Počítačová algebra

Cvičení

27. března 2020

Problém 1. Spočtěte pomocí FFT algoritmu v tělese $\mathbb{Z}_{13}$ hodnotu

$$\mathrm{FFT}(4, 8; 1, 1, 2, 3)$$

(tj. $n = 4$, $\omega = 8$ a polynom je $1 + x + 2x^2 + 3x^3$).

Řešení.
$FFT(n = 4, \omega = 8, (1, 1, 2, 3)) :$
$b_0, b_1?$
$FFT(n = 2, \omega = -1, (1, 2)) :$
$b = FFT(n = 1, \omega = 1, 1) = 1$
$c = FFT(n = 1, \omega = 1, 1) = 2$
$d_0 = b + \omega^0 c = 3, \quad d_1 = b - \omega^0 c = -1$
vrátili jsme se z rekurze, máme $b_0 = 3, b_1 = -1$
$c_0, c_1?$
$FFT(n = 2, \omega = -1, (1, 3)) :$
$b = FFT(n = 1, \omega = 1, 1) = 1$
$c = FFT(n = 1, \omega = 1, 3) = 3$
$d_0 = b + \omega^0 c = 4, \quad d_1 = b - \omega^0 c = -2$
vrátili jsme se z rekurze, máme $c_0 = 4, c_1 = -2$
dopočítáme nejvyšší úroveň:
$d_0 = b_0 + \omega^0 c_0 = 3 + 4 = 7, \quad d_2 = b_0 - \omega^0 c_0 = 3 - 4 = -1 = 12$
$d_1 = b_1 + \omega^0 c_1 = -1 + 8 \cdot (-2) = 9, \quad d_3 = b_1 - \omega^0 c_1 = -1 - 8 \cdot (-2) = 2$
Výsledek je $(7, 9, 12, 2)$.

Problém 2. Pomocí FFT rychle vynásobte v $\mathbb{Z}[x]$ polynomy $x+1$ a x^2-1. Primitivní odmocninu si buď vezměte z $\mathbb{C}$, nebo počítejte modulo velké prvočíslo (Jak velké? Str. 66 v učebnici vám odpoví.).

Řešení. Výsledný polynom má stupeň 3, je tedy určen $n=4$ koeficienty. Budeme počítat v $\mathbb{C}$, jako primitivní čtvrtou domocninu z jedné si vezmeme $\omega = i$.

Spočítáme FFT polynomu $x+1$:
$n=4, \omega = i, (1,1,0,0):$
$n=2, \omega=-1, (1,0)$
$\implies b_0 = 1+0=0, b_1 = 1-0=0$
Druhé rekurzivní volání je totožné, tedy
$c_0 = c_1 = 1$
$d_0 = 1+1=2 \quad d_2 = 1-1=0$
$d_1 = 1+i \quad d_3 = 1-i$
Výsledek je $(2, 1+i, 0, 1-i)$.

Spočítáme FFT polynomu x^2-1:
$n=4, \omega = i, (-1,0,1,0):$
$n=2, \omega=-1, (-1,1):$
$\implies b_0 = -1+1=0, b_1 = -1-1=-2$
Druhé rekurzivní volání počítá s nulama, tedy
$c_0 = c_1 = 0$
$d_0 = 0+0=0 \quad d_2 = 0-0=0$
$d_1 = -2+0i=-2 \quad d_3 = -2-0i=-2$
Výsledek je $(0,-2,0,-2)$.

Pokud obě modulární reprezentace vynásobíme po složkách dostaneme

$$(2, 1+i, 0, 1-i) \cdot (0,-2,0,-2) = (0, -2-2i, 0, -2+2i).$$

Na tento výsledek budeme chtít aplikovat inverzní DFT. Budeme tedy počítat $\frac{1}{4}FFT(n=4, \omega = i^{-1} = -i, (0,-2-2i,0,-2+2i))$:
První rekurzivní volání počítá s nulama, tedy
$b_0 = 0, b_1 = 0$
$n=2, \omega=-1, (-2-2i, -2+2i)$:
$\implies c_0 = (-2-2i)+(-2+2i) = -4 \quad c_1 = (-2-2i)-(-2+2i) = -4i$
$d_0 = 0+(-4) = -4 \quad d_2 = 0-(-4) = 4$
$d_1 = 0+(-i)(-4i) = -4 \quad d_3 = 0-(-i)(-4i) = 4$
Výsledek je $\frac{1}{4}(-4,-4,4,4) = (-1,-1,1,1)$ neboli polynom x^3+x^2-x-1.

Problém 3. Proč nejde modulární metoda násobení použít i na dělení polynomů se zbytkem (třeba v $\mathbb{Z}[x]$)? Ukažte na příkladu, že to nefunguje.

Řešení. Příklad je například $(x^2+1) : x$ v bodech $0, 1, -1$. Dojde tam k dělení nulou a i kdyby nedošlo, tak vyjdou nesmyslné polynomy.

Pro modulární násobení polynomů jsme využívali fakt, že

$$(f \cdot g)(a) = f(a) \cdot f(a),$$

(první násobení je v $T[x]$, druhé v T). Jak bychom vztah upravili např. pro mod? Něco jako

$$(f \bmod g)(a) \stackrel{?}{=} f(a) \bmod g(a)$$

neplatí (už třeba proto, že v tělese jsou všechny prvky dělitelné přesně - ne se zbytkem).

Problém 4 (Schönhage-Strassenův trik)**.** Dokažte podrobně, že 2^u je 2^k-tá primitivní odmocnina z 1 v $\mathbb{Z}_{2^{2^{k-1}u}+1}$.

Řešení. Jde o $\sqrt[2^k]{1}$, protože $(2^u)^{2^k} = 2^{u2^{k-1}\cdot 2} = (2^{u2^{k-1}})^2 = (-1)^2 = 1$.
Předpokládejme pro spor, že 2^u není primitivní odmocnina, tedy, že $(2^u)^{2^c} = 1$ pro $c < k$. Potom

$$1 = 1^{2^{k-1-c}} = ((2^u)^{2^c})^{2^{k-1-c}} = 2^{u2^{k-1-c}2^c} = 2^{u2^{k-1}} = -1.$$

Problém 5 (Barto, Stanovský, cv. 1 na str. 74)**.** Najděte inverzní mocninnou řadu k $x^2 + x + 1$.

Řešení. Hledáme $b_0, b_1, b_2, \dots$ t.ž.

$$(1x^0 + 1x^1 + 1x^2)(b_0x^0 + b_1x^1 + b_2x^2 + \dots) = 1.$$

Ze vzorce pro násobení mocninných řad máme podmínky

$$\begin{aligned}
1 &= 1 \cdot b_0 \\
0 &= 1 \cdot b_0 + 1 \cdot b_1 \\
0 &= 1 \cdot b_0 + 1 \cdot b_1 + 1 \cdot b_2 \\
0 &= 1 \cdot b_1 + 1 \cdot b_2 + 1 \cdot b_3 \\
0 &= 1 \cdot b_2 + 1 \cdot b_3 + 1 \cdot b_4 \\
0 &= 1 \cdot b_3 + 1 \cdot b_4 + 1 \cdot b_5 \\
&\vdots
\end{aligned}$$

neboli

$$\begin{aligned}
b_0 &= 1 \\
b_1 &= -b_0 &&= -1 \\
b_2 &= -b_0 - b_1 &&= 0 \\
b_3 &= -b_1 - b_2 &&= 1 \\
b_4 &= -b_2 - b_3 &&= -1 \\
b_5 &= -b_3 - b_4 &&= 0 \\
&\vdots
\end{aligned}$$

Dostáváme, že

$$(x^2 + x + 1)^{-1} = \sum_{i=1}^{\infty} x^{3i} - x^{3i+1}.$$

Problém 6 (Barto, Stanovský, cv. 2 na str. 74)**.** Spočtěte pomocí inverzních mocninných řad podíl $x^4 + 2x^3 + 2 : x^3 - x$ v $\mathbb{Z}[x]$.

Řešení.

$$\begin{aligned} f &= x^4 + 2x^3 + 2, & n &= 4 \\ g &= x^3 - x, & m &= 3 \\ f^* &= 2x^4 + 2x + 1 \\ g^* &= -x^2 + 1 \end{aligned}$$

Potřebujeme určit prvních $n - m + 1 = 2$ členů řady, kterou když vynásobíme s g^*, dostaneme 1. Její konstatní člen musí být 1 a koeficient u x musí být 0. To je vše co potřebujeme.
Položíme tedy

$$h = 1$$

a počítáme

$$w = f^* \cdot h \bmod x^{n-m+1} = 2x^4 + 2x + 1 \bmod x^2 = 2x + 1.$$

Obrátíme pořadí koeficientů u w a dostaneme

$$q = x + 2.$$

Nyní již snadno dopočítáme zbytek

$$r = f - gq = x^2 + 3x + 2.$$