Показатели

Определение 1. Напомним, что число a *принадлежит показателю* t (или t является *показателем* числа a) по модулю n, если t является наименьшим натуральным числом таким, что $a^t \equiv 1 \pmod{n}$.

1. Пусть a принадлежит показателю t по модулю n. Тогда верны следующие утверждения:
а) числа $1 = a^0$, a^1, ..., a^{t-1} различны по модулю n.
б) $a^d \equiv 1 \pmod{n}$ тогда и только тогда, когда $d \,\vdots\, t$.
в) $a^d \equiv a^s \pmod{n}$ тогда и только тогда, когда $d - s \,\vdots\, t$.
г) $\varphi(n)$ делится на t.

2. а) Докажите, что в разложении на простые сомножители числа $2^q - 1$, где q — простое, любое число будет давать остаток 1 по модулю q.
б) Выведите из этого, что простых чисел бесконечно много.

3. Докажите, что $\varphi(a^n - 1)$ делится на n для натуральных a и n.

4. Пусть p и q — простые, $q > 5$. Известно, что $2^p + 3^p$ делится на q. Докажите, что $q > 2p$.

5. Докажите, что если m – степень двойки, то любой простой делитель числа $2^m + 1$ сравним с 1 по модулю $2m$.

6. Найдите все пары простых чисел (p, q) такие, что $5^p + 5^q \,\vdots\, pq$.

7. Докажите, что $2^n - 1$ не делится на n, $n > 1$.

8. Пусть g — первообразный корень по модулю p, p —простое. Докажите, что число $a = g^k$ принадлежит показателю $\dfrac{p-1}{(p-1, k)}$ по модулю p.

9. Докажите, что количество правильных положений кубика Рубика (то есть таких, которые можно получить из исходного положения, где все грани одноцветны) делится на а) 4; б) 3; в) 5; г) 7; д) 11.