10-1 Первообразные корни 15 марта 2021

Определение. Если $(a, m) = 1$ и показатель числа a по модулю m равен $\varphi(m)$, то a называется *первообразным корнем* по модулю m.

Замечание. Тем самым, $a^0, a^1, a^2, \ldots, a^{\varphi(m)-1} \pmod m$ – это *все* вычеты, взаимно простые с m.

Воспоминание о простом модуле. По любому простому модулю p существует первообразный корень.

1. Пусть по модулю m существует первообразный корень.

а) Пусть d — некоторое натуральное число. Сколько существует вычетов r, для которых $r^d \equiv 1 \pmod m$?

б) Сколько существует первообразных корней по модулю m?

2. Даны натуральные взаимно простые a и n. Докажите, что a не является первообразным корнем по модулю n тогда и только тогда, когда для некоторого простого делителя q числа $\varphi(n)$ выполнено сравнение $a^{\frac{\varphi(n)}{q}} \equiv 1 \pmod n$.

3. Пусть g — первообразный корень по простому модулю $p = 4k + 3$, удовлетворяющий условию $g^2 \equiv g + 1 \pmod p$. Докажите, что $g - 1$ и $g - 2$ — также первообразные корни по модулю p.

Воспоминание об Эйлере. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ – разложение m на простые множители, $s = \text{НОК}(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \ldots, \varphi(p_n^{\alpha_n}))$. Тогда $a^s \equiv 1 \pmod m$ для любого целого a, взаимно простого с m.

4. а) Пусть g – первообразный корень по модулю простого нечётного p. Докажите, что для любого натурального α хотя бы одно из чисел g и $g + p$ является первообразным корнем по модулю p^α.

б) Пусть g – первообразный корень по модулю p^α. Докажите, что какое-то из чисел g и $g + p^\alpha$ является первообразным корнем по модулю $2p^\alpha$.

в) Докажите, что первообразные корни существуют только по модулям 1, 2, 4, p^α, $2p^\alpha$ (где $p > 2$ — простое, α — натуральное).

5. Докажите, что для любого простого числа $p > 2$ существует натуральное $g < p$, являющееся первообразным корнем по всем модулям p^k одновременно (для всех натуральных k).