Первообразные корни

10 класс
03.03.14

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

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

Упражнение 1. Существует ли первообразный корень по модулю 8? По модулю 9?

1. По модулю m существует первообразный корень.
   а. Сколько тогда существует элементов a для которых $a^d \equiv 1 \ (mod\ m)$?
   б. Сколько имеется первообразных корней?
2. а. Над $\mathbb{Z}_p$ (p - простое) многочлен степени d имеет не более d корней.
   б. При $d|p-1$ уравнение $x^d = 1$ имеет ровно d корней.
   в. Если $d|p-1$, то обозначим $\psi(d)$ количество вычетов показателя ровно d. Докажите, что $d = \sum\limits_{d'} \psi(d')$, где суммирование ведется по всем делителям d' числа d.
   г. Выведите из пунктов $а, б, в$: **Теорема (Гаусс).** Существует первообразный корень по модулю простого p.
3. Пусть p - простое, $p > 2$
   а. Докажите, что если a - первообразный корень по модулю p, то либо a, либо $a + p$ является первообразный корень по модулю p^2.
   б. a - первообразный корень по модулю p^2. Докажите тогда, что a является первообразным корнем по модулю p^α.

Упражнение 2.
а. Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?
б. Покажите, что 2 - первообразный корень по модулю 29.

Замечание 2. По модулю m существует первообразный корень тогда и только тогда, когда m имеет вид $2, 4, p^\alpha, 2p^\alpha$, где $p > 2$ - простое.

---

1. Решите уравнение $1 + x + \ldots + x^6 \equiv 0 \ (mod\ 29)$.
2. Докажите, что числа $1, 2, \ldots, p-1$ можно расставить по кругу так, что для любых трёх последовательных a, b, c разность $b^2 - ac$ будет делится на простое p.
3. Докажите, что для каждого n найдется такое m, что $2^m + 2014 \vdots 3^n$.