Bevezetés a Számításelméletbe II. vizsgatételek
(2010/2011. első félév)

1. Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör és -út létezésére. Elégséges feltételek: Dirac és Ore tétele.

2. Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, alternáló út és javítóút fogalma, Hall és Frobenius tételei.

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

4. Gráfok színezése, kromatikus szám. A kromatikus szám becslései a klikkszám és a maximális fokszám segítségével. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

5. Síkbarajzolható gráfok kromatikus száma. Élkromatikus szám, viszonya a maximális fokszámhoz, Vizing-tétel (biz. nélkül). Perfekt gráfok. Páros gráfok és intervallumgráfok perfektsége, perfekt gráf tétel (biz. nélkül), erős perfekt gráf tétel (biz. nélkül).

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

7. Menger tételei. Többszörös összefüggőség és élösszefüggőség, Dirac tétele (biz. nélkül).

8. Oszthatóság, prímek, prímek száma, hézag mérete szomszédos prímek között, a számelmélet alaptétele (biz. nélkül). Legnagyobb közös osztó, legkisebb közös többszörös, osztók száma. Euklideszi algoritmus.

9. Kongruencia fogalma, alapműveletek kongruenciákkal. Lineáris kongruenciák megoldása euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma.

10. Teljes és redukált maradékrendszer fogalma, φ-függvény, kiszámítása. Euler-Fermat tétel, kis Fermat-tétel.

11. Művelet fogalma, félcsoport, csoport, Abel-csoport. Csoportok számokon, mátrixokon, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.

12. Elem rendje, részcsoport, egy elem generált részcsoport, ciklikus csoport. Mellékosztályok, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele (biz. nélkül).

13. Gyűrű, ferdetest és test fogalma. Példa véges és végtelen testre, illetve véges és végtelen gyűrűre, ami nem ferdetest. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben.

14. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosírás és digitális aláírás fogalma, megvalósításuk az RSA-kód segítségével.

Kiegészítések a tételsorhoz
Bevezetés a Számításelméletbe II.
(2010/2011. első félév)

Bizonyos tételeknél esetleg nem teljesen nyilvánvaló, hogy pontosan mit is kell tudni a hallgatóknak, ennek tisztázására szolgál ez a kiegészítés, melyet **a vizsgán nem lehet használni**. Érdemes még tanulmányozni a `www.cs.bme.hu/bsz2` oldalról letölthető „Tanácsok vizsgára" című dokumentumot is.

4. tétel: *Mycielski konstrukciója.*
Nem csak azt kell tudni (még az elégségesért is), hogy mire való a konstrukció, hanem azt is, hogy hogyan készül. Ez utóbbi tehát nem a bizonyítás része.

5. tétel: *perfekt gráf tétel (biz. nélkül), erős perfekt gráf tétel (biz. nélkül)*
A perfekt gráf tétel a Lovász-tétel, azaz hogy egy gráf akkor és csak akkor perfekt, ha a komplementere perfekt. Az erős perfekt gráf tétel pedig karakterizálja a perfekt gráfokat: egy gráf akkor és csak akkor perfekt, ha sem ő, sem a komplementere nem tartalmaz feszített részgráfként legalább 5 hosszú páratlan kört.

6. tétel: *Hálózat, hálózati folyam és (s,t)-vágás fogalma, folyam értéke, (s,t)-vágás kapacitása.*
E fogalmakat tudni kell precízen definiálni, nem elég a „vízhálózatos" modell ismertetése. (Vagyis pl.: a folyam egy olyan függvény, amely az élekhez valós számokat rendel és teljesül rá ...) Tudni kell ezen kívül természetesen a maximális folyam keresésére tanult algoritmust is (az elégségesért is).

7. tétel: *Menger tételei.*
Minden tételre igaz, hogy a megtanulása/kimondása előtt a vonatkozó definíciókat kell pontosan érteni; ez a Menger-tételeknél szokott a leggyakrabban elmaradni.

8. tétel: *a számelmélet alaptétele (biz. nélkül)*
Minden egynél nagyobb abszolút értékű egész előáll prímek szorzataként, a szorzat a tényezők sorrendjétől és esetleges (-1)-es szorzóktól eltekintve egyértelmű.

9. tétel: *Lineáris kongruenciák megoldása euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma.*
Elképzelhető, hogy a vizsgáztató egy általa adott konkrét példán is kéri az euklideszi algoritmus e célra való alkalmazását.

14. tétel: *Nyilvános kulcsú titkosírás és digitális aláírás fogalma, megvalósításuk az RSA-kód segítségével.*
Az előadáson tanult, számelméleti ismeretekre támaszkodó (és a netről letölthető jegyzetben, illetve a Katona-Recski-Szabó könyvben is szereplő) megvalósítás az RSA-kód, amit természetesen tudni kell.