Ex.

1. Dacă există permutări de ordin 50 în grupul de permutări S_{14} trebuie ca $50 \mid 14!$

$14! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 =$

$= 2 \cdot 3 \cdot 4 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 50 \; \vdots \; 50 \Rightarrow$

$\Rightarrow 50 \mid 14! \Rightarrow \exists$ permutări de ordin 50 în S_{14}

2. $\sigma = (1 \dots 7)(8, \dots 14)$

$\tau = ?$ a.î. $\tau^2 = \sigma$

$\tau^2 = (1 \dots 7)(8 \dots 14)$

Pp că $(\exists)\ \tau \in S_{14}$ a.î. $\tau^2 = \sigma$ Fie $\tau = c_{i_1} \cdot c_{i_2} \cdot \dots \cdot c_{i_k}$ → desc. lui în produs de cicli disjuncți $1 \le k \le 14$

(dc $k = 14 \Rightarrow \tau = e$ ~~id~~)

$\tau^2 = \sigma = (1 \dots 7)(8 \dots 14) \Longrightarrow$

$\tau^2 = c_{i_1}^2 \cdot c_{i_2}^2 \cdot \dots \cdot c_{i_k}^2$

Prin urmare $c_{i_j}^2$ e un ciclu de lungime i_j $\forall j = \overline{1,k} \Rightarrow$

$\Rightarrow k = 2$ și pot pp că $i_1 = 7$ $i_2 = 7$ deci $\tau = c_{i_1} c_{i_2}$

Deci $\tau^2 = c_{i_1}^2 \cdot c_{i_2}^2$ $\qquad c_{i_1}^2 = (1 \dots 7) = (1\,5\,2\,6\,3\,7\,4)$

$c_{i_2}^2 = (8 \dots 14) = (8\,12\,9\,13\,10\,14\,11)$

$(c_{i_1}^2)^4 = (1\,2\,3\,4\,5\,6\,7)^4 = (1\,5\,2\,6\,3\,7\,4)$ $\quad \tau = (1\,5\,2\,6\,3\,7\,4)(8\,12\,9\,13\,10\,14\,11)$

$\Rightarrow k=1$ pot pp că $i_1 = 14$ $\tau = c_{i_1}$

$\tau^2 = c_{i_1}^2$

$\tau^2 = (1\,2\,3\,4\,5\,6\,7)(8\,9\,10\,11\,12\,13\,14)$

$\tau^2 = (1\,2\,3\,4\,5\,6\,\cancel{7})(\cancel{8}\,9\,10\,11\,12\,13\,14)$

9 10 11 12 13 14 8
10 11 12 13 14 8 9
11 12 13 14 8 9 10
12 13 14 8 9 10 11
13 14 8 9 10 11 12
14 8 9 10 4 12 13

$\tau = (1\,8\,2\,9\,3\,10\,4\,11\,5\,12\,6\,13\,7\,14)$

1 9 2 10 3 11 4 12 5 13 6 14 7 8
1 10 2 11 3 12 4 13 5 14 6 8 7 9
1 11 2 12 3 13 4 14 5 8 6 9 7 10
1 12 2 13 3 14 4 8 5 9 6 10 7 11
1 13 2 14 3 8 4 9 5 10 6 11 7 12
1 14 2 8 3 9 4 10 5 11 6 12 7 13

3) $7^{7^{17^{17}}} \pmod{29}$

29 prim $\overset{\text{Fermat}}{\Rightarrow} 7^{28} \equiv 1 \pmod{29}$

Pt a calcula $7^{7^{17^{17}}} \pmod{29}$ e suficient să calculez

$7^{17^{17}} \pmod{28}$

$(7, 28) \neq 1.$

$7^1 = 7 \pmod{28}$

$7^2 = 21 \pmod{28} = -7 \pmod{28}$

$7^3 = (-7) \cdot 7 = -49 \pmod{28} = -21 \pmod{28} = 7$

$7^{2k+1} \equiv 7 \pmod{28}$

($\Leftrightarrow$ sau ultima cifră)

Trebuie să calculăm $14^{14} \pmod{2}$ $\quad 17^2 \equiv 1 \pmod{2}$

$17^{17} \pmod{2} = 17^{16+1} = 17^{2 \cdot 8} \cdot 17 \pmod{2} = 14 \pmod{2} =$

$\equiv 1 \pmod{2}$

$7^{17^{17}} \pmod{28} \equiv 7^1 \pmod{28} = 7 \pmod{28}$

$7^{7^{17^{14}}} \pmod{29} \equiv 7^7 \pmod{29} \equiv (7^2)^3 \cdot 7 \pmod{29} \equiv$

$\equiv (343)^2 \cdot 7 \pmod{29} \equiv 24^2 \cdot 7 \pmod{29} \equiv$

$\equiv 576 \cdot 7 \pmod{29} \equiv 25 \cdot 7 \pmod{29} \equiv -4 \cdot 7 \pmod{29} \equiv$

$\equiv -28 \pmod{29} \equiv 1 \pmod{29}$

4.) Numărul elementelor de ordin 24 din $(\mathbb{Z}_{2^7},+)\times(\mathbb{Z}_{3^7},+)$

$$\{(\hat{k},\bar{l})\in\mathbb{Z}_{2^7}\times\mathbb{Z}_{3^7} \mid ord(\hat{k},\bar{l})=24\}$$

$$ord((\hat{k},\bar{l}))=[ord(\hat{k}), ord(\bar{l})]=24 \Rightarrow$$

$$\quad m \qquad\quad n$$

$[m,n]=24 \Rightarrow (m,n)=\{(1,24),(24,1),(3,8),\underline{(8,3)},(4,6),(6,4),(2,12),(12,2)\}$

Lagrange $ord(\hat{k}) \mid 2^7 \Rightarrow ord(\hat{k})=8$

$ord(\bar{l}) \mid 3^7 \Rightarrow ord(\bar{l})=3$

~~$\Rightarrow$ Nu există elem de ordin 24 în $(\mathbb{Z}_{2^7},+)\times(\mathbb{Z}_{3^7},+)$~~

$$ord(\hat{k})=\frac{2^7}{(2^7,k)} \Rightarrow 8=\frac{2^7}{(2^7,k)} \Rightarrow (2^7,k)=2^4$$

$$k=\{2^4, 2^4\cdot 3, 2^4\cdot 5, 2^4\cdot 7\}$$

$$ord(\bar{l})=3 \Rightarrow \frac{3^7}{(3^7,l)}=3 \Rightarrow (3^7,l)=3^6$$

$$l=\{3^6, 3^6\cdot 2\}$$

$4\times 2=8$ elemente

8. $\begin{cases} n \equiv 3 \pmod{5} \\ n \equiv 2 \pmod{7} \\ n \equiv 8 \pmod{9} \end{cases}$

Not $a_1 = 3$, $a_2 = 2$ $a_3 = 8$

$m_1 = 5$, $m_2 = 7$, $m_3 = 9$

Obs că $(m_1, m_2) = (m_1, m_3) = (m_2, m_3) = 1$

$M = 5 \cdot 7 \cdot 9$

$M_1 = \frac{M}{m_1} = 7 \cdot 9$

$M_2 = \frac{M}{m_2} = 5 \cdot 9$

$M_3 = \frac{M}{m_3} = 5 \cdot 7$

$M_1 x_1 \equiv 1 \pmod{m_1} \rightarrow 63 x_1 \equiv 1 \pmod{5} \rightarrow$

$M_2 x_2 \equiv 1 \pmod{m_2} \rightarrow 45 x_2 \equiv 1 \pmod{7} \rightarrow$

$M_3 x_3 \equiv 1 \pmod{m_3} \rightarrow 35 x_3 \equiv 1 \pmod{9} \rightarrow$

$\rightarrow 3 x_1 \equiv 1 \pmod{5} \rightarrow x_1 \equiv 2 \pmod{5}$

$\rightarrow 3 x_2 \equiv 1 \pmod{7} \,|\, 5 \rightarrow x_2 \equiv 5 \pmod{7}$

$\rightarrow 8 x_3 \equiv 1 \pmod{9} \rightarrow x_3 \equiv 8 \pmod{9}$

Soluția unică modulo $M = 315$ este $x \pmod{M}$

unde $x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 =$

$= 3 \cdot 63 \cdot 2 + 2 \cdot 45 \cdot 5 + 8 \cdot 35 \cdot 8 = 3068$

$3668 \pmod{315} \equiv 233 \ (315)$ Unica sol a sistemului mod 315 este 233

$a \cdot b+1$

1. Există permutări de ordin 37 în grupul permutărilor S_{13}

~~37~~ Ca să existe permutări de ordin 37 în S_{13} trebuie ca $37 \mid 13!$

dar $37 \nmid 13! \Rightarrow$ nu există permutări de ordin 37 în S_{13}

$a \cdot b-1$

2. Există permutări de ordin 35 în grupul S_{13}

Ca să $\exists$ permutări de ordin 35 în S_{13} trebuie ca $35 \mid 13!$

$$13! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 =$$

$$= 35 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \vdots 35$$

$35 \mid 13! \Rightarrow \exists$ perm de ord. 35 în S_{13}

3. Să se det. nr de permutări de ordin 4 din S_9

-> 1 ciclu de lungime 4

$$\frac{A_9^4}{4} = \frac{9!}{5!\,4} = \frac{6\cdot 7\cdot \cancel{8}^{2}\cdot 9}{\cancel{4}} = 12\cdot 7\cdot 9 = 756$$

-> 2 cicli de lungime 4

$$\frac{C_9^4\cdot C_5^4}{2} = \frac{\frac{\cancel{6}^{3}\cdot 7\cdot \cancel{8}^{2}\cdot 9}{\cancel{2}\cdot\cancel{3}\cdot\cancel{4}}\cdot\frac{5!}{4!}}{2} = \frac{\cancel{126}^{63}\cdot 5}{\cancel{2}} = 315$$

$756 + 315 = 1071$ permutări de ordin 4 în S_9

$n = \overline{abcd}$

- Se consideră permutarea

$\sigma = (1 \ldots 4)(5 \ldots 13)$ 4, 9 din S_{13}

$\tau \in S_{13}$ $\tau = ?$

$\tau^{11} = \sigma$

Pp că $(\exists)\, \tau \in S_{13}$ a.î. $\tau^{11} = \sigma$

Fie $\tau = c_{i_1} \cdot c_{i_2} \cdot \ldots \cdot c_{i_k}$ → descompunerea lui τ în prod de cicli disjuncți

$i_1 + i_2 + \ldots + i_k = 13$ $1 \le k \le 13$ $(k = 13 \Rightarrow \tau = e \ \text{\&})$

$\tau^{11} = c_{i_1}^{11} \cdot c_{i_2}^{11} \cdot \ldots \cdot c_{i_k}^{11}$

$\tau^{11} \overset{(\alpha)}{=} \sigma = (1 \ldots 4)(5 \ldots 13) \underset{\substack{\text{unicitatea} \\ \text{desc. în} \\ \text{prod de cicli} \\ \text{disjuncți}}}{\Rightarrow} 11 \nmid i_j \quad \forall j = \overline{1,k}$

Prin urmare $c_{i_j}^{11}$ e un ciclu de lungime i_j

$\overset{(\alpha)}{\Rightarrow} k = 2$ și pot pp. că $i_1 = 4$ și $i_2 = 9$ deci $\tau = c_4 \cdot c_9$

$\tau^{11} = c_4^{11} \cdot c_9^{11}$ cu $c_4^{11} = (1\,2\,3\,4)$

$c_9^{11} = (\cancel{5}\,6\,7\,8\,9\,10\,11\,12\,13)$

$(c_4^{11})^{\cancel{7}} = (1\,2\,3\,4)^{7}$

$c_4^{55} = (1\,2\,3\,4)^{7}$

$(c_4^{4})^{18} \cdot c_4 = c_4$

$\Rightarrow c_4 = (1\,2\,3\,4)^{7} = (1\,2\,3\,4)^{3} = (1\,4\,3\,2)$

$(C_9^{11})^5 = (5\,6\,7\,8\,9\,10\,11\,12\,13)^5 \Rightarrow C_9 = (5\,6\,7\,8\,9\,10\,11\,12\,13)^5$

$C_9 = (5\,10\,6\,11\,7\,12\,8\,13\,9)$

$\tau = (1\,4\,3\,2)(5\,10\,6\,11\,7\,12\,8\,13\,9)$

! Se consideră permutarea

- $\sigma = (1 \ldots 9)(10 \ldots 13)$

  $\tau = ?$

  $\tau^2 = \sigma$

  $sgn(\sigma) = (-1)^{9-1}(-1)^{4-1} = -1$ $\Big| \Rightarrow$ nu are sol.

- $\sigma = (1 \ldots 4)(5 \ldots 13)$

  $\tau = ?$

  $\tau^3 = \sigma$

Pp $\exists$ că $\exists\ \tau \in S_{13}$ a.î. $\tau^3 = \sigma$

Fie $\tau = c_{i_1} \cdot c_{i_2} \cdot \ldots \cdot c_{i_k}$ → desc. a lui în prod de ciclii disjuncți

$\tau^3 = c_{i_1}^3 \cdot c_{i_2}^3 \cdot c_{i_3}^3 \cdot \ldots \cdot c_{i_k}^3$

$3 | 9 \Rightarrow c_9^3$ = prod de 3 ciclii disj de lungime $9/3 = 3$

$ord(\sigma) = [4,9] = 36$

$ord(\tau) = m = [e_1, c_2 \dots c_k]$

$ord(\tau^3) = \frac{m}{(m,3)} = 36 \Rightarrow m = 36(m,3)$

$3 | m$

$(m,3) = 3$ $\Rightarrow m = 36 \cdot 3 = 108$

$ord(\tau) = [c_1, c_2 \dots c_k] = 108 \Rightarrow$ cel puțin un $l_i = 108$

$\tau = C_1, l_1 = 108 > 13 \Rightarrow$ Nu există ciclu de lungime 108 în S_{13}

deci nu exista soluții

sau un $l_i = 4$

$l_j = 27 > 13 \Rightarrow \nexists$ ciclicle lung 27

n impar $n = \overline{abcd}$

$\cancel{x} \equiv 4 \pmod{11}$

$\cancel{x} \equiv 9 \pmod{13}$

Notăm $a_1 = 4$, $a_2 = 9$

$m_1 = 11$, $m_2 = 13$

Obs că $(m_1, m_2) = 1$

$M = 11 \cdot 13$

$M_1 = \frac{M}{m_1} = 13$

$M_2 = \frac{M}{m_2} = 11$

$\begin{cases} M_1 x_1 \equiv 1 \pmod{11} \\ M_2 x_2 \equiv 1 \pmod{13} \end{cases} \Rightarrow \begin{cases} 13 x_1 \equiv 1 \pmod{11} \\ 11 x_2 \equiv 1 \pmod{13} \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} 2 x_1 \equiv 1 \pmod{11} \\ -2 x_2 \equiv 1 \pmod{13} \end{cases} \Rightarrow \begin{cases} x_1 \equiv 6 \pmod{11} \\ x_2 \equiv 6 \pmod{13} \end{cases}$

soluția unică ~~mod~~ $143 = M$ este $x \pmod{M}$

$x = 4 \cdot 13 \cdot 6 + 9 \cdot 11 \cdot 6 = 6(52 + 99) = 6$

$906 \pmod{143} \equiv 48 \pmod{143}$

$n = 7 \cdot 143 + 48 = 1001 + 48 = 1049.$

5. a) Det nr elem. de ord 24 din grupul de produs direct $(\mathbb{Z}_{2^4}, +) \times (\mathbb{Z}_{3^9}, +)$

b) - de ord 6 din gr produs direct $(\mathbb{Z}_{3^4}, +) \times (\mathbb{Z}_{6^9}, +)$

c) - de ordin 8 din gr produs direct $(\mathbb{Z}_{2^4}, +) \times (\mathbb{Z}_{2^9}, +)$ - dat '21

a) $\{(\hat{k}, \bar{l}) \in \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^9} \mid ord((\hat{k}, \bar{e})) = 24\}$

$ord((\hat{k}, \bar{e})) = [ord(\hat{k}), ord(\bar{e})] = 24$

$(ord(\hat{k}), ord(\bar{e})) \in \{(1,24), (24,1), (4,6), (6,4), (8,3)(3,8), (2,12)$
$(12,2)\}$

dar din Lagrange $\Rightarrow ord(\hat{k}) \mid 2^4$
$ord(\hat{e}) \mid 3^9$

$\Rightarrow$

$\Rightarrow (ord(\hat{k}), ord(\bar{e})) \in \{(8,3)\}$

$ord(\hat{k}) = 8 \Rightarrow ord(\hat{k}) = \frac{2^4}{(2^4, k)} \Rightarrow \frac{16}{(16,k)} = 8 \Rightarrow$

~~$ord(\bar{l}) = 3$~~

$\Rightarrow (16, k) = 2 \underset{k<16}{\overset{16=2^4}{\Longrightarrow}} k = \{2, 2\cdot3, 2\cdot5, 2\cdot7\}$

$\Rightarrow k = \{2, 6, 10, 14\}$

$ord(\bar{l}) = 3 \Rightarrow ord(\bar{e}) = \frac{3^9}{(3^9, l)} \Rightarrow \frac{3^9}{(3^9, l)} = 3 \Rightarrow (3^9, l) = 3^8$

$\Rightarrow l = \{3^8, 3^8\cdot2\}$

Deci există $2 \times 4 = 8$ elm de ordin 24 în $(\mathbb{Z}_{2^4}, +) \times (\mathbb{Z}_{3^9}, +)$

b) $\{(\hat{k}, \bar{l}) \in \mathbb{Z}_{3^4} \times \mathbb{Z}_{6^9} \mid ord((\hat{k}, \bar{l})) = 6\}$

$ord((\hat{k}, \bar{e})) = [ord(\hat{k}), ord(\bar{l})] = 6$

$(ord(\hat{k}), ord(\bar{e})) = \{(1,6), (2,3), (3,2), (6,1)\}$

din Lagrange $ord(\hat{k}) \mid 3^4$

$ord(\bar{e}) \mid 6^9$

$(ord(\hat{k}), ord(\bar{e})) = \{(1,6), (3,2)\}$ $\Rightarrow$

Caz 1:

$ord(\hat{k}) = 1 \Rightarrow \hat{k} = \hat{0}$ în $\mathbb{Z}_{3^4}$

$ord(\bar{e}) = 6 \Rightarrow \frac{6^9}{(6^9, l)} = 6 \Rightarrow (6^9, l) = 6^8$

$l = \{6^8, 6^8 \cdot 2, 6^8 \cdot 3, 6^8 \cdot 4, 6^8 \cdot 5\}$

6 elem de ord 6

Caz 2

$ord(\hat{k}) = 3 \Rightarrow \cancel{ord(\hat{k})} = \frac{3^4}{(3^4, k)} = 3 \Rightarrow (3^4, k) = 3^3 \Rightarrow$

$\Rightarrow k \in \{3^3, 3^3 \cdot 2\}$

$ord(\bar{l}) = 2 \Rightarrow \frac{6^9}{(6^9, k)} = 2$

$(6^9, k) = 2^8 \cdot 3^9$

$k = \{2^8 \cdot 3^9\}$

$2 \times 1 = 2$ elm

Deci avem în total 8 elem

c) $\{(\hat{k},\bar{\ell}) \in \mathbb{Z}_{2^4} \times \mathbb{Z}_{2^9} \mid \text{ord}((\hat{k},\bar{\ell})) = 8\}$

$\text{ord}((\hat{k},\bar{\ell})) = [\text{ord}(\hat{k}), \text{ord}(\bar{\ell})] = 8$

$(\text{ord}(\hat{k}), \text{ord}(\bar{\ell})) = \{(1,8),(2,4),(4,2),(8,1)\}$

din Lagrange $\text{ord}(\hat{k}) \mid 2^4$
$\text{ord}(\bar{\ell}) \mid 2^9$

$\Rightarrow (\text{ord}(\hat{k}), \text{ord}(\bar{\ell})) = \{(1,8),(2,4),(4,2),(8,1)\}$

- Caz 1

$\text{ord}(\hat{k}) = 1 \Rightarrow \hat{k} = \hat{0}$ în $\mathbb{Z}_{2^4}$

$\text{ord}(\bar{\ell}) = 8 \Rightarrow \frac{2^9}{(2^9,\ell)} = 8 \Rightarrow (2^9,\ell) = 2^6$

$\ell = \{2^6, 2^6\cdot 3, 2^6 \cdot 5, 2^6 \cdot 7\}$

$\boxed{4 \text{ elem}}$

- Caz 2

$\text{ord}(\hat{k}) = 8 \Rightarrow \frac{2^4}{(2^4,k)} = 2^3 \Rightarrow (2^4,k) = 2 \Rightarrow k = \{2, 2\cdot 3, 2\cdot 5, 2\cdot 7\}$

$\text{ord}(\bar{\ell}) = 1 \Rightarrow \bar{\ell} = 0$ în $\mathbb{Z}_{2^9}$

$\boxed{4 \text{ elm}}$

Caz 3

$\text{ord}(\hat{k}) = 2 \Rightarrow \frac{2^4}{(2^4,k)} = 2 \Rightarrow 2^3 = (2^4,k) \Rightarrow k = \{2^3\}$

$\text{ord}(\bar{\ell}) = 4 \Rightarrow \frac{2^9}{(2^9,\ell)} = 4 \Rightarrow (2^9,\ell) = 2^7 \Rightarrow$

$\Rightarrow \ell = \{2^7, 2^7 \cdot 3\}$

$\boxed{2 \text{ elem}}$

Caz 4

$\operatorname{ord}(\hat{k}) = 4 \Rightarrow \dfrac{2^4}{(2^4, k)} = 4 \Rightarrow 2^2 = (2^4, k) \Rightarrow k = \{2^2, 2^2 \cdot 3\}$

$\operatorname{ord}(\hat{l}) = 2 \Rightarrow \dfrac{2^9}{(2^9, l)} = 2 \Rightarrow 2^8 = (2^9, l) \Rightarrow$

$\Rightarrow l = \{2^8\}$

2 elem

$4 + 4 + 2 + 2 = 12$ elem de ordin 8