№27 Р.1 | Основы теории сравнений. Системы вычетов. Теорема Эйлера

См. билет №26.

Т2 (Эйлера)

$\forall m, \forall a : (a, m) = 1$

$a^{\ell(m)} \equiv 1 \pmod m$

Д-во.

Рассмотрим $\forall$ приведённую систему вычетов по модулю m. $x_1 \dots x_{\ell(m)}$

Рассм $ax_1 \dots ax_{\ell(m)}$

Тогда $ax_1 \dots ax_{\ell(m)}$ - прив. с-ма вычетов.

т.к. $(ax_i, m) = 1$

$ax_i \not\equiv ax_j \pmod m$ (иначе $a(x_i - x_j) \equiv 0 \pmod m$, $x_i \equiv x_j \not\pmod m$)

Тогда

$x_1 \cdot x_2 \dots x_{\ell(m)} \equiv ax_1 \cdot \dots \cdot ax_{\ell(m)} \pmod m$

$1 \equiv a^{\ell(m)} \pmod m$ ▨