

## Теорема Эйлера

**Опр.** Полной системой вычетов по модулю  $n$  называется множество всех остатков по модулю  $n$ . Обозначается  $\mathbb{Z}_n$

**Опр.** Приведенной системой вычетов по модулю  $n$  называется множество остатков по модулю  $n$ , взаимно простых с  $n$ . Обозначается  $\mathbb{Z}_n^*$ .

**Упр.** Сколько элементов в приведенной системе вычетов по модулю  $n$ ?

1. Пусть есть отображение  $f : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n$ ,  $f(x) = ax \pmod{n}$  для некоторого  $a$ , взаимно простого с  $n$ .

(a) Докажите, что  $\forall x \in \mathbb{Z}_n^* : f(x) \in \mathbb{Z}_n^*$ .

(b) Докажите, что  $f$  — биекция  $\mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$ .

(c) Пусть  $\{r_1, \dots, r_{\varphi(n)}\}$  — приведенная система вычетов по модулю  $n$ . Что произойдет с произведением  $r_1 \cdot \dots \cdot r_{\varphi(n)}$  после применения отображения  $f$ ?

(d) Докажите теорему Эйлера: Если  $(a, n) = 1$ , то  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

2. Существует ли степень тройки, оканчивающаяся на 0001?

3. Найдите остаток числа  $43^{4321} \pmod{2025}$ .

4. Найдите последние 4 цифры числа  $2^{1000} + 5^{1000}$ .

5. Пусть известно, что  $(m, 30) = 1$ . Докажите, что  $\underbrace{11 \dots 11}_{\varphi(m)} : m$ .

6. Сделаем теорему Эйлера круче. Пусть  $n = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m}$ . Обозначим  $f(n) = \text{НОК}(\varphi(p_1^{\alpha_1}), \dots, \varphi(p_m^{\alpha_m}))$ . Тогда для любого  $a$ , взаимно простого с  $n$ , выполнено  $a^{f(n)} \equiv 1 \pmod{n}$ .

7. Имеется последовательность  $a_n = x + nd$ , где  $x, d$  — натуральные числа, такие, что  $(x, d) = 1$ . Докажите, что среди членов этой последовательности встречается бесконечно много чисел, которые являются степенями числа  $x$ .