

Algebra és számelmélet
tételsor, 2019 - 2020. I. félév

„Mesélős” tételek: a fogalmakat pontosan definiálni kell, a vonatkozó tételeket pontosan kell megfogalmazni, bizonyítani azonban nem kell azokat, „csak” érteni. Példákkal/ellenpéldákkal illusztrálni is kell a fogalmakat.

A sorozat

1. Komplex számok: kanonikus alak, konjugált, abszolút érték, a komplex számsík.
2. Komplex számok trigonometrikus alakja, hatványozás, gyökvonás, egységgyökök.
3. A harmad- és a negyedfokú egyenletek megoldási eljárásai.
4. A gyűrű, az integritástartomány és a test fogalma.
5. Nevezetes gyűrűk: maradékosztály-gyűrűk, Gauss-egészek.
6. Oszthatóság legnagyobb közös osztó integritástartományokban.
7. Polinomfüggvények, gyökök, interpoláció.
8. Irreducibilis polinomok a komplex- és a valós számtest fölött.
9. Irreducibilis polinomok a racionális számok teste fölött.
10. Polinom deriváltja, többszörös gyökök.
11. Nevezetes prímek: Mersenne- és Fermat prímek.

B sorozat

1. A csoport fogalma, izomorfia.
2. Nevezetes példák csoportokra.
3. Permutációcsoportok.
4. Hatványozás csoportokban, elem rendje, ciklikus csoportok.
5. Részcsoport, generálás.
6. Lagrange tétele véges csoportokra.
7. Számelméleti függvények, az Euler-féle ϕ -függvény.
8. Egész szám rendje modulo m , primitív gyök.
9. Titkosítások, prímtesztek, a Fermat problémakör.

„Bizonyítás” tételek: a zárójelben felsorolt tételek közül 2 - 3 kiválasztottnak a bizonyítását kell elmondani. A kiválasztás a tétel kihúzásakor történik.

A sorozat

1. Gyökvonás komplex számokból (1.4 – 1.8. tételek)
2. Egész számok kongruenciái, lineáris diophantoszi egyenletek, számelméleti függvények (3.3. - 3.7. tételek.)
3. Teljes és redukált maradékrendszerek (3.9. – 3.13. tételek)
4. Wilson kongruencia tétele és megfordítása (3.14, 3.15. tételek)
5. Hatványozás modulo m (3.16. és 3.17. tételek)
6. Test fölötti polinomgyűrű, oszthatóság, maradékos osztás (4.6. – 4.9. tételek)
7. Polinomok számelmélete (4.10. – 4.14. tételek)
8. Kongruenciák testfölötti polinomgyűrűkben, polinomgyűrűk faktorgyűrűi (4.15. – 5.19. tételek)
9. Polinomfüggvények, zéróhelyeik. (5.1. – 5. 6. és 5.8. 5.9. tételek)
10. Irreducibilis polinomok, faktorizáció polinomgyűrűkben (5.11. – 5.17. és 5.20. tételek)
11. Irreducibilis polinomok a racionális számok teste fölött (5.23 – 5.28. tételek)
12. Polinom deriváltja, többszörös gyökök (5.31. – 5.35. tételek)

B sorozat

1. Gyűrűk, integritástartományok és testek (2.1. – 2.11. tételek)
2. Csoportok (6.1.- 6.3. 6.5. tételek)
3. Permutációcsoportok (6.6. 6.7. és 6.11. – 6.12. tételek)
4. Hatványozás, elemrend csoportokban (6.13. – 6.18. tételek)
5. Részcsoport, generálás (6.19. – 6.22. tételek)
6. Lagrange tétele és következményei (6.23. – 6.26. tételek)
7. Normálosztó szerinti faktorcsoportok, homomorfizáció (6.27. – 6.28. tételek)
8. Testbővítések (7.1. – 7.3. és 7.5. tételek)
9. Egyszerű algebrai testbővítések (7.6. – 7.8. tételek)

Megjegyzés. Mindenki húz egy-egy mesélős, illetve bizonyítás tételt. A két tétel különböző sorozatból kerül ki.