

Příklad. Rozložte polynom $f(x) = x^4 + 1 \in \mathbf{F}_3[x]$ na ireducibilní činitele.

Řešení:

Máme $q = 3$ a $n = \deg f = 4$. Platí $f'(x) = x^3$ a $\text{NSD}(f(x), f'(x)) = 1$. Tedy $f(x)$ nemá vícenásobné činitele.

Spočteme $x^{jq} \bmod f(x)$ pro $j = 0, \dots, n-1$.

$$x^0 \equiv 1 \bmod f(x)$$

$$x^3 \equiv x^3 \bmod f(x)$$

$$x^6 \equiv 2x^2 \bmod f(x)$$

$$x^9 \equiv x \bmod f(x)$$

Dostáváme tedy matici

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Gaussovou eliminací ji přivedeme do odstupňovaného tvaru:

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Báze nulového prostoru je např. $(1, 0, 0, 0), (0, 1, 0, 1)$. Dostáváme tedy $h_2(x) = x + x^3$. Platí $f(x) = \prod_{c \in \mathbf{F}_3} \text{NSD}(f(x), h_2(x) - c)$, tedy spočteme

$$c = 0, \text{ pak } \text{NSD}(x^4 + 1, x^3 + x) = 1$$

$$c = 1, \text{ pak } \text{NSD}(x^4 + 1, x^3 + x - 1) = x^2 + 2x + 2$$

$$c = 2, \text{ pak } \text{NSD}(x^4 + 1, x^3 + x - 2) = x^2 - 2x + 2$$

$$\text{a } f(x) = (x^2 + 2x + 2) \cdot (x^2 - 2x + 2).$$

Co však dělat, je-li $q \gg n$? V tom případě bude $\text{NSD}(f(x), h(x) - c) = 1$ pro většinu $c \in \mathbf{F}_q$. Budeme postupovat podobně jako předtím. Začneme Berlekampovým algoritmem a řešíme soustavu $(B - I)x = 0$, najdeme bázi $h_1(x) = 1, h_2(x), \dots, h_k(x)$. Buď $h(x)$ jeden z těchto polynomů a $f(x) = \prod_{c \in \mathbf{F}_q} \text{NSD}(f(x), h(x) - c)$. Označme $C = \{c \in \mathbf{F}_q; \text{NSD}(f(x), h(x) - c) \neq 1\}$. Potom platí rovnost $f(x) = \prod_{c \in C} \text{NSD}(f(x), h(x) - c)$. Odtud plyne, že $f(x) \mid \prod_{c \in C} (h(x) - c)$. Označme $G(y) = \prod_{c \in C} (y - c)$. Pak $f(x) \mid G(h(x))$.

Věta 7.4. Mezi všemi polynomy $G(y) \in \mathbf{F}_q[y]$, pro které platí $f(x) \mid G(h(x))$, má monický polynom $G(y)$ nejmenší stupeň.

Důkaz. Označme $\{0\} \neq J = \{g(y) \in \mathbf{F}_q[y]; f(x) \mid g(h(x))\} \subseteq \mathbf{F}_q[y]$. Snadno se ověří, že J je ideál v $\mathbf{F}_q[y]$. Jsou-li $g_1(y), g_2(y) \in J$, pak $f(x) \mid g_1(h(x))$, $f(x) \mid g_2(h(x))$ a tedy i $f(x) \mid (g_1 - g_2)(h(x))$. Je-li $k(y) \in \mathbf{F}_q[y]$, pak také $f(x) \mid k(h(x)) \cdot g_1(h(x))$.

Jelikož platí, že okruh $\mathbf{T}[x]$ je obor integrity hlavních ideálů pro libovolné těleso $\mathbf{T}$, je $\mathbf{F}_q[y]$ obor integrity hlavních ideálů. Proto existuje $G_0(y) \in J$ takový, že všechny polynomy v J jsou násobkem $G_0(y)$. $G_0(y)$ je monický polynom nejmenšího stupně v J . Speciálně $G_0(y) \mid G(y) = \prod_{c \in C} (y - c)$, tedy $G_0(y) = \prod_{c \in C_1} (y - c)$ pro nějaké $C_1 \subseteq C$. Protože $f(x) \mid G_0(h(x)) = \prod_{c \in C_1} (h(x) - c)$, platí $f(x) = \prod_{c \in C_1} \text{NSD}(f(x), h(x) - c)$ a odtud plyne $C_1 = C$ a $G_0(y) = G(y)$. $\square$

Jak tuto větu využít? Označme $m = |C|$. Pak $G(y) = \prod_{c \in C} (y - c) = \sum_{j=0}^m b_j y^j$ pro nějaké koeficienty $b_0, b_1, \dots, b_{m-1}$ a $b_m = 1$. Dále platí $f(x) | G(h(x)) = \sum_{j=0}^m b_j h^j(x)$. Proto platí $0 \equiv G(h(x)) \bmod f(x) = (\sum_{j=0}^m b_j h^j(x)) \bmod f(x) = \sum_{j=0}^m b_j (h^j(x) \bmod f(x))$ a tedy platí $0 = \sum_{j=0}^m b_j (h^j(x) \bmod f(x))$.

Z vlastností $G(y)$ (přesněji řečeno z vlastnosti, že $G(y)$ je polynom nejmenšího stupně takový, že $f(x) | G(h(x))$) plyne, že posloupnost polynomů $1 = h^0(x) \bmod f(x), h(x) = h^1(x) \bmod f(x), h^2(x) \bmod f(x), \dots, h^{m-1}(x) \bmod f(x)$ je lineárně nezávislá. Dále z rovnosti $f(x) = \prod_{c \in C} \text{NSD}(f(x), h(x) - c)$ plyne, že $m \leq k$, kde k je počet ireducibilních činitelů v rozkladu $f(x)$, protože počet činitelů na úpravě straně poslední rovnosti (každý z nich má stupeň aspoň 1) nemůže být větší než počet různých ireducibilních dělitelů polynomu $f(x)$.

Jak hledáme $G(y)$? Počítáme postupně $h^j(x) \bmod f(x)$ a první index j , pro který platí, že $h^j(x) \bmod f(x)$ je lineární kombinací $h^i(x) \bmod f(x)$ pro $i = 0, \dots, j-1$, se rovná m . Koeficienty této lineární kombinace jsou $b_0, b_1, \dots, b_{m-1}$. Tak dostaneme polynom $G(y)$, najdeme jeho kořeny C a pak dokončíme Berlekampův algoritmus. Berlekampův algoritmus s využitím polynomu $G(y)$ se nazývá *Zassenhausův algoritmus*.

Příklad. Rozložte polynom $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbf{F}_{23}[x]$ pomocí Zassenhausenova algoritmu.

Řešení:

Máme $n = \deg f = 6$ a $q = 23$. Snadno spočteme, že platí $\text{NSD}(f(x), f'(x)) = 1$.

Začneme počítat Berlekampovým algoritmem. Spočteme $x^{jq} \bmod f(x)$ pro $j = 0, \dots, n-1$. Dostáváme matici

$$B = \begin{pmatrix} 1 & 5 & -10 & 0 & 11 & -3 \\ 0 & 0 & 10 & 7 & 0 & 0 \\ 0 & -1 & 10 & 9 & -4 & -10 \\ 0 & 8 & 0 & -8 & 7 & 9 \\ 0 & -3 & 1 & 10 & 7 & 2 \\ 0 & -10 & -9 & -11 & 2 & -9 \end{pmatrix}$$

Matice $B - I$ má hodnotu 3, báze nulového prostoru je např. $h_1 = (1, 0, 0, 0, 0, 0)$, $h_2 = (0, 4, 2, 1, 0, 0)$, $h_3 = (0, -2, 9, 0, 1, 1)$.

Nyní si vezměme např. $h(x) = h_2(x) = x^3 + 2x^2 + 4x$. Platí

$$\begin{aligned} h^0(x) &\equiv 1 \bmod f(x) \\ h^1(x) &\equiv x^3 + 2x^2 + 4x \bmod f(x) \\ h^2(x) &\equiv 7x^5 + 7x^4 + 2x^3 - 2x^2 - 6x - 7 \bmod f(x) \\ h^3(x) &\equiv -11x^5 - 11x^4 - x^3 - 9x^2 - 5x - 2 \bmod f(x) \end{aligned}$$

Platí $h^3(x) - 5h^2(x) + 11h(x) - 10 \equiv 0 \bmod f(x)$, takže $G(y) = y^3 - 5y^2 + 11y - 10$. Kořeny $G(y)$ jsou $-3, 2 - 6$.

Zbývá spočítat

$$\begin{aligned} \text{NSD}(f(x), x^3 + 2x^2 + 4x + 3) &= x - 4 \\ \text{NSD}(f(x), x^3 + 2x^2 + 4x - 2) &= x^2 - x + 7 \\ \text{NSD}(f(x), x^3 + 2x^2 + 4x - 6) &= x^3 + 2x^2 + 4x - 6 \end{aligned}$$