Теорема Эйлера и показатели

1. Пусть $1 = x_1 < \ldots < x_{\varphi(n)} \leqslant n$ — все остатки от деления на n, взаимно простые с n. Для взаимно простых a и n докажите, что

$$(ax_1) \cdot \ldots \cdot (ax_{\varphi(n)}) \equiv x_1 \ldots x_{\varphi(n)} \pmod n$$

и выведите из этого теорему Эйлера: $a^{\varphi(n)} \equiv 1 \pmod n$.

2. Пусть НОД$(a, n) = 1$. Рассмотрим ориентированный граф, вершины которого — остатки от деления на n, взаимно простые с n. Проведём ориентированное ребро из каждого остатка x в остаток ax.

(a) Докажите, что этот граф разбивается на циклы одинаковой длины.

(b) Выведите из этого теорему Эйлера: $a^{\varphi(n)} \equiv 1 \pmod n$.

3. **(a)** Пусть НОД$(a, p) = 1$ для некоторого простого числа p. По индукции по k докажите, что $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$

(b) Выведите из этого теорему Эйлера: $a^{\varphi(n)} \equiv 1 \pmod n$.

4. Даны взаимно простые натуральные числа a и n. *Показателем* числа a по модулю n назывется такое минимальное натуральное число d, что $a^d \equiv 1 \pmod n$.

(a) Докажите, что $a^k \equiv 1 \pmod n$ тогда и только тогда, когда k делится на d.

(b) Докажите, что $\varphi(n)$ делится на d.

5. Известно, что k^{33} заканчивается на 0001. На что может заканчиваться само k?

6. Докажите, что $k^2 + k + 1$ не может делиться на 101 ни при каком целом k.

7. Докажите, что при любом четном n число $2^{n!} - 1$ делится на $n^2 - 1$.

8. Дано простое нечётное число p.

(a) Докажите, что каждый простой делитель числа $a^p - 1$ является делителем числа $a - 1$ или имеет вид $2pk + 1$ для некоторого k.

(b) Докажите, что каждый простой делитель числа $a^{p-1} + \ldots + a + 1$ имеет вид $2pk + 1$ для некоторого k или равен p.

(c) Докажите, что простых чисел вида $2pk + 1$ бесконечно много.

9. Дано натуральное число n.

(a) Докажите, что каждый простой делитель числа $2^{2^n} + 1$ имеет вид $2^{n+1}k + 1$ для некоторого k.

(b) Докажите, что простых чисел вида $2^{n+1}k + 1$ бесконечно много.