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

**stupeň $p(x)$:** $\deg p(x) = n$ - nejvyšší mocnina, na kt. je umocněna neznámá $\underline{x}$.

- **nulový polynom:** $0 \in R[x]$, kde $R[x]$ je okruh polynomu
- **konstantní p.:** $p(x) = a$, $a \in R[x]$
- **normovaný p.:** $p(x) = a_0 + a_1 x + \dots + a_n x^n$, $\deg p(x) = n \wedge a_n = 1$
- **lineární p.:** $p(x) = ax + b$, $a \neq 0$
- **kořen** polynomu $p(x)$ je $a \iff (x-a) \mid p(x)$
- kořen $a$ má **násobnost $k$** $\iff (x-a)^k \mid p(x)$
- **Ireducibilní p.** - polynom, kt. nelze rozložit na součin nekonstantních polynomu nižšího stupně.

Pozn.: V $\mathbb{C}$ jsou ireducibilní pouze polynomy nejvýše stupně 1 tj. lineární.

Př 1) a) $p(x) = x^2 - 2 \qquad p(x) \in \mathbb{Q}[x]$

$$0 = x^2 - 2$$
$$2 = x^2$$
$$\pm\sqrt{2} = x \notin \mathbb{Q}$$

tj. nad $\mathbb{Q}$ je to ireducibilní

Ale $\mathbb{R}$ lze rozložit:
$$p(x) = (x - \sqrt{2}) \cdot (x + \sqrt{2})$$

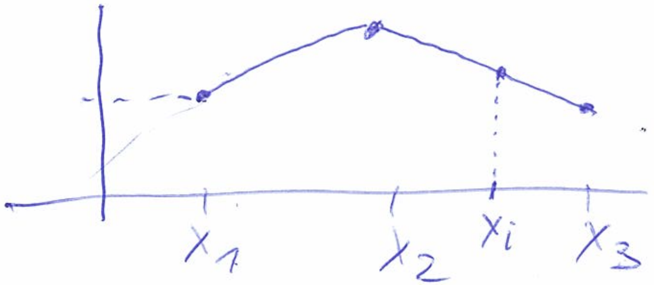
b) $p(x) = x^2 + 1$ nad $\mathbb{R}$

$$0 = x^2 + 1$$
$$-1 = x^2 \notin \mathbb{R}$$

tj. nad $\mathbb{R}$ je to ireducibilní

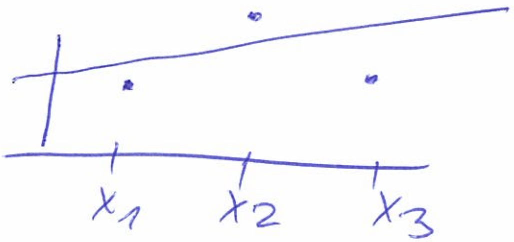
Ale $\mathbb{C}$ lze rozložit:
$$p(x) = (x + i) \cdot (x - i)$$

## Interpolace




- proložení bodů $x_1, \dots, x_n$ křivkou, kt. prochází těmito body.
- pomocí interpolace zjistíme, jak dopadne měření v $x_j$.

Pozn.) Aproximace:




- je jen odhad, křivka neprochází přímo body

- Lagrangův vzorec

$$\boxed{p(x) = \sum y_i \frac{g_i(x)}{g_i(x_i)}}, \text{ kde zlomek } \boxed{\frac{g_i(x)}{g_i(x_i)} = \frac{(x-x_1)\cdots(x-x_{i-1})\cdot(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_1)\cdots(x_i-x_{i-1})\cdot(x_i-x_{i+1})\cdots(x_i-x_n)}}$$

Př 2 body $[\underset{x_1}{-1}, \underset{y_1}{4}], [\underset{x_2}{1}, \underset{y_2}{1}], [\underset{x_3}{2}, \underset{y_3}{4}]$

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

$$x_1 = -1: \quad \frac{g_1(x)}{g_1(x_1)} = \frac{(x-x_2)\cdot(x-x_3)}{(x_1-x_2)\cdot(x_1-x_3)} = \frac{(x-1)\cdot(x-2)}{(-1-1)\cdot(-1-2)} = \underline{\underline{\frac{1}{6}(x^2-3x+2)}}$$

$$x_2 = 1: \quad \frac{g_2(x)}{g_2(x_2)} = \frac{(x-x_1)\cdot(x-x_3)}{(x_2-x_1)\cdot(x_2-x_3)} = \frac{(x+1)\cdot(x-2)}{(1+1)\cdot(1-2)} = \underline{\underline{-\frac{1}{2}(x^2-x-2)}}$$

$$x_3 = 2: \quad \frac{g_3(x)}{g_3(x_3)} = \frac{(x-x_1)\cdot(x-x_2)}{(x_3-x_1)\cdot(x_3-x_2)} = \frac{(x+1)\cdot(x-1)}{(2+1)\cdot(2-1)} = \underline{\underline{\frac{1}{3}(x^2-1)}}$$

$$p(x) = 4\cdot\frac{1}{6}(x^2-3x+2) + 1\cdot\left(-\frac{1}{2}\right)(x^2-x-2) + 4\cdot\frac{1}{3}(x^2-1)$$

$$= \underline{\underline{\frac{3}{2}x^2 - \frac{3}{2}x + 1}}$$

## Newtonův vzorec

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

$\lambda_1=y_1=p(x_1)$

$\lambda_2$: $\quad y_2=\lambda_1+\lambda_2(x_2-x_1) \Longrightarrow \lambda_2=\dfrac{y_2-\lambda_1}{x_2-x_1}$

$\lambda_3$: $\quad y_3=\lambda_1+\lambda_2(x_3-x_1)+\lambda_3(x_3-x_1)\cdot(x_3-x_2)$

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

$\vdots$

Př. 3) $[-1,4]$, $[1,1]$, $[2,4]$

$\lambda_1=4=y_1$

$$\lambda_2=\frac{y_2-\lambda_1}{x_2-x_1}=\frac{1-4}{1+1}=-\frac{3}{2}$$

$$\lambda_3=\frac{y_3-\lambda_1-\lambda_2(x_3-x_1)}{(x_3-x_1)\cdot(x_3-x_2)}=\frac{\cancel{4}-\cancel{4}-(-\frac{3}{2})\cdot(2+1)}{(2+1)\cdot(2-1)}=\frac{3}{2}$$

$$p(x) = \lambda_1 + \lambda_2 (x - x_1) + \lambda_3 (x - x_1)\cdot(x - x_2)$$

$$= 4 + \left(-\frac{3}{2}\right)\cdot(x+1) + \frac{3}{2}\underbrace{(x+1)\cdot(x-1)}_{x^2-1}$$

$$= 4 - \frac{3}{2}x - \frac{3}{2} + \frac{3}{2}x^2 - \frac{3}{2} = \underline{\frac{3}{2}x^2 - \frac{3}{2}x + 1}$$

Pozn: Pokud máme nový bod, přepočítáme interpolační polynomy

- Lag. vzorce: se musí přepočítat $\forall$ zlomky $\frac{g_i(x)}{g_i(x_i)}$ s novým bodem
- New. vzorec: stačí dopočítat $\lambda_4$ pro ten nový bod.

**Obor integrity**

- je to okruh, který nemá dělitele nuly, tj.

$$a\cdot b = 0 \implies a = 0 \lor b = 0$$

Př4: $(\mathbb{Z}_6, +, \cdot) \rightarrow$ Není obor integrity, pt.

$[2]_6, [3]_6$ : $[2]_6 \cdot [3]_6 = [2\cdot 3]_6 = [6]_6 = [0]_6$

- má dělitele nuly!

Pozn.: Okruh $(\mathbb{Z}, +, \cdot)$ nemá dělitele ~~nuly~~ nuly, tj. je to obor integrity.

- **Největší společný dělitel**

NSD čísel $a_1, \dots, a_n$ lze vypočítat z rozkladu čísel $a_1, \dots, a_n$ na jejich prvočinitele.

$$\boxed{NSD(a_1, \dots, a_n) = p_1^{\min\limits_{1 \le i \le n}(e_{i1})} \cdots p_r^{\min\limits_{1 \le i \le n}(e_{ir})}}$$

$e_i$ jsou exponenty, $p_1, \dots, p_r$ prvočinitelé

Př 5: $NSD(128, 36) = ?$

$$128 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^7 \cdot 3^0$$

$$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$$

$$NSD(128, 36) = 2^{\min(2,7)} \cdot 3^{\min(2,0)} = 2^2 \cdot 3^0 = \underline{\underline{4}}$$

**Nejmenší společný násobek**

NSN čísel $a_1, \dots, a_n$ se vypočítá:

$$\boxed{NSN(a_1, \dots, a_n) = p_1^{\max\limits_{1 \le i \le n}(e_{i1})} \cdots p_r^{\max\limits_{1 \le i \le n}(e_{ir})}}$$

Př 6| $NSN(128, 36) = ?$

$128 = 2^7$

$36 = 2^2 \cdot 3^2$

$NSN(128, 36) = 2^{\max(2,7)} \cdot 3^{\max(0,2)} = 2^7 \cdot 3^2 = 128 \cdot 9 = \underline{\underline{1152}}$

## Dělitelnost v oboru integrity $I$

- Prvek $b$ dělí prvek $a$, $b|a \iff \exists c \in I$ tak, že $a = b \cdot c$
- prvky $a, b$ jsou asociované $(a \sim b) \iff a|b \wedge b|a$

pozn; v $\mathbb{Z}$ to jsou $a \sim b$ takové že $\boxed{a = \pm b}$

- Triviální dělitelé prvku $a$ jsou takové $\forall$ ~~prv~~ prvky $b$, pro kt. platí že $a \sim b$ nebo $b$ je jednotka oboru integrity.
- Prvočinitelé jsou čísla $p \iff p$ jsou ireducibilní
  $\iff p|a \cdot b$ pak $p|a$ v $p|b$

- Gaussův okruh
  - okruh, kde lze prvek $a$ rozložit na součin prvočinitelů
  - v $\mathbb{Z}$ je to rozklad čísla na prvočísla
  - v $R[x]$ je to rozklad polynomů na ireducibilní polynomy

• Euklidův okruh

- v okruzích platí, že pro $a, b \in I$, $a \neq 0$ existují prvky $q, r \in I$ tak, že $\boxed{b = a \cdot q + r, \quad 0 \le r < a}$

- polynom v bodě a:

$\boxed{p(x) = (x-a)\cdot q(x) + r}$, kde $r = p(a)$ - hodnota polynomu v bodě a.

Hornerovo schéma

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

$$\boxed{p(x) = ((a_n x + a_{n-1})x + \dots)x + a_1)x + a_0}$$

Výpočet $p(x)$ v bodě $a$

| | | | | | |
|---|---|---|---|---|---|
| | $a_n$ | $a_{n-1}$ | $\dots$ | $a_1$ | $a_0$ |
| $a$ | $a_n = b_n$ | $b_{n-1}$ | | $b_1$ | $\boxed{b_0}$ |

→ $b_0$ je hodnota polynomu $p(x)$ v bodě $a$

$b_{n-1} = a \cdot b_n + a_{n-1}$ $\qquad b_1 = a \cdot b_2 + a_1$ $\qquad b_0 = a \cdot b_1 + a_0$

$$\boxed{p(x) = (x-a)\cdot(b_n x^{n-1} + b_{n-1} x^{n-2} + \dots + b_2 x + b_1) + b_0}$$

Př 7) Vypočítejte hodnotu $p(x) = x^5 + 2x^4 - 2x^2 - 4x + 2$ v bodě $a = -2$

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 0 | −2 | −4 | 2 |
| −2 | 1 | 0 | 0 | −2 | 0 | $\boxed{2}$ |

$\to p(a) = 2$

$$p(x) = (x+2)\cdot(x^4 - 2\cdot x) + 2$$

Př 8) Polynom $p(x) = x^6 + x^5 + x^4 + 2x^2 + 2x + 2$ nad $\mathbb{Z}_3$ rozložit na součin ireducibilních polynomů pomocí Hornera.

- kořeny jsou ze $\mathbb{Z}_3$, tj. mohou to být 0, 1, 2
- 0 můžeme hned vyloučit

$\Rightarrow p(0) = 2$, tj. není kořenem polynomu

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 1 | 1 | 0 | 2 | 2 | 2 | |
| 1 | 1 | 2 | 3=0 | 0 | 2 | 4=1 | 3=0 | → bod 1 je kořenem p(x) |
| 1 | 1 | 3=0 | 0 | 0 | 2 | 3=0 | | → bod 1 je dvojnásobný kořen p(x) |
| 1 | 1 | 1 | 1 | 1 | 3=0 | | | → bod 1 je trojnásobný kořen |
| 1 | 1 | 2 | 3=0 | $1 \neq 0$ | | | | → bod 1 <u>NENÍ</u> čtyřnásobný kořen |
| 2 | 1 | 3=0 | 1 | 3=0 | | | | → bod 2 je kořenem p(x) |
| 2 | 1 | 2 | $5=2\neq 0$ | | | | | → bod 2 NENÍ vícenásobný kořen |

$$p(x) = x^6 + x^5 + x^4 + 2x^2 + 2x + 2 = (x-1)^3 \cdot (x-2) \cdot (x^2 + 0 \cdot x + 1)$$

$$= \underline{\underline{(x-1)^3 \cdot (x-2) \cdot (x^2+1)}}$$

<u>Pozn.</u> Využití Hornerova s. při převodu čísla z jedné číselné soustavy do desítkové.

Př 9 | máme číslo $\underline{3652}$ v osmičkové soustavě.

- dva způsoby převodu do desítkové soustavy

a) pomocí polynomu:

$$p(x) = 3\cdot x^3 + 6\cdot x^2 + 5\cdot x + 2$$ → za x se dosadí číslo, na kt. je soustava definovaná, tj. 8

$$= 3\cdot 8^3 + 6\cdot 8^2 + 5\cdot 8 + 2$$

$$= \underline{\underline{1962}}$$

b) pomocí Hornera:

$$((3x+6)\cdot x+5)\cdot x+2 = ((3\cdot 8+6)\cdot 8+5)\cdot 8+2 = \underline{\underline{1962}}$$

Př 10 | Šestnáctková číselná soustava:

0, 1, . . . . , 9, A, B, C, D, E, F  kde A – F má hodnoty 10 – 15

- Převeďte z této soustavy číslo A3F do desítkové (pomocí Hornera).

$x = 16$

$$(Ax+3)\cdot x+F = (10\cdot x+3)\cdot x+15$$

$$= (10\cdot 16+3)\cdot 16+15$$

$$= \underline{2623}$$

Pozn. Tato soustava se využívá v informatice, pro zkrácený zápis binárního kódu, pt. platí $16 = 2^4$ a tedy převod z 16. soustavy do binární je jednoduchý.
$\Rightarrow$ $\forall$ 4 znaky binárního kódu lze prezentovat jedním znakem z 16. soustavy.

- Euklidův algoritmus pro výpočet NSD

$NSD(a,b) = ?$ , kde $a < b$

Algoritmus:

$$b = a \cdot q_1 + r_1 \quad , \quad 0 \leq r_1 < a$$
$$a = r_1 \cdot q_2 + r_2 \quad ; \quad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + \boxed{r_n} \quad , \quad 0 \leq r_n \leq r_{n-1}$$
$$r_{n-1} = r_n \cdot q_{n+1} + \boxed{0}$$

$\Rightarrow$ číslo $r_n$ je hledaný $NSD(a,b)$

Pozn. Pokud v posledním kroce je zbytek roven 1 místo 0, pak $NSD(a,b) = 1$ a čísla jsou nesoudělná.

Př 11 $NSD(123, 456) = ?$ pomocí Euklidova algoritmu:

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

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

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

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

$$15 = 6 \cdot 2 + 3 \longrightarrow NSD(123, 456) = 3$$

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

Př 12 $NSD(p(x), g(x)) = ?$ nad $\mathbb{Z}_3$

$$p(x) = 2x^4 + x^3 + 2x \qquad g(x) = x^2 + 2x + 1$$

$$p(x) > g(x)$$

$$p(x) = g(x) \cdot r_1(x) + z_1$$

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

$$- \quad 2x^4 + 4x^3 + 2x^2$$

násobíme

násobíme

$$-3x^3 - 2x^2 + 2x = x^2 + 2x$$

$$\overset{\shortparallel}{0}$$

$$(x^2 + 2x)$$

$$- \quad x^2 + 2x + 1$$

$$-1 = 2 \text{ nad } \mathbb{Z}_3$$

- $(2x^4 + x^3 + 2x) = (x^2 + 2x + 1) \cdot (2x^2 + 1) + 2$

$$(x^2 + 2x + 1) = 2 \cdot ? \quad + \quad ?$$

$$(x^2 + 2x + 1) : 2 = 2x^2 + x + 2 \qquad \text{zbytek } 0.$$

$$- \quad x^2$$

násobí

$$2x + 1$$

$$- \quad 2x$$

$$1$$

$$- \quad 1$$

$$0$$

Euklidův algoritmus má tvar.

$$(2x^4+x^3+2x) = (x^2+2x+1)\cdot(2x^2+1)+2$$

$$(x^2+2x+1) = 2\cdot(2x^2+x+2)+0$$

$$\underline{\underline{NSD(p(x), q(x)) = 2}}$$

<u>Pozn)</u> Využití dělení polynomů se zbytkem v šifrování binárních zpráv.

<u>Př 13|.</u> $z_1 = 10011$ máme ji šifrovat polynomem $p(x)$

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

- délka vstupní zprávy $z_1 \Rightarrow k=5$
- stupeň šifrovacího polynomu $p(x)$ je $s=3$
- délka výstupní zprávy $z_2$ je $n = k+s = 5+3 = \underline{\underline{8}}$
- $z_1$ lze přepsat na polynom $m(x)$

$$z_1 = 10011 \rightarrow m(x) = 1+0\cdot x+0\cdot x^2+1\cdot x^3+1\cdot x^4 = \underline{\underline{1+x^3+x^4}}$$

$\Rightarrow$ polynom je ze $\mathbb{Z}_2$, tj. koeficienty jsou 0 a 1

- výpočet té zprávy $z_2$:

$$V(x) = x^{n-k} \cdot m(x) + r(x)$$ , kde $x^{n-k} = x^{8-5} = x^3$

$\hookrightarrow$ $r(x)$ je zbytek po dělení polynomu $x^{n-k} \cdot m(x)$ polynomem $p(x)$

$$x^{n-k} \cdot m(x) = x^3 \cdot (1 + x^3 + x^4) = \underline{x^3 + x^6 + x^7}$$

- $(x^7 + x^6 + x^3) : (x^3 + x) = x^4 + x^3 + x^2 + x$

$$
\begin{array}{l}
\quad (x^7 + x^6 + x^3) \\
- \ (x^7 + x^5) \\
\hline
\quad \underbrace{x^6 - x^5 + x^3}_{} \text{ nad } \mathbb{Z}_2 \\
\quad \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \\
\quad (x^6 + x^5 + x^3) \\
- \ (x^6 + x^4) \\
\hline
\quad (x^5 + x^4 + x^3) \\
- \ (x^5 + x^3) \\
\hline
\quad x^4 \\
- \ (x^4 + x^2) \\
\hline
\quad -x^2 = x^2 \text{ v } \mathbb{Z}_2 \Rightarrow \underline{\underline{r(x)}}
\end{array}
$$

Tedy : $v(x) = x^{n-k} \cdot m(x) + r(x)$

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

↳ polynom reprezentující zprávu $z_2$

$v(x) = 0 + 0 \cdot x + 1 \cdot x^2 + 1 \cdot x^3 + 0 \cdot x^4 + 0 \cdot x^5 + 1 \cdot x^6 + 1 \cdot x^7$

$\Rightarrow z_2 = 00110011$