

**A mérnök–informatikus szakos hallgatók  
Bevezetés a Számításelméletbe II. tárgyának vizsgatételei  
(2009/2010. tanév, első félév)**

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. Élőkromatikus szám:  $\chi_e(G)$  viszonya  $\Delta(G)$ -hez, Vizing-tétel (biz. nélkül).
5. Perfekt gráfok: erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. 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. Gráfok és mátrixok. Szomszédossági mátrix (hatványainak jelentése, reguláris gráf esetén egy sajátértéke). Illeszkedési mátrix, annak rangja.
11. 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,  $\pi(n)$  nagyságrendje (biz. nélkül), prímek számtani sorozatokban (Dirichlet tétele) (biz. nélkül).
12. Kongruencia fogalma, alpműveletek kongruenciákkal. Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Wilson tétele.
13. Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is). 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.
15. Számelmélet és algoritmusok: alpműveletek, hatványozás az egészek körében és modulo  $m$ . Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.
16. Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport, szimmetrikus csoport.
17. Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Csoportok izomorfiaja, Cayley tétele (biz. nélkül).
18. Mellékosztály, Lagrange tétele, elemrend és csoport rendjének kapcsolata.
19. Gyűrű és test fogalma. Nullosztómentes gyűrű, test nullosztómentessége. Példák:  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $n \times n$ -es mátrixok, polinomok,  $\mathbb{Z}_n$  (ez milyen  $n$ -re test), kvaterniók .