2.147 Definition Let $n \geq 3$ be odd with prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined to be

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

Observe that if n is prime, then the Jacobi symbol is just the Legendre symbol.

2.148 Fact (*properties of Jacobi symbol*) Let $m \geq 3$, $n \geq 3$ be odd integers, and $a, b \in \mathbb{Z}$. Then the Jacobi symbol has the following properties:

(i) $\left(\frac{a}{n}\right) = 0, 1,$ or -1. Moreover, $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a, n) \neq 1$.
(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. Hence if $a \in \mathbb{Z}_n^*$, then $\left(\frac{a^2}{n}\right) = 1$.
(iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
(iv) If $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
(v) $\left(\frac{1}{n}\right) = 1$.
(vi) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$. Hence $\left(\frac{-1}{n}\right) = 1$ if $n \equiv 1 \pmod{4}$, and $\left(\frac{-1}{n}\right) = -1$ if $n \equiv 3 \pmod{4}$.
(vii) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. Hence $\left(\frac{2}{n}\right) = 1$ if $n \equiv 1$ or $7 \pmod{8}$, and $\left(\frac{2}{n}\right) = -1$ if $n \equiv 3$ or $5 \pmod{8}$.
(viii) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$. In other words, $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ unless both m and n are congruent to 3 modulo 4, in which case $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

By properties of the Jacobi symbol it follows that if n is odd and $a = 2^e a_1$ where a_1 is odd, then

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \bmod a_1}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}.$$

This observation yields the following recursive algorithm for computing $\left(\frac{a}{n}\right)$, which does not require the prime factorization of n.

2.149 Algorithm Jacobi symbol (and Legendre symbol) computation

---

JACOBI(a,n)
INPUT: an odd integer $n \geq 3$, and an integer a, $0 \leq a < n$.
OUTPUT: the Jacobi symbol $\left(\frac{a}{n}\right)$ (and hence the Legendre symbol when n is prime).

1. If $a = 0$ then return(0).
2. If $a = 1$ then return(1).
3. Write $a = 2^e a_1$, where a_1 is odd.
4. If e is even then set $s \leftarrow 1$. Otherwise set $s \leftarrow 1$ if $n \equiv 1$ or $7 \pmod{8}$, or set $s \leftarrow -1$ if $n \equiv 3$ or $5 \pmod{8}$.
5. If $n \equiv 3 \pmod{4}$ and $a_1 \equiv 3 \pmod{4}$ then set $s \leftarrow -s$.
6. Set $n_1 \leftarrow n \bmod a_1$.
7. If $a_1 = 1$ then return(s); otherwise return($s \cdot$ JACOBI(n_1,a_1)).

2.150 Fact Algorithm 2.149 has a running time of $O((\lg n)^2)$ bit operations.