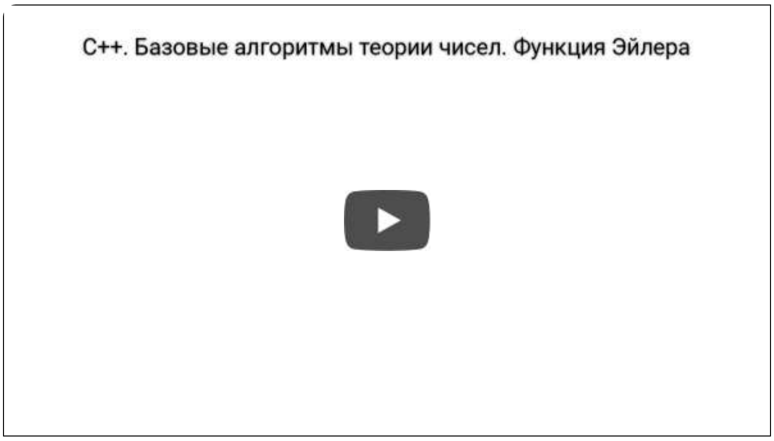
Функция Эйлера



Функция Эйлера от числа n (обозначается $\varphi(n)$) — это количество чисел от 1 до n, взаимно простых с n.

Например, $\varphi(1) = 1$.

Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, то $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_s^{\alpha_s} - p_s^{\alpha_s - 1})$.

Преобразуем формулу:

$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_s^{\alpha_s} - p_s^{\alpha_s - 1}) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_s}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$.

Из первой формулы для функции Эйлера видно, что она мультипликативна. А вторая формула удобна для реализации алгоритма вычисления функции Эйлера.

Теорема Эйлера

Для взаимно простых натуральных чисел $m > 1$ и a выполнено $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Эта теорема является обощением малой теоремы Ферма. Это легко проверить, вычислив значение функции Эйлера от простого числа p: $\varphi(p) = p - 1$.

Теорема Эйлера помогает при поиске обратного для числа a по составному модулю m в $\mathbb{Z}_m$, если a и m взаимно простые. Верно соотношение: $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$.

Если $gcd(m, a) \neq 1$, то для такого числа a не существует обратного.

Докажем это. Пусть $d = gcd(a, m) > 1$. Предположим, что a^{-1} существует, тогда $a^{-1}a \equiv 1 \pmod{m}$. Это значит, что $(a^{-1}a - 1) \vdots m$, отсюда следует, что и $(a^{-1}a - 1) \vdots d$, однако $a^{-1}a$ при этом также делится на d, а 1 на d не делится. Получаем противоречие.