Óramenet - Algebra és Számelmélet

1. hét, szeptember 13-14, számelmélet: Peano-féle axiómarendszer, teljes indukció. Oszthatóság. Számelmélet alaptétele. Eukleidész I. tétele. Eratoszthenészi szita. Eukleidész II. tétele (végtelen sok prím létezik). Prímszámtétel (bizonyítás nélkül). Fermat számok, Fermat prímek, Mersenne prímek. Eukleidesz II. tételének második bizonyítása. Prímképletek. Goldbach sejtés, Eukleidész, maradékos osztás lemma. *Irodalom:* Elemi Számelmélet jegyzet 1-27, 33-44. oldal.

2. hét, szeptember 20-21, algebra: Mátrixok, Gauss-elimináció. Inverz számítás Gauss eliminációval. Polinomok. Szumma és produktum jelölés. *Irodalom:* Kiss Emil 1., 2. és 3. diái, Kiegészítő anyagok: Mátrixok, Gauss elimináció, példa, Mátrix inverzszámítás Gauss eliminációval.

3. hét, szeptember 27-28, számelmélet: Egységek. Legnagyobb közös osztó, kitüntetett közös osztó, a kettő $\mathbb{Z}$-ben azonos. Eukleideszi algoritmus. Prímek, felbonthatatlanok, a kettő $\mathbb{Z}$-ben azonos. Racionális gyökteszt. Polinomok maradékos osztása. Kongruenciák (alapok). Kongruenciák osztása egész számmal. Teljes maradékrendszer (TMR), redukált maradékrendszer (RMR). Ezek bizonyos speciális transzformáltjai is TMR-t, illetve RMR-t alkotnak. φ függvény definíciója és képlete. Euler-Fermat tétel (bizonyítás két hét múlva). *Irodalom:* Elemi Számelmélet jegyzet: 44-75 oldal.

4. hét, október 4-5, algebra: A Horner elrendezés, és szerepe a gyöktényező kiemelésénél, iterált Horner. Gyöktényezők kiemelhetősége, gyökök száma, gyöktényezős alak. Komplex számok. Konjugált, abszolútérték. Algebrai és trigonometrikus alak. Szorzásnál a szögek összeadódnak, a hosszak összeszorzódnak. Szorzás és forgatva nyújtás. Komplex számok hatványozása. Gyökvonás komplex számból. A 2×2-es determináns definíciója. Tulajdonságaik. Egy oszlophoz egy másik oszlop skalárszorosát adva a determináns értéke nem változik; a determináns oszlopcserénél előjelet vált. A transzponált mátrix determinánsa. Következmény: az oszlopokra teljesülő tulajdonságok a sorokra is érvényesek. Felső háromszögmátrix determinánsa. *Irodalom:* Kiss Emil, 4., 5., 6., 7. diái és 14. dia első kilenc oldala.

5. hét, október 11-12, számelmélet: Euler-Fermat, kis-Fermat tétel (a 6.15 Tétel kimarad). Moduláris hatványozás. Lineáris kongruencia megoldhatósága. Lineáris kongruencia megoldása φ-vel és eukleideszi algoritmussal. Pár példa diofantikus egyenletekre. Kongruenciamódszerrel $3x^2 - y^2 = 2023$

nem oldható meg (tekintsük mod 3). Lineáris diofantikus egyenletek. $\sqrt{2}$ és e irracionalitásának bizonyítása, π irracionalitása (bizonyítás nélkül). *Irodalom:* Elemi Számelmélet jegyzet: 75-77, 80-96 oldal.

6. hét, október 18-19, algebra: 3x3-as determinánsok. Permutáció, transzpozíció, inverzió. Permutációk előjele. Determináns általános definíciója, alaptulajdonságai, Gauss elimináció. Előjeles aldeterminány. Kifejtési tétel, Ferde kifejtési tétel. Inverz (pl. az adjungált mátrixszal megadott alak). Cramer-szabály. Vandermonde determináns. *Irodalom:* Kiss Emil 14., 15. 16. diái és 17. dia első tizenegy oldala.

7. hét, október 25, algebra: Befejeztük a múlt hétről maradt 17. diát.

7. hét, október 25-26, számelmélet: Pitagoraszi számhármasok. Nagy Fermat-tétel. Kínai Maradéktétel. Összetett modulusú kongruencia visszavezetése prímhatvány modulusúra. Prímhatvány modulusú kongruenciák megoldása. Fokszám redukció. Fokszám tétel (bizonyítás csak az őszi szünet után). *Irodalom:* Elemi Számelmélet jegyzet 101-107 és 109-121 oldal.

8. hét, november 8-9, algebra: Lineáris algebra: Lineáris kombináció, oszlopvektorok függetlensége, jellemzése lineáris egyenletrendszer megoldhatóságával. A függetlenség és a függés kapcsolata. Vektorrendszer és mátrix rangja, sorrang=oszloprang=determinánsrang. A rang meghatározása Gauss-eliminációval. Lineáris egyenletrendszer megoldhatóságának, és a megoldás egyértelműségének jellemzése a rang segítségével. A determináns eltűnésének jellemzése. Absztrakt algebra: Művelet, asszociativitás, kommutativitás. Nullelem, egységelem, ellentett, inverz. Csoport, gyűrű, nullosztómentesség. Additív és multiplikatív csoport. Egységelemes, kommutatív, szokásos gyűrű, test. Az egyszerűsítési szabály, szorzat inverze. Polinomgyűrűk. *Irodalom:* Kiss Emil 18., 19. és 20. dia (első 9 oldala). Az oszloprang=sorrang=determinánsrang tétel esetében elég a „Kiegészítő anyagok az Algebrához" link alatt szereplő bizonyítást tudni.

9. hét, november 15-16, számelmélet: Fokszám tétel bizonyítása. Wilson tétel (csak az I. bizonyítás volt). Számelméleti függvények. Nevezetes függvények ($d(n)$, $\sigma(n)$, $\omega(n)$, $\Omega(n)$, $\varphi(n)$), ezek multiplikativitása, explicit képlete. Multiplikatív függvény összegzési függvénye is multiplikatív. Möbiüs féle megfordítási formula (bizonyítás nélkül). Tökéletes számok, barátságos számok, hiányos és bővelkedő számok (a bizonyítások nem szerepeltek). Rend. Rend alaptulajdonságai. *Irodalom:* Elemi Számelmélet jegyzet, 120-125, 132-160 oldal.

10. hét, november 22-23, algebra: Polinomok azonossági tétele, fokszámtétel polinomokra, többszörös gyök és derivált kapcsolata. Gyökök és együtthatók közötti összefüggés. Többváltozós polinomok. Elemi szimmetrikus polinomok. Szimmetrikus polinomok alaptétele. Eukleideszi gyűrű. Euklideszi algoritmus, minden euklideszi gyűrű alaptételes. Interpoláció és a kínai maradéktétel. *Irodalom:* Kiss Emil 20., 21. és 22. dia (első 14 oldala).

11. hét, november 29-30, számelmélet: Primitív gyök, diszkrét logaritmus (index). Binom kongruencia megoldhatósága. Diffie-Hellman kulcscsere, DHP és DLP. Másodfokú kongruenciák. Kvadratikus maradékok és nem-maradékok. Legendre szimbólum. Alaptulajdonságok és Gausss kvadratikus reciprocitási tétele. *Irodalom:* Elemi Számelmélet jegyzet: 161-185 oldal.

12. hét: december 6-7, algebra: Lagrange és Newton interpoláció. Oszthatóság polinomgyűrűkben. Első, másod és harmadfokú polinomok irreducibilitása. Páratlan fokú, valós együtthatós polinomnak van valós gyöke. Ha egy valós együtthatós polinomnak c gyöke, akkor $\overline{c}$ is, sőt ugyanannyiszoros gyökök. $\mathbb{R}[x]$, $\mathbb{C}[x]$ és $\mathbb{Z}[x]$ irreducibilis polinomjai. Schönemann-Eisenstein féle irreducibiltási kritérium. Primitív polinom. $\mathbb{Z}[x]$ alaptételes gyűrű. Ha $\mathbb{R}$ alaptételes gyűrű, akkor $\mathbb{R}[x]$ is. Komplex számok rendje. Csoportokban csoport elem rend. Jó kitevő és rend kapcsolata. Permutációk rendje. Primitív n-edik egységgyök. Körosztási polinom. $\prod_{d|n} \Phi_d(x) = x^n - 1$. *Irodalom:* Kiss Emil 22., 23., 24. 25. és 26. dia (első 6 oldala).

13. hét: december 13, algebra: Körosztási polinomok. Harmadfokú egyenlet megoldása. Cardano képlete. Casus irreducibilis. Ötödfokú egyenletre nincs általános gyökképlet. *Irodalom:* Kiss Emil 26. dia.

13. hét: december 13-14, számelmélet: Jacobi szimbólum alaptulajdonságai és alkalmazása Legendre szimbólum kiszámítására. Titkosítások. Mono-alfebetikus rejtjel. Vernam-féle titkosító eljárás. Pszeudovéletlen sorozatok. RSA. $\pi(x)$-re becslések. Csebisev tétele. Primszámtétel. Li (x). Csebisev tételének bizonyítása. $\prod_{p \leq x} < 4^x$, Néhény tétel bizonyítás nélkül: Csebisev: n és $2n$ közé mindig esik prím. Dirichlet tétel. A prímek tartalmaznak tetszőlegesen hosszú számtani sorozatot. $d_n = p_{n+1} - p_n$ végtelen sokszor kisebb egyenlő mint 246. *Irodalom:* Elemi Számelmélet jegyzet: 190-192, 197-222.