Показатели и первообразные корни. 14 июля

Определение: Для взаимно простых натуральных чисел a и n наименьшее такое натуральное t, что $a^t \equiv 1 \pmod{n}$, называется **показателем** числа a по модулю n. Если показатель равен $\phi(n)$, то остаток a называется **первообразным корнем** по модулю n.

1 а) Докажите, что $a^d \equiv 1 \pmod{n} \Leftrightarrow d$ делится на t.

б) Докажите, что $\phi(a^n - 1)$ делится на n.

в) Найдите все простые p и q, такие что $2^p - 1$ делится на q и $2^q - 1$ делится на p

г) Докажите, что любой простой делитель числа $2^{2^n} + 1$ имеет вид $2^{n+1}x + 1$ и выведите бесконечность множества простых чисел такого вида (для фиксированного n).

д) Для фиксированного простого p докажите бесконечность множества простых чисел вида $2px + 1$ (*Подсказка:* Посмотрите на простые делители $\frac{a^p-1}{a-1}$, не делящие $a - 1$).

2 а) Докажите, что $n = \sum_{d|n} \phi(d)$ (*Подсказка:* рассмотрите дроби $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$).

Для следующих пунктов вспоминаем про многочлены над F_p.

б) Докажите, что для любого d существует не более d остатков (по модулю p) показателя, делящего d.

в) Докажите, что для $d|p - 1$ существует ровно d остатков (по модулю p) показателя, делящего d.

г) Докажите, что для $d|p - 1$ существует ровно $\phi(d)$ остатков показателя d по модулю p (в частности $\phi(p - 1) > 0$, так что первообразные корни по простому модулю существуют).

3 а) Докажите, что числа $1, 2, \ldots, p - 1$ можно расставить по окружности так, что квадрат любого числа будет сравним по модулю p с произведением его соседей.

б) Для каждого натурального d найдите $\sum_{n=0}^{p-1} n^d \pmod{p}$.

в) При помощи первообразных корней докажите, что $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

4 а) Докажите, что для нечетного простого p и натуральных u, r (u не делится на p) число $(1 + pu)^{p^r} - 1$ делится на p^{r+1}, но не на p^{r+2}.

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

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

5 Александр Львович задумал s натуральных чисел и выписал на доску все их попарные суммы, в том числе суммы числа с самим собой. Для какого наибольшего s могло так оказаться, что все выписанные числа дают разные остатки по модулю $p(p - 1)$ (p - простое число)?