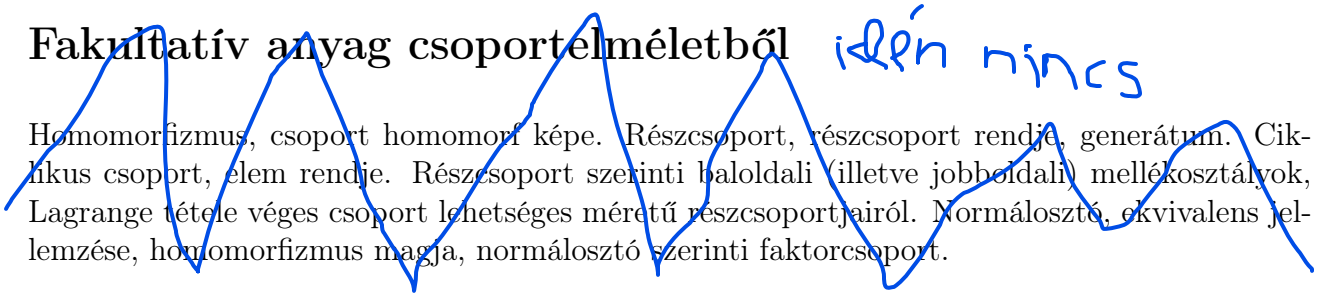
1. Számelméleti alapok

Oszthatóság az egész számok körében. Egységek; asszociált számok. Felbonthatatlan (irreducibilis) számok és prímszámok (és ezek azonossága az egészek körében de csak az egyikből következik a másik ravaszabb számkörökben). Maradékos osztás tétele (nemnegatív) egészek körében. Legnagyobb közös osztó és legkisebb közös többszörös. Bővített euklideszi algoritmus. A számelmélet alaptétele, kanonikus prímtényezős alak. Osztók számának ($\tau(n)$ számelméleti függvény) és az Euler-féle φ függvénynek a kiszámítása a kanonikus alakból. Prímek száma, Euklidész és Dirichlet tételei, Eratoszthenész szitája. Kongruenciák: $a \equiv b \pmod{m}$ definíciója, tulajdonságai. Lineáris kongruenciák megoldása, lineáris diofantikus egyenletek, szimultán kongruenciák, Kínai maradék-tétel. Maradékosztályok, teljes és redukált maradékrendszerek, redukált maradékosztályok halmaza. Műveletek maradékosztályokkal. Euler-féle φ függvény definíciója. Kis Fermat-tétel, Euler-Fermat tétel. Gyors hatványozás. Generátor (primitív gyök) modulo p prím, diszkrét logaritmus. Titkosítás Cæsar kóddal, RSA-titkosítás, Diffie-Hellman kulcscsere protokoll.

2. Algebrai alapok, polinomokkal kapcsolatos alapfogalmak

Definiáld a (binér) művelet fogalmát! Definiáld az asszociativitás fogalmát! Adj példát nem asszociatív binér műveletre! Definiáld a kommutativitás fogalmát! Adj példát nem kommutatív binér műveletre! Definiáld az algebrai struktúra fogalmát! Definiáld a grupoid fogalmát! Definiáld a félcsoport fogalmát! Adj példát olyan grupoidra, ami nem félcsoport! Definiáld a semleges elem fogalmát! Definiáld a monoid fogalmát! Definiáld az inverz fogalmát! Definiáld a csoport fogalmát! Definiáld az Abel-csoport fogalmát! Definiáld a disztributivitás fogalmát! Definiáld a gyűrű fogalmát! Definiáld a nullelem/egységelem fogalmát gyűrűben! Definiáld az egységelemes gyűrű fogalmát! Definiáld a kommutatív gyűrű fogalmát! Definiáld a nullosztómentes gyűrű fogalmát! Definiáld az integritási tartomány fogalmát! Definiáld a karakterisztika fogalmát! Definiáld az osztó/többszörös fogalmát! Definiáld az egység fogalmát! Adj példákat gyűrűre! Adj példákat véges és végtelen testre! Mi teljesül nullelemmel való szorzás esetén gyűrűben? Mit mondhatunk testben a nullosztókról? (Bizonyítsd is be!) Definiáld a polinomokat a műveletekkel! Milyen tulajdonságok öröklődnek egy gyűrűről az adott gyűrű fölötti polinomgyűrűre? Definiáld az együttható, a főtag és a konstans tag fogalmát! Definiáld a főegyüttható és a polinom fokának fogalmát! Definiáld a konstans polinom fogalmát! Definiáld a nullpolinomot! Definiáld a lineáris polinom fogalmát! Definiáld a monom fogalmát! Definiáld a főpolinom fogalmát! Mit mondhatunk polinomok összegének/szorzatának fokáról? (Bizonyítsd is be!) Adj példát, amikor a polinom összegére/szorzatára vonatkozó becslésben szigorú egyenlőtlenség teljesül! R milyen tulajdonságai öröklődnek $R[X]$-re? (Bizonyítsd is be!) Definiáld a helyettesítési érték fogalmát! Definiáld a gyök fogalmát! Definiáld a polinomfüggvény fogalmát! Adj példát, amikor különböző polinomokhoz ugyanaz a polinomfüggvény tartozik!

Fakultatív anyag csoportelméletből



Homomorfizmus, csoport homomorf képe. Részcsoport, részcsoport rendje, generátum. Ciklikus csoport, elem rendje. Részcsoport szerinti baloldali (illetve jobboldali) mellékosztályok, Lagrange tétele véges csoport lehetséges méretű részcsoportjairól. Normálosztó, ekvivalens jellemzése, homomorfizmus magja, normálosztó szerinti faktorcsoport.

3. Polinomok maradékos osztásának tétele és következményei

Hogyan szól a polinomok maradékos osztásának tétele? (Bizonyítsd is be!) Definiáld a gyöktényező fogalmát! Hogy szól a gyöktényező leválasztására vonatkozó tétel? (Bizonyítsd is be!) Hány gyöke lehet egy polinomnak? (Bizonyítsd be!) Adj példát olyan polinomra, amelynek különböző polinomgyűrűben különböző számú gyöke van! (A gyűrűket is add meg!) Ismertesd a Horner-elrendezést! Mit mondhatunk két darab, $n+1$ helyen megegyező, legfeljebb n-edfokú polinomról? (Bizonítsd be!) Mit mondhatunk végtelen R esetén az $R[X]$-beli polinomokhoz rendelt polinomfüggvényekről? (Bizonyítsd be!) Definiáld az oszthatóságot polinomok körében! Definiáld polinomok kitüntetett közös osztóját! Milyen polinomokra tudjuk biztosan alkalmazni az euklideszi algoritmust? (Válaszodat indokold!) Ismertesd a bővített euklideszi algoritmust és bizonyítsd helyességét!

4. Polinomok algebrai deriváltja, véges testek, racionális gyökteszt, Lagrange-interpoláció

Definiáld az algebrai derivált fogalmát! Milyen tulajdonságokkal rendelkezik az algebrai derivált? Mivel egyenlő elsőfokú főpolinom n-edik hatványának deriváltja? (Bizonyítsd!) Definiáld a többszörös gyök fogalmát! Definiáld gyök multiplicitását! Milyen kap csolat van egy polinom gyökei illetve a deriváltjának a gyökei között? (Bizonyítsd!) Adj példát olyan polinomra, amelynek van olyan n-szeres gyöke, ami a deriváltjának is n-szeres gyöke! Milyen alakú egy Lagrange-interpolációs alappolinom? Ismertesd a Lagrange-interpolációt! (És bizonyítsd helyességét!) Hogyan használható a Lagrange-interpoláció titokmegosztásra? Hogyan konstruálunk p^n elemű testet? Mit mondhatunk véges testekről az elemszámmal kapcsolatosan? Mik lehetnek egy primitív egész együtthatós polinom racionális gyökei? (Bizonyítsd!) Bizonyítsd be, hogy $\sqrt{2} \notin \mathbb{Q}$!

5. Polinomok felbonthatósága

Hogyan jellemezhetőek test fölötti polinomgyűrűben az egységek? (Bizonyítsd!) Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban? (Bizonyítsd!) Adj példát olyan elsőfokú polinomra, amelynek nincs gyöke! Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben felbonthatóság szempontjából? (Bizonyítsd!) Hogyan jellemezhetők a test fölötti másod-, illetve harmadfokú polinomok felb onthatóság szempontjából? (Bizonyítsd!) Hogyan jellemezhetők a $\mathbb{C}$ fölötti felbonthatatlan polinomok? (Bizonyítsd!) Hogyan jellemezhetők az $\mathbb{R}$ fölötti felbonthatatlan polinomok? (Bizonyítsd!) Definiáld a primitív polinom fogalmát! Hogy szól Gauss lemmája? (Bizonyítsd!) Hogyan írhatóak fel az egész együtthatós polinomok primitív polinomok segítségével? Hogyan írhatóak fel a racionális együtthatós polinomok primitív polinomok segítségével? Hogy szól a Gauss-tétel egész együtthatós polinomokra? (Bizonyítsd!) Hogy szól a Schönemann-Eisenstein-tétel egész együtthatós polinomokra? (Bizonyítsd!)

6. Entrópia, forráskódolás

Add meg a kommunikáció vázlatos ábráját! Definiáld az információ fogalmát! Hogyan mérjük? Definiáld a gyakoriság/relatív gyakoriság fogalmát! Definiáld az üzenetek eloszlásának fogalmát! Definiáld üzenet egyedi információtartalmát! Definiáld üzenetek átlagos információtartalmát! Mit nevezünk eloszlásnak? Definiáld eloszlás entrópiáját! Definiáld a konvex és a szigorúan konvex függvény fogalmát! Hogyan szól a Jensen-egyenlőtlenség? Milyen felső korlát adható az entrópiára? (Bizonyítsd!) Definiáld a kódolás fogalmát! Mit nevezünk kódnak? Definiáld a felbontható/egyértelműen dekódolható/veszteségmentes kódolást! Definiáld az ábécé, betű és szó fogalmát! Definiáld az A^+ és az A^* halmazokat! Definiáld a betűnkénti kódolást! Mit érdemes feltenni egy betűnkénti kódolás alapjául szolgáló leképezésről? Definiáld a prefix, infix, szuffix fogalmát! Definiáld a triviális prefix/infix/szuffix fogalmát! Definiáld a valódi prefix/infix/szuffix fogalmát! Definiáld a prefixmentes halmaz fogalmát! Definiáld a prefix kód fogalmát! Definiáld az egyenletes/fix hosszúságú/blokk kód fogalmát! Definiáld a vesszős kód fogalmát! Milyen kap csolat van a prefix, egyenletes, vesszős és felbontható kódok között? (Bizonyítsd is be ezt az összefüggést!) Adj példát nem prefix, de felbontható kódra! Hogyan szól a McMillan egyenlőtlenség és a "megfordítása"? Definiáld a kód átlagos szóhosszát! Definiáld az optimális kód fogalmát! Mit mondhatunk optimális kód létezésével kap csolatosan? (Bizonyítsd!) Hogyan szól Shannon tétele zajmentes csatornára? (Bizonyítsd!) Mit mondhatunk Shannon-kód átlagos szóhosszáról? (Bizonyítsd!) Hogyan konstruálunk Huffman-kódot? Hogyan konstruálunk Shannon-kódot? Definiáld a kódfa fogalmát!

7. Hibakorlátozó és lineáris kódolás

Mi az a paritásbites kód? Mi az a kétdimenziós paritásellenőrzés? Definiáld a t-hibajelző és a pontosan t-hibajelző kód fogalmát! Definiáld szavak Hamming-távolságát! Milyen tulajdonságokkal rendelkezik a Hamming-távolság? Definiáld a kód távolságát! Mit jelent a minimális távolságú dekódolás? Definiáld a t-hibajavító és a pontosan t-hibajavító kód fogalmát! Mi az az ismétléses kód? Fogalmazd meg a Singleton-korlátra vonatkozó állítást! (Bizonyítsd!) Definiáld az MDS-kód fogalmát! Fogalmazd meg a Hamming-korlátra vonatkozó állítást! (Bizonyítsd!) Definiáld a perfekt kód fogalmát! Mi a kap csolat kód távolsága és hiba*jelző* képessége között? (Bizonyítsd!) Mi a kap csolat kód távolsága és hiba*javító* képessége között? (Bizonyítsd!) Milyen műveletekkel alkot lineáris teret $\mathbb{F}_n$? Definiáld a lineáris kód fogalmát! Milyen paraméterekkel jellemezzük a lineáris kódokat? Milyen alakot ölt a Singleton-korlát lineáris kód esetén? Adj példát lineáris kódra! Definiáld a kódszó súlyát! Definiáld a kód súlyát! Milyen összefüggés van lineáris kód súlya és távolsága között? (Bizonyítsd!) Definiáld lineáris kód generátormátrixát! Definiáld lineáris kód ellenőrző mátrixát! Mi a kap csolat a generátormátrix és ellenőrző mátrix között? Definiáld a szisztematikus kódolás fogalmát! Definiáld az üzenetszegmens fogalmát! Definiáld a paritásszegmens fogalmát! Hogyan dekódolunk szisztematikus kódolás esetén? Mi a kapcsolat szisztematikus kód generátormátrixa és ellenőrző mátrixa között? (Bizonyítsd!) Mi a kapcsolat az ellenőrző mátrix és a kód távolsága között? (Bizonyítsd!) Definiáld a szindróma fogalmát! Definiáld a hibavektor fogalmát! Definiáld egy adott hibavektorhoz tartozó mellékosztályt! Hogyan jellemezhetőek az azonos mellékosztályban lévő szavak a szindrómájuk segítségével? Definiáld a mellékosztály-vezető fogalmát! Írd le a szindrómadekódolást! Mi a kap csolat a szindrómadekódolás és a minimális távolságú dekódolás között? (Bizonyítsd!) Definiáld a Hamming-kód fogalmát! Adj példát bináris Hamming-kódra az ellenőrző mátrixa segítségével!