Теоремы Эйлера и Ферма

1 Теорема Эйлера

Теорема 1 (Т. Эйлера)**.** *Если два целых положительных числа* $\boldsymbol{n}$ *и* $\boldsymbol{a}$ *взаимно просты, то верно следующее утверждение*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \qquad \text{где } \varphi(n) \text{ — функция Эйлера}$$

Доказательство. Пусть $x_1, x_2, \ldots, x_{\varphi(n)}$ — приведенная система вычетов по модулю n.
Тогда $ax_1, ax_2, \ldots, ax_{\varphi(n)}$ — тоже приведенная система вычетов по тому же модулю n. Тогда получается, что верно сравнение

$$x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \equiv ax_1 \cdot ax_2 \cdot \ldots \cdot ax_{\varphi(n)} \pmod{n}$$

Очевидно, что a перемножилось $\varphi(n)$ раз, поэтому имеем:

$$x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \equiv a^{\varphi(n)} \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(n)} \pmod{n}$$

Заметим, x_i взаимно просты с n так как x_i входит в приведенную систему вычетов по модулю n и воспользуемся свойством сравнения по модулю. Получаем:

$$1 \equiv a^{\varphi(n)} \pmod{n}$$

Что нам и требовалось доказать. □