A mérnök–informatikus szakos hallgatók
Bevezetés a Számításelméletbe II. tárgyának vizsgatételei
(2014/2015. tanév, első félév)

1. Szélességi keresés, használata az összefüggőség eldöntésére. Euler-séta és -körséta, létezésésük szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.

2. Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Hall és Frobenius tételei.

3. Kőnig tétele. Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei.

4. Gráfok színezése. $\chi(G)$ fogalma és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez, mohó színezés. Mycielski konstrukciója.

5. Síkbarajzolható gráfok kromatikus száma, ötszíntétel. Algoritmus intervallumgráfok optimális színezésére. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$-hez, Vizing-tétel (biz. nélkül).

6. Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus maximális folyam és minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.

7. Menger pontpárok közötti diszjunkt utakra vonatkozó tételei. Többszörös összefüggőség és élösszefüggőség fogalma, Menger vonatkozó tételei.

8. Oszthatóság, prímszámok, a számelmélet alaptétele (biz. nélkül). Osztók számának meghatározása. Prímek száma, $\pi(n)$ nagyságrendje (biz. nélkül), hézag lehetséges nagysága egymást követő prímek között. Euklideszi algoritmus. Kongruencia fogalma, alapműveletek kongruenciákkal.

9. Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus alkalmazása lineáris kongruenciák megoldására.

10. Teljes és redukált maradékrendszer fogalma, Euler-féle φ-függvény, kiszámítása (bizonyítás csak prímhatványokra). Euler-Fermat-tétel, kis Fermat-tétel.

11. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosírás és digitális aláírás, RSA-kód.

12. Kétváltozós művelet fogalma, félcsoport, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.

13. Elem rendje, részcsoport, ciklikus csoport, példák. Mellékosztály fogalma, példák, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele (biz. nélkül).

14. Gyűrű, ferdetest és test fogalma. Nullosztó fogalma, ferdetest nullosztómentessége. Példák véges és végtelen ferdetestre, illetve véges és végtelen gyűrűre, ami nem ferdetest.