

Polinomok alapjai

Feladatsor

Diszkrét modellek alkalmazásai

Matematikai kérdések

1. Mik az $2x^4 - 2x^3 + 3x + 1$ polinom együtthatói, főegyütthatója, konstans tagja, másodfokú együtthatója és fokszáma?
2. Hozzuk az alábbi polinomokat kanonikus alakra:
a) $1 + x - x^2 + x - 2$; b) $(x + 1)^3$; c) $(x^2 + 2)(2x - 3)$; d) $(x + 1)(x + 2) - (x - 1)(x - 2)$.
3. Írjuk fel a p polinomot a Horner-módszerben használt alakba, és értékeljük ki a c helyen:
a) $p = 2x^3 - x^2 - 4x + 3$, $c = 2$;
b) $p = 2x^4 - 5x^3 - 6x^2 + 3x + 2$, $c = -1$;
c) $p = x^4 - 2x^3 - 2x - 20$, $c = 3$.
4. Mi a feltétele annak, hogy egy p polinomnak kétszeres gyöke legyen az 5?
5. a) Legfeljebb hány gyöke lehet egy hatodfokú polinomnak?
b) Legfeljebb hány különböző gyöke lehet egy hatodfokú polinomnak, ha tudjuk, hogy van két különböző kétszeres gyöke?
6. Írjuk fel az algebra alaptételét.
7. Írjuk fel a $p = 4x^2 + 2x - 2$ polinomot gyöktényezős alakban.
8. Számítsuk ki azt a p polinomot (kanonikus alakban), amelyre:
a) $\deg p = 2$, $p(3) = 0$, $p(4) = 2$, $p(5) = 0$;
b) $\deg p = 2$, $p(1) = 1$, $p(2) = 0$, $p(3) = -3$;
c) $\deg p = 2$, $p(1) = 1$, $p(2) = 3$, $p(4) = 1$;
d) $\deg p = 2$, $p(0) = 1$, $p(1) = 4$, $p(-1) = 4$;
e) $\deg p = 1$, $p(5) = 7$, $p(7) = 5$;
f) $\deg p = 3$, $p(1) = 0$, $p(2) = 0$, $p(3) = 0$, $p(5) = 4$.
Ellenőrizzük, hogy az eredményen teljesülnek a megadott feltételek.

Programozási feladatok

9. Állítsuk elő az alábbi polinomokat tetszőleges $n \in \mathbb{N}^+$ -ra. Írassuk ki őket $n = 4$ -re.
(Az eredmény típusa polinom legyen, ne általános szimbolikus kifejezés. Ezt ellenőrizhetjük `type(p)`-vel, vagy például hogy működik-e rajta a `p.degree()` lekérdezés.)
- a) $nx^n + (n-1)x^{n-1} + (n-2)x^{n-2} + \dots + 2x^2 + x$;
 - b) $x^{2n} + x^{2n-2} + \dots + x^4 + x^2 + 1$;
 - c) melynek gyökei $1, 2, 3, \dots, n$ (mind egyszeres);
 - d) melynek egyetlen, de n -szeres gyöke a 2;
 - e) melynek 1-szeres gyöke az 1, 2-szeres gyöke a 2, $\dots$, n -szeres gyöke az n , és más gyöke nincs.
10. Írjunk függvényt, amely kiszámítja egy p polinom c helyen felvett helyettesítési értékét a Horner-módszerrel. (A polinomnak csak az együtthatóit használhatjuk.) Teszteljük a 3-as feladat példáira, valamint a $p = x^{1000000} - x^{999999} - \dots - x^2 - x - 1$ polinomra a $c = 2$ helyen.
11. Keressünk olyan c egész számot, amelyre az $x^5 - cx^2 - cx + 1$ polinomnak van többszörös gyöke. Használhatjuk a Sage gyökkereső függvényét.
12. Implementáljuk a Lagrange-interpolációt, azaz írjunk függvényt, amely kap $n+1$ helyettesítési értéket egy listában: $[(x_1, y_1), (x_2, y_2), \dots, (x_{n+1}, y_{n+1})]$ (ahol x_i -k mind különbözőek), és kiszámítja azt a legfeljebb n -edfokú polinomot, amelyre $p(x_1) = y_1, p(x_2) = y_2, \dots, p(x_{n+1}) = y_{n+1}$. Ne használjuk a Sage interpolációs függvényét, legfeljebb ellenőrzésre.
13. Szimuláljuk a Shamir-féle titokmegosztást $\mathbb{Q}[x]$ -ben:
- a) Írjunk függvényt, amely az n, k, S paraméterekből generálja az n résztvevő titokrészeit. Visszatérési érték: (x_i, y_i) pontok n -elemű listája. A kiértékelési helyek legyenek $1, 2, 3, \dots$, az együtthatók pedig 1 és 100 közötti véletlen számok.
 - b) Írjunk függvényt, amely a fenti n részből pontosan k -t kap meg (egy k -elemű listát az (x_i, y_i) pontokkal), és ebből visszaállítja az S titkot. Ellenőrizzük, hogy ha különféleképpen választunk ki k titokrészt az n -ből, akkor is ugyanazt a titkot kapjuk vissza.
14. A Shamir-féle titokmegosztás $\mathbb{Q}[x]$ -ben nem teljesen biztonságos. Ennek belátásához generáljunk titokrészeket egy rögzített S titokhoz $n = 5$ résztvevővel és $k = 3$ küszöbértékkel az előző feladat alapján, és próbáljuk meg azt megfejteni a szükséges három helyett mindössze két titokrész ismeretében. Egészen pontosan vegyük a $(3, y_3)$ és a $(4, y_4)$ ismert titokrészeket, és az "ismeretlen" $(5, y_5)$ részt próbálgassuk végig minden y_5 -re 1-től 100-ig. Számítsuk ki minden esetben a feltételezett S titkot, és írassuk ki ezek maradékát 12-vel osztva. Ha a módszer biztonságos lenne, akkor minden maradék egyenlő eséllyel fordulna elő, azaz semmit nem tudnánk meg az S -ről csupán két titokrész ismeretében. Ehhez képest mit tapasztalunk? Mennyivel kerültünk közelebb az S megfejtéséhez? (A probléma matematikai magyarázata a jegyzet végén található, és a biztonságos verzióról a következő jegyzetben lesz szó.)