



Серия №34. Первообразный корень

20 июля

Определение. Пусть показатель остатка x по модулю n равен t . Если $t = \varphi(n)$, то x называется первообразным корнем по модулю n .

- 1. Усиление теоремы Эйлера.** Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Докажите, что если $(a, n) = 1$, то $a^{\text{НОК}(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_k^{\alpha_k}))} \equiv 1 \pmod{n}$.
- Обратите внимание, что НОК из усиления теоремы Эйлера обычно меньше $\varphi(n)$, и докажите, что:
 - а) Не существует первообразного корня по модулю $n : pq$, где p, q – различные нечётные простые числа.
 - б) Не существует первообразного корня по модулю $n : 4p$, где p – нечётное простое число (эта задача у вас уже была!).
 - в) Не существует первообразного корня по модулям 8 и $8 \cdot 2^k$.

Следствие. Первообразные корни могут существовать только по модулю $2, 4, p^k, 2p^k$.

- а) Пусть существует остаток u , показатель которого по модулю p равен t . Найдите все корни уравнения $x^t \equiv 1 \pmod{p}$.
 - б) Докажите, что существует либо $\varphi(t)$, либо 0 остатков, имеющих показатель, равный t .
- а) Рассмотрим дроби $\frac{1}{p-1}, \frac{2}{p-1}, \dots, \frac{p-1}{p-1}$. Сократим все дроби. Пусть t – делитель числа $p-1$. Сколько дробей будут иметь знаменатель, в точности равный t ?
 - б) **Лемма Гаусса.** Докажите формулу (суммирование по всем делителям числа $p-1$):

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

- в) Докажите, что существует не 0, а ровно $\varphi(t)$ остатков с показателем t .

Теорема. По нечётному простому p существует $\varphi(p-1)$ первообразных корней.

Задачи

- Докажите, что при любом натуральном k , где $\text{НОД}(k, 2026) = 1$, верно:

$$1^k + 2^k + 3^k \dots + 2026^k \equiv 1 + 2^k + 2^{2k} + \dots + 2^{2025k} \equiv 0 \pmod{2027}.$$

Число 2 является первообразным корнем по простому модулю 2027.

- Докажите, что для любого простого p первые $(p-1)$ натуральных чисел можно расставить по кругу так, чтобы для любых трех подряд идущих чисел a, b, c разность $b^2 - ac$ делилась на p .
- Пусть $p > 3$ – простое число. Докажите, что произведение всех первообразных корней по модулю p сравнимо с 1 по модулю p .
- Пусть q – простое число, а $4q+1$ – тоже простое. Докажите, что 2 является первообразным корнем по модулю $4q+1$.
- Докажите, что для любого натурального n найдётся такое m , что $2^m + 2026 : 3^n$.

- 10.а)** Пусть a – первообразный корень по простому нечетному модулю p . Докажите, что если a не является первообразным корнем по модулю p^2 , то $a + p$ – является.
- б) Докажите, что если b – первообразный корень по модулю p^2 , то b – первообразный корень и по модулю p^k при $k > 2$.