Letölthető: http://compalg.inf.elte.hu/~ajarai

BEVEZETÉS A MATEMATIKÁBA II

Programtervező informatikus A,B szak, 1. év 2. félév

2006–2007. év 2. félév
Vizsga

Előfeltételek: Legalább elégséges gyakorlati jegy, az indexbe beírva, index, utóvizsgánál befizetett utóvizsgadíj az indexben regisztrálva, jelentkezés az adott napra.

Jelentkezés: Az ETR rendszeren keresztül, legkésőbb a vizsga előtt 36 órával. Aki bejelentkezik, nem mondja le az időpontot, de nem jelenik meg, elveszít egy vizsgaalkalmat. Utóvizsgázni akármelyik vizsganapon lehet.

Konzultáció: Kérésre a vizsgák előtt (ajarai@moon.inf.elte.hu, legalább 2 munkanappal az időpont előtt), D2-211.

A vizsga anyaga: Ami az előadáson elhangzott, de beleértve az ott nem részletezett (például „nyilvánvaló”, „hasonlóan belátható”, stb.) részeket is.

A vizsga lefolyása: Írásbeli „beugró”, 60 perc alatt 15 kérdésre kell válaszolni. Minden kérdés 1–1 pont (definíciók, tételek, egyszerű példák és ellenpéldák, stb.). A feladatokat írásban kapják meg. Legalább 5 pontot kell szerezni. Utána szóbeli vizsga.

Segédeszközök: Csak papír és toll használható, és az a papír, amin a feladatsor van, semmilyen más eszköz (például semmilyen elektronikus eszköz) nem. Aki meg nem engedett eszközt próbál használni, beszélgetni próbál, stb., az ellen a legszigorúbb eljárást fogom kezdeményezni.

Javítás: Csak névvel és ETR kóddal ellátott dolgozatokat fogadok el. A feladatsort mindenképpen visszakérem, a viták elkerülésére névvel és kóddal ellátva. A dolgozatokat még aznap kijavítjuk, kiosztjuk, a vizsgázók és a javításban résztvevők számától függő időpontban. A kiosztáskor az esetleges javítási hibák észrevételezhetők (később már nem), ezután a dolgozatokat visszakérem, és a szóbeli vizsga megkezdődik. Az írásbeli kiosztásának helyét és időpontját, valamint a szóbeli helyét az írásbelin közöljük.

Járai Antal

Vizsgatételek

-1. A számelmélet alaptétele, prímek, lnko, lkkt, szita. Kongruenciák, maradékosztályok, $\mathbb{Z}_m$ tulajdonságai. Komplemens ábrázolás. Kulcscsere.

0. Az Euler-féle φ függvény. Euler–Fermat tétel, Fermat tétele. Lineáris kongruenciák és kongruenciarendszerek megoldása, diofantikus problémák. A kínai maradéktétel. Az RSA eljárás és alkalmazásai. Számelméleti függvények, példák, az Euler-függvény. Intervallumaritmetika.

1. Irányítatlan gráfokkal kapcsolatos alapfogalmak. Gráfok Descartes-szorzata, izomorfiája. Teljes gráfok, páros gráfok, részgráfok.

2. Séták, vonalak, utak és körök. Séta helyettesítése úttal, zárt séta felbontása körökre. Összefüggőség, fák, szükséges és elégséges feltételek arra, hogy egy gráf fa legyen.

3. Feszítőfa, létezése, vágás, vágások száma. Erdők. Euler-vonal, felbontás éldiszjunkt vonalakra. Hamilton-út, Hamilton-kör. Címkézett és súlyozott gráfok, Kruskal algoritmusa.

4. Irányított gráfok: alapfogalmak, példák, éllistás ábrázolás, irányított gráfok izomorfiája. Irányított részgráf, irányított séták, vonalak, utak és körök. Erős összefüggőség. Irányított fák. Dijstra módszere, dinamikus programozás.

5. Morfizmusok (homomorfizmus, stb.) és kapcsolatuk tulajdonságokkal. Reprezentációk. A csoportdefiníció ekvivalensei. Példák csoportokra.

6. Részcsoport, a definíció ekvivalensei. Generált részcsoport és előállítása. Ciklikus csoportok szerkezete. Csoport és elem rendje. Ciklikus csoportok részcsoportjai. Mellékosztályok. Lagrange tétele és következményei.

7. Normálosztó, ekvivalens megfogalmazások. A művelettel kompatibilis osztályozás generálása. Faktorcsoport, példák. Cayley tétele. Permutációcsoportok, permutációk párossága.

8. Oszthatóság gyűrűkben, egységek és asszociáltak. Gyűrűk morfizmusai. Gyűrű karakterisztikája. Részgyűrű, ideál, példák. Mellékosztályok, az osztályozás kompatibilitása a műveletekkel, faktorgyűrű. Példák.

9. Generált főideálok szerkezete, oszthatóság és ideálok. Gauss-gyűrűk. Euklideszi gyűrűk, egységek és asszociáltak, bővített euklideszi algoritmus, felbonthatatlan és prímelem, egyértelmű faktorizáció euklideszi gyűrűkben. Hányadostest.

10. Polinomok, polinomfüggvények, maradékos osztás és következményei. Polinom algebrai deriváltja. Többszörös gyökök.

11. Irreducibilis polinomok és testbővítések. Véges testek. Irreducibilis polinomok $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ és $\mathbb{Z}$ felett. Gauss tétele.

12. Lagrange-interpoláció, titokmegosztás. Kronecker-eljárás. Racionális törtfüggvények. Parciális törtekre bontás. Többhatározatlanú polinomok.

13. Kommunikáció és kódolás. Információ, bit, entrópia, az entrópia maximuma.. Betűnkénti kódolás, példa. Prefix, szuffix, infix. Kódfa. Prefix kód, egyenletes és veszős kód. Példák.

14. McMillan-egyenlőtlenség. Shannon tétele zajmentes csatornára. Optimális kód létezése, tulajdonságai, konstrukciója: Huffman-kód.. A kódolandó ábécé kiterjesztése. Szótárkódok.

15. Hibajelző kódok, paritásbites kód. Kódok távolsága és súlya. Kód hibajelző és hibajavító képessége. Minimális távolságú dekódolás. Ismétléses kód, kétdimenziós paritásellenőrzés. Hamming-korlát, Singleton-korlát.

16. Lineáris kód, generátormátrix, ellenőrzőmátrix, szindróma-dekódolás. Példa: Fano-kód. Polinomkódok, CRC-kódok. Reed–Solomon-kódok és dekódolásuk.

17. Számítási eljárás, szimulálás, példák. Ordó. Az algoritmus szemléletes fogalma. Turing-gépek, példák.

18. Turing-gép szimulálása csökkentett jelkészlettel. Egy szalagos gép, példák, szimulálás egy szalaggal. Szemétgyűjtés. Univerzális Turing-gépek.

19. Félszalagos gépek, Post-gép, korlátozott gépmodellek. RAM gép, ekvivalenciája Turing-géppel. Tárolt programú gép..