

1)  $a \sim b \Leftrightarrow \exists m, n \in \mathbb{N}^* \text{ s.t. } a | b^m \text{ și } b | a^n$

~reflexivitate;  $a | a$  (dacă  $m = n = 1$ )

~simetricitate;  $a \sim b \Leftrightarrow \exists m, n \in \mathbb{N}^* \text{ s.t. } a | b^m \text{ și } b | a^n$

Cant  $p, q \in \mathbb{N}^*$  s.t.  $b \mid a$ , adică  $b \mid a^p$  și  $a \mid b^q$

Răbdarea numără  $p = m$  și  $q = n$ . Deci  $b \sim a$ .

~transitivitate;  $a \sim b \wedge b \sim c \Rightarrow \exists m, n \in \mathbb{N}^* \text{ s.t. } a | b^m, b | c^n$

$b \sim c \Leftrightarrow \exists q, r \in \mathbb{N}^* \text{ s.t. } b | c^q, c | b^r$

$$\begin{array}{c} a | b^m \\ b | c^n \Rightarrow b^m | c^{nm} \end{array} \Rightarrow a | c^{nm} \quad \left\{ \begin{array}{l} a | c^{nm} \\ a \sim c \end{array} \right\}$$

$$\begin{array}{c} c | b^r \\ b | a^m \Rightarrow b^r | a^{mr} \end{array} \Rightarrow c | a^{mr} \quad \left\{ \begin{array}{l} c | a^{mr} \\ c \sim a \end{array} \right\}$$

Dacă:  $a \sim b \Leftrightarrow \exists m, n \in \mathbb{N}^* \text{ s.t. } a | b^m \text{ și } b | a^n$

Analog, dacă  $p \mid a$  și  $q \mid b \Rightarrow p \mid b^m \text{ și } q \mid a^n \Rightarrow p \mid a \dots a \underset{n-\text{ori}}{\dots} \Rightarrow p \mid a$

Prin

Dacă  $a \sim b$  au aceiasi dezvoltări primă  $\Leftrightarrow a \sim b$  (,  $\Rightarrow$ )

dacă  $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$  sau  $m = \max\{\alpha_i\}_{i=1, t}; a | b^m$   
 $b = p_1^{\beta_1} \dots p_t^{\beta_t}$  sau  $n = \max\{\beta_i\}_{i=1, t}; b | a^n$

E dacă ambele  $\sim$  este rezultatul.

$$\hat{o} = \{b \mid b \sim o\} = \{b \mid \exists m, n \in \mathbb{N}^* \text{ s.t. } b | o^m \text{ și } o | b^n\}$$
$$= \{o\}$$

$$\hat{1} = \{b \mid b \sim 1\} = \{b \mid \exists m, n \in \mathbb{N}^* \text{ s.t. } b | 1^m \text{ și } 1 | b^n\}$$
$$= \{1\}$$

$\forall a \in \mathbb{N} \setminus \{0, 1\}, a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$  - descompunerea în prime distincte

$\hat{a} = \{b \mid b \text{ are ca dezvoltare primă } \forall i \in \{1, \dots, t\}\}$

$$\hat{a} = \{p_1^{\beta_1} \dots p_t^{\beta_t} \mid \beta_j \in \mathbb{N}^*, \forall j = 1, t\} = \overbrace{p_1 \dots p_t}^t$$

Un set complet de reprezentanțe  $\sim$  este  $\{0, 1, p_1 \dots p_t, \frac{p_1 \dots p_t}{p_i}, \dots, \frac{p_1 \dots p_t}{p_1 \dots p_t}\}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \in S_6$$

(i)  $\sigma = (1\ 3\ 4\ 5\ 6\ 2) \rightarrow$  ciclu de lungime 6.

$$\sigma = (1\ 3)(3\ 4)(4\ 5)(5\ 6)(6\ 2)$$

(ii)  $E(\sigma) = (-1)^5 = -1 \Rightarrow \sigma = \text{permutare impară}$

$\theta(\sigma) =$  numărul de ordinea ciclurilor care apar în descompunerea lui  $\sigma$

$$\theta(\sigma) = 6.$$

$$\sigma^{6 \times 1} = \sigma^5 \cdot \sigma^{-1} = (2\ 6\ 5\ 4\ 3\ 1)$$

(iii) Memoriaj elementelor de ordin 3 din  $S_6$ .

Fie  $\gamma \in S_6$  de ordin 3 și  $\gamma = \theta_1 \dots \theta_t$ . Dacă  $\theta_i$  este o ciclu de lungime 3, atunci  $\theta_i = [\theta_i(\theta_j) | j=1, t] = 3$

$\Rightarrow \theta_i(\theta_j) \in \{1, 3\}$ ,  $\forall j=1, t$ , cu cel puțin un  $\theta_j$  de ordin 3.

Rezultă  $\gamma = (abc)(def)$  sau  $\gamma = (abc)(d)(e)(f)$

în vr. de

în vr. de

Obs: Prin descompunerea în produs de cicluri disjointe avem  $k_1$  cicluri de lungime 1,  $\forall 1 \leq i \leq n$  ( $\forall i \in \{1, \dots, n\}$ ).

$(k_1, \dots, k_n)$  - se numește tipul de descompunere al lui  $\gamma$ ; el verifică relația  $k_1 + 2k_2 + 3k_3 + \dots + nk_n = n$ .

Nr. permutărilor din  $S_n$  cu un tipul de descompunere

$$(k_1, \dots, k_n)$$
 este egal cu  $\frac{n!}{k_1! k_2! \dots k_n!}$

Aleg  $k_1$ , elem din  $\{1, \dots, n\}$  care formează  $k_1$  cicluri

de lungime 1  $\rightarrow A_n^{k_1}$  moduri.

Aleg  $2k_2$  elem din mult. numărătore care formează  $k_2$

cicluri de lungime 2  $\rightarrow A_{n-k_1}^{2k_2}$  moduri

Aleg  $i k_i$ , elem din mult. numărătore care formează

$k_i$  cicluri de lungime  $i \rightarrow A_{n-k_1-\dots-(i-1)k_{i-1}}^{ik_i}$

Să răspundem că ciclurile de lungime  $i$  se întâlnesc în  $V$ -moduri diferite

$$(a_1 \dots a_i) = (a_2 a_3 \dots a_i a_1) = (a_3 \dots a_i a_1 a_2)$$

$\Rightarrow$  produsul a  $k_i$  cicluri distincte de lungime  $i$

se poate scrie în  $k_i!$  moduri

Răsuflare și rezultă că rezultat este  $\frac{A_n^{k_1} A_{n-k_1}^{2k_2} \dots A_{n-k_1-\dots-(m-1)k_{m-1}}^{ik_m}}{k_1! k_2! \dots k_m!} =$

$$k_1 + \dots + (m-1)k_{m-1} + m k_m = n$$

$$= \frac{m!}{(k_1 k_2 \dots k_m)!}$$

Revenim la problema noastră

$$\cdot \gamma = (a b c) \in S_6 \rightsquigarrow (3, 0, 1, 0, 0, 0) \Rightarrow \frac{6!}{3! \cdot 3!} = 40$$

$$\cdot \gamma = (a b c)(d e f) \in S_6 \rightsquigarrow (1, 0, 2, 0, 0, 0) \Rightarrow \frac{6!}{2! \cdot 2!} = 40$$

$\Rightarrow$  sunt 80 de elem de ordin 3 în  $S_6$ .

$$9) f = x^3 - x^2 + 2x + 1 \in \mathbb{Z}[x]$$

$$\mathcal{I} = (3, f) \subseteq \mathbb{Z}[x]$$

$$\left( \mathcal{I} = \langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^n a_i x_i \mid x_i \in \mathcal{I} \right\} \subseteq \mathbb{R} \right)$$

$$\mathcal{I} = \{ 3u + fv \mid u, v \in \mathbb{Z}[x] \} \subseteq \mathbb{Z}[x].$$

(i)  $g \in \mathbb{Z}[x] \setminus \mathcal{I}$ .

$$f(1) = 3 \Rightarrow (3u + fv)(1) = 3u(1) + 3v(1) \stackrel{!}{=} 3$$

Einfach dann  $h \in \mathbb{Z}[x]$  mit  $3 \nmid h(1)$  (d.h.  $h \notin \mathcal{I}$ )

z.B. exemplarisch,  $h = 1$  dann  $h = x$  dann  $h = x+1$   
etc.

(ii) Praktisch  $\exists g \in \mathbb{Z}[x]$  a.s.  $(g) = (3, f)$  in  $\mathbb{Z}[x]$

$$3 \in (3, f) = (g) = \{gh \mid h \in \mathbb{Z}[x]\} \Rightarrow \exists h \in \mathbb{Z}[x] \text{ a.s.}$$

$$3 = gh \Rightarrow \text{grad}(g) = \text{grad}(h) = 0 \Rightarrow g = a, h = b \in \mathbb{Z}$$

grad 0

$$\text{Kai } ab = 3 \text{ in } \mathbb{Z} \Rightarrow a \in \{\pm 1, \pm 3\}.$$

$$\text{Kai } g \in \{\pm 1\} = U(\mathbb{Z}[x]) = U(\mathbb{Z}) \Rightarrow (g) = \mathbb{Z}[x] = (3, f)$$

$\downarrow$      $\not\in$      $x$

$1, x, x+1$

$$\text{Kai } g \in \{\pm 3\} \Rightarrow (3, f) = (3) \Leftrightarrow f \in (3) = 3 \mathbb{Z}[x]$$

$\not\in$

$$\Rightarrow \exists h \in \mathbb{Z}[x] \text{ a.s. } f = 3h \text{ in } \mathbb{Z}[x]$$

$\begin{matrix} \not\mid 3 \\ x^3 - x^2 + 2x + 1 \end{matrix}$

Kai  $\not\exists g \in \mathbb{Z}[x]$  a.s.  $\mathcal{I} = (g)$ .

$$(iii) \frac{\mathbb{Z}[x]}{(3, f = x^3 - x^2 + 2x + 1)} \simeq \frac{\mathbb{Z}_3[x]}{(x^3 - x^2 + 2x + 1)}$$

not  
only  
but  
also

$$\begin{aligned} \mathbb{Z}[x] &\rightarrow \mathbb{Z}_3[x] & \xrightarrow{\psi} & \overline{\mathbb{Z}_3[x]} \\ f = \sum a_i x^i &\rightarrow \hat{f} = \sum \hat{a}_i x^i & \uparrow & (\hat{f} = x^3 - x^2 + 2x + 1) \\ && \text{only canonical} & \\ \hat{f} &\rightarrow \pi(\hat{f}) = \overline{\hat{f}} & \xrightarrow{\quad} & \end{aligned}$$

$$\begin{aligned} \mathbb{Z}[x] &\xrightarrow{\psi} \frac{\mathbb{Z}_3[x]}{(\hat{f})} \\ \psi(f) &= \overline{\hat{f}} \end{aligned}$$

not only  
but also

Following the input current in  $\mathbb{Z}_3[x]$  ( $\mathbb{Z}_3$  corp) se  
obtinem ca  $\ker \psi = (3, f)$ .

$$\text{TFI (enell)} \Rightarrow \frac{\mathbb{Z}[x]}{(3, f)} \simeq \frac{\mathbb{Z}_3[x]}{(\hat{f})} \text{ not } \subset$$

$\uparrow$   
nu este corp peste  $\mathbb{Z}_3$ , inseamna,

$\frac{K[x]}{(h)}$  este corp  $\Leftrightarrow h$  este irred in  $K[x]$ .

pentru  $h = \hat{f} = x^3 - x^2 + 2x + 1 \in \mathbb{Z}_3[x]$  nu are rad ( $\hat{i} \in \mathbb{Z}_3$ )  
in  $\mathbb{Z}_3$ , deci  $h$  este redusibil in  $\mathbb{Z}_3[x]$

$\ker L = \frac{\mathbb{Z}_3[x]}{(\hat{f})}$  nu este corp.

$$2) G = \mathbb{Z}_k \times \mathbb{Z}_{15}$$

$$(i) \forall x \in G \text{ ca } \vartheta(x) = 10 \quad \text{X}$$

$$\text{Solut: } x = (\hat{a}, \hat{b}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{15}$$

$$\begin{aligned} \vartheta(x) &= [\vartheta(\hat{a}), \vartheta(\hat{b})] = 10 \\ \text{Lagrange: } \vartheta(\hat{a}) &\mid 12, \quad \vartheta(\hat{b}) \mid 15 \\ &1, 2, 3, 4, 6, 12 \quad 1, 3, 5, 15 \end{aligned}$$

Ob: In general  $\mathbb{Z}_m = \langle \tilde{\pi}^m \rangle ; (\mathbb{Z}_m, +) \text{ mit } \vartheta(\tilde{1}) = m$ .

$$\begin{aligned} \text{da } \tilde{a} \text{ ist ord. und } \vartheta(\tilde{a}) &= \frac{\vartheta(\tilde{1})}{(\alpha, \vartheta(\tilde{1}))} = \frac{m}{(\alpha, m)} \\ \Rightarrow \vartheta(\hat{a}) &= \frac{\vartheta(\tilde{a})}{[\vartheta(\tilde{a}), k]} \end{aligned}$$

$$\vartheta(\hat{a}) = 2 \text{ in } \mathbb{Z}_{12} \Leftrightarrow \frac{12}{(\alpha, 12)} = 2 \Leftrightarrow (\alpha, 12) = 6 \Leftrightarrow$$

$$\Leftrightarrow \hat{a} = \hat{6}$$

$$\vartheta(\hat{b}) = 5 \text{ in } \mathbb{Z}_5 \Leftrightarrow \frac{15}{(\beta, 15)} = 5 \Leftrightarrow (\beta, 15) = 3 \Leftrightarrow$$

$$\Leftrightarrow \hat{b} \in \{ \overline{3} \hat{b} \mid 5 \hat{b} \in \} = \{ \overline{3}, \overline{6}, \overline{9}, \overline{12} \}$$

Sunt deci 4 elem de ordin 10 in  $G = \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ .

$$(ii) \hat{k} \in \mathbb{Z}_{20} \text{ si } \hat{k}^{-8} \cdot \hat{k} \cdot \hat{k}^{21} = \hat{3}.$$

$$\hat{k}, \hat{3} \in \mathbb{U}(\mathbb{Z}_{20}) \Rightarrow \hat{k} = \hat{17}^8 \cdot \hat{7}^{-2021} \cdot \hat{3}^{-9} \text{ in } \mathbb{Z}_{20}.$$

$$|\mathbb{U}(\mathbb{Z}_{20})| = \varphi(20) = \varphi(2 \cdot 5) = 2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 8$$

Lagrange:  $\hat{x}^8 = \hat{1}$  in  $\mathbb{Z}_{20}$ ,  $\forall \hat{x} \in \underbrace{\mathbb{U}(\mathbb{Z}_{20})}_{\text{grup cu 8 elem}}$ .

$$\Rightarrow \hat{k} = \hat{17}^8 \cdot \hat{7}^{-5} \cdot \hat{3}^{-1} = \hat{3}^5 \cdot \hat{7}^{-1} = \hat{3}^4 = \hat{7}^4 = \hat{1}.$$