СИСТЕМЫ ВЫЧЕТОВ

ОПРЕДЕЛЕНИЕ. *Полной системой вычетов по модулю* m называется совокупность m целых чисел, содержащая точно по одному представителю из каждого класса вычетов по модулю m.

ОПРЕДЕЛЕНИЕ. Совокупность чисел $0, 1, 2, \dots, m-1$ называется *системой наименьших неотрицательных вычетов по модулю* m.

(т.е. члены $a + km$ при $k = 0$)

ОПРЕДЕЛЕНИЕ. Совокупность чисел

$$0, \pm 1, \pm 2, \dots, \pm\frac{m-1}{2} \text{ при нечетном } m,$$

$$-\frac{m}{2}+1, \dots, -1, 0, 1, \frac{m}{2} \text{ при четном } m$$

называется *системой абсолютно наименьших вычетов по модулю* m, т.е. каждый из абсолютно наименьших вычетов по абсолютной величине не превосходит половины модуля.

ОПРЕДЕЛЕНИЕ. Часть полной системы вычетов, состоящая из чисел, взаимно простых с модулем называется *приведенной системой вычетов*.

ПРИМЕР 1. Выписать: 1) любые три полные системы вычетов (ПоСВ) по модулю m; 2) Систему наименьших неотрицательных вычетов (СННВ) по модулю m; 3) Две любые приведенные системы вычетов (ПрСВ) по модулю m. Сравнить количество чисел в приведенной системе вычетов по модулю m со значением функции Эйлера от m.

а) $m = 7$; б) $m = 4$; в) $m = 2$; г) $m = 9$.

ПРИМЕР 2. Вычислить абсолютно наименьший и наименьший неотрицательный вычеты числа a по модулю m:

а) $a = 12, m = 15$; б) $a = 35, m = 31$; в) $a = -1, m = 81$;

г) $a = 50, m = 12$; д) $a = 8, m = 15$; е) $a = 8, m = 17$;

ё) $a = -80, m = 100$; ж) $a = -4, m = 3$; з) $a = 11, m = 11$.

ФУНКЦИЯ ЭЙЛЕРА. ТЕОРЕМА ЭЙЛЕРА. МАЛАЯ ТЕОРЕМА ФЕРМА.

Функция Эйлера:

1) $\varphi(1) = 1$;

2) если p – простое, то $\varphi(p) = p - 1$;

3) если НОД$(m, n) = 1$, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$;

4) если p – простое, то $\varphi(p^n) = p^n - p^{n-1}$;

5) если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ – каноническое разложение числа n, то
$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdot \ldots \cdot \varphi\left(p_s^{\alpha_s}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_s}\right)$

Теорема Эйлера: НОД$(a, m) = 1 \quad \Longrightarrow \quad a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Малая теорема Ферма: p – простое и НОД$(a, p) = 1 \implies a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

ПРИМЕР 1. Пользуясь свойствами функции Эйлера, вычислить $\varphi(n)$: а) $\varphi(73)$; б) $\varphi(81)$; в) $\varphi(97)$; г) $\varphi(343)$; д) $\varphi(28)$; е) $\varphi(210)$; ё) $\varphi(10800)$; ж) $\varphi(32)$; з) $\varphi\big(\varphi(125)\big)$; и) $\varphi(63000)$; й) $\varphi(1000000)$.

ПРИМЕР 2. Найти остаток от деления n на m:

а) $n = 90^{42}, m = 41$; б) $n = 34^{160\,003}, m = 15$; в) $n = (-5)^{100\,016}, m = 11$; г) $n = 8^{485}, m = 187$; д) $n = (-2)^{634\,178}, m = 117$; е) $n = 50^{190\,021}, m = 38$; ё) $n = 3^{161\,613}, m = 16$; ж) $n = 5^{186\,609}, m = 9$; з) $n = 347^{174\,007}, m = 349$; и) $n = (-3)^{49}, m = 15$; й) $n = (-714)^{3043}, m = 52$.