

# ALGEBRA ÉS SZÁMELMÉLET

szorgalmi feladatok

2016 őszi félév, BSc

## Komplex számok

- 1. feladat** Határozza meg az  $5 + 12i$  komplex szám négyzetgyökeit kanonikus alakban.
- 2. feladat** Oldja meg az  $(1 - 2i)x^2 + (3 + i)x + i = 0$  egyenletet a komplex számok halmazán.
- 3. feladat** Oldja meg az  $i\bar{z} = z^2$  egyenletet a komplex számok halmazán.
- 4. feladat** Ábrázolja a komplex számsíkon a  $\{z^2 : \operatorname{Re} z = 1\}$  halmazt.
- 5. feladat** Ábrázolja a komplex számsíkon a  $\operatorname{Re}\left(\frac{1}{z}\right) = \lambda$  egyenlőséget kielégítő  $z$  komplex számok halmazát.
- 6. feladat** Mekkora szöveget zárnak be egymással az origót a  $(2, 1)$  és az  $(1, 3)$  ponttal összekötő szakaszok?
- 7. feladat** Bizonyítsa be, hogy  $\arctg 1 + \arctg 2 + \arctg 3 = \pi$ .
- 8. feladat** Mutassa meg, hogy  $4 \arctg \frac{1}{5} - \arctg \frac{1}{239} = \frac{\pi}{4}$ .
- 9. feladat** Rajzoljunk az  $ABC$  háromszög  $AC$  oldalára kifelé egy négyzetet; ennek  $A$ -val szomszédos csúcsai legyenek  $C$  és  $D$ . Hasonlóképpen, a  $BC$  oldalra rajzolt négyzet  $B$ -vel szomszédos csúcsai  $C$  és  $E$ . Mutassa meg, hogy ha a háromszög  $C$  csúcsát mozgatjuk (de az  $AB$  oldal fix), akkor a  $DE$  szakasz felezőpontja helyben marad.
- 10. feladat** Rajzoljunk egy tetszőleges háromszög oldalaira kifelé szabályos háromszögeket. Bizonyítsa be, hogy ezen háromszögek középpontjai által meghatározott háromszög szabályos.
- 11. feladat** Rajzoljunk egy tetszőleges négyszög oldalaira kifelé négyzeteket. Bizonyítsa be, hogy a szemközti oldalakra rajzolt négyzetek középpontjait összekötő szakaszok egyenlő hosszúak és egymásra merőlegesek.
- 12. feladat** Bizonyítsa be, hogy nem létezik szabályos rácsháromszög.
- 13. feladat** Igazolja, hogy az  $x, y, z \in \mathbb{C}$  komplex számok által meghatározott háromszög akkor és csak akkor szabályos, ha  $x^2 + y^2 + z^2 = xy + yz + zx$ .
- 14. feladat** Fejezze ki  $\cos(2016x)$ -et  $\cos x$  és  $\sin x$  segítségével.
- 15. feladat** Adjon zárt formulát a  $\sin x + \sin 2x + \dots + \sin nx$  összegre.
- 16. feladat** Mutassa meg, hogy  $\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \binom{n}{7} + \dots = \sqrt{2}^n \sin \frac{n\pi}{4}$ . (Útmutatás: Számítsa ki az  $(1 + i)^n$  hatványt kétféleképpen.)
- 17. feladat** Hogyan bolyong a komplex számsíkon a  $z^n$  sorozat, amint  $n$  tart végtelenbe? (A válasz persze  $z$ -től függ.)
- 18. feladat** Oldja meg az  $|z^3 + 2 - 2i| + z\bar{z}|z| = 2\sqrt{2}$  egyenletet a komplex számok halmazán.
- 19. feladat** Mikor lehet  $\varepsilon$  és  $\varepsilon + 1$  is egységgyök?
- 20. feladat** Határozza meg  $\sin 72^\circ$  értékét. (Útmutatás: Tekintsük a  $z = \operatorname{cis} 72^\circ$  komplex számot. Ez ötödik egységgyök, így gyöke az  $\frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$  polinomnak.)
- 21. feladat** Mennyi az  $n$ -edik egységgyökök  $k$ -edik hatványainak összege?
- 22. feladat** Határozza meg az  $n$ -edik egységgyökök szorzatát.
- 23. feladat** Határozza meg mindazokat a komplex számokat, amelyek hetvenhatodik és századik egységgyökök is.

## Gyűrűk és testek

- 24. feladat** Gyűrűt, integritástartományt, illetve testet alkot-e a  $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$  halmaz (a szokásos összeadással és szorzással), ahol  $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ ?
- 25. feladat** Legyen  $\xi \in \mathbb{C} \setminus \mathbb{Q}$  egy gyöke az  $x^2 + px + q$  polinomnak, ahol  $p$  és  $q$  egész számok. Mutassa meg, hogy ekkor a  $\mathbb{Z}[\xi] = \{a + b\xi : a, b \in \mathbb{Z}\}$  halmaz integritástartományt alkot a szokásos összeadással és szorzással.
- 26. feladat** Határozza meg a  $8 + i$  és  $4 - 2i$  Gauss-egészek legnagyobb közös osztóját.
- 27. feladat** Jelölje  $\mathcal{P}(U)$  az  $U$  halmaz hatványhalmazát, azaz  $U$  összes részhalmazainak halmazát. Gyűrűt, integritástartományt, illetve testet alkot-e a  $\mathcal{P}(U)$  halmaz a szimmetrikus differencia és a metszés műveletével? (A válasz függ  $U$  elemszámától!)

**28. feladat** A duális számokat a komplex számokhoz hasonlóan definiáljuk, de itt a „képzetes egység” négyzete nem  $-1$ , hanem  $0$ . Tehát  $\mathbb{D} = \{a + b\varepsilon : a, b \in \mathbb{R}\}$ , ahol  $\varepsilon$  egy olyan szimbólum, amelyre  $\varepsilon^2 = 0$ . (Mi lehet ennek az értelme? Miért pont  $\varepsilon$ -t használunk?) Mutassa meg, hogy a duális számok (a természetes módon definiált összeadással és szorzással) kommutatív egységelemes gyűrűt alkotnak. Határozza meg a  $\mathbb{D}$  gyűrű zérusosztóit és egységeit.

**29. feladat** Határozza meg a  $\mathbb{Z}[\omega]$  gyűrű egységeit (lásd a 24. feladatot).

**30. feladat** Keressen egy  $\pm 1$ -től különböző egységet a  $\mathbb{Z}[\sqrt{2}]$  gyűrűben, majd ennek segítségével konstruáljon meg végtelen sok egységet.

**31. feladat** Határozza meg a véges tizedestörtek gyűrűjének egységeit.

**32. feladat** Definiáljunk egy újfajta összeadást és egy újfajta szorzást a valós számok halmazán: legyen  $a \oplus b = a + b - 1$  és  $a \odot b = a + b - ab$ . Igazolja, hogy az  $(\mathbb{R}; \oplus, \odot)$  struktúra test.

**33. feladat** Bizonyítsa be, hogy az  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  alakú valós mátrixok testet alkotnak a szokásos mátrixműveletekkel.

**34. feladat** Definiáljunk egy újfajta „összeadást” a pozitív valós számok halmazán: legyen  $a \oplus b = a \cdot b$ . Adjon meg olyan  $\odot$  „szorzást”, amelyre  $(\mathbb{R}^+; \oplus, \odot)$  test.

**35. feladat** Bizonyítsa be, hogy minden véges integritástartomány test.

**36. feladat** Adjon meg olyan összeadást és szorzást a  $T = \{0, 1, a, b\}$  halmazon, amellyel  $(T; +, \cdot)$  test.

**37. feladat** Mennyi lehet egy véges test összes elemének összege?

### Test feletti egyhatározatlanú polinomok

**38. feladat** Számítsa ki az  $(x - \bar{1})(x - \bar{2}) \cdots (x - \overline{p-1}) \in \mathbb{Z}_p[x]$  polinomban  $x^{p-1}$ ,  $x^{p-2}$ ,  $x^{p-3}$  és  $x^0$  együtthatóját, ahol  $p \geq 5$  prímszám.

**39. feladat** Oldja meg az  $(x^3 + x^2)u + (x^3 + x^2 + x)v + (x^3 + \bar{1})w = \bar{1}$  egyenletet a  $\mathbb{Z}_2[x]$  polinomgyűrűben.

**40. feladat** Határozza meg  $x^{100} - 1$  és  $x^{44} - 1$  legnagyobb közös osztóját. Hogyan lehetne általánosítani a feladatot?

**41. feladat** Mely  $p$  prímszámok esetén létezik multiplikatív inverze az  $x - \bar{1} \in \mathbb{Z}_p[x]$  polinomnak modulo  $x^3 + x + \bar{1}$ ? Számítsa is ki a multiplikatív inverzet, amikor létezik.

**42. feladat** Bézout tételének segítségével vizsgálja meg, hogy teljesül-e a  $g \mid f$  oszthatóság a  $g = x^2 - 1$  és  $f = x^{17} - x^{16} + x^{15} - x^{14} + x^7 - x^3 + x - 1$  polinomokra a  $\mathbb{Q}$ ,  $\mathbb{Z}_3$ , illetve  $\mathbb{Z}_7$  testek fölött.

**43. feladat** Mely  $n$  pozitív egészekre osztható az  $x^{2n} + x^n + 1$  polinom az  $x^2 + x + 1$  polinommal? (Útmutatás: használjuk Bézout tételét.)

**44. feladat** Az  $a$  valós paraméter mely értékeire lesz az  $1$  kétszeres gyöke az  $x^5 + 3ax^4 - 4ax^3 - 5x + 1$  polinomnak?

**45. feladat** Legyen  $f$  a  $(k, (-1)^k)$ ,  $k = 0, \dots, 9$  pontokra illesztett interpolációs polinom. Mennyi  $f(10)$  értéke?

**46. feladat** Legyenek  $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$  az  $n$ -edik egységgyökök, és legyen  $f \in \mathbb{C}[x]$  az  $(\varepsilon_0, y_0), (\varepsilon_1, y_1), \dots, (\varepsilon_{n-1}, y_{n-1})$  pontokra illesztett Lagrange-féle interpolációs polinom. Igazolja, hogy  $f(0)$  éppen az  $y_0, \dots, y_{n-1}$  számok átlaga.

**47. feladat** A  $(0, a_0), (1, a_1), (2, a_2)$  pontokra akkor és csak akkor illeszthető egyenes, ha  $a_0 - 2a_1 + a_2 = 0$  (ugye?). Mutassa meg, hogy a  $(0, a_0), (1, a_1), (2, a_2), (3, a_3)$  pontokra akkor és csak akkor illeszthető parabola (amely elfajuló esetben lehet egyenes is), ha  $a_0 - 3a_1 + 3a_2 - a_3 = 0$ .

**48. feladat** Az előző feladat általánosításaként bizonyítsa be, hogy a  $(0, a_0), (1, a_1), \dots, (n+1, a_{n+1})$  pontok akkor és csak akkor illeszkednek egy legfeljebb  $n$ -edfokú polinomfüggvény grafikonjára, ha

$$\binom{n+1}{0}a_0 - \binom{n+1}{1}a_1 + \binom{n+1}{2}a_2 + \cdots + (-1)^k \binom{n+1}{k}a_k + \cdots + (-1)^{n+1} \binom{n+1}{n+1}a_{n+1} = 0.$$

**49. feladat** Mutassa meg, hogy egy  $f \in \mathbb{R}[x]$  polinom akkor és csak akkor vesz fel egész értéket minden egész helyen, ha előáll  $\binom{x}{k} = \frac{x(x-1)\cdots(x-(k-1))}{k!}$  alakú polinomok egész együtthatós lineáris kombinációjaként.

**50. feladat** Adja meg az  $x^5 + \bar{6}x^4 + x^3 + \bar{6}x^2 + \bar{2}x + \bar{5} \in \mathbb{Z}_7[x]$  polinom irreducibilis felbontását.

**51. feladat** Hány másodfokú irreducibilis polinom van  $\mathbb{Z}_p[x]$ -ben?

**52. feladat** Adja meg az  $x^p - x \in \mathbb{Z}_p[x]$  polinom irreducibilis felbontását tetszőleges  $p$  prímszám esetén.

**53. feladat** Adja meg az  $x^5 + x^3 + ax^2 + a \in T[x]$  polinom irreducibilis felbontását, ahol  $T = \{0, 1, a, b\}$  a négyelemű test.

**54. feladat** Határozza meg a 121-elemű test összes elemének összegét.

**55. feladat** Határozza meg az összes olyan  $p$  prímszámot, amelyre  $x^2 + \bar{1} \mid x^{2008} - \bar{23}x^{1922} + \bar{13}x^{600} + \bar{8}$  teljesül a  $\mathbb{Z}_p[x]$  polinomgyűrűben. (Útmutatás: használjuk Bézout tételét vagy magában a  $\mathbb{Z}_p$  testben, vagy annak egy alkalmas bővítésében.)

**56. feladat** Képzelje el (de ne írja fel!) az  $x^{1973} - 1997$  polinom irreducibilis felbontását  $\mathbb{R}$  felett. Hány tényezőt lát (a lelki szemeivel), és hányadfokúak ezek?

**57. feladat** Írja fel az  $f = (x-1)(x^2-1)(x^3-1)(x^4-1)$  és  $g = (x+1)(x^2+1)(x^3+1)(x^4+1)$  polinomok irreducibilis felbontását a kedvenc számteste felett, majd számítsa ki ennek segítségével  $f$  és  $g$  legnagyobb közös osztóját.

**58. feladat** Határozza meg az egységkörbe írt szabályos  $n$ -szög egy csúcsából kiinduló átlói hosszának szorzatát. (Itt most átlónak tekintjük az oldalakat is, tehát egy csúcsból  $n-1$  átló indul ki.)

**59. feladat** Anélkül, hogy megkeresné a gyököket, határozza meg a  $3x^5 + 6x^4 + 9x^3 + 2x^2 + 4x + 1$  polinom gyökeinek négyzetösszegét.

**60. feladat** Határozza meg a  $\lambda$  komplex paraméter értékét úgy, hogy az  $x^3 - 7x + \lambda$  polinom egyik gyöke valamelyik másik gyök kétszerese legyen.

**61. feladat** Adja meg az  $x^p - 1 \in \mathbb{Q}[x]$  polinom irreducibilis felbontását, ahol  $p$  tetszőleges prímszám. (Útmutatás: térjünk át az  $y = x - 1$  határozatlanra.)

**62. feladat** Adjon meg végtelen sok olyan  $n$  egész számot, melyre az  $x^2 + 100x + n$  polinom irreducibilis  $\mathbb{Q}$  felett, és végtelen sok olyat is, amelyre nem irreducibilis.

**63. feladat** Mely  $p$  prímszámok esetén van racionális gyöke az  $x^4 + 2x^3 - 16x^2 + 2x + p$  polinomnak?

**64. feladat** Bizonyítsa be, hogy tetszőleges  $T$  test és tetszőleges  $a_0, \dots, a_n \in T$ ,  $a_0, a_n \neq 0$  elemek esetén az  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in T[x]$  polinom akkor és csak akkor irreducibilis, ha  $a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$  is az.

**65. feladat** Mutassa meg, hogy a  $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$  halmaz nem zárt a szorzásra.

**66. feladat** Legyen  $f \in \mathbb{Z}[x]$  egy olyan 101-edfokú polinom, amely legalább 101 egész számra  $\pm 1$  értéket vesz fel. Bizonyítsa be, hogy  $f$  irreducibilis  $\mathbb{Q}$  felett. (Útmutatás: használjuk Kronecker módszerét.)

**67. feladat** Bizonyítsa be, hogy az  $f = x^n + ax + p$  polinom irreducibilis  $\mathbb{Q}$  felett bármely  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $p$  prímszám,  $p > |a| + 1$  esetén. (Útmutatás: Először azt mutassuk meg, hogy  $f$  minden  $\alpha$  gyökére  $|\alpha| > 1$ .)

**68. feladat** Legyen  $f \in \mathbb{Z}[x]$  egy főpolinom, melynek konstans tagja nem nulla (azaz  $f(0) \neq 0$ ). Tegyük fel, hogy  $f$ -nek egyetlen komplex gyöke van az egységkörtől kívül, az összes többi gyöke pedig az egységkör belsejében helyezkedik el (a körvonalon nincs egy gyök se). Bizonyítsa be, hogy  $f$  irreducibilis  $\mathbb{Q}$  felett.

**69. feladat** Mikor osztható egy polinom a saját deriváltjával?

**70. feladat** Határozza meg az  $a, b$  paraméterek értékét úgy, hogy legyen háromszoros gyöke a  $3x^5 - 10x^3 + ax + b \in \mathbb{C}[x]$  polinomnak.

**71. feladat** Mutassa meg, hogy az  $1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$  polinomnak nincs többszörös gyöke a komplex számok testében.

**72. feladat** Legyenek az  $f \in \mathbb{C}[x]$  polinom komplex gyökei  $\alpha_1, \dots, \alpha_n$ . Tegyük fel, hogy a gyökök páronként különbözők, és egy konvex  $n$ -szöget alkotnak a komplex számsíkon. Bizonyítsa be, hogy  $f'$  gyökei csak ennek a sokszögnek a belsejében vagy a határán helyezkedhetnek el.

## Csoportok

**73. feladat** Tetszőleges  $R$  kommutatív egységelemes gyűrű esetén legyen  $L_R = \{x \mapsto ax + b : a \in R^*, b \in R\}$  az  $R$  feletti bijektív „lineáris” függvények halmaza. Mutassa meg, hogy  $L_R$  csoportot alkot a leképezésszorozás műveletével.

**74. feladat** Érvényes-e minden csoportban tetszőleges  $x, y$  elemekre az  $x^2 = y^2, x^3 = y^3 \implies x = y$  következtetés?

**75. feladat** Bizonyítsa be, hogy a  $(\mathbb{Q}^+; \cdot)$  és  $(\mathbb{Z}[x]; +)$  csoportok izomorfak egymással.

**76. feladat** Hány eleme van a  $GL(\mathbb{Z}_p, 2)$  csoportnak?

**77. feladat** Hány eleme van a kocka mozgás-, illetve szimmetriacsoportjának?

**78. feladat** Oldja meg  $S_6$ -ban a  $\pi^2 = (1\ 2)$ , illetve a  $\pi^2 = (1\ 2\ 3)$  egyenleteket.

**79. feladat** A páronként idegen ciklusokra bontott alak segítségével adjon meg szükséges és elegendő feltételt arra, hogy egy permutáció előálljon valamely permutáció négyzeteként (azaz második hatványaként).

- 80. feladat** Milyen a ciklusszerkezete egy  $n$  hosszúságú ciklus  $k$ -adik hatványának?
- 81. feladat** Bizonyítsa be, hogy  $S_n$  minden permutációja felírható legfeljebb  $n - 1$  transzpozíció szorzataként.
- 82. feladat** Igazolja, hogy egy  $n$  hosszúságú ciklus nem írható fel  $n - 1$ -nél kevesebb transzpozíció szorzataként.
- 83. feladat** Igazolja, hogy ha egy csoportban az  $a$  és  $b$  véges rendű elemek felcserélhetőek, akkor  $o(ab) \mid \text{lkk}(o(a), o(b))$ .
- 84. feladat** Határozza meg az  $L_{\mathbb{R}}$  csoport véges rendű elemeit (lásd a 73. feladatot).
- 85. feladat** Adjon meg olyan végtelen csoportot, amelynek minden eleme véges rendű, valamint olyan végtelen csoportot, melyben csak véges sok véges rendű elem van. Van-e olyan csoport, amelynek véges sok végtelen rendű eleme van?
- 86. feladat** Igazolja, hogy ha egy csoportban az egységelemtől különböző összes elem rendje ugyanaz, akkor az végtelen vagy prímszám.
- 87. feladat** Igazolja, hogy ha egy csoport minden elemének rendje legfeljebb 2, akkor a csoport kommutatív.
- 88. feladat** Mutassa meg, hogy ha egy véges csoport elemszáma páros, akkor a csoportban van másodrendű elem.
- 89. feladat** Mutassa meg, hogy tetszőleges  $k \in \mathbb{N} \cup \{\infty\}$  esetén van olyan csoport és abban két olyan másodrendű elem, amelyek szorzatának rendje  $k$ .
- 90. feladat** Mutassa meg, hogy minden Abel-csoport legfeljebb másodrendű elemeinek halmaza részcsoportot alkot. Adjon példát olyan Abel-csoportra, melyben a legfeljebb harmadrendű elemek nem alkotnak részcsoportot.
- 91. feladat** Igazolja, hogy  $S_n$  minden részcsoportjában vagy minden permutáció páros, vagy a permutációknak pontosan a fele páros.
- 92. feladat** Mutassa meg, hogy tetszőleges  $p$  prímszám esetén a  $\mathbb{C}^*$  csoportban részcsoportot alkot a következő halmaz:  $E_{p^\infty} = \{u \in \mathbb{C}^* : \text{van olyan } k \in \mathbb{N}_0, \text{ amelyre } u^{p^k} = 1\}$ .
- 93. feladat** Bizonyítsa be, hogy az  $E_{p^\infty}$  csoport minden valódi részcsoportja ciklikus (lásd a 92. feladatot).
- 94. feladat** Jelölje  $D_\infty$  a  $\dots$  TTTTTTTTTTTTTT  $\dots$  alakzat szimmetriacsoportját. Mutassa meg, hogy  $D_\infty \cong L_{\mathbb{Z}}$ , továbbá ez a csoport izomorf az  $\begin{pmatrix} \varepsilon & k \\ 0 & 1 \end{pmatrix}$  alakú mátrixok csoportjával, ahol  $\varepsilon \in \{1, -1\}$  és  $k \in \mathbb{Z}$  (lásd a 73. feladatot).
- 95. feladat** Igazolja, hogy egy csoport akkor és csak akkor véges, ha véges sok részcsoportja van.
- 96. feladat** Igazolja, hogy az  $S_n$  csoportot generálják az  $(1\ 2)$  és  $(1\ 2\ \dots\ n)$  permutációk.
- 97. feladat** Igazolja, hogy az  $A_n$  csoportot generálják az összes 3 hosszúságú ciklusok.
- 98. feladat** Adjon meg 1, 2, illetve 3 elemű *minimális* generátorrendszert a  $\mathbb{Z}_{18}$ , illetve az  $S_3$  csoportban (ha létezik).
- 99. feladat** Mutassa meg, hogy ha egy  $G$  csoport nem Abel-féle, de minden valódi részcsoportja Abel-féle, akkor  $G$ -nek van kételemű generátorrendszere.
- 100. feladat** Bizonyítsa be, hogy a  $\mathbb{Q}$  csoport minden végesen generált részcsoportja ciklikus, és adjon meg olyan valódi részcsoportját, amely nem ciklikus.

### Hatványozás modulo $m$

- 101. feladat** Mennyit ad 53-mal osztva maradékul  $80^{(111^{50})}$ ?
- 102. feladat** Mennyit ad héttel osztva maradékul  $111 \dots 111$  (99 egyes)?
- 103. feladat** Bizonyítsa be, hogy minden  $n \in \mathbb{N}$  esetén az  $n$ ,  $n^8 - 1$ ,  $n^8 + 1$  számok valamelyike osztható 17-tel.
- 104. feladat** Mutassa meg, hogy ha  $(a, 100) = 1$ , akkor  $a^{20} \equiv 1 \pmod{100}$  teljesül. Hasonlítsa össze ezt az állítást az Euler-Fermat-tétellel.
- 105. feladat** Igazolja, hogy  $a^{561} \equiv a \pmod{561}$  bármely  $a$  egész számra.
- 106. feladat** Bizonyítsa be, hogy ha  $n$  nem osztható se 2-vel se 5-tel, akkor van  $99 \dots 99$  alakú többszöröse.
- 107. feladat** Legyen  $p$  és  $q$  két különböző prímszám. Mutassa meg, hogy  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .
- 108. feladat** Igazolja, hogy bármely  $p$  páratlan prímszámra  $2^2 \cdot 4^2 \cdot 6^2 \cdot \dots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ .
- 109. feladat** Legyen  $p$  páratlan prímszám. Lehetséges-e, hogy két modulo  $p$  primitív gyök szorzata is primitív gyök?