УКАЗАНИЕ К РЕШЕНИЮ ЗАДАЧИ № 28

В силу теоремы Эйлера, для любых взаимно простых a и n выполняется соотношение:

$$a^{f(n)} \circ 1 \; mod \; n, \qquad (9.1)$$

где $f(n)$ обозначает функцию Эйлера, значение которой равно числу положительных целых значений, меньших n и взаимно простых с n. Для простого числа p

$$f(p)=p-1,$$

Если предположить, что два числа p и q простые, тогда для $n=p^a*q^b$ функция Эйлера будет иметь вид

$$f(n)= f(p^a*q^b)= f(p^a)* f(q^b)=[(p-1)\, p^{a-1}]*[(q-1)q^{b-1}]. \qquad (9.2)$$

Рассмотрим более общее соотношение, чем (9.1). Говорят, что число a, взаимно простое с модулем n, <u>принадлежит показателю</u> m, если m – такое наименьшее натуральное число, что выполняется сравнение

$$a^m \circ 1 \; mod \; n. \qquad (9.3)$$

Если a и n являются взаимно простыми, то существует, по крайней мере, одно число $m=f(n)$, удовлетворяющее (9.3). Наименьшее из положительных чисел m, для которых выполняется (9.3), является длиной периода последовательности, генерируемой степенями a.

Справедливы следующие свойства.

Свойство 1. Числа a^0, a^1,… ,a^{m-1} попарно несравнимы по модулю n. Действительно, $a^l \circ a^k \; mod \; n$, $l > k \Rightarrow a^{l-k} \circ 1 \; mod \; n$, где $l – k \in \mathrm{N}$, $l – k < m$.

Свойство 2. $a^g \circ a^{g'} \; mod \; n \Leftrightarrow g \circ g' \; mod \; m$. Разделим g, g' на m с остатками $g = mq + r$, $g' = mq' + r'$. Тогда $a^g \circ a^{g'} \Leftrightarrow a^{mq+r} \circ a^{mq'+r'} \Leftrightarrow a^r \circ a^{r'} \Leftrightarrow r'=r$. Отсюда вытекает следующее свойство.

Свойство 3. $m|\; f(n)$. Число, принадлежащее показателю $f(n)$, называется *первообразным корнем* по модулю n.

Свойство 4. По любому простому модулю p существует первообразный корень. Первообразные корни существуют по модулям 2, 4, p^a, $2p^a$, где p – нечетное простое, $a \in$ N.

Свойство 5. Пусть $c = f(n)$ и $q_1, q_2, \ldots, q_k$ – различные простые делители числа c. Число a, взаимно простое с модулем n, будет первообразным корнем тогда и только тогда, когда не выполнено ни одно из следующих сравнений:

$$a^{c/q_1} \equiv 1 \bmod n, a^{c/q_2} \equiv 1 \bmod n, \ldots, a^{c/q_k} \equiv 1 \bmod n$$

Необходимость следует из того, что $a^{f(n)} \circ 1 \ mod\ n$ и сравнение не имеет места при меньших показателях степени. Обратно, допустим, что a не удовлетворяет ни одному из сравнений, и пусть a принадлежит показателю $m < c$. Тогда $m|c$ $\Rightarrow c=mn$. Обозначим через q простой делитель u. Тогда легко получить противоречие:

$$a^{c/q} = a^{mu/q} = (a^m)^{u/q} \circ 1 \ mod\ n.$$

Если некоторая последовательность имеет длину $f(n)$, тогда целое число a генерирует своими степенями множество всех ненулевых вычетов по модулю n. Такое целое число называют первообразным корнем числа a по модулю n. Количество их равно для числа n

$$f(n-1), \tag{9.4}$$

где f - функция Эйлера.

<u>Пример (*Проверка Свойства 5.*).</u> Пусть n=41. Имеем $c = f(41) = 40 = 2^3 \cdot 5$. Итак, первообразный корень не должен удовлетворять двум сравнениям

$$a^8 \equiv 1 (mod 41), \ a^{20} \equiv 1 (mod 41).$$

Испытаем числа 2, 3, 4, …: $2^8 \equiv 10$, $2^{20} \equiv \mathbf{1}$, $3^8 \equiv \mathbf{1}$, $4^8 \equiv \mathbf{18}$, $4^{20} \equiv \mathbf{1}$, $5^8 \equiv \mathbf{18}$, $5^{20} \equiv \mathbf{1}$, $6^8 \equiv 10$, $6^{20} \equiv 40$. Отсюда видим, что 6 является наименьшим первообразным корнем по модулю 41.