Počítačová algebra: Cvičení 3

7. listopadu 2022

1. Sestrojte okruhy polynomů nad okruhy $\mathbb{Z}$, $\mathbb{Z}_{13}$ a $\mathbb{Q}[x]/(x^2+1)$. Rozložte nad těmito okruhy polynom $x^4 - 1$.

2. Najděte v Sagi metodu, která vám vrátí náhodný celočíselný polynom daného stupně *deg* s celočíselnými koeficienty z intervalu $[a, b]$.

   Hint: Většina struktur v Sagi, jejichž základem je nějaká množina, obsahuje metodu .random_element(). *Koukněte se do její dokumentace u polynomů.*

3. Naprogramujte funkce na vyčíslování polynomů v daném bodě α. Udělejte to jednak pomocí přímočarého vyhodnocení (počítání mocnin α), jednak pomocí Hornerova schématu. Porovnejte rychlosti navzájem a i se zabudovaným vyhodnocování v Sagi.

4. Naprogramujte algoritmus na školské násobení dvou polynomů.

5. Najděte celé číslo, které má v modulární reprezenaci $x \to (x \mod 251, x \mod 1511, x \mod 2048)$ hodnotu $(156, 1004, 751)$. Je jednoznačně určeno?

6. Pokud jste to ještě neudělali, tak v Sagi najděte funkci řešící přesně předchozí typ úlohy, tedy převod z modulární reprezentace na normální pomocí čínské zbytkové věty.

   Hint: Anglicky Chinese remainder theorem, zkracuje se jako crt ...

7. Najděte nějaký polynom f nad $\mathbb{Z}_7$, který splňuje $f(3) = 2$, $f(-1) = 5$ a $f \equiv 4x + 3 \pmod{x^2 + 1}$. Jak vypadá množina všech takovýchto polynomů?

   Hint: Nejde také použít funkce z předchozí úlohy?

8. Naprogramujte funkci, která pro zadané celočíselné hodnoty a_i, b_i, $1 \leq i \leq n$ (a_i po dvou různé) najde polynom splňující $f(a_i) = b_i$ pomocí Lagrangeova algoritmu.

   Poznámka: Pro zjednodušení můžete předpokládat, že jsou hodnoty racionální a hledáte racionální polynom, třeba v proměnné x (obecná verze by předpokládala, že jsou a_i, b_i ze stejného tělesa a vracela by polynomy nad tímto tělesem).

9. Naprogramujte Euklidův algoritmus na počítání NSD dvou polynomů v $\mathbb{Q}[x]$. Pozorujte, jak v průběhu výpočtu exponenciálně rostou koeficienty.

10. Rozmyslete si, jak aplikovat Karacubův trik na rychlejší násobení polynomů a daný algoritmus naprogramujte. Porovnejte rychlost s klasickým školským násobením.