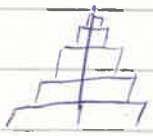
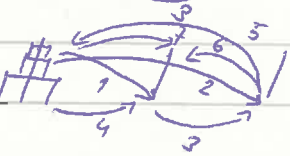
max. 3 absence
absence navíc -2b
úlohy +2b
test max. 10b
---
součet ≥ 5b

Hanojské věže



① Vždycky lze přesunout 1 kolečko
② Nikdy nepokládám větší na menší

H_n = minimální počet kroků k přesunutí n-věže na jiný kolík
$H_1 = 1$
$H_2 = 3$
$H_3 = 7$ 

$H_n = 2H_{n-1} + 1$

n	1	2	3	4	5	6	7
H_n	1	3	7	15	31	63	127

$H_n \overset{?}{=} 2^n - 1$, po $n = 1, \dots, 7$ platí
indukcí na n dokážeme
Vycházíme z předpokladu $H_n = 2^n - 1$

$H_{n+1} = 2H_n + 1 \overset{IP}{=} 2(2^n - 1) + 1 = 2^{n+1} - 1$, $H_1 = 1$ ✓

Jiný (obecnější) postup:

$$H_n = 2H_{n-1} + 1 = 2(2H_{n-2} + 1) + 1 = 2^2 H_{n-2} + 2 + 1 =$$
$$= 2^2(2H_{n-3} + 1) + 2 + 1 = 2^3 H_{n-3} + 2^2 + 2 + 1 = \dots = 2^{n-1} H_1 + 2^{n-2} + 2^{n-3} + \dots + 2 + 1$$
$$= \sum_{i=0}^{n-1} 2^i = \frac{2^{n-1}}{2-1} = 2^n - 1$$

$(H_n)_{n\geq 1}$: $H_1 = 1$
$H_2 = 2H_1 + 1$
$H_3 = 2H_2 + 1$
$\vdots$
$H_n = 2H_{n-1} + 1$

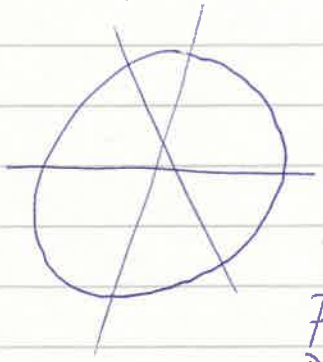
$H_1 = 1 \quad / 2^{n-1}$
$H_2 - 2H_1 = 1$
$H_3 - 2H_2 = 1$
$H_4 + 2H_3 = 1$
$\vdots$
$H_n - 2H_{n-1} = 1 \quad / 2^0$

$/2^2$ ⊕
$/2$ ⊕

$H_n = \sum_{i=0}^{n-1} 2^i = 2^n - 1$

Krájení pizzy

Max. počet kousků, na které rozřeže pizzu n rovnými řezy



$P_0 = 1$
$P_1 = 2$
$P_2 = 4$
$P_3 = 7$
$P_4 = 11$
$P_n = P_{n-1} + n$

n	1	2	3	4	5	6	7	8	9
P_n	2	4	7	11	16	22	29	37	46

① Řezy různoběžné,
② Nepotkají se 3 a víc v jednom bodě. } Krájíme rovinou přímkou

$$P_n - P_{n-1} = n$$
$$P_{n-1} - P_{n-2} = n-1$$
$$P_{n-2} - P_{n-3} = n-2$$
$$\vdots$$
$$P_2 - P_1 = 2$$
$$P_1 - P_0 = 1$$
$$P_0 = 1$$

$$P_n = \sum_{i=1}^{n} i + 1 = \frac{n(n+1)}{2} + 1 = \frac{n^2+n+2}{2}$$

$$x_n = \alpha_1(n)\, x_{n-1} + \alpha_0(n) \Rightarrow x_n - \alpha_1(n) x_{n-1} = \alpha_0(n)$$
$$x_{n-1} - \alpha_1(n-1) x_{n-2} = \alpha_0(n-1)$$
$$x_{n-2} - \alpha_1(n-2) x_{n-3} = \alpha_0(n-2)$$
$$\vdots$$
$$x_2 - \alpha_1(2) x_1 = \alpha_0(2)$$
$$x_1 = \alpha_0$$

Definice

Nechť $(\alpha_0(n))_{n\geq 0}, (\alpha_1(n))_{n\geq 0}, \ldots, (\alpha_{k-1}(n))_{n\geq 0}$ jsou komplexní posloupnosti takové, že $\alpha_0(n) \neq 0$, $k \in \mathbb{N}$.
Nechť $(f(n))_{n\geq 0}$ je komplexní posloupnost.
Vztah $x_{n+k} + \alpha_{k-1}(n) x_{n+k-1} + \alpha_{k-2}(n) x_{n+k-2} + \ldots + \alpha_1(n) x_{n+1} + \alpha_0(n) x_n = f(n)$ nazýváme lineární diferenční rovnicí k-tého řádu s pravou stranou.
Pokud $f(n) = 0$ $\forall n \geq 0$ pak je nazýváme homogenní.

Příklad

$H_n = 2H_{n-1} + 1$ $n \geq 2 \Leftrightarrow H_{n+1} - 2H_n = 1 \Rightarrow \begin{matrix} k=1 \\ \alpha_0 = -2, \forall n \in \mathbb{N} \\ f(n) = 1, \forall n \in \mathbb{N} \end{matrix}$

$P_{n+1} = P_n + n + 1 \Rightarrow P_{n+1} - P_n = n+1 \Rightarrow \begin{matrix} k=1 \\ \alpha_0(n) = -1, \forall n \in \mathbb{N} \\ f(n) = n+1 \end{matrix}$

Fibonacciho posloupnost
$F_{n+2} - F_{n+1} - F_n = 0$, $k=2$, homogenní; $\alpha_0(n) = \alpha_1(n) = -1$, $\forall n \in \mathbb{N}$

$a_{n+2} = a_n + 1$, $k=2$, $a_0 = \dots$

$a_1 = \dots$

řád k určuje počet počátečních podmínek

$F_{n+2} - F_{n+1} - F_n = 0$, $F_0 = 0$, $F_1 = 1$

n	0	1	2	3	4	5	6	7	8
F_n	0	1	1	2	3	5	8	13	21

F_n = Binetův vzorec

$l = \{(a_n)_{n\geq 0} \mid a_n \in \mathbb{C}, \forall n \geq 0\}$ vektorový prostor nad tělesem $\mathbb{C}$

$\oplus$ $(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}$, $\forall (a_n), (b_n) \in l$

$\odot$ $\alpha (a_n)_{n\geq 0} = (\alpha a_n)_{n\geq 0}$, $\forall (a_n) \in l, \forall \alpha \in \mathbb{C}$

$\dim l = +\infty$ $d_1(1, 0, 0, \dots)$

$d_2(0, 1, 0, \dots)$

$d_3(0, 0, 1, \dots)$

$\vdots$

$d_m(0, 0, 0, \dots, 1, 0, \dots)$

$\oplus$ $\sum_{i=1}^{m} \alpha_i e_i = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_m, 0, \dots) = (0, 0, \dots) \Rightarrow (*)$

$\Rightarrow (*) (\alpha_i = 0) (\forall i \in \hat{m})$

$l \supset M = \{(a_n)_{n\geq 0} \in l \mid a_{n+2} - a_{n+1} - a_n = 0\}$

tvrzení: $M \subset\subset l$

důkaz: $M \subset l$ ✓

$M \neq \emptyset$ ✓, nulový $(0)_{n\geq 0} = \vec{0} \in M$

$(\forall (a_n), (b_n) \forall \alpha \in \mathbb{C})(\alpha (a_n) + (b_n) \in M)$

$\alpha a_{n+2} + b_{n+2} - (\alpha a_{n+1} + b_{n+1}) - (\alpha a_n + b_n) =$

$= \alpha (a_{n+2} - a_{n+1} - a_n) + (b_{n+2} - b_{n+1} - b_n) = 0, \forall n \in \mathbb{N}$

e_1 e_2

$\begin{pmatrix}1\\0\\\vdots\end{pmatrix}\begin{pmatrix}0\\1\\\vdots\end{pmatrix}$ LN $\Rightarrow \dim M \geq 2$

pro libovolné a_0, a_1, které generují $(a_n) \in M$ platí $(a_n) = a_0(e_1) + a_1(e_2)$ a tedy generují celé M a jsou tedy báze

Chceme najít jinou bázi

Zvolme $(\lambda^n)_{n\geq 0}$

Pro které $\lambda \in \mathbb{C}$ je $(\lambda^n)_{n\geq 0} \in M$?

Dosadíme do rekurence

$\lambda^{n+2} - \lambda^{n+1} - \lambda^n = 0 \quad \forall n \in \mathbb{N}$

$\lambda^n(\lambda^2 - \lambda - 1) = 0$

předpokládáme, že $\lambda \neq 0$, neboť to je triviální

$P(\lambda) = \lambda^2 - \lambda - 1$ charakteristický polynom rekurence

$P(\lambda) = 0$ charakteristická rovnice

$\lambda^2 - \lambda - 1 = 0 \Rightarrow \lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$

$(\lambda^n)_{n\geq 0} \in M \Leftrightarrow \lambda = 0$ nebo $\lambda = \frac{1\pm\sqrt{5}}{2}$

dostáváme tedy posloupnosti $\left(\left(\frac{1+\sqrt{5}}{2}\right)^n\right)_{n\geq 0}$ a $\left(\left(\frac{1-\sqrt{5}}{2}\right)^n\right)_{n\geq 0}$

Ověříme, že jsou LN, pak bude jasné, že tvoří bázi

$\alpha\left(\left(\frac{1+\sqrt{5}}{2}\right)^n\right) + \beta\left(\left(\frac{1-\sqrt{5}}{2}\right)^n\right) = (0^n) \overset{?}{\Rightarrow} \alpha = \beta = 0$

zvolme $n=0$ a $n=1$: $\left.\begin{array}{l}\alpha + \beta = 0 \\ \alpha\frac{1+\sqrt{5}}{2} + \beta\frac{1-\sqrt{5}}{2} = 0\end{array}\right\} \Rightarrow \alpha = \beta = 0$ LN

nebo:

$\alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n = 0$

$\lim_{n\to+\infty}$: $\alpha > 0$: $LS = +\infty$ $\quad$ Lim PS = 0

$\alpha < 0$: $LS = -\infty$

to už implikuje, že $\alpha = 0 \Rightarrow \beta = 0$

Fibonacciho posloupnost $(F_n)_{n\geq 0}$ je LK $\left(\left(\frac{1+\sqrt{5}}{2}\right)^n\right)_{n\geq 0}, \left(\left(\frac{1-\sqrt{5}}{2}\right)^n\right)_{n\geq 0}$

$\exists \alpha, \beta \in \mathbb{C}: F_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n$

Najdeme α, β z počátečních podmínek

$F_0 = 0 = \alpha + \beta$

$F_1 = 1 = \alpha\frac{1+\sqrt{5}}{2} + \beta\frac{1-\sqrt{5}}{2}$

$\alpha = -\beta$

$2 = \alpha(1+\sqrt{5}) + \beta(1-\sqrt{5})$

$2 = -\beta(1+\sqrt{5}) + \beta(1-\sqrt{5})$

$\Rightarrow \beta = -\frac{1}{\sqrt{5}} \Rightarrow \alpha = \frac{1}{\sqrt{5}}$

$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

$$\underbrace{a_{n+k} + \alpha_{k-1}(n)\, a_{n-k+1} + \ldots + \alpha_1(n) a_{n+1} + \alpha_0(n) a_n}_{A(a_n)_{n\geq 0} := (a_{n+k} + \ldots + \alpha_0(n) a_n)} = 0, \quad (a_n)_{n\geq 0} \in l$$

$A : l \to l$

$A \in \mathcal{L}(l)$

$A\vec{x} = \vec{0} \iff \vec{x} \in \ker A$

$A\vec{x} = \vec{a} \iff \vec{x} \in \vec{a} + \ker A$, kde $\vec{a}$ je partikulární řešení

Linearita A:

$(\forall \beta \in \mathbb{C})(\forall (a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in l)(A(\beta (a_n)_{n\geq 0} + (b_n)_{n\geq 0}) = \beta A(a_n)_{n\geq 0} + (b_n)_{n\geq 0})$

Důkaz:

$$(\beta a_{n+k} + b_{n+k}) + (\beta \alpha_{k-1}(n) a_n + \alpha_{k-1}(n) b_n) + \ldots + (\beta \alpha_0(n) a_n + \alpha_0(n) b_n) =$$
$$= \beta (a_{n+k} + \alpha_{k-1}(n) a_{n+k-1} + \ldots + \alpha_0(n) a_n) + (b_{n+k} + \alpha_{k-1}(n) b_{n+k-1} + \ldots + \alpha_0(n) b_n)$$

$M = \{(a_n)_{n\geq 0} \in l \mid A(a_n)_{n\geq 0} = (0)_{n\geq 0}\} = \ker A$

Chceme popsat $\ker A$

Zvolíme $\underbrace{(1, 0, 0, \ldots, 0}_{k\text{-volím}}, \underbrace{*, *, \ldots}_{dopočítám}) =: e_1 \in \ker A$

$(0, 1, 0, \ldots, 0, *, *, \ldots) =: e_2 \in \ker A$

$\vdots$

$(0, 0, 0, \ldots, 1, *, *, \ldots) =: e_k \in \ker A$

$$\sum_{i=1}^{k} \alpha_i e_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k, *, *, \ldots) = (0, 0, 0, \ldots, 0, \ldots) \Rightarrow$$

$$\Rightarrow (\forall i \in \hat{k})(\alpha_i = 0)$$

$e_1, \ldots, e_k$ jsou LN $\Rightarrow \dim \ker A \geq k$

Zvolme $(x_n)_{n\geq 0} \in \ker A$ libovolně

$(x_n)_{n\geq 0} = (\underbrace{x_1, x_2, x_3, \dots, x_k}_{\text{poč. podmínky}}, *, *, \dots)$

Lze vyjádřit $(x_n)_{n\geq 0}$ jako LK $e_1, \dots, e_k$?

Tj.: $(x_n)_{n\geq 0} = \sum_{i=1}^{k} \alpha_i e_i = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k, *, *, \dots)$

Zřejmě stačí zvolit $\alpha_i = x_i$ pro všechna $i \in \hat{k}$ a potom se shodují počáteční podmínky, tedy i všechny následující členy musí být nutně shodné

$\Rightarrow \dim \ker A \leq k$

To celkově znamená, že $\dim \ker A = k$.

Hledáme báze ve tvaru $(\lambda^n)_{n\geq 0}$ a ptáme se pro které $\lambda \in \mathbb{C}$ je $(\lambda^n)_{n\geq 0} \in \ker A$.

$\forall n \geq 0 : \lambda^{n+k} + \alpha_{k-1}(n)\lambda^{n+k-1} + \dots + \alpha_0(n)\lambda^n = 0$

$\lambda \neq 0 \wedge \alpha_i(n) = \alpha_i$ pro všechna $i \in \hat{n}$, pak

$\underbrace{\lambda^k + \alpha_{k-1}\lambda^{k-1} + \dots + \alpha_0 \neq 0}$

$P(\lambda)$ - charakteristický polynom rekurence

Posloupnost $(\lambda^n)_{n\geq 0}$ pro $\lambda \in \mathbb{C} - \{0\}$ patří do $\ker A$ právě tehdy když λ je kořen charakteristického polynomu $P(\lambda)$

I. Nechť $P(\lambda)$ má k různých jednoduchých kořenů $\lambda_1, \dots, \lambda_k \in \mathbb{C} \setminus \{0\}$
Pak $(\lambda_1^n)_{n\geq 0}, \dots, (\lambda_k^n)_{n\geq 0} \in \ker A$

Důkaz:
Prostor je jich k, tak stačí ověřit LN
Máme rovnici

$$\alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n + \dots + \alpha_k \lambda_k^n = 0, \quad \forall n \in \mathbb{N}_0$$

a chceme ukázat, že nutně $\alpha_1 = \alpha_2 = \dots = \alpha_k = 0$

$n=0$: $\alpha_1 + \alpha_2 + \dots + \alpha_k = 0$
$n=1$: $\alpha_1\lambda_1 + \alpha_2\lambda_2 + \dots + \alpha_k\lambda_k = 0$
$\vdots$
$n=k-1$: $\alpha_1\lambda_1^{k-1} + \alpha_2\lambda_2^{k-1} + \dots + \alpha_k\lambda_k^{k-1} = 0$

Označme matici soustavy $A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \dots & \lambda_k \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \lambda_3^{k-1} & \dots & \lambda_k^{k-1} \end{pmatrix}$

$\det A = \prod_{1\leq i<j\leq k} (\lambda_i - \lambda_j) \neq 0$, neboť jsou to různé kořeny

a proto existuje jenom triviální řešení této soustavy.

Každou posloupnost $(x_n)_{n\geq 0} \in \ker A$ lze napsat jako
$(x_n)_{n\geq 0} = \alpha_1 (\lambda_1^n)_{n\geq 0} + \dots + \alpha_k (\lambda_k^n)_{n\geq 0}$
$\Leftrightarrow x_n = \alpha_1 \lambda_1^n + \dots + \alpha_k \lambda_k^n, \forall n \geq 0$

Koeficienty $\alpha_1, \dots, \alpha_k$ dopočítáme z počátečních podmínek

I. Nechť $P(\lambda)$ má kořeny $\lambda_1, \dots, \lambda_l \in \mathbb{C}$ i s násobnostmi $j_1, \dots, j_l$, $l \leq k$ a platí, že $\sum_{i=1}^{l} j_i = k$

Věta
Nechť (λ^n) je řešením lineární diferenční rovnice $x^{n+k} + \alpha_{k-1} x^{n+k-1} + \dots + \alpha_0 x^n = 0$ s násobností j_i.
Pak i $(n\lambda^n), \dots, (n^{j-1}\lambda^n)$ je řešením této rovnice.

Důkaz
$P(\lambda)$ je charakteristický polynom
$P(\lambda) = \lambda^k + \alpha_{k-1}\lambda^{k-1} + \dots + \alpha_0 = 0$
$\lambda^n(P(\lambda)) = \lambda^{n+k} + \alpha_{k-1}\lambda^{n+k-1} + \dots + \alpha_0\lambda^n = 0$
$\lambda(\lambda^n(P(\lambda)))' = (n+k)\lambda^{n+k} + \alpha_{k-1}(n+k-1)\lambda^{n+k-1} + \dots + \alpha_0 n\lambda^n = 0$
$\lambda(\lambda(\lambda^n(P(\lambda)))')' = (n+k)^2\lambda^{n+k} + \alpha_{k-1}(n+k-1)^2\lambda^{n+k-1} + \dots + \alpha_0 n^2\lambda^n = 0$
$\vdots$
$(n+k)^{j-1}\lambda^{n+k} + \alpha_{k-1}(n+k-1)^{j-1}\lambda^{n+k-1} + \dots + \alpha_0 n^{j-1}\lambda^n = 0$

Mějme diferenční rovnici k-tého řádu,

(*) $a_{n+k} + \alpha_{k-1} a_{n+k-1} + \dots + \alpha_1 a_1 + \alpha_0 a_n = 0, \quad n \geq 0$

$P(\lambda) = \lambda^k + \alpha_{k-1}\lambda^{k-1} + \dots + \alpha_1 \lambda + \alpha_0 = 0$ charakteristický polynom

Obecné řešení (*) je ve tvaru $a_n = \sum_{i=1}^{l} \lambda_i^n \cdot p_i(n), \quad n \geq 0,$

kde $\lambda_1, \dots, \lambda_l$ jsou různé kořeny char. polynomu násobnosti $j_1, \dots, j_l$ a $p_1(n), \dots, p_l(n)$ jsou polynomy stupňů $j_1 - 1, \dots, j_l - 1$

Pozn. $\sum_{i=1}^{l} j_i = k, \quad 1 \leq l \leq k$

Př. $a_{n+2} + 2a_{n+1} + 4a_n = 0, \quad a_0 = a_1 = 1$

$P(\lambda) = \lambda^2 + 2\lambda + 4 = 0$

$\lambda_{1,2} = \frac{-2 \pm \sqrt{4-16}}{2} = -1 \pm i\sqrt{3}$

$a_n = \alpha(-1+i\sqrt{3})^n + \beta(-1-i\sqrt{3})^n$

$n = 0: \; a_0 = 1 = \alpha + \beta$

$n = 1: \; a_1 = 1 = \alpha(-1+i\sqrt{3}) + \beta(-1-i\sqrt{3})$

$1 = \alpha(-1+i\sqrt{3}) + (1-\alpha)(-1-i\sqrt{3}) = \alpha(2i\sqrt{3}) - (1+i\sqrt{3})$

$\alpha = \frac{2+i\sqrt{3}}{2i\sqrt{3}} = \frac{-2i\sqrt{3}+3}{6} \Rightarrow \beta = \frac{3+2i\sqrt{3}}{6}$

$a_n = \frac{3-2i\sqrt{3}}{6}(-1+i\sqrt{3})^n + \frac{3+2i\sqrt{3}}{6}(-1-i\sqrt{3})^n, \quad n \geq 0$

$a_n = 2\,\mathrm{Re}\left(\frac{3-2i\sqrt{3}}{6}(-1+i\sqrt{3})^n\right)$

$-1+i\sqrt{3} = 2\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 2\cdot\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$

$(-1+i\sqrt{3})^n = 2^n\left(\cos n\frac{2\pi}{3} + i\cdot\sin n\frac{2\pi}{3}\right)$

$$2\,\mathrm{Re}\left(\tfrac{1}{2}-\tfrac{1}{3}i\sqrt{3}\right)\left(2^n\cos\tfrac{2\pi}{3}n+i2^n\sin\tfrac{2\pi}{3}n\right)=$$
$$=\tfrac{1}{2}\,2^n\cos\tfrac{2\pi}{3}n+\tfrac{\sqrt{3}}{3}2^{n+1}\sin\tfrac{2\pi}{3}n=a_n,\ \forall n\geq 0$$

Pozn.: Polynom s reálnými koeficienty má s komplexním kořenem $\lambda_0\in\mathbb{C}\setminus\mathbb{R}$ i kořen λ_0 stejné násobnosti

$$P(\lambda_0)=0$$
$$\lambda_0^k+\alpha_{k-1}\lambda_0^{k-1}+\ldots+\alpha_0=0$$
$$\bar{\lambda}_0^k+\alpha_{k-1}\bar{\lambda}_0^{k-1}+\ldots+\alpha_0=0$$

$$P(x)=(x-\lambda_0)(x-\bar{\lambda}_0)\tilde{P}(x)$$
$$P(x)=(x^2-2\mathrm{Re}\,\lambda_0\,x+|\lambda_0|^2)(\tilde{P}(x))$$
když P má reálné koeficienty, tak $\tilde{P}$ taky

$$(\lambda_0^n)_{n\geq 0},\ (\bar{\lambda}_0^n)_{n\geq 0}\ \text{konv.}$$

$$\underbrace{\left(\frac{\lambda_0^n+\bar{\lambda}_0^n}{2}\right)_{n\geq 0}}_{(\mathrm{Re}(\lambda_0^n))_{n\geq 0}},\ \underbrace{\left(\frac{\lambda_0^n-\bar{\lambda}_0^n}{2i}\right)_{n\geq 0}}_{(\mathrm{Im}(\lambda_0^n))_{n\geq 0}}\ \text{konv.}$$

$$\lambda_0=|\lambda_0|(\cos\varphi+i\sin\varphi)$$
$$\lambda_0^n=|\lambda_0|^n(\cos n\varphi+i\sin n\varphi)$$

$$(|\lambda_0|^n\cos n\varphi)_{n\geq 0},\ (|\lambda_0|^n\sin n\varphi)_{n\geq 0}$$

Kdyby $\lambda_0, \bar{\lambda}_0$ měly násobnost f_0:

$(\lambda_0^n), (n\lambda_0^n), \dots, (n^{f_0-1}\lambda_0^n), (\bar{\lambda}_0^n), \dots, (n^{f_0-1}\bar{\lambda}_0^n)$

$$a_n = \lambda_0^n \underbrace{p_0(n)}_{\text{stupeň } f_0-1} + \bar{\lambda}_0^n \underbrace{\tilde{p}_0(n)}_{\text{stupeň } f_0-1}$$

po prvních jsou v bázi posloupnosti k sobě komplexně sdružené

$$= (n\lambda_0^n), (n\bar{\lambda}_0^n)$$
$$\Leftrightarrow (Re(n\lambda_0^n)), (Im(n\bar{\lambda}_0^n)$$
$$\Leftrightarrow (n|\lambda_0|^n \cos n\varphi), (n|\lambda_0|^n \sin n\varphi)$$

Platí

Má-li $P(\lambda)$ reálné koeficienty, pak obecné řešení (a_n) je ve tvaru

$$a_n = \sum_{i=1}^{l} \lambda_i^n p_i(n) + \sum_{j=1}^{m} |\mu_j|^n q_j(n) \cdot \cos n\varphi_j + \sum_{j=1}^{m} |\mu_j|^n \tilde{q}_j(n) \cdot \sin n\varphi_j$$

$\lambda_1, \dots, \lambda_l \in \mathbb{R}$, $\mu_1, \bar{\mu}_2, \dots, \mu_m, \bar{\mu}_m \in \mathbb{C}$ jsou kořeny $P(\lambda)$ násobnosti $f_1, \dots, f_l$, a $\delta_1, \delta_1, \dots, \delta_m, \delta_m$ a platí

$$\sum_{i=1}^{l} f_i + 2\sum_{j=1}^{m} \delta_i = k$$

Polynomy p_i jsou stupně $f_i - 1$, polynomy $q_j, \tilde{q}_j$ jsou stupně $\delta_j - 1$, $\forall i \in \hat{l}, \forall j \in \hat{m}$

Nehomogenní diferenční rovnice

$$a_{n+k} + \alpha_{k-1} a_{n+k-1} + \dots + \alpha_1 a_1 + \alpha_0 a_n = f(n)$$

Celkové řešení je $a + \ker A$,
kde a je partikulární řešení

Př) $a_{n+2} - 3a_{n+1} + 2a_n = 1 \quad (\Delta)$

$$\oplus \quad \underline{a_{n+3} - 3a_{n+2} + 2a_{n+1} = 1}$$

$$a_{n+3} - 4a_{n+2} + 5a_{n+1} - 2a_n = 0 \quad (\square)$$

Každé řešení (Δ) je řešení $(\square)$

Řešíme $(\square)$: $\lambda^3 - 4\lambda^2 + 5\lambda - 2 = (\lambda-1)(\lambda-2)(\lambda-1)$

Obecné řešení $(\square)$: $a_n = \alpha 1^n + \beta n 1^n + \gamma \cdot 2^n, \ n \geq 0$

$$a_n = (\alpha + \beta n) + \gamma \cdot 2^n$$

Dosadíme do (Δ):

$$\underbrace{\alpha + \beta(n+2) + \gamma \cdot 2^{n+2}}_{a_{n+2}} - 3\underbrace{(\alpha + \beta(n+1) + \gamma 2^{n+1})}_{a_{n+1}} + 2\underbrace{(\alpha + \beta n + \gamma \cdot 2^n)}_{a_n} = 1$$

$$\alpha \underbrace{(1-3+2)}_{=0} + \beta \underbrace{(n+2-3(n+1)+2n)}_{=-1} + \gamma \underbrace{(2^{n+2} + 3 \cdot 2^{n+1} + 2^n)}_{=0} = 1$$

$\Rightarrow \beta = -1$, α, γ libovolné

$a_n = \alpha - n + \gamma \cdot 2^n$ je obecné řešení (Δ)

$a_n = \underbrace{\alpha + \gamma \cdot 2^n}_{\ker A} \underbrace{- n}_{a}$ ... partikulární řešení

$$P(\lambda): \quad \lambda^{n+2} - 3\lambda^{n+1} + 2\lambda^n = \lambda^n(\lambda^2 - 3\lambda + 2) = 0$$

$$\lambda^{n+3} - 3\lambda^{n+2} + 2\lambda^{n+1} = \lambda^{n+1}(\lambda^2 - 3\lambda + 2) = 0$$

$$\lambda^n(\lambda - 1)(\lambda^2 - 3\lambda + 2) = 0$$

$c_i \in \mathbb{C}$

(♡)

$\forall n \in \mathbb{N}$, $a_{n+k} + \alpha_{k-1} a_{n+k-1} + \dots + \alpha_0 a_n = f(n) = c_0 + c_1 n + \dots + c_t n^t$, $t \in \mathbb{N}_0$

$a_{n+k+1} + \alpha_{k-1} a_{n+k} + \dots + \alpha_0 a_{n+1} = f(n+1) = c_0 + c_1(n+1) + \dots + c_t (n+1)^t$

odečteme: lineární $a_{n+k-1}, \dots, a_n$

char. pol.: $(\lambda - 1)(P(\lambda)) = 0$ $\Leftrightarrow$ $f(n+1) - f(n) = \tilde{c}_0 + \tilde{c}_1 n + \dots + \tilde{c}_{t-1} n^{t-1}$

polynom stupně $t-1$

provedu $t+1$ krát char. polynom: $(\lambda - 1)^{t+1} P(\lambda) = 0$

dif. rovnice $k+1+1$ řádu homogenní (♡)

Každé řešení (♡) je řešení (♡)

Řešení (♡) je LK posloupností

$(1^n), (n 1^n), \dots, (n^{s-1} 1^n), (n^s 1^n), \dots, (n^{s+t} 1^n)$

$(\lambda_2^n), (n \lambda_2^n), \dots, (n^{s-1} \lambda_2^n)$

part. s. řešení

řešení $P(\lambda)$ (ker A)

Partikulární řešení k pravé straně $f(n)$ je polynom stupně $t \in \mathbb{N}_0$, je tvaru $b_n = d_0 n^s + d_1 n^{s+1} + \dots + d_t n^{s+t} = n^s \cdot Q(n)$

kde s je násobnost kořene $\lambda = 1$ v char. polynomu ♡

$Q(n)$ polynom stupně t

Koeficienty polynomu $Q(n)$ zjistím dosazením do (♡) a porovnáním stran

Kvazi polynomiální pravá strana

$$a_{n+k} + \alpha_{k-1} a_{n+k-1} + \dots + \alpha_1 a_{n+1} + \alpha_0 a_n = f(n)$$

$$f(n) = k^n (c_0 + c_1 n + \dots + c_\ell n^\ell)$$
$$f(n+1) = k^{n+1} (c_0 + c_1 (n+1) + \dots + c_\ell (n+1)^\ell)$$

Posunu index $n \to n+1$ a odečtu od $n+1$ k-násobek n-tého na pravé straně: k^n polynom stupně $\ell - 1$

Opakuji $\ell + 1$ - krát

$$(\lambda - k)^{\ell+1} \cdot P(\lambda)$$

Každé řešení původní rovnice je řešením homogenní rovnice s char. polynomem $(\lambda - k)^{\ell+1} P(\lambda)$. Nenapak

$P(\lambda)$ má kořeny $\lambda = k$ s násobností $r \geq 0$ a $\lambda_i \in \mathbb{C} \setminus \{0, k\}$ násobnost μ_i

$(\lambda - k)^{\ell+1} P(\lambda)$ má kořeny $\lambda = k$ násobnost $r + \ell + 1$
$\lambda_i \in \mathbb{C} \setminus \{0, k\}$

$\lambda = k$: $(k^n)_{n\geq 0}, (n k^n)_{n\geq 0}, \dots, (n^{r-1} k^n)_{n\geq 0}, (n^r k^n)_{n\geq 0}, \dots, (n^{r+\ell} k^n)_{n\geq 0}$
$(\lambda_i^n)_{n\geq 0}, (n\lambda_i^n)_{n\geq 0}, \dots, (n^{\mu_i - 1} \lambda_i^n)_{n\geq 0}$

LK těchto posloupností je řešením původní rovnice bez pravé strany

Partikulární řešení je ve tvaru LK posloupností $(n^r k^n)_{n\geq 0}, \dots, (n^{r+\ell} k^n)_{n\geq 0}$.

$$a_n^p = d_0 \cdot n^r k^n + d_1 n^{r+1} k^n + \dots + d_\ell n^{r+\ell} k^n =$$
$$= n^r k^n (d_0 + d_1 n + \dots + d_\ell n^\ell) = n^r k^n q(n),$$
kde $q(n)$ je polynom stupně ℓ v proměnné n

Nemohmy polynom $q(n)$ zjistím dosazením a_n^p do původní rovnice a porovnáním stran.

Př. $a_{n+2} - 4a_{n+1} + 4a_n = 2^n(n+3)$

$a_n = a_n^h + a_n^p$

a_n^h: $\lambda^2 - 4\lambda + 4 = (\lambda-2)^2$

$a_n^h = \alpha \cdot 2^n + \beta \cdot n 2^n$

$a_n^p = n^r k^n q(n)$, $k=2$, $r=2$, $\epsilon = 1$

$a_n^p = n^2 2^n q(n) = n^2 2^n (d_0 + d_1 n)$

$(n+2)^2 \cdot 2^{n+2}(d_0 + d_1(n+2)) - 4[(n+1)^2 2^{n+1}(d_0 + d_1(n+1))] + 4[n^2 2^n (d_0 + d_1 n)] = 2^n(n+3)$

$4(n^2+4n+4)(d_0 + d_1 \cdot 2 + d_1 n) - 8(n^2+2n+1)(d_0 + d_1 + d_1 n) + 4n^2(d_0 + d_1 n) = n+3$

n^3: $4d_1 - 8d_1 + 4d_1 = 0$

n^2: $4d_0 + 8d_1 + 16d_1 - 8d_0 - 8d_1 - 16d_1 + 4d_0 = 0$

n^1: $16d_0 + 32d_1 + 16d_1 - 16d_0 - 16d_1 - 8d_1 = 1 \Leftrightarrow d_1 = \frac{1}{24}$

n^0: $16d_0 + 32d_1 - 8d_0 - 8d_1 = 3 \Leftrightarrow d_0 = \frac{1}{4}$

$a_n^p = n^2 2^n \left(\frac{1}{4} + \frac{1}{24} n\right)$

$a_n = \alpha \cdot 2^n + \beta n 2^n + n^2 2^n \left(\frac{1}{4} + \frac{1}{24} n\right)$

Pravá strana tvaru $f(n) = k^n g(n) \cos(n\varphi)$, resp. $k^n g(n) \sin(n\varphi)$

Př: $a_{n+1} - 2a_n = \sqrt{2}^n n \cdot \cos\frac{n\pi}{4}$

$b_{n+1} - 2b_n = \sqrt{2}^n n \cdot \sin\frac{n\pi}{4} \quad / \cdot i$

$\oplus \quad \underbrace{a_{n+1} + i b_{n+1}}_{c_{n+1}} - 2\underbrace{(a_n - i b_n)}_{c_n} = \sqrt{2}^n \cdot n\left(\cos\frac{n\pi}{4} + i \sin\frac{\pi}{4}\right)$

$c_{n+1} - 2c_n = n\left(\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)^n\right)$

$c_{n+1} - 2c_n = n(1+i)^n$

$c_n = c_n^h + c_n^p$

$c_n^h = \alpha \cdot 2^n$

$c_n^p = n^r \cdot k^n g(n), \; k = 1+i, \; r = 0, \; t = 1$

$c_n^p = (1+i)^n (d_0 + d_1 n)$

$(1+i)^{n+1}(d_0 + d_1(n+1)) - 2(1+i)^n(d_0 + d_1 n) = n(1+i)^n$

$(1+i)(d_0 + d_1 + d_1 n) - 2(d_0 + d_1 n) = n$

$n^1: \; d_1 + i d_1 - 2d_1 = 1 \Rightarrow d_1 = \frac{1}{i-1} = -\frac{+1+i}{2}$

$n^0: \; (1+i)(d_0 + d_1) - 2d_0 = 0 \Rightarrow$

$d_0(i-1) + d_1(i+1) = 0$

$d_0 = -\frac{d_1(i+1)}{i-1} = \frac{-i+1}{(i-1)^2} = +\frac{i+1}{2i} = \frac{1-i}{2}$

$c_n = \underbrace{\alpha}_{(\beta + i\gamma)} \cdot 2^n + (1+i)^n\left(\frac{1-i}{2} - n\frac{1+i}{2}\right)$

$Re(c_n) = a_n = \beta \cdot 2^n + Re\left(\left(\sqrt{2}\left(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4}\right)\right)^n\left(\frac{1-i}{2} - n\frac{1+i}{2}\right)\right) =$

$= \beta \cdot 2^n + \sqrt{2}^n \cdot \cos\left(n\frac{\pi}{4}\right)\left(\frac{1}{2} - \frac{n}{2}\right) + \sqrt{2}^n \sin\left(\frac{n\pi}{4}\right)\left(\frac{1}{2} + \frac{n}{2}\right)$

Superpozice partikulárního řešení

$$A\vec{x} = \vec{b}_1 + \vec{b}_2$$
$$x \in \ker A + \vec{a}_1 + \vec{a}_2$$

Racionální kořeny polynomů s celočíselnými koeficienty

Věta: Polynom $f(x) = \sum_{i=0}^{k} a_i x^i$, $a_i \in \mathbb{Z}$, $a_k \neq 0 \neq a_0$ kořen $\frac{p}{q} \in \mathbb{Q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $p \perp q$, pak $p \mid a_0$, $q \mid a_k$

Př: $f(x) := x^4 - 4x^2 + x + 2$

$p \mid 2$, $q \mid 1$ $\Rightarrow$ $p \in \{\pm 1, \pm 2\}$, $q \in \{1\}$

$f(1) = 0$
$f(-1) \neq 0$
$f(2) \neq 0$
$f(-2) = 0$

$f(x) = (x-1)(x-2)(x^2 - x - 1)$

Důkaz:

$$f\left(\frac{p}{q}\right) = 0 = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0 = 0 \quad / q^n$$

$$0 = a_n p^n + a_{n-1} q p^{n-1} + \dots + a_1 q^{n-1} p + a_0 q^n$$
$$0 = a_n p^n + q \underbrace{(a_{n-1} + \dots + a_1 q^{n-2} p + a_0 q^{n-1})}_{\in \mathbb{Z}}$$

$\Rightarrow q \mid a_n p^n$ a $p \perp q \Rightarrow q \mid a_n$

Př. $G(x) = 3x^4 + 5x^3 + x^2 + 5x + 2$

$a_0 = -2, \; a_4 = 3$

$p \mid 2 \Rightarrow p \in \{\pm 1, \pm 2\}$

$q \mid 3 \Rightarrow q \in \{1, 3\}$

$\Rightarrow \frac{p}{q} \in \{\pm 1, \pm 2, \pm \frac{1}{3}, \pm \frac{2}{3}\}$

$G(\frac{p}{q}) \stackrel{?}{=} 0$

Hornerovo schéma

$G(x) = -2 + x(5 + x(1 + x(5 + 3x))) \Rightarrow G(\frac{1}{3}) = 0$

$5 + 3x = 6$

$1 + x \cdot 6 = 3$

$5 + x \cdot 3 = 6$

$-2 + x \cdot 6 = 0$

	3	5	1	5	-2
$\frac{1}{3}$	3	6	3	6	0

koeficienty polynomu vydělného kořenem $x = \frac{1}{3}$

$G(x) = (x - \frac{1}{3})(3x^3 + 6x^2 + 3x + 6) =$

$= (x - \frac{1}{3})(x^2(3x + 6) + (3x + 6)) =$

$= (x - \frac{1}{3})(3x + 6)(x^2 + 1) =$

$= 3(x - \frac{1}{3})(x + 2)(x + i)(x - i)$

Josefův problém

n-lidí v kruhu, škrtáme každého druhého

$J(n) = ?$ pozice přeživšího

n 1

2

3

4

5

6

7

$J(1) = 1$

$J(2) = 1$ $\binom{1}{2}$

$J(3) = 3$ 3 1 2

$J(4) = 1$ 4 1 2 3

$J(5) = 3$ 5 1 2 4 3

$J(6) = 5$

$J(7) = 7$

$J(8) = 1$

$J(2^k) = 1$

$J(2^k + l) = 1 + 2l, \; 0 \le l \le 2^k - 1$

$J(2n) = 2J(n) - 1$

~~2n~~ 1

2n-1 ~~2~~

~~2n-2~~ 3 → 2

~~4~~

5 → 3

~~6~~

7 → 4

Po 1 průchodu vyškrtáme n lidí, zbyde n

přejmenuje 1, …, n, počítám od 1

V novém značení přežije $J(n)$

ve starém značení $2J(n) - 1$

$J(2n+1) = 2J(n) + 1$

n ~~1~~

2n+1 ~~2~~

n-1 ~~2n~~

2n-1 3 → 1

~~n-2~~ ~~4~~

5 → 2

~~6~~

7 → 3

Po vyškrtání sudých zbyde n+1 lidí, tak škrtu ještě číslo 1, zbyde n lidí počítám od 3

$J(1) = 1$

$J(2n) = 2J(n) - 1$

$J(2n+1) = 2J(n) + 1$

Dk hypotézy indukcí

$n = 2^k + l,\ k \in \mathbb{N}_0,\ 0 \le l \le 2^k - 1$

$k \ge 1$: $2l+1 = J(n) = J(2^k + l) =$ a) l sudé $= 2\underbrace{J(2^{k-1} + \frac{l}{2})}_{2(\frac{l}{2})+1} - 1 =$

$\overset{IP}{=} 2(l+1) - 1 = 2l+1$

$=$ b) l liché $= 2\underbrace{J(2^{k-1} + \frac{l-1}{2})}_{2(\frac{l-1}{2})+1} + 1 = 2l+1$

$k = 0$: $n = 2^k + l = 1$ $\quad k=0,\ l=0$

$J(1) = 2l+1 = 1$

Řešení ve dvojkové soustavě

$n = \sum_{j=0}^{k} b_j 2^j = (b_k b_{k-1} \dots b_1 b_0)_2$, $\quad b_k = 1$

$b_j \in \{0; 1\}$

$J((b_k b_{k-1} \dots b_1 b_0)_2) = 2l+1 = (b_{k-1} b_{k-2} \dots b_1 b_0 0)_2 + 1 =$
$= (b_{k-1} b_{k-2} \dots b_1 b_0 1)$

Z rekurence

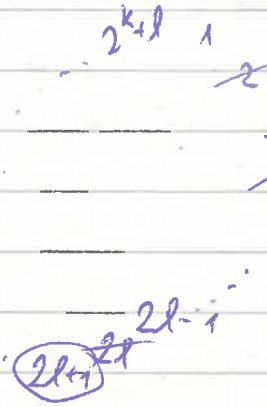
$J(b_k b_{k-1} \dots b_1 0) = 2J(b_k b_{k-1} \dots b_1) + 1$
$J(b_k b_{k-1} \dots b_1 1) = 2J(b_k b_{k-1} \dots b_1) + 1$

$J(b_k b_{k-1} \dots b_1 b_0) = 2J(b_k b_{k-1} \dots b_1) - (-1)^{b_0}$

Jinak na Josefa

$J(2^k) = 1$ vidět ISV (i slepý vidí)

$J(2^k + l)$



1. Zobecnění

$J(1) = \alpha$

$J(2n) = 2J(n) + \beta_0$

$J(2n+1) = 2J(n) + \beta_1$

$J(b_k b_{k-1} \dots b_1 b_0) = 2J(b_k b_{k-1} \dots b_1) + \beta_{b_0} =$

$= 2(2J(b_k b_{k-1} \dots b_2) + \beta_{b_1}) + \beta_{b_0} =$

$= 2^2 J(b_k b_{k-1} \dots b_2) + 2\beta_{b_1} + \beta_{b_0} =$

$= 2^2(2J(b_k \dots b_3) + \beta_{b_2}) + 2\beta_{b_1} + \beta_{b_0} =$

$= 2^3 J(b_k \dots b_3) + 2^2\beta_{b_2} + 2\beta_{b_1} + \beta_{b_0} =$

$= 2^k \underbrace{J(b_k)}_{\alpha} + 2^{k-1}\beta_{b_{k-1}} + \dots + 2^1\beta_{b_1} + 2^0\beta_{b_0}$

$J(b_k \dots b_0) = 2^k\alpha + \sum_{j=0}^{k-1} 2^j \beta_{b_j} = (\alpha, \beta_{k-1}, \beta_{k-2}, \dots, \beta_{b_1}, \beta_{b_0})_2$

2. zobecnění

$f(dn) = c f(n) + \beta_0$, $d \in \mathbb{N}$, $d \geq 2$
$f(dn+1) = c f(n) + \beta_1$ $\quad c \in \mathbb{C}$
$\vdots$ $\qquad \beta_0, \dots, \beta_{d-1} \in \mathbb{C}$
$f(dn+d-1) = c f(n) + \beta_{d-1}$ $\quad \alpha_1, \dots, \alpha_{d-1} \in \mathbb{C}$

$f(1) = \alpha_1$
$f(2) = \alpha_2$
$\vdots$
$f(d-1) = \alpha_{d-1}$

Řešení: $f((r_k r_{k-1} \dots r_1 r_0)_d) = c f((r_k \dots r_1)_d) + \beta_{r_0} =$

$= \dots = c^k \cdot \alpha_{r_k} + c^{k-1} \beta_{r_{k-1}} + c^{k-2} \beta_{r_{k-2}} + \dots + c^1 \beta_{r_1} + c^0 \beta_{r_0} =$

$= (\alpha_{r_k}, \beta_{r_{k-1}}, \beta_{r_{k-2}}, \dots, \beta_{r_1}, \beta_{r_0})_c$

$G_n := \{1, \ldots, n-1\}$, $n \in \mathbb{N}$

definuji operaci násobení mod n

$x, y \in G_n \quad x \otimes y = \underbrace{x \cdot y \bmod n}_{\text{zbytek}}$

a) G_n uzavřená na $\otimes$?

b) Pro které $x \in G_n$ $\exists y \in G_n : x \otimes y = 1$

ad a) $n \mid x \cdot y$

n prvočíslo: $x, y \in G_n$ $x \perp n$, $y \perp n$, nenásobné $\Rightarrow G_n$ uzavřená

n složené: v G_n existují $d \mid n$ tj. $d, \frac{n}{d} \in G_n$ $x \otimes y = 0$

$\Rightarrow G_n$ není uzavřená

ad b) $x \cdot y = 1 \bmod n$

$x \cdot y = 1 + kn$ asociace

$x \cdot y - kn = 1$, k daného $x \in G_n$ existuje právě $y \in G_n \Leftrightarrow x \perp n$

Grupy

Definice 1
Nechť G je množina a $\&: G \times G \to G$.
Pak $(G, \&)$ je grupa, když:

1. $x \& (y \& z) = (x \& y) \& z$, $\forall x, y, z \in G$
   asociativita
2. $\exists l \in G$ tak, že $l \& x = x \& l = x$, $\forall x \in G$
   neutrální prvek
3. $\forall x \in G \ \exists y \in G$ tak, že $x \& y = y \& x = l$
   zn.: $y = x^{-1}$, inverzní k x

Př. $\mathbb{Z}_p^* = \{1, \dots, p-1\}$, $\&$: násobení mod p
$l = 1$
$\forall x \in \mathbb{Z}_p^* : x \perp p \Rightarrow \exists x^{-1}$

$(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$
$\mathbb{Q}$ $\mathbb{Q} \setminus \{0\}$
$\mathbb{C}$ $\mathbb{C} \setminus \{0\}$
$\mathbb{H}$

Bijekce na $\mathbb{R}$, $G = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ bijekce}\}$
& skládání
$l = id$

Definice 1
Grupa G je Abelova, pokud $\forall x, y \in G$ platí $x \& y = y \& x$

Tabulka $(\mathbb{Z}_5^*, \cdot)$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(Př) $G = \{A \in \mathbb{R}^{2,2} \mid \det A \neq 0\}$, & násobení matic není Abelova

Definice
Nechť $(G, \&)$ je grupa a $G' \subset G$
Pak $(G', \&)$ je podgrupa, pokud $(G', \&)$ je grupa.

(Př) $(\mathbb{C} \setminus \{0\}, \cdot)$ má podgrupu $(\mathbb{R} \setminus \{0\}, \cdot)$
$(\mathbb{Z}, +)$ má podgrupu $(m\mathbb{Z}, +)$
$m \in \mathbb{Z}$

Věta
Je-li $(G, \&)$ konečná grupa a $(G', \&)$ její podgrupa, pak $\#G' \mid \#G$

Důkaz
Zavedeme značení $x \& y \equiv xy$

$\forall x \in G$ vezmeme $xG' = \{xu \mid u \in G'\}$
① $\forall x, y \in G \quad xG' \cap yG' = \emptyset$ nebo $xG' = yG'$
② $\#(xG') = \#G'$
③ $\forall y \in G \quad \exists x \in G : y \in xG'$

$G = \bigcup_{x \in G} xG'$, G je disjunktní sjednocení množin velikosti $\#G'$

ad 3) jasné, $x=y$: $y \in yG'$, neboť $y = y1 \in yG'$

ad 1) Vezmu $x, y \in G$ a předp. s průnikem $xG' \cap yG'$

$xz = yw$ pro $z, w \in G'$

$\underbrace{xzw^{-1}}_{\in G'} = yww^{-1} = y1 = y$

$\Rightarrow y \in xG'$

vezmu lib. prvek $t \in yG'$, $t = yr$, $r \in G'$

$t = x \cdot \underbrace{zw^{-1}r}_{\in G'}$

$\Rightarrow t \in xG'$

ad 2) $\#(xG') = \#G'$, $\forall x \in G$

- sestrojím bijekci: $G' \to xG'$

$z \to xz$

- musí být prostá a na

kdyby $z \neq w$ a $xz = xw$ / x^{-1}

$x^{-1}xz = x^{-1}xw$

$z = w$, spor

(Př) $G' = \{1, 4\}$

$x = 1$: $xG' = \{1, 4\}$

$x = 2$: $xG' = \{2, 3\}$

$x = 3$: $xG' = \{3; 2\}$

$x = 4$: $xG' = \{4; 1\}$

Definice

Je-li $(G, \&)$ grupa, pak řád grupy je $\# G$

Když $x \in G$ a $\exists k \in \mathbb{N}$ tak, že $\underbrace{x \& x \& \dots \& x}_{k\text{-krát}} =: x^k = e$, pak minimální k s touto vlastností je řád prvku x v G^*.

Pozn: Z asociativity je značení $x^k := x^{k-1} \& x$ dobře definovaný

Př) Řád prvku 1 v $\mathbb{Z}_5^*$: $r_1 = 1$

2 v $\mathbb{Z}_5^*$: $r_2 = 4$

3 v $\mathbb{Z}_5^*$: $r_3 = 4$

4 v $\mathbb{Z}_5^*$: $r_4 = 2$

V konečné grupě má každý prvek konečný řád

Dk) $x, x^2, x^3, x^4, \dots, \in G$

tj. $\exists k, l \in \mathbb{N}$ tak, že $x^k = x^l$, BÚNO $k > l$

aplikuji l-krát x^{-1}: $x^{k-l} = e$

Platí: Je-li $(G, \&)$ konečná grupa a $x \in G$, pak $\{x, x^2, \dots, x^r = e\}$ s polu s $\&$ je podgrupa $(G^*, \&)$

Dk) • uzavřenost na $\&$ $x^j \cdot x^l = \underbrace{x^j \cdot x^{r-j}}_{e} \cdot r^{l-(r-j)} \in \{x, x^2, \dots, x^r\} = G'$

$j, l \in \{1, \dots, r\}$

• inverze: $(x^j)^{-1} \in G'$?

$x^{r-j} x^j = x^r = e$ pro $j < r$

$x^r = e = e^{-1}$ $j = r$

Důsledek

Řád každého prvku konečné grupy dělí řád grupy.

$\# G' = r \mid \# G$

Definice
Grupa $(G, \circ)$ je cyklická, pokud existuje prvek $x \in G$ tak, že $G = \{x, x^2, \dots, x^n = e\}$
Prvek x je generátor.

Př. 2 je generátor grupy $(\mathbb{Z}_5^*, \cdot)$
3 je generátor grupy $(\mathbb{Z}_5^*, \cdot)$

$(\mathbb{Z}_{17}^*, \cdot)$ je grupa, 3 je generátor $(\mathbb{Z}_{17}^*, \cdot)$
3^k je generátor, pokud $k \perp 16$
počet generátorů: $\varphi(16) = 8$
Eulerova funkce

Věta
Je-li $(G, \circ)$ cyklická grupa a x generátor, pak x^k je generátor, právě když $k \perp \#G$ = řád x
Je jich $\varphi(\#G)$.

Najděte minimální množinu $M \subset \mathbb{Z}^{2,2}$ tak, aby $M \supset \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = A$.
M je grupa s maticovým násobením.
Rozhodněte zda je Abelova.
Určete řády prvků
Najděte všechny podgrupy.

Najděte všechny generátory cyklické grupy $(\mathbb{Z}_6, +)$, $\{0,1,2,3,4,5\}$ $+ \bmod 6$

Kolik prvků má grupa G, jestliže má podgrupy H, K.
$\#H = 70$, $\#K = 16$, víme $\#G < 1000$

Mezi $\underbrace{(\mathbb{Z}_4, +)}_{G_1}$ a $\underbrace{(\mathbb{Z}_5^*, \cdot)}_{G_2}$ najděte bijekci φ, pro které platí
$\forall x, y \in G_1 \quad \varphi(x+y) = \varphi(x) \cdot \varphi(y)$

Nechť $(G, \circ)$ je grupa, $\#G$ je sudý.
Dokažte, že $\exists a \in G$, $a \neq e$ tak, že $a^2 = e$.

Čínská věta o zbytcích:

Nechť $m_1, \dots, m_n$ jsou vzájemně po dvojicích nesoudělná čísla.

Pak soustava $x \equiv r_1 \bmod m_1$

$\vdots$

$x \equiv r_n \bmod m_n$

Má právě jedno řešení x modulo m, kde $m = m_1 \cdot \dots \cdot m_n$

Důkaz:

• Definujme a_i vztahem:

$$m = m_1 a_1 = m_2 a_2 = \dots = m_n a_n$$

• Pak platí:

$$\begin{aligned} nsd(m_i, a_i) = 1 &\to \exists x_i, y_i \in \mathbb{Z} : m_i x_i + a_i y_i = 1 \Leftrightarrow \\ &\Leftrightarrow m_i x_i = 1 - a_i y_i \\ &\Rightarrow m_i \mid 1 - a_i y_i \to m_i \mid a_i y_i - 1 \end{aligned}$$

$$\to a_i y_i \equiv 1 \bmod m_i$$

Tvrzení:

Obecné řešení je tvaru:

$$x \equiv r_1 a_1 y_1 + \dots + r_n a_n y_n \bmod m$$

Důkaz:

zvolme $i \in \hat{n}$ libovolně:

$$x \equiv r_1 a_1 y_1 + \dots + r_n a_n y_n \bmod m_i$$

$\Leftrightarrow$ $x \equiv r_i a_i y_i \bmod m_i$

$\Leftrightarrow$ $x \equiv r_i \bmod m_i$

Jednoznačnost