

Počítačová algebra – DÚ č. 2

Termín odevzdání: 10. prosince 2024, 12:00

Naprogramujte Garnerův algoritmus pro převod z modulární reprezentace. Výstupem by měla být funkce `garner(r,m)` fungující pro obecný Euklidovský obor R (euklidovskost využijeme na dělení se zbytkem). Na vstupu bude seznam zbytků $\mathbf{r} = [r_1, \dots, r_n] \in R^n$ a seznam po dvou nesoudělných modulů $\mathbf{m} = [m_1, \dots, m_n] \in R^n$, výstupem bude prvek $a \in R$ splňující $a \equiv r_i \pmod{m_i}$ pro všechna $i \in \{1, \dots, n\}$. (Pro nalezení modulárních inverzů se může hodit metoda `inverse_mod` nebo funkce `xgcd`, nemusíte to psát sami).

Aplikujte funkci na nějaké vstupy z oborů $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}_{13}[x]$ a $\mathbb{F}_4[x]$ (kde $\mathbb{F}_4$ je čtyřprvkové těleso). Ověřte, že na těchto datech dává funkce správné hodnoty (ke srovnání lze použít funkci `crt`).

Úkol (vypracovaný v Jupyter notebooku či jiném čitelném formátu) prosím odevzdejte v systému Sova <https://owl.mff.cuni.cz/>.