$a \equiv_m b \overset{def}{\Leftrightarrow} m \mid a-b \overset{def}{\Leftrightarrow} \exists y \in \mathbb{Z},\ a-b = m \cdot y$ $\quad \mathbb{Z}_6^* = \{1,5\}$ $\quad |\mathbb{Z}_6^*| = \phi(6) = \phi(2)\phi(3) = 1 \cdot 2 = 2$ $\quad \mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ $\quad \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid (a,m) = 1\}$ $\quad a \in \mathbb{Z}_m^* \Rightarrow \exists! a', \ a \cdot a' \equiv 1 \bmod m$

Inversul modular $a \cdot x \equiv 1 \bmod m \Leftrightarrow m \mid ax-1 \Rightarrow \exists y \in \mathbb{Z},\ ax-1 = my \Leftrightarrow ax - my = 1$ $\exists$ sol în $\mathbb{Z} \Leftrightarrow (a,m) \mid 1$

$4 \cdot \boxed{4} \equiv 1 \bmod 5$ $\quad 2 \cdot \boxed{3} \equiv 1 \bmod 6$ $\quad \boxed{\ } \cdot x \equiv \boxed{\ } \bmod m \ / \cdot x^{-1}$ $\quad x \cdot x^{-1} \equiv 1 \bmod m$ $\quad ax + by = c$ Ec. diofantiană

$|\mathbb{Z}_m^*|$

Funcția lui Euler $\phi(m) = |\mathbb{Z}_m^*|$

$\phi(1) = 1$

$\phi(p) = p-1$, $\forall p$ prim

$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, $(a,b) = 1$

$\phi(p^e) = p^e - p^{e-1}$

$\phi(6) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$.

$\phi(12) = \phi(2^2) \cdot \phi(3^1) = (2^2 - 2^1) \cdot (3^1 - 3^0) = 2 \cdot 6 = 12$

$\phi(m) = \phi(p_1^{e_1} \cdot \dots \cdot p_k^{e_k}) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k - 1})$ $\quad p_i \neq p_j \ \forall i \neq j$

I Alg. Euclid $\to (a,b)$

II $(a,b) \mid c \Rightarrow \exists$ sol în $\mathbb{Z}$

III comp. sol. în $\mathbb{Z}$

Ext. Euclid $d = (a,b) = \alpha a + \beta b$ $\quad \forall (\alpha, \beta)$

$x_0 = \alpha \cdot \frac{c}{(a,b)}$

Thm. Euler $m \geq 1$, $(a,m) = 1$ atunci $a^{\phi(m)} \equiv 1 \bmod m$

Corolar Fermat p prim, $p \nmid a$ $\quad a^{\phi(p)} \equiv 1 \bmod p$

Ecuații congruențiale $\overset{def}{\Leftrightarrow} m \mid ax-b \Rightarrow \exists y \in \mathbb{Z},\ ax - b = my$

$ax \equiv b \bmod m \to ax - my = b$, $\exists$ sol în $\mathbb{Z} \Leftrightarrow (a,m) \mid b \to x_0$

$\exists \#(a,m)$ soluții de forma $\left(x_0 + i \cdot \frac{m}{(a,m)}\right) \bmod m$

$(4,5,16) = 1$ $\quad 6, 16) = 2 \neq 1$

CRT $k \geq 1$, $m_1, \dots, m_k \geq 1$, $m = m_1 \cdot \dots \cdot m_k$, co-prime 2-2; $\forall b_1, \dots, b_k \in \mathbb{Z}$

$$(S) \begin{cases} x \equiv b_1 \bmod m_1 \\ \vdots \\ x \equiv b_k \bmod m_k \end{cases}$$

$c_i = \frac{m}{m_i}$; $\quad c_i x_i \equiv b_i \bmod m_i$ $\quad$ Obs. $(c_i, m_i) = 1 \Rightarrow \exists!$ sol

$x = \left(\sum_{i=1}^{k} c_i x_i\right) \bmod m$

(S) admite sol. unică în $\mathbb{Z}_m$

$c_i x_i - m_i y = b_i$ $\quad \#$ sol ?

$\Rightarrow (c_i, m_i) = 1$ $\quad 1 \mid b_i \Rightarrow \exists!$ în $\mathbb{Z}_{m_i}$

T: $\forall a,b,c \in \mathbb{Z}$, $a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c$

$m \mid a-c \Rightarrow a \equiv_m c$

$a \equiv_m b \Rightarrow m \mid a-b$ | $\Rightarrow m \mid \alpha(a-b)+\beta(b-c)$ ($\alpha, \beta = 1$)

$b \equiv_m c \Rightarrow m \mid b-c$ |

$m \mid a-b+b-c \Rightarrow m \mid a-c$

$m \mid x$ și $m \mid y \Rightarrow m \mid \alpha x + \beta y$

b) $a \equiv_m b$ și $c \equiv_m d \Rightarrow a+c \equiv_m b+d$

c) $ac \equiv_m bc$, $(m,c)=1 \Rightarrow a \equiv_m b$

Ex3 Calc. invers modular al lui a modulo m

a) $a=35$ $m=46$

b) $a=18$ $m=23$

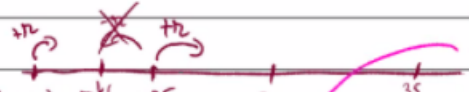
$ax \equiv 1 \mod m$ $\overset{def}{\Rightarrow} \dots \overset{def}{\Rightarrow} ax - my = 1$

$0 \le x < |b|$

$35x - 46y = 1$

$\alpha \cdot a + \beta \cdot b = (a,b)$ (35, -46)

$V_d = V_{(a,m)} = (\alpha, \beta)$



$35 = -46 \cdot 0 + 35$

$-46 = 35 \cdot (-2) + 24$

$35 = 24 \cdot 1 + 11$

$24 = 11 \cdot 2 + 2$

$11 = 2 \cdot 5 + 1$

$2 = 1 \cdot 2 + 0$

$V_{35} = (1,0)$ $V_{-46} = (0,1)$

$V_{24} = V_{-46} - (-2)V_{35} = (0,1) - (-2)\cdot(1,0) = (0,1) - (-2,0) = (2,1)$

$V_{11} = V_{35} - 1 \cdot V_{24} = (1,0) - (2,1) = (-1,-1)$

$V_2 = V_{24} - 2 \cdot V_{11} = (2,1) - 2 \cdot (-1,-1) = (4,3)$

$V_1 = V_{11} - 5 \cdot V_2 = (-1,-1) - 5(4,3) = (-21,-16)$

$-46 = 35 \cdot (-2) + 24$

$z = x + y$

$y = z - x$

$24 = -46 - 35 \cdot (-2)$

$875 : 46 = 19, \dots$

$875 - 46 \cdot 19 =$ [redacted]

$x = \alpha \cdot \frac{c}{(a,b)} = \alpha \cdot \frac{1}{(a,m)} \to (-21) \cdot \frac{1}{1} = -21$

! Atenție !

Vf: $35 \cdot 25 = 875 \mod 46 \equiv 1$ ✓

$x = a^{-1} = -21 \mod 46 = \boxed{25}$

Ex 4 Ecuații congruențiale (toate soluțiile din $\mathbb{Z}_m$) — $\#(a,m)$

a) $18x \equiv 12 \bmod 42$

b) $14x \equiv 6 \bmod 18$

a) $18x \equiv 12 \bmod 42$ — I ec. dif.: $\overset{a}{18}x - \overset{b}{42}y = \overset{c}{12}$ — $x = \alpha \cdot \frac{c}{(a,b)}$

$42 \mid 18x - 12 \Rightarrow 18x - 12 = 42y$

$18 = (-42)\cdot 0 + 18$ — $V_{18} = (1,0)$ $V_{-42} = (0,1)$

$-42 = 18 \cdot (-3) + 12$ — $V_{12} = V_{-42} - (-3)V_{18} = (3,1)$

$18 = 12 \cdot 1 + \boxed{6}$ — $V_6 = V_{18} - 1 \cdot V_{12} = (-2,-1)$ (α, β)

$12 = 6 \cdot 2 + 0$ — $V_f: (-2)\cdot 18 + (-1)\cdot(-42) = 6$ ✓

$a \equiv b \bmod m$ ⇔ $a \underset{m}{\equiv} b$ ⇔ $m \mid a-b$ (def) ⇓ $m \mid x$ ⇓ $\exists y \in \mathbb{Z}$, $x = m \cdot y$

$(18,-42) = 6 \Rightarrow$ 6 sol în $\mathbb{Z}_{42}$ — $\alpha = -2$

$x_0 = \alpha \cdot \frac{c}{(a,m)} = (-2)\cdot\frac{12}{6} = -4$ — $\beta = -1$

$x_1 = x_0 + i \cdot \frac{m}{(a,m)} = -4 + 1 \cdot \frac{42}{6} = 3$

$x_2 = -4 + 2\cdot 7 = 10 \bmod 42$

$x_3 = -4 + 3\cdot 7 = 17 \bmod 42$

$x_4 = -4 + 4\cdot 7 = 24 \bmod 42$

$x_5 = -4 + 5\cdot 7 = 31 \bmod 42$

6 sol. în $\mathbb{Z}_{42}$! $x \in \{3, 10, 18, 24, 31, 38\}$

$x_0 = -4 \bmod 42 = 38$

$\boxed{ax \equiv c \bmod b} \longrightarrow ax - by = c$

Ex 5

(S) $\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$

$c_1 = 5\cdot 7$ — $35x_1 \equiv 2 \bmod 3$ — $35x_1 - 3y_1 = 2$ — $x_1 = 1$

$c_2 = \frac{3\cdot 5\cdot 7}{5}$ — $21x_2 \equiv 3 \bmod 5$ — $21x_2 - 5y_2 = 3$ — $x_2 = 3$

$c_3 = \frac{3\cdot 5\cdot 7}{7}$ — $15x_3 \equiv 1 \bmod 7$ — $15x_3 - 7y_3 = 1$ — $x_3 = 1$

I Vf. coprimi 2-2 ✓

II Aducem ec. din (S) la forma ec. congr., apoi la forma ec. diof. $\Rightarrow x_i$

III $x = (c_1x_1 + c_2x_2 + c_3x_3) \bmod 105$

$= (35\cdot 1 + 21\cdot 3 + 15\cdot 1) \bmod 105$

$x = 8 \bmod 105$

Vf.