Показатели

Если вы уверенно знаете, как решать задачу 0, то её можно не сдавать. Если сомневаетесь — сдавайте.

0. Пусть a и n — взаимно простые натуральные числа. Докажите, что последовательность остатков чисел $1, a, a^2, a^3, \ldots$по модулю n периодическая без предпериода.

Определение. *Показателем* числа n по модулю a называется наименьшее натуральному d такое, что $a^d \equiv 1 \pmod{n}$. В терминах предыдущей задачи d — это длина минимального периода.

1. Докажите, что $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

2. Пусть d — показатель a по модулю n.
(a) Докажите, что если $a^k \equiv 1 \pmod{n}$, то k делится на d.
(b) Докажите, что если $a^k \equiv a^l \pmod{n}$, то $k \equiv l \pmod{d}$.
(c) Докажите, что показатель a по модулю n является делителем $\varphi(n)$, где $\varphi(n)$ — функция Эйлера. В частности, если $n = p$ — простое число, то d является делителем числа $p - 1$.

3. Пусть p — простое число.
(a) Докажите, что все делители числа $2^p - 1$ больше p.
(b) Докажите, что каждый простой делитель числа $2^p - 1$ имеет вид $2pk + 1$ для некоторого k.

4. Пусть p — простое число, d — делитель числа $p - 1$. Выберем среди остатков $1, 2, \ldots, p - 1$ те, чьи показатели по модулю p равны d. Докажите, что произведение всех выбранных чисел сравнимо с единицей по модулю p.

5. **(a)** Докажите, что не существует натурального $n > 1$ такого, что $2^n - 1$ делится на n.
(b) Пусть $3^n - 1$ делится на n. Докажите, что если $n > 2$, то n кратно 4.
(c) Найдите все пары натуральных a и b таких, что $2^a - 1$ делится на b и $2^b - 1$ делится на a.

6. Найдите все пары простых чисел p и q таких, что $(5^p - 2^p)(5^q - 2^q)$ делится на pq.