**Alkalmazott Matematika MSc- záróvizsga tételsor**

1. **Bevezetés az algoritmus elméletbe:**

Turing gépek. Gráfok színezése. Greedy színezés. A magyar módszer. Standard linearizáció. Tökéletes egyezés SAT-el. Balas algoritmus (Lazy-verzió) Elégedettségi probléma.

2. **Egész programozás:**

A hátizsák probléma szabványos formája. Hátizsák problémák. Elágazás és korlátozás módszer.

3. **Az absztrakt algebra témakörei:**

Alapvető algebrai struktúrák (fél csoport, csoport, gyűrű, test). Részcsoportok. Csoport morfizmusok. Mellékosztályok és Lagrange-tétel. Normálosztók és faktorcsoportok. Gyűrű morfizmusok. Részgyűrűk és ideálok. Faktorgyűrűk. Véges testek.

4. **A számelmélet alapjai:**

Oszthatóság, maradékos osztás tétele (euklideszi algoritmus, legnagyobb közös osztó), számelmélet alaptétele, kongruenciák, és a maradékosztályok algebrája, Euler-függvény, RSA algoritmus

5. **Kódok és szimmetrikus struktúrák:**

Véges geometria, projektív síkok, homogén koordináták, véges projektív síkok kombinatorikai tulajdonságai, Desarguesi síkok, affin síkok, affin síkok kombinatorikai tulajdonságai, latin négyzetek, latin négyzetek ortogonalitása, Bruck-Ryser tétel, blokkrendszerek, oszthatósági feltételek, Wilson-tétel, Steiner hármas rendszerek, Möbius síkok, Dobble, SET játék, Cayley gráfok.

6. **Az analízis alapjai:**

Metrikus terek. Topologikus terek. Folytonos függvények metrikus terekben. Teljes metrikus terek. Euklideszi, Hilbert, Banach terek és tulajdonságaik. Fix pont tétel. Ortogonális rendszerek. Sorozatok és függvények terei. Differenciálhatóság. Rieman és Lebesgue integrál.

7. **Alkalmazott analízis:**

Periodikus jelek Fourier-sora. Fourier-sorok konvergenciája: pontonkénti, egyenletes, norma konvergencia. Fejér közepek. Fourier-transzformált és tulajdonságai. Laplace-transzformált és tulajdonságai. A Laplace- és Fourier-transzformáltak közti kapcsolat. Konvergencia tartomány. Diszkrét Fourier-transzformált. Kapcsolat a folytonos és diszkrét Fourier-transzformáltak között. Alkalmazások a jelfeldolgozásban.

8. **Komplex analízis:**

Analitikus függvények. Cauchy integrálformula. Hardy terek. Harmonikus függvények. A határfüggvények tulajdonságai. Poisson integrál. Egységapproximáció és kapcsolata a Fourier sorokkal. Fourier sorok Abel-Poisson közepe.

9. **Információ elmélet:**

Entrópia, relatív entrópia, kölcsönös információ, Kolmogorov-komplexitás**.**

10. **Numerikus matematika:**

Gépi számok, A matematikai modellezés hibatípusai, Lineáris egyenletrendszerek direct ( Gauss-elimináció, LU-felbontás, Cholesky felbontás, QR-felbontás) és iterációs megoldási módszerei (Iterációs módszerek konvergenciája, Jacobi-, Gauss-Seidel és Richardson típusú iterációk és konvergencia tételeik ), Nem-lineáris egyenletek megoldási módszerei (intervallum felezés, fixpont-iteráció Newton-módszer, Húr módszer, Szelő módszer, Becslés polinomok gyökeinek elhelyezkedésére), Polinom-interpoláció és alkalmazásai, Spline-interpoláció, Legkisebb négyzetek módszere (mátrix általánosított inverze és egyenletrendszer általánosított megoldása, approximáció Hilbert terekben, polinom-approximáció második normában), Numerikus integrálás (klasszikus quadratúra-formulák, Newton-Cotes formulák, Csebisev- és Gauss-típusú formulák)

11. **Valószínűség és statisztika:**

Valószínűségi modellek és axiómák, számlálás, kombinatorika, diszkrét véletlenszerű változók, folytonos véletlenszerű változók, többszörös folytonos véletlenszerű változók, feltétel (feltételes valószínűségek) és Bayes szerepe, függetlenség, klasszikus statisztikai következtetés, Bayes-féle statisztikai következtetés, diszkrét és folytonos Bayes-féle következtetés eloszlások, kovariancia, Iterált elvárások, Bernuolli-folyamatok, nagy számok törvénye, centrális határtétel, Markov-folyamatok.

12. **Kriptográfia:**

Szimmetrikus kulcsos kriptográfia, Titkosítási módszerek tervezési elvei (Kerchkoffs elvei), támadó eszközkészlete, Klasszikus titkosítási protokollok (shift titkosítás, mono-alfabetikus csere, Vigenére titkosítás, polialfabetikus eltolás), Biztonságos titkosítás meghatározása, tökéletes biztonság és titkosság, Számítástechnika titkosság, tökéletesen titkos séma, OTP (egyszeri betét), véletlenszerű sorozatok, biztonsági igazolások redukálással, álvéletlenség, adatfolyam titkosítás, CPA-biztonsági titkosítás, blokk titkosítás, működési módok: ECB (elektronikus kódkönyv mód), CBC (rejtjel) Block Chaining mód), OFB (Output Feedback mód), CTR ((véletlenszerű) számláló mód), Feistel hálózat, helyettesítő-permutációs hálózatok, AES kulcs generálás és bővítés, Rijndael-teszt, Hash funkciók: adatstruktúrákban, kriptográfia, Merkle- Damgård konstrukció, üzenethitelesítési kód (MAC), szimmetrikus vs. nyilvános kulcsú titkosítás.

13. **Közönséges differenciálegyenletek ODE-k:**

ODE-k osztályozása, Kezdetiérték-feladatok, Elsőrendű lineáris ODE (Bernoulli és Lagrange-módszer), Egzakt DE, Bernoulli-egyenlet, Ricatti-egyenlet, Clairaut-egyenlet, Integráló tényező, Magasrendű DE, Peremérték problémák, differenciáloperátor, n-edik rendű (differenciális) polinom operátor, n-edrendű lineáris ODE (homogén és nem homogén eset), konstans variálásának módszere, annihilátor operátor, Laplace-transzformáció (differenciálegyenletek megoldása), inverz Laplace-transzformáció, ODE-k megoldásának megadása hatványsor alakban, Differenciál egyenletrendszerek.

14. **Parciális differenciálegyenletek PDE-k:**

A PDE-k osztályozása, Lineáris transzportegyenlet, elemi PDE-k, Peremfeltételek, A karakterisztikus görbék módszere, kvázilineáris PDE, Másodrendű PDE-k osztályozása (parabolikus, hiperbolikus, elliptikus): kanonikus formák, megoldások, D'Alambert-módszer, Fourier-féle változók szétválasztásának módja, Dirichlet-probléma formális megoldása, PDE-k stady-state megoldása, Gyenge deriváltak, gyenge deriváltak tulajdonságai, Sobolev-terek, Sobolev-terek teljessége, közelítés sima függvényekkel. Elsőrendű Szobolev tér, Szobolev egyenlőtlenség, Sobolev-Gagliardo-Nirenberg egyenlőtlenség, Sobolev-Poincaré egyenlőtlenség.

15. **Statisztika és alkalmazásai:**

Mintaméret-számítások, Statisztikai következtetés alapjai: hipotézisvizsgálat, Konfidenciaszint, hatásméret, teszteljesítmény, egy- és kétoldali tesztek, nem-parametrikus és parametrikus statisztikai tesztek, többszörös tesztelés korrekciója: post hoc tesztek, mintanagyság számítás a variancia meghatározásához.

16. **Numerikus modellezés, ODE-k numerikus megoldásai:**

A sajátérték probléma numerikus tárgyalása: Becslés a sajátértékek elhelyezkedésére, Gersgorin-tétel és alkalmazásai, Fadejev-féle Trace-módszer, Tridiagonális mátrixok karakterisztikus polinomja, Hatvány-módszer, inverz-iteráció és változataik, Jacobi módszer, LU- és QR-algoritmusok.

Közönséges differenciálegyenletek numerikus módszerei: Fokozatos közelítések módszere, Taylor-sor módszer, (egylépéses) Euler-módszer, Többlépéses (implicit) Euler módszer, Explicit Runge-Kutta módszerek, Lineáris többlépéses módszerek (Adams- és Adams-Bashfort módszerek konstrukciója)

17. **Integrálgeometria:**

Differenciálgeometriai alapfogalmak, görbék paraméterezése, görbület, torzió, Frenet formulák, görbék alaptétele. Felületek paraméterezése, geodetikusok, alapmennyiségek, Gauss görbület. Radon transzformáció, alkalmazások.