СУЩЕСТВОВАНИЕ ПЕРВООБРАЗНОГО КОРНЯ

ПОРЯДОК ОСТАТКА ДЕЛИТСЯ НА ПОРЯДОК ЕГО СТЕПЕНИ

При доказательстве малой теоремы Ферма мы обнаружили, что все ненулевые остатки по модулю $p = 7$ соответствуют различным степеням остатка $a = 3$:

$3^0 = 1$; $3^1 = 3$; $3^2 = 2$; $3^3 = 6$; $3^4 = 4$; $3^5 = 5$.

Такой остаток a называется, как мы уже говорили, первообразным корнем.

Напомним также, что степень $k \neq 0$, в которой остаток a впервые становится сравним с 1 по модулю p называется порядком остатка a:

$Ord_p a = k \Leftrightarrow a^k \equiv 1 \bmod p$

ТЕОРЕМА

Для любого простого нечетного модуля p существует первообразный корень.

Эту теорему мы будем долго доказывать через ряд вспомогательных утверждений.

УТВЕРЖДЕНИЕ

Если k — порядок остатка a по модулю p, то k делится на порядок a^n для любой степени n, т.е.

$Ord_p a = k \Leftrightarrow k \vdots Ord_p(a^n)\ \forall n \in \mathbb{N}$.

ДОКАЗАТЕЛЬСТВО

Во-первых, $(a^n)^k = (a^k)^n \equiv 1 \bmod p$.

Во-вторых, помним, что если $t = Ord_p(a^n)$, то $(a^n)^l \equiv 1 \bmod p \Leftrightarrow l \vdots t$. В нашем случае $l = k$. Доказано.

Вопрос: когда $Ord_p(a^n) = k$?

Ответ: $Ord_p(a^n) = k \Leftrightarrow НОД(n, k) = 1$.

Сейчас мы это докажем.

СТЕПЕНИ ОСТАТКА, ИМЕЮЩИЕ ТОТ ЖЕ ПОРЯДОК

Далее, т.к. речь идет об одном и том же простом модуле p, индекс p в обозначении порядка остатка будем опускать.

УТВЕРЖДЕНИЕ

Пусть $k = Ord\ a$.

Тогда: $Ord(a^n) = k \Leftrightarrow НОД(n, k) = 1$.

ДОКАЗАТЕЛЬСТВО

1-й случай: $НОД(n, k) > 1$, т.е. существует делитель $d > 1$ такой, что $n \vdots d$, $k \vdots d$. Тогда:

$a^n = a^{d \cdot (\frac{n}{d})}$, $(a^n)^{\frac{k}{d}} = (a^k)^{\frac{n}{d}} \equiv 1^{\frac{n}{d}} \equiv 1 \bmod p$.

Значит, $Ord(a^n) \leq \frac{k}{d} < k$.

2-й случай: $НОД(n, k) = 1$. Тогда $nm + kl = 1$ при некоторых целых m, l. Получаем:

$a^{nm} = a^{1-kl} = a(a^k)^{-l} \equiv a \bmod p$.

Тогда $k = Ord\ a = Ord(a^{nm}) = Ord(a^n)^m \leq Ord(a^n)$.

А значит, они равны: $Ord_p(a^n) = k$. Доказано.

Из этого утверждения следует, что количество степеней a, у которых такой же порядок, как у a, равно количеству чисел, не превосходящих k и взаимно простых с k. А это ни что иное, как функция Эйлера!

ЭЛЕМЕНТОВ ПОРЯДКА k РОВНО $\varphi(k)$

ОПРЕДЕЛЕНИЕ

Функция Эйлера $\varphi(k)$ — это число остатков по модулю k, взаимно простых с $k (k \in \mathbb{N}, k > 1)$.

Мы получили, что если $Ord\ a = k$, то существует как минимум $\varphi(k)$ элементов порядка k (все такие a^l, что $l < k$, НОД$(l, k) = 1$).

УТВЕРЖДЕНИЕ

Элементов порядка k ровно $\varphi(k)$.

ДОКАЗАТЕЛЬСТВО

Рассмотрим многочлен $x^k - 1$. Его корнями являются $a^0, a^1, \ldots a^{k-1}$ и только они, т.к. это k различных чисел, удовлетворяющих уравнению $x^k - 1 \equiv 0 \bmod p$, а больше корней многочлен степени k над полем иметь не может.

Значит, любой элемент b порядка k находится в этом списке, а среди них ровно $\varphi(k)$ элементов порядка k.

Доказано.

ЛЕММА О ФУНКЦИИ ЭЙЛЕРА

ЛЕММА: $\forall\, n \in \mathbb{N}, n > 1 \sum_{r|n} \varphi(r) = n$

ДОКАЗАТЕЛЬСТВО

Запишем ряд из чисел: $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots \frac{n}{n}$.
Их ровно n штук.

Сокращаем до несократимых дробей. Заметим, что:

1) в знаменателях получатся делители числа n;
2) встречаются все делители числа n;
3) со знаменателем r будет ровно $\varphi(r)$ дробей.

Получаем, что сумма по всем делителям r числа n дробей со знаменателем r равна n. Доказано.

СУЩЕСТВОВАНИЕ ПЕРВООБРАЗНОГО КОРНЯ

По лемме мы можем записать:

$$p - 1 = \sum_{k|p-1} \varphi(k)$$

Все порядки $Ord\ a$ являются делителями числа $p - 1$. Если мы будем суммировать количества элементов данного порядка, то их либо 0, либо $\varphi(k)$. Но если хотя бы в одном месте стоит 0, то мы получим сумму, меньшую $p - 1$. Значит, для каждого порядка k существует ровно $\varphi(k)$ элементов этого порядка, а в том числе, и для $k = p - 1$. А такой элемент a, что $Ord\ a = p - 1$, и есть первообразный корень.

Таким образом, теорема о существовании первообразного корня по простому модулю доказана.