

Первообразный корень

1. **Повторение.** Пусть $1 = d_1 < d_2 < \dots < d_k = n$ — все делители числа n . Докажите, что $\varphi(d_1) + \dots + \varphi(d_k) = n$.

Обозначим через $\psi(t)$ количество остатков от деления на p , чей показатель равен t .

2. Пусть p — простое число. $1 = d_1 < d_2 < \dots < d_k = p - 1$ — все делители числа $p - 1$. Докажите, что $\psi(d_1) + \dots + \psi(d_k) = p - 1$.
3. Пусть показатель остатка a по модулю p равен d .
- (а) Докажите, что $1, a, \dots, a^{d-1}$ — это все корни многочлена $x^d - 1$.
- (б) Пусть показатель остатка b по модулю p также равен d . Докажите, что $b \equiv a^s \pmod{p}$.
- (в) В условиях предыдущего пункта докажите, что $\text{НОД}(d, s) = 1$.
4. Выведите из предыдущей задачи, что $\psi(d) \leq \varphi(d)$ для любого делителя $d|p - 1$.
5. Докажите, что $\psi(d) = \varphi(d)$ для любого делителя $d|p - 1$.

Из задачи 5 следует, что $\psi(p - 1) = \varphi(p - 1) > 0$. Значит, существует остаток g (и не один, а целых $\varphi(p - 1)$ штук) такой, что показатель g равен $p - 1$. Такой остаток называется *первообразным корнем по модулю p* .

6. Для каких простых p первообразный корень может быть квадратичным вычетом?
7. Докажите, что любой ненулевой остаток a от деления на p представим в виде $a \equiv g^t \pmod{p}$ для некоторой степени t .
8. Сколько решений имеет уравнение
- (а) $x^5 \equiv 1 \pmod{101}$?
- (б) $x^{70} \equiv 1 \pmod{101}$?
- (в) $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{101}$?
9. Найдите остаток $1^{10} + 2^{10} + \dots + 100^{10}$ от деления на 101.
10. Пусть p — простое. Можно ли расставить по кругу числа $1, 2, \dots, p - 1$ так, чтобы для любых трех подряд идущих чисел a, b, c (именно в таком порядке) число $b^2 - ac$ делилось бы на p ?
11. Можно ли разбить числа от 1 до 2016 на группы по 7 так, чтобы сумма чисел в каждой семёрке делилась на 2017?