

Počítačová algebra – DÚ č. 2
Termín odevzdání: 18. listopadu 2021, 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 $[r_1, \dots, r_n]$ zbytků
- m : seznam $[m_1, \dots, m_n]$ 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 na alespoň 5 různých konkrétních oborů R (alespoň jeden z nich by měl být okruh polynomů) pro nějaké konkrétní hodnoty vstupu a ověřte, že na těchto datech dává 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*.