№26 Р.1 | Основы теории сравнений. Системы вычетов. Малая теорема Ферма | Два д-ва

Опр. Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}_+$.
a сравнимо с b по модулю m если $a - b \vdots m$
Обз. $a \equiv b (m)$

Note Очевидно, что $a - b \vdots m \iff a$ и b дают одинаковые остатки по модулю m.

Note Отношение $\equiv$ - отн-е эквивалентности $\Rightarrow \mathbb{Z}$ распадается на классы эквив-сти.

Опр. Вычетом по модулю m наз-ся $\forall$ представитель класса эквивалентности, содержащий данный остаток при делении на m

Опр. Полная с-ма вычетов - $\forall$ набор из m всевозможных вычетов.

Опр. Приведенной с-мой вычетов наз-ся мн-во вычетов из полной с-мы, которые взаимно просты с m.

Th (Малая теорема Ферма)
Если p - пр-е, то $a^p \equiv a (p)$

Д-во

1 способ

$$\underbrace{(1 + \dots + 1)^p}_{a \text{ раз}} = \underbrace{1^p + \dots + 1^p}_{a \text{ раз}} + \sum P(n_1 \dots n_a) \equiv a (p) \text{ т.к.}$$

$$P(n_1 \dots n_a) = \frac{p!}{n_1! \dots n_a!}, \text{ где } n_i < p \Rightarrow \text{НОД}(n_1! \dots n_a!, p) = 1$$ ✓

2 способ При $a \equiv 0 (p)$ верно.
Пусть $\text{НОД}(a, p) = 1$. Рассмотрим полную с-му вычетов по модулю p
Утв. $\{1 \dots (p-1)\}$ и $\{a \dots (p-1)a\}$ - полные с-мы вычетов.

Д-во
$a1 \dots a(p-1)$
Предположим, что $ax \equiv ay (p)$ $x \neq y$
$\Rightarrow a(x-y) \equiv 0 (p) \Rightarrow x - y \equiv 0 (p) \Rightarrow x = y$?!

Тогда
$1 \cdot 2 \cdots (p-1) = a \cdot a \cdot 2 \cdots a \cdot (p-1)$
$a^{p-1} \equiv 1 (p)$. ✓