Polinomosztás

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Írjuk fel a maradékos osztás tételét polinomokra.

2. Definiáljuk az *osztó* fogalmát integritási tartományban. Mutassuk be a definíciót konkrét polinomokon.

3. Definiáljuk az *egység* fogalmát. Mik $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ és $\mathbb{R}$ egységei?

4. Definiáljuk az *asszociált* fogalmát. Adjuk meg $x^2 + x + 2$ *két* asszociáltját $\mathbb{R}[x]$-ben.

5. Definiáljuk az *irreducibilis* elem fogalmát integritási tartományokban. Mik ezek $\mathbb{Z}$-ben?

6. a) Adjunk példát irreducibilis polinomra $\mathbb{R}[x]$-ben.
b) Adjunk példát másodfokú irreducibilis polinomra $\mathbb{Z}[x]$-ben.
c) Adjunk példát olyan polinomra, amely $\mathbb{R}[x]$-ben irreducibilis, de $\mathbb{C}[x]$-ben nem az.
d) Adjunk példát olyan polinomra, amely $\mathbb{Z}[x]$-ben irreducibilis, de $\mathbb{R}[x]$-ben nem az.

7. a) Definiáljuk a *legnagyobb közös osztó* fogalmát integritási tartományban.
b) Definiáljuk a *legkisebb közös többszörös* fogalmát integritási tartományban.

8. Definiáljuk az *algebrai derivált* fogalmát. Mi $p = 5x^5 + 4x^3 - 3x^2 + 5x - 10 \in \mathbb{Z}[x]$ algebrai deriváltja?

9. Ha $c \in \mathbb{Q}$ a $p \in \mathbb{Q}[x]$ polinomnak négyszeres gyöke, $q \in \mathbb{Q}[x]$-nek pedig kétszeres gyöke, akkor hányszoros gyöke
a) $\text{lnko}(p, q)$-nak; b) p'-nek; c) $\text{lnko}(p, p')$-nek; d) $p \,/\, \text{lnko}(p, p')$-nek?

Programozási feladatok

10. Írjunk függvényt, amely kiszámítja egy p polinom $x - c$-vel vett maradékos osztásának hányadosát és maradékát egyszerre, a Horner-módszerrel. (A polinomnak csak az együtthatóit használhatjuk.) Az eredményt ugyanolyan formában adja vissza, mint `p.quo_rem(x-c)`.

11. Implementáljuk a CRC-t a következők szerint, a $g = x^4 + x + 1$ generátorpolinommal.

a) Írjunk függvényt, amely egy adott m üzenetből (ami egy bitsorozat) kiszámítja az elküldött kódszót, azaz m-et kiegészítve a CRC ellenőrző kóddal. Használhatjuk a Sage polinom-műveleteit, de a bemenő és a visszatérési érték ne polinom, hanem bitsorozat legyen, azaz 0-k és 1-esek listája.

b) Írjunk függvényt, amely a kapott kódszót ellenőrzi, és visszaadja, hogy helyesnek találta-e.

c) Generáljunk egy véletlen 16-bites m üzenetet, és próbáljuk ki rajta a)-t, majd a kapott kódszót ellenőrizzük b)-vel.

d) Rontsuk el a kapott kódszót, és ellenőrizzük azt is.

e) Rontsuk el a kapott kódszót úgy, hogy az ellenőrzésen átmenjen.

12. a) Adaptáljuk az euklideszi algoritmust polinomokra. (Kell rajta bármit változtatni?)

b) Adaptáljuk a bővített euklideszi algoritmust polinomokra. (És ezen?)

c) Próbáljuk ki mind a kettőt a $2x^3 + x^2 - 2x - 1$ és az $x^2 - 2x + 1$ polinomokra $\mathbb{Q}[x]$-ben, és ellenőrizzük az eredményt a Sage megfelelő függvényeivel.

d) Határozzuk meg $2x^3 + x^2 - 2x - 1$ és $x^2 - 2x + 1$ közös gyökeit anélkül, hogy a két polinom gyökeit külön-külön kiszámítanánk.

13. Keressünk olyan $c \in \mathbb{Z}_{19}$ elemet, amelyre $x^2 + cx + c^2 \mid x^5 + x^3 + \overline{4}x + \overline{2}$, ahol mindkét polinom $\mathbb{Z}_{19}[x]$-ben értendő.

14. Írjunk függvényt, amely kiszámítja egy polinom algebrai deriváltját. Csak az együtthatóival dolgozzunk, ne használjunk polinommműveleteket.

15. a) Állítsuk elő azt a hatodfokú $p \in \mathbb{Q}[x]$ polinomot, melynek egyszeres gyöke a 3, kétszeres gyöke az 5, és háromszoros gyöke a 8. Ellenőrizzük a gyököket a Sage segítségével.

b) Számítsuk ki p' gyökeit. Mi a köze p gyökeihez?

c) Számítsuk ki $\mathrm{lnko}(p, p')$ gyökeit. Mi a köze p gyökeihez?

d) Számítsuk ki $p \,/\, \mathrm{lnko}(p, p')$ gyökeit. Mi a köze p gyökeihez?

16. Írjunk függvényt, amely egy adott p polinomra és c számra kiszámítja $p(c)$-t és $p'(c)$-t egyszerre, a Horner-módszer segítségével, p' kiszámítása nélkül. (A polinomnak csak az együtthatóit használhatjuk.)