FELADATOK A
BEVEZETŐ FEJEZETEK A MATEMATIKÁBA
TÁRGY III. FÉLÉVÉHEZ

ÖSSZEÁLLÍTOTTA: LÁNG CSABÁNÉ
ELTE IK Budapest 2007-07-25

A 2. és a 4. fejezet feladatai megoldva megtalálhatók a *Testbővítés, véges testek; hibajavító kódok: Példák és megoldások* anyagban.

Az 1. fejezet feladataihoz hasonlóak megoldva találhatóak a *Polinomok: Példák és megoldások* anyagban.

Mindkettő letölthető Láng Csabáné honlapjáról:

http: //compalg.inf.elte.hu/∼zslang

valamint az IK Digitális Könyvtárából:

//www.inf.elte.hu/konyv_jegyzet_kep/digitalis_tar/oktatast_tamogato_letoltheto_anyagok

Mind a négy témakörben megoldott példák találhatók a következő, nyomtatásban megjelent és a Jegyzetboltban kapható példatárban:

Gonda János: *Gyakorlatok és feladatok a Bevezetés a matematikába c. tárgyhoz Polinomok, véges testek, kongruenciák, kódolás* ELTE TTK, Budapest, 2001

Tartalomjegyzék

1. Polinomok

1.1. Gyűrűk-testek

1.1-1. Gyűrűt, illetve testet alkotnak-e a szokásos műveletekre:

a. az egész számok;

b. a racionális számok;

c. azok a valós számok, amelyeknek van valós 100-dik gyöke;

d. azok a komplex számok, amelyeknek van valós 100-dik gyöke;

e. azok a komplex számok, amelyeknek van komplex 100-dik gyöke;

f. a 2×2-es, valós elemű mátrixok;

g. a valós együtthatós polinomok.

1.1-2. A modulo m maradékosztályok mikor alkotnak testet a szokásos műveletekre?

1.1-3. Melyek igazak az alábbi állítások közül:

a. Bármely testben $ab = ac,\ a \neq 0 \Rightarrow b = c$.

b. Bármely gyűrűben $ab = ac,\ a \neq 0 \Rightarrow b = c$.

c. Ha egy kommutatív, legalább két elemű gyűrűben

$ab = ac,\ a \neq 0 \Rightarrow b = c$, akkor az test.

d. Véges, legalább két elemű kommutatív gyűrűben ha

$ab = ac,\ a \neq 0 \Rightarrow b = c$, akkor az test.

1.1-4. Melyek igazak az alábbi állítások közül:

a. Ha egy testben $d \neq 0$ és $c \cdot d = d$, akkor c egységelem.

b. Ha egy kommutatív gyűrűben $d \neq 0$ és $cd = d$, akkor c egységelem.

1.2. Polinomok maradékos osztása $\mathbb{Q}$ és $\mathbb{Z}_p$ fölött

1.2-5. Legyen $f = x^5 + x^4 - 15x^3 + 25x^2 + 2x - 3$ és $g = x^2 + 4x - 5$.

Végezzünk maradékos osztást az f és g polinomokkal

a. Q fölött,

b. Z_3 fölött

1.2-6. Hogy kell megválasztani a p, q, m értékeket, hogy az $x^3 + px + q$ polinom osztható legyen az $x^2 + mx - 1$ polinommal $\mathbb{C}$ fölött.

1.2-7. Határozza meg az először megadott polinomnak a másodszorra megadott polinommal való osztásakor kapott maradékát $\mathbb{Q}$ fölött.

a. $2x^4 - 3x^3 + 4x^2 - 5x + 6, \quad x^2 - 3x + 1$

b. $x^3 - 3x^2 - x - 1, \quad 3x^2 - 2x + 1$

1.2-8. Hogyan kell megválasztani p, q, m értékét, hogy az $x^4 + px + q$ polinom osztható legyen az $x^2 + mx + 1$ polinommal $\mathbb{Q}$ fölött.

1.3. Legnagyobb közös osztó euklideszi algoritmussal és lineáris kombináció; közös gyök

1.3-9.

a. Keressük meg az 5. feladatban szereplő polinomok legnagyobb közös osztóját $\mathbb{Q}$ fölött. Van-e közös racionális gyökük?

b. Keressük meg a polinomok legnagyobb közös osztóját $\mathbb{Z}_3$ fölött.

1.3-10. Van-e az alábbi polinomoknak közös gyökük $\mathbb{C}$ fölött? (Határozza meg a következő polinomok legnagyobb közös osztóját.)

$$(x^4 + x^3 - 3x^2 - 4x - 1, \quad x^3 + x^2 - x - 1)$$

1.3-11. Bizonyítsa be, hogy $f(x)$ és $g(x)$ $\mathbb{Q}$ fölötti polinomok legnagyobb közös osztója 1, és határozzon meg olyan $u(x)$ és $v(x)$ polinomokat, amelyekre

$$1 = f(x)u(x) + g(x)v(x).$$

a. $f(x) = 3x^3 - 2x^2 + x + 2, \quad g(x) = x^2 - x + 1;$

b. $f(x) = x^4 - x^3 - 4x^2 + 4x + 1, \quad g(x) = x^2 - x + 1$

1.4. Horner-elrendezés

$$f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0 =$$
$$= (\ldots(((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + a_{n-3})\alpha + a_{n-4}\ldots)\alpha + a_0$$

	a_n	a_{n-1}	a_{n-2}	a_{n-3}	$\ldots$	a_1	a_0	$f(\alpha)$
α		$b_{n-1} =$	$b_{n-2} =$	$b_{n-3} =$	$\ldots$	b_1	$b_0 =$	
		$= a_n$	$= a_n\alpha + a_{n-1}$	$= b_{n-2}\alpha + a_{n-2}$	$\ldots$		$= b_1\alpha + a_1$	$b_0\alpha + a_0$
			$= b_{n-1}\alpha + a_{n-1}$					

1.4-12. Keressük meg az $f(x) = x^4 - 3x^3 + x + 6$ polinom helyettesítési értékét a $3, -1, 2, -2$ helyeken.

1.4-13. Határozza meg a következő polinomok osztási maradékát. Oldja meg a feladatot maradékos osztással és Horner-elrendezéssel is.

a. $x^4 - 2x^3 + 4x^2 - 6x + 8$ osztva $x - 1$-gyel,

b. $2x^5 - 5x^3 - 8$ osztva $x + 3$-mal,

c. $4x^3 + x^2$ osztva $x + 1 + i$-vel,

d. $x^3 - x^2 - x$ osztva $x - 1 + 2i$-vel.

1.4-14. Határozzuk meg p értékét úgy, hogy az $f(x) = x^5 + 3x^4 + 5x + p$ polinom osztható legyen $x - 2$-vel. Oldjuk meg a feladatot maradékos osztással és Horner-elrendezéssel is.

A hányados polinom együtthatói a Horner elrendezés során keletkező számok

$$(a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0) : (x - \alpha) =$$
$$a_nx^{n-1} + (a_n\alpha + a_{n-1})x^{n-2} + ((a_n\alpha + a_{n-1})\alpha + a_{n-2})x^{n-3} + \ldots$$
$$\underline{a_nx^n - a_nx^{n-1}\alpha}$$
$$(a_n\alpha + a_{n-1})x^{n-1} + \ldots$$
$$\underline{(a_n\alpha + a_{n-1})x^{n-1} - (a_n\alpha + a_{n-1})\alpha x^{n-2}}$$
$$((a_n\alpha + a_{n-1})\alpha + a_{n-2})x^{n-2}$$

1.5. Többszörös gyök keresése f és f' legnagyobb közös osztójával

1.5-15. Határozza meg az a paramétert úgy, hogy az $x^5 - ax^2 - ax + 1$ polinomnak -1 legalább kétszeres gyöke legyen. Oldja meg a feladatot

a. maradékos osztással,

b. Horner-elrendezéssel,

c. a derivált polinom felhasználásával.

1.5-16. Határozza meg az a, b paraméterek értékét úgy, hogy $ax^4 + bx^3 + 1$ osztható legyen $(x-1)^2$-nel.

1.5-17. Határozza meg a következő polinomok és deriváltjaik legnagyobb közös osztóját:

a. $f(x) = (x-1)^3(x+1)^2(x-3) \quad f \in \mathbb{Z}[x]$

b. $f(x) = (x-1)(x^2-1)(x^3-1)(x^4-1) \quad f \in \mathbb{Z}[x]$

1.5-18. Van-e többszörös gyöke az $f(x) = x^5 - 5x^3 + 5x + 2$ polinomnak?

1.5-19. Bizonyítsuk be, hogy egy, a racionális test felett irreducibilis polinomnak a komplex számok körében sem lehet többszörös gyöke.

1.6. Racionális és egész együtthatós polinomok racionális és egész gyökei; polinomok felbontása

1.6-20. Legyen $f(x)$ egész együtthatós polinom. Bizonyítandó, hogy ha $f(0)$ és $f(1)$ páratlan, akkor az $f(x)$ polinomnak nincs zérushelye az egész számok körében.

1.6-21. Irreducibilisek-e az alábbi polinomok.

a. x^2-2 $\mathbb{Q}$ fölött, $\mathbb{R}$ fölött,

b. x^2-1 tetszőleges test fölött,

c. x^2+1 $\mathbb{Q}$, $\mathbb{R}$ fölött, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_2$ fölött,

d. x^2 és x^2+x $\mathbb{F}_2$ fölött.

1.6-22. Lássuk be, hogy ha az egész együtthatós f polinomnak gyöke a p/q racionális szám, $(p,q)=1$, akkor p osztója a konstans tagnak, q osztója a főegyütthatónak.

1.6-23. Lássuk be, hogy ha $\alpha \in \mathbb{Z}$ gyöke az $f(x) \in \mathbb{Z}[x]$ polinomnak, akkor

$$1-\alpha \left| \sum_0^n a_i \qquad \text{és} \qquad 1+\alpha \right| \sum_0^n (-1)^i a_i$$

1.6-24. Keressük meg az $f(x)=x^3-6x^2+15x-14$ polinom racionális gyökeit.

1.6-25. Keressük meg az $f(x)=x^5-4x^4-6x^3+16x^2+29x+12$ polinom racionális gyökeit.

1.6-26. Adjuk meg az összes olyan c egész számot, amelyre a $81x^{100}+c\cdot x^{65}+64=0$ egyenletnek van racionális gyöke.

1.6-27. Bizonyítsuk be, hogy ha k és n pozitív egészek, és $\sqrt[k]{n}$ nem egész, akkor $\sqrt[k]{n}$ irracionális.

1.6-28. Schönemann–Eisenstein tétel.

Legyen $f(x)=a_0+a_1x+\ldots+a_nx^n, f(x)\in\mathbb{Z}[x]$. Ha létezik p prím, amelyre

(i) $p \not| a_n$,

(ii) $p|a_i (i=0,\ldots,n-1)$,

(iii) $p^2 \not| a_0$,

akkor $f(x)$ felbonthatatlan $\mathbb{Z}$ fölött.

Megjegyzés. Ha egy egész együtthatós polinom felbonthatatlan $\mathbb{Z}$ fölött, akkor a Gauss-tétel következményeként $\mathbb{Q}$ fölött is felbonthatatlan.

1.6-29. Bizonyítsuk be, hogy minden $n\in\mathbb{N}$ esetén létezik $f(x)\in\mathbb{Q}[x]$ n-edfokú irreducibilis polinom.

1.6-30. $f(x)=3x^5+2x^3-12x^2+10x+14$ -et bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ fölött.

1.6-31. $f(x)=20x^4+26x^3+65x^2+91$ -et bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ fölött.

1.6-32. Mik az $f(x)=40x^4+45x+15$ polinom racionális gyökei.

1.6-33. Mik az

$$f(x)=\frac{5}{4}x^3-\frac{15}{2}x^2+\frac{55}{4}x-\frac{15}{2}$$

polinom racionális gyökei.

1.6-34. Mik az $f(x)=x^3+x^2-5x+3$ polinom racionális gyökei.

1.6-35. Bontsuk fel az x^4+1 polinomot irreducibilis polinomok szorzatára

a. $\mathbb{C}$ fölött,

b. $\mathbb{R}$ fölött.

1.6-36. Bontsuk fel $\mathbb{R}$ felett irreducibilis polinomok szorzatára az x^6+27 polinomot.

1.6-37. Bontsuk fel $\mathbb{R}$ felett irreducibilis polinomok szorzatára az x^4+4 polinomot.

1.7. Gyökök és együtthatók közötti összefüggés

Vieta formulák

Legyen R egységelemes integritási tartomány, és tegyük fel, hogy az

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$

n-edfokú polinom – multiplicitással együtt vett – n gyöke mind R-ben van. Legyenek ezek a gyökök $c_1,\ c_2,\ \ldots,\ c_n$. Ekkor

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = \\ &= a_n(x-c_1)(x-c_2)\cdots(x-c_n) = \\ &= a_n\big(x^n - (c_1+c_2+\ldots+c_n)x^{n-1} + \\ &\quad +(c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n)x^{n-2} + \\ &\quad \vdots \\ &\quad +(-1)^n(c_1\cdot c_2\cdots c_n)\big) \end{aligned}$$

amiből

$$\begin{aligned} \frac{a_{n-1}}{a_n} &= -(c_1+c_2+\ldots+c_n) \\ \frac{a_{n-2}}{a_n} &= (c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n) \\ &\vdots \\ \frac{a_0}{a_n} &= (-1)^n(c_1\cdot c_2\cdots c_n) \end{aligned}$$

1.7-38. Határozza meg a d paraméter értékét, ha a $2x^3 - x^2 - 7x + d = 0$ egyenlet két gyökének összege 1.

1.7-39. Számtani sorozat egymás utáni három eleme-e a $8x^3 - 12x^2 - 2x + 3 = 0$ egyenlet három gyöke?

1.7-40. Számítsa ki az $x^3 + 2x - 3 = 0$ egyenlet gyökeinek négyzetösszegét.

1.7-41. Mi az $x^5 - 5x^3 + 5x + 2$ polinom gyökeinek négyzetösszege?

2. Testbővítés, véges testek

2.0.1. Testbővítés, véges testek, felbonthatatlan (irreducibilis) polinomok

2.0-1. Van-e a valós számoknak olyan részteste, amelyet a valós számok minden részteste tartalmaz?

2.0-2. Testet alkotnak-e a szokásos műveletekre a következő halmazok?

a. $T_1 = \left\{a + b\sqrt[4]{2} \mid a, b \in \mathbb{Q}\right\}$ b. $T_2 = \left\{a + bi\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$

2.0-3. Mi a kapcsolat a $\mathbb{Q}(\sqrt{2})$, a $\mathbb{Q}(1+\sqrt{2})$ és a $\mathbb{Q}(\sqrt{8})$ testek között?

2.0-4. Mely a, b racionális számokra teljesül, hogy $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(a + b\sqrt{2})$?

2.0-5. Van-e olyan szám, amellyel bővítve a racionális számok testét, rögtön a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ testet kapjuk?

2.0-6. Felbonthatatlan-e az $x^5 + 5$ polinom $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, illetve $\mathbb{Z}_5$ felett?

2.0-7. Keressük meg $\mathbb{Z}_2$ fölött az összes másod-, harmad-, és negyedfokú felbonthatatlan (irreducibilis) polinomot.

2.0-8. Igazoljuk, hogy az alábbi polinomok felbonthatatlanok (irreducibilisek) $\mathbb{F}_2$ felett.

a. $x^5 + x^2 + \overline{1}$,

b. $x^6 + x + \overline{1}$,

c. $x^7 + x^3 + \overline{1}$.

2.0-9. Hány másodfokú normált (1 főegyütthatójú) irreducibilis polinom van egy q

elemű testben?

2.0-10. Készítsünk 9 elemű testet.

a. Adjuk meg a művelettáblákat.

b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.

c. Határozzuk meg az egyes elemek additív rendjét.

2.0-11. Készítsünk 4 elemű testet.

a. Adjuk meg a művelettáblákat.

b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.

2.0-12.

a. Bizonyítsuk be, hogy az $f(x) = x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.

b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az f többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.

2.0-13.

a. Bizonyítsuk be, hogy az $f(x) = x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.

b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az f többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.

2.0-14.

a. Igazoljuk, hogy $f(x) = x^3 + x + \overline{2}$ reducibilis $\mathbb{Z}_7$ felett.

b. Hány eleme van a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrűnek ($\overline{f}$ az f polinom többszöröseiből álló ideál)? Adjunk meg egy reprezentánsrendszert.

c. Mutassuk meg, hogy a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrű tartalmaz nullosztót.

2.0.2. Elem felírása bázisban

2.0-15. Legyen $u \in \mathbb{C}$ a $\mathbb{Q}$ feletti $x^3 - 2x + 2$ polinom egyik gyöke. Lássuk be, hogy a polinom $\mathbb{Q}$ felett irreducibilis. Írjuk fel $\mathbb{Q}(u) \mid \mathbb{Q}$ $\{1,\ u,\ u^2\}$ bázisában a következő elemeket:

a. u^7 b. u^{-1} c. $u^4 + u^{-2}$

2.0-16. Legyen $u \in \mathbb{C}$ az $x^3 - 6x^2 + 9x + 3$ $\mathbb{Q}$ felett irreducibilis polinom gyöke. Fejezzük ki $\mathbb{Q}(u) \mid \mathbb{Q}$ $\{1,\ u,\ u^2\}$ bázisában a következő elemeket:

a. $3u^5 - 2u$ b. $\frac{1}{1+u}$

2.0.3. Minimálpolinom, felbontási test

2.0-17. Határozzuk meg $\sqrt{2-\sqrt[3]{2}}$ minimálpolinomját $\mathbb{Q}$ felett.
2.0-18. Mutassuk meg, hogy

$$\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}$$

egész szám.
2.0-19. Határozzuk meg az $(x^2+1)(x^2-2x+1)$ polinom felbontási testét $\mathbb{Q}$ felett.
2.0-20. $\mathbb{Q}(\sqrt[3]{2})$ megegyezik-e $\sqrt[3]{2}$ minimálpolinomjának a felbontási testével?
2.0-21. Van-e racionális gyöke az $f(x)=x^3-x^2-x-2$ polinomnak? Mi az $f(x)$ felbontási teste $\mathbb{Q}$ felett?
2.0-22. Bizonyítsuk be, hogy ha $\alpha\in\mathbb{C}$ megoldása a $10x^3-105x^2+84x+210=0$ racionális együtthatós egyenletnek, és valamely K testre fennáll, hogy $\mathbb{Q}(\alpha)|K$ és $K|\mathbb{Q}$, akkor $K=\mathbb{Q}(\alpha)$ vagy $K=\mathbb{Q}$.
2.0-23. Legyen $K=\mathbb{F}_q$, és $f(x)$ K fölötti irreducibilis n-edfokú polinom. Lássuk be, hogy

$$f(x)|x^{q^n}-x.$$

($\mathbb{F}_q$ a q elemű testet jelöli.)
2.0-24. Legyen $K=\mathbb{F}_q$, $f(x)$ K fölötti irreducibilis n-edfokú polinom, és legyen α gyöke f-nek. Lássuk be, hogy K-t α-val bővítve megkapjuk f K fölötti felbontási testét. (Más szóval lássuk be, hogy ha f egyik gyöke a bővített véges testben van, akkor f mindegyik gyöke benne van.) ($\mathbb{F}_q$ a q elemű testet jelöli.)

Megjegyzés. 0 karakterisztikájú testben ez általában nem igaz (lásd a 20. példát).

2.0.4. Bővítés foka, véges és algebrai bővítés

2.0-25. A következő bővítések közül melyik véges és melyik algebrai? (A az algebrai számok halmaza)

a. $\mathbb{C}|\mathbb{R}$ b. $\mathbb{Q}(\sqrt{5})|\mathbb{Q}$ c. $A|\mathbb{Q}$ d. $A|\mathbb{Q}(\sqrt{5})$ e. $\mathbb{R}|\mathbb{Q}(\pi)$

2.0-26. Mennyi a $\mathbb{Q}(\pi)|\mathbb{Q}(\pi^2)$ testbővítés foka?
2.0-27. Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol T az alábbi. Mi a bővítő elem minimálpolinomja $\mathbb{Q}$ fölött? Adjunk meg egy bázist.

a. $\mathbb{Q}(\sqrt{7})$ **b.** $\mathbb{Q}(i\sqrt{5})$
c. $\mathbb{Q}(1+i\sqrt{3})$ **d.** $\mathbb{Q}(i+\sqrt{5})$
e. $\mathbb{Q}(u+i\sqrt{v})$, $u,v\in\mathbb{Q}, \sqrt{v}\notin\mathbb{Q}$

2.0-28. Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol T az alábbi. Adjunk meg egy bázist.

a. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ **b.** $\mathbb{Q}(i,\sqrt{8})$

2.0.5. Véges test elemeinek összege, szorzata, Vieta-formulák, gyökök és együtthatók közötti összefüggések

2.0-29. Bizonyítsuk be a Wilson-tételt: $(p-1)! \equiv -1 \pmod{p}$, ha p prím.
2.0-30. Mennyi valamely véges test nem nulla elemeinek a szorzata?
2.0-31. Véges testben mi az elemek számának paritása?

Vieta-formulák, gyökök és együtthatók közötti összefüggések

Legyen R egységelemes integritási tartomány, és tegyük fel, hogy az

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 \in R[x]$$

n-edfokú polinom – multiplicitással együtt vett – n gyöke mind R-ben van. Legyenek ezek a gyökök $c_1,\ c_2,\ \ldots,\ c_n$. Ekkor

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = \\ &= a_n(x-c_1)(x-c_2)\cdots(x-c_n) = \\ &= a_n\left(x^n - (c_1+c_2+\ldots+c_n)x^{n-1} + \right. \\ &\quad +(c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n)x^{n-2} + \\ &\quad \vdots \\ &\quad \left. +(-1)^n(c_1\cdot c_2\cdots c_n)\right) \end{aligned}$$

amiből

$$\begin{aligned} \frac{a_{n-1}}{a_n} &= -(c_1+c_2+\ldots+c_n) \\ \frac{a_{n-2}}{a_n} &= (c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n) \\ &\vdots \\ \frac{a_0}{a_n} &= (-1)^n(c_1\cdot c_2\cdots c_n) \end{aligned}$$

2.0-32. Legyen L véges test, $|L| = q^k$. Számítsuk ki a következő összeget:

$$\sum_{l\in L} l.$$

2.0-33. Legyen L véges test, $|L| = q^k$. Jelölje L^* az L multiplikatív csoportját. Számítsuk ki a következő szorzatot:

$$\prod_{l\in L^*} l.$$

(Lásd a 30. példát is.)

3. Magasabbfokú kongruenciák

3.1. Gyök keresése modulo p

3.1-1. Keressük meg az f polinom gyökeit modulo 7.

$$f = -6x^{12} + 17x^{10} + 23x^9 - 10x^8 + 6x^6 + 36x^5 + 4x^4 + 18x^3 + 67x^2 + 14x - 21$$

3.1-2. Keressük meg az f polinom gyökeit modulo 7.

$$f = 3x^{23} + 5x^{21} + 5x^{17} + 6x^{15} + 2x^{11} + x^9 + 4x^5 + 2x^3$$

3.1-3. Keressük meg az f polinom gyökeit modulo 7.

$$f = 3x^{23}+5x^{21}+5x^{17}+6x^{15}+2x^{11}+x^9+12x^7+60x^6+51x^5-121x^4-135x^3-10x^2-37x+6$$

3.1-4. Keressük meg az f polinom gyökeit modulo 7.

$$f = -4x^{25} + 12x^{21} + 2x^{19} + 20x^{15} + 4x^{11} - 13x^9 + 3x^8 + 32x^7 + 3x^3 + 4x^2 + 4x + 14$$

3.2. Gyök keresése modulo p^r

3.2-5. Keressük meg az f polinom gyökeit modulo 27.

$$f = x^3 + x^2 + 65x + 11 \quad f$$

3.2-6. Keressük meg az f polinom gyökeit modulo 125.

$$f = x^3 - 2x^2 + 11 \quad f$$

3.2-7. Keressük meg az f polinom gyökeit modulo 27.

$$f = (x-1)^6 =$$
$$\binom{6}{0}x^6 - \binom{6}{1}x^5 + \binom{6}{2}x^4 - \binom{6}{3}x^3 + \binom{6}{4}x^2 - \binom{6}{5}x + \binom{6}{6} =$$
$$= x^6 - 6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x + 1$$

3.2-8. Keressük meg az f polinom gyökeit modulo 8.

$$f = 3x^5 + 2x^4 + 5x^3 + x^2 + 6x + 7$$

3.2-9. Keressük meg az f polinom gyökeit modulo 49.

$$f = 2x^4 - 5x^3 + x^2 + 3x + 5$$

4. Hibajavító kódok

A feladatok általában bináris kódokra vonatkoznak, vagyis olyanokra, amelyek esetén az S alaphalmaz a $\{0,1\}$ halmaz. Néhány feladat általánosabban van megfogalmazva, ezekben az S alaphalmaz tetszőleges nem üres halmaz.

4.0.1. Alapfogalmak

A részleteket lásd a megoldásnál.

4.0.2. Blokk-kódok

4.0-1. Tegyük fel, hogy az üzenetek bináris jelsorozatok, vagyis az $S = \{0,1\}$ halmaz elemeiből épülnek fel. Rendeljünk hozzá a kettő hosszú üzenetekhez öt hosszú kódokat a következő szabály szerint.

$$(0\ 0) \to (0\ 0\ 0\ 0\ 0)$$

$$(0\ 1) \to (0\ 1\ 1\ 1\ 0)$$

$$(1\ 0) \to (1\ 0\ 1\ 0\ 1)$$

$$(1\ 1) \to (1\ 1\ 0\ 1\ 1)$$

Így négy elemből álló blokk-kódot kapunk. Ha a csatornán például a $(0\ 1\ 0\ 0\ 0)$ jelsorozat érkezik, tudjuk, hogy hiba történt, hiszen ez a szó nem szerepel a kódszavak között.

Mekkora az $u = (0\ 1\ 1\ 1\ 0)$ és $v = (1\ 0\ 1\ 0\ 1)$ kódszavak távolsága, a kód távolsága, a $z = (1\ 1\ 0\ 1\ 1)$ vektor súlya, valamint a kód súlya?

4.0-2. Az 1. példa S halmaza legyen $\mathbb{F}_2$, a kételemű test. $\mathbb{F}_2$ az összeadásra csoportot alkot. Az $\mathbb{F}_2$ elemeiből készített n hosszú vektorok is csoportot alkotnak az elemenkénti összeadásra nézve. Lássuk be, hogy a példa K kódhalmaza részcsoport S^n-ben, így K *csoportkód*.

4.0-3. Legyen K az 1. példabeli kód, $u = (0\ 0\ 0\ 0\ 0)$, $t = 1$. Adjuk meg az u körüli 1 sugarú gömbben szereplő sorozatokat.

4.0-4. Az 1. példa kódját alkalmazva tegyük fel, hogy a $(0\ 1\ 0\ 0\ 0)$ hibás jelsorozat érkezik. Minimális távolságú dekódolás esetén melyik szót választjuk helyette?

4.0-5. Legyen $S = \mathbb{F}_2$, a közleményszavak pedig k hosszú sorozatok. Állapítsuk meg, hogy az alábbi kódok esetén mi jellemzi a kódszavakat, mennyi a kód minimális távolsága, hibajelző és (minimális távolságú dekódolással) a hibajavító képessége.

a. Kétszeri ismétlés kódja. A kódszót megkapjuk, ha a közleményszót kétszer egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

kódszó keletkezik.

b. Háromszori ismétlés kódja. A kódszót megkapjuk, ha a közleményszót háromszor egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

kódszó keletkezik.

c. Paritásvizsgálat kódja. A kódszót megkapjuk, ha a közleményszó végére az elemek ($\mathbb{F}_2$-ben számított) összegét írjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \beta), \quad \beta = \sum_{i=1}^{k} \alpha_i$$

kódszó keletkezik.

4.0-6. Hamming-korlát.

Bizonyítsuk be a következőt. Legyen az alaphalmaz S, a $K \subseteq S^n$ kód t-hiba javító. Ekkor

$$|K| \cdot \sum_{i=0}^{t} \binom{n}{i} (s-1)^i \leq s^n,$$

ahol $s = |S|$.

4.0-7. Bináris blokk-kódot készítünk 3 hosszú üzenetekhez. Legalább mekkora legyen a kódszavak hossza, ha azt akarjuk, hogy a kód (minimális távolságú dekódolással) pontosan 1-hiba javító legyen?

4.0-8. k hosszú bináris szavakból (üzenet) 19 hosszú bináris szavakat (kódszót) készítünk. Legfeljebb mekkora lehet az üzenetek hossza, ha azt akarjuk, hogy a kód minimális távolsága 8 legyen?

4.0-9. Állapítsuk meg, hogy van-e 5 minimális távolságú, 13 hosszú perfekt bináris kód?

A K blokk-kód *tökéletes* (*perfekt*), ha a Hamming-korlát egyenlőséggel teljesül. Perfekt kód esetén a kódszavak körüli $\lfloor \frac{d-1}{2} \rfloor$ sugarú gömbök teljesen kitöltik az n hosszú sorozatok terét, s így minden szóhoz pontosan egy kódszó van, amelytől legfeljebb $\lfloor \frac{d-1}{2} \rfloor$ távolságra van.

4.0-10. Létezik-e 3 minimális távolságú perfekt bináris kód $n = 147$ esetén?

4.0-11. Van-e 12 hosszú kódszavakból álló 1-hiba javító perfekt bináris kód?

4.0.3. Lineáris kód alapfogalmai

A részleteket lásd a megoldásnál.

4.0.4. Lineáris kód

4.0-12. Valamely kód generátormátrixa legyen a következő:

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Ezt a mátrixot használva kódolásra, adjuk meg az összes közleményszót, valamint a megfelelő kódszavakat.

4.0-13. Állapítsuk meg, hogy az 5. példa kódjai közül melyik lineáris, és a lineárisoknak adjuk meg a generátormátrixát.

4.0-14. Az alábbi bináris kódok esetében állapítsuk meg a minimális távolságot, a hibajelző illetve (minimális távolságú dekódolással) a hibajavító képességet, valamint azt, hogy melyik lineáris, a lineárisoknak pedig adjuk meg a generátormátrixát.

a. Legyen $k = 3$, $n = 4$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + 1$$

b. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \alpha_2 + \alpha_3$$

c. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \max(\alpha_2, \alpha_3)$$

4.0-15. Lássuk be, hogy ha az $\mathbb{F}_k$ fölötti $[n, k]$ kód generátormátrixa $G = (I_k \quad P)$ alakú, akkor a $H = (-P^T \quad I_{n-k})$ mátrix a kód ellenőrző mátrixa. (I_k a $k \times k$ méretű egységmátrixot jelöli, P pedig tetszőleges $k \times (n-k)$ méretű, $\mathbb{F}_k$ fölötti mátrix.) A kételemű test fölött $-P$ helyett P is írható, mert $\mathbb{F}_2$-ben $1 = -1$.

Megjegyzés. Hasonlóan igaz az is, hogy ha egy $[n,k]$ kód ellenőrző mátrixa $H = (I_{n-k} \quad R)$ alakú, ahol R tetszőleges $((n-k)\times k)$ méretű, $\mathbb{F}_k$ fölötti mátrix, akkor a $G = (-R^T \quad I_k)$ mátrix megfelel generátormátrixnak.

4.0-16. Adjuk meg a 14. példában szereplő lineáris kód ellenőrző mátrixát a

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

generátormátrix felhasználásával.

4.0-17. Lássuk be, hogy egy $[n,k,d]$ kód H ellenőrző mátrixában van d lineárisan összefüggő oszlop, de bármely d-nél kevesebb oszlop lineárisan független.

4.0-18. Adjuk meg a 14. és 16. példában szereplő lineáris kód

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

ellenőrző mátrixának segítségével a kód távolságát és hibajelző, valamint (minimális távolságú dekódolással) a hibajavító képességét.

4.0-19. Legyen egy bináris lineáris kód generátormátrixa:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Adjuk meg az (egyik) ellenőrző mátrixát. Az ellenőrző mátrix felhasználásával mondjuk meg a kódtávolságot.

4.0-20. Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Adjuk meg a kód paritásellenőrző mátrixát és távolságát.

4.0-21. Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Adjuk meg a kód paritásellenőrző mátrixát és távolságát.

4.0-22. Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Mennyi a kód számossága? Adjuk meg a kód paritásellenőrző mátrixát, és ennek segítségével határozzuk meg a távolságát.

4.0-23. Egy bináris kód paritásellenőrző mátrixa

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Lássuk be, hogy 1-hiba javító perfekt lineáris kódról van szó.

4.0.5. Hamming-kód

Az 1-hiba javító perfekt lineáris kódot *Hamming-kódnak* nevezzük.

4.0-24. Hamming-kód készítése.

Bináris Hamming-kódot készíthetünk a következőképpen. Legyen

r pozitív egész szám (ellenőrző jegyek száma),

$n = 2^r - 1$ a kódszavak hossza,

$k = 2^r - 1 - r$ a közleményszavak hossza.

A H $r \times n$-es ellenőrző mátrix j-edik oszlopában a j 2-es számrendszerbeli alakjának jegyei szerepelnek.

Legyen például $r = 3, n = 7, k = 4$. Adjuk meg a kód ellenőrző mátrixát.

4.0-25. Adjuk meg az előző példában megismert szabály szerinti Hamming-kód ellenőrző mátrixát, ha $r = 2$, és ha $r = 4$.

4.0-26. A Hamming-kód generátormátrixa. Adjuk meg a 24. példabeli $[7, 4]$ Hamming-kód H ellenőrző mátrixának ismeretében a kód (egyik) generátormátrixát. Ha ezt a generátormátrixot alkalmazzuk a kódolásnál, mi lesz a $(0\ \ 1\ \ 1\ \ 1)$ üzenet kódja?

4.0-27. Hibajavítás bináris Hamming-kóddal.

A részleteket lásd a megoldásnál.

4.0-28. $[7, 4]$ bináris Hamming-kódnál, feltételezve, hogy egynél több hiba nem lépett fel az átvitelnél, mi volt a továbbított kódvektor, ha

a. $a^T = (0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0)$ illetve

b. $b^T = (0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0)$ érkezett.