DHARMA INITIATIVE

Diszkrét Matematika 1. – Definíciók (középszint)

E dokumentum az ELTE IK Diszkrét Matematika 1. 2010/2011-es vizsgájára készült. Az elkészítéshez a korábbi évek kidolgozott listáit használtuk.
Amennyiben hibát talált a definíciók között, azt kérjük, hogy jelezze a kurzusfórumon.

Sikeres felkészülést kívánunk!
DHARMA Initiative

1. Mondjon legalább három példát predikátumra.

$E(x)$: x egyenes
$P(x)$: x pont
$I(x, y)$: x illeszkedik y-ra.

2. Sorolja fel a logikai jeleket.

$\neg$: negáció (tagadás)

$\wedge$: konjukció (és)

$\vee$: diszjunkció (vagy)

$\Rightarrow$: implikáció (ha… akkor…)

$\Leftrightarrow$: ekvivalencia (akkor és csak akkor)

$\oplus$: antivalencia (kizáró vagy)

|: konnegáció (sem… sem…[A | B = $\neg(A \vee B)$])

||: exklúzió (összeférhetetlen vagy: [A || B = $\neg(A \wedge B)$])

3. Milyen kvantorokat ismer? Mi a jelük?

∀ : univerzális kvantor (minden).
∃ : egzisztenciális kvantor (létezik).

4. Hogyan kapjuk a logikai formulákat?

A logikai formulák az adott elmélet predikátumaiból épülnek fel a logikai jelek valamint a kvantorok segítségével.

5. Mikor van egy változó egy kvantor hatáskörében?

Egy formula egy ($\exists x\, A$) vagy ($\forall x\, A$) típusú részformulája esetén az x változó minden, a két zárójel közötti előfordulására (a kvantor után vagy A-ban) a kvantor hatáskörében van.

6. Mik a nyitott és mik a zárt formulák?

Ha egy formulában egy változó egy adott előfordulása egy kvantor hatáskörében van, akkor azt mondjuk, hogy az adott előfordulás kötött előfordulás, egyébként az adott előfordulás szabad előfordulás. Ha egy változónak egy formulában van szabad előfordulása, akkor azt mondjuk, hogy a változó szabad változó. Ha egy formulának nincs szabad változója, akkor a formulát zárt formulának, egyébként nyitott formulának mondjuk.

7. Mondjon két példát nyitott formulára.

$A(x,y) = ((P(x) \wedge P(y)) \wedge \neg x = y)$;

$B(x) = ((E(x) \wedge P(y)) \wedge I(x,y))$

8. Mondjon egy példát zárt formulára.

$\forall x(E(x) \Rightarrow \exists y(P(x) \wedge I(x,y)))$

9. Definiálja a részhalmaz és a valódi részhalmaz fogalmát és adja meg jelöléseiket.

Akkor mondjuk, hogy az A halmaz részhalmaza a B halmaznak, ha A minden eleme a B halmaznak is eleme. Jele: $A \subset B$ vagy $B \supset A$.
Ha A részhalmaza B-nek, de nem egyenlő vele, akkor azt mondjuk, hogy A valódi részhalmaza B-nek. Jele: $A \subsetneq B$ vagy $B \supsetneq A$.

10. Milyen tulajdonságokkal rendelkezik a ,,részhalmaz" fogalom?

***Reflexivitás**: $A \subset A$*

***Trantitivitás**: $A \subset B \wedge B \subset C \Rightarrow A \subset C$*

***Antiszimmetria**: $A \subset B \wedge B \subset A \Rightarrow A = B$* (a meghatározottsági axióma szerint).

11. Milyen tulajdonságokkal rendelkezik a halmazok egyenlősége?

***Reflexivitás**: $A=A$*

***Tranzitivitás**: $A = B \wedge B = C \Rightarrow A = C$*

***Antiszimmetria**: $A=B \wedge B = A \Rightarrow A = B$*

***Szimmetria**: $A = B \Rightarrow B = A$*

12. Írja le a részhalmaz fogalmát. Milyen jelölést használunk részhalmazok megadására?

Az A halmaz részhalmaza B halmaznak, ha A minden eleme a B halmaznak is eleme. (jele: $A \subset B$)

13. Írja le az üres halmaz fogalmát.

Az üres halmaz az a halmaz, amelynek nincsen eleme (jele: ∅).

14. Igaz-e, hogy csak egy üres halmaz van?

Igen. A meghatározottság axiómája miatt csak egy üres halmaz van.

15. Írja le két halmaz unióját és a megfelelő jelöléseket.

Az A és B halmaz uniója az a halmaz, amelynek pontosan azokat a dolgokat tartalmazza, melyek elemei A-nak vagy B-nek (vagy mindkettőnek). Jele: A ∪ B

16. Írja le halmazrendszer unióját és a megfelelő jelöléseket.

Egy halmazrendszer uniója az a halmaz, amely pontosan azokat a dolgokat tartalmazza, amelyek a halmazrendszer legalább egy elemének elemei.
Jelölései: $\cup A$, $\cup\{A:A\in A\}$ $\cup_{A\in A} A$.

17. Fogalmazza meg a halmazok uniójának alaptulajdonságait.

$A\cup\emptyset=A$
Kommutativitás: $A\cup B = B\cup A$
Asszociativitás: $A\cup(B \cup C)=(A\cup B)\cup C$
Idempotencia: $A\cup A = A$
$A\subset B \Leftrightarrow A\cup B = B$.

18. Definiálja halmazrendszer és két halmaz metszetét, és adja meg a jelöléseket.

Egy halmazrendszer metszete az a halmaz, amely pontosan azokat a dolgokat tartalmazza, amely a halmazrendszer minden elemének elemei. Jelölései:

$\cap A$, $\cap\{A: A\in A\}$ $\cap_{A\in A} A$.

Az *A* és *B* halmaz metszete az a halmaz, amelynek pontosan azok a dolgok az elemei, melyek elemei *A*-nak és *B*-nek is. Jele: $A \cap B$

19. Definiálja a diszjunktság és páronként diszjunktság fogalmát.

Ha A ∩ B =∅, akkor A és B halmazok diszjunktak. Ha egy halmazrendszer bármely két halmaza diszjunkt, akkor a halmazrendszer elemei páronként diszjunktak.

20. Fogalmazza meg a halmazok metszetének alaptulajdonságait.

A ∩ ∅ =∅;
Kommutativitás: A∩B=B∩A

Asszociativitás: $A\cap(B\cap C)=(A\cap B)\cap C$
Idempotencia: $A\cap A=A$ (idempotencia)
$A\subset B \Leftrightarrow A\cap B=A$.

21. Fogalmazza meg az unió és a metszet disztributivitását.

Az unió és a metszet műveletek kölcsönösen disztributívak egymásra nézve.
A metszet disztributivitása az unióra nézve: $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$
Az unió disztributivitása a metszetre nézve: $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

22. Definiálja halmazok különbségét, szimmetrikus differenciáját és komplementerét.

Különbség: $A\backslash B:=\{x\in A : x\notin B\}$
Szimmetrikus differencia: $A \triangle B:=(A\backslash B)\cup(B\backslash A)$
Komplementer: $C_xA := X \setminus A$ (A'-val is jelöljük).

23. Fogalmazza meg a halmazok komplementerének alaptulajdonságait.

- $(A')'=A$
- $\emptyset'=X$
- $X'=\emptyset$
- $A\cap A'=\emptyset$
- $A\cup A'=X$
- $A\subset B\Leftrightarrow B'\subset A'$
- $(A\cup B)'=A'\cap B'$
- $(A\cap B)'=A'\cup B'$

24. Írja le a hatványhalmaz fogalmát. Milyen jelölések kapcsolódnak hozzá?

Minden *A* halmazhoz létezik egy olyan halmazrendszer, amelynek elemei pontosan *A* részhalmazai(Hatványhalmaz-axióma). Jele: $\wp(A)$ vagy 2^A.

25. Definiálja a rendezett pár fogalmát és koordinátáit.

Rendezett pár alatt az (a,b) szimbólumot értjük, ahol $(a,b) = (c,d) \Leftrightarrow a = c \wedge b = d$. A rendezett pár fogalmát ennek megfelelően halmazként definiáljuk: $(a,b) = \{\{a\},\{a,b\}\}$. Az (a,b) rendezett pár első koordinátája a, második b.

26. Definiálja két halmaz Descartes-szorzatát.

Az X,Y halmazok Descartes-szorzatán az $X\times Y:=\{(x,y):x\in X,y\in Y\}$ halmazt értjük.

27. Definiálja a binér reláció fogalmát és adja meg a kapcsolódó jelöléseket.

Az R halmaz binér reláció, ha minden eleme rendezett pár. Ha $(x,y) \in R$, akkor xRy-ként is jelölhetjük, melynek jelentése: x és y között fenáll R reláció.

28. Adjon három példát binér relációra.

kisebb reláció ($a < b$,)
nagyobb reláció ($a > b$)
egyenlőség ($a = b$)

29. Mit jelent az, hogy R reláció X és Y között? Mit jelent az, hogy R egy X-beli reláció?

Ha X és Y halmazokra $R \subset X \times Y$, akkor azt mondjuk, hogy R reláció X és Y között.
Ha X=Y, akkor azt mondjuk, hogy R egy X-beli binér reláció (homogén binér reláció).

30. Definiálja binér reláció értelmezési tartományát és értékkészletét, és adja meg a kapcsolódó jelöléseket.

Az R binér reláció értelmezési tartománya az elemeinek első koordinátáiból álló halmaz. Jele: dmn(R). $dmn(R):=\{x:\exists(x,y)\in R\}$

Az R binér reláció értékkészlete az elemeinek második koordinátáiból álló halmaz. Jele: rng(R). $rng(R):=\{y:\exists(x,y)\in R\}$

31. Definiálja binér reláció kiterjesztését, leszűkítését és leszűkítését egy halmazra és adja meg a kapcsolódó jelöléseket.

Az R binér relációt az S binér reláció kiterjesztésének, illetve S-et az R leszűkítésének (vagy megszorításának) nevezzük, ha $S \subset R$. Ha X egy halmaz, az R reláció X-re való leszűkítésén (vagy megszorításán) az $R_{|X}:=\{(x,y)\in R:x\in X\}$ relációt értjük.

32. Definiálja egy binér reláció inverzét és sorolja fel az inverz három egyszerű tulajdonságát.

Egy binér reláció inverzét elemeinek két koordinátájának megcserélésével kapjuk (jele: R^{-1}).

Formálisan: $R^{-1} := b(b,a)(a,b) \in R\}$
Az inverz három egyszerű tulajdonsága:

- $(R^{-1})^{-1}=R$;
- ha R reláció *X* és *Y* között, akkor R^{-1} reláció *Y* és *X* között;
- *dmn*(R^{-1}) = *rng*(R) és *rng*(R^{-1}) = *dmn*(R).

33. Definiálja halmaz képét és inverz képét binér relációnál és adja meg a kapcsolódó jelöléseket.

Legyen R egy binér reláció és A egy halmaz. Az A halmaz kepe az $R(A):=\{y: \exists x \in A:(x,y) \in R\}$ halmaz. *rng*(A) pontosan akkor üres, ha A és *dmn*(R) diszjunktak. Az A halmaz inverz kepe az R relációnál R-1(A). Ha A={a}, akkor *rng*({a}) helyett *rng*(a)-t írunk.

34. Definiálja binér relációk kompozícióját. Lehet-e a kompozíció üres?

Az R és S binér relációk összetételén (kompozícióján, szorzatán) az $R \circ S:=\{(x,y): \exists z: (x,z)\in S \wedge (z,y)\in R\}$ relációt értjük. Két reláció kompozíciója lehet üres: ez a helyzet, ha *rng*(S) és *dmn*(R) diszjunktak.

35. Fogalmazzon meg három, binér relációk kompozíciójára vonatkozó állítást.

Legyenek R,S,T binér relációk. Ekkor
(1) ha $rng(S) \supset dmn(R)$, akkor $rng(R \circ S) = rng(R)$;

(2) $R \circ (S \circ T) = (R \circ S) \circ T$ (asszociativitás);
(3) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

36. Mit jelent az, hogy egy reláció tranzitív, szimmetrikus, illetve dichotóm? Ezek közül mi az, ami csak a relación múlik?

Az R legyen egy X halmazbeli reláció. Ekkor R:

Tranzitív, ha minden x,y,z-re $(x,y) \in R$ és $(y,z) \in R$ eseten $(x,z) \in R$;

Szimmetrikus, ha minden x,y-ra $(x,y) \in R$ eseten $(y,x) \in R$;

Dichotom, ha minden $x,y \in X$ eseten $(x,y) \in R$ vagy $(y,x) \in R$

Ezek közül a tranzitivitás és a szimmetrikusság függ csak a relációtól.

37. Mit jelent az, hogy egy reláció antiszimmetrikus, illetve trichotóm? Ezek közül mi az, ami csak a relación múlik?

Az *R* legyen egy *X* halmazbeli reláció. Ekkor *R*:

Intranzitív, ha minden x,y,z-re $(x,y) \in R$ és $(y,z) \in R$ eseten $(x,z) \notin R$;

Antiszimmetrikus, ha minden x,y-ra $(x,y) \in R$ és $(y,x) \in R$ eseten x=y;

Trichotóm, ha minden $x,y \in X$ eseten x=y, $(x,y) \in R$ és $(y,x) \in R$ közül pontosan egy teljesül.
Ezek közül az intranzitivitás és az antiszimmetrikusság függ csak a relációtól.

38. Mit jelent az, hogy egy reláció szigorúan antiszimmetrikus, refexív illetve irreflexív? Ezek közül mi az, ami csak a relación múlik?

Az *R* legyen egy *X* halmazbeli reláció. Ekkor *R*:

reflexív, ha minden $x \in X$ eseten $(x,x) \in R$
irreflexív, ha minden $x \in X$ eseten $(x,x) \notin R$
szigorúan antiszimmetrikus, ha minden *x*,*y*-ra $(x,y) \in R$ eseten $(y,x) \notin R$
Ezek közül a szigorúan antiszimmetrikusság függ csak a relációtól.

39. Definiálja az ekvivalenciareláció, illetve az osztályozás fogalmát.

Egy X halmazbeli binér reláció ekvivalenciareláció, ha reflexív, szimmetrikus és tranzitív.
Az X részhalmazainak egy *O* rendszerét X osztalyozasanak nevezzuk, ha *O* páronként diszjunkt nem üres halmazokból álló halmazrendszer, amelyre $\cup O = X$.

40. Mi a kapcsolat az ekvivalenciarelációk és az osztályozások között?

Egy X halmazon értelmezett ekvivalenciareláció X-nek egy osztályfelbontását adja.
Megfordítva, X minden osztályfelbontása egy ekvivalenciarelációt hoz létre.

41. Definiálja a részbenrendezés és a részbenrendezett halmaz fogalmát. Mit mondhatunk egy részbenrendezett halmaz egy részhalmazáról?

Egy X halmazbeli binér reláció részbenrendezés, ha reflexív, antiszimmetrikus és tranzitív.
Ekkor X halmaz részbenrendezett. Ha $x,y \in X$: $x \leq y \vee y \leq x$, akkor x és y elemek

összehasonlíthatóak. Egy részbenrendezett halmaz minden részhalmaza is részbenrendezett, ha a ≤ relációt csak ennek elemei között tekintjük.

42. Definiálja a rendezés, a rendezett halmaz és a lánc fogalmát.

A rendezett X halmaz olyan részbenrendezett halmaz, amely dichotóm, azaz bármely két eleme összehasonlítható. Tehát egy X halmazbeli binér reláció rendezés, ha reflexív, antiszimmetrikus, tranzitív és dichotóm. Láncnak nevezzük egy részbenrendezett halmaz részhalmazát, amely rendezett, ha a ≤ relációt csak ennek elemei között tekintjük.

43. Mondjon példát részbenrendezett de nem rendezett halmazra.

A természetes számok körében az n|m reláció részbenrendezés, de nem rendezés.

44. Definiálja egy relációnak megfelelő szigorú illetve gyenge reláció fogalmát.

Egy X-beli reláció R relációhoz definiálhatunk egy X-beli S relációt úgy, hogy xSy akkor álljon fenn, ha xRy de x≠y, ez az R-nek megfelelő szigorú reláció. Megfordítva, egy X-beli R relációhoz a megfelelő T gyenge relációt úgy definiáljuk, hogy legyen xTy, ha xRy vagy x=y.

45. Definiálja a szigorú részbenrendezést és fogalmazza meg kapcsolatát a részbenrendezéssel.

Szigorú részbenrendezés az a részbenrendezés, amelyet szigorúan rendezünk. Ez tranzitív, irreflexív és szigorúan antiszimmetrikus (jele: <). Ha egy részbenrendezett relációt szigorúan, majd gyengén rendezünk, akkor a kiindulási részbenrendezést kapjuk vissza.

46. Mi az, hogy kisebb, nagyobb, megelőzi, követi? Adja meg a kapcsolódó jelöléseket.

Ha x<y, akkor azt mondjuk, hogy x kisebb, mint y vagy y nagyobb, mint x, illetve hogy x megelőzi y-t vagy y követi x-et. A gyenge reláció eseten hozzátesszük, hogy „vagy egyenlő”.

47. Definiálja az intervallumokat és adja meg a kapcsolódó jelöléseket.

Legyen X egy részbenrendezett halmaz. Ha x≤z és z≤y, akkor azt mondjuk, hogy z az x és y közé esik, ha pedig x<z és z<y, akkor azt mondjuk, hogy z szigorúan x és y köze esik. Az összes ilyen elemek halmazát [x,y], illetve]x,y[jelöli.

48. Mi az hogy közvetlenül követi illetve közvetlenül megelőzi?

Ha egy intervallumban x<y, és nem létezik szigorúan x és y közé eső elem, akkor azt mondjuk, hogy x közvetlenül megelőzi y-t, vagy y közvetlenül követi x-et.

49. Definiálja a kezdőszelet fogalmát és adja meg a kapcsolódó jelöléseket.

Legyen X egy részbenrendezett halmaz. Egy x elemhez tartozó kezdőszeletnek a {y∈ X: y<x} részhalmazt nevezzük. A kezdőszelet jelölése:] ←,x[.

50. Definiálja a legkisebb és a legnagyobb elem fogalmát.

Az X részbenrendezett halmaz legkisebb elemén egy olyan $x \in X$ elemet értünk, amelyre $x \leq y$ minden $y \in X$-re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű. Hasonlóan, X legnagyobb elemén egy olyan x elemet értünk, amelyre $y \leq x$ minden $y \in X$ -re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű.

51. Definiálja a minimális és a maximális elem fogalmát és adja meg a kapcsolódó jelöléseket.

Legyen $x \in X$. Az x-et minimálisnak nevezzük, ha nincs nála kisebb elem, maximálisnak pedig akkor, ha nincs nála nagyobb elem. Maximális és minimális elem lehet több is. Jelölések: min X, max X.

52. Adjon meg olyan részbenrendezett halmazt, amelyben több minimális elem van.

Az $N := \mathbb{N} \setminus \{0,1\}$ halmazon $\forall n, m \in N$ –re az $n \leq m : n \mid m$ reláció részbenrendezés, melyben minden prímszám minimális elem.

Formálisan $\leq := \{(n,m) \in N \times N : n \mid m\}$

53. Adjon meg olyan részbenrendezett halmazt, amelyben nincs maximális elem.

A természetes számok halmaza ilyen a szokásos rendezéssel.

54. Igaz-e, hogy rendezett halmazban a legkisebb és a minimális elem fogalma egybeesik?

Igen. Minimális és maximális elem több is lehet, és hogy ha X rendezett, akkor a legkisebb és a minimális elem fogalma egybeesik, de egyébként nem feltétlenül.

55. Definiálja az alsó és a felső korlát fogalmát.

Egy X részbenrendezett halmaz egy x elemet az Y részhalmaz alsó korlátjának nevezzük, ha minden $y \in Y$-ra $x \leq y$. Ha minden $y \in Y$-ra $y \leq x$ akkor x az Y felső korlátja. Ha letézik alsó illetve felső korlát, akkor azt mondjuk, hogy Y alulról illetve felülről korlátos.

56. Igaz-e, hogy ha egy részbenrendezett halmaz egy részhalmaza tartalmaz a részhalmaz alsó korlátjai közül elemeket, akkor csak egyet?

Igen, ha az alsó korlátok között van olyan, mely eleme a részhalmaznak, úgy csak egy ilyen van.

57. Definiálja az alsó és a felső határ tulajdonságot.

Ha az X részbenrendezett halmaz bármely nem üres, felülről korlátos részhalmazának van felső határa, akkor felső határ tulajdonságúnak nevezzük.

58. Igaz-e, hogy ha egy részbenrendezett halmaz egy részhalmaza tartalmazza a részhalmaz egy alsó korlátját, akkor az a részhalmaznak minimális eleme?

Igen, ha az alsó korlátok között van olyan, mely eleme a részhalmaznak, úgy csak egy ilyen van.

59. Definiálja az infimum és a szuprémum fogalmát.

Amennyiben X halmaz Y részhalmaza alulról korlátos, akkor az alsó korlátok halmazában a legnagyobb elem az infimum (jele: infY). Hasonlóan, ha Y felülről korlátos, akkor a felső korlátok halmazában a legkisebb elem a szuprémum (jele: supY).

60. Definiálja a jólrendezés és a jólrendezett halmaz fogalmát.

Az X részbenrendezett halmazt jólrendezett, részbenrendezése pedig jólrendezés, ha X bármely nem üres részhalmazának van legkisebb eleme.

61. Adjon meg olyan rendezett halmazt, amely nem jólrendezett.

Az egész számok halmaza a szokásos rendezéssel.

62. Adjon példát jólrendezett halmazra.

A természetes számok halmaza jólrendezett a szokásos rendezéssel.

63. Adjon meg két részbenrendezett halmaz Descartes-szorzatán a halmazok részbenrendezései segítségével két részbenrendezést.

Az X és Y részbenrendezett halmazok Descartes-szorzatán értelmezzük az alábbi részbenrendezéseket:

$R_1 := \{((x,y) \in X \times Y, (x',y') \in X \times Y): x \leq x' \wedge y \leq y'\}$
$R_2 := \{((x,y) \in X \times Y, (x' y') \in X \times Y): x \leq x' \vee (x=x' \wedge y \leq y')\}$

64. Két jólrendezett halmaz Descartes-szorzatán a lexikografikus részbenrendezést tekintjük. Mit állíthatunk erről?

Ha X és Y rendezettek, illetve jólrendezettek, akkor X×Y is rendezett, illetve jólrendezett a lexikografikus részbenrendezéssel.

65. Definiálja a függvény fogalmát. Ismertesse a kapcsolódó jelöléseket.

A függvény egy olyan f reláció, amelynél minden x-hez legfeljebb egy olyan y létezik, amelyre (x,y) ∈f. Az f függvény x helyen felvett y értékét szokás f(x) = y-ként illetve fx-szel is jelölni. A függvény hozzárendelési szabályát az f:x→y formulával szokás felírni, ahol a függvény jelölését olykor elhagyják és egyszerűen x → y-t írnak.

66. Mi a különbség a között, hogy $f \in X \to Y$ és hogy $f : X \to Y$?

Az $f \in X \to Y$ esetén $\mathrm{dmn}(f) \subset X$, míg a $f: X \to Y$ esetében $\mathrm{dmn}(f) = X$

67. Mikor nevezünk egy függvényt kölcsönösen egyértelműnek?

Az *f* függvényt kölcsönösen egyértelműnek nevezzük, ha f(x)=y és f(x')=y eseten x=x'. Ez azzal ekvivalens, hogy az f^{-1} reláció függvény. Más néven injektívnek nevezzük a kölcsönösen egyértelmű függvényeket.

68. Igaz-e, hogy az identikus leképezés mindig szürjektív?

Igen, az identikus leképzés definíciójából következik, hogy dmn(𝕀x) = X és rng(𝕀x) = X, így a függvény szürjektív.

69. Definiálja a permutáció fogalmát.

Egy halmaz permutációján a halmaznak önmagára való kölcsönösen egyértelmű leképezését értjük.

70. Igaz-e, hogy két függvény összetétele függvény?

Igen. Ha f és g függvények, akkor $f \circ g$ is az.

71. Mikor állíthatjuk, hogy két függvény összetétele injektív, szürjektív illetve bijektív?

Ha a két függvény injektív, szürjektív illetve bijektív, akkor és csak akkor lesz a két függvény összetétele is injektív, szürjektív valamint bijektív.

72. Mi a kapcsolat függvények és ekvivalenciarelációk között?

Ha az X halmazon adott egy ekvivalenciareláció, akkor az x elemhez az ekvivalenciaosztályát rendelő leképezést kanonikus leképezésnek nevezzük. Megfordítva, ha f: X→Y egy függvény, akkor az $x \sim x'$, ha $f(x)=f(x')$ reláció egy ekvivalenciareláció.

73. Mikor nevezünk egy függvényt monoton növekedőnek illetve monoton csökkenőnek?

Az f: X→Y függvény monoton növekedő, ha $\forall x \in X(\forall y \in X, x \leq y)$: $f(x) \leq f(y)$ teljesül. Monoton csökkenő, ha $\forall x \in X(\forall y \in X, x \leq y)$: $f(x) \geq f(y)$ teljesül.

74. Mikor nevezünk egy függvényt szigorúan monoton növekedőnek illetve szigorúan monoton csökkenőnek?

Az f: X→Y függvény szigorúan monoton növekedő, ha $\forall x \in X(\forall y \in X, x < y)$: $f(x) < f(y)$ teljesül. Szigorúan monoton csökkenő, ha $\forall x \in X(\forall y \in X, x < y)$: $f(x) > f(y)$ teljesül.

75. Mi a kapcsolat a szigorúan monoton növekedő függvények és a kölcsönösen egyértelmű függvények között?

Ha X,Y rendezettek, akkor szigorúan monoton növekedő (illetve csökkenő) függvény nyilván kölcsönösen egyértelmű. Megfordítva, ha X,Y rendezettek, akkor egy f:X→Y kölcsönösen egyértelmű monoton növekedő (illetve csökkenő) leképezés szigorúan monoton növekedő (illetve csökkenő) is, és az inverze is monoton növekedő (illetve csökkenő) f(X)-en.

76. Mit állíthatunk a monoton növekedő függvények inverz függvényéről?

A monoton növekedő függvények inverz függvénye is monoton növekedő.

77. Mit értünk indexhalmaz, indexelt halmaz és indexelt család alatt?

Egy x függvény i helyen felvett értékét néha x_i-vel jelöljük. Ilyenkor gyakran a függvény I értelmezési tartományát indexhalmaznak, az elemeit indexeknek, értékkészletét indexelt halmaznak, az x függvényt magát pedig családnak nevezzük.

78. Definiálja indexelt halmazcsaládok unióját és metszetét.

Ha az értékkészlet elemei halmazok, akkor halmazcsaládról beszélünk. Egy X_i, $i\in I$ halmazcsalád unióját a $\cup_{i\in I}X_i := \cup\{X_i : i\in I\}$ összefüggéssel értelmezzük. Rövidebb jelölése: $\cup_i X_i$. Ha $I\neq\emptyset$, akkor a halmazcsalád metszetét is definiáljuk a $\cap_{i\in I}X_i := \cap\{X_i : i\in I\}$.

79. Fogalmazza meg az indexelt halmazcsaládokra vonatkozó De Morgan szabályokat.

Ha Xi, $i\in I$ az X halmaz részhalmazainak egy nem üres családja (azaz $I\neq\emptyset$), akkor az X-re vonatkozó komplementert vesszővel jelölve:
$(\cup_{i\in I}X_i)' = \cap_{i\in I}X_i'$;
$(\cap_{i\in I}X_i)' = \cup_{i\in I}X_i'$.

80. Definiálja véges sok halmaz Descartes-szorzatát és ismertesse a kapcsolódó jelöléseket.

Véges sok, n darab halmaz Descartes – szorzatát formálisan így definiáljuk:
$X_1 \times X_2 \times \ldots \times X_n := \{(x_1,x_2,\ldots,x_n) : x_1 \in X_1,\ x_2 \in X_2,\ \ldots\ x_n \in X_n\}$
Ha $X_1 = X_2 = \ldots = X_n := X_1 \times X_2 \times \ldots \times X_n$ helyett egyszerűen X^n-t szokás írni.

81. Definiálja a (nem feltétlenül binér) reláció fogalmát és a kapcsolódó jelöléseket.

Az *R* halmaz *n*-változós reláció, ha minden eleme rendezett *n*-es elemekből épül fel.

82. Definiálja tetszőleges indexelt halmazcsalád Descartes-szorzatát és ismertesse a kapcsolódó jelöléseket.

Az X_i, $i\in I$ halmazcsalád $\times_{i\in I}X_i$ Descartes-szorzata a halmazcsaládhoz tartozó összes kiválasztási függvénynek halmaza. Jelölése: $\times_i X_i$.

83. Definiálja a binér, unér és nullér művelet fogalmát és ismertesse a kapcsolódó jelöléseket.

Legyen X egy halmaz. Egy X-beli binér műveleten egy $*:X\times X\to X$ leképezést értünk. Ha $x,y\in X$, akkor $*(x,y)$ a művelet eredménye, x és y pedig az operandusai. Rendszerint a binér művelet
jelét az operandusok közé írjuk: $x*y$. Egy X-beli unér művelet egy $*:X\to X$ leképezés. Mivel $X^{\emptyset}=\{\emptyset\}$, egy nullér művelet egy $*:\{\emptyset\}\to X$ leképezés, ami tulajdonképpen X egy elemének a kijelölését jelenti, operandusa nincs, csak eredménye.

84. Adjon meg egy binér és egy unér műveletet táblázattal.

∧	↑	↓
↑	↑	↓
↓	↓	↓

¬	↑	↓
	↓	↑

85. Hogyan definiálunk műveleteket függvények között?

Ha X és Y halmazok. $*$ binér műveletet pedig Y halmaz elemei között értelmezzük, akkor f, g: X → Y függvények között is értelmezhetjük „pontonként” $*'$ binér műveletet az alábbi módón formálisan:

$\forall x \in X: (f *' g)(x) = f(x) * g(x)$

A két műveletet általában ugyanazzal a jellel szokás jelölni. Analóg módon definiálhatók unér illetve nullér műveletek is függvények között.

86. Adjon példát műveletekre függvények között.

Egy n-bites számítógépen rendszerint rendelkezésre állnak a logikai műveletek n-bites szavakon, azaz a {0,1,...,n-1} halmazt a {↑,↓} halmazba képező függvények halmazán.

87. Definiálja a művelettartó leképezés fogalmát.

Legyenek $*$ és $*'$ binér műveletek rendre X és X’ halmazokon. Egy $\phi: X \to X'$ leképezés művelettartó, ha $\forall x,y \in X :(f *' g)(x) = f(x) * g(x)$

A két műveletet általában ugyanazzal a jellel szokás jelölni. Analóg módon definiálhatók unér illetve nullér műveletek is függvénytereken.

88. Adjon példát művelettartó leképezésre.

Ha a>1, az $x|\to a^x$ leképzés művelettartó és kölcsönösen egyértelmű leképzése az összeadással tekintett valós számoknak a szorzással tekintett pozitív valós számokra.

89. Fogalmazza meg a rekurziótételt.

Legyen X egy halmaz, $a \in X$ és $f:X \to X$ egy függvény. Ha a Peano-axiómák teljesülnek, akkor egy és csak egy olyan $\mathbb{N}$-et X-be képező g függvény létezik, amelyre $g(0)=0$ és $g(n^+)=f(g(n))$ minden $n \in \mathbb{N}$-re.

90. Definiálja a karakterisztikus függvény fogalmát és ismertesse a kapcsolódó jelöléseket.

Az X és Y halmazokra, ha Y ⊂ X, akkor legyen $_{XY}$(x):=1, ha x ∈Y és $_{XY}$(x):=0, ha x ∈X\Y. A $_{XY}$ függvény az Y halmaz X-en értelmezett karakterisztikus függvénye.

Formalizálva $_{XY}$(x) : = $\begin{cases} 1, ha\ x \in \mathrm{Y} \\ 0, ha\ x \in \mathrm{X}\backslash\mathrm{Y} \end{cases}$

91. Definiálja a baloldali semleges elem, a jobboldali semleges elem és a semleges elem fogalmát.

A (G,∗) grupoid esetén G halmaz egy s elemét bal, illetve jobb oldali semleges elemnek nevezzük, ha s ∗ g = g, illetve g ∗ s = g minden g ∈G-re. Ha s bal és jobb oldali semleges elem is, akkor semleges elemnek nevezzük.

92. Definiálja a félcsoport, a balinverz, a jobbinverz és az inverz fogalmát és ismertesse a kapcsolódó jelöléseket.

Ha a ∗ binér művelet *G* halmazon asszociatív (azaz ∀*x*, *y*, *z* ∈*G*: (*x*∗*y*)∗*z* = *x* ∗ (*y* ∗ *z*)), akkor (*G*,∗) grupoid félcsoport.

Ha (*G*,∗) félcsoportban s semleges elem, akkor *g*, g^* ∈ *G*-re *g* ∗ g^* = s esetén *g* a g^* balinverze, g^* pedig a *g* jobbinverze. Ha g^* a *g*-nek bal- és jobbinverze is, akkor g^* a *g* inverze.

93. Igaz-e, hogy egy egységelemes multiplikatív félcsoportban ha h-nak és g-nek van inverze, akkor hg-nek is, és ha igen, mi?

Igen. Ha g-nek g^* az inverze, és h-nak h^* az inverze, akkor a g∗h inverze h^* ∗ g^*.

94. Definiálja a csoport és az Abel-csoport fogalmát.

Ha egy semleges elemes félcsoport minden elemének van inverze, akkor csoport. Ha a ∗ binér műveletet a *G* halmazon és ∀*g,h* ∈ *G*: *g* ∗ *h* = *h* ∗ *g* teljesül, akkor *g* és *h* felcserélhetőek. Ha *G* bármely két eleme felcserélhető, akkor a ∗ művelet kommutatív. A kommutatív csoportok az Abel-csoportok.

95. Igaz-e, hogy ha X tetszőleges halmaz, akkor℘(X), ∩ egy egységelemes félcsoport?

Igen, (℘(X), ∩) kommutatív egységelemes félcsoport.

96. Igaz-e, hogy ha X tetszőleges halmaz, akkor(℘(X), ∪)egy csoport?

Nem igaz, (℘(X), ∪) kommutatív egységelemes félcsoport.

97. Igaz-e, hogy ha X tetszőleges halmaz, akkor (℘(X), Δ) egy félcsoport?

Igaz, mivel (℘(X), Δ) Abel-csoprt.

98. Igaz-e, hogy ha X tetszőleges halmaz, akkor az X-beli binér relációk a kompozícióval egységelemes félcsoportot alkotnak?

Igen, mert a kompozíció művelet asszociatív, hiszen R, Q, S relációkra $(R \circ Q) \circ S = R \circ (Q \circ S)$, az $\mathbb{I}_x = \{(x,x) \in X \times X : x \in X\}$ pedig egységelem, mivel $\forall R \in X \times X$-re $R \circ \mathbb{I}_x = \mathbb{I}_x \circ R = R$.

99. Igaz-e, hogy ha X tetszőleges halmaz, akkor az X-et X-re képező bijektív leképezések a kompozícióval, mint művelettel csoportot alkotnak?

Igaz. Ha csak az összes injektív, illetve az összes szürjektív leképezéseket tekintjük, akkor is egységelemes félcsoportot kapunk. Az összes bijektív leképezések csoportot alkotnak.

100. Fogalmazza meg a természetes számokra a ≤ reláció és a műveletek kapcsolatát leíró tételt.

Ha $k,m,n \in \mathbb{N}$, akkor:

(1) n^+ közvetlenül követi n-et;
(2) $m \leq n \Leftrightarrow m+k \leq n+k$;
(3) $k \neq 0 : m \leq n \Leftrightarrow m \cdot k \leq n \cdot k$;
(4) $m < n \Leftrightarrow m+k < n+k$;
(5) $k \neq 0$: esetén $m < n \Leftrightarrow m \cdot k < n \cdot k$;
(6) ha $m \cdot k = n \cdot k \wedge k \neq 0 \Rightarrow m = n$ (egyszerűsítési /törlési szabály).

101. Definiálja a véges sorozatokat.

Ha $n \in \mathbb{N}$, akkor a $[0,n] \subset \mathbb{N}$ vagy $[1,n] \subset \mathbb{N}^+$ halmazon értelmezett függvényeket véges sorozatnak nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0,x_1,...,x_n$ vagy x_i, $i = 0,1,2,...,n$.

102. Fogalmazza meg az általános rekurziótételt.

Legyen adott X halmaz és egy olyan f függvény, amelynek értékkészlete X részhalmaza, értelmezési tartománya pedig az összes olyan függvények halmaza, amelyek értékkészlete X részhalmaza, értelmezési tartománya pedig $\mathbb{N}$ valamely kezdőszelete. Ekkor egyértelműen létezik egy $g: \mathbb{N} \to X$ függvény, amelyre $\forall a \in \mathbb{N}$: $g(a) = f(g|_{]\leftarrow,a[})$ teljesül.

103. Hogyan használható az általános rekurziótétel a Fibonacci-számok definiálására?

Legyen $X = \mathbb{N}$, és legyen az $n|\to n^-$ leképezése $\mathbb{N}^+$-nak $\mathbb{N}$-re az $n|\to n^+$ leképezés inverze, $f(\emptyset)=0$, $f(\{(0,k)\}) := 1$ bármely $k \in \mathbb{N}$-re, és ha $n>1$, $h:] \leftarrow,n[\to \mathbb{N}$ egy függvény, akkor legyen $f(h) := h(n^-) + h(n^{--})$. ($n=\min(\mathbb{N} \setminus dmn(h))$)

104. Definiálja véges sok elem szorzatát félcsoportban és egységelemes félcsoportban.

Ha G egy félcsoport, $x: \mathbb{N}^+ \to G$ egy sorozat, akkor az általános rekurziótételt alkalmazva definiálhatjuk a $\prod_{k=1}^{n} x_k = 1$ és $\prod_{k=1}^{n+1} x_k = (\prod_{k=1}^{n} x_k) \cdot x_{(n+1)}$ szorzatokat úgy, hogy . Ha G egységelemes félcsoport e egységelemmel, akkor $\prod_{k=0}^{0} x_k = e$.

105. Fogalmazza meg a hatványozás két tulajdonságát félcsoportban és egységelemes félcsoportban.

Egy tetszőleges G multiplikatív félcsoportra minden g ∈G-re teljesülnek az alábbiak minden m, n ∈$\mathbb{N}^+$-ra (egységelemes G félcsoport esetén minden m,n ∈$\mathbb{N}$-re):

- $g^{m+n} = g^m \cdot g^n$
- $(g^m)^n = g^{mn}$

106. Fogalmazza meg a hatványozásnak azt a tulajdonságát, amely csak felcserélhető elemekre érvényes.

Ha g,h a G félcsoport felcserélhető elemei, akkor indukcióval $(gh)^n=g^nh^n$ minden n∈$\mathbb{N}^+$-ra, ha G egységelemes félcsoport, akkor minden n∈$\mathbb{N}$-re.

107. Hogyan értelmeztük $\sum_{(a\in A)} x_a$ jelölést?

Ha G egy kommutatív félcsoport, x:A → G egy tetszőleges függvény és van olyan φ:{k ∈$\mathbb{N}$: 1 ≤ k ≤ n} → A kölcsönösen egyértelmű leképezés (n ∈$\mathbb{N}^+$-ra, illetve nullelemes G félcsoport esetén n ∈$\mathbb{N}$-re}, amely A-ra képez, akkor minden ilyen leképezésre $\sum_{k=1}^{n} x_{\varphi(k)}$ ugyanaz – ez az általános kommutativitás tétele. Ezt a közös értéket $\sum_{(a\in A)} x_a$ – val is jelölhetjük.

108. Mikor mondjuk, hogy egy binér művelet kompatibilis egy osztályozással? Adjon ekvivalens megfogalmazást, és Definiálja a műveletet az osztályok között.

Legyen adott *X* halmaz és az *R* mint *X*-beli binér reláció, továbbá *X* egy osztályozása, illetve a megfelelő ~ ekvivalenciareláció. Az *R* reláció kompatibilis az osztályozással, illetve az ~ ekvivalenciarelációval, ha $x\sim x' \wedge y \sim y' \Rightarrow (xRy \Rightarrow x'Ry')$. (Az ekvivalenciareláció tulajdonságai miatt $x\sim x' \wedge y \sim y' \Rightarrow \big(xRy \Rightarrow (x'Ry \wedge xRy')\big)$ teljesülése is elegendő.)

Ha az *R* reláció kompatibilis az osztályozással, akkor az ekvivalenciaosztályok terén, $\tilde{X}$-on bevezethető egy $\tilde{R}$ relációt az $xRy \Rightarrow \tilde{x}\tilde{R}\tilde{y}$ definícióval. Általában $\tilde{R}$ helyett *R*-et írunk.

109. Definiálja a nullgyűrű és a zérógyűrű fogalmát.

A nullgyűrű olyan gyűrű, amelynek csak egyetlen eleme van, ez pedig szükségszerűen a 0 nullelem. (Különben a gyűrű R alaphalmaza nem alkotna az összeadással Abel-csoportot, de még csoportot se.) A zérógyűrűben bármely két elem szorzata 0 nullelem.

110. Definiálja a bal és jobb oldali nullosztó és a nullosztópár fogalmát.

Ha x és y egy gyűrű nullától különböző elemei és x · y = 0, akkor x és y egy nullosztópár, ahol x a bal oldali, y pedig a jobb oldali nullosztó.

111. Definiálja az integritási tartomány fogalmát.

Egy legalább kételemű gyűrű nullosztómentes, ha nincsenek benne nullosztópárok. A kommutatív nullosztómentes gyűrű az integritási tartomány.

112. Definiálja a rendezett integritási tartomány fogalmát.

R-et rendezett integritási tartománynak nevezzük, ha rendezett halmaz, integritási tartomány, és
(1) ha x,y,z∈R és x≤y, akkor x+z≤y+z (az összeadás monoton);
(2) ha x,y∈R és x,y≥0, akkor x·y≥0 (a szorzás monoton).

113. Fogalmazzon meg szükséges és elégséges feltételt arra vonatkozóan, hogy egy integritási tartomány rendezett integritási tartomány legyen.

Egy R rendezett halmaz, amely integritási tartomány akkor és csak akkor rendezett integritási tartomány, ha az összeadás és szorzás is szigorúan monoton.
Formálisan: $\forall x,y,z \in \mathbb{R}$ (x<y): x+z < y+z (az összeadás szigorúan monoton)
$\forall x,y \in \mathbb{R}$ (x,y >0): x·y>0 (a szorzás szigorúan monoton)

114. Fogalmazza meg a rendezett integritási tartományban az egyenlőtlenségekkel való számolás szabályait leíró tételt.

Legyen R rendezett halmaz, amely integritási tartomány. Ekkor teljesül az alábbi 5 szabály $\forall x,y,z \in \mathbb{R}$-re:
(1) ha x>0, akkor –x<0, és ha x<0, akkor –x>0;
(2) ha x<y és z>0, akkor xz<yz;
(3) ha x<y és z<0, akkor xz>yz;
(4) ha x≠0, akkor x^2>0; speciálisan, ha van egységelem, akkor az pozitív;
(5) ha 1 az egységelem, 0<x<y, és y-nak is van multiplikatív inverze, akkor $0 < \frac{1}{y} < \frac{1}{x}$.

115. Definiálja a test fogalmát és adjon három példát testre.

Egy F gyűrűt ferdetestnek nevezünk, ha a nullelemet 0-val jelölve F\{0} a szorzással csoport. Ha a szorzás kommutatív, akkor a ferdetestet testnek nevezzük.
Példák testre: $\mathbb{Q}$, valós számok, komplex szamok.

116. Definiálja a rendezett test fogalmát és adjon példát olyan testre, amely nem tehető rendezett testté.

A rendezett test olyan test, amely rendezett integritási tartomány is.
A {0,1} halmaz a 0 + 0 = 1 + 1 = 0, 0 + 1 = 1 + 0 = 1 összefüggésekkel megadott összeadással és a 0 · 0 = 0 · 1 = 1 · 0 = 0, 1 · 1 = 1 összefüggésekkel megadott szorzással kételemű test, de nincsen olyan rendezés, amellyel rendezett test lenne, mert a rendezett testben 1>0 és -1<0, de a fenti kételemű testben -1 = 1.

117. Fogalmazza meg az arkhimédeszi tulajdonságot.

Az F rendezett test arkhimédeszi tulajdonságú, ha $\forall x,y \in F$, x,y≥ 0 ($\exists y \in \mathbb{N}$): nx ≥y.

118. Mi a kapcsolata az arkhimédeszi tulajdonságnak a felső határ tulajdonsággal?

Egy felső határ tulajdonságú test mindig arkhimédészi tulajdonságú is.

119. Fogalmazza meg a racionális számok felső határ tulajdonságára és az arkhimédeszi tulajdonságára vonatkozó tételt.

A racionális számok rendezett teste arkhimédészi tulajdonságú, de nem felső határ tulajdonságú.

120. Fogalmazza meg a valós számok egyértelműségét leíró tételt.

Legyen $\mathbb{R}'$ és $\mathbb{R}''$ két felső határ tulajdonságú test. Ekkor létezik egy φ kölcsönösen egyértelmű leképezése $\mathbb{R}'$-nek $\mathbb{R}''$-re, amely monoton növekedő, összeadás- és szorzástartó. Egy felső határ tulajdonságú testet a valós számok testének nevezzük, az előbbiek értelmében legfeljebb egy ilyen van.

121. Definiálja a bővített valós számokat.

A bővített valós számok halmaza: $\mathbb{R}:= \mathbb{R}'$(' = feslsővonal) $\cup\{+\infty,-\infty\}$.

122. Fogalmazza meg a valós számok létezését leíró tételt.

Létezik felső határ tulajdonságú test. Egy felső határ tulajdonságú testet a valós számok testének nevezzük.

123. Fogalmazza meg a valós számok körében a gyökvonásra vonatkozó tételt.

Minden $x\geq 0$ valós számhoz és $n\in\mathbb{N}^+$ természetes számhoz pontosan egy olyan $y\geq 0$ valós szám található, amelyre $y^n=x$. Az y számot az x n-edik gyökének nevezzük és $\sqrt[n]{x}$-el jelöljük (n=2 esetén $\sqrt{x}$-el is) vagy $x^{\frac{1}{n}}$-el jelöljük.

124. Fogalmazza meg a valós számok körében a szorzat gyökére vonatkozó állítást.

Ha a és b nemnegatív számok és $n\in\mathbb{N}^+$, akkor $\sqrt[n]{ab} = \sqrt[n]{a}\sqrt[n]{b}$.

125. Definiálja a komplex számok halmazát a műveletekkel.

A komplex számok halmaza $\mathbb{C} = \mathbb{R}\times\mathbb{R}$, a valós számpárok halmaza az $(x,y)+(x',y')=(x+x',y+y')$ összeadással és az $(x,y)\cdot(x',y')=(xx'-y'y,y'x+yx')$ szorzással, mint műveletekkel. A $\mathbb{C}$ test a fenti műveletekkel: a nullelem a (0,0) pár, az (x,y) pár additív inverze a (-x,-y) pár, egységelem az (1,0) pár, és a nullelemtől különböző (x,y) pár multiplikatív inverze az $\left(\frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}\right)$ pár.

126. Adja meg $\mathbb{R}$ beágyazását $\mathbb{C}$ -be.

Ha $x,x'\in\mathbb{R}$, akkor $(x,0)+(x',0)=(x+x',0)$ és $(x,0)\cdot(x',0)=(x\cdot x',0)$, így az $x\rightarrow(x,0)$ leképezés injektív, összeadás- és szorzástartó leképezése $\mathbb{R}$-nek $\mathbb{C}$-be, ezért az összes $(x,0)\in\mathbb{C}$, $x\in\mathbb{R}$ alakú komplex számok halmazát azonosíthatjuk $\mathbb{R}$-rel.

127. Definiálja i-t, komplex szám valós és képzetes részét, konjugáltját és a képzetes számok fogalmát.

A $(0,1)$ komplex számot az *i* jelöli, segítségével a tetszőleges (x,y) komplex szám $x+iy$ alakba írható. Ez a komplex számok algebrai alakja, ami természetesen egyértelmű felírás.
Ha $z=x+iy\in\mathbb{C}$, ahol $x,y\in\mathbb{R}$, akkor az x a z valós része (jele: $\Re(z)$ vagy $\mathrm{Re}(z)$), az y pedig a z képzetes része (jele: $\Im(z)$ vagy $\mathrm{Im}(z)$).
A fenti algebrai alakban felírt z komplex szám konjugáltja a $\bar{z}=\overline{x+\imath y}=x-iy\in\mathbb{C}$ szám.
Ha egy komplex szám képzetes része nulla, akkor valósnak nevezzük. Ha a valós része nulla és a képzetes része nem nulla, akkor képzetesnek nevezzük.

128. Fogalmazza meg a komplex konjugálás tulajdonságait.

Ha $z, w \in \mathbb{C}$, akkor teljesülnek az alábbi konjugálásra vonatkozó összefüggések:

- $\bar{\bar{z}} = z$
- $\overline{z+w} = \bar{z} + \bar{w}$
- $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $z + \bar{z} = 2\Re(z)$
- $z - \bar{z} = 2i\Im(z)$

129. Definiálja komplex szám abszolút értékét. Milyen tételt használt?

A komplex számokat a sík origóból kiinduló vektorainak tekintve a komplex számok abszolút értéke ennek a vektornak a hossza. Azaz az (x,y) ∈ ℂ szám abszolút értéke : |(x,y)| = $\sqrt{x^2+y^2}$. Ehhez felhasználtuk azt az analízisbeli tételt, mely szerint x ∈ ℝ, x≥0, n ∈$\mathbb{N}^+$: ! ∃y ∈$\mathbb{R}_0^+$(y^n = x). Ekkor az y szám n. gyöke, jele: y = $\sqrt[n]{x}$.

130. Fogalmazza meg komplex számok abszolút értékének tulajdonságait.

Ha $z, w \in \mathbb{C}$ és $x \in \mathbb{R}$, akkor teljesülnek az alábbi abszolút értékre vonatkozó összefüggések:

- $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$, ha $z \neq 0$
- $|(x,0)| = |x|$ (Valós számok abszolút értéke a megszokott.)
- $z \cdot \bar{z} = |z|^2$
- $|0| = 0$
- $|z| > 0$, ha $z \neq 0$
- $|\bar{z}| = |z|$
- $|z \cdot w| = |z| \cdot |w|$
- $|\Re(z)| \leq |z|$
- $|\Im(z)| \leq |z|$
- $|z| \leq |\Re(z)| + |\Im(z)|$
- $|z + w| \leq |z| + |w|$ (A háromszög-egyenlőtlenség.)
- $||z| - |w|| \leq |z - w|$

131. Definiálja komplex számokra a sgn függvényt és fogalmazza meg tulajdonságait.

Az előjel függvény a komplex számokon tetszőleges $z \in \mathbb{C}$-re: $\operatorname{sgn}(z) := 0$, ha z= 0 és $\operatorname{sgn}(z) := \frac{z}{|z|}$ egyébként. A valós számokra visszakapjuk a valós számok halmazán definiált *sgn* függvényt. Továbbá teljesülnek a következő tulajdonságok tetszőleges $z \in \mathbb{C}$-re:

- $\operatorname{sgn}(\bar{z}) = \overline{\operatorname{sgn}(z)}$
- $|\operatorname{sgn}(z)| = 1$, ha $z \neq 0$

132. Definiálja komplex számok trigonometrikus alakját és argumentumát.

Ha 0≠z ∈ℂ, akkor van olyan t valós szám, amelyre sgn(z) = cos t + i sin t. Ha ez az összefüggés fennáll t-re, akkor a t + 2kπ, k ∈ℤ számokra is, és csak ezekre.
Ekkor z =|z| · (cos t + i sin t), ez a komplex szám trigonometrikus alakja.
Ha z = 0, akkor akármilyen t ∈ ℝ szám választható. Ha z≠0 ∈ℂ, akkor z argumentuma (jele: arg(z)) az az egyetlen t valós szám, amelyre –π<t≤π és sgn(z) = cos t + i sin t; ez az egyetlen t valós szám a]–π; π] intervallumon, amelyre z = |z| · (cos t + i sin t).

133. Írja fel két komplex szám szorzatát és hányadosát trigonometrikus alakjuk segítségével.

Legyen z,w ∈ ℂ trigonometrikus alakjukban z:=|z| · (cos t + i sin t) és w :=|w| · (cos s + i sin s), ahol t,s ∈ ℝ. Ekkor z és w szorzata valamint hányadosa a trigonometrikus alakjuk segítségével:

- z · w = |z| · (cos t + i sin t) · |w| · (cos s + i sin s)
  = |zw| · (cos t cos s – sin t sin s + i(cos t sin s + cos s sin t))
  = |zw| · $(\cos(t+s) + i\sin(t+s))$

- $\frac{z}{w} = \frac{z\cdot\bar{w}}{|w|^2} = \frac{|z|}{|w|}\cdot(\cos(t-s) + i\sin(t-s))$, figyelembe véve, hogy $w \neq 0$.

134. Ha n ∈ℕ⁺ és w ∈ ℂ, írja fel a z = w egyenlet összes megoldását.

$z_k = \sqrt[n]{|w|}\cdot\left(cos\left(\frac{t+2k\pi}{n}\right) + i\,sin\left(\frac{t+2k\pi}{n}\right)\right)$ k = 0,1, … ,n – 1

135. Írja fel az n-edik komplex egységgyököket. Mit értünk primitív n-edik egységgyök alatt?

A $\varepsilon^n = 1$ egyenlet megoldásai az n. komplex egységgyökök. Ekkor $|\varepsilon| = 1$ és t =0, így:
$\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$, k = 0,1,…, n -1
Azok az n. egységgyökök, amelyek hatványaként az összes többi előáll, az úgynevezett primitív n. komplex egységgyökök. (Például n≥2 esetén ε1 és εn-1 mindig primitív egységgyökök.)

136. Ha n ∈ ℕ⁺ és w ∈ ℂ, írja fel a z^n = w egyenlet összes megoldását az n-edik egységgyökök segítségével.

$z_k = z \cdot \varepsilon_k$, k = 0,1,…,n – 1

137. Fogalmazza meg az algebra alaptételét.

Ha n∈ℕ⁺, valamint $c_0,c_1,\ldots,c_n$ komplex számok, $c_n \neq 0$, akkor van olyan z komplex szám, amelyre $\sum_{k=0}^{n} c_k z^k = 0$ .Másként fogalmazva, minden legalább elsőfokú komplex együtthatós algebrai egyenletnek van komplex gyöke.

138. Definiálja halmazok ekvivalenciáját és sorolja fel tulajdonságait.

Az X és Y halmazok ekvivalensek, ha létezik X-et Y-ra leképező injektív leképezés. Jelölése: X ∼ Y. Amennyiben X, Y, és Z halmazok, akkor teljesülnek az alábbi tulajdonságok:

- Reflexivitás: X ∼ X
- Szimmetria: X ∼ Y ⇒ Y ∼ X
- Tranzitivitás: X ∼ Y ∧ Y ∼ Z ⇒ X ∼ Z

139. Ha az X és X' illetve Y és Y' halmazok ekvivalensek, milyen más halmazok ekvivalenciájára következtethetünk még ebből?

Ha X ∼ X' és Y ∼ Y', akkor X×Y ∼ X' × Y' az (x,y) →(f(x),g(y)) leképzéssel.

140. Definiálja a véges és a végtelen halmazok fogalmát.

Egy X halmaz véges, ha valamely n számra ekvivalens {1,2,…,n} a halmazzal, egyébként végtelen.

141. Definiálja egy véges halmaz elemeinek számát. Hogyan jelöljük? Mit használt fel a definícióhoz?

Az az egyértelműen meghatározott természetes szám, mely egy adott X véges halmaz ekvivalens {1,2,…,n}-nel, az X halmaz elemeinek száma, más néven számossága.

Jelölése: #(X) vagy card(X).

A definícióhoz felhasználtuk, hogy minden halmaz legfeljebb egy n-re ekvivalens {1,2,…,n} halmazzal.

142. Fogalmazza meg a véges halmazok és elemszámuk tulajdonságait leíró tételt.

Legyenek X és Y halmazok. Ekkor teljesülnek rájuk a következő tulajdonságok:

(1) Ha X véges és $Y \subset X$, akkor Y is véges, és $\#(Y) \leq \#(X)$;
(2) Ha X véges és $Y \subsetneq X$, akkor $\#(Y) < \#(X)$;
(3) Ha X és Y végesek és diszjunktak, akkor $X \cup Y$ is véges, és $\#(X \cup Y) = \#(X) + \#(Y)$;
(4) Ha X és Y végesek, akkor $\#(X \cup Y) + (X \cap Y) = \#(X) + \#(Y)$;
(5) Ha X és Y végesek, akkor $X \times Y$ is véges, és $\#(X \times Y) = \#(X) \cdot \#(Y)$;
(6) Ha X és Y végesek, akkor X^Y is véges, és $\#(X^Y) = \#(X)^{\#(Y)}$;
(7) Ha X véges halmaz, akkor $\wp(X)$ is véges, és $\#(\wp(X)) = 2^{\#(X)}$;
(8) Ha X véges és f függvény X-et Y-ra képezi, akkor Y is véges, $\#(Y) \leq \#(X)$, és ha f nem injektív, akkor $\#(Y) < \#(X)$.

143. Fogalmazza meg a skatulyaelvet.

Ha X és Y véges halmazok, és $\#(X) > \#(Y)$, akkor $f: X \to Y$ leképezés nem lehet injektív.

144. Mit mondhatunk véges halmazban minimális és maximális elem létezéséről?

Részbenrendezett halmaz bármely nem üres véges részhalmazának van maximális és minimális eleme.

145. Mit mondhatunk egy véges halmaz összes permutációinak számáról?

Ha egy A halmaz ekvivalens {1,2,...,n}-nel, akkor permutációinak halmaza ekvivalens {1,2,...,n} permutációinak halmazával. Ha $A=\{a_1,a_2,...,a_n\}$ és $p_1,p_2,...,p_n$ az {1,2,...,n} egy permutációja, akkor az A megfelelő permutációja az $a_i \mid \to a_{pi}$ leképzés. Így A permutációinak száma csak n = #(A)-tól függ. Jelölje ezt a számot P_n. $P_n=n!$.

146. Mit értünk egy véges halmaz variációin és mit mondhatunk az összes variációk számáról?

Az A halmaz elemeiből készíthető, különböző tagokból álló $a_1,a_2,\dots,a_n$ sorozatokat, azaz {1,2,…,n}-t A-ba képező kölcsönösen egyértelmű leképzéseket az A halmaz k-ad osztályú variációinak nevezzük. Ha A véges halmaz, #(A)=n, akkor ezek V_n^k száma megegyezik az {1,2,..,k}-t {1,2,…,n}-be képező kölcsönösen egyértelmű leképezések számával.

$V_n^k = \frac{\mathrm{n!}}{(\mathrm{n-k})!} = \mathrm{n}(\mathrm{n}-1)\dots(\mathrm{n}-\mathrm{k}+1)$, ha $\mathrm{k} \leq \mathrm{n}$, egyébként 0.

147. Definiálja az ismétléses variációk fogalmát. Mit mondhatunk egy véges halmaz összes ismétléses variációinak számáról?

Az A halmaz elemeiből készíthető $a_1,a_2,\dots,a_k$ sorozatokat, azaz {1,2,…,k}-t A-ba képező leképezéseket az A halmaz k-ad osztályú ismétléses variációinak nevezzük. Ha A véges halmaz, #(A) = n, akkor ezek ${}^{\mathrm{i}}V_n^k$ számáról (a $V_n^{k,i}$ jelölés is szokásos) már tudjuk, hogy n^k.

148. Mit értünk egy véges halmaz kombinációin és mit mondhatunk az összes kombinációk számáról?

Ha k ∈ℕ, akkor A halmaz k elemű részhalmazait az A halmaz k-ad osztályú kombinációinak nevezzük. Ha A véges halmaz, akkor #(A)=n, akkor ezek C_n^k száma megegyezik a {1,2,…,n} halmaz k elemű részhalmazainak számával. $C_n^k = \frac{n!}{k!(n-k)!} = \binom{n}{k}$, ha k≤n, egyébként 0.

149. Mit értünk egy véges halmaz ismétléses kombinációin és mit mondhatunk az összes ismétléses kombinációk számáról?

Ha k ∈ℕ, akkor A halmazból k elemet kiválasztva, de ismétléseket is megengedve, nem tekintve a sorrendre, az A halmaz k-ad osztályú ismétléses kombinációit kapjuk. Pontosabban, tekintsük mindazokat az f:A→ℕ függvényeket, amelyek csak véges sok helyen vesznek fel nem nulla értéket, és ezen értékek összege k; ezek az A halmaz ismétléses kombinációi. Ha A véges halmaz, akkor #(A)=n, így feltehetjük, hogy A={1,2,..,n}. Minden g:{1,2,..,k}→{1,2,...,n} monoton növekedő hozzárendelve az f(j) = #(g^{-1}(j)) függvényt, kölcsönösen egyértelmű megfeleltetést kapunk. *A* ismétléses kombinációi és az {1,2,...,k}-t {1,2,...,n}-be képező monoton növekedő függvények között, így ezek száma az A ismétléses kombinációinak ${}^{\mathrm{i}}C_n^k$ száma. ${}^{\mathrm{i}}C_n^k = \binom{n+k-1}{k}$

150. Mit értünk egy véges halmaz ismétléses permutációin és mit mondhatunk az összes ismétléses permutációk számáról?

Ha $r,i_1,i_2,\dots,i_r \in \mathbb{N}$, akkor az $a_1,a_2,\dots,a_r$ (különböző) elemek $i_1,i_2,\dots,i_r$ ismétlődésű ismétléses permutációi az olyan $n=i_1+i_2+\dots+i_r$-tagú sorozatok, amelyekben az a_j elem i_j-szer fordul elő. Az $A=\{a_1,a_2,\dots,a_r\}$ jelöléssel ezek olyan {1,2,...,n}-et A-ba képező leképzések, amelyeknél a_j teljes inverz kepe i_j elemű.

$$P_n^{i_1,i_2,\dots,i_r} = \frac{n!}{i_1!\,i_2!\dots i_r!}$$

151. Fogalmazza meg a binomiális tételt.

Legyenek x,y egy R kommutatív egységelemes gyűrű elemei, n∈ℕ Ekkor:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

152. Írja fel a Pascal-háromszög első 8 sorát.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1

153. Mennyi a binomiális együtthatók összege, illetve váltakozó előjellel vett összege?

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \text{ és } \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

154. Fogalmazza meg a polinomiális tételt.

Legyen $r \in \mathbb{N}$, $x_1, x_2, \dots, x_r$ egy R kommutatív egységelemes gyűrű elemei, $n \in \mathbb{N}$. Ekkor:

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{i_1+i_2+\cdots+i_r=n} P_n^{i_1,i_2,\dots,i_r} \cdot x_1^{i_1} \cdot x_2^{i_2} \dots x_r^{i_r}$$

155. Fogalmazza meg a logikai szita formulát.

Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X-en értelmezett, értékeket egy Abel-csoportban felvevő függvény. Ha $1 \le i_1 < i_2 < \cdots < i_r \le k$, akkor legyen:

$$Y_{i_1,i_2,\dots,i_r} = X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}$$

Legyen továbbá:

$$S = \sum_{x \in X} f(x)$$

$$S_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le k} \; \sum_{x \in Y_{i_1,i_2,\dots,i_r}} f(x)$$

Valamint legyen:

$$S_0 = \sum_{x \in X \setminus \bigcup_{i=1}^{k} X_i} f(x)$$

Ekkor:

$$S_0 = S - S_1 + S_2 - S_3 + \cdots + (-1)^k S_k$$

156. Definiálja a természetes számok körében az oszthatóságot és adja meg a jelölését.

Az m természetes számot az n természetes szám osztójának, az n-et pedig m többszörösének nevezzük, illetve azt mondjuk, hogy n osztható m-el, ha van olyan k természetes szám, hogy n=mk.
jelölése: m|n.

157. Sorolja fel a természetes számok körében az oszthatóság alaptulajdonságait.

A természetes számok körében
(1) ha m|n és m'|n', akkor mm'|nn';
(2) a nullának minden természetes szám osztója;
(3) a nulla csak saját magának osztója;
(4) az 1 minden természetes számnak az osztója;
(5) ha m|n, akkor mk|nk minden k $\in\mathbb{N}$-re;
(6) ha k$\in\mathbb{N}^+$ és mk|nk, akkor m|n;
(7) ha m|n_i és $k_i\in\mathbb{N}$, (i=1,2,...,j), akkor m|$\sum_{i=1}^{j} k_i n_i$;
(8) bármely nem 0 természetes szám bármely osztója kisebb vagy egyenlő, mint a szám;
(9) az | reláció reflexív, tranzitív és antiszimmetrikus, azaz részbenrendezés.

158. Definiálja a természetes számok körében a prímszám és a törzsszám fogalmát. Mi a kapcsolat a két fogalom között?

Az n>1 természetes szám törzsszám, ha az 1-en és saját magán kívül nincs más osztója, azaz csak triviális módon, 1·n = n · 1 alakban írható fel természetes számok szorzataként.

A p>1 természetes számot prímszámnak nevezzük, ha p|km (k,m$\in\mathbb{N}$) eseten p|k vagy p|m.

A törzsszámok és prímszámok halmaza egyenlő.

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

Egy R egységelemes integritási tartományban, ha a,b$\in$R, akkor b az a osztója, vagy *a* a *b* többszöröse, azaz a osztható b-vel, ha van olyan c$\in$R, hogy a=bc.

jelölése b|a.

160. Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

Egy egységelemes integritási tartomány elemei körében
(1) ha a|b és a'|b', akkor aa'|bb';
(2) a 0-nak minden természetes szám osztója;
(3) a 0 csak saját magának osztója;
(4) az 1 minden elemnek az osztója;
(5) ha b|a, akkor bc|ac minden c $\in$R -re;
(6) ha bc|ac és c≠0, akkor b|a;
(7) ha b|a_i és $c_i\in$R, (i=1,2,...,j), akkor *b*|$\sum_{i=1}^{j} c_i a_i$
(8) az | reláció reflexív és tranzitív.

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

Ha egy R egységelemes integritási tartomány a és b elemére igaz, hogy a|b ∧ b|a, akkor a és b asszociáltak. Ez a reláció ekvivalenciareláció, továbbá kompatibilis a szorzással. A nullának (nullelem) mindig csak saját maga az asszociáltja. A | reláció kompatibilis ezzel az ekvivalenciarelációval, és az ekvivalenciaosztályokon tekintve részbenrendezést kapunk.

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

Az egységek az 1 (egységelem) asszociáltjai. Egy elem asszociáltjait leírhatjuk az egységek segítségével, amelyek nem mások, mint 1 osztói, hiszen 1 bárminek osztója.

Másképpen: az egységek R egységelemes integritási tartomány azon elemei, amelyeknek van a szorzásra nézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját. Az egységek bármely a ∈R-nak osztói, mert 1a-nak osztói.

163. Mi a kapcsolat az egységek és az asszociáltak között?

Az a ∈R asszociáltjai az εa alakú elemek, ahol ε egység, R pedig egységelemes integritási tartomány.

164. Mi a kapcsolat a természetes számok és az egész számok körében vett oszthatóság között?

Mivel ha k,m ∈$\mathbb{Z}$, akkor |km| = |k| · |m|, az egész számok körében m|n pontosan akkor teljesül, ha |m|||n| az $\mathbb{N}$-ben.

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

A Gauss-egészek egységelemes gyűrűje: G = {n + im: n,m ∈$\mathbb{Z}$} ⊂ $\mathbb{C}$. Négy egység van ±1 és ±i.

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

Az R egységelemes integritási tartomány egy a ≠ 0 eleme felbonthatatlan (más néven: irreducibilis), ha nem egység, és csak triviális módon írható fel szorzatként, tehát a =bc (b,c ∈R) esetén b vagy c egység.

A 0≠p ∈R elem prímelem, ha nem egység, és p|ab (a,b ∈R) esetén p|a vagy p|b.

A felbonthatatlan elemek és prímelemek halmaza egyenlő.

167. Mit értünk egységelemes integritási tartományban legnagyobb közös osztó alatt?

Az R egységelemes integritási tartományban az $a_1,a_2,\ldots,a_n \in R$ elemeknek a b ∈R elem legnagyobb közös osztója, ha i = 1,2,…,n esetén b|a_i és b'|a_i, akkor b'|b.

168. Mikor mondjuk egységelemes integritási tartomány elemeire, hogy relatív prímek?

Az R egységelemes integritási tartományban az $a_1,a_2,\dots,a_n \in R$ elemek legnagyobb közös osztói egységek, akkor $a_1,a_2,\dots,a_n$ relatív prímek.

169. Mit értünk egységelemes integritási tartományban legkisebb közös többszörös alatt?

Az R egységelemes integritási tartományban az $a_1,a_2,\dots,a_n \in R$ elemeknek a $b \in R$ elem legkisebb közös többszöröse, ha $i = 1,2,\dots,n$ esetén $b' | a_i$, akkor $b | b'$.

170. Egyértelmű-e az egész számok körében a legnagyobb közös osztó? Ismertesse a kapcsolódó jelölést.

Nem. Az $a_1,a_2,\dots,a_n \in \mathbb{Z}$ számok legnagyobb közös osztói közül az egyik nemnegatív, ezt $\text{lnko}(a_1,a_2,\dots,a_n)$-nel jelöljük. (Használt jelölés még az $\gcd(a_1,a_2,\dots,a_n)$ és az $(a_1,a_2,\dots,a_n)$ is.)

171. Egyértelmű-e az egész számok körében a legkisebb közös többszörös? Ismertesse a kapcsolódó jelölést.

Nem. A $a_1,a_2,\dots,a_n \in \mathbb{Z}$ számok legkisebb közös többszörösei közül az egyik nemnegatív, ezt $\text{lkkt}(a_1,a_2,\dots,a_n)$-nel jelöljük. (Használt jelölés még az $\text{lcm}(a_1,a_2,\dots,a_n)$ és az $[a_1,a_2,\dots,a_n]$ is.)

172. Ismertesse a bővített euklideszi algoritmust.

A bővített euklideszi algoritmus meghatározza az $a, b \in \mathbb{Z}$ egészek egy d legnagyobb közös osztóját, valamint az $x, y \in \mathbb{Z}$ egész számokat úgy, hogy $d = ax + by$ teljesüljön. (Az eljárás során végig $ax_n + by_n = r_n,\ n = 0,1,\dots$)

(1) *[Inicializálás.]* Legyen $x_0 \leftarrow 1, y_0 \leftarrow 0, r_0 \leftarrow a, x_1 \leftarrow 0, y_1 \leftarrow 1, r_1 \leftarrow b, n \leftarrow 0$.

(2) *[Vége?]* Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n,\ y \leftarrow y_n,\ d \leftarrow r_n$, és az eljárás véget ért.

(3) *[Ciklus.]* Legyen $q_{n+1} \leftarrow \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor, r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1},\ x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1},$ $y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1},\ n \leftarrow n + 1$ és menjünk (2)-re.

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

Bármely $a_1,a_2,\dots,a_n \in \mathbb{Z}$ számoknak létezik legnagyobb közös osztója, és: $\text{lnko}(a_1,a_2,\dots,a_n) = \text{lnko}(\text{lnko}(a_1,a_2),a_3,a_4,\dots,a_n)$.

174. Fogalmazza meg a számelmélet alaptételét.

Minden pozitív természetes szám a sorrendtől eltekintve egyértelműen felbontható prímszámok szorzataként.

175. Definiálja prímtényezős felbontásnál a kanonikus alakot.

A számelmélet alaptételében szereplő prímtényezős felbontást gyakran $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$ alakban írjuk, ahol $p_1,p_2,\dots,p_k$ különböző prímek, a kitevők pedig $\mathbb{N}^+$ elemei. Ezt nevezzük a szám kanonikus alakjának.

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

Ha adott *a* szám kanonikus alakban, akkor azok a természetes számok osztják *a*-t, amelyek kanonikus alakjában csak *a* prímtényezői szerepelnek és egyik prímtényező sem szerepel nagyobb hatványon, mint *a* kanonikus alakjában. Formálisan: *a* kanonikus alakja legyen $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$, ekkor:

$\forall b \in \mathbb{N}\ (b|a) \Leftrightarrow b = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}: \beta_i \le \alpha_i$, (i = 1,2,…k).

Bármely $a_1,a_2,\dots,a_n \in \mathbb{N}$ számok legnagyobb közös osztóját és legkisebb közös többszörösét úgy kapjuk meg, hogy ha felírjuk mindegyik szám kanonikus alakját úgy kiegészítve, hogy mindegyikben ugyanazok a prímtényezők szerepeljenek (a feleslegesek a 0. hatványon), akkor:

$a_i = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$, (i = 1,2,…,k),

$$lnko(a_1, a_2, \dots, a_n) = p_1^{min(\alpha_{1_1},\alpha_{2_1},\dots,\alpha_{k_1})} p_2^{min(\alpha_{1_2},\alpha_{2_2},\dots,\alpha_{k_2})} \dots p_k^{min(\alpha_{1_k},\alpha_{2_k},\dots,\alpha_{k_k})},$$

$$lkkt(a_1, a_2, \dots, a_n) = p_1^{max(\alpha_{1_1},\alpha_{2_1},\dots,\alpha_{k_1})} p_2^{max(\alpha_{1_2},\alpha_{2_2},\dots,\alpha_{k_2})} \dots p_k^{max(\alpha_{1_k},\alpha_{2_k},\dots,\alpha_{k_k})}.$$

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

$lnko(a,b) \cdot lkkt(a,b) = |ab|$

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

Tetszőleges $a_1,a_2,\dots,a_n \in \mathbb{Z}$ számoknak létezik legkisebb közös többszöröse, és $lkkt(a_1,a_2,\dots,a_n)=lkkt(lkkt(a_1,a_2),\dots,a_n)$.

179. Ismertesse Eratoszthenész szitáját.

Ha egy adott n-ig az összes prímet meg akarjuk tálalni, a következő egyszerű eljárás hatékony módszert ad: írjuk fel a számokat 2-től n-ig. Az első szám, a 2 prím, összes (valódi) többszöröse összetett, ezeket húzzuk ki. A megmaradó számok közül az első a 3, ez prím, ennek minden (valódi) többszöröse összetett, ezeket húzzuk ki stb. Az eljárás végén az n-nél nem nagyobb prímek maradnak meg.

180. Definiálja egész számok kongruenciáját és adja meg a kapcsolódó jelöléseket.

Ha $a,b,m \in \mathbb{Z}$ és m osztója a - b-nek, akkor azt mondjuk, hogy a és b kongruensek modulo m.

Ezt úgy jelöljük, hogy $a \equiv b \pmod m$.

181. Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

Ha a ≡ b(mod m) és d|m, akkor a ≡ b(mod m) is teljesül. Ha 0≠d ∈ℤ, akkor a≡b(mod m) ekivalens azzal, hogy ad≡bd(mod md). Az oszthatóság tulajdonságaiból következik, hogy bármely adott m∈ℤ-re a kongruencia ekvivalenciareláció ℤ -ben. Az m és a -m szerinti kongruencia ugyanazt jelenti.

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

Egy m∈ℤ modulus szerinti kongruencia ekvivalenciaosztályait maradékosztályoknak nevezzük. Ha egy maradékosztály valamelyik eleme relatív prím a modulushoz, akkor mindegyik, és ekkor a maradékosztály redukált maradékosztálynak nevezzük. Páronként inkongruens egészek egy rendszerét maradékrendszernek nevezzük. Ha egy maradékrendszer minden maradékosztályából tartalmaz elemet, akkor teljes maradékrendszernek nevezzük. Ha egy maradékrendszer pontosan a redukált maradékosztályokból tartalmaz elemet, akkor redukált maradékrendszernek nevezzük.

183. Definiálja ℤm-et. Milyen algebrai struktúra ℤm?

Egy m∈ ℤ modulus szerinti kongruencia ekvivalenciaosztályait maradékosztályoknak nevezzük. A kongruencia kompatibilis az összeadással és a szorzással. Az ekvivalenciaosztályok kommutatív egységelemes gyűrűt alkotnak az összeadással és a szorzással. Ezt a gyűrűt ℤm-el jelöljük.

184. Ismertesse a komplemens ábrázolásokat.

Negatív számok számítógépes ábrázolására elterjedt a komplemens ábrázolás. Csak bináris gépek esetével foglalkozunk.
Egy n-bites számítógépen használt lehetőségek 0≤k<2n-1 eseten –k ábrázolására:
1. -k mod (2^n-1) kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakját levonjuk 2^n-1 kettes számrendszerbeli alakjából. Mivel ez utóbbi csupa egyesből áll, a kivonás során nincs átvitel, k kettes számrendszerbeli alakját csak bitenként komplementáljuk. (egyesekre komplementálás)

2. Kettes komplementálás: k mod 2^n kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakjának vesszük a bitenkénti komplementerét, majd hozzáadunk 1-et.

185. Fogalmazza meg a ℤm gyűrű tulajdonságait leíró tételt.

Legyen m>1 egész. Ha 1<lnko(a,m)<m, akkor a maradékosztálya nullosztó $\mathbb{Z}_m$-ben. Ha lnko(a,m)=1, akkor a maradékosztályának van multiplikatív inverze $\mathbb{Z}_m$-ben. Speciálisan, ha m prímszám, akkor $\mathbb{Z}_m$ test.

186. Ismertesse a diszkrét logaritmus problémát.

$\mathbb{Z}_m$-ben nem nehéz hatványozni. Azonban a tapasztalat szerint még ha m prím is, $\mathbb{Z}_m$ invertálható elemeinek multiplikatív csoportjában egy a alap és egy a^k hatvány ismeretében nehéz meghatározni a k kitevőt, legalábbis ha m-1-nek vannak nagy prímtényezői: ez a diszkrét logaritmus probléma. A probléma számos más csoport esetén is nehéznek tűnik.

187. Ismertesse a Diffie–Hellmann–Merkle kulcscserét.

A felhasználók megállapodnak egy nagy Sophie Germain prímben, azaz olyan p prímben, amelyre q=2p+1 is prím valamint egy 1<g<p-1 alapban. Ha a két felhasználó valamely szokásos rejtjelezési rendszer, például AES felhasználásával titkosított üzenetet akar váltani, akkor szükségük lesz egy véletlenszerű közös kulcsra. Választanak egy 1<a<p illetve 1<b<p véletlen kitevőt, kiszámolják, és közzéteszik a g^a mod q illetve g^b mod q értéket. Mindketten ki tudják számolni g^{ab} mod q értékét, ez lesz a titkos kulcs. Az eljárás biztonsága azon múlik, hogy g, g^a mod q és g^b mod q ismeretében sem látszik jobb megoldás g^{ab} mod q meghatározására, mint az a és b megkeresése, ez viszont nehéz diszkrét logaritmus probléma. (Ezt a kulcscsere módszert használja az ssh, az SSL, és a TLS.)

188. Definiálja az Euler-féle φ függvényt.

Legyen m>0 egész szám, és jelölje φ (m) a modulo m redukált maradékosztályok számát; φ az Euler-féle φ függvény.

189. Mit mondhatunk az aai + b számokról, ha ai egy maradékrendszer, illetve egy redukált maradékrendszer elemeit futja be?

Legyen m>1 egész szám, a relatív prím m-hez. Ha $a_1,a_2,...,a_m$ teljes maradékrendszer modulo m és b∈ℤ, akkor aa_1+b, aa_2+b,..., aa_m+b is teljes maradékrendszer modulo m. Ha $a_1,a_2,...,a$ φ (m) redukált maradékrendszer modulo m, akkor $aa_1,aa_2,...,aa$ $\varphi_{(m)}$ is redukált maradékrendszer modulo m.

190. Fogalmazza meg az Euler–Fermat-tételt.

Legyen m>1 egész szám, a relatív prím m-hez. Ekkor $a^{\varphi(m)} \equiv 1 \pmod m$.

191. Fogalmazza meg a Fermat-tételt.

Legyen p prímszám. Ha a∈ℤ és p∤a akkor $a^{p-1} \equiv 1 \pmod p$. Ha a∈ℤ tetszőleges, akkor $a^p \equiv 1 \pmod p$.

192. Mit értünk diofantikus problémán?

Ha egy egyenlet vagy egyenletrendszer egész megoldásait keressük, akkor diofantikus problémáról beszélünk.

193. Mondjon két példát diofantikus problémára.

- $x^2 + y^2 = -4$, nincs se egész, se valós megoldása.
- $x^4 – 4y^4 = 3$, nincs egész megoldása, mivel $x^4 – 4y^4 \equiv 0 \vee 1 \pmod 4$, míg $3 \equiv 3 \pmod 4$.

194. Fogalmazza meg a kínai maradéktételt.

Legyenek $m_1,m_2,...m_n$ egynél nagyobb, páronként relatív prím természetes számok,

$c_1,c_2,...,c_n \in \mathbb{Z}$. Az $x \in c_j \pmod{m_j}$, $j=1,2,...,n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1,m_2,...m_n$.