
Лекция №9

---

6. Примитивные корни и индексы.

6.3. Примитивные корни по составному модулю.

Следующим шагом является определение всех составных чисел, по модулю которых существуют примитивные корни. Некоторая информация содержится в следующих двух отрицательных результатах.

Теорема 1. *Для $k \geq 3$ не существует примитивных корней по модулю 2^k.*

Теорема 2. *Если НОД$(m, n) = 1$, где $m > 2$ и $n > 2$, то не существует примитивных корней по модулю mn.*

Ниже представим некоторые частные случаи:

Следствие 1. *По модулю n не существует примитивного корня, если*

1. *либо n делится на два нечетных простых числа,*
2. *либо $n = 2^m p^k$, где p – нечетное простое и $m \geq 2$.*

Существенной особенностью последних результатов является то, что они ограничивают наш поиск примитивных корней по модулям 2, 4, p^k и $2p^k$, где p – нечетное простое число.

Лемма 1. *Если p – нечетное простое, то существует примитивный корень r по модулю p, такой, что $r^{p-1} \not\equiv 1 \pmod{p^2}$.*

Следствие 2. *Если p – простое, то существует примитивный корень по модулю p^2. В действительности, для примитивного корня r по модулю p, либо r, либо $r + p$ будет примитивным корнем по модулю p^2.*

Лемма 2. *Пусть p – простое, r – примитивный корень по модулю p, такой, что $r^{p-1} \not\equiv 1 \pmod{p^2}$. Тогда для всякого $k \geqslant 2$ имеет место*

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Теорема 3. *Если p – простое и $k \geqslant 1$, тогда существует примитивный корень по модулю p^k.*

Следствие 3. *Существуют примитивные корни по модулю $2p^k$, где p – простое число и $k \geqslant 1$.*

Подытоживая все выше сказанное в следующей теореме:

Теорема 4. *Примитивный корень по модулю $n > 1$ существует тогда и только тогда, когда*

$$n = 2, \quad 4, \quad p^k \quad \text{или} \quad 2p^k,$$

где p – простое число.

6.4. Теория индексов.

Оснавная часть этого параграфа посвящена понятию индекса. Пусть n – произвольное целое число, по модулю которого существует примитивный корень r. Как мы знаем, первые $\phi(n)$ степени числа r:

$$r, r^2, ..., r^{\phi(n)}$$

сравнимы по модулю n в некотором порядке с теми целыми числами, которые меньше n и взаимно просты с n. Следовательно, если a является произвольным целым, взаимно простым с n, то a может быть представлен в виде

$$a \equiv r^k \pmod{n}$$

для подходящего k, где $1 \leq k \leq \varphi(n)$.

Определение 1. *Пусть r – примитивный корень по модулю n. Если НОД$(a, n) = 1$, то наименьшее положительное целое k, такое, что $a \equiv r^k \pmod{n}$ называется индексом a относительно r.*

Будем обозначать индекс числа a относительно r как $\mathrm{ind}_r a$ или просто $\mathrm{ind} a$. Очевидно, что $1 \leq \mathrm{ind}_r a \leq \varphi(n)$ и

$$r^{\mathrm{ind}_r a} \equiv a \pmod{n}.$$

Теорема 5. *Если существует примитивный корень r по модулю n, то*

1. $\mathrm{ind}(ab) = \mathrm{ind} a + \mathrm{ind} b \pmod{\varphi(n)}$.

2. $\text{ind} a^k \equiv k\text{ind} a \pmod{\varphi(n)}$ *для* $k > 0$.

3. $\text{ind} 1 \equiv 0 \pmod{\varphi(n)}$, $\text{ind} r \equiv 1 \pmod{\varphi(n)}$.

Далее представим критерий разрешимости:

Теорема 6. *Пусть существует примитивный корень по модулю* n *и* $НОД(a, n) = 1$. *Тогда сравнение* $x^k \equiv a \pmod{n}$ *имеет решение тогда и только тогда, когда*

$$a^{\varphi(n)/d} \equiv 1 \pmod{n},$$

где $d = НОД(k, \varphi(n))$. *Если решение существует, то существует в точности* d *решений по модулю* n.