18.11.25 **Сравнения** Синицын Е.А.

Определение

$$a \equiv b \pmod m \iff m \mid (a-b)$$

Свойства:

1) $a \equiv b \pmod m$ $\quad m \mid 0$

2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ $\quad m \mid (a-b) \Rightarrow m \mid (b-c)$ — Отношение эквивалентности

3) $a \equiv b \pmod m,\ b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

$\blacktriangle$ $m \mid (a-b),\ m \mid (b-c)$ $\quad a-c = (a-b)+(b-c) \Rightarrow m \mid (a-c)$ $\blacktriangle$

4) $a \equiv b \pmod m,\ c \equiv d \pmod m \Rightarrow m \mid (a-b),\ m \mid (c-d)$

$a+b = b+d \pmod m$ $\quad (a+c)-(b+d) = (a-b)+(c-d) \Rightarrow m \mid ((a+c)-(b+d))$

$a-b = b-d \pmod m$ $\quad (a-c)-(b-d) = (a-b)-(c-d) \Rightarrow m \mid ((a-c)-(b-d))$

$ac = bd \pmod m$ $\quad ac-bd = a(c-d)+ad-bd = a(c-d)+d(a-b) \Rightarrow$

$\Rightarrow m \mid (ac-bd)$

5) $a \equiv b \pmod m$, $P(x)$ – многочлен, $P(a) = P(b) \pmod m$

6) $ab = cb \pmod m,\ (b,m)=1 \Rightarrow a = c \pmod m$

$\blacktriangle$ $m \mid (ab-cb) \Rightarrow m \mid (a-c)b \Rightarrow m \mid (a-c) \Rightarrow a = c \pmod m$ $\blacktriangle$

7) $a \equiv b \pmod m \Rightarrow ac = bc \pmod m,\ c \neq 0$

8) $ac = bc \pmod{m},\ c \neq 0$

$mc \mid (ac-bc) \Rightarrow mc \mid c(a-b) \Rightarrow m \mid (a-b) \Rightarrow a \equiv b \pmod m$

Обозн.

$\mathbb{Z}$ классы эквивалентности

$\overline{m} = \overline{0} = \{0, \pm m, \pm 2m, \dots\}$, $\quad a \equiv 0 \pmod m \Rightarrow m \mid (a-0)$

$\overline{m+1} = \overline{1} = \{1, \pm m+1, \pm 2m+1, \dots\}$ $\quad a \equiv 1 \pmod m \Rightarrow m \mid (a-1)$

$\{2, \pm m+2, \pm 2m+2, \dots\}$ — Классы вычетов по модулю "m"

$\dots$

$\overline{-1} = \overline{m-1} = \{m-1, 2m-1, -1, 3m-1, -m-1, \dots\}$

Кольцо классов вычетов по модулю "m"

$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}m$ $\quad$ $\overline{a}+\overline{b} = \overline{a+b}$, $\quad \overline{a}\cdot\overline{b} = \overline{ab}$ — По св-ву 4

Проверка аксиомы

$\overline{a}+\overline{0} = \overline{a+0} = \overline{a}$ $\Rightarrow$ Zm - Кольцо

Пример

$x^2 - 5y^2 = 3, \quad x, y \in \mathbb{Z}$

mod 5

$x^2 = 3 \pmod 5$

$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$

$$\left.\begin{array}{l} 0^2 = 0 \neq 3 \pmod 5 \\ 1^2 = 1 \neq 3 \pmod 5 \\ 2^2 = 4 \neq 3 \pmod 5 \\ 3^2 = 4 \neq 3 \pmod 5 \\ 4^2 = 1 \neq 3 \pmod 5 \end{array}\right\} \Rightarrow$$

Нет решений в целых числах

Сравнения 1-й степени

$ax = b \pmod m$

$a^{-1}ax = a^{-1}b \pmod m$?

$\mathbb{Z}_m \quad \bar{0}^{-1} \times$

$\mathbb{Z}_4 \quad \bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

$\bar{2}$ – делитель нуля

Теорема

$\mathbb{Z}_m, \quad \bar{a}$ – обратим $(\exists\, \bar{a}^{-1}) \Leftrightarrow (a, m) = 1$

▲ 1) $(a, m) = 1 \Rightarrow$ По алг. Евклида $\exists u, v: \; a \cdot u + mv = 1$

$\bar{a} \cdot \bar{u} = 1 \pmod m \Rightarrow \bar{u} = \bar{a}^{-1} \pmod m$

2) $(a, m) \neq 1 \Rightarrow \bar{a}$ – делитель нуля ▲

$\mathbb{Z}_m \quad \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1} \qquad -\frac{m}{2} \le \alpha \le \frac{m}{2}$

$\mathbb{Z}_7 \quad \boxed{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}}$

$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \overline{-3}, \overline{-2}, \overline{-1}$

$\boxed{\overline{-3}, \overline{-2}, \overline{-1}, \bar{0}, \bar{1}, \bar{2}, \bar{3}}$

Полная система вычетов

$\mathbb{Z}_m$ – обратимых элементов? $(a, m) = 1$

$\varphi(m)$ классов с обратимыми элементами

$\bar{1}, \ldots, \overline{m-1}$ – Приведённая система вычетов

Теорема Вильсона

If p – простое $\Rightarrow (p-1)! + 1 \equiv 0 \pmod p$

Теорема Эйлера

If $(a, m) = 1 \Rightarrow a^{\varphi(m)} = 1 \pmod m$

Малая теорема Ферма

p - простое $\Rightarrow a^{p-1} \equiv 1 \pmod p$

$ax \equiv b \pmod m$

Теорема

1) $(a, m) = 1 \Rightarrow$ 1 решение

2) $(a, m) = d$, $b \not\vdots\, d \Rightarrow$ нет решений

3) $(a, m) = d$, $b \,\vdots\, d \Rightarrow d$ решений

Способы решения $ax \equiv b \pmod m$:

1) $m \mid (ax - b) \Rightarrow ym = ax - b \Rightarrow ax - my = b$

Диафантово уравнение $\Rightarrow$ алгоритм Евклида

2) $45x \equiv 21 \pmod{132}$

$(45, 21) = (21, 45) = (21, 3) = (3, 0) = 3$ – НОД $(45, 21)$

$132 \,\vdots\, 3 \Rightarrow 3$ решения

$15x \equiv 7 \pmod{44}$

$15x \equiv (7 + 44) \pmod{44} \Rightarrow 15x \equiv 51 \pmod{44} \Big| \,\vdots\, 3 \Rightarrow 5 \equiv 17 \pmod{44}$

$5 \equiv 61 \pmod{44}$

$5 \equiv 105 \pmod{44} \Big| \,\vdots\, 5 \Rightarrow 1 \equiv 21 \pmod{44}$ – решение

$$\left[\begin{array}{l} x_1 \equiv 21 \pmod{132} \\ x_2 \equiv 65 \pmod{132} \\ x_3 \equiv 109 \pmod{132} \end{array}\right.$$

3) $x \equiv b a^{\varphi(m) - 1} \pmod m$ – формула Эйлера

$15x \equiv 7 \pmod{44}$

$x \equiv 7 \cdot 15^k \pmod{44} \Rightarrow$

$\varphi(44) = 44 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right) = 20 = k$

$44 = 2^2 \cdot 11$

$\Rightarrow x \equiv 7 \cdot 15^{19} \pmod{44} = 7 \cdot 5^9 \cdot 15 \pmod{44} = \ldots =$

и) Цепная дробь $a = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots}}}$

$a_0 = [a]$, $a_i > 0$

$a = [a_0; a_1, a_2, a_3, \dots]$

$$\frac{105}{29} = 3 + \frac{18}{29} = 3 + \cfrac{1}{\frac{29}{18}} = 3 + \cfrac{1}{1 + \frac{11}{18}} = \dots = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{3}}}}}$$

$[3; 1, 1, 1, 1, 3]$