n}{k}\right)\left(\frac{n}{m}\right) /; \gcd(n, m) == 1 \bigwedge \gcd(n, k) == 1 \bigwedge \frac{m-3}{2} \in \mathbb{N} \bigwedge \frac{k-3}{2} \in \mathbb{N}$$

13.08.16.0002.01

$$\left(\frac{k\,n}{m}\right) == \left(\frac{k}{m}\right)\left(\frac{n}{m}\right) /; \gcd(n, m) == 1 \bigwedge \gcd(n, k) == 1 \bigwedge \frac{m-3}{2} \in \mathbb{N}$$

Products, sums, and powers of the direct function

Products of the direct function

13.08.16.0003.01

$$\prod_{k=1}^{r}\left(\frac{p_k}{m}\right) == \left(\frac{n}{m}\right) /; n == \prod_{k=1}^{r} p_k^{n_k} \bigwedge p_k \in \mathbb{P} \bigwedge \gcd(n, m) == 1 \bigwedge \frac{n-3}{2} \in \mathbb{N}$$

13.08.16.0004.01

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) == (-1)^{\frac{1}{4}(m-1)(n-1)} /; \gcd(m, n) == 1 \bigwedge \frac{n-1}{2} \in \mathbb{N} \bigwedge \frac{m-1}{2} \in \mathbb{N}$$

13.08.16.0005.01

$$\left(\frac{n}{m}\right)\left(\frac{n}{k}\right) == \left(\frac{n}{k\,m}\right) /; \gcd(n, m) == 1 \bigwedge \gcd(n, k) == 1 \bigwedge \frac{m-3}{2} \in \mathbb{N} \bigwedge \frac{k-3}{2} \in \mathbb{N}$$

13.08.16.0006.01

$$\left(\frac{n}{m}\right)\left(\frac{k}{m}\right) == \left(\frac{n\,k}{m}\right) /; \gcd(n, m) == 1 \bigwedge \gcd(n, k) == 1 \bigwedge \frac{m-3}{2} \in \mathbb{N}$$

Identities

Functional identities

13.08.17.0001.01

$$\left(\frac{n}{m}\right) == -\left(\frac{m}{n}\right) /; \frac{m-3}{4} \in \mathbb{N} \bigwedge \frac{n-3}{4} \in \mathbb{N}$$

13.08.17.0002.01

$$\left(\frac{n}{m}\right) == \left(\frac{m}{n}\right) /; \neg\left(\frac{m-3}{4} \in \mathbb{N} \bigwedge \frac{n-3}{4} \in \mathbb{N}\right)$$

13.08.17.0003.01

$$\left(\frac{n}{m}\right) == \left(\frac{k}{m}\right) /; \gcd(n, m) == 1 \bigwedge \gcd(k, m) == 1 \bigwedge n \bmod m == k \bigwedge \frac{m-3}{2} \in \mathbb{N}$$

13.08.17.0004.01

$$\left(\frac{n}{m}\right) == \left(\frac{\frac{n}{4}}{m}\right) /; \frac{n}{4} \in \mathbb{N} \bigwedge \frac{m-1}{2} \in \mathbb{N}$$

13.08.17.0005.01

$$\left(\frac{n}{m}\right) == \prod_{k=1}^{r}\left(\frac{p_k}{m}\right) /; n == \prod_{k=1}^{r} p_k^{n_k} \bigwedge p_k \in \mathbb{P} \bigwedge \gcd(n, m) == 1 \bigwedge \frac{n-3}{2} \in \mathbb{N}$$

13.08.17.0006.01

$$\left(\frac{n}{m}\right) = \left(\frac{n \bmod m}{m}\right) /; \frac{m-1}{2} \in \mathbb{N} \bigwedge n \in \mathbb{Z} \bigwedge n \geq m$$

13.08.17.0007.01

$$\left(\frac{\frac{n}{4}}{m}\right) = \left(\frac{n}{m}\right) /; \frac{n}{4} \in \mathbb{N} \bigwedge \frac{m-1}{2} \in \mathbb{N}$$

13.08.17.0008.01

$$\left(\frac{a_1}{c_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{a_3}{c_3}\right) = (-1)^{((c_1-1)(c_2-1)+(c_3-1)(c_2-1)+(c_1-1)(c_3-1))/4} /;$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -1 & 0 \end{pmatrix} \bigwedge a_1 d_1 - b_1 c_1 = 1 \bigwedge a_2 d_2 - b_2 c_2 = 1 \bigwedge$$

$$a_3 d_3 - b_3 c_3 = 1 \bigwedge \{a_1, b_1, d_1, a_2, b_2, d_2, a_3, b_3, d_3\} \in \mathbb{Z} \bigwedge \left\{\frac{c_1+1}{2}, \frac{c_2+1}{2}, \frac{c_3+1}{2}\right\} \in \mathbb{N}$$

13.08.17.0009.01

$$\left(\frac{a_1}{c_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{a_3}{c_3}\right) = (-1)^{(c_1 c_2+c_1 c_3+c_2 c_3)/4} /; \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -1 & 0 \end{pmatrix} \bigwedge a_1 d_1 - b_1 c_1 = 1 \bigwedge$$

$$a_2 d_2 - b_2 c_2 = 1 \bigwedge a_3 d_3 - b_3 c_3 = 1 \bigwedge \{a_1, b_1, d_1, a_2, b_2, d_2, a_3, b_3, d_3\} \in \mathbb{Z} \bigwedge \left\{\frac{c_1+1}{2}, \frac{c_2+1}{2}, \frac{c_3+1}{2}\right\} \in \mathbb{N}$$

Representations through equivalent functions

With related functions

13.08.27.0001.01

$$\left(\frac{n}{p}\right) = \operatorname{sgn}\left(\frac{p}{2} - n^{\frac{p-1}{2}} \bmod p\right) /; p \in \mathbb{P} \bigwedge \frac{n-1}{2} \in \mathbb{N} \bigwedge \gcd(n, p) = 1$$

Inequalities

13.08.29.0001.01

$$-1 \leq \left(\frac{n}{m}\right) \leq 1$$

Zeros

13.08.30.0001.01

$$\left(\frac{n}{p}\right) = 0 /; \frac{n}{p} \in \mathbb{Z} \bigwedge p \in \mathbb{P} \bigwedge p > 2$$

13.08.30.0002.01

$$\left(\frac{0}{m}\right) = 0 /; \frac{m-3}{2} \in \mathbb{N}$$

Theorems

The Gauss reciprocity law

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} /;\ p,\, q > 2 \bigwedge p,\, q \in \mathbb{P}$$

Eigenvector of the discrete Fourier transform

For the odd prime p ($p \bmod 4 \neq 3$) the list $\left\{\left(\frac{0}{p}\right), \left(\frac{1}{p}\right), \ldots, \left(\frac{p-1}{p}\right)\right\}$ is an eigenvector of the discrete Fourier transform with eigenvalue one:

$$\left(\frac{n}{p}\right) = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) e^{2\pi i k n/p}.$$

Gauss' sums

Gauss sums can be calculated using the Jacobi symbol

$$\sum_{\substack{k=1 \\ \gcd(k,p)=1}}^{p} e^{\frac{2 h \pi i k^2}{p}} = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p} - 1 /; \qquad p \in \mathbb{P},\ p > 2 \bigwedge h \in \mathbb{N}^+.$$

History

– L. Euler (1729, published in 1785)
– A.-M. Legendre (1785, 1798) introduced the symbol $\left(\frac{n}{m}\right)$ for solving quadratic congruences
– C.F. Gauss (1796)
– C. G. J. Jacobi (1837)

Copyright