

**A műszaki informatika szakos hallgatók  
Bevezetés a Számításelméletbe II. tárgyának vizsgatételei  
(2005/2006. tanév első félév — kerestfélév)**

1. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.
2. Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele.
3. Gráfok színezése.  $\chi(G)$  fogalma és viszonya  $\omega(G)$ -hez, illetve  $\Delta(G)$ -hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója.
4. Síkbarajzolható gráfok kromatikus száma, ötszintétel. Élchromatikus szám:  $\chi_e(G)$  viszonya  $\Delta(G)$ -hez, Vizing-tétel (biz. nélkül).
5. Perfekt gráfok: erős perfekt gráf tétel (a szükségesség bizonyításával), Lovász tétele (ez miatt következik az erős perfekt gráf tételből). Intervallumgráfok perfektsége.
6. Páros gráfok. Párosítások páros gráfban, König tétele, Hall tétele, Frobenius tétele. Magyar módszer.
7. Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei.
8. Hálózati folyamok. Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül). Egészértékűségi lemma. A folyamprobléma általánosításai.
9. Menger tételei. Többszörös összefüggőség, élösszefüggőség. Dirac tétele (biz. nélkül).
10. Aciklikus irányított gráfok, PERT módszer.
11. Gráfok és mátrixok. Szomszédossági mátrix (hatványainak jelentése, reguláris gráf esetén egy sajátértéke). Illeszkedési mátrix, annak rangja (csak a „kisebb vagy egyenlő” bizonyításával).
12. Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma és összege. Nevezetes tételek prímszámokról: prímek száma, hézag a szomszédos prímek között, nagy prímszámtétel (biz. nélkül), Dirichlet tétele (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.
13. Euklideszi algoritmus. Lineáris kongruenciák megoldása (konkrét példán, illetve az euklideszi algoritmussal is), a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).
14. Euler féle  $\varphi$ -függvény, redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Wilson tétele.
15. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo  $m$ . Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.
16. Művelet fogalma, félcsoport, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsportja, diédercsoport.
17. Részcsoport. Csoportok izomorfiája. Szimmetrikus csoport, Cayley tétele (biz. nélkül).
18. Elem rendje, ciklikus csoport. Mellékosztály, Lagrange tétele, elemrend és csoport rendjének kapcsolata.
19. Gyűrű és test fogalma, példák ( $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $n \times n$ -es mátrixok, polinomok, kvaterniók,  $\mathbb{Q}(\sqrt{2})$ ,  $p$  elemű test).