NI-MPI přednáška 17

Algebra V

Štěpán Starosta

14. 12. 2022

FIT ČVUT

Aritmetické operace

Uvedeme si základní přístupy pro provádění aritmetických operací v tělese $GF(p^n)$.

Uvažujeme, že konečné těleso máme vybudováno kanonicky tedy pomocí polynomů nad $\mathbb{Z}_p$ a ireducibilního polynomu (nad $\mathbb{Z}_p$) stupně n.

Budeme uvažovat obecné p a n a elementární operace v $\mathbb{Z}_p$. Např. pro $n = 1$ a $p = 2$ jsou známy lepší algoritmy (co do komplexity).

Sčítání polynomů

Po koeficientech, tedy $\mathcal{O}(n)$.

Násobení

Násobení polynomů: $\mathcal{O}(n^2)$.

Hledání zbytku po dělení: opět $\mathcal{O}(n^2)$.

(Pro polynomy velkých stupňů existují algoritmy, které mohou být efektivnější.)

Celkem: $\mathcal{O}(n^2)$.

Mocnění

Mocněním myslíme výpočet g^k, kde $g \in GF(p^n)$ a $k < p^n$.

Klasický přístup: **metoda opakovaných čtverců** *Square & multiply*, v aditivních grupách *Double & add*

Strategie pro hledání multiplikativních inverzí

Hledáme multiplikativní inverzi k prvku g.

1. hrubou silou: $\mathcal{O}(p^n)$
2. výpočtem g^{p^n-2}: $\mathcal{O}(n^3 \log p)$.
3. EEA: $\mathcal{O}(n^2)$ (toto je výsledek jemnější analýzy, nahrubo vyjde $\mathcal{O}(n^3)$)
4. ...

Např. Itoh-Tsujiho inverze, využívající následující větu

Věta 40.1

Nechť $g \in GF(q^m)^*$ a $r = \frac{q^m-1}{q-1}$. Platí

$$g^{-1} = (g^r)^{-1} g^{r-1}$$

Jelikož g^r je prvkem podstruktury se stejnými vlastnostmi vzhledem k daným operaci (konkrétně podtělesa řádu q), lze dosáhnout lepších výsledků.

EEA: ukázka v $GF(3^3)$

V $GF(3^3)$ počítejme modulo ireducibilní polynom $P(x) = x^3 + 2x + 1$. Hledejme inverzi k $Q(x) = x^2 + 2x + 2$, tj. prvku 122.

1. Počítáme $\gcd(P(x), Q(x))$, vyjde $P(x) = (x+1)Q(x) + x + 2$.
2. Počítáme $\gcd(Q(x), x+2)$, vyjde $Q(x) = x \cdot (x+2) + 2$ a proto $2 = Q(x) - x \cdot (x+2) = (x^2 + x + 1) \cdot Q(x) + 2x \cdot P(x)$.

Tudíž

$$2 \equiv (x^2 + x + 1) \cdot Q(x) \pmod{P(x)},$$

a jelikož $2^{-1} = 2$ v $GF(3)$, dostaneme

$$1 \equiv (2x^2 + 2x + 2) \cdot Q(x) \pmod{P(x)}.$$

Hledanou inverzí k 122 v tomto tělese proto je 222.

Hledání izomorfismu

Mějme prvočíslo p a kladné celé číslo n. Zkonstruujme dvě tělesa řádu p^n pomocí dvou ireducibilních polynomů $f_1 \in \mathbb{Z}_p[x], f_2 \in \mathbb{Z}_p[y]$ stupně n.

Označme tato tělesa F_1 (tady násobíme modulo f_1) a F_2 (tady násobíme modulo f_2).

Víme, že F_1 je izomorfní s F_2. Jak lze najít takový izomorfismus?

(Pro $n = 1$ již umíme...)

Pro lepší čitelnost budeme prvky F_1 psát s formální proměnnou x, prvky F_2 s proměnnou y.

Konstrukce izomorfismu

Mějme $t \in F_1$. Do polynomu f_1 můžeme dosadit t a operace chápat jako operace v F_1, a dostat tedy $f_1(t) \in F_1$.

Prvek $x \in F_1$ splňuje $f_1(x) = 0$ (neboli je kořenem polynomu f_1 nad F_1).

Protože F_1 je izomorfní s F_2, tak nějaký zvolený izomorfismus Ψ zobrazuje $x \in F_1$ na $\Psi(x) \in F_2$. Protože x je kořenem polynomu f_1 a nutně $\Psi(0) = 0$, tak $\Psi(x)$ je kořenem polynomu f_1 **nad** F_2. (Tím myslíme polynom z $\mathbb{Z}_p[y]$ se stejnými koeficienty jako f_1.)

Tedy polynom f_1 nad F_2 má v F_2 kořen. Označme nějaký takový kořen symbolem θ ($\theta \in F_2$).

Označíme-li obecný prvek tělesa F_1 jako $g(x)$ (polynom nad $\mathbb{Z}_p$ stupně nejvýše $n-1$), pak hledané zobrazení definujeme:

$$\Psi : \underbrace{g(x)}_{\in F_1} \mapsto \underbrace{g(\theta)}_{\in F_2}.$$

Náznak důkazu (1 ze 2)

I. Zobrazení Ψ je homomorfismus z F_1 do F_2:

Důkaz: nechť $g_1(x), g_2(x) \in F_1$, pak

$$\Psi(g_1(x) + g_2(x)) = \Psi((g_1 + g_2)(x)) = (g_1 + g_2)(\theta)$$

$$\Psi(g_1(x)) + \Psi(g_2(x)) = g_1(\theta) + g_2(\theta) = (g_1 + g_2)(\theta)$$

$$\Psi(g_1(x) \cdot g_2(x)) = \Psi((g_1(x) \cdot g_2(x) \bmod f_1)(x)) = (g_1(x) \cdot g_2(x) \bmod f_1)(\theta) \bmod f_2$$

$$\begin{aligned} \Psi(g_1(x)) \cdot \Psi(g_2(x)) &= g_1(\theta) \cdot g_2(\theta) \bmod f_2 \\ &= (g_1(x) \bmod f_1)(\theta) \cdot (g_2(x) \bmod f_1)(\theta) \bmod f_2 \\ &= (g_1(x) \cdot g_2(x) \bmod f_1)(\theta) \bmod f_2 \end{aligned}$$

Náznak důkazu (2 ze 2)

II. Zobrazení Ψ je bijekce F_1 a F_2.

Náznak (opravdu!) důkazu: předpokládejme, že $g_1(x), g_2(x) \in F_1$ a $\Psi(g_1(x)) = \Psi(g_2(x))$.

(...)

Protože θ není kořenem nad F_2 žádného polynomu nad $\mathbb{Z}_p$ stupně menšího než n, tak $g_1(x) = g_2(x)$.

Ukázka hledání izomorfismu

Mějme $p = 3, n = 3$ a $f_1(x) = x^3 + 2x + 1$ a $f_2(y) = y^3 + 2y + 2$.

Hledáme θ: kořen f_1 nad F_2.

Označme $\theta = a + by + cy^2 \in F_2$ a hledejme

$$\begin{aligned}
0 = f_1(\theta) &= f_1(a + by + cy^2) \\
&= (a + by + cy^2)^3 + 2(a + by + cy^2) + 1 \\
&= (a^3 + b^3y^3 + c^3y^6) + 2(a + by + cy^2) + 1 \\
&= (a + by^3 + cy^6) + 2(a + by + cy^2) + 1 \\
&= (a + b(y + 1) + c(y^2 + 2y + 1)) + 2(a + by + cy^2) + 1 \\
&= 2cy + b + c + 1
\end{aligned}$$

A tedy $c = 0$, $b = 2$ a a lze zvolit (z $\mathbb{Z}_3$).

Volme $a = 0$ a tedy hledané $\theta = 2y$, a $\Psi(g(x)) = g(2y)$.

Soustavy lineárních kongruencí (1 ze 2)

Problém: řešíme soustavu rovnic

$$\begin{aligned} a &\equiv a_1 \pmod{m_1} \\ a &\equiv a_2 \pmod{m_2} \\ &\vdots \\ a &\equiv a_N \pmod{m_N} \end{aligned} \tag{3}$$

kde $m_1, \ldots, m_N$ jsou navzájem nesoudělná $a_1 \in \mathbb{Z}_{m_1}$, ..., $a_N \in \mathbb{Z}_{m_N}$, a $a \in \mathbb{Z}_n$ je neznámá.

- Pokud nejsou m_i navzájem nesoudělná, nemusí řešení existovat a situace se celkově komplikuje.
- **Myšlenka**: zkusíme zkonstruovat čísla $x_1, \ldots, x_N$ tak, že x_i bude řešit i-tou rovnici, tj. $x_i \equiv a_i \pmod{m_i}$, a pro ostatní rovnice bude $x_i \equiv 0 \pmod{m_k}$, kde $k \neq i$.
- Potom bude jistě $a = x_1 + x_2 + \cdots + x_N$ **řešením soustavy** (3).

Soustavy lineárních kongruencí (2 ze 2)

Jak taková x_i najdeme?

- Položme $M = \prod_{i=1}^{N} m_i$ a $M_i = \frac{M}{m_i}$ a pomocí postupu uvedeného dříve vyřešme rovnici

$$y_i M_i \equiv 1 \pmod{m_i}.$$

  s neznámou y_i.

- Položíme-li

$$x_i = y_i M_i a_i,$$

  dostáváme čísla s požadovanými vlastnostmi, a tedy

$$a = y_1 M_1 a_1 + y_2 M_2 a_2 + \cdots + y_N M_N a_N.$$

- Tím jsme (skoro) dokázali slavnou čínskou větu o zbytcích.

Čínská věta o zbytcích

Věta 42.1 (Čínská věta o zbytcích (*Chinese remainder theorem – CRT*))

Nechť $m_1, \ldots, m_N$ jsou navzájem nesoudělná čísla a nechť $M = \prod_{i=1}^{N} m_i$. Pro libovolnou N-tici $a_1 \in \mathbb{Z}_{m_1}$, ..., $a_N \in \mathbb{Z}_{m_N}$ existuje jednoznačně určené $a \in \mathbb{Z}_M$ tak, že

$$a \equiv a_i \pmod{m_i} \quad \text{pro všechna } i = 1, \ldots, N.$$

Platí

$$a \equiv \sum_{i=1}^{N} a_i y_i M_i \pmod{M},$$

kde $M_i = \frac{M}{m_i}$ a pro všechna i a $j \neq i$ platí

$$y_i M_i \equiv 1 \pmod{m_i} \quad \text{a} \quad y_i M_i \equiv 0 \pmod{m_j}.$$

Existenci řešení jsme ukázali, dokonce i postup jak jej nalézt. Zbývá dokázat jednoznačnost.

CRT: důkaz jednoznačnosti řešení

Při zachování značení z předchozí věty označme

$$\Gamma : \mathbb{Z}_M^+ \mapsto \mathbb{Z}_{m_1}^+ \times \cdots \times \mathbb{Z}_{m_N}^+$$

zobrazení, které číslu $a \in \mathbb{Z}_M^+$ přiřadí N-tici $(a_1, \ldots, a_N)$, kde platí $a \equiv a_i \pmod{m_i}$ pro všechna i.

- CRT nám říká, jak najít vzor N-tice $(a_1, \ldots, a_N)$ při zobrazení Γ (rozmyslet!).
- Zatím jsme si ukázali, že zobrazení Γ je surjektivní, neb pro každou N-tici $(a_1, \ldots, a_N)$ umíme najít $a \in \mathbb{Z}_M$ tak, že $\Gamma(a) = (a_1, \ldots, a_N)$.
- Jelikož jsou ale množiny $\mathbb{Z}_M^+$ a $\mathbb{Z}_{m_1}^+ \times \cdots \times \mathbb{Z}_{m_N}^+$ stejně velké, musí toto zobrazení být i injektivní, a tedy se jedná o bijekci.
- Je tedy nemožné, aby dvě různé N-tice měly dva různé vzory a jednoznačnost řešení a z CRT je dokázána!

Residue number system

Zobrazení Γ je (dokažte si!):

- izomorfismus grupy $\mathbb{Z}_M^+$ a grupy $\mathbb{Z}_{m_1}^+ \times \cdots \times \mathbb{Z}_{m_N}^+$, kde bereme operaci sčítání po složkách: i-tou složku sčítáme modulo m_i;
- izomorfismus grupy $\mathbb{Z}_M^\times$ a grupy $\mathbb{Z}_{m_1}^\times \times \cdots \times \mathbb{Z}_{m_N}^\times$, kde bereme operaci násobení po složkách: i-tou složku násobíme modulo m_i.

Zobrazení Γ určuje tzv. Residue number system. Místo modulo M počítáme v systému modulo $(m_1, \ldots, m_N)$. Jelikož zobrazení lze chápat též jako izomorfismus mezi **okruhy** $\mathbb{Z}_M$ a

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_N},$$

jediná problematická operace v tomto číselném systému zůstane dělení.