

A mérnök–informatikus szakos hallgatók
Bevezetés a Számításelméletbe II. tárgyának vizsgatételei
(2013/2014. tanév, első félév)

1. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele. Euler-körséták és -séták, ezek létezésének szükséges és elégséges feltétele.
2. Gráfok színezése. $\chi(G)$ fogalma és viszonya $\omega(G)$ -hez, illetve $\Delta(G)$ -hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója.
3. Síkbarajzolható gráfok kromatikus száma, ötszintétel. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$ -hez, Vizing-tétel (biz. nélkül), páros gráfok élkromatikus száma.
4. Perfekt gráfok: erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. az erős perfekt gráf tételből). Intervallumgráfok perfektsége.
5. Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Kőnig, Hall és Frobenius tételei.
6. Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei.
7. Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus a maximális folyam és a minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.
8. Menger pontpárok közötti diszjunkt utakra vonatkozó tételei. Többszörös összefüggőség és éösszefüggőség fogalma, Menger ezekre vonatkozó tételei.
9. Gráfok szomszédossági mátrixa, a szomszédossági mátrix hatványainak jelentése. Irányított gráf illeszkedési mátrixa.
10. Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma. Prímek száma, hézag a szomszédos prímek között, $\pi(n)$ nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.
11. Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, ennek alkalmazása lineáris kongruenciák megoldására is. Wilson tétele.
12. Euler-féle φ -függvény, redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).
13. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m . Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.
14. Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.
15. Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Szimmetrikus csoport. Csoportok izomorfája.
16. Mellékosztály fogalma, példák. Lagrange tétele, elemrend és csoport rendjének kapcsolata.
17. Gyűrű, ferdetest 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, $\mathbb{Q}(\sqrt{2})$.