## VIZSGAANYAG

### Kérdések (1-1 pont)

Mely tétel alapján számolhatjuk ki véges sok egész szám legnagyobb közös osztóját prímfelbontás nélkül?

Fogalmazza meg a számelmélet alaptételét.

Definiálja prímtenyezős felbontásnál a kanonikus alakot.

Hogyan határozhatók meg természetes számok esetén az osztók, a legnagyobb közös osztó és a legkisebb közös többszörös a prímtényezős felbontás segítségével?

Mi a kapcsolat két egész szám legnagyobb közös osztója és legkisebb közös többszöröse között?

Hogyan számolhatjuk ki véges sok egész szám legkisebb közös többszörösét prímfelbontás nélkül?

Ismertesse Erathoszthenész szitáját.

Definiálja egész számok kongruenciáját és adja meg a kapcsolódó jelöléseket.

Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

Definiálja a maradékosztály, redukált maradékosztály, teljes és redukált maradékrendszer fogalmát.

Definiálja $\mathbb{Z}_m$-et. Milyen algebrai struktúra $\mathbb{Z}_m$?

Ismertesse a komplemens ábrázolásokat.

Fogalmazza meg a $\mathbb{Z}_m$ gyűrű tulajdonságait leíró tételt.

Ismertesse a Diffie–Hellmann–Merkle kulcscserét.

Definiálja az Euler-féle $\varphi$ függvényt.

Mit mondhatunk az $aa_i + b$ számokról, ha $a_i$ egy maradékrendszer, illetve egy redukált maradékrendszer elemeit futja be?

Fogalmazza meg az Euler–Fermat-tételt.

Fogalmazza meg a Fermat-tételt.

Mit értünk diofantikus problémán?

Mondjon két példát diofantikus problémára.

Fogalmazza meg a kínai maradéktételt.

Ismertesse az RSA eljárást.

Ismertesse az RSA eljárás felhasználását digitális aláírásra.

Ismertesse az RSA eljárás felhasználását bizonyítványok kiállítására.

Definiálja a számelméleti függvény, az additív számelméleti függvény és a teljesen additív számelméleti függvény fogalmát.

Definiálja a számelméleti függvény, az multiplikatív számelméleti függvény és a teljesen multiplikatív számelméleti függvény fogalmát.

Fogalmazza meg az additív, multiplikatív, teljesen additív és teljesen multiplikatív számelméleti függvények kiszámítására vonatkozó tételt.

Adjon egyszerű példák additív, multiplikatív, teljesen additív és teljesen multiplikatív számelméleti függvényekre.

Definiálja a $\mu$, $\kappa$ és $\nu$ számelméleti függvényeket. Milyen tulajdonságúak?

Definiálja a $\tau$, $\sigma$ és $\sigma_r$ számelméleti függvényeket. Milyen tulajdonságúak?

Írja fel a $\tau$, $\sigma$ és $\sigma_r$ számelméleti függvények kiszámítására használható formulákat.

Fogalmazza meg az Euler-féle $\varphi$ függvény kiszámítására vonatkozó tételt.

Ismertesse az intervallum-aritmetikát.

Definiálja a gráf, csúcsok, élek és illeszkedési leképezés fogalmát.

Definiálja az „illeszkedik”, „végpontja” és „izolált csúcs” fogalmakat.
Definiálja az üres gráf és az illeszkedési reláció fogalmát.
Definiálja csúcsok, illetve élek szomszédosságát.
Definiálja a hurokél és a párhuzamos élek fogalmát.
Definiálja az egyszerű gráf és a véges gráf fogalmát.
Definiálja gráfban a fokszám és a reguláris gráf fogalmát.
Mit mondhatunk gráfban a fokszámok összegéről?
Definiálja gráfok izomorfiáját.
Mondjon elégséges feltételt arra, hogy két gráf ne legyen izomorf.
Mondjon elégséges feltételt arra, hogy két egyszerű gráf izomorf legyen.
Definiálja a teljes gráf fogalmát.
Hány éle van egy teljes gráfnak?
Definiálja a páros gráf fogalmát.
Adja meg a „három ház, három kút” gráfot.
Definiálja a részgráf és a feszített részgráf fogalmát.
Definiálja részgráf komplementerét.
Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott gráfot.
Definiálja a séta és a séta hossza fogalmát.
Definiálja a nyílt és a zárt sétát.
Definiálja az út fogalmát.
Mikor lesz egy nulla illetve egy hosszú séta út?
Definiálja a vonal fogalmát.
Definiálja a kör fogalmát.
Van-e egy illetve kettő hosszú kör?
Hogyan kaphatunk sétából utat? Fogalmazza meg az állítást.
Definiálja az összefüggőség és a komponens fogalmát.
Igaz-e, hogy egy gráf minden éle valamely komponenshez tartozik?
Mi a kapcsolat a komponensek és az összefüggőség között?
Definiálja a fa fogalmát.
Fogalmazzon meg két szükséges és elégséges feltételt arra, hogy egy egyszerű gráf fa legyen.
Egy véges gráfban nincs kör, de van él. Mit állíthatunk fokszámokkal kapcsolatban?
Egy egyszerű véges gráfnak $n$ csúcsa van. Fogalmazzon meg két olyan szükséges és elégséges feltételt amelyben szerepel az élek száma, arra, hogy a gráf fa.
Definiálja a feszítőfa fogalmát.
Mit állíthatunk feszítőfa létezéséről?
Mikor mondjuk, hogy egy csúcshalmaz illetve élhalmaz elvág két csúcsot?
Definiálja az elvágó élhalmaz és a vágás fogalmát.
Mit állíthatunk véges összefüggő gráfban a vágások számáról?
Definiálja az erdő fogalmát. Mi az összefüggés a fákkal?
Definiálja a feszítő erdő fogalmát. Hány éle van egy véges gráf feszítő erdőjének?
Definiálja az Euler-vonal fogalmát.
Fogalmazza meg a véges összefüggő gráfok vonalak egyesítéseként való előállítására vonatkozó tételt.
Definiálja a Hamilton-út illetve Hamilton-kör fogalmát.
Definiálja a címkézett gráf fogalmát.
Definiálja a súlyozott gráf fogalmát és egy véges részhalmaz súlyát.
Fogalmazza meg a Kruskal algoritmust és a rá vonatkozó tételt.

Mit értünk mohó algoritmuson? Mondjon példát, amikor egy mohó algoritmus nem ad optimális megoldást.

Definiálja az irányított gráf, csúcsok, élek és illeszkedési leképezés fogalmát.

Definiálja irányított gráfban a kezdőpont és a végpont fogalmát.

Hogyan kaphatunk irányított gráfból irányítatlan gráfot? Miért használhatjuk irányított gráfokra az irányítatlan gráfokra definiált fogalmakat?

Definiálja a gráf irányítása illetve megfordítása fogalmát.

Definiálja a szigorúan párhuzamos élek fogalmát.

Definiálja az egyszerű gráf és a véges gráf fogalmát.

Definiálja csúcs befokát és kifokát.

Mit mondhatunk irányított gráfokra a fokszámok összegéről?

Hogyan szemléltethetünk egy relációt irányított gráffal?

Definiálja irányított gráfok izomorfiáját.

Definiálja az irányított részgráf és a feszített irányított részgráf fogalmát.

Definiálja irányított részgráf komplementerét.

Definiálja az élhalmaz illetve csúcshalmaz törlésével kapott irányított gráfot.

Definiálja a irányított séta és az irányított séta hossza fogalmát.

Definiálja a nyílt és a zárt irányított sétát.

Definiálja az irányított út fogalmát.

Definiálja az irányított kör fogalmát.

Definiálja az erős összefüggőség és az erős komponens fogalmát.

Igaz-e, hogy egy irányított gráf minden éle valamely erős komponenshez tartozik?

Mi a kapcsolat az erős komponensek és az erős összefüggőség között?

Definiálja az irányított fa és gyökere fogalmát.

Definiálja a irányított fa szintjeit.

Definiálja irányított fában a leveleket.

Definiálja egy művelet esetén a homomorfizmus és a homomorf kép fogalmát.

Definiálja egy művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.

Definiálja egy művelet esetén az endomorfizmus és az automorfizmus fogalmát.

Mit mondhatunk homomorfizmusnál félcsoport, egységelem, inverz és felcserélhető elemek esetén?

Mi mondhatunk homomorfizmusnál csoport, kommutatív félcsoport és Abel-csoport esetén?

Adjon meg szükséges és elégséges feltételeket arra, hogy egy félcsoport csoport legyen.

Fogalmazza meg csoportban az egyszerűsítési szabályt.

Adjon példát invertálható műveletre, amellyel nem kapunk csoportot.

Adja meg a szorzással mint művelettel tekintett egységnyi abszolút értékű komplex számok csoportjának három valódi részcsoportját.

Mit értünk a Klein-féle csoporton? Kommutatív-e?

Mit értünk diédercsoporton?

Definiálja a részcsoport, triviális részcsoport és valódi részcsoport fogalmát.

Adjon meg szükséges és elégséges feltételeket arra, hogy egy csoport egy részhalmaza részcsoport legyen.

Mit mondhatunk részcsoportok metszetéről és egyesítéséről?

Definiálja a generátum és a generátorrendszer fogalmát.

Definiálja a ciklikus csoport és generátora fogalmát.

Fogalmazza meg a generátumot leíró állítást.

Mit mondhatunk ciklikus csoport homomorf képéről?

Definiálja csoport és elem rendjét.

Fogalmazza meg a ciklikus csoportok szerkezetét leíró tételt.

Mi a kapcsolat elem és részcsoport rendje között?

Mit mondhatunk ciklikus csoport részcsoportjairól?

Mit mondhatunk véges ciklikus csoport részcsoportjai generátorainak számáról?

Definiálja a bal- és jobboldali mellékosztályokat.

Mi a kapcsolat a bal- és a jobboldali mellékosztályok között?

Definiálja részcsoport indexét.

Fogalmazza meg Lagrange tételét.

Mi a kapcsolat elem rendje és a csoport rendje között?

Fogalmazzon meg olyan tételt, amely lehetővé teszi, hogy egy csoport rendjéből a ciklikusságára következtessünk.

Adjon meg szükséges és elégséges feltételt arra, hogy egy csoportnak ne legyen nem triviális részcsoportja.

Definiálja a normálosztó fogalmát.

Adjon meg három olyan csoportot, amelyben minden részcsoport normálosztó.

Adjon meg szükséges és elégséges feltételeket arra, hogy egy részcsoport normálosztó legyen.

Mit mondhatunk normálosztók metszetéről és egyesítéséről?

Fogalmazza meg kompatibilis osztályozások és a normálosztók közötti kapcsolatot leíró tételt.

Definiálja a faktorcsoport fogalmát és fogalmazza meg a definícióban felhasznált tételt.

Adjon meg három példát faktorcsoportra.

Fogalmazza meg Cayley tételét.

Definiálja az $n$-ed fokú szimmetrikus csoportot.

Két véges halmaznak ugyanannyi eleme van. Igaz-e, hogy permutációcsoportjaik izomorfak?

Írja le $S_n$ elemeinek hagyományos jelölését és adja meg ezzel a jelöléssel a szorzást.

Definiálja a páros és páratlan permutációkat.

Ismertesse permutációk ciklus jelölését.

Mi a transzpozíció?

Fogalmazza meg a páros illetve páratlan permutációk és a transzpozíciók száma közötti összefüggést leíró tételt.

Fogalmazza meg a permutációk szorzatának párosságára vonatkozó tételt.

Definiálja az alternáló csoportokat.

Igaz-e hogy egy egységelemes integritási tartomány akkor és csak akkor test, ha minden nem nulla eleme egység?

Igaz-e hogy egy véges integritási tartomány test?

Definiálja egységelemes integritási tartományban az oszthatóságot és adja meg a jelölését.

Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

Definiálja az asszociáltak fogalmát és sorolja fel ennek a kapcsolatnak a tulajdonságait.

Definiálja az egységek fogalmát és sorolja fel az egységek halmazának tulajdonságait.

Mi a kapcsolat az egységek és az asszociáltak között?

Definiálja a Gauss-egészek gyűrűjét. Igaz-e, hogy két egység van?

Definiálja egységelemes integritási tartományban a prímelem és az irreducibilis elem fogalmát. Mi a kapcsolat a két fogalom között?

Mit értünk egységelemes integritási tartományban legnagyobb közös osztó alatt?

Mikor mondjuk egységelemes integritási tartomány elemeire, hogy relatív prímek?

Mit értünk egységelemes integritási tartományban legkisebb közös többszörös alatt?

Igaz-e, hogy egy adott halmazt egy testbe képező függvények gyűrűje is test?

Definiálja két művelet esetén a homomorfizmus és a homomorf kép fogalmát.

Definiálja két művelet esetén a monomorfizmus, az epimorfizmus és az izomorfizmus fogalmát.

Definiálja két művelet esetén az endomorfizmus és az automorfizmus fogalmát.

Mi mondhatunk homomorfizmusnál gyűrű képéről?

Definiálja gyűrű karakterisztikáját. Milyen állítást használt?

Fogalmazza meg a gyűrűk karakterisztikájára vonatkozó tételt.

Definiálja a részgyűrű fogalmát.

Definiálja a jobbideál, balideál és ideál fogalmát.

Definiálja a triviális ideál és a valódi ideál fogalmát.

Definiálja az egyszerű gyűrű fogalmát.

Definiálja a generált ideál és a főideál fogalmát.

Mondjon négy példát $\mathbb{R}^{\mathbb{R}}$ részgyűrűjére.

Mondjon példát $\mathbb{Z}$-ben ideálra. Főideál-e?

Definiálja gyűrűben a mellékosztályokat.

Fogalmazza meg kompatibilis osztályozások és az ideálok közötti kapcsolatot leíró tételt.

Definiálja a faktorgyűrű fogalmát és fogalmazza meg a definícióban felhasznált tételt.

Adjon példát $\mathbb{Z}$ faktorgyűrűjére.

Fogalmazza meg egy kommutatív egységelemes gyűrűben a főideálokat leíró állítást.

Fogalmazza meg egy egységelemes integritási tartományban az oszthatóság és a generált főideálok kapcsolatát leíró állítást.

Definiálja a Gauss-gyűrű fogalmát.

Gauss-gyűrűben hogyan olvashatók le a faktorizációból az osztók?

Igaz-e hogy Gauss-gyűrűben létezik legnagyobb közös osztó és legkisebb közös többszörös?

Igaz-e hogy Gauss-gyűrűben minden irreducibilis elem prím?

Definiálja az euklideszi gyűrű fogalmát.

Fogalmazza meg az euklideszi gyűrűben az egységeket és az asszociáltakat leíró tételt.

Fogalmazza meg a bővített euklideszi algoritmust euklideszi gyűrűben.

Mi a kapcsolat euklideszi gyűrűben a prímelemek és az irreducibilis elemek között?

Fogalmazza meg euklideszi gyűrűben a faktorizációra vonatkozó tételt.

Definiálja a hányadostest fogalmát. Milyen állítást használt?

Hogyan ágyazható be egy integritási tartomány a hányadostestébe?

Definiálja az egyhatározatlanú polinom fogalmát.

Definiálja egyhatározatlanú polinomok összeadását és szorzását.

Hogyan azonosíthatjuk a gyűrű elemeit bizonyos polinomokkal? Hogy hívjuk ezeket a polinomokat?

Definiálja polinom együtthatóit, főegyütthatóját és fokszámát.

Definiálja a lineáris polinomokat.

Definiálja a monom fogalmát egy határozatlan esetén.

Definiálja a főpolinom fogalmát.

Mit mondhatunk polinomok szorzatának főegyütthatójáról?

Mit mondhatunk polinomok szorzatának fokáról?

Definiálja polinom helyettesítési értékét és gyökét.

Definiálja a polinomhoz tartozó polinomfüggvényt. Tartozhat-e különböző polinomokhoz ugyanaz a polinomfüggvény?

Fogalmazza meg a maradékos osztás tételét polinomokra.

Fogalmazza meg a gyöktényező leválasztására vonatkozó állítást.

Legfeljebb hány gyöke van egy polinomnak? Fogalmazza meg az állítást.

Milyen esetben kölcsönösen egyértelmű a megfeleltetés a polinomok és a polinomfüggvények között? Fogalmazza meg az állítást.

Milyen esetben alkotnak a polinomok euklideszi gyűrűt? Fogalmazza meg az állítást.

Ismertesse a Horner-elrendezést.

Mondjon példát, amikor egy adott másodfokú polinomnak nulla, egy illetve két gyöke van.

Definiálja polinom algebrai deriváltját.

Milyen négy tulajdonsággal jellemezhető a polinomhoz az algebrai deriváltját rendelő leképezés?

Az $f$, $g$ polinomokra $g^n \mid f$. Mit állíthatunk $f'$-ről? Fogalmazza meg az állítást.

Hogyan kaphatunk egy polinomból négyzetmentes polinomot? Fogalmazza meg az állítást.

Definiálja polinom többszörös gyökét.

Mi a kapcsolat a polinom gyökei és a deriváltjának a gyökei között? Fogalmazza meg az állítást.

Lehet-e egy polinom $n$-szeres gyöke a deriváltnak is legalább $n$-szeres gyöke?

Írja le az egységeket test feletti polinomok körében.

Hogyan kaphatunk véges testeket?

Fogalmazza meg a véges testek elemszámát leíró tételt.

Fogalmazza meg a véges test nem nulla elemei multiplikatív csoportjának szerkezetét leíró tételt.

Van-e minden prímhatványhoz olyan elemszámú véges test?

Írja le az irreducibilis polinomokat a $\mathbb{C}$ feletti polinomok körében.

Írja le az irreducibilis polinomokat az $\mathbb{R}$ feletti polinomok körében.

Mit tud a $\mathbb{Q}$ feletti irreducibilis polinomokról?

Igaz-e, hogy $\mathbb{Z}[x]$ euklideszi gyűrű?

Igaz-e, hogy $\mathbb{Z}[x]$ Gauss-gyűrű?

Fogalmazza meg Gauss tételét egyértelmű faktorizációs tartományokról.

Ismertesse a Lagrange-interpolációt.

Ismertessen egy titokmegosztási eljárást.

Ismertesse a Kronecker-eljárást.

Fogalmazza meg a véges testek alaptételét.

Hogyan kaphatunk véges testeket? Irjon le olyan eljárást, amely minden véges testet megad.

Definiálja a racionális függvényeket.

Fogalmazza meg a parciális törtekre bontás tételét $1/g$ alakú racionális függvényre.

Fogalmazza meg a parciális törtekre bontás tételét $f/g$ alakú racionális függvényre két alakban.

Fogalmazza meg a parciális törtekre bontás tételét $u/v^k$ alakú racionális függvényre.

Definiálja a többhatározatlanú polinom fogalmát.

Hogyan azonosíthatjuk a gyűrű elemeit bizonyos többhatározatlanú polinomokkal? Hogy hívjuk ezeket a polinomokat?

Definiálja többhatározatlanú polinom együtthatóit, tagjainak multifokát és fokát.

Definiálja a többhatározatlanú monom fogalmát.

Definiálja többhatározatlanú polinom fokát. Milyen megállapodások mellett egyértelmű egy többhatározatlanú polinom felírása?

Definiálja a többhatározatlanú lineáris polinomokat.

Hogyan írhatjuk fel két többhatározatlanú polinom összegének, illetve szorzatának az együtthatóit?

Milyen esetben lesz a többhatározatlanú polinomok gyűrűje nullosztómentes?

Mit mondhatunk két többhatározatlanú polinom szorzatának a fokáról?

Milyen esetben lesz a többhatározatlanú polinomok gyűrűje Gauss-gyűrű? Fogalmazza meg az állítást.

Definiálja a gyakoriság és a relatív gyakoriság fogalmát.

Definiálja egyedi üzenet információtartalmát. Mi a bit?

Definiálja az eloszlás és az entrópia fogalmát.

Adja meg a pontos felső korlátot eloszlás entrópiájára. Mikor teljesül egyenlőség?

Mi a forráskódolás? Mik a részei?

Rajzolja fe l az üzenetátvitel részletes sémáját.

Ismertesse a betűnkénti kódolást.

Definiálja a prefix, infix és szuffix fogalmát.

Ismertesse a kód és a kódfa kapcsolatát.

Definiálja a prefix, egyenlete és vesszős kódot. Mi a kapcsolatuk?

Adjon példát nem dekódolható kódra.

Adjon példát fejthető, de nem prefix kódra.

Fogalmazza meg a McMillen-egyenlőtlenséget tartalmazó tételt.

Definiálja az átlagos szóhosszúság és az optimális kód fogalmát.

Van-e mindig optimális kód betűnkénti kódolásnál?

Fogalmazza meg Shannon tételét zajmentes csatornára.

Ismertesse egy optimális kód kódfájának tulajdonságait.

Fogalmazza meg azt a három állítást, amelynek alapján optimális kód konstruálható.

Írja le, hogyan konstruálunk Huffman-kódot.

Írja le, mit érhetünk el a kódolandó ábécé kiterjesztésével.

Ismertesse a szótárkódok alapgondolatát.

Ismertesse a paritásbites kódot.

Definiálja a $t$-hibajelző és pontosan $t$-hibajelző kód fogalmát.

Definiálja kód távolságát és súlyát.

Mi a kapcsolat a kód távolsága és hibajelző képessége között?

Ismertesse a minimális távolságú dekódolást.

Definiálja a $t$-hibajavító és pontosan $t$-hibajavító kód fogalmát.

Mi a kapcsolat a kód távolsága és hibajavíto képessége között?

Definiálja a lineáris kód fogalmát és a kapcsolódó jelöléseket.

Ismertesse a kétdimenziós paritásellenőrzést.

Mi a Hamming-korlát?

Mi a Singleton-korlát?

Mi az MDS-kód és miért hívják így?

Definiálja a lineáris kód fogalmát és a kapcsolódó jelöléseket.

Definiálja a generátormátrix, ellenőrző mátrix és s szindróma fogalmát.

Ismertesse a szindróma-dekódolást.
Ismertesse a Fano-kódot.
Ismertesse a polinomkódokat.
Ismertesse a CRC-t.
Adja meg Reed–Solomon-kód esetén a kódolást.
Adjon meg Reed–Solomon-kód esetén egy ellenőrző mátrixot.
Definiálja a hibahelypolinomot és a hibaértékpolinomot.
Hogyan történik a hibahelypolinom és a hibaértékpolinom ismertében a Reed–Solomon-kód dekódolása?
Fogalmazza meg a tételt, amely lehetővé teszi a hibahelypolinom és a hibaértékpolinom meghatározását.
Definiálja a számítási eljárás fogalmát.
Definiálja a szimulálást.
Definiálja a nagy ordót, a nagy omegát és thetát.
Definiálja a Turing-gépet.
Definiálja Turing-gép bemenetét és kimenetét.
Fogalmazza meg a Turing-gép csökkentett jelkészlettel történő szimulálására vonatkozó tételt.
Ismertesse szavak kétféle kódolását számmá és vissza.
Fogalmazza meg a Turing-gép egyszalagos géppel történő szimulálására vonatkozó tételt.
Fogalmazza meg a szemétgyüjtésre vonatkozó tételt.
Fogalmazza meg az univerzális Turing-gépekkel kapcsolatban tanult tételt.
Definiálja a félszalagos Turing-gépet.
Fogalmazza meg a félszalagos Turing-gép Turing-géppel történő szimulálására vonatkozó tételt.
Fogalmazza meg a Turing-gép félszalagos Turing-géppel történő szimulálására vonatkozó tételt.
Definiálja a Post-gépet.
Fogalmazza meg a Post-gép Turing-géppel történő szimulálására vonatkozó tételt.
Fogalmazza meg a Turing-gép Post-géppel történő szimulálására vonatkozó tételt.
Ismertesse a korlátozott gépmodelleket.
Fogalmazza meg a Turing-gép kétveremtáras géppel történő szimulálására vonatkozó tételt.
Fogalmazza meg a kétveremtáras gép Turing-géppel történő szimulálására vonatkozó tételt.
Ismertesse a RAM-gépet.
Mi a logaritmikus költség?
Fogalmazza meg a Turing-gép RAM-géppel történő szimulálására vonatkozó tételt.
Fogalmazza meg a RAM-gép Turing-géppel történő szimulálására vonatkozó tételt.
Ismertesse a tárolt programú gépet.