Зад 1 $4x \equiv 3 \pmod 7$

$a=4 \quad b=3 \quad m=7$

$(4,7)=1 \Rightarrow$ ф-ма 1 решение

1 нач. Непосредствена проверка

$m=7$ (сам 0 ÷ 6)

$x=0 \quad 4.0=0 \not\equiv 3 \pmod 7$

$x=1 \quad 4.1=4 \not\equiv 3 \pmod 7$

$x=6 \quad 4.6 \equiv 3 \pmod 7$

Qmv $\Rightarrow$ $\boxed{x \equiv 6 \pmod 7}$

$\overline{6} \in \mathbb{Z}_7$

II нач. С елементарни преобразувания $\rightarrow$ чрез прибавяне на модула

$4x \equiv 3 \pmod 7$

$4x \equiv 3+7=10 \pmod 7$

$4x \equiv 10+7=17 \pmod 7$

$4x \equiv 17+7=24 \pmod 7$ $\quad | :4$, но $(4,7)=1$

$\boxed{x \equiv 6 \pmod 7}$

① $ka \equiv kb \pmod m \Rightarrow a \equiv b \pmod{\frac{m}{(m,k)}}$

② ако $(m,k)=1 \Rightarrow a \equiv b \pmod m$

III нач. Свеждане до диофантово уравнение

$ax+by=c \quad x,y \in \mathbb{Z}$

$d=(a,b) \quad d \mid c \Rightarrow$ има решение

(x_0, y_0) - един. решение

$$\begin{cases} x = x_0 + \frac{b}{d} k \\ y = y_0 - \frac{a}{d} k, \ k \in \mathbb{Z} \end{cases}$$

$4x \equiv 3 \pmod 7$

$4x = 7y + 3 \Rightarrow y \in \mathbb{Z}$

$4x - 7y = 3$ - диф. ур-е

$x = \frac{7y+3}{4} = \frac{4y+3y+3}{4}$

$x = y + 3\frac{y+1}{4}$ цяло ч.

$y_0 = 3$

$x_0 = 3 + 3\frac{3+1}{4} = 6$

$x = 6 - 7k, \ k \in \mathbb{Z} \Rightarrow x \equiv 6 \pmod 7$

$\mathbb{Z}_m$

$\overline{a} \in \mathbb{Z}_m$ е обратим $\Leftrightarrow (a, m) = 1$

$\Rightarrow \exists \overline{a}^{-1} \in \mathbb{Z}_m : \overline{a} \cdot \overline{a}^{-1} = \overline{1}$

$ax \equiv b \pmod m \ | \cdot a^{-1}$

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

$1 \cdot x \equiv a^{-1}b \pmod m$

$x_0 \equiv a^{-1}b \pmod m$

Пример. $a^{-1} = ?$

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

I/ нод $(a, m) = 1$

$\exists u, v : ua + vm = 1$

$a \cdot u = 1 - v \cdot m \Rightarrow a \cdot u \equiv 1 \pmod{m} \Rightarrow$

$\boxed{u = a^{-1}}$

II/ С използване на обратен елемент

$a = 4 \quad m = 7$

$7 = 4 \cdot 1 + 3 \Rightarrow 3 = 7 - 4 \cdot 1$

$4 = 3 \cdot 1 + 1$ - НОД $\Rightarrow 1 = 4 - 3 \cdot 1$

$3 = 1 \cdot 3 + 0$

$1 = 4 - 3 \cdot 1$

$1 = 4 - (7 - 4 \cdot 1) \cdot 1 \qquad 1 = 4 \cdot (7 - 4) - 2 \cdot 4 - 7$

$2 \cdot 4 + (-1) \cdot 7 = 1$

$u \qquad v$

$4^{-1} = 2$ обратен елемент

$4x \equiv 3 \pmod{7}$

$x \equiv 4^{-1} \cdot 3 \pmod{7}$

$\boxed{x \equiv 6 \pmod{7}}$

зад 1. Да се реши уравнението $12x \equiv 9 \pmod{15}$

$a = 12 \quad b = 9 \quad m = 15$

$(a, m) = 3 \quad 3 \mid 9 \Rightarrow$ имаме 3 решения

$12x \equiv 9 \pmod{15} \mid 3$

$4x \equiv 3 \pmod{5}$

$a_1 = 4 \quad b_1 = 3 \quad m_1 = 5$

$(a_1, m_1) = 1$

$4x \equiv 3 + 5 = 8 \pmod{5} : 4$

$\boxed{x \equiv 2 \pmod{5}} \quad \boxed{x \equiv 7 \pmod{5}} \quad \boxed{x \equiv 12 \pmod{5}}$

$\overline{2}, \overline{7}, \overline{12} \in \mathbb{Z}_{15}$

зад 2 $10x \equiv 25 \pmod{35}$

$a = 10 \quad b = 25 \quad m = 35$

$(a, m) = 5 \quad 5 \mid 25 \Rightarrow$ 5 решения

$10x \equiv 25 \pmod{35} : 5$

$2x \equiv 5 \pmod{7}$

$a = 2 \quad b = 5 \quad m = 7$

$(a, m) = 1$

$2x \equiv 12 \pmod 7$ | :2

$x \equiv 6 \pmod 7$

$x \equiv 13 \pmod 7$

$x \equiv 20 \pmod{35}$

$x \equiv 27 \pmod{35}$

$x \equiv 34 \pmod{35}$

Зад 3.

$39x \equiv 84 \pmod{93}$ | :3

$a = 39 \quad b = 84 \quad m = 93$

$(a, m) = 3 = d \quad d \mid 84 \Rightarrow$ 3 решения

$93 = 39 \cdot 2 + 15$

$39 = 15 \cdot 2 + 9$

$15 = 9 \cdot 1 + 6$

$9 = 6 \cdot 1 + 3$

$6 = 3 \cdot 2 + 0$

$13x \equiv 28 \pmod{31}$

$x_0 \equiv 13^{-1} \cdot 28 \pmod{31}$

$(13, 31) = \underline{1}$

$31 = 13 \cdot 2 + 5$

$13 = 5 \cdot 2 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$5 = 31 - 13 \cdot 2$

$3 = 13 - 5 \cdot 2$

$2 = 5 - 3 \cdot 1$

$1 = 3 - 2 \cdot 1$

$1 = 3 - 2 \cdot 1$

$1 = 3 - 1(5 - 3)$

$1 = 3 - 5 + 3$

$1 = 2 \cdot 3 - 5$

$1 = 2(13 - 5 \cdot 2) - 5$

$1 = 2 \cdot 13 - 4 \cdot 5 - 5$

$1 = 2 \cdot 13 - 5 \cdot 5$

$1 = 2 \cdot 13 - 5(31 - 13 \cdot 2)$

$1 = 2 \cdot 13 - 5 \cdot 31 + 10 \cdot 13$

$1 = \boxed{12} \cdot 13 - \boxed{5} \cdot 31$

$\boxed{12 = 13^{-1}}$

Omv

$13x \equiv 28 \pmod{31}$

$x \equiv 13^{-1} \cdot 28 \pmod{31}$

$x \equiv 12 \cdot 28 \pmod{31}$

$x \equiv 336 \pmod{31}$

$26, \quad 57, \quad 88 \in \mathbb{Z}_{93}$

B: $ag^k \quad 13x \equiv 7 \pmod{22}$

$a = 13 \quad b = 7 \quad m = 22$

$x_0 \equiv a^{-1} b \pmod{m}$

$a^{-1} \equiv a^{\varphi(22)-1} \pmod{m}$

$13^{-1} \equiv 13^{9} \pmod{22}$

$13^{2} = 169 \equiv 15 \pmod{22} \quad / \cdot 13$

$13^{3} \equiv 195 \equiv 19 \pmod{22}$

$13^{3} \equiv -3 \pmod{22} \quad / \cdot 13$

$$19^3 \equiv -27 \pmod{22} \equiv -5 \pmod{22}$$

$$13^7 \equiv -5 \pmod{22}$$

$$x_0 \equiv -5 \cdot 7 \pmod{22}$$

$$x_0 \equiv -35 \pmod{22} \equiv -13 \pmod{22}$$

$$\boxed{x_0 \equiv 9 \pmod{22}}$$