Diszkrét matematika II. tételsor a szóbeli vizsgához (2019 ősz)

1. **Számelmélet 1.** *Az oszthatóság alapfogalmai, maradékos osztás, Euklideszi és Bővített euklideszi algoritmus*

   Definíciók: oszthatóság az egész számok körében; egységek fogalma; asszociáltak; triviális osztók; felbonthatatlan (irreducibilis) számok és prímszámok; osztási maradék fogalma és jelölése; legnagyobb közös osztó és legkisebb közös többszörös és kapcsolódó jelölések; relatív prímek fogalma; legnagyobb közös osztó általános definíciója (tetszőleges számú egészre)

   Példák: példák asszociáltakra; példa olyan számhalmazra (gyűrűre), amelyben nem minden felbonthatatlan prím

   Állítások bizonyítással:

   Állítás, mely kimondja, hogy (az egészek körében) minden prím felbonthatatlan. (9. dia); Maradékos osztás tétele az egész számok körében (11. dia); Számok különböző számrendszerekben történő felírásáról szóló tétel (14. dia); Maradékos osztás tétele az egész számok körében (11. dia); Tétel az Euklideszi algoritmusról (az egészek körében) (18. dia); Tétel a legnagyobb közös osztó kiszámításáról rekurzióval (21. oldal); A Bővített euklideszi algoritmusról szóló tétel (23. dia)

   Állítások bizonyítás nélkül:

   Oszthatóság alaptulajdonságai (10 tulajdonság, 6. dia); Állítás az egységekről az egészek körében (7. dia); Asszociáltak ekvivalens jellemzése (8. dia)

2. **Számelmélet 2.** *Kétváltozós lineáris diofantikus egyenletek, Számelmélet alaptétele*

   Definíciók: kanonikus alak; kétváltozós lineáris diofantikus egyenlet; $\tau(n)$ jelölés

   Állítások bizonyítással:

   A kétváltozós lineáris diofantikus egyenletek megoldhatóságáról (és egy megoldásáról) szóló tétel (26. dia); Kétváltozós lineáris diofantikus egyenlet összes megoldásáról szóló tétel (27. dia); Tétel, amely kimondja, hogy az egészek körében minden felbonthatatlan szám prím (29. dia); A Számelmélet alaptétele (30. dia); Tétel (pozitív) oszók számának meghatározásáról a kanonikus alak alapján (32. dia)

   Állítások bizonyítás nélkül:

   Legnagyobb közös osztó és legkisebb közös többszörös kiszámítása a kanonikus alakból (31. dia)

3. **Számelmélet 3.** *Kongruenciák, RSA és prímek*

   Definíciók: modulo m kongruencia relációk és jelölésük; modulo m maradékosztályok; lineáris kongruencia-rendszer; teljes és redukált maradékrendszerek; Euler-féle φ függvény; RSA-eljárás ismertetése; Eratoszthenész szitája

   Állítások bizonyítással:

   Kongruenciák néhány alaptulajdonsága (6 db. tulajdonság, 34. dia); Kongruencia osztásáról szóló tétel (37. dia); Lineáris kongruenciák megoldásáról szóló tétel (39. dia); Kínai maradéktétel (46. dia)

   Állítások bizonyítás nélkül:

   Tétel $\varphi(m)$ kiszámításáról m kanonikus alakjából (51. dia); Euler-Fermat tétel (52. dia); Fermat tétel (52. dia); Teljes, illetve redukált maradékrendszer lineáris transzformációiról szóló lemma (53. dia); Euklidesz tétele a prímek számáról (56. oldal); Dirichlet tétele (56. dia); Prímszámtétel (57. dia);

4. **Algebra** *Egy, illetve két binér műveletes algebrai struktúrák definíciói és kapcsolódó alapfogalmak*

   Definíciók: r-változós, binér, illetve unér művelet; algebrai struktúra; grupoid; binér művelet asszociatívitása, kommutativitása; semleges elem (adott binér műveletre nézve); elem inverze (adott binér műveletre nézve); félcsoport; monoid; csoport; Abel-csoport; disztributivitás; gyűrű; nullelem/egységelem gyűrűben; egységelemes gyűrű; kommutatív gyűrű; nullosztómentes gyűrű; integritási tartomány; gyűrű elemének additív rendje; karakterisztika; osztó/többszörös fogalma kommutatív gyűrűben; egység fogalma; ferdetest; test; maradékosztályok összeadása és szorzása; $\mathbb{Z}_m$

   Példák: példák nem kommutatív binér műveletre, gyűrűkre, nullosztómentes és nem nullosztómentes gyűrűre; véges és végtelen testekre; Írjuk fel a $\mathbb{Z}_m$-beli maradékosztályok összeadásának, illetve szorzásának műveleti tábláját valamely m egészre. Milyen algebrai struktúrát alkotnak a következők: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, ahol $+$, ill. $\cdot$ a szokásos összeadás, ill. szorzás?

   Állítások bizonyítás nélkül:

   Állítás a nullelemmel való szorzásról gyűrűben (8. dia); Állítás, amely kimondja, milyen algebrai struktúra $\mathbb{Z}_m$, illetve $\mathbb{Z}_p$, a maradékosztályok összeadásával és szorzásával teszőleges m egész, illetve p prím esetén (15. dia); Állítás nemnulla elemek additív rendjéről nullosztómentes gyűrűben (16. dia)

5. **Polinomok 1.** *Polinomok alapfogalmai*

   Definíciók: polinom; polinomok összeadása és szorzása; polinom főtagja, konstans tagja, együtthatói, főegyütthatója; polinom foka és jelölése; konstans polinom; nullpolinom; konstans polinom; főpolinom; monom; adott R gyűrű feletti polinomgyűrű fogalma és jelölése; polinom adott helyen felvett helyettesítési értéke; polinom gyöke; polinomfüggvény; Horner-elrendezés ismertetése

   Példák: Adjunk példát, amikor különböző polinomokhoz ugyanaz a polinomfüggvény tartozik.

   Állítások bizonyítással:

   Állítás kommutatív gyűrű feletti polinomgyűrű kommutativitásáról (20. dia); Állítás egységelemes gyűrű feletti polinomgyűrű egységeleméről (21. dia); Állítás nullosztómentes gyűrű feletti polinomgyűrű nullosztómentességéről (21. dia); Állítás polinomok összegének és szorzatának fokáról (22. dia)

6. **Polinomok 2.** *Polinomok maradékos osztása és következményei*

   Definíciók: gyöktényező; oszthatóság polinomok körében; polinomok legnagyobb közös osztója

   Állítások bizonyítással:

   Polinomok maradékos osztásáról szóló tétel (egységelemes integritási tartomány felett) (28. dia); Gyöktényező leválasztásáról szóló állítás (egységelemes integritási tartomány feletti polinomok esetén) (Következmény, 31. dia); Egységelemes integritási tartomány feletti polinom gyökeinek számáról szóló állítás (Következmény, 32. dia); Állítás (n + 1) helyen megegyező legfeljebb n-ed fokú polinomokról egységelemes integritási tartomány felett (Következmény, 33. dia); Állítás polinomok és polinomfüggvények kapcsolatáról végtelen egységelemes integritási tartomány felett (Következmény, 33. dia); Bővített euklideszi algoritmusról szóló tétel test feletti polinomgyűrűben (35. dia);

7. **Polinomok 3.** *Az algebrai derivált és tulajdonságai, polinom gyökének multiplicitása és kapcsolat az algebrai deriválttal, Lagrange-interpoláció, titokmegosztás*

   Definíciók: polinom algebrai deriváltja; többszörös gyök, gyök multiplicitása; Lagrange-interpolációs alappolinom; ismertessük, hogyan használható a Lagrange-interpoláció titokmegosztásra

   Példák: Adjunk példát olyan polinomra, amelynek van olyan n-szeres gyöke, ami a deriváltjának is n-szeres gyöke.

   Állítások bizonyítással:

   Tétel polinom gyökeinek multiplicitása és az algebrai derivált kapcsolatáról (40. dia); Lagrange-interpolációról szóló tétel (42. dia)

   Állítások bizonyítás nélkül:

   Az algebrai derivált tulajdonságai (4 tulajdonság, 38. dia); Az $(x - c)^n$ alakú polinomoknak (azaz elsőfok főpolinomok n-edik hatványának) az algebrai deriváltjáról szóló állítás (39. dia)

8. **Polinomok 4.** *Polinomok felbonthatósága általános testek, illetve $\mathbb{C}$ és $\mathbb{R}$ felett*

   Definíciók: felbonthatatlan (irreducibilis) és felbontható (reducibilis) polinomok egységelemes integritási tartomány felett

   Példák: példa olyan elsőfokú polinomra valamely R gyűrű felett (nem test, tehát nem $\mathbb{C}$ vagy $\mathbb{R}$ felett), amelynek nincs gyöke

   Állítások bizonyítással:

   Állítás az egységekről test feletti polinomgyűrűben (47. dia); Állítás, amely kimondja, hogy test feletti polinomgyűrűben minden elsőfokú polinomnak van gyöke (48. dia); Állítás elsőfokú polinomok felbonthatatlanságáról test feletti polinomgyűrűben (49. dia); Állítás másod- és harmadfokú polinomok felbonthatatlanságáról test feletti polinomgyűrűben (50. dia); Tétel a $\mathbb{C}$ feletti felbonthatatlan polinomokról (51. dia); Tétel az $\mathbb{R}$ feletti felbonthatatlan polinomokról (51. dia)

9. **Polinomok 5.** *Polinomok felbonthatósága $\mathbb{Q}$, illetve $\mathbb{Z}$ felett*

   Definíciók: felbonthatatlan (irreducibilis) és felbontható (reducibilis) polinomok egységelemes integritási tartomány felett; primitív polinom

   Példák: példa primitív polinomra; példa $\mathbb{Z}$, illetve $\mathbb{Q}$ feletti polinom felírására primitív polinom segítségével (a tanult tételnek megfelelően)

   Állítások bizonyítással:

   Gauss-lemma (54. dia); Állítás $\mathbb{Q}$ feletti polinom felírásáról primitív polinom segítségével (56. dia); Gauss tétele (57. dia); Állítás, amely kimondja, hogy egy primitív polinom pontosan akkor felbontható $\mathbb{Z}$ felett, ha felbontható $\mathbb{Q}$ felett (Következmény, 58. dia)

   Állítások bizonyítás nélkül:

   Állítás $\mathbb{Z}$ feletti polinom felírásáról primitív polinom segítségével (55. dia); Schönemann-Eisenstein-kritérium (59. dia); Racionális gyöktesztről szóló tétel (61. dia)

10. **Kódolás**

    Definíciók: a kommunikáció vázlatos ábrája; információ; információforrás által kibocsátott üzenetek gyakorisága, relatív gyakorisága; üzenetek eloszlása; üzenet egyedi információtartalma; információ egysége; információforrás által kibocsátott üzenetek átlagos információtartalma; forrás entrópiája; eloszlás, eloszlás entrópiája; konvex és szigrorúan konvex függvény; kódolás; felbontható (egyértelműen dekódolható/veszteségmentes) kódolás; veszteséges kódolás; kódolandó ábécé; kódábécé; A^+ és A^* halmazok; üres szó és jelölése; betűnkénti kódolás, kódszavak; szó prefixe, infixe és szuffixe, triviális prefixe, triviális infixe és triviális szuffixe, valódi infixe és valódi szuffixe; prefixmentes halmaz; prefix kód; egyenletes kód; vesszős kód;

    Példák: példa prefix, illetve nem prefix kódra; példa egyenletes kódra; példa vesszős kódra; példa nem prefix, de felbontható kódra;

    Állítások bizonyítással: Tétel eloszlás entrópiájára vonatkozó felső korlátról (5. dia)

    Állítások bizonyítás nélkül:

    Jensen-egyenlőtlenség (4. dia); Állítások a prefix, egyenletes, vesszős és felbontható kódok közötti kapcsolatról (10. és 11. diák); McMillan egyenlőtlenség és megfordítása (13. dia)