8. Výpočet kořenů polynomů nad konečnými tělesy

Buď $f(x) \in \mathbf{F}_q[x]$. Při hledání kořenů polynomu f, které leží v $\mathbf{F}_q$, napřed izolujeme tu část polynomu $f(x)$, která obsahuje lineární dělitele. To uděláme snadno, neboť víme, že každý prvek $a \in \mathbf{F}_q$ je kořenem polynomu $x^q - x \in \mathbf{F}_q[x]$. Každý lineární dělitel polynomu $f(x)$ tak dělí také polynom $x^q - x$ a tedy také $\mathrm{NSD}(f(x), x^q - x)$. Tento největší společný dělitel je tak součinem všech lineárních dělitelů polynomu $f(x)$.

Můžeme tedy od začátku předpokládat, že polynom $f(x) \in \mathbf{F}_q[x]$, jehož kořeny chceme najít, se nad $\mathbf{F}_q$ rozkládá na součin lineárních činitelů.

Budeme se zabývat pouze případem, kdy q se rovná nějakému prvočíslu p. Předpokládáme, že

$$f(x) = \prod_{i=1}^{n}(x - c_i),$$

kde $c_1, \ldots, c_n$ jsou navzájem různé prvky $\mathbf{F}_p$. Je-li p mal= číslo, pak lze najít kořeny $f(x)$ zkusmo dosazováním, neboli výpočtem hodnot $f(0), f(1), \ldots, f(p-1)$.

Pro velké $p > 2$ použijeme následující metodu. Pro $b \in \mathbf{F}_p$ platí

$$f(x-b) = \prod_{i=1}^{n}(x - (b + c_i))|x^p - x = x(x^{(p-1)/2} + 1)(x^{(p-1)/2} + 1).$$

Pokud je x dělitelem $f(x-b)$, platí $f(-b) = 0$ a našli jsme kořen $f(x)$.

Pokud x není dělitelem $f(x-b)$, platí $f(x)|x^{(p-1)/2} + 1)(x^{(p-1)/2} + 1)$ a tedy

$$f(x-b) = \mathrm{NSD}(f(x-b), x^{(p-1)/2} + 1)\mathrm{NSD}(f(x), x^{(p-1)/2} - 1).$$

Dělí-li $f(x-b)$ jednoho z činitelů na pravé straně, pak platí buď $x^{(p-1)/2} \equiv 1 \bmod f(x-b)$ nebo $x^{(p-1)/2} \equiv -1 \bmod f(x-b)$. Pokud

$$x^{(p-1)/2} \not\equiv \pm 1 \bmod f(x-b),$$

pak rovnost $f(x-b) = \mathrm{NSD}(f(x-b), x^{(p-1)/2} + 1)\mathrm{NSD}(f(x), x^{(p-1)/2} - 1)$ dává netriviální rozklad $f(x-b)$. Dosadíme-li $x + b$ za x, dostaneme netriviální rozklad $f(x)$. V málo pravděpodobném případě, že $x^{(p-1)/2} \equiv \pm 1 \bmod f(x-b)$ prostě zkusíme jiné $b \in \mathbf{F}_p$. Tím dostáváme pravděpodobnostní algoritmus pro nalezení kořenů $f(x) \in \mathbf{F}_p[x]$. To, jak funguje, si ukážeme v následujícím příkladu.

Příklad. Najděte ty kořeny polynomu $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in \mathbf{F}_{17}$, které leží v $\mathbf{F}_{17}$.

Řešení: Hledané kořeny polynomu $f(x)$ jsou právě kořeny polynomu $g(x) = \mathrm{NSD}(f(x), x^{17} - x)$. Euklidovým algoritmem zjistíme, že $g(x) = x^4 + 6x^3 - 5x^2 + 7x - 2$. Při hledání kořenů $g(x)$ budeme postupovat způsobem uvedený před příkladem.

Napřed zvolíme $b = 0$. Přímým výpočtem zjistíme, že

$$x^{(p-1)/2} = x^8 \equiv 1 \bmod g(x),$$

takže tato volba b nedává netriviální rozklad $g(x)$. Zvolíme tedy $b = 1$. Pak $g(x-1) = x^4 + 2x^3 - 3x - 2$ a $x^{(p-1)/2} = x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \bmod g(x-1)$, takže volba $b = 1$ nám dává nteriviální faktorizaci $g(x-1)$. Platí

$$\mathrm{NSD}(g(x-1), x^8 + 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 4) = x^2 - 7x + 4$$

a

$$\mathrm{NSD}(g(x-1), x^8 - 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 6) = x^2 - 8x + 8,$$

a tedy $g(x-1) = (x^2 - 7x + 4)(x^2 - 8x + 8)$, což vede k částečné faktorizaci

$$g(x) = (x^2 - 5x - 2)(x^2 - 6x + 1) = g_1(x)g_2(x).$$

Abychom rozložili $g_1(x)$ a $g_2(x)$, zkusíme $b = 2$. Platí $g_1(x-2) = x^2 + 8x - 5$ a $x^8 \equiv -8x + 2 \bmod g_1(x-2)$. Spočítáme

$$\mathrm{NSD}(g_1(x-2, x^8 + 1)) = \mathrm{NSD}(x^2 + 8x - 5, -8x + 3) = x + 6$$

a tedy $g_1(x-2) = (x+6)(x+2)$, a také $g_1(x) = (x+8)(x+4)$.

Pokud jde o $g_2(x)$, platí $g_2(x-2) = x^2 + 7x = x(x+7)$, čili -2 je kořen $g_2(x)$ a $g_2(x) = (x+2)(x-8)$. Zjistili jsme tak, že

$$g(x) = g_1(x)g_2(x) = (x+8)(x+4)(x+2)(x-8),$$

a kořeny $g(x)$ a tedy i $f(x)$ v $\mathbf{F}_{17}$ jsou $-8, -4, -2, 8$.

Pro hledání kořenů polynomů s koeficienty v konečných tělesech, která nemají prvočíselnou velikost, se používají jiné algoritmy.