MBN211G: KLASSZIKUS ALGEBRA ÉS SZÁMELMÉLET GYAKORLAT

(2010. május 11.)

1. Leképezések és relációk

1.1. Feladat. (1 pt. közösen megbeszéltük)
Döntsük el, hogy az $\mathbb{R}^2$ halmaz $\{\,(x,y) : x^2+y^2=1\,\}$ részhalmaza előáll-e $A\times B$ alakban.

1.2. Feladat. (1 pt. közösen megbeszéltük)
Vizsgáljuk meg, hogy injektív-e, illetve szürjektív-e az alábbi $f:\mathbb{N}\to\mathbb{N}$ leképezés, és adjuk meg az f^2 leképezést.

$$nf=\begin{cases}6n+1, & \text{ha } n \text{ páros, és}\\ 6n-1, & \text{ha } n \text{ páratlan.}\end{cases}$$

1.3. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítandó, hogy ha az $f:A\to B$, $g:B\to C$ és $h:C\to A$ leképezésekre $fgh=\mathrm{id}_A$, továbbá g bijektív, h pedig injektív, akkor az f leképezés szürjektív.

1.4. Feladat. (2 pt.)
Legyen A véges halmaz és $f:A\to A$ leképezés.

(1) Mutassuk meg, hogy van olyan n, hogy $f^{2n}=f^n$.
(2) Az első részt felhasználva mutassuk meg, hogy ha f injektív, akkor bijektív is.
(3) Az első részt felhasználva mutassuk meg, hogy ha f szürjektív, akkor bijektív is.

1.5. Feladat. (3 pt. előadta Ádám)
Legyen $f:\mathbb{N}\to\mathbb{N}$ olyan leképezés, hogy tetszőleges $n\in\mathbb{N}$-re $(n+1)f>nf^2$. Bizonyítsuk, hogy $f=\mathrm{id}_{\mathbb{N}}$.

1.6. Feladat. (2 pt. közösen megbeszéltük)
Tetszőleges n pozitív egészre legyen $Z_n=\{0,\dots,n-1\}$ és R_n a Z_n halmaz n-hez relatív prím elemeinek halmaza. Legyenek m és n relatív prímek. Mutassuk meg, hogy ekkor

(1) az $f:Z_{mn}\to Z_m\times Z_n,\ p\mapsto(p_m,p_n)$, ahol p_m a p m-mel és p_n a p n-nel való nem negativ osztási maradéka, leképezés bijektív,
(2) a $g:R_{mn}\to R_m\times R_n,\ p\mapsto(p_m,p_n)$ jól definiált leképezés és szintén bijektív.

1.7. Feladat. (2 pt. közösen megbeszéltük)
Ha az $f:A\to B$ és $g:B\to A$ leképezésekre fennáll $fg=\mathrm{id}_A$, akkor azt mondjuk, hogy a g az f-nek jobbinverze, f pedig a g-nek balinverze. Adjuk meg

(1) az $f:\mathbb{N}\to\mathbb{N}$, $n\mapsto n^2$ keképezés két különböző jobbinverzét,
(2) a $g:\mathbb{Z}\to\mathbb{N}_0$, $n\mapsto|n|$ leképezés két különböző balinverzét.

1.8. Feladat. (2 pt.)
Legyenek A, B tetszőleges halmazok, s tegyük fel, hogy A-nak legalább két eleme van. Igazoljuk, hogy bármely $f:A\to B$ leképezésre

(1) f akkor és csak akkor injektív, ha f-nek van jobbinverze,
(2) f akkor és csak akkor szürjektív, ha f-nek van balinverze.

1.9. Feladat. (2 pt. előadta Lívia)
Legyen A véges halmaz. Mutassuk meg, hogy tetszőleges $f,g:A\to A$ leképezésekre, ha $fg=\mathrm{id}_A$, akkor $gf=\mathrm{id}_A$. Adjunk példát olyan végtelen A halmazra és f,g leképezésekre, amelyre az állítás nem teljesül.

1.10. Feladat. (1 pt. közösen megbeszéltük)
Legyen $f:X\to Y$ egy leképezés. Bizonyítsuk be, hogy tetszőleges $A,B\subseteq X$ részhalmazokra

(1) $(A \cup B)f = Af \cup Bf$,
(2) $(A \cap B)f \subseteq Af \cap Bf$,
(3) a (2) részben akkor és csak akkor teljesül minden $A, B \subseteq X$ részhalmaz esetén egyenlőség, ha f injektív.

1.11. Feladat. (2 pt.)
Legyen $f : A \to B$ tetszőleges leképezés, továbbá $C \subseteq A,\ D \subseteq B$, és jelölje g az $f \cap (C \times D)$, C-ből D-be menő megfeleltetést. Rögzített $A,\ B,\ C,\ D$ esetén mely f leképezésekre lesz g is leképezés?

1.12. Feladat. (2 pt.)
Határozzuk meg $\alpha\beta$, illetve, ha lehet $\beta\alpha$ szorzatot, ahol $\alpha = \{\,(x, y) : y = \sin x\,\} \subseteq [-\pi, \pi] \times \mathbb{R}$ és $\beta = \{\,(x, y) : y \neq 0, x = y + \frac{1}{y}\,\} \subseteq \mathbb{R} \times \mathbb{R}$.

1.13. Feladat. (2 pt. előadta Gergő)
Fejezzük ki a

(1) $\gamma = \{\,(a, b) : b \text{ az } a \text{ nagyszülője}\,\}$, és
(2) $\delta = \{\,(a, b) : b \text{ az } a \text{ anyai nagyszülője}\,\}$

relációkat az emberek halmazán értelmezett

$$\alpha = \{\,(a, b) : b \text{ az } a \text{ apja}\,\} \text{ és } \beta = \{\,(a, b) : b \text{ az } a \text{ apja vagy anyja}\,\}$$

relációk segítségével.

1.14. Feladat. (3 pt. előadta Ádám)
Legyen ϱ az A halmazból a B halmazba történő tetszőleges megfeleltetés. Bizonyítsuk be, hogy ϱ akkor és csak akkor leképezés, ha $\varrho^{-1}\varrho \subseteq \mathrm{id}_B$, és $\varrho\varrho^{-1} \supseteq \mathrm{id}_A$. Milyen hasonló feltételekkel lehetne leírni az injektív és szürjektív fogalmakat?

1.15. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsuk be, hogy a reflexivitás, a szimmetria és a tranzitivitás egymástól független tulajdonságok, azaz adjunk meg olyan relációt, amely

(1) szimmetrikus és tranzitív, de nem reflexív,
(2) reflexív és tranzitív, de nem szimmetrikus,
(3) reflexív és szimmetrikus, de nem tranzitív.

1.16. Feladat. (2 pt. előadta Fanni)
Tekintsük a $P = (\{4, 6, 7, 14, 24, 42, 48\}, |)$ részbenrendezett halmazt, ahol $|$ a szokásos oszthatósági reláció. Rajzoljuk fel P Hasse-diagramját. Adjuk meg a legkisebb, legnagyobb, minimális, maximális elemeket, amennyiben léteznek.

1.17. Feladat. (2 pt. előadta Gábor)
Mutassuk meg, hogy ha egy véges részbenrendezett halmazban egyetlen minimális elem van, akkor az legkisebb elem is. Adjunk példát olyan végtelen részbenrendezett halmazra, amelyre ez nem teljesül.

1.18. Feladat. (2 pt.)
Defininiáljuk P és Q részbenrendezett halmazok $P \times Q$ szorzatát a következő módon. A $P \times Q$ részbenrendezett halmaz alaphalmaza P és Q alaphalmazainak direktszorzata, valamint $(p, q) \leq (p', q')$ pontosan akkor teljesül $P \times Q$-ban, ha P-ben $p \leq p'$ és Q-ban $q \leq q'$.

(1) Rajzoljuk fel $P \times Q$ Hasse-diagramját, ha $P = (\{4, 6, 7, 14, 24, 42, 48\}, |)$ és $Q = (\{0, 1\}, \leq)$.
(2) Egy véges részbenrendezett halmaz *magassága* láncai hosszának maximuma. Tetszőleges P és Q véges részbenrendezett halmazok esetén fejezzük ki $P \times Q$ magasságát P és Q magasságának segítségével.

1.19. Feladat. (2 pt. közösen megbeszéltük)
Határozzuk meg azokat a relációkat, amelyek egyidejűleg részbenrendezések és ekvivalenciák.

1.20. Feladat. (1 pt. előadta Lívia)
Hány osztályozása van az $\{1, 2, 3, 4\}$ halmaznak?

1.21. Feladat. (2 pt.)
Legyen $f : A \to B$ szürjektív, $g : A \to C$ pedig tetszőleges leképezés. Mutassuk meg, hogy

(1) akkor és csak akkor létezik olyan $h : B \to C$ leképezés, amelyre $g = fh$, ha $\ker(f) \subseteq \ker(g)$,
(2) h egyértelműen meghatározott.

1.22. Feladat. (2 pt.)
Legyen ϱ reflexív, tranzitív reláció az A halmazon. Bizonyítsuk, hogy $\alpha = \varrho \cap \varrho^{-1}$ ekvivalencia A-n. Legyen β az a reláció A/α-n, melyre $\overline{a}\ \beta\ \overline{b}$ pontosan akkor, ha $a\ \varrho\ b$. Bizonyítsuk, hogy β részbenrendezés A/α-n.

1.23. Feladat. (2 pt.)
Tekintsük a $\varrho = \{\, ((a,b),(c,d)) : ad = bc \,\}$ ekvivalenciát a $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ halmazon. Adjuk meg a ϱ-hoz tartozó osztályozást (azaz a $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\varrho$ faktorhalmazt) úgy, hogy minden osztályát pontosan egyszer soroljuk fel.

1.24. Feladat. (3 pt. előadta Miklós)
Egy részbenrendezett halmaz *jólrendezett*, ha nincs benne végtelen antilánc és nincs benne végtelen leszálló lánc. Mutassuk meg, hogy ha az A és B részbenrendezett halmazok jólrendezettek, akkor $A \times B$ is az.

2. Oszthatóság az egész számok körében

2.1. Feladat. (2 pt. közösen megbeszéltük)
Oldjuk meg a $623x + 217y = 35$ és a $623x + 217y - 2z = 8$ diofantoszi egyenleteket.

2.2. Feladat. (2 pt. előadta Gábor)
Tekintsük az $F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}, n > 0$, rekurzióval megadott ú.n. Fibonacci-sorozatot. Mutassuk meg, hogy a Fibonacci sorozat n-edik tagja

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Továbbá $F_n \geq (\frac{1+\sqrt{5}}{2})^{n-2}$, ha $n \geq 2$.

2.3. Feladat. (3 pt. közösen megbeszéltük)

(1) Legyen $\alpha = \frac{1+\sqrt{5}}{2}$. Bizonyítsuk, hogy az a, b pozitív egészeken végrehajtott euklideszi algoritmus legfeljebb $\frac{\log_2 b}{\log_2 \alpha}$ lépésben véget ér.
(2) Igazoljuk, ha az euklideszi algoritmust a legkisebb abszolút értékű maradékokat véve hajtjuk végre, akkor az legfeljebb $\log_2 b$ lépésben véget ér.

2.4. Feladat. (2 pt. előadta Ádám)
Bizonyítsuk, hogy tetszőleges $n >$ 1-re az $\{1, \ldots, n\}$ halmazból $[\frac{n}{2}] + 1$ elemet akárhogyan kiválasztva biztosan van két olyan kiválasztott elem, hogy az egyik relatív prím a másikhoz, és $[\frac{n+1}{2}] + 1$ elemet kiválasztva van két olyan kiválasztott elem is, hogy az egyik osztója a másiknak.

2.5. Feladat. (1 pt. közösen megbeszéltük)
Legyen s_n az $\{1, 2, \ldots, n\}$ halmazba eső prímek száma plusz 1. Mutassuk meg, hogy $\{1, 2, \ldots, n\}$ halmaznak legfeljebb s_n darab eleme választható ki úgy, hogy bámely kettő relatív prím.

2.6. Feladat. (1 pt. előadta Gábor)
Mely y egészre lesz $4 + y^4$ prímszám?

2.7. Feladat. (1 pt.)
Határozzuk meg az összes p prímet, melyre $29p + 1$ négyzetszám. Hasonlóan, mikor lesz $24p + 1$ négyzetszám?

2.8. Feladat. (2 pt.)

(1) Bizonyítandó, hogy $n!$ prímtényezős felbontásában a p prím

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]$$

kitevőn szerepel.
(2) Határozzuk meg 10! prímtényezős felbontását.

(3) Bizonyítsuk, hogy

$$\sum_{p\le n}\frac{\ln p}{p}\ge\frac{\sum_{i=1}^{n}\ln i}{n}-\sum_{i=1}^{n}\frac{2}{i^{\frac{3}{2}}}.$$

2.9. Feladat. (1 pt. előadta Lívia)
Találjuk meg az összes olyan a, b pozitív egészet, melyekre $a+b=57$, és a és b legkisebb közös többszöröse 680.

2.10. Feladat. (1 pt. előadta Ádám)
Mutassuk meg, hogy

$$\sum_{i=1}^{n}\frac{1}{i}$$

nem egész, ha $n>1$.

2.11. Feladat. (1 pt.)
Bizonyítsuk, hogy minden m nemnegatív egészhez létezik egy $ax+by=c$, $a,b,c\in\mathbb{Z}$, alakú egyenlet, melynek pontosan m megoldása van a pozitív egészek körében.

2.12. Feladat. (1 pt.)
Keressük meg azokat az a, b pozitív egész számokat, melyekre $\text{lnko}(a,b)=6$ és $\text{lkkt}(a,b)=1260$.

2.13. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsuk, ha a k és n pozitív egészek relatív prímek és $k<n$, akkor n osztója $\binom{n}{k}$-nak.

2.14. Feladat. (2 pt. közösen megbeszéltük)
Legyenek k és n pozitív egészek, $k<2^n$. Bizonyítsuk, hogy $\binom{2^n}{k}$ páros.

2.15. Feladat. (2 pt. előadta Ádám)
Legyenek a, m, n pozitív egészek. Bizonyítsuk, hogy

$$\text{lnko}(a^m-1,a^n-1)=a^{\text{lnko}(m,n)}-1.$$

2.16. Feladat. (2 pt. előadta Fanni, Ádám és Gábor)
Határozzuk meg azon p prímeket, melyekre $\frac{2^{p-1}-1}{p}$ négyzetszám.

2.17. Feladat. (2 pt. közösen megbeszéltük)
A 10^n szám osztói között legfeljebb hány olyan szám van, melyek között egyik sem osztója a másiknak?

2.18. Feladat. (2 pt.)
Legyen $n=p_1^{k_1}\dots p_m^{k_m}$, ahol $p_1,\dots,p_m$ páronként különböző prímek, és $k_1,\dots,k_m$ pozitív egészek.

(1) Határozzuk meg n osztóinak számát.
(2) Mely n számokra páratlan az osztók száma?
(3) Határozzuk meg n osztóinak szorzatát.

2.19. Feladat. (2 pt. előadta Fanni)
Smaragdia köztársaság elnöke a nemzeti ünnep alkalmából amnesztiában részesíti a köztársaság top secret börtönének lakóit. A 256 bebörtönzött mindegyike magánzárkában tölti büntetését. Mindegyik zárka az ajtaján elhelyezett egyetlen gomb megnyomásával nyitódik, illetve záródik. Kezdetben minden zárka ajtaja zárva van. Az elnök futárt küld azzal a paranccsal, hogy mind a 256 zárkaajtó gombját nyomja meg. A dolgot jobban meggondolva újabb futárt küld azzal, hogy minden második ajtó gombját nyomja meg. Majd küld egy következő futárt azzal, hogy nyomja meg minden harmadik ajtó gombját, és így tovább. Utoljára a 256-dik futár indul el azzal a paranccsal, hogy a 256-dik ajtó gombját nyomja meg. Végül pontosan azok a rabok kapnak amnesztiát, akik olyan zárkában laknak, melynek ajtaja az összes parancs végrehajtása után nyitva áll. Hány rab szabadul a nemzeti ünnep alkalmából?

2.20. Feladat. (2 pt.)
Legyen n pozitív egész, $a_0,a_1,\dots,a_n$ egészek, és $a_n\ge 1$. Bizonyítsuk, hogy végtelen sok összetett szám van az $a_nx^n+a_{n-1}x^{n-1}+\dots+a_0$, $x=1,2,\dots$, sorozatban.

2.21. Feladat. (2 pt.)
Keressünk végtelen sok olyan $a\neq b$ számpárt, hogy a és b-nek, illetve $a+1$ és $b+1$-nek is ugyan azok a prímosztói (például $a=2$ és $b=8$).

3. Kongruenciák

3.1. Feladat. (2 pt. előadta Gábor)
Bizonyítsa be, hogy ha n nem osztható se 2-vel se 5-tel, akkor van olyan többszöröse, ami csak 9-es számjegyekből áll.

3.2. Feladat. (1 pt.)
Oldjuk meg az alábbi kongruenciákat:

(1) $19x \equiv 73 \pmod{2005}$,
(2) $143x \equiv 221 \pmod{91}$.

3.3. Feladat. (2 pt. előadta Gergő)
Legyen F_n a Fibonacci-sorozat n-edik tagja, és n tetszőleges pozitív egész.

(1) Mutassuk meg, hogy $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.
(2) Oldjuk meg az $F_{n-1}x \equiv 1 \pmod{F_n}$ kongruenciát.

3.4. Feladat. (2 pt.)
Igazoljuk, hogy tetszőleges p prímszámra

(1) $p \mid a^{p^p} - a$,
(2) $p^2 \mid (2p-1)! - p$,
(3) $p^p \mid (p^2-1)! - p^{p-1}$.

3.5. Feladat. (2 pt.)
Igazoljuk, hogy tetszőleges p páratlan prímszámra és n pozitív egészre

$$\prod_{1 \le k \le p^n,\ p \nmid k} k \equiv -1 \pmod{p^n}.$$

3.6. Feladat. (2 pt. előadta Ádám)
Bizonyítsuk be, hogy tetszőleges a egész számra és n pozitív egészre $n \mid a^n - a^{n-\varphi(n)}$.

3.7. Feladat. (2 pt. előadta Fanni és Gábor)
Mutassuk meg, hogy tetszőleges a, b egészek és p prím esetén, ha $a^p \equiv b^p \pmod{p}$, akkor $a^p \equiv b^p \pmod{p^2}$.

3.8. Feladat. (2 pt.)
Igazoljuk, hogy az $(n-1)! = n^k - 1$ diofantoszi egyenletnek az $(n,k) = (2,1),\ (3,1)$ és $(5,2)$ párokon kívül nincs más megoldása a pozitív egészek körében.

3.9. Feladat. (2 pt.)
Határozzuk meg azokat az pozitív egész n-eket, amelyekre $\varphi(n) \mid n$.

3.10. Feladat. (2 pt.)
Igazoljuk, hogy a $\varphi(n) = a$ egyenlet végtelen sok páros a pozitív egészre megoldhatatlan.

3.11. Feladat. (2 pt. közösen megoldottuk)
Igazoljuk, hogy a $\varphi(n) = a$ egyenletnek rögzített a mellett csak véges sok megoldása van.

3.12. Feladat. (2 pt.)
Bizonyítsuk, hogy $2^{2^n} + 1$ prímosztói $2^{n+1}x + 1$ alakúak, ahol x pozitív egész.

3.13. Feladat. (2 pt.)
Bizonyítsuk, hogy bármely a pozitív egészre $n \mid \varphi(a^n - 1)$.

3.14. Feladat. (2 pt.)
Bizonyítsuk, hogy tetszőleges olyan páratlan p prím, amelyre az összes négyzetes nemmaradék primitív gyök, $2^{2^n} + 1$ alakú.

3.15. Feladat. (2 pt.)
Oldjuk meg az alábbi kongruenciarendszert:

$$\begin{aligned} 15x &\equiv 27 \pmod{7}, \\ 18x &\equiv 14 \pmod{5}, \\ 6x &\equiv 12 \pmod{8}. \end{aligned}$$

4. Hatványozás modulo m

4.1. Feladat. (2 pt. előadta Gergő, Lívia és Ádám)
Mennyit ad 73-mal osztva x maradékul, ha $x^{99} \equiv 22 \pmod{73}$ és $x^{100} \equiv 69 \pmod{73}$?

4.2. Feladat. (2 pt. előadta Fanni és Lívia)
Határozzuk meg, hogy milyen maradékot ad

(1) 13-mal osztva a 35^{600},
(2) 17-tel osztva a 19^{2007}?

4.3. Feladat. (2 pt. részben megbeszéltük)
Határozzuk meg a következő számok utolsó két számjegyét: $39^{39^{3900}}$, $39^{39^{39}}$.

4.4. Feladat. (2 pt. előadta Gergő)
Határozzuk meg a $17^{18^{19}}$ számnak az utolsó két számjegyét.

4.5. Feladat. (2 pt.)
Az x négyjegyű szám a bankkártyám PIN kódja. Elárulom, hogy $x^{275} \equiv 2 \pmod{4187}$. Hogyan lehetne ebből x-et kitalálni? (Elárulom, hogy $4187 = 53 \cdot 79$.)

4.6. Feladat. (2 pt. előadta Lívia)
Döntsük el, hogy megoldhatók-e az alábbi kongruenciák.

(1) $x^2 \equiv 5 \pmod{73}$,
(2) $x^2 \equiv 226 \pmod{563}$.

4.7. Feladat. (2 pt. közösen megbeszéltük)
Legyen p egy $2^n + 1$ alakú prím, ahol $n \geq 2$. Mutassuk meg, hogy

(1) 3 négyzetes nemmaradék modulo p,
(2) 3 primitív gyök modulo p.

4.8. Feladat. (2 pt.)
Oldjuk meg az alábbi kongruenciákat (indextáblázat használatával)

(1) $x^2 \equiv 5 \pmod{73}$,
(2) $x^{30} \equiv 14 \pmod{67}$,
(3) $44x^{21} \equiv 53 \pmod{73}$.

4.9. Feladat. (2 pt.)
Legyen p prím és $S = \sum_{i=1}^{p-1} i^n$. Mutassuk meg, ha $p - 1 \mid n$, akkor $S \equiv -1 \pmod{p}$, és $S \equiv 0 \pmod{p}$ különben.

4.10. Feladat. (2 pt. előadta Fanni)
Oldjuk meg az alábbi lineáris kongruenciarendszert

$$2x \equiv 13 \pmod{25}$$
$$3x \equiv 7 \pmod{4}$$

4.11. Feladat. (2 pt.)
Számítsuk ki a $\left(\frac{103}{151}\right)$ Legendre-szimbólum értékét a négyzetes reciprocitási tétel felhasználásával.

4.12. Feladat. (2 pt.)
Legyenek a és m relatív prím természetes számok. Az $\frac{1}{m}$ törtet a alapú számrendszerben felírva egy tiszta szakaszos végtelen a-ados törtet kapunk. Igazoljuk, hogy a szakasz hossza nem más, mint a rendje modulo m. (Például $a = 10$ és $m = 7$ esetén $\frac{1}{7}$ tízes számrendszerbeli felírása $0{,}\dot{1}42857\dot{}$, vagyis a szakasz hossza 6, ami éppen 10 rendje modulo 7.)

4.13. Feladat. (2 pt.)
Mennyit ad 53-mal osztva maradékul $80^{(111^{50})}$?

4.14. Feladat. (2 pt. előadta Gergő)
Igazoljuk, hogy bármely a egész számra $a^{561} \equiv a \pmod{561}$.

4.15. Feladat. (2 pt. előadta Fanni)
Igazoljuk a következő kongruenciákat tetszőleges p páratlan prímszám esetén:

(1) $2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2(p-1) \equiv -1 \pmod{p}$,
(2) $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$,
(3) $2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

4.16. Feladat. (5 pt.)
Bizonyítsuk be, hogy minden kettőnél nagyobb páros szám előáll két prímszám összegeként.

5. Számelméleti függvények

Tetszőleges n pozitív egészre legyen $\tau(n)$ az n osztóinak száma, $\sigma(n)$ az n osztóinak összege, $\nu(n)$ az n prímosztóinak a száma, $\kappa(n)$ az n prímtényezős felbontásában szereplő kitevők összege, valamint μ a Möbius-féle és φ az Euler-féle függvény.

5.1. Feladat. (2 pt.)
Igazoljuk, hogy bármely $\varepsilon > 0$-hoz létezik olyan $n_0 = n_0(\varepsilon)$, amelyre $n > n_0$ esetén $\varphi(n) > n^{1-\varepsilon}$.

5.2. Feladat. (2 pt.)
Igazoljuk, hogy tetszőleges n természetes számra

$$\frac{n}{\nu(n)+1} \leq \varphi(n) \leq n \leq \sigma(n) \leq n(\nu(n)+1).$$

5.3. Feladat. (2 pt.)
Igazoljuk, hogy $2^{\nu(n)} \leq \tau(n) \leq 2^{\kappa(n)} \leq n$.

5.4. Feladat. (2 pt.)
Legyen $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $\text{lnko}(a, n) = 1$, valamint M teljes maradékrendszer, illetve R redukált maradékrendszer modulo n. Igazoljuk, hogy

$$\sum_{x \in M} \left\{ \frac{ax+b}{n} \right\} = \frac{1}{2}(n-1), \quad \sum_{x \in R} \left\{ \frac{ax}{n} \right\} = \frac{1}{2}\varphi(n).$$

5.5. Feladat. (2 pt.)
Milyen maradékot ad n-nel osztva egy modulo n redukált maradékrendszer elemeinek szorzata?

5.6. Feladat. (2 pt.)
Bizonyítsuk be a következőket:

(1) $\sum_{j=1}^{n} \mu(j) \left[\frac{n}{j}\right] = 1$.
(2) $\sum_{d|n} |\mu(d)| = 2^{\nu(n)}$.
(3) Minden k pozitív egészhez van olyan n pozitív egész, amelyre $\mu(n+1) = \cdots = \mu(n+k) = 0$.

5.7. Feladat. (2 pt. közösen megbeszéltük)
Keressünk példát olyan számelméleti függvényre, amely teljesen multiplikatív, de összegzési függvénye nem az.

5.8. Feladat. (2 pt. közösen megbeszéltük)
Legyen f tetszőleges gyengén multiplikatív számelméleti függvény. Mutassuk meg, hogy

(1) $\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$,
(2) $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$,
(3) $\sum_{d|n} \mu(d)\tau(d) = (-1)^{\nu(n)}$.

5.9. Feladat. (2 pt. előadta Fanni)
Határozzuk meg a $\mu, \varphi, id_{\mathbb{N}}$ függvények összegzési függvényét.

5.10. Feladat. (2 pt. közösen megbeszéltük)
Határozzuk meg a μ, τ, σ függvények megfordítási függvényét.

5.11. Feladat. (2 pt. előadta Fanni)
Az f gyengén multiplikatív számelméleti függvényről tudjuk, hogy $f(3) = 2$, $f(5) = 7$, és $f(45) = 21$.

(1) Határozzuk meg $F(45)$ értékét, ahol F jelöli az f összegzési függvényét.
(2) Határozzuk meg $t(45)$ értékét, ahol t jelöli az f megfordítási függvényét.

5.12. Feladat. (2 pt.)
Oldja meg az alábbi egyenleteket

(1) $\varphi(2n) = n$,
(2) $\varphi(n) = n - 2$,
(3) $\varphi(n^2) = n\varphi(n)$.

5.13. Feladat. (2 pt. előadta Fanni)
Határozza meg a $\varrho(n) = \frac{1}{n}$ számelméleti függvény összegzési függvényét, és írja fel rá a Möbius-féle inverziós formulát.

5.14. Feladat. (2 pt.)
Mutassuk meg, hogy minden páros tökéletes szám utolsó két számjegye 06, 28, 36, 56, 76 vagy 96.

5.15. Feladat. (2 pt.)
Mutassuk meg, hogy minden n páratlan tökéletes számra

(1) $n = s^2p$ alakban írható fel, ahol p alkalmas prímszám és $p \equiv 1 \pmod 4$.
(2) $n \equiv 1 \pmod{12}$ vagy $n \equiv 9 \pmod{36}$.

5.16. Feladat. (2 pt.)
Azt mondjuk, hogy az n természetes szám *hiányos*, ha $\sigma(n) < 2n$, és *bővelkedő*, ha $\sigma(n) > 2n$. Mutassuk meg, hogy

(1) minden prímhatvány hiányos,
(2) minden $n = p^\alpha q^\beta$ alakú szám hiányos, ahol p és q különböző páratlan prímszámok és $\alpha, \beta \in \mathbb{N}$,
(3) bővelkedő szám többszöröse is bővelkedő.

5.17. Feladat. (2 pt. közösen megbeszéltük)
Mutassuk meg, hogy az alábbi egyenlőtlenségeket:

(1) $\frac{n^2}{2} < \sigma(n)\varphi(n) \leq n^2$,
(2) $2n \leq \sigma(n) + \varphi(n)$.

5.18. Feladat. (2 pt.)
Mutassuk meg, hogy tetszőleges n természetes számra

$$\tau(n^2) = |\{\, (a,b) \in \mathbb{N}^2 : \mathrm{lkkt}(a,b) = n \,\}|.$$

5.19. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsuk be, hogy minden n természetes számra $\sum_{d|n} \tau(d)\frac{n}{d} = \sum_{d|n} \sigma(d)$.

6. Komplex számok

6.1. Feladat. (2 pt.)
Ábrázolja a következő komplex számokat a Gauss-féle számsíkon, és adja meg a trigonometrikus, illetve kanonikus alakjukat.

(1) $\frac{7}{2} - \frac{7\sqrt{3}}{2}i$,
(2) $-2 - 2i$,
(3) $\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}$,
(4) $2(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3})$.

6.2. Feladat. (2 pt.)
Milyen mértani alakzatot határoznak meg a Gauss-számsíkon azon komplex számok,

(1) melyek abszolút értéke 2,
(2) melyek argumentuma $\pi/6$?

6.3. Feladat. (2 pt. közösen megbeszéltük)
Határozza meg két komplex szám egymáshoz viszonyított helyzetét a Gauss-számsíkon, ha

(1) szorzatuk valós,
(2) összegük valós,

(3) hányadosuk valós,
(4) különbségük valós.

6.4. Feladat. (2 pt. közösen megbeszéltük)
Adja meg a következő komplex számokat a kanonikus és trigonometrikus alakban: $(1+i)^3$, $(1+\sqrt{3}i)^{100}$, $i/(1-i)$, $(3+i)/(1-i)$, $(3+4i)^{-1}$, $1+i+i^2+i^3+\cdots+i^{77}$, $(\frac{1+\sqrt{3}i}{1-i})^{20}$.

6.5. Feladat. (2 pt.)
Végezze el az alábbi gyökvonásokat:

(1) $\sqrt{3-4i}$,
(2) $\sqrt[6]{\frac{1-i}{\sqrt{3}+i}}$.

6.6. Feladat. (2 pt. közösen megbeszéltük)
Fejezze ki $\sin 4\varphi$ és $\cos 5\varphi$ értékét $\sin\varphi$ és $\cos\varphi$ segítségével.

6.7. Feladat. (2 pt.)
Bizonyítsa, hogy

$$\sum_{j=1}^{n} \sin(jx) = \frac{\sin\frac{(n+1)x}{2}\cdot\sin\frac{nx}{2}}{\sin\frac{x}{2}}.$$

6.8. Feladat. (2 pt.)
Keresse meg az alábbi egyenletek összes megoldását:

(1) $z^2 = \bar{z}$
(2) $z^3 = -8$,
(3) $z^6 = 64$,
(4) $z^2 + 2iz = -i$.

6.9. Feladat. (2 pt. közösen megbeszéltük)
Tetszőleges $n \geq 1$ esetére számolja ki az n-edik egységgyökök összegét és szorzatát.

6.10. Feladat. (2 pt.)
Jelölje E_n az n-edik egységgyökök halmazát. Bizonyítsa be, hogy tetszőleges $n, m \geq 1$ egészekre $E_n \cap E_m = E_{\text{lnko}(n,m)}$.

6.11. Feladat. (2 pt.)
Jelölje P_n az n-edik primitív egységgyökök halmazát. Bizonyítsa be, hogy tetszőleges $n, m \geq 1$ egészekre ha $\varepsilon \in P_n$, akkor $\varepsilon^m \in P_{\frac{n}{\text{lnko}(n,m)}}$.

6.12. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsa be, hogy tetszőleges $n \geq 1$ egészre $E_n = \bigcup_{d|n} P_d$, és azt, hogy az únió diszjunkt.

6.13. Feladat. (2 pt. előadta Ádám és Miklós)
Tetszőleges $n \geq 1$ esetére számolja ki az n-edik primitív egységgyökök összegét és szorzatát.

6.14. Feladat. (2 pt. előadta Ádám)
Mely ε egységgyökre lesz $1+\varepsilon$ is egységgyök?

6.15. Feladat. (2 pt. közösen beszéltünk róla)
Hogyan lehetne tetszőleges z, u komplesz számokra a z^u hatványt értelmezni úgy, hogy a hatványozás szokásos azonosságai teljesüljenek? Számolja ki az i^i hatvány értékét.

7. Algebrai struktúrák

7.1. Feladat. (2 pt.)
Legyen G tetszőleges csoport és $a, b \in G$. Mutassuk meg, hogy $o(a^{-1}ba) = o(b)$ és $o(ab) = o(ba)$.

7.2. Feladat. (2 pt. előadta Ádám)
Legyen G tetszőleges kommutatív csoport, a és b véges rendű elemek G-ben. Bizonyítsuk, hogy ekkor $o(ab) \mid \text{lkkt}(o(a), o(b))$, továbbá, ha $\text{lnko}(o(a), o(b)) = 1$, akkor $o(ab) = o(a)o(b)$ is teljesül.

7.3. Feladat. (2 pt.)
Mutassuk meg, hogy G kommutativitása nem hagyható el az előző állításban.

7.4. Feladat. (2 pt.)
Mutassuk meg, hogy egy véges G csoport pontosan akkor ciklikus, ha bármely $a, b \in G$-re $o(a) = o(b)$ esetén $[a] = [b]$.

7.5. Feladat. (2 pt. közösen megbeszéltük)
Tetszőleges A halmazra definiáljuk

$$\mathrm{Eq}_A = \{\, \varrho \subseteq A \times A : \varrho \text{ ekivivalenciareláció} \,\}.$$

Döntse el, hogy az $(\mathrm{Eq}_A; \cap)$ félcsoport egységelemes-e, és hogy minden elemnek létezik-e inverze?

7.6. Feladat. (2 pt.)
Adjon meg az $\{a, b, c\}$ halmazon olyan kétváltozós műveletet, mely

(1) asszociatív, van egységeleme, de nincs minden elemnek inverze,
(2) van egységeleme, minden elemnek van inverze, de nem asszociatív.

7.7. Feladat. (2 pt.)
Csoportot alkotnak-e az alábbi halmazok a szokásos összeadásra, illetve szorzásra nézve:

(1) $\{\, 2n : n \in \mathbb{Z} \,\}$,
(2) $\mathbb{R} \setminus \mathbb{Q}$,
(3) $\mathbb{Z}_{15}$,
(4) $\{\, z \in \mathbb{C} : |z| = 1 \,\}$.

7.8. Feladat. (2 pt.)
Csoport művelettáblázata-e az alábbi két művelettáblázat:

$\circ$	e	f	g	h
e	g	h	e	f
f	h	g	f	e
g	e	f	g	h
h	f	e	h	g

$*$	e	f	g	h
e	f	h	g	e
f	h	g	h	f
g	g	h	f	g
h	e	f	g	h

7.9. Feladat. (2 pt.)
Csoportot alkot-e az $\mathbb{R} \setminus \{0\}$ halmaz a következő műveletettel:

$$x \star y = \begin{cases} xy & \text{ha } x > 0, \\ x/y & \text{ha } x < 0. \end{cases}$$

7.10. Feladat. (2 pt. közösen megbeszéltük)
Legyen $(S; \cdot)$ olyan félcsoport, amelyben létezik bal oldali egységelem, azaz

$$(\exists e \in S)(\forall x \in S)(e \cdot x = x),$$

és minden elemnek van bal oldali inverze, azaz

$$(\forall x \in S)(\exists y \in S)(y \cdot x = e).$$

Bizonyítsa be, hogy $(S; \cdot)$ csoport.

7.11. Feladat. (2 pt. közösen megbeszéltük)
Jelölje $\mathcal{F} = A^A$ az A véges halmaz összes transzformációinak halmazát a leképezésszorzás művelettel. Állapítsa meg, hogy $(\mathcal{F}; \circ)$

(1) asszociatív-e,
(2) kommutatív-e,
(3) van-e egységeleme,
(4) létezik-e minden elemnek balinverze,
(5) létezik-e minden elemnek jobbinverze,
(6) hány bal oldali illetve jobb oldali zéruseleme van.

7.12. Feladat. (2 pt.)
Az alábbi halmazok közül melyek alkotnak gyűrűt, integritástartományt, illetve testet a szokásos összeadás és szorzás műveletekkel?

(1) $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,
(2) $\{\, k \in \mathbb{Z} : 2 \mid k \,\}$,
(3) $\{\, a + b\sqrt{5} \in \mathbb{R} : a, b \in \mathbb{Z} \,\}$,
(4) $\mathbb{Z}_5$, $\mathbb{Z}_{15}$, $\mathbb{Z}_4$,
(5) $\{\, a + bi \in \mathbb{C} : a, b \in \mathbb{Z} \,\}$,
(6) $\{\, a/2^n \in \mathbb{R} : a \in \mathbb{Z}, n \in \mathbb{N} \,\}$.

7.13. Feladat. (2 pt. közösen megbeszéltük)
Adjon meg olyan gyűrűt, amely

(1) egységelemes, kommutatív, de nem zérusosztómentes,
(2) egységelemes, zérusosztómentes, de nem kommutatív,
(3) kommutatív, zérusosztómentes, de nem egységelemes.

7.14. Feladat. (2 pt.)
Bizonyítsa, hogy minden véges, legalább kételemű, kommutatív zérusosztómentes gyűrű test.

7.15. Feladat. (2 pt. közösen megbeszéltük)
Minden $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_3$ leképezéshez keressen olyan $f \in \mathbb{Z}_3[x]$ polinomot, melynek polinomfüggvénye φ.

7.16. Feladat. (2 pt.)
Legyen T egy tetszőleges véges test. Határozzuk meg T elemeinek összegét $|T|$ függvényében.

7.17. Feladat. (2 pt. előadta Gábor)
Legyen G tetszőleges csoport és $g \in G$ rögzített elem. Mutassuk meg, hogy a $\varphi : \mathbb{Z} \to G$, $k\varphi = g^k$ leképezés homomorfizmus (azaz tetszőleges $k, l \in \mathbb{Z}$ egészekre $(k+l)\varphi = (k\varphi)(l\varphi)$).

7.18. Feladat. (2 pt. előadta Gábor)
Mutassuk meg, hogy $\Gamma = \{\, \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2} : a, b \in \mathbb{R} \,\}$ a szokásos mátrix összeadás és szorzás műveletekkel testet alkot.

7.19. Feladat. (2 pt.)
Igaz-e, hogy ha az $(A; \cdot)$ grouppoid egységelemes, művelettáblázata Latin-négyzet, és teljesül benne az $(xy)^{-1} = y^{-1}x^{-1}$ azonosság, akkor $(A; \cdot)$ csoport?

8. Test feletti polinomgyűrűk

8.1. Feladat. (2 pt.)
Végezze el az alábbi maradékos osztást a megadott polinomgyűrűben:

(1) $\mathbb{R}[x]$-ben $(x^4 - 10x^2 + 1) : (x^2 - 2\sqrt{2}x - 1)$,
(2) $\mathbb{C}[x]$-ben $(x^3 - 2) : (x^2 + ix - 1)$,
(3) $\mathbb{Z}_7[x]$-ben $(\overline{3}x^5 - x^3 - \overline{2}x^2 + x - \overline{1}) : (x^3 - \overline{2}x^2 + x - \overline{1})$.

8.2. Feladat. (2 pt. előadta Lívia)
Határozza meg az alábbi polinomok legnagyobb közös osztóját és legkisebb közös többszörösét a megadott polinomgyűrűben:

(1) $x^5 - 5x^3 + 5x + 1, 3x^3 - 2x + 1 \in \mathbb{Q}[x]$,
(2) $x^4 + \overline{1}, x^3 - x \in \mathbb{Z}_3[x]$,

8.3. Feladat. (2 pt.)
Adja meg az R polinomgyűrűben a megadott polinomegyenlet összes (u, v) megoldását, valamint azt a megoldást, ahol u a lehető legkisebb fokú.

(1) $R = \mathbb{Q}[x]$: $(x^4 + 2x^3 + x + 1)u + (x^4 + x^3 - 2x^2 + 2x - 1)v = x^3 - 2x$;
(2) $R = \mathbb{C}[x]$: $(x - i)u + (x^2 + 1)v = x^3 + i$;
(3) $R = \mathbb{Z}_2[x]$: $(x^4 + x^2 + \overline{1})u + (x^5 + x^4 + x^2 + x)v = x^4 + x^3 + x^2$;

8.4. Feladat. (2 pt. előadta Fanni)
Legyenek adottak az alábbi polinomok:

$$\begin{aligned} f &= x^6+2x^5-2x^4+2x^3+12x^2-2x-4 \in \mathbb{R}[x], \\ g &= x^3+3x+2i \in \mathbb{C}[x], \\ u &= x^3+x^2+x+\overline{1} \in \mathbb{Z}_2[x], \\ v &= x^4-x^3-x^2+x \in \mathbb{Z}_3[x], \\ w &= x^5+x^4+x^3+x^2+x+\overline{1} \in \mathbb{Z}_5[x], \\ z &= x^3+\overline{2}x^2-\overline{3} \in \mathbb{Z}_7[x]. \end{aligned}$$

Horner-elrendezés alkalmazásával

(1) számolja ki az $f(-1), g(2i), v(-\overline{1}), w(\overline{2}), z(-\overline{3})$ helyettesítési értékeket;
(2) döntse el, hogy gyöke-e, és ha igen, akkor hányszoros gyöke f-nek -2, g-nek $-i$, u-nak $\overline{1}$, v-nek $\overline{1}$, w-nek $-\overline{2}$ és z-nek $\overline{3}$;
(3) végezze el az $f : (x+1)$, $g : (x-1)$, $u : (x+\overline{1})$, $v : (x-\overline{1})$, $w : (x-\overline{2})$ és a $z : (x+\overline{2})$ maradékos osztást.

8.5. Feladat. (2 pt.)
Adja meg elempárok halmazaként az előző feladatbeli u, v, w, z, valamint a következő polinomokhoz tartozó polinomfüggvényeket:

$$\begin{aligned} f &= x^5+x^3+\overline{1} \in \mathbb{Z}_2[x], \\ g &= -x^4-x^3+x+\overline{1} \in \mathbb{Z}_3[x], \\ h &= x^6+x^4+x^3+\overline{2}x+\overline{1} \in \mathbb{Z}_5[x], \\ p &= x^7+\overline{2}x^4-\overline{3}x+\overline{2} \in \mathbb{Z}_7[x]. \end{aligned}$$

Döntse el, hogy vannak-e közöttük azonosak.

8.6. Feladat. (2 pt. közösen megbeszéltük)
Határozza meg azt a legkisebb fokú $\mathbb{Z}_7$-beli polinomot, amely $\overline{2}x$-et ad maradékul $(x-\overline{1})^2$-nel osztva, és $\overline{3}x$-et ad maradékul $(x-\overline{2})^3$-nel osztva.

8.7. Feladat. (2 pt.)
Legyen K tetszőleges test, $f, g, u, v \in K[x]$ tetszőleges polinomok, és jelölje d az f és g polinomok legnagyobb közös osztóját $K[x]$-ben. Határozza meg az u és v polinomok legnagyobb közös osztóját $K[x]$-ben, ha tudjuk, hogy $fu+gv=d$.

8.8. Feladat. (2 pt.)
Legyen K, L két test, melyre $K \subseteq L$, és legyen $f, g \in K[x]$. Ekkor persze $f, g \in L[x]$ is fennáll. Igazolja, hogy

(1) $f \mid g$ pontosan akkor teljes $K[x]$-ben, ha $L[x]$-ben teljesül,
(2) az f és g polinomnak ugyanaz a legnagyobb közös osztója, illetve legkisebb közös többszöröse $K[x]$-ben, mint $L[x]$-ben,
(3) bármely $h \in K[x]$ és $u, v \in L[x]$ polinomok esetén, ha $fu+gv=h$, akkor $u, v \in K[x]$, és így az $fu+gv=h$ egyenletnek ugyanazok a polinompárok a megoldásai $K[x]$-ben, mint $L[x]$-ben.

8.9. Feladat. (2 pt.)
Mutassa meg, hogy $x^d-1 \mid x^n-1$ teljesül $\mathbb{Q}[x]$-ben, ha $d, n \in \mathbb{N}$-re $d \mid n$.

8.10. Feladat. (2 pt.)
Mely a, b valós, illetve $\mathbb{Z}_p$-beli (p prímszám) együtthatók esetén teljesül $(x-1)^2 \mid ax^{n+1}+bx^n+1$?

8.11. Feladat. (2 pt.)
Legyen p prímszám és f, g két polinom $\mathbb{Z}_p$ felett. Igazolja, hogy az $f(x)$ és $g(x)$ polinomfüggvények pontosan akkor azonosak, ha

$$x(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p-1}) \mid f-g.$$

8.12. Feladat. (2 pt. előadta Gábor)
Mutassa meg, hogy tetszőleges p prímszámra $\mathbb{Z}_p[x]$-ben fennáll az

$$x^p-x = x(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p-1})$$

egyenlőség.

8.13. Feladat. (2 pt. közösen megbeszéltük)
Adja meg az alábbi valós együtthatós polinomok irreducibilis felbontását a komplex, illetve a valós számtest fölött:

(1) $x^3 - 1$,
(2) $x^4 - 1$,
(3) $x^3 + 1$,
(4) $x^4 + 1$,
(5) $x^4 + x^2 + 1$,
(6) $x^6 - x^3 + 1$.

8.14. Feladat. (2 pt.)
Adjon meg

(1) harmadfokú irreducibilis polinomot $\mathbb{Z}_5$ fölött;
(2) negyedfokú irreducibilis polinomot $\mathbb{Z}_3$ fölött;
(3) ötödfokú irreducibilis polinomot $\mathbb{Z}_3$ fölött;
(4) negyedfokú irreducibilis polinomot $\mathbb{Z}_2$ fölött;
(5) ötödfokú irreducibilis polinomot $\mathbb{Z}_2$ fölött;
(6) hetedfokú irreducibilis polinomot $\mathbb{Z}_2$ fölött.

8.15. Feladat. (2 pt.)
Döntse el, hogy irreducibilis-e az alábbi polinom a megadott polinomgyűrűben:

(1) $x^3 + x^2 + \overline{1} \in \mathbb{Z}_2[x]$,
(2) $x^4 + x^2 + \overline{1} \in \mathbb{Z}_2[x]$,
(3) $x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$,
(4) $x^4 + x^3 + x^2 + \overline{1} \in \mathbb{Z}_3[x]$,
(5) $x^5 - \overline{2}x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$.

8.16. Feladat. (2 pt.)
Adja meg az alábbi valós együtthatós polinomok irreducibilis felbontását a komplex, illetve a valós számtest fölött:

(1) $x^n + 1$ $(n \in \mathbb{N})$,
(2) $x^{2n} - x^n + 1$ $(n \in \mathbb{N})$.

8.17. Feladat. (2 pt.)
Mutassa meg, hogy az $\mathbb{R}[x]$ polinomgyűrűben pontosan akkor teljesül $x^2 + x + 1 \mid x^{2k} + x^k + 1$ oszthatóság, ha $3 \nmid k$.

9. Polinomok II.

9.1. Feladat. (2 pt.)
Maradékos osztás segítségével döntse el, hogy osztható-e az f polinom a g polinommal.

(1) $f = x^4 - 5x^3 + 2x^2 - 3x - 1$, $g = x^2 + 1 \in \mathbb{Q}[x]$,
(2) $f = x^{17} - x^{16} + x^{15} - x^{14} + x^7 - x^3 + x - 1$, $g = x^2 - 1 \in \mathbb{Q}[x]$,
(3) $f = 7$, $g = 3 \in \mathbb{Q}[x]$,
(4) $f = x^3 + (3+i)x^2 + (2+3i)x + 2i$, $g = 2x + 2i \in \mathbb{C}[x]$,
(5) $f = x^4 + \overline{3}x^3 + x^2 + \overline{4}$, $g = (x - \overline{3})^2 \in \mathbb{Z}_7[x]$,
(6) $f = x^4 + \overline{3}x^3 + x^2 + \overline{4}$, $g = (x - \overline{3})^2 \in \mathbb{Z}_{11}[x]$.

9.2. Feladat. (2 pt. közösen megbeszéltük)
Milyen R gyűrűkre teljesül a következő feltétel?

(1) $(\forall f, g \in R[x])(\deg fg = \deg f + \deg g)$.
(2) $(\forall f, g \in R[x])(fg = gf)$.

9.3. Feladat. (2 pt. közösen megbeszéltük)
Számolja ki f és g polinomok legnagyobb közös osztóját:

(1) $f = x^3 + x^2 + \overline{1}$, $g = x^3 + x + \overline{1} \in \mathbb{Z}_2[x]$,
(2) $f = x^2 - 2x + 1$, $g = x^3 - 3x^2 + 2 \in \mathbb{Q}[x]$,
(3) $f = x^4 + x^3 + x + \overline{1}$, $g = x^3 + \overline{2}x^2 + \overline{2}x + \overline{1} \in \mathbb{Z}_5[x]$.

9.4. Feladat. (2 pt. közösen megbeszéltük)
Határozza meg az $fu+gv=h$ polinomegyenlet u, v általános megoldását az alábbi h polinomokra és az előző feladatban megadott f és g polinomokra.

(1) $h = x^2 \in \mathbb{Z}_2[x]$,
(2) $h = x^2 + 1 \in \mathbb{Q}[x]$,
(3) $h = x^2 + x \in \mathbb{Z}_5[x]$.

9.5. Feladat. (2 pt.)
Határozza meg az alábbi f és g polinomok közös gyökeit, majd számítsa ki külön-külön f és g gyökeit.

(1) $f = x^4 + 2x^3 - x^2 - 4x - 2$, $g = x^4 + x^3 - x^2 - 2x - 2 \in \mathbb{R}[x]$,
(2) $f = x^2 - 2x + 1$, $g = x^3 - 3x^2 + 2 \in \mathbb{Q}[x]$.

9.6. Feladat. (2 pt.)
Határozza meg a kételemű, illetve háromelemű test feletti összes irreducibilis első-, másod- és harmadfokú polinomot.

9.7. Feladat. (2 pt.)
Gyűrűt alkotnak-e

(1) $\mathbb{C}[x]$ páros fokú polinomjai a 0 polinommal együtt,
(2) $\mathbb{R}[x]$ legfeljebb huszadfokú polinomjai.
(3) $\mathbb{C}[x]$ elemei a szokásos összeadás, és a kompozícióra, mint szorzásra.

9.8. Feladat. (2 pt.)
Igazolja, hogy ha R integritástartomány, akkor minden nem konstans $f \in R[x]$ polinom minden $c \in R$ értéket csak véges sok R-beli helyen vehet föl.

9.9. Feladat. (2 pt.)
Mely m pozitív egészekre van $\mathbb{Z}_m[x]$-ben olyan nemnulla polinom, hogy gyökeinek száma nagyobb, mint foka?

9.10. Feladat. (2 pt.)
Adjon meg olyan f legfeljebb harmadfokú komplex együtthatós polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 15$ és $f(-1) = 0$.

9.11. Feladat. (2 pt.)
Létezik-e olyan $f \in \mathbb{Z}[x]$ polinom, melyre $f(10) = 400$, $f(14) = 440$ és $f(18) = 520$?

9.12. Feladat. (2 pt.)
Döntse el, hogy a következő polinomok irreducibilisek-e:

(1) $3x - 2 \in \mathbb{C}[x]$,
(2) $3x^2 + 2x + 10 \in \mathbb{C}[x]$,
(3) $2x^2 - 4x + 1 \in \mathbb{R}[x]$,
(4) $3x^2 + 2x + 10 \in \mathbb{R}[x]$,
(5) $3x^2 + 2x + 10 \in \mathbb{Q}[x]$,
(6) $2x^2 - 4x + 1 \in \mathbb{Q}[x]$,
(7) $x^4 + x^2 + \bar{1} \in \mathbb{Z}_2[x]$,
(8) $x^5 + x^2 + \bar{1} \in \mathbb{Z}_2[x]$.

9.13. Feladat. (2 pt.)
A Horner-elrendezés segítségével számítsa ki az alábbi f polinomok helyettesítési értékét a megadott c helyen. Amennyiben c gyöke f-nek állapítsa meg azt is, hogy hányszoros.

(1) $f = x^3 + 2x^2 - 3x + 2 \in \mathbb{C}[x]$ és $c = 1 + i$,
(2) $f = x^4 - (1+i)x^3 - (2+3i)x + 1 \in \mathbb{C}[x]$ és $c = 1 - 2i$,
(3) $f = \bar{2}x^6 + \bar{3}x^2 + \bar{4}x + \bar{5} \in \mathbb{Z}_{11}[x]$ és $c = \bar{7}$,
(4) $f = x^5 + x^4 + x^2 + \bar{1} \in \mathbb{Z}_2[x]$ és $c = \bar{1}$.

9.14. Feladat. (2 pt.)
Határozza meg az alábbi polinomok irreducibilis felbontását a komplex, valós és racionális számok teste felett:

(1) $x^8 - 16$,
(2) $x^3 - 6x^2 + 11x - 6$.
(3) $x^5 + x^4 + x^3 + x^2 + x + 1$,
(4) $x^4 - 10x^2 + 1$.

9.15. Feladat. (2 pt. közösen megbeszéltük)
Hány darab valós együtthatós irreducibilis polinom szorzatára bomlik fel az $x^{2007} + 2007x + 2007$ polinom?

9.16. Feladat. (2 pt.)
Határozza meg az alábbi $f \in \mathbb{Q}[x]$ polinomok racionális gyökeit és prímhatványtényezős alakját $\mathbb{Q}[x]$-ben:

(1) $f = x^3 - x^2 - x - 2$,
(2) $f = x^5 - 12x^3 + 36x - 12$,
(3) $f = 4x^4 - 7x^2 - 5x - 1$,
(4) $f = x^4 - x^3 + 2x + 1$,
(5) $f = 5x^8 - 5x^7 + 4x^2 - 2x - 2$.

9.17. Feladat. (2 pt.)
Mely k, m, n kitevőkre teljesül, hogy $x^2 - x + 1 \mid x^{3k} - x^{3m+1} + x^{3n+2}$.

9.18. Feladat. (2 pt.)
Minden n, m pozitív egész számra adja meg az $x^n - 1$ és $x^m - 1 \in \mathbb{R}[x]$ polinomok legnagyobb közös osztóját.

9.19. Feladat. (2 pt.)
Legyen T tetszőleges test. Mutassa meg, hogy $a_n x^n + \ldots a_1 x + a_0 \in T[x]$ ahol $a_n, a_0 \neq 0$ akkor és csak akkor irreducibilis, ha $a_0 x^n + \ldots a_{n-1} x + a_n$ is az.

9.20. Feladat. (2 pt.)
Határozza meg tetszőleges $n \in \mathbb{N}$ egészre az $nx^{n+1} - (n+1)x^n + 1$ és $x^n - nx + n - 1$ polinomok legnagyobb közös osztóját $\mathbb{Q}[x]$-ben.

9.21. Feladat. (2 pt. közösen megbeszéltük)
Keressen olyan $f \in \mathbb{C}[x]$ polinomot, hogy

(1) f' minden gyöke gyöke f-nek,
(2) f'-nek van olyan gyöke amely gyöke f-nek, és olyan is, amely nem gyöke f-nek.

9.22. Feladat. (2 pt.)
Igaz-e tetszőleges K test, $a \in K$ és $f \in K[x]$ esetén, hogy

(1) ha a többszörös gyöke f-nek, akkor a gyöke f'-nek,
(2) ha a k-szoros gyöke f-nek, akkor a $(k-1)$-szeres gyöke f'-nek?

9.23. Feladat. (2 pt. közösen megbeszéltük)
Tekintsük $f = x^4 + 6x^3 + 13x^2 + 12x + 4 \in \mathbb{C}[x]$ polinomot. A gyökök meghatározása nélkül adjon meg olyan $g \in \mathbb{C}[x]$ polinomot, amelynek minden gyöke egyszeres, és ugyanazok a gyökei, mint f-nek.

9.24. Feladat. (2 pt.)
Határozza meg az alábbi komplex együtthatós polinomok többszörös gyökeit:

(1) $x^7 - 3x^6 + 5x^5 - 7x^4 + 7x^3 - 5x^2 + 3x - 1$,
(2) $x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$,
(3) $x^6 - 5x^5 + 13x^4 - 20x^3 + 20x^2 - 12x + 4$.

9.25. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsa be, hogy tetszőleges p prímszámra és $c \in \mathbb{Z}_p$ konstansra az $x^p + c \in \mathbb{Z}_p[x]$ polinom nem irreducibilis.

9.26. Feladat. (2 pt.)
Bizonyítsa be, hogy tetszőleges p prímszámra $f_p = x^{p-1} + x^{p-2} + \cdots + 1$ polinom irreducibilis $\mathbb{Q}$ felett. Adja meg $\bar{f}_p$ irreducibilis felbontását $\mathbb{Z}_p$ felett.

9.27. Feladat. (2 pt. közösen megbeszéltük)
Tetszőleges p prímszám esetén adja meg az összes irreducibilis másodfokú polinom számát $\mathbb{Z}_p[x]$-ben.

9.28. Feladat. (2 pt.)
Keresse meg az összes olyan p prímszámot, amelyre az $x+\bar{2}$ polinom faktora az $x^4+x^3+x^2-x+\bar{1} \in \mathbb{Z}_p[x]$ polinomnak.

9.29. Feladat. (2 pt. közösen megbeszéltük)
Bizonyítsa be, hogy különböző $\mathbb{Q}[x]$-beli irreducibilis polinomoknak különböző komplex gyökei vannak. Ennek felhasználásával mutassa meg, hogy tetszőleges $f \in \mathbb{Q}[x]$ polinomra

(1) ha $a+b\sqrt{2}$ gyöke f-nek ahol $a, b \in \mathbb{Q}$, akkor $a-b\sqrt{2}$ is az,
(2) ha $\sqrt[3]{24}$ gyöke f-nek, akkor $-\sqrt[3]{3}+\sqrt[6]{3^5}i$ is az.

9.30. Feladat. (2 pt.)
Oldja meg az alábbi harmadfokú egyenleteket a komplex számok halmazán:

(1) $x^3-6x+4=0$,
(2) $x^3+9x-26=0$,
(3) $x^3-9x^2+18x+28=0$.

9.31. Feladat. (2 pt.)
Oldja meg az alábbi negyedfokú egyenleteket a komplex számok halmazán (segítségűl adott a kubikus rezolvens egy α gyöke):

(1) $x^4+2x^3+8x^2+2x+7=0$, $\alpha=4$;
(2) $x^4-2x^3+4x^2-2x+3=0$, $\alpha=2$.

9.32. Feladat. (2 pt.)
Fejezze ki elemi szimmetrikus polinomokkal a következő szimmetrikus polinomokat:

(1) $x_1^3+x_2^3+x_3^3-2x_1x_2x_3$,
(2) $x_1^2x_2x_3+\cdots+x_{n-2}x_{n-1}x_n^2$.

9.33. Feladat. (2 pt.)
Számítsa ki az $f=x^3-2x^2+1$ polinom gyökeinek k-adik hatványösszegét, ahol $k=1,2,3,4$.

9.34. Feladat. (2 pt.)
Legyenek x_1, x_2, x_3, x_4 az $f=x^4+ax^3+bx^2+cx+d \in \mathbb{C}[x]$ polinom gyökei $\mathbb{C}$-ben. Határozza meg

$$g=(x-(x_1x_2+x_3x_4))(x-(x_1x_3+x_2x_4))(x-(x_1x_4+x_2x_3))$$

polinom együtthatóit.

9.35. Feladat. (2 pt.)
Mutassa meg, hogy $\mathbb{Q}[x,y]$ Gauss gyűrű, de nem euklideszi gyűrű.

9.36. Feladat. (2 pt.)
A alábbi $\mathbb{Q}[x,y]$-beli polinomokat állítsa elő irreducibilis polinomok szorzataként.

(1) $f=5xy^7+3xy^6+2y+1$,
(2) $f=x^3y^6+y^5+x^4y+x$,
(3) $f=y^5x^3+(1-3y^5)x^2+3y^5x+y^7-y^5-1$.

9.37. Feladat. (2 pt.)
Jelölje $\mathbb{Q}(x)$ a $\mathbb{Q}[x]$ hányadostestét. Vegye észre, hogy $\mathbb{Q}(x)$ vektortér $\mathbb{Q}$ felett, és adja meg $\mathbb{Q}(x)$ egy $\mathbb{Q}$ feletti bázisát.

9.38. Feladat. (2 pt.)
Egy komplex szám algebrai egész, ha gyöke egy $\mathbb{Z}[x]$-beli főpolinomnak.

(1) Mutassa meg, hogy az algebrai egészek az algebrai számok testének egy részgyűrűjét alkotják.
(2) Bizonyítsa, hogy minden $r \in \mathbb{C}$ algebrai számhoz van olyan nemnulla $a \in \mathbb{Z}$, hogy ra algebrai egész.
(3) Határozza meg a $\mathbb{Q}$-beli algebrai egészek gyűrűjét.
(4) Határozza meg a $\mathbb{Q}(\sqrt{3}i)=\{\, a+b\sqrt{3}i \mid a,b \in \mathbb{Q} \,\}$-beli algebrai egészek gyűrűjét.

10. Integritástartományok

Az alábbi feladatokban legyen $\nu = \sqrt{3}i$, és $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

10.1. Feladat. (2 pt.)
Határozzuk meg a $D = \{a/b\colon\ a, b \in \mathbb{Z},\ 2 \not| b\}$ integritástartományban az egységeket és az irreducibilis elemeket. Mutassuk meg, hogy D euklideszi gyűrű.

10.2. Feladat. (2 pt.)
Igazoljuk, hogy ha egy euklideszi gyűrű a elemére $\|a\| = 1$, akkor a egység.

10.3. Feladat. (2 pt.)
Mutassuk meg, hogy $\mathbb{Q}[x, y]$ integritástartomány nem euklideszi gyűrű.

10.4. Feladat. (2 pt. közösen megbeszéltük)
Mutassuk meg, hogy $\mathbb{Z}[\nu]$ integritástartományban teljesül a leszálló oszthatósági láncfeltétel, de $\mathbb{Z}[\nu]$ nem Gauss gyűrű.

10.5. Feladat. (2 pt.)
Bizonyítsuk, hogy $\mathbb{Z}[\omega]$ euklideszi gyűrű az $\|a + b\omega\| = a^2 - ab + b^2,\ a, b \in \mathbb{Z}$, euklideszi normával.

10.6. Feladat. (2 pt.)
Adjuk meg $\mathbb{Z}[\omega]$ egységeit.

10.7. Feladat. (2 pt.)
Bizonyítsuk, hogy ha $d \in \mathbb{Z}[\omega]$ irreducibilis, akkor $\|d\|$ prím $\mathbb{Z}$-ben, vagy d egy $\mathbb{Z}$-beli prím asszociáltja $\mathbb{Z}[\omega]$-ban. Ha $\|d\|$ $\mathbb{Z}$-beli prím, akkor d irreducibilis $\mathbb{Z}[\omega]$-ban. Így ν irreducibilis $\mathbb{Z}[\omega]$-ban.

10.8. Feladat. (2 pt.)
Lássuk be, hogy ν asszociáltjai $\mathbb{Z}[\omega]$-ban: $\pm(1-\omega), \pm(1-\omega^2), \pm(\omega-\omega^2)$.

10.9. Feladat. (2 pt.)
Mutassuk meg, hogy $\mathbb{Z}[\omega] = \{\frac{a+b\nu}{2}\colon\ a, b \in \mathbb{Z},\ 2 \,|\, a-b\}$. Továbbá, tetszőleges $u \in \mathbb{Z}[\omega]$-ra u kongruens a $\pm 1, 0$ számok egyikével modulo ν.

10.10. Feladat. (2 pt.)
Bizonyítsuk, ha $u \in \mathbb{Z}[\omega]$-ra $u \equiv \pm 1 (\mathrm{mod}\ \nu)$, akkor $u^3 \equiv \pm 1 (\mathrm{mod}\ 9)$.

10.11. Feladat. (2 pt.)
Mutassuk meg, hogy $\mathbb{Z}[\omega]$-ban, ha $u^3 + v^3 = z^3$, akkor $\nu \,|\, uvz$.

10.12. Feladat. (2 pt.)
Legyenek $u, v, z \in \mathbb{Z}[\omega]$ és legyenek $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}[\omega]$-beli egységek. Lássuk be, hogy ha u, v, z, ν páronként relatív prímek, és $u^3 + \varepsilon_2 v^3 + \varepsilon_3(\nu^r z)^3 = 0$, akkor $\varepsilon_2 = \pm 1$ és $r \geq 2$.

10.13. Feladat. (2 pt.)
Mutassuk meg, hogy $\mathbb{Z}[\omega]$-ban $u^3 + v^3 = (u+v)(u+\omega v)(u+\omega^2 v)$. Továbbá, ha u, v, z és ν páronként relatív prímek, $r \geq 2$, ε egység, és $u^3 + v^3 + \varepsilon(\nu^r z)^3 = 0$, akkor léteznek $\varepsilon_1, \varepsilon_2, \varepsilon_3$ egységek, ν-höz és egymáshoz páronként relatív prím z_1, z_2, z_3 elemek $\mathbb{Z}[\omega]$-ban úgy, hogy

$$u + v = \varepsilon_1 \nu^a z_1^3, \quad u + \omega v = \varepsilon_2 \nu^b z_2^3, \quad u + \omega^2 v = \varepsilon_3 \nu^c z_3^3,$$

ahol $a + b + c = 3r$, és az a, b, c kitevők közül pontosan kettő egyenlő 1-gyel.

10.14. Feladat. (2 pt.)
Az előző feladat feltételei mellett mutassuk meg, hogy vannak olyan α, β, γ egységek, melyekre $\alpha\nu^a z_1^3 + \beta\nu^b z_2^3 + \gamma\nu^c z_3^3 = 0$. Továbbá az általánosság megszorítása nélkül $a = b = 1$, és így valamely $\varepsilon_2, \varepsilon_3$ egységekre és $r - 1 \geq 1$-re $z_1^3 + \varepsilon_2 z_2^3 + \varepsilon_3(\nu^{r-1} z_3)^3 = 0$.

10.15. Feladat. (2 pt.)
Mutassuk meg, hogy az $u^3 + v^3 = z^3$ egyenletnek nincs nemtriviális megoldása $\mathbb{Z}[\omega]$-ban és így $\mathbb{Z}$-ben sincs.

11. Véges testek

11.1. Feladat. (2 pt.)
Mutassa meg, hogy tesz̋leges p-karakterisztikájú véges test bármely eleme p-dik hatványa a test valamely elemének.

11.2. Feladat. (2 pt.)
Mutassa meg, hogy K véges test feletti irreducibilis polinomnak nincs többszörös gyöke K semilyen L bővítésében.

11.3. Feladat. (2 pt.)
Adjon meg olyan p-karakterisztikájú K testet és $f \in K[x]$ irreducibilis polinomot úgy, hogy f-nek van többszörös gyöke K valamely bővítésében.

11.4. Feladat. (2 pt.)
Lehet-e véges test algebrailag zárt?

11.5. Feladat. (2 pt.)
Tekintsük a $K = (\{ax^2+bx+c : \ a,b,c \in \mathbb{Z}_3\}; +, \cdot)$ huszonhét elemű testet, ahol a $+$ és $\cdot$ műveleteket modulo $x^3+2x+2 \in \mathbb{Z}_3[x]$ értjük. Határozza meg a $2x^2$ és x^2+x+1 elemek összegét, szorzatát és inverzét K-ban.

11.6. Feladat. (2 pt.)
Van-e gyöke az $3x^2+2x-3$ polinomnak a 121 elemű testben?

11.7. Feladat. (2 pt.)
Bizonyítsa, hogy véges test tetszőleges eleme két elem négyzetének összege.

11.8. Feladat. (2 pt.)
Mutassa meg, hogy $x^{p^n} - x \in \mathbb{Z}_p[x]$ polinom $\mathbb{Z}_p$ feletti felbontási teste egy p^n elemű test.

11.9. Feladat. (2 pt.)
Mutassa meg, hogy $\mathbb{Z}_p$ felett minden pozitív n egészre létezik n-ed fokú irreducibilis polinom.

11.10. Feladat. (2 pt.)
Mutassa meg, hogy tetszőleges $f \in \mathbb{Z}_p[x]$-beli irreducibilis polinomra $\deg f \mid n$ pontosan akkor teljesül, ha $f \mid x^{p^n} - x$.

11.11. Feladat. (2 pt.)
Bizonyítsa, hogy $x^{p^n} - x = \prod f$, ahol f végig fut azokon a $\mathbb{Z}_p[x]$-beli irreducibilis főpolinomokon, melyekre $\deg f \mid n$. Továbbá, $p^n = \sum_{d \mid n} d a_d$, ahol a_d a $\mathbb{Z}_p$ feletti d-ed fokú irreducibilis főpolinomok száma.

11.12. Feladat. (2 pt.)
Határozza meg a $\mathbb{Z}_p$ feletti n-ed fokú irreducibilis polinomok számát.

11.13. Feladat. (2 pt.)
Legyen K tetszőleges test, $f \in K[x]$ és a az f gyöke K valamely bővítésében. Bizonyítsa, hogy f pontosan akkor irreducibilis K fölött, ha $\deg f$ megegyezik $K(a)$ test K feletti dimenziójával.

11.14. Feladat. (2 pt.)
Legyen K véges test, $a \in K$ generátoreleme K multiplikatív csoportjának. Bizonyítsa, hogy $x^{|K|-1} - a$ irreducibilis K felett.

11.15. Feladat. (2 pt.)
Dirichlet számtani sorozatokra vonatkozó tételét felhasználva mutassa meg, hogy minden pozitív n egészhez van olyan p prím és $a \in \mathbb{Z}_p$, hogy $x^n - a$ irreducibilis.

11.16. Feladat. (2 pt.)
Legyen p tetszőleges prím. Bizonyítsa, hogy bármely n esetén, ha $p \nmid n$, akkor létezik egy K p^m-elemű test és $a \in K$ úgy, hogy $x^n - a$ irreducibilis K felett.

11.17. Feladat. (2 pt.)
Legyen K tetszőleges véges test. Mely n-ekre áll elő K bármely eleme valamely K-beli elem n-dik hatványaként?

11.18. Feladat. (2 pt.)
Legyen K tetszőleges test. Azt mondjuk, hogy $\varepsilon \in K$ n-edik egységgyök, ha ε gyöke az $x^n - 1$ polinomnak. Az ε egységgyök primitív n-edik egységgyök, ha rendje n a K multplikatív csoportjában. Mutassa meg, hogy ha $\mathrm{char}(K) \nmid n$, akkor K valamely bővítése tartalmaz primitív n-edik egységgyököt. Mi a helyzet, akkor ha $\mathrm{char}(K) \mid n$?

11.19. Feladat. (2 pt.)
Legyen K olyan test, amely tartalmaz primitív n-edik egységgyököt. Jelölje P_n a K-beli primitív n-edik egységgyökök halmazát. Tekintsük az $f_n = \prod_{\varepsilon \in P_n}(x - \varepsilon)$ (ú.n. n-edik körosztási) polinomot $K[x]$-ben. Bizonyítsa, hogy f_n a K prímteste fölötti polinom. Továbbá, $f_n = \prod_{d \mid n}(x^d - 1)^{\mu(n/d)}$.

11.20. Feladat. (2 pt.)
Legyen $p \nmid n$ prím. Legyen ε primitív n-edik egységgyök $\mathbb{Z}_p$ valamely bővítésében. Bizonyítsa, hogy $\mathbb{Z}_p(\varepsilon)$ dimenziója $\mathbb{Z}_p$ felett megegyezik p modulo n rendjével. Keressen olyan n-t és $p \nmid n$ prímet, amelyre f_n reducibilis $\mathbb{Z}_p$ felett.

11.21. Feladat. (2 pt.)
Bizonyítsa, hogy K véges test alaphalmazán értelmezett tetszőleges n-változós művelet K feletti polinomfüggvény.

11.22. Feladat. (2 pt.)
Bizonyítsa Minkowski tételét: Legyen adott egy paralellogrammarács a síkon T területű alapparalellogrammával, valamint egy S origó középpontú centrálisan szimmetrikus, konvex síkidom, melynek területe nagyobb, mint $4T$. Ekkor S tartalmaz az origótól különböző rácspontot.

11.23. Feladat. (2 pt.)
Minkowski tételét felhasználva bizonyítsa, hogy bármely $3k + 1$ alakú prímszám felírható $a^2 + 3b^2$ alakban, ahol a, b egészek.

11.24. Feladat. (2 pt.)
Mutassa meg, hogy $\mathbb{Z}(\omega)$ irreducibilis elemei asszociáltságtól eltekintve a következők:

- ν,
- a $3k - 1$ alakú $\mathbb{Z}$-beli prímek,
- a $3k + 1$ alakú $\mathbb{Z}$-beli prímek $a + b\nu$ alakú osztói, ahol $a, b \in \mathbb{Z}$ és $3k + 1 = a^2 + 3b^2$.