

$$\text{Polynomy} = p(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \dots + a_n x^n$$

stupen polynomu $\deg p(x) = n$ - je to nejvyšší možný stupeň, na kterou je umocněna neznámá veličina x .

homogenní polynom: $\beta \in R[x]$, $R[x]$ je okruh polynomů

konstantní polynom: $p(x) = a$, $a \in R[x]$

homogený polynom: $p(x) = a_0 + a_1 x + \dots + a_n x^n$, kde $\deg p(x) = n$ a $a_n \neq 0$

lineární polynom: $a_1 x + a_0 = p(x)$

koren polynomu $p(x)$ je $a \Leftrightarrow (x-a) | p(x)$

koren a má násobnost $k \Leftrightarrow (x-a)^k | p(x)$

irreducibilní polynom - polynom, který nelze rozložit na součin nekonstantních polynomů nížejšího stupně.

$V \subset K$ jsou irreducibilní pouze polynomy stupně prvního, tj. lineární.

Pr a) $p(x) = x^2 - 2$ - je irreducibilní nad \mathbb{Q}

$$x^2 - 2 = 0$$

$$x^2 = 2$$

$$x = \pm \sqrt{2} \notin \mathbb{Q}$$

Ale nad \mathbb{R} je $p(x)$ lze rozložit na součin
 $\underbrace{x^2 - 2 = (x - \sqrt{2}) \cdot (x + \sqrt{2})}$

b) $p(x) = x^2 + 1$ - je irreducibilní nad \mathbb{R}

$$0 = x^2 + 1$$

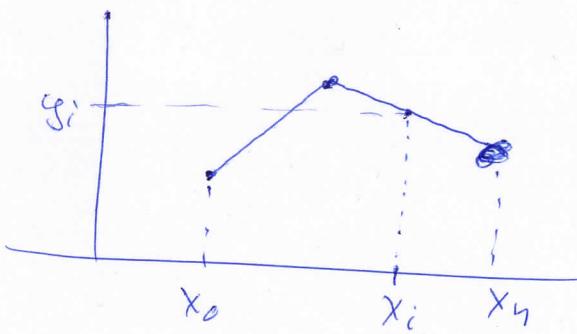
$$-1 = x^2$$

Ale nad \mathbb{C} polynom $p(x)$ je rozložit na součin
irreducibilních polynomů

$$x^2 + 1 = (x - i) \cdot (x + i)$$

Výpočet polynomů: existují vzorce pro výpočet 1. 2. stupně.
3. a 4. stupně.

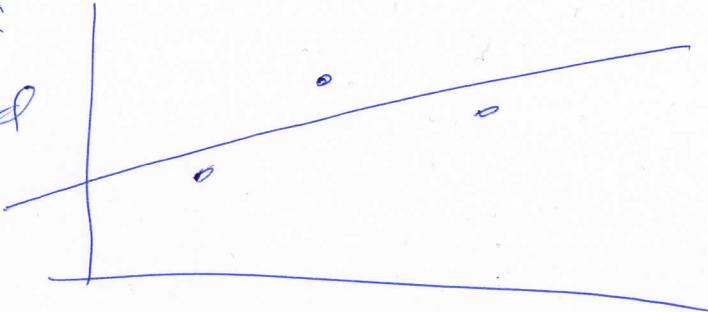
Interpolace



- křivka prochází první náměřenými body
- pomocí interpolace zjistíme jak by dopadlo měření v bodě x_i

Aproximace:

- je jen odhad
neprochází
náměřenými
body



Lagrangeova interpolace

Interpolaciní polynom $p(x) = \sum_{i=1}^n y_i \cdot \frac{g_i(x)}{g_i(x_i)}$; kde zlomek

má tvor

$$\frac{g_i(x)}{g_i(x_i)} = \frac{(x-x_1) \cdot (x-x_2) \cdots (x-x_{i-1}) \cdot (x-x_{i+1}) \cdots (x-x_n)}{(x_i-x_1) \cdots (x_i-x_{i-1}) \cdot (x_i-x_{i+1}) \cdots (x_i-x_n)}$$

Řeš $[-7, 9], [7, 7], [2, 6]$. Vypočítejte $p(x)$ pomocí

Lagrangeovy metody.

$$x_1 = -7, y_1 = 9, \quad x_2 = 7, y_2 = 7, \quad x_3 = 2, y_3 = 6$$

$$p(x) = y_1 \frac{g_1(x)}{g_1(x_1)} + y_2 \frac{g_2(x)}{g_2(x_2)} + y_3 \frac{g_3(x)}{g_3(x_3)}$$

pro bod x_1 :

$$\frac{(x-x_2) \cdot (x-x_3)}{(x_1-x_2) \cdot (x_1-x_3)} = \frac{(x+7) \cdot (x-2)}{(-7-7) \cdot (-7-2)} = \boxed{\frac{1}{6} (x^2 - x - 2x + 14)}$$
$$= \boxed{\frac{1}{6} (x^2 - 3x + 14)}$$

pro bod x_2 :

$$\frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} = \frac{(x+7) \cdot (x-2)}{(7+7) \cdot (7-2)} = \boxed{\frac{1}{2} (x^2 - x - 2)}$$

pro bod x_3 :

$$\frac{(x-x_1) \cdot (x-x_2)}{(x_3-x_1)(x_3-x_2)} = \frac{(x+7) \cdot (x-7)}{(2+7) \cdot (2-7)} = \boxed{\frac{1}{3} (x^2 - 49)}$$

$$p(x) = 9 \cdot \frac{1}{6} (x^2 - 3x + 14) + 7 \left(-\frac{1}{2}\right) (x^2 - x - 2) + 6 \cdot \frac{1}{3} (x^2 - 49)$$

$$= \frac{3}{2}x^2 - \frac{9}{2}x + 3 - \frac{7}{2}x^2 + \frac{7}{2}x + 7 + 2x^2 - 2$$

$$= \underline{\underline{3x^2 - 8x + 2}}$$

Newtonova metoda

$$p(x) = \sum_{i=1}^n x_i y_i (x) = (\lambda_1 + \lambda_2 (x-x_1) + \lambda_3 (x-x_1)(x-x_2) + \dots + \lambda_n (x-x_1) \cdot (x-x_2) \cdot \dots \cdot (x-x_{n-1}))$$

$$\lambda_1 = \underline{y_1}$$

$$\lambda_2 = \frac{\underline{y_2 - \lambda_1}}{(x_2 - x_1)} \Rightarrow y_2 = \underline{\lambda_1 + \lambda_2 (x_2 - x_1)}$$

$$\lambda_3 = \frac{\underline{y_3 - \lambda_1 - \lambda_2 (x_3 - x_1)}}{(x_3 - x_1) (x_3 - x_2)}$$

Príklad: $x_1 = -1, y_1 = 9, x_2 = 1, y_2 = 1, x_3 = 2, y_3 = 6$

$$\lambda_1 = \underline{9}$$

$$\lambda_2 = \frac{\underline{y_2 - \lambda_1}}{(x_2 - x_1)} = \frac{1 - 9}{1 + 1} = -\frac{8}{2} = -4$$

$$\lambda_3 = \frac{6 - 9 + (-4)(2+1)}{(2+1) \cdot (2-1)} = \frac{9}{3} = 3$$

$$\begin{aligned}
 P(x) &= 9 + (-4)(x+1) + 3 \underbrace{(x+1)(x-1)}_{x^2-1} = \\
 &= 9 - 4x - 4 + 3x^2 - 3 = \\
 &= \underline{\underline{3x^2 - 4x + 2}}
 \end{aligned}$$

- Výhoda Newtonovy metody - při přidání nového bodu stačí dopočítat λ_k pouze. U Lagrangeovy metody se musí dopočítat všechny zlomky.

Obor Integrif

z okraje Lergy' nemá děliteli než 1 tj. pro jeho první platí: $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

Pr] $(\mathbb{Z}_8, +, \cdot)$

↳ NENI obor integrif:

$$[\mathbb{Z}]_8, [\mathbb{S}]_8 \neq [\mathbb{O}]_8$$

$$[\mathbb{Z}]_8 \cdot [\mathbb{S}]_8 = [\mathbb{S}]_8 = \underline{\underline{[\mathbb{O}]_8}}$$

↳ má děliteli než 1!

Prvky v $\mathbb{C}[x]$ ($\mathbb{Z}_1 + \mathbb{I}$) nemají dělitelé nuly, tj. je to obor integrit.

Dělitelnost v oboru integrit I.

- ~~Prvek~~ b dělí a, tj. $b|a \Leftrightarrow \exists c \in I$ takové, že $a = b \cdot c$
- Asociované prvek a, b (znací $a \sim b$) $\Leftrightarrow a/b \in I$ a $b/a \in I$
například v \mathbb{Z} jsou to prvek takové, že $a = \pm b$
- triviální dělitelé prvek a: jsou takové všechny prvek b, pro které platí, že $a \sim b$ nebo b je jednotka oboru integrit.
- vlastní dělitelé prvek a: + prvek b, které nejsou asociované tj.
 $a \neq b$ a nejsou to jednotky oboru integrit
- Prostoinitely jsou tisla p $\Leftrightarrow p$ jsou irreducibilní
 $\Leftrightarrow p \nmid ab$ pro každou $a, b \in I$.

Gaussovy okruhy:

- prvek Gaussových okruhu lze rozložit na součin prostoinitelů
- v \mathbb{Z} jsou to prostoměra
- v $\mathbb{R}[\text{Ex}]$ je to rozklad polynomu na irreducibilní polynomy.

- Největší společný dělitel NSD císel a_1, \dots, a_n lze vypočítat z rozkladu těchto císel na prvočinitele

$$NSD(a_1, \dots, a_n) = p_1^{\min_{1 \leq i \leq n}(e_{i1})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ir})}$$

kde e_i jsou exponenty prvočinitelů

Pr] $NSD(144, 32)$

$$144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^4 \cdot 3^2$$

$$32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 \cdot 3^0$$

$$NSD(144, 32) = 2^{\min(4, 5)} \cdot 3^{\min(2, 0)} = 2^4 \cdot 3^0 = 2^4 = \underline{\underline{16}}$$

- Nejménší společný násobek NSN

$$NSN(a_1, \dots, a_n) = p_1^{\max(e_{i1})} \cdots p_r^{\max(e_{ir})}$$

Pr] $NSN(144, 32)$

$$144 = 2^4 \cdot 3^2 \quad | \quad 32 = 2^5 \cdot 3^0$$

$$NSN(144, 32) = 2^{\max(4, 5)} \cdot 3^{\max(2, 0)} = 2^5 \cdot 3^2 = \underline{\underline{288}}$$

- Euklidov očrak
V Euklidových očrakich platí, že pro prvek $a, b \in \mathbb{Z}$, $a \neq 0$ existuje prvek $q, r \in \mathbb{Z}$ tak, že $b = a \cdot q + r$, $0 \leq r < a$
- Polynomy v bodě a :

$$p(x) = (x-a) \cdot g(x) + r$$
, kde $r = p(a)$ hodnota polynomu v bodě a .

Hornerovo schema

$$p(x) = a_n x^n + \dots + x^1 a_1 + a_0$$

vypočet polynomu $p(x)$ v bodě a :

| | a_n | a_{n-1} | \dots | a_1 | a_0 |
|-----------------------|-------------|-------------|---------|---------------------------|---|
| <u>a</u> | $b_n = a_n$ | $b_{n-1} =$ | \dots | $b_1 = a \cdot b_2 + a_1$ | $b_0 = a \cdot b_1 + a_0$ — b_0 je hodnota polynomu $p(x)$ v bodě a . |

$$b_{n-1} = a \cdot b_n + a_{n-1}$$

$$b_{n-2} = a \cdot b_{n-1} + a_{n-2}$$

Pr $x^5 + 7x^4 - 2x^3 + x^2 - 6x + 3$ máme vypočítat hodnotu polynomu
v bodě $a=2$.

$$\begin{array}{c|cccccc|c} & 1 & 7 & -2 & 1 & -6 & 3 \\ \hline 2 & 1 & 9 & 16 & 33 & 60 & 123 \\ & \downarrow & & & & & \\ & 2 \cdot 1 + 7 & 2 \cdot 9 - 2 & & & & \end{array} \rightarrow p(a) = 123$$

$$[p(x) = (x-2) \cdot (x^4 + 9x^3 + 16x^2 + 33x + 60) + 123]$$

Pr Rozložte polynom $p(x) = x^6 + x^5 + x^4 + 2x^3 + 2x^2 + 2x + 2$ nad \mathbb{P}_3 na součin
irreducibilních polynomů pomocí Hornerova schématu.

- budeme hledat kořeny polynomu $p(x)$, které jsou ze \mathbb{P}_3
- tj. $[0]_3, [1]_3, [2]_3$
- $[0]$ mižeme hned vyfoučit, protože dosazením 0 do polynomu
dostaneme číslo 2, tj. nemá to být

| | | | | | | | | |
|----|---|---------------|----------------------|---------------|---------------|---------------|---------------|--|
| | 1 | 1 | 1 | 0 | 2 | 2 | 2 | |
| 1 | 1 | 2 | 0 | 0 | 2 | 1 | $\boxed{3=0}$ | \rightarrow tj. 1 je kořenem polynomu. |
| 1 | 1 | $\boxed{3=0}$ | 0 | 0 | $\boxed{2}$ | $\boxed{3=0}$ | | 1 je dvojnásobným kořenem polynomu |
| 1 | 1 | 1 | 1 | 1 | $\boxed{3=0}$ | | | 1 je trojnásobným kořenem |
| -1 | 1 | 2 | $\boxed{3=0}$ | 1 | $\neq 0$ | | | 1 není 4-násobným kořenem X |
| 2 | 1 | 3=0 | 1 | $\boxed{3=0}$ | | | | 2 je kořenem polynomu. |
| 2 | 1 | 2 | $\boxed{5=2 \neq 0}$ | | | | | 2 není dvojnásobným kořenem |

$$\begin{aligned}
 p(x) &= x^6 + x^5 + x^4 + 2x^2 + 2x + 2 = (x-1)^3 \cdot (x-2) \cdot (x^2 + 0 \cdot x + 1) \\
 &= (x-1)^3 \cdot (x-2) \cdot (x^2 + 1)
 \end{aligned}$$

je rozklad polynomu na ipeuducibilní polynomy nad \mathbb{P}_3 .

Pr $p(x) = 12x^6 + 8x^5 - 85x^4 + 15x^3 + 55x^2 + x - 6$ nad \mathbb{Q}

- možné kořeny $\in \mathbb{Q}$ lze najít následovně:

$c = \frac{p}{q}$ je možný kořen polynomu $p(x)$, kde $p, q \in \mathbb{Z}$

fj. $p|6$ a $q|12$

$$\Rightarrow p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

$$q \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

* je $\frac{1}{3}$ kořenem $p(x)$?

| | | | | | | | |
|---------------|----|----|-----|-----|----|----|----------|
| | 12 | 8 | -85 | 15 | 55 | 1 | -6 |
| $\frac{1}{3}$ | 12 | 12 | -81 | -12 | 51 | 18 | <u>0</u> |

\Rightarrow Číslo $\frac{1}{3}$ je kořenem polynomu $p(x)$.

• Využít Hornerova schéma pri prevade čísla z jiného
číselného soustavy do desítkové.

Pr máme číslo 2736 v osmickovej číselnej soustave.
Prevedeme číslo do desítkovej číselnej soustavy:

1) pomocí polynomu:

$$p(x) = 2x^3 + 7x^2 + 3x + 6$$

$$= 2 \cdot 8^3 + 7 \cdot 8^2 + 3 \cdot 8 + 6$$

$$= \underline{\underline{1502}}$$

→ za x dosadíme číslo,
na ktorom je dana soustava definovaná, t.j. 8

2) prevod pomocí Hornerova schéma:

$$(((2 \cdot 8 + 7) \cdot 8 + 3) \cdot 8 + 6 = \underline{\underline{1502}}$$

prvá cifra
čísla

druhá
cifra čísla --

Pr 3F7 číslo je 16-kové číselné soustavy +

16. soustava: $0, \dots, 9, A, \dots, F$ kde $A=10, \dots, F=15$

Prevod čísla do desítkovej číselnej soustavy:

$$(3 \cdot 16 + 7) \cdot 16 + 7 = (3 \cdot 16 + 15) \cdot 16 + 7 = 1015$$

Tedy číslo 3F7 v 16. čísel. soustavě je číslo 1015 v desítkové.

- využití v informatice: převod binární soustavy na desítkovou.
- využití v informatice: snadný prototyp $16 = 2^4$.
Von je snadný prototyp $16 = 2^4$.
 \Rightarrow každý 4 znak v bináru lze reprezentovat jedním znakem v desítkové.

Euklidov algoritmus pro výpočet NSD

$$NSD(a, b) = ? \quad \text{kde } a < b$$

$$\begin{aligned} \text{Algoritmus: } b &= a \cdot q_1 + r_1 \quad , \quad 0 \leq r_1 < a \\ a &= r_1 \cdot q_2 + r_2 \quad , \quad 0 \leq r_2 < r_1 \end{aligned}$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \cdot q_n + \boxed{r_n} \quad , \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+1} + \boxed{0} \quad NSD(a, b) = r_n$$

Poznámka: místo 0 vysta 1 tak to znamená, že čísla a, b jsou nesoudělná a ~~je~~ $NSD(a, b) = 1$.

Pr] NSD (123, 456) vypočítat pomocí Euklidova algoritmu.

$$456 = 123 \cdot 3 + 87$$

$$123 = 87 \cdot 1 + 36$$

$$87 = 36 \cdot 2 + 15$$

$$36 = 15 \cdot 2 + 6$$

$$15 = 6 \cdot 2 + \boxed{3} \rightarrow \text{NSD}(123, 456) = \underline{\underline{3}}$$

$$6 = 3 \cdot 2 + \boxed{0}$$

≡

Pr] máme zjistit NSD ($p(x)$, $q(x)$) = ?

$$p(x) = x^4 + x^3 + 3x + 3$$

$$q(x) = x^3 + 2x^2 + 5x + 3$$

$$p(x) > q(x)$$

$$x^3 : x^3$$

nad \mathbb{R}_5

$$(x^4 + x^3 + 3x + 3) : (x^3 + 2x^2 + 5x + 3) = x + 1$$

$$\underline{-} (x^4 + 2x^3 + 5x^2 + 3x)$$

$$\begin{array}{r} -x^3 - 5x^2 + 3 \\ \underline{-} (5x^3 + x^2 + 3) : (x^3 + 2x^2 + 5x + 3) = 5 \\ \hline -3x^3 - 3x^2 - x + 2 \\ \hline -2x^2 - x + 1 \Rightarrow 3x^2 + 5x + 1 \end{array}$$

$$p(x) : g(x) = x+5 \quad \text{zu bilden} \quad 3x^2 + 5x + 7$$

$$\bullet x^4 + x^3 + 3x + 3 = (x^3 + 2x^2 + 5x + 3) \cdot (x+5) + \underline{(3x^2 + 5x + 7)}$$

$$\bullet x^3 + 2x^2 + 5x + 3 = (3x^2 + 5x + 7) \cdot \frac{2x+3}{\uparrow} + \underline{\underline{0}} \quad \uparrow$$

$$\begin{array}{r} (\underline{x^3 + 2x^2 + 3x + 3}) : (\underline{3x^2 + 5x + 7}) = \cancel{2x + 3} \\ \cancel{6x^3 + 8x^2 + 2x} \\ \cancel{-} \quad \cancel{x^3 + 3x^2 + 2x} \end{array} \quad \text{zu bilden } \underline{\underline{0}}$$

$$\begin{array}{r} -x^2 + 2x + 3 = 24x^2 + 2x + 3 \\ - \quad \cancel{25x^2 + 42x + 3} \\ \hline \cancel{0} \end{array}$$

$$NSD(p(x), g(x)) = \underline{\underline{3x^2 + 5x + 7}}$$

Kódování binární zprávy pomocí polynomů:

$$z_1 = \underline{110} \underline{10}$$

- pomocí polynomu $x^3 + x = p(x)$
- $v(x) = r(x) + x^{n-k} \cdot m(x) \rightarrow v(x)$ je polynom reprezentující zprávu z_2 zakódovanou.
- $m(x)$ - polynom reprezentující zprávu z_1
 $m(x) = \underline{\boxed{1+x+0 \cdot x^2+1 \cdot x^3+0 \cdot x^4}} = \underline{1+x+x^3}$
- $x^{n-k} = x^{8-5} = x^3$
- $k \rightarrow$ počet cifer zprávy z_1 , $n = k + \text{stupen kódovacího polynomu}$
 $n = 5 + 3$
- $r(x)$ je zbytek po dělení polynomu $\underbrace{x^3(1+x+x^3)}_{x^3+x^4+x^6}$ a
 $p(x) = x^3 + x$
jsme nad \mathbb{P}_2 (binární zprávy)

$$\begin{array}{r}
 \underline{(x^6 + x^5 + x^3)} : \underline{(x^3 + x)} = x^3 + 1 \\
 - \underline{x^6 + x^5} \\
 \hline
 \underline{x^3} \\
 - \underline{x^3 + x} \\
 \hline
 -x \quad \dots \text{ nad } P_2 \text{ bude prepisat jake } \underline{x}
 \end{array}$$

• $r(x) = x$

kodova zpráva z_2 : $v(x) = r(x) + x^3 \cdot m(x) = \boxed{x + x^6 + x^5 + x^3}$

$n=5+3 \rightarrow$ určuje délku zprávy z_2 :

$$v(x) = 0 + x + 0 \cdot x^2 + x^3 + x^4 + 0 \cdot x^5 + x^6 + 0 \cdot x^7$$

$$\underline{\underline{z_2 = 01011010}}$$

Pomocí polynomu zakódované binární zpráva z_1 .