Az I. éves műszaki informatika szakos hallgatók
Bevezetés a számításelméletbe II. c. tárgyának vizsgatételei
(2005/2006-os tanév II. félév)

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 és Ore tétele.

3. Hálózati folyamok, Ford-Fulkerson tétel, maximális folyam keresése algoritmikusan, Edmonds-Karp tétel (biz. nélkül).

4. Menger-tételek, magasabb összefüggőség. Dirac-tétel (k-szorosan összefüggő gráfok k ponton áthaladó köreiről; biz. csak a $k = 2$ esetben).

5. Párosítás és teljes párosítás fogalma, páros gráfok fogalma, karakterizációja. $\nu(G)$ és $\tau(G)$ viszonya általában, Kőnig-tétel.

6. Hall-tétel, Frobenius-tétel, Tutte tétele (biz. csak a könnyű irányban).

7. Gallai tételei.

8. Kromatikus szám fogalma és becslései a klikkszám, illetve a maximális fokszám függvényében. Brooks tétele (biz. nélkül), Mycielski konstrukciója.

9. Élgráfok és színezésük, Vizing-tétel (biz. nélkül), síkgráfok színezése, ötszíntétel.

10. Perfekt gráfok, perfektség bizonyítása nevezetes speciális esetekben (páros gráfok, ezek komplementere, páros gráfok élgráfja, ezek komplementere, intervallumgráfok). Perfekt gráf tétel (biz. nélkül), erős perfekt gráf tétel (biz. nélkül).

11. Mantel és Turán tétele.

12. Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, prímszámok és felbonthatatlan számok, a számelmélet alaptétele, osztók száma, osztók összege, euklideszi algoritmus, prímszámok számának végtelensége, egyéb nevezetes tételek prímszámokról (Csebisev-tétel, Dirichlet-tétel, prímszámtétel; ezek biz. nélkül).

13. Kongruencia fogalma, teljes és redukált maradékrendszer, $\varphi-$függvény, tulajdonságai, Euler-Fermat tétel.

14. Lineáris kongruencia megoldhatósága és 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. Gyűrűk, testek, nevezetes példák, $\mathbb{Z}$ részgyűrűinek jellemzése, véges integritási tartomány test voltának bizonyítása.

18. Aritmetikai algoritmusok bonyolultsága (alapműveletek, hatványozás, mod m hatványozás, euklideszi algoritmus), nyilvános kulcsú titkosírás.