Первообразные корни

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

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

0. Существует ли первообразный корень по модулю 8? По модулю 9?

1. Пусть m — такое натуральное число, что по его модулю существует первообразный корень, и пусть d — произвольное натуральное число.

   a) Сколько существует вычетов a, для которых $a^d \equiv 1 \pmod{m}$?

   b) Сколько существует первообразных корней по модулю m?

2. Пусть p – простое.

   a) Докажите, что если $p-1$ делится на d, то многочлен $x^d - 1$ имеет ровно d корней по модулю p.

   b) Докажите, что для любого натурального n справедливо $\sum_{d|n} \varphi(d) = n$

   c) Докажите, что для любого d делящего $p-1$ есть ровно $\varphi(d)$ вычетов, показатель которых по модулю p равен d. В частности, существует первообразный корень по модулю p.

3. Пусть p – простое, $p > 2$.

   a) Докажите, что если a – первообразный корень по модулю p, то либо a, либо $a + p$ является первообразным корнем по модулю p^2

   b) Пусть a – первообразный корень по модулю p^2. Докажите, что a является первообразным корнем по модулю p^n при любом натуральном n.

4. a) Как выяснить, является ли a первообразным корнем по модулю m, возводя a не во все $\varphi(m)$ степеней?

   b) Покажите, что 2 – первообразный корень по модулю 29.

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

5. a) Решите сравнение $1 + x + \ldots + x^6 \equiv 0 \pmod{29}$

   b) Как найти все решения сравнения $x^d \equiv 1 \pmod{p}$, если известен первообразный корень?

6. Докажите, что для каждого n найдется такое m, что $2^m + 2020$ делится на 3^n.