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 $1 + x + 2x^2 + 3x^3$).

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.).

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.

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

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

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