Символ Якоби

Обобщением понятия символа Лежандра является символ Якоби.

Определение 2.7. Пусть $m, n \in \mathbb{Z}$, где $n = p_1 p_2 \ldots p_r$ и числа $p_i \neq 2$ простые (не обязательно различные). *Символ Якоби* $\left(\frac{m}{n}\right)$ определяется равенством

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\ldots\left(\frac{m}{p_r}\right).$$

Если число n — простое, то символ Якоби является символом Лежандра.

Символ Якоби обладает следующими свойствами.

1. $\left(\frac{a}{n}\right)$ принимает значения 0, 1 или -1, причем $\left(\frac{a}{n}\right) = 0$ тогда и только тогда, когда НОД(a, n) $\neq 1$. Полагают $\left(\frac{a}{\pm 1}\right) = 1$.

2. $\left(\frac{a + kn}{n}\right) = \left(\frac{a}{n}\right)$ для всех $a, k \in \mathbb{Z}$.

3. $\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right)$ для всех $a, b \in \mathbb{Z}$, НОД(b, n) = 1.

4. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ для всех $a, b \in \mathbb{Z}$.

5. $\left(\frac{1}{n}\right) = 1$; $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$. Следовательно, $\left(\frac{-1}{n}\right) = 1$ при $n \equiv 1 \pmod 4$; $\left(\frac{-1}{n}\right) = -1$ при $n \equiv -1 \pmod 4$.

6. $\left(\dfrac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$. Следовательно, $\left(\dfrac{2}{n}\right)=1$ при $n\equiv\pm1 \pmod 8$; $\left(\dfrac{2}{n}\right)=-1$ при $n\equiv\pm3 \pmod 8$.

7. Для нечетных целых чисел m, n справедливо равенство $\left(\dfrac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\dfrac{n}{m}\right)$.

Из свойств символа Якоби следует, что если n — нечетное целое число и $a=2^k a_1$, где число a_1 нечетное, то

$$\left(\frac{a}{n}\right)=\left(\frac{2^k}{n}\right)\left(\frac{a_1}{m}\right)=\left(\frac{2}{n}\right)^k\left(\frac{n \pmod{a_1}}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}}.$$

Отсюда получаем алгоритм вычисления символа Якоби [4].

Алгоритм 2.1. Вычисление символа Якоби.

Вход. Нечетное целое число $n\geq3$, целое число a, $0\leq a<n$.

Выход. Символ Якоби $\left(\dfrac{a}{n}\right)$.

1. Положить $g\leftarrow1$.
2. При $a=0$ результат: 0.
3. При $a=1$ результат: g.
4. Представить a в виде $a=2^k a_1$, где число a_1 нечетное.
5. При четном k положить $s\leftarrow1$. При нечетном k положить $s\leftarrow1$, если $n\equiv\pm1 \pmod 8$; положить $s\leftarrow-1$, если $n\equiv\pm3 \pmod 8$.
6. При $a_1=1$ результат: $g\cdot s$.

7. Если $n \equiv 3 \pmod 4$ и $a_1 \equiv 3 \pmod 4$, то $s \leftarrow -s$.

8. Положить $a \leftarrow n \pmod{a_1}$, $n \leftarrow a_1$, $g \leftarrow g \cdot s$ и вернуться на шаг 2. □

Сложность алгоритма равна $O(\log^2 n)$.

Пример 2.25. Вычислим символ Якоби $\left(\frac{532}{2739}\right)$. Полагаем $g = 1$.

Первая итерация. Находим представление числа a: $532 = 2^2 \cdot 133$, $a_1 = 133$. Число $k = 2$ четное, поэтому $s = 1$. Полагаем $a = 2739 \equiv 79 \pmod{133}$, $n = 133$, $g = 1 \cdot 1 = 1$.

Вторая итерация. Находим представление числа a: $79 = 2^0 \cdot 79$, $a_1 = 79$. Число $k = 0$ четное, поэтому $s = 1$. Полагаем $a = 133 \equiv 54 \pmod{79}$, $n = 79$, $g = 1 \cdot 1 = 1$.

Третья итерация. Находим представление числа a: $54 = 2^1 \cdot 27$, $a_1 = 27$. Число $k = 1$ нечетное и $n = 79 \equiv -1 \pmod 8$, поэтому $s = 1$. Кроме того, $n \equiv 3 \pmod 4$ и $a_1 \equiv 3 \pmod 4$, поэтому $s = -1$. Полагаем $a = 79 \equiv 25 \pmod{27}$, $n = 27$, $g = 1 \cdot (-1) = -1$.

Четвертая итерация. Находим представление числа a: $25 = 2^0 \cdot 25$, $a_1 = 25$. Число $k = 0$ четное, поэтому $s = 1$. Полагаем $a = 27 \equiv 2 \pmod{25}$, $n = 25$, $g = (-1) \cdot 1 = -1$.

Пятая итерация. Находим представление числа a: $2 = 2^1 \cdot 1$, $a_1 = 1$. Число $k = 1$ нечетное и $n \equiv 1 \pmod 8$, поэтому $s = 1$.

Поскольку $a_1 = 1$, алгоритм заканчивает работу на шаге 6 с результатом: $-1 \cdot 1 = -1$. □