Polynom stupně n v proměnné x nad tělesem $\mathbb{K}$ je výraz:

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

kde $a_n \neq 0$ a $a_n, \dots, a_0 \in \mathbb{K}$. Píšeme $p \in \mathbb{K}(x)$

Dělení polynomu jiným polynomem se zbytkem:

Nad $\mathbb{Z}_5$

$$4x^5 + 2x^4 + 3x^2 + 3 : 3x^2 + 4x + 2 = 3x^3 + 3x + 2$$

výsledek

$$\begin{array}{l} 4x^5 + 2x^4 + 3x^2 + 3 \\ \underline{-4x^5 - 2x^4 - x^3} \\ \quad 4x^3 + 3x^2 \\ \quad \underline{-4x^3 - 2x^2 - x} \\ \qquad \underline{x^2 + 4x + 3} \\ \qquad x + 4 \end{array}$$

zbytek

Vždy to dělám tak, abych prvním číslem polynomu dělitele dostal v součtu nulu s dělencem

Malá Fermatova věta:

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

Zobrazení $i \to xi$ je bijekce na $\{1, \dots, p-1\}$ 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 $\prod_{i=1}^{p-1} i$

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

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

Kořen polynomu $p \in \mathbb{K}(x)$ je $r \in \mathbb{K}$ takové, že $p(r) = 0$

Násobnost kořene r z $p \in \mathbb{K}(x)$ je největší kladné celé číslo k takové, že $(x-r)^k = p$

Každý polynom $p \in \mathbb{C}(x)$ má alespoň jeden kořen.

$\to$ Každý polynom $p \in \mathbb{C}(x)$ lze rozložit na součin lineárních faktorů, t.j. na polynom 1. st.

Algebraicky uzavřené těleso je takové $\mathbb{K}$, kdy $\forall p \in \mathbb{K}(x)$ má vlastní kořen.

Vandermonova matice $V_{n+1}(x_0, \dots x_n)$ je matice následující soustavy:

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

→ Tento polynom je řešením → Použití se známe-li $n+1$ dvojic (x_i, y_i), tedy kořenů a hodnot.

Vandermonova matice je regulární $\iff$ $x_0 \dots x_n$ jsou různé

Dk:

$$V_{n+1}(x_0 \_ x_n) = \begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix}$$

Odečteme první řádek od ostatních. Následně vytkneme $(x_i - x_0)$ $\forall i$ z itého řádku.
V prvním sloupci je n nul, takže můžu podle něj rozvést:

$$\det(V_{n+1}) = \prod_{i=1}^{n} (x_i - x_0) \cdot \begin{vmatrix} 1 & x_1 + x_0 & x_1^2 + x_1 \cdot x_0 + x_0^2 & \dots & x_1^{n-1} + x_1^{n-2} x_0 + \dots + x_0^{n-1} \\ 1 & x_2 + x_0 & x_2^2 + x_2 x_0 + x_0^2 & \dots & x_2^{n-1} + x_2^{n-2} x_0 + \dots + x_0^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & x_n + x_0 & x_n^2 + x_n x_0 + x_0^2 & \dots & x_n^{n-1} + x_n^{n-2} x_0 + \dots + x_0^{n-1} \end{vmatrix}$$

ukázka toho rozšíření →

$0 \quad x_1 - x_0 \quad x_1^2 - x_0^2 \quad \dots \quad x_1^n - x_0^n$

$(x_1 + x_0) \cdot (x_1 - x_0)$

$1 \quad x_1 - x_0 \quad \dots$

→ tzn. vlevo

Nyní odzadu odečteme od $\forall$ sloupce x_0-násobek předchozího. Tak se zbavíme všech sčítanců obsahujících x_0

Získali jsme rekurenci $\operatorname{Det}(V_{n+1}(x_0 \dots x_n)) = \left(\prod_{i=1}^{n} (x_i - x_0)\right) \det(V_n(x_1 \dots x_n)) = \prod_{i<j} (x_j - x_i)$

Lagrangova interpolace:

– způsob interpolace polynomu pe $\mathbb{K}(x)$ stupně n skrz $n+1$ bodů (x_i, y_i) pro $i = 1, \dots, n+1$

1) Určíme $n+1$ pomocných polynomů stupně n

$$p_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} = \frac{(x - x_1) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_{n+1})}{(x_i - x_1) \dots (x_i - x_{i-1}) \cdot (x_i - x_{i+1}) \dots (x_i - x_{n+1})}$$

$p_i(x_i) = 1, \ p_i(x_j) = 0$ pro $j \neq i$

2) Sestavíme $p(x)$ jako lin. kom. $p(x) = \sum_{i=1}^{n+1} y_i p_i(x)$. Potom platí: $p(x_i) = y_i p_i(x_i) = y_i$

protože všude jinde je $p_j(x_i) = 0$

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 $\mathbb{Z}_{11}$!!)

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

Nejprve vypočítáme pomocné polynomy $p_1, \ldots, p_5$.
Tyto polynomy splňují: $p_i(x_i) = 1$ a také $j \neq i : p_i(x_j) = 0$.

$$p_1(x) = \frac{(x-2)(x-3)(x-4)(x-5)}{(1-2)(1-3)(1-4)(1-5)} = \frac{x^4+8x^3+5x^2+10}{2} = 6x^4 + 4x^3 + 8x^2 + 5$$
$$p_2(x) = \frac{(x-1)(x-3)(x-4)(x-5)}{(2-1)(2-3)(2-4)(2-5)} = \frac{x^4+9x^3+4x^2+3x+5}{5} = 9x^4 + 4x^3 + 3x^2 + 5x + 1$$
$$p_3(x) = \frac{(x-1)(x-2)(x-4)(x-5)}{(3-1)(3-2)(3-4)(3-5)} = \frac{x^4+10x^3+5x^2+10x+7}{4} = 3x^4 + 8x^3 + 4x^2 + 8x + 10$$
$$p_4(x) = \frac{(x-1)(x-2)(x-3)(x-5)}{(4-1)(4-2)(4-3)(4-5)} = \frac{x^4+8x^2+5x+8}{5} = 9x^4 + 6x^2 + x + 6$$
$$p_5(x) = \frac{(x-1)(x-2)(x-3)(x-4)}{(5-1)(5-2)(5-3)(5-4)} = \frac{x^4+x^3+2x^2+5x+2}{2} = 6x^4 + 6x^3 + x^2 + 8x + 1$$

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

$$
\begin{aligned}
p(x) &= \sum_{i=1}^{5} y_i p_i(x) = 5p_1(x) + p_2(x) + 3p_3(x) + 4p_4(x) + 3p_5(x) \\
&= 3x^4 + 5x^2 + 2x + 6
\end{aligned}
$$

V $\mathbb{Z}_p$: $a^p = a$

$a^{p-1} = 1$

Zredukujte následující polynom do tělesa $\mathbb{Z}_5$:

$\mathbb{Z}_5$ $\quad q(x) = 4x^{20} + 3x^{17} + 2x^{16} + x^{13} + 3x^{12} + 2x^{10} + 4x^9 + 2x^7 + 2x^5 + x + 3$

$p(x) = 4x^4 + 3x + 2x^4 + x + 3x^4 + 2x^2 + 4x + 2x^3 + 2x + x + 3$

$= \boxed{4x^4 + 2x^3 + 2x^2 + x + 3}$

$\mathbb{Z}_7$ $\quad q(x) = 5x^{16} + 6x^{15} + 4x^{13} + x^{12} + 3x^{11} + 6x^{10} + 2x^9 + 3x^7 + 5x^5 + 2x + 1$

$p(x) = 5x^4 + 6x^3 + 4x + x^6 + 3x^5 + 6x^4 + 2x^3 + 3x + 5x^5 + 2x + 1$

$= \boxed{x^6 + x^5 + 4x^4 + x^3 + 2x + 1}$

$a^{p-1} = 1$

tedy: $5x^{16} = 5 \cdot x^6 \cdot x^6 \cdot x^4 = 5 \cdot 1 \cdot 1 \cdot x^4 = 5x$

Dělení polynomu se zbytkem: Vydělte polynom $p(x)$ lin. polyn. $(x-c)$. Ukažte, že zbytek je roven $p(c)$

Platí: $p(x) = q(x)(x-c) + r(x)$

- stupeň r je menší než st. pol. $(x-c)$, tedy $r(x) = r$
- Dosadím $x = c$ do $p(x) = q(x)(x-c) + r$: $p(c)(c-c) + r = r$