Počítačová algebra – DÚ č. 2

Termín odevzdání: 20. listopadu 2022, 23:59

Naprogramujte Garnerův algoritmus pro převod z modulární reprezentace. Výstupem by měla být funkce *garner(r,m)* fungující pro obecný obor integrity hlavních ideálů R.

VSTUP:

- r: seznam $[r_1, \ldots, r_n]$ zbytků
- m: seznam $[m_1, \ldots, m_n]$ po dvou nesoudělných modulů

Prvky r_i, m_i jsou prvky nějakého OIHI R.

VÝSTUP:
Prvek $a \in R$ splňující $a \equiv r_i \pmod{m_i}$.

Aplikujte funkci pro nějaké konkrétní hodnoty vstupu z oborů $\mathbb{Z}, \mathbb{Q}[x], \mathbb{Z}_{13}[x]$ a $\left(\mathbb{Q}[t]/(t^2+1)\right)[x]$. Ověřte, že na těchto datech dává funkce správné hodnoty (ke srovnání lze použít funkci *crt*).

Co se stane, když do funkce dáte jako vstup prvky z okruhu celočíselných polynomů? Proč?

Hint: K úspěšnému naprogramování se může hodit funkce *xgcd*.
Upozornění na častou chybu: Při testování na konkrétních oborech si dávejte pozor, aby prvky, které do funkce předáváte, byly skutečně ze chtěného oboru. A taky aby m_i byly nesoudělné.