
Лекция №9 (16.11.20)

---

6. Примитивные корни и индексы.

6.1. Порядок целого числа по модулю n.

Из теоремы Эйлера нам известно, что $a^{\phi(n)} \equiv 1 \pmod{n}$, когда НОД$(a, n) = 1$. Тем не менее, часто существуют степени a, меньшие, чем $a^{\phi(n)}$, но сравнимые с 1 по модулю n. Отсюда следует определение:

Определение 1. *Пусть $n > 1$ и НОД$(a, n) = 1$. Порядком a по модулю n называется наименьшее положительное целое число k, такое, что $a^k \equiv 1 \pmod{n}$.*

Теорема 1. *Пусть целое число a имеет по модулю n порядок k. Тогда $a^h \equiv 1 \pmod{n}$ тогда и только тогда, когда $k|h$. В частности $k|\phi(n)$.*

Вот другое фундаментальное утверждение о порядке целого числа.

Теорема 2. *Если a имеет порядок k по модулю n, тогда $a^i \equiv a^j \pmod{n}$ тогда и только тогда, когда $i \equiv j \pmod{k}$.*

Следствие 1. *Если a имеет порядок k по модулю n, тогда a, a^2, ..., a^k не сравнимы по модулю n.*

Может возникнуть справедливый вопрос: возможно ли выразить порядок степеней a через порядок самого a?

Теорема 3. *Если целое число a имеет порядок k по модулю n и $h > 0$, тогда a^h имеет порядок $k/$НОД(h, k) по модулю n.*

Следствие 2. *Пусть a имеет порядок k по модулю n. Тогда a^h также имеет порядок k тогда и только тогда, когда НОД$(h, k) = 1$.*

Если целое число a имеет наибольший возможный порядок, оно называется *примитивным корнем* по модулю n.

Определение 2. *Если НОД*$(a, n) = 1$ *и порядок* a *по модулю* n *равен* $\phi(n)$, *тогда* a *– примитивный корень* n.

Другими словами, a является примитивным корнем по модулю n, если $a^{\phi(n)} \equiv 1 \pmod{n}$, но $a^k \not\equiv 1 \pmod{n}$ для любого положительного $k < \phi(n)$.

Теорема 4. *Пусть НОД*$(a, n) = 1$, *элементы* $a_1, a_2, ..., a_{\phi(n)}$ *являются положительными целыми числами, меньшими* n *и взаимно простыми с* n. *Если* a *– примитивный корень по модулю* n, *тогда*

$$a^1, a^2, ..., a^{\phi(n)}$$

будут сравнимы по модулю с $a_1, a_2, ..., a_{\phi(n)}$ *в некотором порядке.*

Из представленной теоремы можно сделать следующий вывод: в тех случаях, когда существует примитивный корень, можно сказать сколько всего существует примитивных корней.

Следствие 3. *Если по модулю* n *существует примитивный корень, тогда существует ровно* $\phi(\phi(n))$ *примитивных корней по этому модулю.*

6.2. Примитивные корни по простому модулю.

Теорема 5 (Лагранжа). *Если* p *– простое число и*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \qquad a_0 \not\equiv 0 \pmod{p}$$

– многочлен степени $n \geqslant 1$ *с целыми коэффициентами, тогда сравнение*

$$f(x) \equiv 0 \pmod{p}$$

имеет максимум n *несравнимых между собой решений по модулю* p.

Из этой теоремы легко выводится следующее следствие:

Следствие 4. *Если* p *– простое число и* $d \mid p - 1$, *тогда сравнение*

$$x^d - 1 \equiv 0 \pmod{p}$$

имеет ровно d *решений.*

Теорема 6. *Если* p *– простое и* $d|(p - 1)$, *то существует в точности* $\varphi(d)$ *несравнимых между собой целых чисел, имеющих порядок* d *помодулю* p.

Полагая $d = p - 1$, мы имеем следующее утверждение:

Следствие 5. *Если* p *– простое, то существует ровно* $\varphi(p - 1)$ *несравнимых между собой примитивных корней по модулю* p.