Порядки

Определение. Пусть $(a, n) = 1$. Наименьшее натуральное число k, для которого $a^k \equiv 1 \pmod{n}$, называют *порядком* числа a по модулю n. Будем обозначать его через $\exp_n(a)$.

1. (a) Докажите, что для простого p, $\exp_p(a)$ является делителем числа $p-1$.
(b) Докажите, что $\exp_n(a)$ делит $\varphi(n)$.

2. Докажите, что если простое число p является делителем числа $a^4+a^3+a^2+a+1$ для некоторого a, то $p = 5$ или $p \equiv 1 \pmod{5}$.

3. Докажите, что ни при каком целом a число $a^2 + a + 1$ не кратно
(a) 5; (b) 17; (c) $6m - 1$, где m — натуральное число.

4. Пусть p простое. Докажите, что число $p^p - 1$ имеет простой делитель, сравнимый с единицей по модулю p.

5. Докажите, что для всяких натуральных $a > 1$ и $n > 1$ число $\varphi(a^n - 1)$ делится на n.

6. (a) Докажите, что любой нечетный простой делитель числа $a^2 + 1$ имеет вид $p = 4k + 1$. (b) Докажите, что если p — нечетный простой делитель числа $a^{2^n} + 1$, то $p - 1$ делится на 2^{n+1}.

7. Найти все пары (p, q) простых чисел такие, что число $2^p - 1$ делится на q, и среди простых делителей числа $q - 1$ имеются только числа 2, 3, 5 и 7.

8. Пусть $2^n + 1$ делится на n. Докажите, что n делится на 3.

9. Найдите все натуральные n, для которых $2^n + 1$ кратно n^2.

10. Докажите, что ни для какого натурального $n > 2$ число $2^n - 1$ не делится на n.