ПЕРВООБРАЗНЫЕ КОРНИ

ПРИМЕРЫ ПЕРВООБРАЗНЫХ КОРНЕЙ

На этом и следующем уроках мы докажем теорему о существовании первообразного корня еще одним способом. Но прежде рассмотрим примеры первообразных корней для некоторых простых модулей.

$p = 3$. Множество ненулевых остатков: $\{1, 2\}$, первообразный корень: 2.

$p = 5$. Множество ненулевых остатков: $\{1, 2, 3, 4\}$, первообразные корни: 2, 3.

$p = 7$. Множество ненулевых остатков: $\{1, 2, 3, 4, 5, 6\}$, первообразные корни: 3, 5.

$p = 11$. Мы знаем, что количество первообразных корней равно $\varphi(p - 1) = \varphi(10) = 4$.

Проверим $a = 2$:

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 5$; $2^5 = -1$.

Уже видно, что т.к. $2^{\frac{p-1}{2}} = -1$, следующие 5 степеней будут равны этим же остаткам, только с минусами, и следовательно, 2 — первообразный корень по модулю 11.

$p = 13$. $\varphi(12) = 4$. Будем искать первообразные корни при помощи метода, который позже оформим в виде утверждения и докажем. Кандидатами будут остатки, которые не равны 1 в степенях $\frac{12}{2} = 6$ и $\frac{12}{3} = 4$.

$a = 2$. $2^4 = 16 \equiv 3 \bmod 13$, $2^6 = 64 - 1 \bmod 13$, следовательно, 2 — первообразный корень.

$p = 17$. $\varphi(16) = \varphi(2^4) = 2^3 = 8$, ровно половина (все нечетные остатки). Найдем хотя бы один из восьми.

На этот раз $a = 2$ не является первообразным корнем, т. к. $2^8 = 64 \equiv 1 \bmod 17$.

Проверим $a = 3$.

$3^8 = \left((3^2)^2\right)^2 = (81)^2 \equiv (-4)^2 \equiv -1 \bmod 17$, а значит $a = 3$ — первообразный корень по модулю 17.

Теперь перейдем к обоснованию метода поиска первообразных корней, который мы только что применили.

КРИТЕРИЙ ПЕРВООБРАЗНОГО КОРНЯ

ТЕОРЕМА

Пусть p — нечетное простое, и $p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ — каноническое разложение на простые множители числа $p - 1$.

Тогда: остаток a — первообразный корень по модулю $p \Leftrightarrow a^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$ ни при каком i.

ДОКАЗАТЕЛЬСТВО

$\Rightarrow$) очевидно: если $a^{\frac{p-1}{q_i}} \equiv 1 \bmod p$,

то $Ord\ a \leqslant \frac{p-1}{q_i} < p - 1$, значит, a — не первообразный корень.

$\Leftarrow$) Пусть все неравенства выполнены, но a — не первообразный корень. Тогда $Ord\ a < p - 1$.

Но $Ord\ a$ — делитель $p-1$ (собственный), поэтому он имеет каноническое разложение на множители $Ord\ a = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$, где все $\beta_i \leqslant \alpha_i$ и хотя бы одно $\beta_j < \alpha_j$ (строго). $\beta_j \leqslant \alpha_j - 1$, и $Ord\ a$ является делителем числа $q_1^{\alpha_1} q_j^{\alpha_j - 1} \dots q_s^{\alpha_s}$.

А это число и есть $\frac{p-1}{q_i}$, и т.к. оно делится на $Ord\ a$, должно быть выполнено $a^{\frac{p-1}{q_i}} \equiv 1 \bmod p$. Получили противоречие. Значит, a — первообразный корень. Теорема доказана.

С помощью этой характеризации мы еще одним способом выведем существование первообразного корня.

ПОИСК ПЕРВООБРАЗНОГО КОРНЯ

Будем исходить из канонического разложения для $p-1$:

$p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$.

Тогда $\forall\ a \in \{1, 2, \dots p-1 \qquad Ord\ a = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$, где $\beta_j \leqslant \alpha_j$.

ЛЕММА

Существует такой остаток a, что $\beta_1 = \alpha_1$, т. е. $Ord\ a = q_1^{\alpha_1} q_2^{\gamma_2} \dots q_s^{\gamma_s}$

ДОКАЗАТЕЛЬСТВО

От противного. Если $\forall\ a$ строго $\beta_1 < \alpha_1$, то все остатки имеют порядки, являющиеся делителями числа

$q_1^{\alpha_1 - 1} q_2^{\alpha_2} \dots q_s^{\alpha_s} = \frac{p-1}{q_1}$

Но тогда $\forall a\ a^{\frac{p-1}{q_i}} \equiv 1 \bmod p$.

Отсюда многочлен $x^{\frac{p-1}{q_i}} - 1$ имеет $p-1$ корней, а количество корней не может превосходить степень многочлена. Противоречие. Лемма доказана.

Значит, существует остаток a_1 такой, что $Ord\ a_1 = q_1^{\alpha_1} q_2^{\gamma_2} \dots q_s^{\gamma_s}$.

Аналогично существует остаток a_2 такой, что в разложение $Ord\ a_2$ входит $q_2^{\alpha_2}$ и т.д. Наконец, существует остаток a_s такой, что в разложение $Ord\ q_s$ входит $q_s^{\alpha_s}$.

На следующем уроке мы завершим доказательство существования первообразного корня на основе этого факта.