

**Az I. éves műszaki informatika szakos hallgatók
Bevezetés a számításelméletbe c. tárgyának vizsgatételei
(2003/2004-es tanév)**

II. félév

1. Euler-körök és -utak, Euler tétele. Hamilton-körök és -utak. Hamilton-kör létezésének tanult szükséges feltétele, annak bizonyítása, hogy e feltétel nem elégséges.
2. Elégséges feltételek Hamilton-kör létezésére: Dirac, Ore, Pósa és Chvátal tétele, e tételek egymáshoz való viszonya.
3. Gallai-azonosságok. Páros gráfok fogalma, karakterizációja.
4. Párosítás és teljes párosítás fogalma, Hall-tétel, Frobenius-tétel, König-tétel.
5. Kromatikus szám fogalma és becslései a klikkszám, illetve, a maximális fokszám függvényében. Brooks tétele (biz. nélkül), Mycielski konstrukciója.
6. Élgráfok és színezésük, Vizing-tétel (biz. nélkül), síkgráfok színezése, ötszinttétel.
7. Perfekt gráfok, perfektség bizonyítása nevezetes speciális esetekben (páros gráfok, ezek komplementere, páros gráfok élgráfja, ezek komplementere, összehasonlítási gráfok).
8. Perfekt Gráf Tétel, Lovász erősebb tétele, Erős Perfekt Gráf Sejtés.
9. Mantel és Turán tétele.
10. Hálózati folyamatok, Ford-Fulkerson tétel, maximális folyam keresése algoritmikusan, Edmonds-Karp tétel (biz. nélkül).
11. Menger-tételek, magasabb összefüggőség. PERT-módszer. Gráfok tárolása.
12. Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, prímek, a számelmélet alaptétele, osztók száma, euklideszi algoritmus, nevezetes tételek prímszámokról.
13. Kongruencia fogalma, teljes és redukált maradékrendszer, φ -függvény, tulajdonságai, Euler-Fermat tétel.
14. Lineáris kongruencia megoldása, Wilson-tétel.
15. Csoport fogalma, ciklikus csoport, diédercsoport, szimmetrikus csoport, Cayley-tétel.
16. Részcsoportok, mellékosztályok, Lagrange tétele, elem rendjének viszonya a csoport rendjével.
17. Normálosztók, jellemzéseik, faktorcsoport, homomorfizmus-tétel.
18. Gyűrűk, testek, nevezetes példák, véges integritási tartomány test voltának bizonyítása, kvaterniók ferdeteste.
19. Aritmetikai algoritmusok bonyolultsága, prímtesztelés.
20. Nyilvános kulcsú titkosítások, bizonyítás információközlés nélkül.