Polynomy (mnohočleny)

Definice: *Polynom* stupně n v proměnné x nad tělesem T je výraz

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

kde $a_n \neq 0$ a $a_n, \ldots, a_0 \in T$. Píšeme $p \in T(x)$.

Operace s polynomy $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i$:

- sčítání, odčítání: $(p \pm q)(x) = \sum_{i=0}^{\max\{n,m\}} (a_i \pm b_i) x^i$
- skalární násobek pro $t \in T$: $(tp)(x) = \sum_{i=0}^{n} (t a_i) x^i$
- součin $(pq)(x) = \sum_{i=0}^{n+m} c_i x^i$, kde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$
- dělení se zbytkem — existují jedinečné polynomy $s, r \in T(x)$ takové, že $p = qs + r$, kde stupeň r je menší než stupeň q.

Ukázka — operace s polynomy nad $\mathbb{Z}_5$

Součet:

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

stupeň se může snížit:

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

Násobek:

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

Součin:

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

Příklad — operace s polynomy nad $\mathbb{Z}_5$

Dělení se zbytkem:

$$\begin{array}{rrrrrrl}
4x^5 & +2x^4 & & +3x^2 & & +3 & : \ 3x^2+4x+2 \ = \ 3x^3+3x+2 \\
\underline{-4x^5} & \underline{-2x^4} & \underline{-\ x^3} & & & & \\
 & & 4x^3 & +3x^2 & & & \\
 & & \underline{-4x^3} & \underline{-2x^2} & \underline{-\ x} & & \\
 & & & x^2 & +4x & +3 & \\
 & & & \underline{-\ x^2} & \underline{-3x} & \underline{-4} & \\
 & & & & x & +4 &
\end{array}$$

Kontrola správnosti $p = qs + r$:

$$4x^5 + 2x^4 + 3x^2 + 3 \ = \ (3x^2 + 4x + 2)(3x^3 + 3x + 2) \ + \ (x + 4)$$

Malá Fermatova věta

Věta: Pro libovolné $x \in \mathbb{Z}_p \setminus \{0\} : x^{p-1} = 1$.

Důkaz: zobrazení $i \to xi$ je bijekce na $\{1, \ldots, p-1\}$ v $\mathbb{Z}_p$.
V $\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} xi = x^{p-1} \prod_{i=1}^{p-1} i$ zkrátíme nenulový člen $\prod_{i=1}^{p-1} i$.

Důsledek: Pro libovolné $x \in \mathbb{Z}_p : x^p - x = 0$.

Důsledek: Pro každý $q \in \mathbb{Z}_p(x)$ existuje $r \in \mathbb{Z}_p(x)$ stupně nejvýše $p-1$ takový, že $\forall x \in \mathbb{Z}_p : q(x) = r(x)$.

Ukázka:

$$4x^5 + 2x^4 + 3x^2 + 3 \;=\; 4(x^5 - x) \;+\; 2x^4 + 3x^2 + 4x + 3$$

t.j. polynom $q(x) = 4x^5 + 2x^4 + 3x^2 + 3$ dává na $\mathbb{Z}_5$
stejné výsledky jako $r(x) = 2x^4 + 3x^2 + 4x + 3$.

Kořeny

Definice: *Kořen* polynomu $p \in T(x)$ je $r \in T$ takové, že $p(r) = 0$.

Pozorování: Prvek $r \in T$ je kořenem polynomu p, právě když lineární dvoučlen $x - r$ dělí p beze zbytku.

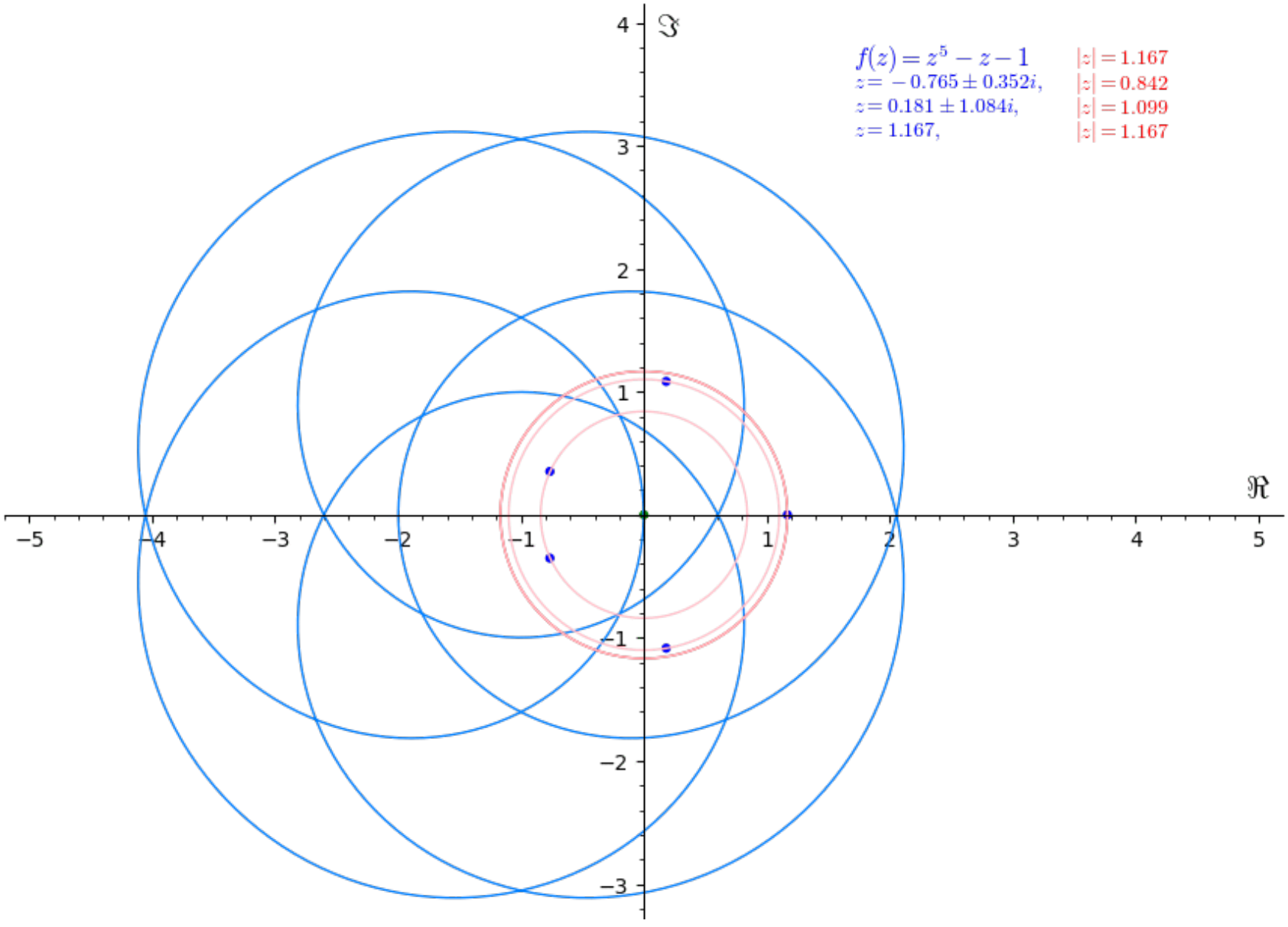
Definice: *Násobnost* kořene r z $p \in T(x)$ je největší kladné celé číslo k takové, že $(x - r)^k$ dělí p .

Věta: (Základní věta algebry)
Každý polynom $p \in \mathbb{C}(x)$ má alespoň jeden kořen.

Důsledek: Každý polynom $p \in \mathbb{C}(x)$ lze rozložit na součin lineárních faktorů, t.j. na polynomy prvního stupně.

Definice: Pokud každý polynom $p \in T(x)$ stupně alespoň jedna má alespoň jeden kořen, pak je těleso T *algebraicky uzavřené*.

Ukázka k základní větě algebry



Reprezentace polynomů stupně n

- koeficienty $a_0, \ldots, a_n$,
- v algebraicky uzavřených tělesech pomocí koeficientu a_n a n kořenů $r_1, \ldots, r_n$,
- hodnotami polynomu v $n+1$ různých bodech.

Problém: Dáno $n+1$ dvojic (x_i, y_i) pro $i = 0, \ldots, n$, určete $p \in T(x)$ stupně nejvýše n takový, že $p(x_i) = y_i$ pro každé i.

Pozorování: Koeficienty $a_0, \ldots, a_n$ z p jsou řešením soustavy:

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Definice: Matice této soustavy je *Vandermondova matice* $\boldsymbol{V}_{n+1}(x_0, \ldots, x_n)$

Věta: Vandermondova matice $\boldsymbol{V}_{n+1}(x_0, \ldots, x_n)$ je regulární, právě když $x_0, \ldots, x_n$ jsou navzájem různá.

Důkaz regularity Vandermondovy matice

Odzadu odečteme od každého sloupce x_0-násobek předchozího (až na první). Poté rozvineme podle prvního řádku a pro každé $i = 1, \ldots, n$ vytkneme z i-tého řádku $x_i - x_0$:

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ 1 & x_2 & x_2^2 & \ldots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{vmatrix} =$$

$$\begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & x_1 - x_0 & x_1(x_1 - x_0) & \ldots & x_1^{n-1}(x_1 - x_0) \\ 1 & x_2 - x_0 & x_2(x_2 - x_0) & \ldots & x_2^{n-1}(x_2 - x_0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n - x_0 & x_n(x_n - x_0) & \ldots & x_n^{n-1}(x_n - x_0) \end{vmatrix} = \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix} \prod_{i=1}^{n} (x_i - x_0)$$

Získali jsme následující rekurenci, již už lze snadno rozvést:

$$\det(\boldsymbol{V}_{n+1}(x_0, \ldots, x_n)) = \det(\boldsymbol{V}_n(x_1, \ldots, x_n)) \prod_{i=1}^{n} (x_i - x_0) = \prod_{i<j} (x_j - x_i)$$

Ukázka pro $n = 3$

$$\det(\boldsymbol{V}_4(x_0,\ldots,x_3)) = \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \end{vmatrix} \quad \begin{matrix} \\ -x_0\mathrm{I} \\ -x_0\mathrm{II} \\ -x_0\mathrm{III} \end{matrix}$$

$$= \begin{vmatrix} 1 & x_0 - x_0\cdot 1 & x_0^2 - x_0x_0 & x_0^3 - x_0x_0^2 \\ 1 & x_1 - x_0\cdot 1 & x_1^2 - x_0x_1 & x_1^3 - x_0x_1^2 \\ 1 & x_2 - x_0\cdot 1 & x_2^2 - x_0x_2 & x_2^3 - x_0x_2^2 \\ 1 & x_3 - x_0\cdot 1 & x_3^2 - x_0x_3 & x_3^3 - x_0x_3^2 \end{vmatrix} \Leftarrow$$

$$= \begin{vmatrix} x_1 - x_0 & x_1(x_1 - x_0) & x_1^2(x_1 - x_0) \\ x_2 - x_0 & x_2(x_2 - x_0) & x_2^2(x_1 - x_0) \\ x_3 - x_0 & x_3(x_3 - x_0) & x_3^2(x_1 - x_0) \end{vmatrix} \begin{matrix} \\ :(x_1 - x_0) \\ :(x_2 - x_0) \\ :(x_3 - x_0) \end{matrix}$$

$$= \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} \prod_{i=1}^{3}(x_i - x_0) = \det(\boldsymbol{V}_3(x_1,x_2,x_3)) \prod_{i=1}^{3}(x_i - x_0)$$

$$= \det(\boldsymbol{V}_3(x_1,x_2,x_3))(x_1 - x_0)(x_2 - x_0)(x_3 - x_0)$$

$$= \det(\boldsymbol{V}_2(x_2,x_3))(x_2 - x_1)(x_3 - x_1)(x_1 - x_0)(x_2 - x_0)(x_3 - x_0)$$

$$= (x_3 - x_2)(x_2 - x_1)(x_3 - x_1)(x_1 - x_0)(x_2 - x_0)(x_3 - x_0) = \prod_{i<j}(x_j - x_i)$$

Lagrangeova interpolace

... alternativní způsob interpolace polynomu $p \in T(x)$ stupně n skrz $n+1$ bodů (x_i, y_i) pro $i = 0, \ldots, n$.

1. Určíme $n+1$ pomocných polynomů $p_0, \ldots, p_n$ stupně n:

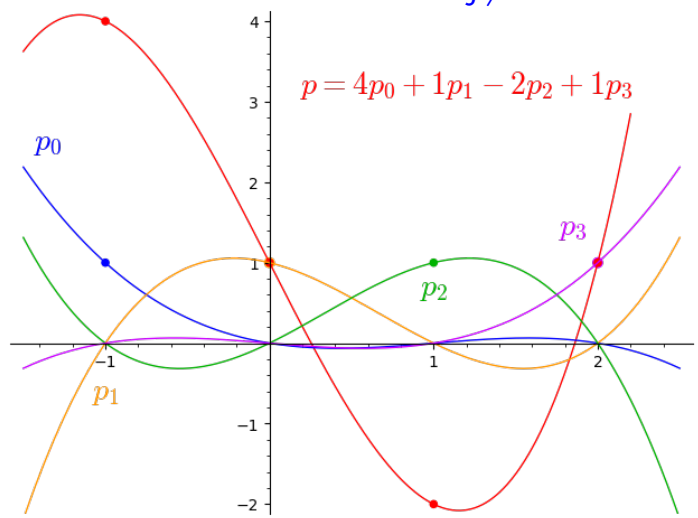
$$p_i(x) = \frac{(x-x_0)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)} = \frac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)}$$

Pomocné polynomy splňují:
$p_i(x_i) = 1$ a pro $i \neq j : p_i(x_j) = 0$.

Ukázka: Pro kubický reálný polynom skrz $(-1,4), (0,1), (1,-2)$ a $(2,1)$ je:

$$p_0(x) = \frac{x(x-1)(x-2)}{(-1)(-2)(-3)} = \frac{-x^3+3x^2-2x}{6},$$

$$p_1(x) = \frac{x^3-2x^2-x+2}{2}, \ldots$$



2. Hledaný $p(x)$ získáme lineární kombinací $p(x) = \sum_{i=0}^{n} y_i p_i(x)$.

Potom platí $p(x_j) = y_j p_j(x_j) = y_j$,
protože ve všech ostatních sčítancích je $p_i(x_j) = 0$.

Ukázka Lagrangeovy interpolace

Cíl: proložit polynom $p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ nad $\mathbb{Z}_{11}$ skrz body $(1, 5)$, $(2, 1)$, $(3, 3)$, $(4, 4)$, $(5, 3)$, $(6, 5)$ a $(7, 10)$.

Hledáme a_4, a_3, a_2, a_1 a a_0, které splňují (nad $\mathbb{Z}_{11}$!!)

$$
\begin{array}{rcrcrcrcrcr}
a_4 & + & a_3 & + & a_2 & + & a_1 & + & a_0 & = & 5 \\
5a_4 & + & 8a_3 & + & 4a_2 & + & 2a_1 & + & a_0 & = & 1 \\
4a_4 & + & 5a_3 & + & 9a_2 & + & 3a_1 & + & a_0 & = & 3 \\
3a_4 & + & 9a_3 & + & 5a_2 & + & 4a_1 & + & a_0 & = & 4 \\
9a_4 & + & 4a_3 & + & 3a_2 & + & 5a_1 & + & a_0 & = & 3 \\
9a_4 & + & 7a_3 & + & 3a_2 & + & 6a_1 & + & a_0 & = & 5 \\
3a_4 & + & 2a_3 & + & 5a_2 & + & 7a_1 & + & a_0 & = & 10
\end{array}
$$

Ve skutečnosti stačí jen 5 bodů.
Můžeme se omezit na prvních 5 rovnic (a prvních 5 bodů).

Nejprve vypočítáme pomocné polynomy $p_0, \ldots, p_4$.
Tyto polynomy splňují: $p_i(x_i) = 1$ a také $j \neq i : p_i(x_j) = 0$.

$$p_0(x) = \frac{(x-2)(x-3)(x-4)(x-5)}{(1-2)(1-3)(1-4)(1-5)} = \frac{x^4+8x^3+5x^2+10}{2} = 6x^4 + 4x^3 + 8x^2 + 5$$
$$p_1(x) = \frac{(x-1)(x-3)(x-4)(x-5)}{(2-1)(2-3)(2-4)(2-5)} = \frac{x^4+9x^3+4x^2+3x+5}{5} = 9x^4 + 4x^3 + 3x^2 + 5x + 1$$
$$p_2(x) = \frac{(x-1)(x-2)(x-4)(x-5)}{(3-1)(3-2)(3-4)(3-5)} = \frac{x^4+10x^3+5x^2+10x+7}{4} = 3x^4 + 8x^3 + 4x^2 + 8x + 10$$
$$p_3(x) = \frac{(x-1)(x-2)(x-3)(x-5)}{(4-1)(4-2)(4-3)(4-5)} = \frac{x^4+8x^2+5x+8}{5} = 9x^4 + 6x^2 + x + 6$$
$$p_4(x) = \frac{(x-1)(x-2)(x-3)(x-4)}{(5-1)(5-2)(5-3)(5-4)} = \frac{x^4+x^3+2x^2+5x+2}{2} = 6x^4 + 6x^3 + x^2 + 8x + 1$$

Požadovaný polynom je zkombinován z pomocných polynomů a z čísel v daných bodech $(i, p(i))$ následovně:

$$p(x) = \sum_{i=0}^{4} y_i p_i(x) = 5p_0(x) + p_1(x) + 3p_2(x) + 4p_3(x) + 3p_4(x)$$
$$= 3x^4 + 5x^2 + 2x + 6$$

Můžeme zkontrolovat, zda ostatní body $(6, 5)$, $(7, 10)$ leží na $p(x)$

$$p(6) = 3 \cdot 6^4 + 5 \cdot 6^2 + 2 \cdot 6 + 6 = 3 \cdot 9 + 5 \cdot 3 + 2 \cdot 6 + 6 = 5$$
$$p(7) = 3 \cdot 7^4 + 5 \cdot 7^2 + 2 \cdot 7 + 6 = 3 \cdot 3 + 5 \cdot 5 + 2 \cdot 7 + 6 = 10$$

Aplikace

Problém: Pro čísla m a n navrhněte m klíčů tak, aby:

- bylo možné určit tajný kód z každé kombinace n klíčů,
- ale nikdy nebylo možné učit kód z méně než n klíčů.

Předpokládejme, že způsob konstrukce klíčů je veřejně známý.

Řešení: Zvolíme nějaký polynom stupně $n-1$ a jako klíče rozdáme m různých dvojic $(x_i, p(x_i))$. Tajný kód je polynom (např. absolutní člen, jsou-li $x_i \neq 0$). Těleso může být např. $\mathbb{R}$ nebo $\mathbb{Z}_p$ s $p \geq m$.

Problém: Lze vynásobit dvě n-ciferná celá čísla v čase $o(n^2)$?

Řešení:

- Interpretujeme daná čísla jako polynomy p a q stupně $n-1$,
- vybereme $2n$ dvojic $(i, p(i)), (i, q(i))$ a spočítáme $(i, p(i)q(i))$,
- pak najdeme koeficienty součinu pq v čase $O(n \log n)$.

Volba vhodného tělesa a efektivní rekurentní výpočet je principem tzv. *rychlé Fourierovy transformace*.

Kvíz — řešení

Je-li u některých otázek více možností správných, vyberte všechny.

1. Pravda nebo lež? Pro libovolné p platí, že dva polynomy nad $\mathbb{Z}_p$ mají stejné kořeny, právě když mají stejné koeficienty.
2. Kolik polynomů p nad $\mathbb{Z}_5$ stupně nejvýše 4 splňuje $p(3) = 4$?
   a) žádný, b) 1, c) 5, d) 20, e) 25, f) 125, g) 625, h) 3 125.
3. Mějme čtvercovou matici $\boldsymbol{A}$ řádu 4, která má na 10 pozicích reálné číslo a na 6 pozicích proměnnou x. Pokud vyjádříme $\det \boldsymbol{A}$ jako polynom v proměnné x, pak může mít stupeň:
   a) -1, čili jde o nulový polynom, b) 0, c) 1, d) 2,
   e) 3, f) 4, g) 5, h) 6, i) 10, j) 16, k) 24, l) i víc
4. Máme-li nad $\mathbb{Z}_p$ navrhnout 8 klíčů, aby 4 určily kód, je třeba:
   a) polynom stupně 3 a $p \geq 8$, b) polynom stupně 7 a $p \geq 4$,
   c) polynom stupně 5 a $p \geq 8$, d) polynom stupně 9 a $p \geq 4$.

Komentář k řešení kvízu

1. Neplatí už ani pro lineární polynomy: $p(x) = x$ a $q(x) = 2x$, nad $\mathbb{Z}_2$ lze místo q vzít $q'(x) = x^2$.
2. Koeficienty splňují rovnici $3^4 a_4 + 3^3 a_3 + 3^2 a_2 + 3a_1 + a_0 = 4$, jejímž řešením je afinní prostor dimenze 4 a ten má 5^4 prvků.
3. Nejvyšší možný stupeň je 4, protože každý součin v determinantu má 4 činitele. Pro ostatní stupně je možné zkonstruovat trojúhelníkovou matici s 0 až 3 výskyty x na diagonále, případně matici s nulovým řádkem.
4. Klíče odpovídají bodům, kterými má být polynom proložen. Polynom stupně n je určen $n + 1$ body a pro p různých bodů je třeba mít těleso o alespoň p prvcích.

Otázky k porozumění tématu přednášky

- Kolik aritmetických operací vyžadují operace s polynomy?
- Proč je algoritmus na dělení polynomů konečný?
- Jaký je (souhrnný) stupeň Vandermondova determinantu, jsou-li $x_0, \ldots, x_n$? brány jako proměnné?
- Kolik aritmetických operací vyžaduje Lagrangeova interpolace?
- Pomocné polynomy tvoří bázi jistého prostoru polynomů. Čím je tento prostor určen?
- Sestavíme-li z koeficientů polynomů získaných Lagrangeovou interpolací matici (po sloupcích), jaký bude vztah této matice k Vandermondově matici?
- Proč je v součinu n-ciferných čísel třeba polynom vyhodnotit ve $2n$ bodech a nestačí jen n?

Poznámky k pojmosloví a značení

Výpočet koeficientu $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ v součinu polynomů se nazývá *konvoluce* posloupností $(a_0, \ldots, a_j)$ a $(b_0, \ldots, b_j)$.

Základní větu algebry pro reálné polynomy zformuloval Albert Girard v roce 1629.

O důkaz se pokusili mj. d'Alembert (1746), Euler (1749), de Foncenex (1759), Lagrange (1772), Laplace (1795) a Gauss (1799).

První korektní důkaz věty podal až v roce 1814 J.-R. Argand, francouzský knihkupec a amatérský matematik. Mimo jiné ji jako první zformuloval v oboru komplexních čísel.

Jean-Robert Argand
(1768 – 1822)

Metoda návrhu klíčů se nazývá *Šamirovo sdílení tajemství* podle Adi Šamira (jednoho z tvůrců šifrovacího algoritmu RSA), který ji publikoval v roce 1979, včetně využití polynomů.