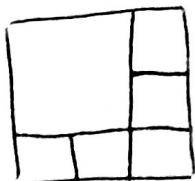


Algebra I

Multimi, funcții

Inducție:

①



pathat

$$m = 6$$

$P(m)$

$m \geq 6, m \in \mathbb{N}$, există o
parte „particulară” în m patrate.
„pava”

Inducție în pasul 3

$P(m)$ adevărată $\Rightarrow P(m+3)$ adevărată

② Arătăm că, $\forall m \in \mathbb{N}, m \geq 3 \exists a_1 < a_2 < \dots < a_m$

numere naturale a_i încât $\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_m} = 1$

DP ext m=3 $\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} = 1$

$a_3 \in \mathbb{N}^* \quad \forall j = \overline{1, 3}$

simultane cu $\frac{1}{2} \Rightarrow \frac{1}{2a_1} + \frac{1}{2a_2} + \dots + \frac{1}{2a_m} = \frac{1}{2}$

$\frac{1}{2} + \frac{1}{2a_1} + \frac{1}{2a_2} + \dots + \frac{1}{2a_m} = \frac{1}{2} + \frac{1}{2} = 1$

$2 < 2a_1 < 2a_2 < \dots < 2a_m$ deoarece $a_i \neq 1$.

Dacă $a_1 = 1 \quad x + \frac{1}{a_2} + \dots + \frac{1}{a_m} = x \quad$ Am demonstrat că
 $P(m) \Rightarrow P(m+1)$

$$\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} = 1 < \frac{3}{a_1} \Rightarrow 1 < a_1 < 3 \Rightarrow a_1 = 2$$

$$\frac{1}{2} = \frac{1}{a_2} + \frac{1}{a_3} < 2 \cdot \frac{1}{a_2} \Rightarrow 2 < a_2 < 4 \Rightarrow a_2 = 3$$

$$\frac{1}{a_3} = \frac{1}{2} - \frac{1}{a_2} = \frac{1}{2} - \frac{1}{3} = \frac{1}{6} \Rightarrow a_3 = 6$$

Exercitiu:

Anătați că:

$$1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4} \quad \forall n \in \mathbb{N}^*$$

Verificare:

$$n=1 \Rightarrow 1^3 = \frac{1^2 \cdot 2^2}{4} \Rightarrow 1=1 \quad A.$$

Presupunem enunțul adevărat pt n și demonstrăm pt $n+1$.

$$1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$$

$$\underbrace{1^3 + 2^3 + \dots + n^3}_{= \frac{(n+1)^2(n+2)^2}{4}} + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 \stackrel{?}{=} \text{egalitatea trebuie verificată}$$

$$\frac{n^2}{4} + (n+1) = \frac{(n+2)^2}{4}$$

$$n^2 + 4(n+1) = (n+2)^2$$

$$n^2 + 4n + 4 = n^2 + 4n + 4$$

$$(a+b)^2 = a^2 + b^2 + 2ab$$

Mica teorema a lui Fermat.

Dacă p prim, $a \in \mathbb{Z}$ atunci $p \mid a^p - a$

Pt $p=2 \Rightarrow 2 \mid a^2 - a = \underbrace{a(a-1)}_{2\text{ numere consecutive}}$

Pt $p \geq 3 \mid p$ impar
 p prim

Dacă p impar $a^p - a = [(-a)^p - (-a)] \cdot (-1)$

E suficient să demonstrezi enunțul pt p prim, $p \geq 3$
în $a \in \mathbb{N}$.

Veificare

$$a=0 \quad p \mid 0^p - 0 = 0$$

$$a=1 \quad p \mid 1^p - 1 = 0$$

Presupun că $p \mid a^p - a$ înseanță arăt că $p \mid (a+1)^p - (a+1)$

$$\begin{aligned} (a+1)^p - (a+1) &= \\ &= a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots + \\ &+ C_p^{p-1} a + 1 \\ &= (\underbrace{a^p - a}) + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \dots \\ &+ C_p^{p-1} a \end{aligned}$$

$\xrightarrow{\text{p.n (către ipoteza de inducție)}}$

Falosim formula
binomului lui Hextan.

$$(a+b)^m = a^m + C_m^1 a^{m-1} b + C_m^2 a^{m-2} b^2 + \dots + C_m^{m-1} a^{m-1} b^{m-1} + b^m$$

E+:

$$\text{pt } p=5 \quad C_5^1 = 5$$

$$C_5^2 = \frac{5!}{2! \cdot 3!} = 10$$

$$C_5^3 = 10$$

$$C_5^4 = 5$$

Dacă pot arăta că $p | C_p \quad \forall 1 \leq j \leq p-1$ atunci pasul de inducție este demonstrat.

$$C_p^j \in \mathbb{H} \quad 1 \leq j \leq p-1$$

$$C_p^j = \frac{p!}{(p-j)! \cdot j!} = \frac{(p-j+1)(p-j+2) \cdots (p-1)p}{1 \cdot 2 \cdot 3 \cdots j}$$

Deoarece $1 \leq j \leq p-1 \Rightarrow p$ nu divide $j!$ ($p \nmid j!$)

Deoarece $j \geq 1 \Rightarrow p-j+1 \leq p-1+1=p$

$\Rightarrow p | C_p^j$ pt orice $1 \leq j \leq p-1$

Dacă A mulțime finită, vom nota $|A|$ = cardinalul mulțimii A (câtă elemente are mulțimea A).

$$|A \cup B| = |A| + |B| - |A \cap B| \quad A \text{ și } B \text{ mulțimi finite}$$

$$A = \{a_1, a_2, \dots, a_m, c_1, c_2, \dots, c_k\}$$

$$B = \{b_1, b_2, \dots, b_n, c_1, c_2, \dots, c_k\}$$

$$A \cap B = \{c_1, c_2, \dots, c_k\}$$

$$C_m^k = \frac{m!}{k!(m-k)!}$$

$$a_i \neq a_j \quad a_i \neq c_j \quad a_i \neq b_j$$

$$b_i \neq b_j \quad b_i \neq c_j$$

$$A \cup B = \{a_1, \dots, a_n, b_1, \dots, b_m, c_1, \dots, c_k\}$$

$$|A \cup B| = n + m + k$$

$$|A| + |B| - |A \cap B| = (n+k) + (m+k) - k = \\ = n + m + k = |A \cup B|$$

Problema:

$$\text{Avem multimea } A = \{m \in \mathbb{N} \mid m \leq 2018, (m, 10) = ?\}$$

Găsiți cardinalul mulțimii.

$$|A| = ?$$

$$\text{O să consider } B = \{m \in \mathbb{N} \mid m \leq 2018, 2 \mid m\} \\ C = \{m \in \mathbb{N} \mid m \leq 2018, 5 \mid m\}$$

$$A \cup B \cup C = ?$$

$$A \cap B = \emptyset$$

$$A \cap C = \emptyset$$

$$B \cap C = \{m \in \mathbb{N} \mid m \leq 2018, \\ 10 \mid m\}$$

$$A \cup B \cup C = \{0, 1, 2, \dots, \\ \dots, 2018\}$$

Obs: Fătăm $a, b \in \mathbb{N}$, nu
ambale 0.

$(a, b) =$ cel mai mare divizor
 comun al numerelor a, b

$(1000, 325) =$ care este c.m.m.d.c?

Descompun
(factori primi) $1000 = 2^3 \cdot 5^3 \Rightarrow$ c.m.m.d.c
 $325 = 13 \cdot 5^2$ este 5^2

Formule de distributivitate.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

În cazul nostru:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) = \emptyset \cup \emptyset = \emptyset$$

$$2019 = |A \cup (B \cup C)| = |A| + |B \cup C| - \underbrace{|A \cap (B \cup C)|}_{\emptyset \Rightarrow \text{cardinalul multimii este } 0}$$

$$|A| = 2019 - |B \cup C|$$

$$|B \cup C| = |B| + |C| - |B \cap C|$$

$$|B| = \frac{2018}{2} + 1 = 1010$$

$$B = \{0, 2, 4, 6, \dots, 2018\}$$

$$|C| = \frac{2015}{5} + 1 = 403$$

$$C = \{0, 5, 10, \dots, 2015\}$$

impărțire la 5 0,1 $\frac{1}{5} \times 403 = 404$

$$|B \cap C| = \frac{2010}{10} + 1 = 202 \quad B \cap C = \{0, 10, 20, \dots, 2010\}$$

$$\Rightarrow |B \cup C| = 1010 + 403 - 202 = 1211$$

$$\Rightarrow 2019 = |A \cup (B \cup C)| = |A| + |B \cup C|$$

$$\Rightarrow |A| = 2019 - |B \cup C| = 2019 - 1211 = 808$$

Dacă A, B, C finite

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Demonstratie.

$$|A \cup B \cup C| = |A| + |B \cup C| - |A \cap (B \cup C)|$$

$\hat{\Downarrow}$

$$|A \cup (B \cup C)| \quad \begin{array}{c} \downarrow \\ \text{aplicam formula} \end{array} \quad \begin{array}{c} \downarrow \\ \text{aplicam formula} \end{array}$$
$$= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)|$$

$$|(A \cap B) \cup (A \cap C)| = |A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|$$
$$= |A \cap B| + |A \cap C| - |A \cap B \cap C|$$

$$= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C|$$

Principiul includerii și excluderii:

Dacă A_1, A_2, \dots, A_m sunt multimi finite, atunci

$$|A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \dots + |A_m| - |A_1 \cap A_2| -$$
$$|A_2 \cap A_3| - \dots - |A_{m-1} \cap A_m| +$$
$$|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| +$$
$$+ \dots + |A_1 \cap A_2 \cap A_3 \cap A_4| - \dots$$
$$(-1)^{m+1} \cdot |A_1 \cap A_2 \dots \cap A_m|$$

Demonstratiu: Se face inducție după m .

Teorema:

Așa că A, B finite cu $|A|=|B|$ și $f: A \rightarrow B$ funcție.

Sunt echivalente următoarele afirmații:

- 1) f bijectivă
- 2) f injectivă
- 3) f surjectivă

- f injectivă ($\Rightarrow \forall a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$)
- f surjectivă $\forall b \in B \exists a \in A$ s.t. $f(a) = b$
- f bijectivă înseamnă o funcție care e simultan injectivă și surjectivă.

Ex: $m, n \in \mathbb{N}^*$ $(m, n) = 1$

$f: \{0, 1, 2, \dots, m-1\} \rightarrow \{0, 1, \dots, m-1\} \times \{0, 1, \dots, m-1\}$

$f(x) = (\text{restul împărțirii lui } x \text{ la } m, \text{ restul împărțirii lui } x \text{ la } n)$

$\Rightarrow f$ bijectivă (Lemma chineză a resturilor)

Produs Cartezian:

Dacă avem A, B multimi

$A + B = \{(a, b) | a \in A, b \in B\}$ produsul cartezian al multimilor A, B

Exemplu:

Dacă $m = 25$ și $n = 4$ găsim unicul $x \in \{0, 1, \dots, 99\}$ a.i.

$f(x) = (17, 3) \quad x: 25 = \text{restul } 17 \text{ și } x: 4 \text{ restul } 3$

$$\Rightarrow x = 67$$

$$17, 42, \boxed{67}, 32$$

$$x = 17 + 42$$

$$\begin{array}{r} 17 \\ 25 \\ \hline 42 \\ 25 \\ \hline 67 \end{array}$$

Curs 1.

Evaluare.

- 1) Găsiți unicul număr $x \in \{0, 1, 2, \dots, 99\}$ astfel încât restul împărțirii lui x la 7 să fie 5 și restul împărțirii lui x la 13 să fie 10.
- 2) $A = \{m \in \mathbb{N} \mid m \leq 200, (m, 210) = 1\}$

Găsiți $|A|$

$$3) x = 1 + 3 \cdot 68 + 5 \cdot 68^2 + 7 \cdot 68^3 + 9 \cdot 68^4 + \dots + 99 \cdot 68^{49}$$

Găsiți restul împărțirii lui x la 64.

- 4) Găsiți $a \in \{0, 1, 2, \dots, 22\}$ astfel încât restul împărțirii lui a^3 la 33 să fie 3.

Úvrs 1.

Rozložení.

$$\textcircled{1} \quad 23, 36, 49, 62, \boxed{75}, 88$$

$\times 23 + 10$

$$\begin{array}{r|l} 75 & \\ \hline & 1 \\ = 15 & \end{array}$$

$$\begin{array}{r|l} 15 & 13 \\ 65 & \\ \hline 10 & \end{array}$$

\textcircled{2}

$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$

$$B_2 = \{m \in \mathbb{N}, m \leq 209, 2|m\}\}$$

$$B_3 = \{m \in \mathbb{N}, m \leq 209, 3|m\}\}$$

$$B_5 = \{m \in \mathbb{N}, m \leq 209, 5|m\}\}$$

$$B_7 = \{m \in \mathbb{N}, m \leq 209, 7|m\}\}$$

$$A \cup B_2 \cup B_3 \cup B_5 \cup B_7 = \{0, 1, \dots, 209\}$$

$$210 = |A \cup B_2 \cup B_3 \cup B_5 \cup B_7|$$

$$A \cap (B_2 \cup B_3 \cup B_5 \cup B_7) = \emptyset$$

$\text{O}(m, 210) = 1$ prvočíslo 210, může jen delit něčím
u 2, 3, 5, 7

$$210 = |A \cup (B_2 \cup B_3 \cup B_5 \cup B_7)| =$$

$$|A| + |B_2 \cup B_3 \cup B_5 \cup B_7|$$

$$|A| = 210 - |B_2 \cup B_3 \cup B_5 \cup B_7| = 210 - 162 = \boxed{48}$$

$$\begin{aligned}
 |B_2 \cup B_3 \cup B_5 \cup B_7| &= |B_2| + |B_3| + |B_5| + |B_7| - \\
 &|B_2 \cap B_3| - |B_2 \cap B_5| - |B_2 \cap B_7| - |B_3 \cap B_5| - \\
 &|B_3 \cap B_7| - |B_5 \cap B_7| + |B_2 \cap B_3 \cap B_5| + |B_2 \cap B_3 \\
 &\cap B_7| + |B_2 \cap B_5 \cap B_7| + |B_3 \cap B_5 \cap B_7| - |B_2 \cap B_3 \cap B_5 \\
 &\cap B_7|
 \end{aligned}$$

$$= \frac{210}{2} + \frac{210}{3} + 42 + 30 - 35 - 21 - 15 - 10 - 6 + 7 + 5 + 3$$

$$+ 2 - 1 = 247 - 101 + 14 - 1 = 162$$

$$B_2 \cap B_3 = \{0, 6, 12, \dots, 204\}$$

se divide cu 2 și 3 \Rightarrow se divide cu 6

$$B_2 \cap B_5 = \text{se divide cu } 10$$

$$B_2 \cap B_7 = \text{se divide cu } 14, \dots$$

$$B_2 \cap B_3 \cap B_5 = \text{care se divide cu } 2, 3, 5 \text{ sau cu } 30.$$

③ II scriu pe 68 ca $67 + 1$

Din binomial $68^m = (67 + 1)^m = 1 + \binom{1}{m} 67 + \binom{2}{m} 67^2 + \dots$
 în Newton $\dots \binom{m}{m} 67^m = 1 + 67 \cdot \mu \text{ (multiplu de } 67)$

$$x = 67\mu + 1 + 3 + 5 + \dots + 99$$

$$\text{Obs: } (2j+1) \cdot 68^m = (2j+1)(1+67\mu) = 2j + 1 + 67\mu$$

din $1 + 3 + 5 + \dots + (2n-1) = n^2$ se demonstrează prin inducție.

$$\underbrace{1+3+\dots+(2n-1)}_{\frac{n}{2}} + (2n+1) = n^2 + 2n + 1 = (n+1)^2$$

$$x = 67u + 50^2$$

$$x = 67u + 21 \rightarrow \text{restul este } 21$$

$$\begin{array}{r} 2500 \\ 201 \\ \hline 490 \\ 469 \\ \hline 21 \end{array}$$

④ $a \neq 0$

$23 \nmid a$ (23 nu divide a) \Rightarrow Dacă Teorema a lui Fermat $\Rightarrow 23 \nmid a^2 - 1$

$$a^3 = 23 \cdot u + 3$$

Radică puterea a $\sqrt[3]{a}$

$$\Rightarrow a^2 = (23u + 3)^2 \stackrel{\text{biți la putere 2 în mod binomial}}{=} 23u_1 + 3^2$$

$$3^2 = 3^3 \cdot 3^3 \cdot 3 = (23+4)(23+4) \cdot 3 = \\ = 23u_2 + (16 \cdot 3) = 23u_2 + 48 \\ = 23u_3 + 2$$

$$\boxed{a = 23u_4 + 2}$$

$$a^2 - 1 = a \cdot a^2 - 1 = a \cdot (23u_4 + 2) - 1 = 23 \cdot a \cdot u_4 + 2a - 1$$

$$\Rightarrow 23 \mid 2a - 1 \quad \begin{matrix} 23 \text{ divide } 2a - 1 \\ 23 \mid 12(2a - 1) \end{matrix}$$

$$\Rightarrow a = 12 \quad 23 \mid 24a - 12$$

$$a = 9 \text{ mult 12} \quad 23 \mid a + 12$$

Aceasta verifică
prin

(5)

$$f(x) = 9 \cos^4 x - 12 \cos^2 x + 4$$

$$\text{Găsiti } \min \{ f(x) \mid x \in \mathbb{R} \}$$

Găsit: ca mai nici văd unele a funcției

$$g(x) = (3 \cos^2 x - 2)^2 + 3$$

$$\min g(x) = 3$$

$$f(x) = \cos^4 x - 4 \cos^2 x + 4 = (\cos^2 x - 2)^2 + 3 \geq 4$$

$$-2 \leq \cos^2 x - 2 \leq -1$$

$$1 \leq (\cos^2 x - 2)^2 \leq 4$$

Algebra Curs II

Grup
 (G, \cdot) G - multime
 • - operatie (o functie definită pe $G \times G$ cu valori în G)

Dacă:

- 1) $x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in G$ (associativitate)
- 2) $\exists e \in G$ a.i. $x \cdot e = e \cdot x = x, \forall x \in G$ (e - se numește elementul neutru al grupului. Dece există, este unic)
- 3) $\forall x \in G, \exists y \in G$ a.i. $x \cdot y = y \cdot x = e$ (y se numește inversul lui x și este unic)

De abicei, notăm $y = x^{-1}$

Reguli de calcul într-un grup:

- 1) $g \cdot x = g \cdot y \Rightarrow x = y$ (nu demonstrați se folosește axiomatică)
- 2) $g^m \cdot g^n = g^{m+n} \quad \forall g \in G, \forall m, n \in \mathbb{Z}$

G înseamnă g^m

$m \in \mathbb{Z}$

$g \in G$

$$g^m = \begin{cases} g \cdot g \cdot g \cdot \dots \cdot g & \text{dacă } m > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{-m \text{ ori}} & \text{dacă } m < 0 \end{cases}$$

$\left\{ \begin{array}{l} e \text{ dacă } m=0 \\ g^m = g^{m+m} \end{array} \right.$

$$3) (g^m)^n = g^{m+n} \quad \forall g \in G; \forall m, n \in \mathbb{Z}$$

Def.

Să numește comutativă dacă $x \cdot y = y \cdot x, \forall x, y \in G$

Obs:

$$\cdot : G \times G \rightarrow G$$

Exemplu:

$$1) (\mathbb{Z}, +); (\mathbb{Q}, +); (\mathbb{R}, +), (\mathbb{C}, +)$$

$$\begin{array}{ll} \text{grup} & (\mathbb{Q}^*, \cdot) \quad \mathbb{Q}^* = \{q \in \mathbb{Q} \mid q \neq 0\} \\ \text{comutativ} & \end{array}$$

$$\begin{array}{ll} & 1\text{-element neutru} \\ & (\mathbb{R}^+, \cdot), (\mathbb{C}, \cdot) \end{array}$$

Grup necomutativ: (S_m, \circ) - grupul permutărilor cu m elemente.

$$S_m = \{\Gamma : \{1, 2, \dots, m\} \rightarrow \{1, 2, \dots, m\} \mid \Gamma \text{ bijectiv}\}$$

$$\Gamma, \tilde{\Gamma} \in S_m \quad \Gamma \circ \tilde{\Gamma} \in S_m \quad (\Gamma \circ \tilde{\Gamma})(j) = \Gamma(\tilde{\Gamma}(j))$$

Care este element neutru? $\forall j = \overline{1, m}$

$$e \in S_m \quad e(j) = j \quad \forall j = \overline{1, m}$$

Cum se calculează inversa unei permutări?

σ	1	2	3	4	5	6	7	8	9	10
$\sigma(\sigma)$	4	7	10	3	6	9	2	5	8	1

σ	1	2	3	4	5	6	7	8	9	10
$\sigma^{-1}(\sigma)$	10	7	4	1	8	5	2	9	6	3

Man pe intolps: Inversa permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ este $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$ \rightarrow I Semnificație
 $\begin{pmatrix} 4 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$
 \rightarrow II Spordaneană linia $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

$$\sigma^{-1}(\sigma) \cdot \sigma(\sigma) = \sigma$$

$$\sigma^{-1}(u) = u$$

Obs: Dacă $n \geq 3 \Rightarrow S_m$ nu este comutativ

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix} \quad \tilde{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}$$

$$(\sigma \circ \tilde{\sigma})(1) = \sigma(\tilde{\sigma}(1)) = \sigma(3) = 3 \quad | \Rightarrow \tilde{\sigma} \circ \sigma \neq \sigma \circ \tilde{\sigma}$$

$$(\tilde{\sigma} \circ \sigma)(1) = \tilde{\sigma}(\sigma(1)) = \tilde{\sigma}(2) = 2$$

$$|S_m| = m!$$

Grup comutativ: $x \circ y = y \circ x \quad \forall x, y \in G$

Grup necomutativ: $\exists x, y \text{ a.i. } x \circ y \neq y \circ x$

G-grup

$$g \circ x = g \circ y \Rightarrow x = y$$

$$g \circ x = y \circ g \text{ nu rezultă neapărat că } x = y$$

{+ exemplu:

$$g + g^{-1}$$

$$\sigma = 1$$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$g + g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = 1$$

$$g + g^{-1}(1) = g + (2) = g(3) = 3$$

$$x \neq 1$$

Fie $(G, *)$ și (G', \circ) două grupuri. O funcție $f: G \rightarrow G'$ se numește morfism dacă $f(x * y) = f(x) \circ f(y)$

$$\forall x, y \in G$$

Descompunerea unei permutări în produs de cicluri disjuncte.

Ciclu din S_m $\sigma = (a_1, a_2, \dots, a_k)$ - ciclu de lungime k

$$\sigma \in S_m \quad a_i \neq a_j \quad \forall i \neq j$$

$$\{a_1, a_2, a_3, \dots, a_k\} \subseteq \{1, 2, 3, \dots\}$$

$$\sigma(x) = \begin{cases} x & \text{dacă } x \neq a_j \quad \forall j = \overline{1, k} \\ a_{j+1} & \text{dacă } x = a_j \quad j \leq k-1 \\ a_1 & \text{dacă } x = a_k \end{cases}$$

$$\sigma(a_j) = a_{j-1}$$

Exemplu:

$$\sigma = \left(\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 8 & 10 \end{matrix} \right) \in S_{10}$$

$$= (1, 2, 3)(4, 5, 6, 7)(8, 9)(10)$$

$$(a_1, a_2, \dots, a_k) \quad (b_1, b_2, \dots, b_k) \quad 2 \text{ uclii}$$

Să numește disjunctii dacă $a_i \neq b_j \quad \forall i, j$

Dacă σ și $\tilde{\sigma}$ sunt ucli disjunctii atunci:

$$\Rightarrow \sigma \circ \tilde{\sigma} = \tilde{\sigma} \circ \sigma$$

Să spunem că avem:

$$S_{10} \ni \sigma = \left(\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 10 & 5 & 6 & 7 & 4 & 9 & 8 & 1 \end{matrix} \right) = (1, 2, 3, 10)$$

$$(4, 5, 6, 7)(8, 9) \xrightarrow{\text{transpozitii}} (1, 2)(2, 3)(3, 10)$$

$$(4, 5)(5, 6)(6, 7)(8, 9)$$

Ciclii de lungime 2 nu numește transpozitii

$$\sigma(i, j) \quad \sigma(i) = j$$

$$i \neq j \quad \sigma(j) = i$$

$$\sigma(k) = k \quad \forall k \neq i, j$$

Sunțea unei permutări ca produs de transpozitii
 $(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3)(a_3, a_4) \dots$
 $\dots (a_{k-1}, a_k)$ sachă

$$(1, 2)(2, 3) = (1, 2, 3)$$

$$(1, 2, 3, 10)(4, 5, 6, 7)(8, 9) = (1, 2)(2, 3)(3, 10)$$

$(4, 5)(5, 6)(6, 7)(3, 9) \Rightarrow$ produs de transpozitii

$$\varepsilon : S_m \rightarrow \{-1, 1\}$$

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq m} \frac{\sigma(j) - \sigma(i)}{j - i}$$

↓ semnul permutării σ

$$\varepsilon(\sigma \circ \tilde{\sigma}) = \varepsilon(\sigma) \cdot \varepsilon(\tilde{\sigma}) \quad \forall \sigma, \tilde{\sigma} \in S_m$$

$$\varepsilon((i, j)) = -1$$

$i \neq j$

$$S_{10} \ni \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 10 & 5 & 6 & 4 & 1 & 9 & 8 & 1 \end{pmatrix}$$

$$\sigma = \underbrace{(1, 2)(2, 3)(3, 10)(4, 5)(5, 6)(6, 7)(7, 4)}_{\text{transpozitii}}$$

$$\varepsilon(\sigma) = (-1)^7 = -1$$

Ce trebuie să stiu:

- Permutări:
- inversa
 - produs de cicli disjuncti
 - produs de transpozitii
 - signatura

$(\mathbb{Z}_m, +)$ - grupul claselor de resturi mod m.

$$x \equiv y \pmod{m} \Leftrightarrow m \mid x - y \quad | \bar{x} = \bar{y}$$

Exemplu:

$$\begin{aligned}\mathbb{Z}_{12} \quad \bar{14} &= \bar{10} + \bar{4} = \bar{2} \\ 14 &\equiv 2 \pmod{12} \\ 12 &\mid 14 - 2\end{aligned}$$

$(\mathbb{Z}_m, +)$ grup cu m elemente

$$\bar{x} + \bar{y} = \overline{x + y}$$

Elementul neutru este $\bar{0}$

Inversul lui \bar{x} este $\overline{m-x}$

$(U(\mathbb{Z}_m), \cdot)$ - grup cu $\varphi(m)$ elemente

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} \quad x \in \mathbb{Z} \quad (+, m) = 1$$

$$U(\mathbb{Z}_m) = \left\{ \bar{x} \mid x \in \mathbb{Z}, (x, m) = 1 \right\}$$

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \quad | \text{ p prim} \quad \tilde{n} \text{ este un element} \\ \text{inversabil}$$

$$U(\mathbb{Z}_{12}) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$$

$$\bar{5} \cdot \bar{7} = \bar{35} = \bar{11} \quad \bar{7} \cdot \bar{7} = \bar{49} = \bar{1}$$

$$\bar{5} \cdot \bar{11} = \bar{55} = \bar{7} \quad \bar{11} \cdot \bar{11} = \bar{121} = \bar{1}$$

$$\bar{5} \cdot \bar{5} = \bar{25} = \bar{1}$$

$\bar{1}$ este elementul inversabil

$$\varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 1/6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4 \Rightarrow \text{elemente}$$

Factorii primi ai lui 12 sunt: 2, 3

Exemplu ①

$$U(\mathbb{Z}_{61}) = \{\bar{1}, \bar{2}, \bar{3}, \dots, \bar{60}\}$$

$$0 \leq m \leq 60 \quad (m, 61) = 1$$

$(U(\mathbb{Z}_{61}), \cdot)$ - grup cu 60 de elemente

$\bar{1}$ - element neutru

Găsiti inversul lui $\bar{30}$

$$\begin{array}{l|l} \bar{30} \cdot \bar{x} = \bar{1} & \bar{60} = \bar{1} \\ \bar{60} \cdot \bar{x} = \bar{2} & 61 | 61 \end{array}$$

$-\bar{x} = -\bar{2} = \bar{59}$ - inversul lui 30

$$\bar{30} \cdot \bar{59} = \bar{1}$$

$$\textcircled{2} \quad \bar{1}\bar{7} \cdot \bar{7} = \bar{1} \mid \bar{4} \quad U(\mathbb{Z}_{61})$$

$$\bar{6}\bar{8} \cdot \bar{7} = \bar{4}$$

$$\bar{7} \cdot \bar{7} = \bar{4} \mid \bar{5}$$

$$\bar{6}\bar{3} \cdot \bar{7} = \bar{3}\bar{6}$$

$$\bar{2} \cdot \bar{7} = \bar{3}\bar{6} \mid \bar{2}$$

$$\bar{7} = \bar{1}\bar{8}$$

$$\bar{1}\bar{2} \cdot \bar{1}\bar{8} = \bar{1} \Rightarrow \bar{1}\bar{8} \text{ este inversul lui } \bar{1}\bar{7}$$

$(\mathbb{Z}_{61}, +)$ 0 element neutru

$$\text{Ex: } \bar{1}\bar{2} + \bar{5}\bar{9} = \bar{0} \Rightarrow \bar{5}\bar{9} \text{ este inversul lui } \bar{1}\bar{2}$$

Teorema (Lagrange)

(G, \cdot) grup finit, $g \in G$ pt $g^{|G|} = e$
 e -element neutru pt G

$(\mathbb{Z}_m, +)$

$$\bar{g} + \bar{g} + \dots + \bar{g} = \bar{m}g = \bar{0}$$

$$|\mathbb{Z}_m| = m \text{ (cardinal)}$$

\mathbb{Z}_m - grup finit cu m elemente

$(U(\mathbb{Z}_m), \cdot)$ - grup cu $\varphi(m)$ elemente

$$\bar{x}^{\varphi(m)} = \bar{1} \quad (x, m) = 1$$

$$\begin{aligned} \mathbb{Z}_m &= \{\bar{x} \mid x \in \mathbb{Z}\} \\ &= \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{m-1}\} \end{aligned}$$

$$\bar{m} = \bar{0}$$

Teorema lui Euler.

$$x \in \mathbb{Z}, (x, m) = 1 \Rightarrow m \mid x^{\varphi(m)} - 1$$
$$m \in \mathbb{N}^*$$

Aplicatie:

Care sunt ultimele 2 cifre ale lui 17^{203}

$\cup (\mathbb{Z}_{100}, \cdot)$ grup cu $\varphi(100)$ elemente.

$$\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

Am ales 100 pt ca trebuie sa aflam restul impartirii cu 2 zecimale

$$(17, 100) = 1 \xrightarrow{\text{T. Euler}} \overline{17}^{\varphi(100)} = \overline{1}$$
$$\overline{17}^{40} = \overline{1}$$

$$\overline{17}^{203} = (\overline{17}^{40})^5 \cdot \overline{17}^3$$
$$= \overline{1}^5 \cdot \overline{17}^3 = \overline{17}^3$$

$$\overline{17}^3 = \overline{17}^2 \cdot \overline{17} = \overline{289} \cdot \overline{17} = \overline{89} \cdot \overline{17} = \overline{1513} = \overline{13}$$

\Rightarrow ultimele cifre sunt 1 și 3 în același ordine.

② Care sunt ultimele 2 cifre ale lui 17^{199} ?

$$\overline{17}^{40} = \overline{1}$$

$$\overline{17}^{199} = \overline{17}^{39} = \overline{x}$$

$$\overline{17} \cdot \overline{x} = \overline{17}^{40} = \overline{1}$$

$$\overline{x} = \overline{53} \Rightarrow 5 \text{ și } 3 \text{ sunt ultimele 2 cifre.}$$

③ Care sunt ultimele 2 cifre ale lui 18^{199} ?
 ! Hu mai pat este un Euler.

$$x = 18^{199}$$

$$x \equiv ? \pmod{4}$$

$$x \equiv ? \pmod{25}$$

$(U(\mathbb{Z}_{25}), \cdot)$ grup cu $\varphi(25)$ elemente

$$\varphi(25) = 25 \left(1 - \frac{1}{5}\right) = 20 \text{ elemente}$$

$$(18, 25) = 1 \implies 18^{\varphi(25)} \equiv 1 \pmod{25} \quad \text{T. Euler}$$

$$\hat{18}^{20} = \hat{1}$$

$$\hat{x} = \hat{18}^{199} = \hat{18}^{19}$$

$$\hat{18} \cdot \hat{x} = \hat{18}^{20} = \hat{1}$$

$$-\hat{2} \cdot \hat{x} = \hat{1} \mid \hat{4}$$

$$\hat{28} \cdot \hat{x} = -\hat{4}$$

$$\hat{3} \cdot \hat{x} = -\hat{4} = \hat{21} \mid \hat{3}$$

$$\hat{x} = \hat{1}, \hat{3} \in U(\mathbb{Z}_{25}) \\ (3, 25)$$

$$\Rightarrow x \equiv 0 \pmod{4}$$

$$x \equiv ? \pmod{25}$$

$$\frac{x \equiv ? \pmod{25}}{? \cdot 32, 54, 82} \Rightarrow \text{Ultimele cifre sunt } 3 \text{ și } 2$$

$$25+4$$

$$?, \boxed{32}, 54, 82$$

Test (nr. 2).

2018 ?

① Care sunt ultimele 2 cifre ale lui 22^{2018} ?

$$22^{2018} = x$$

$$x \equiv 0$$

$$x \equiv \overline{22}^{18} = (-\bar{3})^{18} = \bar{3}^{18}$$

$$\bar{22}^{20} = \bar{1}$$

$$\bar{3}^3 = \bar{27} = \bar{2}$$

$$\bar{3}^{18} = (\bar{3}^3)^6 = \bar{2}^6 = \bar{64} = \bar{14}$$

$x \equiv 14$ $14, 39, \boxed{64}, 89 \Rightarrow$ ultimele 2 cifre sunt
 6×4

② $\tilde{v}_1 = (1, 2, 3, 4, 5, 6, 7, 8) \in S_8$

$\tilde{v}_2 = (1, 2, 3, 4)(5, 6, 7, 8)$

Calculati $\mathcal{E}(\tilde{v}_1) \circ \mathcal{E}(\tilde{v}_2)$

③ Cate solutii are ecuatiei $\sigma^2 = \tilde{v}_1$ in S_8 ?

Presupunem ca $\exists \sigma \in S_8$ a.t. $\sigma^2 = \tilde{v}_1$

$$\left. \begin{array}{l} \mathcal{E}(\sigma^2) = \mathcal{E}(\tilde{v}_1) = -1 \\ \mathcal{E}(\sigma \circ \tilde{v}) = \mathcal{E}(\sigma) \cdot \mathcal{E}(\tilde{v}) \\ \mathcal{E}(\sigma) \cdot \mathcal{E}(\sigma) = 1 \end{array} \right| \Rightarrow \text{nu exista solutii.}$$

④ Cate soluții are ecuația $\sigma_2 + \tau_2 = S_2$ în S_2 ?

$$(a_1, a_2, \dots, a_k)^2 = \begin{cases} (a_1, a_3, \dots, a_k, a_k, a_{k-1}) & \text{dacă } k \text{ par} \\ (a_1, a_3, a_5, \dots, a_{k-1})(a_2, a_4, \dots, a_k) & \text{dacă } k \text{ impar} \end{cases}$$

$$\sigma^2 = (1, 2, 3, 4)(5, 6, 7, 8)$$

σ - ciclu de lungime 8

$$\sigma = \begin{pmatrix} 1 & 5 & 2 & 6 & 3 & 1 & 4 & 8 \\ & 16 & 2 & 7 & 3 & 8 & 4 & 5 \\ & 1 & 12 & 2 & 8 & 3 & 5 & 4 & 6 \\ & 1 & 8 & 2 & 5 & 3 & 6 & 4 & 7 \end{pmatrix} \quad \begin{array}{l} \text{- prima rot} \\ \text{- a doua rot} \\ \text{- a treia} \\ \text{- a patra} \end{array}$$

⑤ Găsești $a \in \{0, 1, 2, 3, \dots, 16\}$ astfel că

$$17 \nmid a^{43} - 3$$

$$(\cup (\mathbb{Z}_{17}), \cdot) \xrightarrow{\text{Euler}} \bar{a}^{\varphi(17)} = \bar{1}$$

$$\varphi(17) = 17 \left(1 - \frac{1}{17}\right) = 16$$

$$\bar{a}^{43} = \bar{3}$$

$$\Rightarrow \bar{a}^{16} = \bar{1}$$

$$\bar{3} = \bar{a}^{43} = a^{16} \cdot a^{16} \cdot a^1 = \bar{1} \cdot \bar{1} \cdot a^1 = \bar{a}^1 = \bar{3}$$

$$\bar{a} \cdot \bar{a}^{16} \cdot \bar{a}^1 \cdot \bar{a}^{33} = \bar{2}^4 = \bar{10} = \bar{a} \Rightarrow \boxed{a = 10}$$

⑥ Care este numărul an după 2018 în care zilele de 10 membre vor sărbători?

$$365 \text{ zile} / 17 \text{ zile}$$

$$\frac{365}{365} = \bar{1}$$

$$\frac{366}{366} = \bar{2}$$

10 mai 2018 nă
19 du
20 ma
21 mi
22 s
23 v

25 l
26 ma
27 mi
28 vi
29 nembař => **(2029)**

Algebra

(17.11.2018)

Ordine

$$g \in G, g^{1G} = e$$

(G, \cdot) grup finit

$$\underline{\text{ord } g} = \min \{ k \in \mathbb{N}^* \mid g^k = e \}$$

Ordinele lui g în grupul (G, \cdot)

În grupul $(\mathbb{Z}_{200}, +)$ trebuie să calculăm $\text{ord } \bar{28} = ?$

• trebuie găsit elementul neutru din grup: este $\bar{0}$

Care este ul mai mic $k \in \mathbb{N}^*$, a.i.

$$\bar{28k} = \underbrace{\bar{28} + \bar{28} + \bar{28} + \dots + \bar{28}}_{k \text{ ori}} = \bar{0} \Rightarrow \text{ultp 50.}$$

$\bar{28k}$ este multiplu de 200 $200 | 28k$ dacă impărtim
cu 4 $\Rightarrow 50 | 7k \Rightarrow$ ul mai mic nr natural care se
divide, este 50 | k

$$\text{În general } (\mathbb{Z}_m, +) \Rightarrow \text{ord } \bar{m} = \frac{m}{(\bar{m}, m)}$$

\Rightarrow este m împărțit la ul mai
mare divizor comun.

Proprietăți ordonului:

(G, \cdot) grup finit
 e - element neutru

- 1) $g^{\text{ord } g} = e$
- 2) $g^m = e, m \in \mathbb{N}$ atunci $\text{ord } g \mid m$ (ordinalul g divide cardinalul)
- 3) $\text{ord } g \mid |G|$ ordinalul divide întotdeauna cardinalul grupului.

4) $\text{ord } g^k = \frac{\text{ord } g}{(\text{ord } g, k)}$ $\text{ord } g$ împărțește cel mai mare divizor comun $\text{ord } g, k$

5) $\left. \begin{array}{l} (\text{ord } g_1, \text{ord } g_2) = 1 \\ g_1 \cdot g_2 = g_2 \cdot g_1 \end{array} \right\} \text{ord } g_1 \cdot g_2 = (\text{ord } g_1) \cdot (\text{ord } g_2)$

$(G, \cdot) = (U(\mathbb{Z}_{55}), \cdot)$ calculăm $\text{ord } \bar{2}$ în G astfel ...

$U(\mathbb{Z}_{55}) = \{ \bar{a} \mid a \in \mathbb{Z}, (a, 55) = 1 \}$
 Elementul neutru este 1

Cel mai mic $k \in \mathbb{N}^*$ a. s. $\bar{2}^k = 1$

Hacăm $\text{ord } \bar{2}$ unde

Falosim proprietatea 3.

Cardinalul grupului $|U(\mathbb{Z}_{55})| =$

Obs:

$0 \leq a \leq 54$ nu multiplu lui 5 care sunt 11
 $\Rightarrow 1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 23, 24, 26, 27, 29, 30, 31, 33, 34, 36, 37, 39, 41, 43, 45, 46, 48, 49, 51, 53$

$$|\text{U}(\mathbb{Z}_{55})| = 55 - 11 - 4 = 40$$

$$|\text{U}(\mathbb{Z}_{55})| = \varphi(n)$$

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \quad p \text{ prim}$$

$$\varphi(55) = 55 \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{11}\right) = (5-1)(11-1) = 4 \cdot 10 = 40$$

$$d \mid |\text{U}(\mathbb{Z}_{55})| = 40 \text{ adică } d \mid 40$$

$d \in \{1, 2, 4, 8, 5, 10, 20, 40\}$ - divizori lui 40

$$2^{10} = 1024 \stackrel{55}{\equiv} 34 \text{ (restul) } \neq 1$$

$$\Rightarrow d \notin \{1, 2, 5, 10\}$$

Consecință

$$g^k \neq e \Rightarrow \text{ord } g \nmid k$$

$$2^{20} = (2^{10})^2 \stackrel{55}{\equiv} 34^2 = 1156 \stackrel{55}{\equiv} 1$$

$$\bar{2}^{20} = \bar{1} \text{ din proprietatea 2 } d \mid 20$$

$$2^k \notin \{1\}$$

$$\Rightarrow \text{ord } \bar{2} \text{ în } G \text{ este } 20$$

$$\begin{aligned} a &\stackrel{m}{\equiv} b, a \equiv b \pmod{m} \\ a &\equiv b \pmod{m} \\ m &\mid a - b \end{aligned}$$

p prim $2^p - 1$ prim
~~2 3 5 7 11 13 17~~ - 1 cel mai mare număr prim

$8191 = 2^{13} - 1$ este prim

In mod obisnuit, calculăm $\sqrt{8191} = 90.50\dots$

Lucrăm cu un prim peste la 90 (2, 3, 5, 7, 11, 13, 17, ..., 89)

Să ia un m prim care divide $2^{13} - 1$

$p | 2^{13} - 1$ p prim

$d = \text{ord } \bar{2}$ în $(U(\mathbb{Z}_p), \cdot)$ grup cu $p-1$ elemente

$$\phi(p) = p \left(1 - \frac{1}{p}\right) = p-1$$

$$p | 2^{13} - 1 \Rightarrow \bar{2}^{13} = 1$$

Folosind proprietatea 2 $\Rightarrow d | 13 \Rightarrow d \in \{1, 13\}$
 Iar valoarea 1 este exclusă deoarece $\bar{2}^1 \neq 1$

$$\Rightarrow d = 13 \Rightarrow \text{ord } \bar{2} = 13$$

Din prop 3 $13 = \text{ord } \bar{2} \mid |U(\mathbb{Z}_p)| = p-1$

$$\Rightarrow p-1 = 13 \cdot t$$

$$\Rightarrow p = 13t + 1$$

Deoarece $p \neq 2 \Rightarrow t$ este un număr $\Rightarrow p = 13t + 1 = 265 + 1$

$$27 + 26 = 53 + 26 = 79 + 26 = 105$$

1, 2, 4, 53, 79

$$\begin{array}{r} 8191 \\ 79 \end{array} \left| \begin{array}{r} 79 \\ 103 \end{array} \right.$$
$$\begin{array}{r} 291 \\ 231 \\ \hline = 54 \end{array}$$

$$\begin{array}{r} 8191 \\ 53 \end{array} \left| \begin{array}{r} 53 \\ 154 \end{array} \right.$$
$$\begin{array}{r} 289 \\ 265 \\ \hline = 241 \\ 212 \\ \hline = 29 \end{array}$$

Ordinalul unei permutări; cum se calculează din S_m
 $(S_m, 0)$

$S_m = \{\sigma : \{1, 2, \dots, m\} \rightarrow \{1, 2, \dots, m\} \text{ și bijectiv}\}$

$$\sigma, \tau \in S_m \Rightarrow \sigma \circ \tau \in S_m$$

$$\sigma \circ \tau(j) = \sigma(\tau(j))$$
$$j \in \{1, 2, \dots, m\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 2 & 8 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} =$$

Cum se descompune (a_1, a_2, \dots, a_k) $a_i \neq a_s \quad \forall i \neq s$

$$\sigma(a_1) = a_2$$

$$\sigma(a_2) = a_3$$

lungimea
este k

$$\vdots$$
$$\sigma(a_{k-1}) = a_k$$

$$\sigma(a_k) = a_1$$

$$\sigma(+)=+ \quad (\forall) x \neq 0_j \quad (\forall)_j = \overline{1, K}$$

$$= (1, 9)(2, 4, 5, 6, 3)(4, 8)$$

$$\text{ord } \sigma = \left\{ \begin{matrix} 2, 5, 2 \\ \in S_m \end{matrix} \right\} = 10 \rightarrow \text{c.m.m.m.c}$$

$\text{ord } \sigma = \text{ul mai mic multiplu comun al lunginii}\newline \text{cicilor din descompunerea permutării în produs de cicluri}\newline \text{disjuncte.}$

Expoziție:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 & 10 & 5 & 12 & 13 & 11 \end{pmatrix} \in S_{13}$$

$$\text{ord } \sigma = ?$$

Calculați $\text{ord } \bar{2}$ în grupul $(U(\mathbb{Z}_{23}), \cdot)$

Găsiți cel mai mic factor prim al lui $2^{23}-1$

Găsiți un $a \in \{1, 2, 3, \dots, 22\}$ a.i. $\text{ord } \bar{a} = 22$ în
grupul $(U(\mathbb{Z}_{23}), \cdot)$.

Algebra

Curs IV

- 1) Găsiti un factor prim al numărului $2^{2^3} - 1$
- 2) Găsiti cel mai mic factor prim al lui $2^{2^3} - 1$
- 2) p prim $p \mid 2^{2^3} - 1$
- $$(U(\mathbb{Z}_p), \cdot) = (\mathbb{Z}_p^*, \cdot)$$
- $$\mathbb{Z}_p^* = \{\bar{a} \mid p \nmid a\}$$
- $\bar{1}$ - element neutru al grupului
- ord $\bar{2}$ în acest grup
- $$\bar{2}^{2^3} = \bar{1} \Rightarrow \text{ord } \bar{2} \mid 2^3 \Rightarrow \text{ord } \bar{2} = 1 \text{ sau ord } \bar{2} = 2^3 \quad \left| \Rightarrow \bar{2} \neq \bar{1} \right.$$
- $\Rightarrow \text{ord } \bar{2} = 2^3$
- $\text{ord } \bar{2} \mid |\mathbb{Z}_p^*| = p - 1$
- $$\mathbb{Z}_p^* = \{1, 2, 3, \dots, p-1\} \Rightarrow |\mathbb{Z}_p^*| = p - 1$$
- $$p - 1 = 2^3t \Rightarrow p = 1 + 2^3t \geq 47$$
- Mai trebuie să arătăm că $47 \mid 2^{2^3} - 1$
- $$2^{2^3} = 2^{11} \cdot 2^{12} \stackrel{47}{\equiv} 2^{11} \cdot 1 = 189 \stackrel{47}{\equiv} 1 \Rightarrow 47 \mid 2^{2^3} - 1$$
- $\left\{ \begin{array}{l} 2^{11} = 2048 \equiv 47 = 27 \\ 2^{12} = 2^{11} \cdot 2 \stackrel{47}{\equiv} 27 \cdot 2 = 54 \stackrel{47}{\equiv} 7 \end{array} \right.$
- $\Rightarrow 47 este cel mai mic factor al lui $2^{2^3} - 1$$

$$1) p \mid 2^{2^g} - 1 \quad , \quad p \text{ prim}$$

$$(U(\mathbb{Z}_p), \cdot) = (\mathbb{Z}_p^*, \cdot)$$

$$2^g = \text{ord } \bar{2} \quad | \quad |\mathbb{Z}_p^*| = p-1$$

$$p-1 = 2^g t \Rightarrow p = 2^g t + 1$$

$$t=2 \Rightarrow p = 5^g - \text{prim}$$

$$t=8 \Rightarrow p = 2^{3g} - \text{prim}$$

$$5^g \mid 2^{2^g} - 1 \quad ?$$

$$2^{2^g} \stackrel{5^g}{\equiv} 2^{11} \cdot 2^{18} \cdot 2^4$$

Prob 2 (fast)

$$2^6 = 64 \equiv -9 \pmod{13}$$

$$2^{12} \equiv 81 \equiv 8 = 2^3 \pmod{13}$$

$$2^{2^g} \equiv 1 \pmod{13}$$

Prob 4 Gezeigt: $a \in \{1, 2, 3, \dots, 22\}$ a.i.

$\text{ord } \bar{a} = 22$ in graphul $(U(\mathbb{Z}_{23}), \cdot)$

$$\text{ord } \bar{1} = 1 \quad |\mathbb{Z}_{23}^*| = 22$$

$$\text{ord } \bar{2} = \bar{2}^2 \neq \bar{1} \quad \text{ord } \bar{a} \mid 22$$

$$2^{11} = 2048 \stackrel{2^3}{\equiv} 1 \quad \text{ord } \bar{a} \in \{1, 2, 11, 22\}$$

$$\Rightarrow \text{ord } \bar{2} = 11$$

$$\text{Se falsoeste prop 5} \quad \text{ord } \bar{21} = 22$$

$$\text{ord } \bar{2} \cdot \bar{22} = \bar{22} \Rightarrow \bar{44} = \bar{21}$$

$$\text{ord } \bar{3} = 11 \quad (3^{11} \equiv 1)$$

$$\text{ord } \bar{5} = 11$$

$$\text{ord } \bar{5} \neq 11 \quad 5^2 = 25 \equiv 2 \pmod{3}$$

$$5^{10} \equiv 2^5 = 32 \stackrel{23}{\equiv} 9$$

$$5^{11} = 5^{10} \cdot 5 \equiv 9 \cdot 5 \stackrel{23}{\equiv} 22$$

$$\Rightarrow \boxed{a=5}$$

Subgroup

$(G, \cdot) \rightarrow \text{grup}$

H subgroups al lui G dacă

$$1) H \subseteq G, H \neq \emptyset$$

$$2) \forall x, y \in H \Rightarrow x \cdot y \in H$$

$$3) \forall x \in H \Rightarrow x^{-1} \in H \rightarrow \text{inversul lui } x \in G$$

Să matemati: $H \leq G$

Ex: $(\mathbb{Z}, +)$

$$H = \{2t \mid t \in \mathbb{Z}\}$$

$$1) H \subseteq \mathbb{Z}$$

$$2) 2t + 2s = 2(t+s) \in H$$

$$3) -2t = 2(-t) \in H$$

T Lagrange
Dacă G este grup finit și $H \leq G \Rightarrow |H| \mid |G|$
→ divide

$\mathbb{Z}_4: (\mathbb{Z}_4, +)$

Sunt: toate subgrupurile acestui grup

$$H \leq \mathbb{Z}_4 \Rightarrow |H| \in \{1, 2, 4\}$$

$$|H|=1 \Rightarrow H = \{0\}$$

$$|H|=4 \Rightarrow H = \mathbb{Z}_4$$

$$|H|=2 \Rightarrow H = \{\bar{0}, \bar{2}\}$$

Obs: Dacă $H \leq G \Rightarrow e \in H$

$$H \neq \emptyset \Rightarrow \exists h \in H \xrightarrow{\text{prop 3}} h^{-1} \in H \quad \rightarrow \text{prop 2}$$

$$e = h \cdot h^{-1} \in H$$

$H \leq (\mathbb{Z}_6, +)$

pt 1) $H = \{e\}$

pt 2) $H = \{\bar{0}, \bar{3}\}$

pt 3) $H = \{\bar{0}, \bar{2}, \bar{4}\}$

Izomorfism

(G_1, \cdot) și (G_2, \perp) grupuri

$f: G_1 \rightarrow G_2$ se numește morfism de grupuri

dacă $f(+ \cdot \gamma) = f(+) \perp f(\gamma)$

$$\forall +, \gamma \in G_1$$

Def: Dacă dării grupuri sunt izomorfe ($G_1 \cong G_2$) dacă există $f: G_1 \rightarrow G_2$, morfism grupuri deci f este bijectivă.

Σ_+ :

$$H = \{\bar{0}, \bar{3}\} \subseteq \mathbb{Z}_6 \quad (H, +) \cong (\mathbb{Z}_2, +)$$

$$f(\bar{0}) = \hat{0}$$

$$f(\bar{3}) = \hat{1}$$

$$f(\bar{0} + \bar{0}) = f(\bar{0}) = \hat{0} = \hat{0} + \hat{0} = f(\bar{0}) + f(\bar{0})$$

$$f(\bar{3} + \bar{0}) = f(\bar{0} + \bar{3}) = f(\bar{3}) = \hat{1} = \hat{0} + \hat{1} = f(\bar{0}) + f(\bar{3})$$

$$f(\bar{3} + \bar{3}) \geq f(\bar{0}) = \bar{0} = \hat{1} + \hat{1} = f(\bar{3}) + f(\bar{3})$$

\bullet $f: G_1 \rightarrow G_2$ f morfism grupuri $(G_1, \cdot) (G_2, \perp)$

e_1 = elem neutru din G_1 e_2 = elem neutru din G_2

$$\Rightarrow \begin{cases} 1) f(e_1) = e_2 \\ 2) f(g^{-1}) = f(g)^{-1} \quad \forall g \in G_1 \end{cases}$$

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) \perp f(e_1) = f(e_1) \Rightarrow f(e_1) = e_2$$

Obs: f izomorfism de grupuri și G_1 și G_2 finite

$$\Rightarrow \text{ord } f(g) = \text{ord}(g), \quad \forall g \in G_1$$

$(G_1, \cdot) (G_2, \perp)$ grupuri

$(G_1 \times G_2, *) \rightarrow$ grup

$$x_1, y_1 \in G_1 \quad x_2, y_2 \in G_2$$

$$(x_1, y_1) \in G_1 + G_2$$

$$(y_1, z_1) \in G_1 + G_2$$

$$(x_1, y_1) * (y_1, z_1) = (x_1 * y_1, y_1 + z_1)$$

$(\mathbb{Z}_8, +) \not\simeq (\mathbb{Z}_2, +) * (\mathbb{Z}_4, +)$ - non surjective
 $\text{ord } \bar{x} = 8$

Przykład: $\exists f: \mathbb{Z}_8 \rightarrow \mathbb{Z}_2 + \mathbb{Z}_4$ izomorf

$$\Rightarrow \text{ord } f(\bar{x}) = \text{ord } \bar{x} = 8$$

$$f(\bar{x}) = (\hat{a}, \tilde{b}) \quad \begin{matrix} \hat{a} \in \mathbb{Z}_2 \\ \tilde{b} \in \mathbb{Z}_4 \end{matrix}$$

$$4(\hat{a}, \tilde{b}) = (4\hat{a}, 4\tilde{b}) = (\hat{a}, 0) \Rightarrow \text{ord } (\hat{a}, \tilde{b}) \in \{1, 2, 4\}$$

$$\text{ord } (\hat{a}, \tilde{b}) = \text{ord } f(\bar{x}) = \text{ord } \bar{x} = 8$$

Et:

$$e^+ + \gamma = e^+ \cdot e^\gamma$$

$$(\mathbb{R}, +) \simeq (G, \cdot)$$

$$G = \{n \in \mathbb{R}, n > 0\}$$

$$f(+) = e^+$$

$$f(+ + \gamma) = e^{+ + \gamma} = e^+ \cdot e^\gamma = f(+) \cdot f(\gamma)$$

Este f b-ijectiva?

$$\text{from } n > 0, n \in \mathbb{R} \Rightarrow \exists x \in \mathbb{R} \text{ a.i. } e^x = n$$

$$\lim_{x \rightarrow 0} e^x = e^0 = 1 \Rightarrow + = \gamma; \quad \lim_{x \rightarrow \infty} e^x = \infty$$

1) Cate subgrupu are $(\mathbb{Z}_{30}, +)$?

$$H \leq \mathbb{Z}_{30} \Rightarrow |H| \in \{1, 2, 3, 5, 6, 10, 15, 30\}$$

$$|H|=1 \Rightarrow \{\bar{0}\}$$

$$|H|=30 \Rightarrow H = \mathbb{Z}_{30}$$

$$|H|=k|30 \quad H = \left\{ \bar{0}, \frac{\bar{30}}{k}, \dots, \frac{\bar{30}}{k}(k-1) \right\}$$
$$k \neq 1, 30$$

$$\bar{x} \in H \quad x \in \{0, 1, 2, \dots, 29\}$$

$$\underbrace{\bar{x} + \bar{x} + \dots + \bar{x}}_{k \text{ ori}} = \bar{0}$$

\rightarrow T Lagrange

$$30|kx \quad \frac{30}{k}|x$$

$$\frac{30}{k}|x \Rightarrow x \in \left\{ 0, \frac{30}{k}, \frac{30}{k} \cdot 2, \dots, \frac{30}{k}(k-1) \right\}$$

^{k valori} $|H|=k$

2) Cate subgrupu are (S_3, \circ) ?

$$H \leq S_3 \Rightarrow |H| \mid |S_3| = 6 \Rightarrow |H| \in \{1, 2, 3, 6\}$$

$$|H|=1 \Rightarrow H = \{\rho\}$$

$$|H|=6 \Rightarrow H = S_3$$

$$|H|=2 \Rightarrow H_1 = \{\rho, \sigma_1\}$$

$\rightarrow 3$ subgrupu

$$\sigma \neq \rho \quad \sigma^2 = \rho$$

$$\Rightarrow \text{ord } \sigma = 2$$

$$\sigma_1 = (1, 2)(3)$$

$$\sigma_2 = (1, 3)(2)$$

$$\sigma_3 = (2, 3)(1)$$

$$|H|=3 \Rightarrow H = \{e, \sigma,$$

$$\sigma^2 \neq e \quad \underbrace{\text{ord } \sigma \mid 3}_H \Rightarrow \text{ord } \sigma^3 = 3$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \Rightarrow 6 \text{ subgroups}$$

$$3) (\mathbb{Z}_u, +) + (\mathbb{Z}_{25}, +) \cong (\mathbb{Z}_{100}, +)?$$

$$f: \mathbb{Z}_{100} \rightarrow \mathbb{Z}_u + \mathbb{Z}_{25}$$

$$f(\bar{x}) = (\hat{x}, \tilde{x})$$

$$\textcircled{1} \quad f(\bar{x}) = (\hat{x}, \tilde{x})$$

$$f(\bar{x} + \bar{y}) = f(\bar{x}) + f(\bar{y})$$

$$f(\bar{x} + \bar{y}) = f(\bar{x} + \bar{y}) = (\hat{x} + \hat{y}, \tilde{x} + \tilde{y}) = (\hat{x}, \tilde{x}) + (\hat{y}, \tilde{y})$$

$$= f(\bar{x}) + f(\bar{y}) \Rightarrow \text{surjective}$$

$$\textcircled{2} \quad |\mathbb{Z}_{100}| = 100 = |\mathbb{Z}_u + \mathbb{Z}_{25}|$$

$$f \text{ injective} \quad f(\bar{x}) = f(\bar{y}) \Rightarrow \bar{x} = \bar{y}$$

$$(\hat{x}, \tilde{x}) = (\hat{y}, \tilde{y}) \Rightarrow \begin{cases} \hat{x} = \hat{y} \\ \tilde{x} = \tilde{y} \end{cases}$$

$$\left. \begin{array}{l} \hat{x} = \hat{y} \Rightarrow u|x-y \\ \tilde{x} = \tilde{y} \Rightarrow 25|x-y \end{array} \right| \Rightarrow 100|x-y \Rightarrow f \text{ inj}$$

$$\Rightarrow f \text{ bijective} \quad \textcircled{1} \text{ in } \textcircled{2} \Rightarrow \text{isomorphism}$$

4) $(\mathbb{Z}, +) \simeq (\mathbb{Q}^*, \cdot)$? sunt izomorf? ?

Presupunem că $\exists f: \mathbb{Q}^* \rightarrow \mathbb{Z}$ și bi:

$$f(x \cdot y) = f(x) + f(y), \forall x, y \in \mathbb{Q}^*$$

$$f(1) = 0$$

$$0 = f(1) = f((-1) \cdot (-1)) = f(-1) + f(-1) = 2f(-1)$$

$$\Rightarrow \begin{cases} f(-1) = 0 \\ f(1) = 0 \end{cases} \quad \Rightarrow 1 = -1 \rightarrow \text{contradictie.}$$

f ∉