EÖTVÖS LORÁND TUDOMÁNYEGYETEM – INFORMATIKAI KAR

Diszkrét matematika I.

Vizsgaanyag

Készítette: Nyilas Árpád

Definíciók, tétel kimondások

1. Mondjon legalább 3 példát predikátumra

   E(x) : x egyenes

   P(x): x pont

   I(x,y): x illeszkedik y-ra

2. Sorolja fel a logikai jeleket

   a. $\neg$: negáció, tagadás

   b. $\oplus$: kizáró vagy

   c. $\wedge$: és, konjukció

   d. $\vee$: megengedő vagy, diszjukció

   e. $\Rightarrow$: implikáció

   f. $\|$: összeférhetetlen vagy

   g. $|$: sem sem

   h. $\Leftrightarrow$: ekvivalencia

3. Milyen kvantorokat ismer? Mi a jelük?

   a. egzisztenciális kvantor $\exists$

   b. univerzális kvantor $\forall$

4. Hogyan kapjuk a logikai formulákat?

   A logikai formulák az adott elmélet predikátumaiból épülnek fel a logikai jelek, valamint a két kvantor segítségével.

5. Mikor van egy változó egy kvantor hatáskörében?

   Egy formula egy ($\forall x\mathcal{A}$) vagy ($\exists x\mathcal{A}$) típusú részformulája esetén az x változó minden a két zárójel közötti előfordulására azt mondjuk, hogy a kvantor hatáskörében van.

6. Mik a nyitott és mik a zárt formulák?

   Ha egy formulának nincs szabad változója, akkor a formulát zárt formulának, egyébként nyitott formulának nevezzük.

7. Mondj két példát nyitott formulára.

$$\Big(\big(E(x) \wedge P(xy)\big) \wedge I(x,y)\Big)$$

$$\exists y\Big(\big(E(x) \wedge P(y)\big) \wedge I(x,y)\Big)$$

8. Mondj egy példát zárt formulára.

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

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

   A halmaz részhalmaza a B halmaznak, ha A minden eleme a B halmaznak is. 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?

    a. reflexivítás :$\forall A(A \subset A)$

    b. tranzitívitás: $\Big((A \subset B) \quad \wedge (B \subset C)\Big) \Rightarrow (A \subset C)$

    c. antiszimmetria : $\big((A \subset B) \wedge (B \subset A)\big) \Rightarrow (A = B)$

11. Milyen tulajdonságokkal rendelkezik a halmazok egyenlősége.

    a. reflexivítás :$\forall A(A = A)$

    b. tranzitívitás: $\Big((A = B) \quad \wedge (B = C)\Big) \Rightarrow (A = C)$

    c. antiszimmetria : $\big((A = B) \wedge (B = A)\big) \Rightarrow (A = B)$

    d. szimmetria: $(B = A) \Rightarrow (A = B)$

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

    A halmaz részhalmaza a B halmaznak, ha A minden eleme a B halmaznak is. Jele $A \subset B \; vagy \; B \supset A$.

13. Írja le az üres halmaz fogalmát.

    Az üres halmaz olyan halmaz, amelynek nincs eleme.

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

    Igen, a meghatározottsági axióma miatt.

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

    A és B halamz uniója az a halmaz, amelynek pontosan azok a dolgok az elemei, melyek elemei A-nak vagy B-nek (vagy mind kettőnek). Jele $A \cup B$.

16. Írja le halmazrendszer unióját és a megfelelő jelöléseket.

    Ha $\mathscr{A}$ egy halmaz, melynek elemei mind halmazok, akkor azt a halmazt, amely pontosan azokat a dolgokat tartalmazza, amelyek $\mathscr{A}$ valamely elemének az elemei, az $\mathscr{A}$ uniójának nevezzük. Jelölései:$\cup \mathcal{A}$, $\cup \{\mathrm{A}: \mathrm{A} \in \mathcal{A}\}$, $\cup_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$

17. Fogalmazza, meg a halmazok uniójának alaptulajdonságait.

    (1) $A \cup \emptyset = A$

    (2) $A \cup B = B \cup A$ (kommutativitás)

    (3) $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás)

    (4) $A \cup A = A$ (idempotencia)

    (5) $(A \subset B) \Leftrightarrow (A \cup B = B)$

18. Definiálja halmazrendszer és két halmaz metszetét, és adja meg jelöléseiket.

    $\mathcal{A}$ halmazok egy nem üres rendszere, akkor a halmazrendszer metszetét a

    $$\cap \mathcal{A} \coloneqq \{x: x \in A \ \ ahol \ \forall A \in \mathcal{A}\}$$

    összefüggéssel definiálhatjuk, más jelölések: $\cap \mathcal{A}$, $\cap \{\mathrm{A}: \mathrm{A} \in \mathcal{A}\}$, $\cap_{\mathrm{A} \in \mathcal{A}} \mathrm{A}$

    A és B halmaz metszete: $A \cap B \coloneqq \{x \in A: x \in B\}$

19. Definiálja a diszjunktság és a páronként diszjunktság fogalmát.

    Ha egy nem üres $\mathcal{A}$ halmazrendszer metszete az üres halmaz, akkor a halmazrendszer diszjunkt. Ha a halmazrendszer bármely két különböző halmazának a metszete üres, akkor elemei páronként diszjunktak.

20. Fogalmazza meg a halmazok metszetének alaptulajdonságait.

    (1) $A \cap \emptyset = A$

    (2) $A \cap B = B \cap A$ (kommutativitás)

    (3) $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás)

    (4) $A \cap A = A$ (idempotencia)

    (5) $(A \subset B) \Leftrightarrow (A \cap B = A)$

21. Fogalmazza meg a unió és a metszet disztributivitását.

    $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (metszet disztributivitása az unióra nézve)

    $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (unió disztributivitása a metszetre nézve)

22. Definiálja halmazok különbségét, szimmetrikus differenciáját, és komplementerét.

    a. különbség: $A \setminus B \coloneqq \{x \in A: x \notin B\}$

    b. szimmetrikus differencia: $A \Delta B \coloneqq (A \setminus B) \cup (B \setminus A)$

    c. A halmaz X-re vonatkozó komplementere: $A' \coloneqq X \setminus A$

23. Fogalmazza meg a halmazok komplementereinek alaptulajdonságait.

    (1) $(A')' = A$

    (2) $\emptyset' = X$

    (3) $\mathrm{X}' = \emptyset$

    (4) $A \cap A' = \emptyset$

    (5) $A \cup A' = X$

    (6) $A \subset B \Leftrightarrow B' \subset A'$

    (7) $(A \cup B)' = A' \cap B'$

    (8) $(A \cap B)' = A' \cup B'$

24. Írja le a hatvány halmaz fogalmát. Milyen jelölések kapcsolódnak hozzá?

    Ha A halmaz akkor azt a halmazrendszert, melynek elemei A részhalmazai, az A hatványhalmazának nevezzük. Jele $\wp(A)$, esetleg 2^A

25. Definiálja a rendezett pár fogalmát és koordinátáit.

    Bármely x, y esetén legyen $(x, y) \coloneqq \{\{x\}, \{x, y\}\}$.

    Az (x,y) rendezett pár első koordinátája x, második koordinátája y.

26. Definiálja két halmaz Descartes szorzatát.

    X,Y halmaz Descartes szorzata: az $X \times Y \coloneqq \{(x, y): x \in X, y \in Y\}$ rendezett párokból álló halmaz.

27. Definiálja a binér relációt, és adja meg a kapcsolódó jelöléseket.

    Egy halmaz binér reláció, ha minden eleme rendezett pár. $(x, y) \in R$ helyett gyakran használatos a xRy

28. Adjon 3 példát binér relációra.

$$I_x = \{(x, x] \in X \times X: x \in X\}$$

$$\emptyset$$

$$X \times Y$$

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

    R reláció X és Y között, ha $R \subset X \times Y$, ha X=Y akkor R X beli reláció.

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

    R reláció értelmezési tartománya: $dmn(R) \coloneqq \{x: \exists y((x, y) \in R)\}$

    R reláció értékkészlete: $rng(R) \coloneqq \{y: \exists x((x, y) \in R)\}$

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 nevezzük, ha $S \subset R$.

    R reláció A halmazra való leszűkítésén az

$$R|_A \coloneqq \{(x, y) \in R: x \in A\}$$

    relációt értjük.

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

    R binér inverze:

$$R^{-1}: = \{(b, a): (a, b) \in R\}$$

    tulajdonságai:

    (1) $(R^{-1})^{-1} = R$

    (2) $R \subset X \times Y \Rightarrow R^{-1} \subset Y \times X$

    (3) $dmn(R^{-1}) = rng(R),\ valamint\ rng(R^{-1}) = dmn(R)$

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

    R binér reláció, A halmaz, akkor az A halmaz képe:

    $$R(A) := \{y: \exists x \in A((x,y) \in R)\}$$

    B halmaz inverz képe az R reláción: $R^{-1}(B)$

    Ha A={a}, akkor R({a}) helyet írhatunk R(a)-t

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

    Az R és S binér reláció kompozícióján az

    $$R \circ S := \{(x,y): \exists z((x,z) \in S \wedge (z,y) \in 1)\}$$

    relációt értjük.

    Két reláció kompozíciója lehet üres, ekkor rng(S) és dmn(R) diszjunktak.

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

    (1) $rng(s) \supset dmn(R) \Rightarrow rng(R \circ S) = rng(R)$

    (2) $R \circ (S \circ T) = (R \circ S) \circ T$

    (3) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$

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

    Legyen R X-beli binér reláció ekkor,

    a. tranzitív ha: $\forall x,y,z\left(((x,y) \in R \wedge (y,z) \in R) \Rightarrow (x,z) \in R\right)$

    b. szimmetrikus ha: $\forall x,y((x,y) \in R \Rightarrow (y,x) \in R)$

    c. dichotóm ha: $\forall x,y \in X((x,y) \in R \vee (y,x) \in R)$

    A tranzitivitás és a szimmetria csak a reláción múlik.

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

    Legyen R X-beli binér reláció ekkor,

    a. antiszemmetrikus ha: $\forall xy\left(((x,y) \in R \wedge (y,x) \in R) \Rightarrow (x=y)\right)$

    b. trichotóm ha: $\forall x,y \in X\left((x=y) \oplus ((x,y) \in R) \oplus ((y,x) \in R)\right)$

    Az antiszimmetria csak a reláción múlik.

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

    Legyen R X-beli binér reláció ekkor,

    a. szigorúan antiszimmetrikus ha $\forall \mathrm{x}, \mathrm{y}\big((x,y) \in R \Rightarrow (y,x) \notin R\big)$

    b. reflexív $\forall x \in X\big((x,x) \in R\big)$

    c. irreflexív $\forall x \in X\big((x,x) \notin R\big)$

    A szigorú antiszimmetria csak a relación múlik.

39. Definiálja az ekvivalenciareláció, illetve az osztályozás fogalmát.

    X halmaz beli reláció ekvivalenciareláció, ha reflexív, szimmetrikus és tranzitív.

    Az X részhalmazainak egy $\mathcal{O}$ rendszerét X osztályozásának nevezzünk, ha $\mathcal{O}$ páronként diszjunkt nem üres halmazokból álló halmazrendszer, amelyre $\cup\mathcal{O} = X$.

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

    Valamely X halmazon értelmezett ~ ekvivalenciareláció esetén a

    $\tilde{\mathrm{x}} = \{y \in X : y \sim x\}, x \in X$ ekvivalenciaosztályok X-nek egy $\tilde{X} = X/\sim$ osztályozását adják.

    Megfordítva:

    az X halmaz bármely $\mathcal{O}$ osztályoza esetén az $\cup\{Y \times Y : Y \in \mathcal{O}\}$ reláció ekvivalencia reláció, amelyhez tartozó ekvivalencia osztályok halmaza $\mathcal{O}$.

    Hasonlóan, ha egy ekvivalenciarelációra képezzük az ekvivalenciaosztályokat, amjd ebből a hozzá tartozó ekvivalencia relációt, akkor az eredeti relációt kapjuk vessza.

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

    X halmazbeli részbenrendezés egy tranzitív reflexív és antiszimmetrikus X-beli reláció. A részben rendezés jelölése: $\leq$. A részben rendezett halmaz, tulajdonképpen (X, $\leq$) pár.

    Egy részbenrendezett halmaz minden részhalmaza is részbenrendezett, ha a $\leq$ relációt csak ennek az elemei között tekintjük.

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

    X részben rendezett halmazon, $\leq$ részben rendezési reláció dichotóm is, azaz X bármely két eleme összehasonlítható, akkor a reláció rendezés, X pedig rendezett halmaz.

    X $\leq$-vel részbenrendezett halmaz Y részhalmaza lánc, ha a $\leq$ relációt csak Y az elemei között tekintve Y $\leq$-vel rendezett.

43. Mondjon példát részbenrendezett, de nem rendezett halmazra.

    A természetes számok körében az „n osztja m-et” reláció

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

    X-beli R relációhoz definiálhatunk X-beli S szigorú relációt, úgy hogy $xSy \Leftrightarrow (xRy \wedge x \neq y)$

    X-beli R relációhoz definiálhatunk X-beli T gyeng relációt, úgy hogy $xTy \Leftrightarrow (xRy \vee x = y)$

45. Definiáljuk a szigorú részbenrendezést és fogalmazzuk meg kapcsolatát a részbenrendezéssel.

    X halmaz $\leq$- relációval részben rendezett halmaz, akkor a megfelelő X-beli szigorú reláció (jele <) szigorú részben rendezés. Ami irreflexív, tranzitív, szigorúan antiszimmetrikus.

    Ha egy $\leq$ részben rendezéshez, definiáljuk a megfeleő szigorú részben rendezést, majd abból a megfelelő gyenge rendezést a $\leq$-t kapjuk vissza, és fordítva.

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

    < szigorú részben rendezés. Ha x<y (ami helyett írhatunk y>x-t) akkor azt mondjuk, hogy x kisebb, mint y vagy y nagyobb, mint x, vagy x megelőzi y-t vagy y követi x-et.

    Gyenge reláció esetén($\leq, \geq$) hozzátesszük, hogy vagy egyenlő.

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

    X egy részbenrendezett halmaz. Ha x$\leq z$ és z$\leq$y, akkor azt mondjuk, hogy z x és y közé esik, az ilyen elem halmazát [x,y]-al jelöljük.

    X egy részbenrendezett halmaz. Ha x<z és z<y, akkor azt mondjuk, hogy z szigorúan x és y közé esik, az ilyen elem halmazát]x,y[-al vagy (x,y) jelöljük.

    ]x,y] és [x,y[halmazok, definíciója analóg, itt is használatos (x,y] és a [x,y) jelölés is.

    A fenti halmazok közös néven intervallumok.

48. Mi az hogy közvetlenül követi, illetve, hogy közvetlenül megelőzi?

    Ha x<y de]x,y[=∅, akkor x közvetlenül megelőzi y-t, illetve y közvetlenül követi x-t.

49. Definiálja a kezdő szelet fogalmát és adja meg a kapcsolódó jelöléseket.

    Egy $x \in X$ elemhez tartozó kezdőszeletnek a $\{y \in X : y < x\}$ részhalmazt nevezzük.

    Jelölése:$] \leftarrow, x[$. A $] \leftarrow, x]$, $]x \rightarrow [$, $[x, \rightarrow [$ jelölések analóg értelmezendők.

50. Definiálja a legkisebb és a legnagyobb elem fogalmát.

    X részbenrendezett halmaz legkisebb eleme $x \in X$, amelyre $\forall y \in X(x \leq y)$.

    X részbenrendezett halmaz legnagyobb eleme $x \in X$, amelyre $\forall y \in X(y \leq x)$.

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

    x-t minimálisnak nevezzük, ha nincs nála kisebb elem, maximálisnak akkor, ha nincs nála nagyobb elem. Ha van egyértelmű minimális elem akkor azt min X-el jelöljük, és ha van egyértelmű maximális elem azt max X-el jelöljük.

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

    A $\mathbb{N}\backslash\{0,1\}$ halmazon az „osztója” részbenrendezés.

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

    A természetes számok halmaza a szokásos rendezéssel.

54. Igaz-e, hogy rendezett halmazban a legkisebb és a minimális elem fogalma egybe esik.

    Igen, mivel rendezett halmazban, bármely két elem összehasonlítható, így $x \in X(\forall y \in X(x \leq y)) \Leftrightarrow x \in X(\nexists y(y \leq x))$.

55. Definiálja az alsó és a felső korlát fogalmát.

    Egy X részben rendezett halmaz x eleme az Y részhalmaz

    a. alsó korlátja ha $\forall y \in Y(x \leq y)$
    b. felső korlátja ha $\forall y \in Y(y \leq x)$

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

    Igen, akkor az az Y legkisebb eleme.

57. Definiálja az alsó és a felső határtulajdonságot.

    Ha X részbenrendezett halmaz bármely nem üres, felülről korlátos részhalmazának van felső határa, akkor a felső határ tulajdonságúnak nevezzük, ha pedig bármely nem üres alulról korlátos részhalmazának van alsó határa, akkor X-et alsó határtulajdonságúnak nevezzük.

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

    Igen, mert ekkor az alsó korlát fogalmának definíciója miatt X halmaz Y részhalmazának x elemére és egyben alsó korlátjára teljesül a $\forall y \in X: x \leq y$, amely a legkisebb elem definíciójával egyezik meg.

    Mivel x az Y összes elemével összehasonlítható - mert alsó korlát -, ezért $\forall y \in X: x \leq y = \neg(\neg(\forall y \in X: x \leq Y)) = \neg(\exists y \in X: y < x) = \nexists y \in X: y < x$ _, ami a minimális elem definíciója, tehát x az *Y* részhalmaz minimális eleme is.

59. Definiálja az infimum és a szuprémium fogalmát.

    Ha X halmaz Y részhalmazának alsó korlátainak halmazában van legnagyobb elem, akkor az Y infimumának nevezzük (jelölés: inf Y), ha Y felsőkorlátainak halmazában van legkisebb elem, azt Y szuprémumának nevezzük(jelölés sup Y).

60. Definiálja a jólrendezést és a jólrendezett halmaz fogalmát.

    X rendezett halmaz jólrendezett, a rendezés pedig jólrendezés, ha **X bármely nem üres részhalmazának van legkisebb eleme**.

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

    Racionális számok halmaza.

62. Adjon példát jólrendezett halmazra.

    Természetes számok halmaza.

63. Adjon meg két részben rendezett halmaz Descartes-szorzatán a halmazok részben rendezései segítségével két részbenrendezést.

    Legyen X és Y részben rendezett halmaz.

    $X \times Y$-ban legyen $(x, y) \leq (x', y')$, ha $x \leq x' \wedge y \leq y'$

    vagy $X \times Y$-ban legyen $(x, y) \leq (x', y')$, ha $x < x' \vee (x = x' \wedge y \leq y')$ (lexikografikus rendezés)

64. Két jól rendezett halmaz Descartes-szorzatán a lexikografikus részbenrendezést tekintjük. Mit állíthatun erről.

    A két halmaz Descartes-szorzata rendezett, illetve jólrendezett a lexikografikus rendezéssel.

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

    A függvény egy olyan f reláció, amelyre $\big((x, y) \in f \wedge (x, y') \in f\big) \Rightarrow y = y'$

    Jelölések: $f(X) = \{y\}$, $f(X) = \{y\}$, f_X, $f: x \mapsto y$ (a függvény x helyen felvett y értéke) $f: X \to Y$ (f X halmazt Y ba képző függvény)

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

    $f \in X \to Y$ $esetén$ $dmn(f) \subset X$ $míg$ $f: X \to Y$ $esetén$ $dmn(f) = X$

67. Mikor nevezünk egy függvényt kölcsönösen egyértelműnek.

    Egy függvény kölcsönösen egyértelmű, ha f(x)=y és f(x')=y esetén x=x'

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

    $\mathbb{I}_x$ X et Y ba képtő identikus leképzés szürjektív, ha X=Y, de nem ha $X \subsetneq Y$

69. Definiálja a permutáció fogalmát.

    Egy X halmaz önmagára való kölcsönösen egyértelmű leképzéseit az X permutációinak nevezzük.

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

    Igaz, ha f X-ből Y-ba és g Y-t Z-ba képző függvények, akkor $g \circ f$ X-et Z-ba képző függvény.

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

    Ha f és g is kölcsönösen egyértelmű függvény, akkor $g \circ f$ is.

    Ha f X-ből Y-ra és g Y-t Z-ra képző függvények, akkor $g \circ f$ X-et Y-ra képző függvény

    Ha f és g is bijektív függvény, akkor $g \circ f$ is.

72. Mi a kapcsolat függvények és ekvivalenciarelációk között?

    Ha az X halmazon adott egy ekvivalencia reláció, akkor az x elemhez az ekvivalenciaosztályát rendelő leképzés X kanonikus leképzése.

    Megfordítva
    ha $f: X \to Y$ egy függvény, akkor az $x \sim x'$ ha f(x)=f(x') reláció egy ekvivalencia reláció.

73. Mikor nevezünk egy függvényt monoton növekvőnek, illetve monoton csökkenőnek?

    X és Y rendezett halmaz, $f: X \to Y$ függvény.

    Egy függvény monoton növekvő ha $\forall x, y \in X\big(x \leq y \Rightarrow f(x) \leq f(y)\big)$

    Egy függvény monoton csökkenő ha $\forall x, y \in X\big(x \leq y \Rightarrow f(x) \geq f(y)\big)$

74. Mikor nevezünk egy függvényt szigorúan monoton növekvőnek illetve szigorúan monoton csökkenőnek.

    X és Y rendezett halmaz, $f: X \to Y$ függvény.

    Egy függvény szigorúan monoton növekvő ha $\forall x, y \in X\big(x < y \Rightarrow f(x) < f(y)\big)$

    Egy függvény szigorúan monoton csökkenő ha $\forall x, y \in X\big(x < y \Rightarrow f(x) > f(y)\big)$

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

    X és Y rendezett halmaz, $f: X \to Y$ szigorúan monoton növekvő függvény, akkor kölcsönösen egyértelmű is.

76. Mit állítunk a monoton növekvő függvények inverz függvényéről?

    Egy monoton növekvő függvény inverz függvénye szigorúan monoton növekvő.

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

    Egy x függvény i helyen felvett értékét jelölhetjük x_i-vel, ekkor
    x értelmezési tartománya (I) index halmaznak,
    értékkészletét indexelt halmaznak,
    a függvényt indexelt családnak nevezzük

78. Definiálja indexelt halmazcsaládok unióját és metszetét.

    Egy X_i, $i \in I$ indexelt halmazcsalád uniója $\bigcup_{\boldsymbol{i \in I}} \boldsymbol{X_i} \coloneqq \bigcup\{\boldsymbol{X_i}: \boldsymbol{i} \in \boldsymbol{I}\}$

    metszete pedig $\bigcap_{i \in I} X_i \coloneqq \bigcap\{X_i: i \in I\}\ feltéve\ hogy\ I \neq \emptyset$

79. Fogalmazza meg az indexelt halmazcsaládokra vonatkozó De Morgan szabályokat

    (1) $\left(\bigcup_{i \in I} X_i\right)' = \bigcap_{i \in I} X_i'$

    (2) $\left(\bigcap_{i \in I} X_i\right)' = \bigcup_{i \in I} X_i'$

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

    $X_1 \times X_2 \times \ldots \times X_n \coloneqq \{(x_1, x_2, \ldots, x_n): x_i \in X_i, ahol\ i \in \{1,2, \ldots, n\}\}$

    Ha $X_1 = X_2 = \cdots = X_n$ akkor, X^n el szokás jelölni.

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

    Egy X_i, $i \in I$ indexelt halmazcsaládhoz tartozó reláción kiválasztási függvények egy tetszőleges halmazát értjük.

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

    A halmazcsalád $\times_{i\in I} X_i$ Descartes szorzata a halmazcsaládhoz tartozó összes kiválasztási függvények halmaza.

    Ha egyértelmű jelölhetjük: $\times_i X_i$

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

    Egy X halmazbeli binér műveleten egy $*: X \times X \to X$ leképzést értünk *(x,y) helyett x*y-t írunk.

    Egy X halmazbeli unér műveleten egy $*: X \to X$ leképzést értünk

    Egy X halmazbeli nullér műveleten egy $*: \{\emptyset\} \to X$ leképzést értünk

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

    $\wedge: X \times X \to X \;\; X = \{\uparrow, \downarrow\}$

$\wedge$	$\uparrow$	$\downarrow$
$\uparrow$	$\uparrow$	$\downarrow$
$\downarrow$	$\downarrow$	$\downarrow$

    $\neg: X \times X \to X \;\; X = \{\uparrow, \downarrow\}$

	$\uparrow$	$\downarrow$
$\neg$	$\downarrow$	$\uparrow$

85. Hogyan definiáljuk a műveleteket függvények között.

    Legyen X halmaz, Y pedig egy halmaz a rajta értelmezett $*$ binér művelettel.

    Ekkor az X-et Y-ba képző függvények között is értelmezhetünk pontonként egy binér műveletet (amelyet ugyan azzal a jellel jelölünk) a következő összefüggéssel.

    $(f * g)(x) \coloneqq \forall x \in X\big(f(x) * g(x)\big)$ ahol$f, g: X \to Y$

    Hasonlóan definiálhatók unér és nullér műveletek függvényeken.

86. Adjon példát műveletekre függvények közt.

    Egy adott X halmazon értelmezett valós értékű függvények esetén az összeadást (, kivonást, szorzást) pontonként értelmezzük függvényekre is.

87. Definiálja a művelettartó leképzés fogalmát.

    Legyen $*$ binér művelet az X, és legyen $*'$ binér művelet az X' halmazon.

    Egy $\varphi: X \to X'$ leképzés művelettartó ha

    $$\forall x, y \in X \left(\varphi(x * y) = \varphi(x) *' \varphi(y) \right)$$

    Hasonlóan értelmezzük a művelettartást unér és nullér műveletekre is.

88. Adjon példát művelettartó leképzésre.

    ha $a > 1$, $x_1 \to a^x$ leképzés művelettartó és kölcsönössen egyértelmű leképzése az összeadással tekintett valós számoknak a szorzással tekintett pozitív valós számokra.

89. Fogalmazza meg a rekurzió tételt.

    Legyen X halmaz, $a \in x, f: X \to X$ függvény ($és\ \mathbb{N} - en\ t$eljesülnek a Peano-axiómák), akkor

    $$\exists!\, g \cdot \mathbb{N} \to x \text{ függvény amelyre } \forall n \in \mathbb{N} \left(g(0) = a \wedge g(n^+) = f\left(g(n)\right) \right)$$

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

    X egy halmaz, $Y \subset X$, ekkor Y karakterisztikus függvénye:

    $\chi_Y: X \to \{0,1\}$ leképezés, melyre teljesül.

    $\chi_Y(x) = 1, \text{ha } x \in Y$

    $\chi_Y(x) = 0, \text{ha } x \in X \backslash Y$

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

    Legyen X halmaz, $*$ pedig rajta értelmezett művelet

    ekkor $s \in X$ bal oldali semleges elem, ha $\forall g \in X (s * g = g)$,

    illetve jobb oldali semleges elem ha$\forall g \in X (g * s = g)$,

    ha s jobb és baloldali semleges elem is, akkor semleges elemnek nevezzük.

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

    (G, $*$) pár félcsoport, ha $*$ művelet értelmezve van G halmazon, és $*$ asszociatív.

    Ha (G, $*$) félcsoportban s semleges elem akkor g* elemet g elem balinverze, ha $g^* * g = s$

    és g pedig jobbinverze g*-nak, ha g* elem jobb és balinverze is g-nek, akkor g* g inverze.

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

    Igaz, hg inverze h*·g*

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

(G, $*$) félcsoport csoport ha

(1) (G, $*$)-nek van semleges eleme

(2) G minden elemének létezik inverze

(G, $*$) csoport Ábel-csoport, ha a $*$ kommutatív

95. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\mathcal{P}(X),\cap)$ egy egységelemes félcsoport.

Igaz, hisz $\mathcal{P}(X)$-en asszociatív művelet a ∩, és X az egységelem.

96. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\mathcal{P}(X),\cup)$ egy csoport.

Nem, hisz ugyan egységelemes félcsoport, ahol az egységelem a ∅ , de két nem üres halmaz uniója soha sem lesz üres halmaz, így nem lesz minden elemnek inverze.

97. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\mathcal{P}(X), \Delta)$ egy félcsoport.

Igaz, hisz Δ aszociatív művelet halmazrendszereken, így $\mathcal{P}(X)$-en is.

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

Igaz, hisz a kompozíció asszociatív művelet a binér relációk halmazán, és az identikus leképzés egységelem.

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

Igaz, hisz a kompozíció asszociatív művelet a leképzések halmazán, az identikus leképzés az egység elem, és mivel bijektív minden elemnek van inverze.

100. Fogalmazza meg a természetes számokra a $\leq$ reláció és a műveletek kapcsolatát leíró tételt.

Legyen $k, m, n \in \mathbb{N}$. Ekkor

(1) n^+ közvetlenül követi n-et

(2) $m \leq n \Leftrightarrow m + k \leq n + k$

(3) $k \neq 0 \; esetén \; m \leq n \Leftrightarrow m \cdot k \leq n \cdot k$

(4) $m < n \Leftrightarrow m + k < n + k$

(5) $k \neq 0 \; esetén \; m < n \Leftrightarrow m \cdot k < n \cdot k$

(6) $k \neq 0 \; esetén \; m \cdot k = n \cdot k \Rightarrow m = n$

101. Definiálja a véges sorozatot.

$[0, n] \subset \mathbb{N} \; vagy \; [1, n] \subset \mathbb{N}^+$ halmazokon értelmezett függvényeket véges sorozatnak nevezzük.

102. Fogalmazza meg az általános rekurzió tételt.

Legyen adott X halmaz

és egy f X-be képző függvény függvény, dmn(f) $\mathbb{N}$ valamely kezdőszeletéből X be képző függvények halmaza.

Ekkor $\exists!\, g\colon \mathbb{N} \to X$ függvény, amely f-zárt, azaz $\forall a \in N \left(g(a) = f\left(g|_{]\leftarrow,a[}\right)\right)$

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

Legyen X:=$\mathbb{N}$

legyen $n \mapsto n^-$ leképcése $\mathbb{N}^+$-nak $\mathbb{N}$-re az $n \mapsto n^+$ leképzés inverze

Továbbá $f(\emptyset) = 0$, $f(\{(0,k)\}) = 1\ \forall k \in \mathbb{N}$

Ha n>1

$h\colon]\leftarrow, n[\to \mathbb{N}$ függvény, akkor legyen $f(h) = h(n^-) + h(n^{--})$

Megjegyzés: n=min($\mathbb{N}$\dmn(h))

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

Ha G egy multiplikatív félcsoport, $x\colon \mathbb{N} \to G$, általános rekurzió tételt alkalmazva definiálhatjuk a

$$(n \in \mathbb{N}^+) \quad \prod_{k=1}^{n} x_k \ \ szorzatokat\ úgy\ hogy\ \prod_{k=1}^{1} x_k = x_1\ és\ \prod_{k=1}^{n+1} x_k = \left(\prod_{k=1}^{n} x_k\right) \cdot x_{n+1}$$

Ha G egy multiplikatív félcsoport e egység elemmel, akkor

$$(n \in \mathbb{N}^+) \quad \prod_{k=1}^{n} x_k \ \ szorzatokat\ úgy\ hogy\ \prod_{k=1}^{0} x_k = e\ és\ \prod_{k=1}^{n+1} x_k = \left(\prod_{k=1}^{n} x_k\right) \cdot x_{n+1}$$

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

G multiplikatív félcsoport, g∈ G

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

(2) $(g^m)^n = g^{mn}$

Minden $n, m \in \mathbb{N}^+$-ra(Ha G egységelemes félcsoport akkor minden $n, m \in \mathbb{N}$-ra)

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

$(gh)^n = g^n \cdot h^n$ minden $n, m \in \mathbb{N}^+$-ra

107. hogyan értelmezzük a $\sum_{a\in A} x_a$ jelölést?

Ha A halmaz, G félcsoport, $x\colon A \to G$ függvény és van olyan $\varphi\colon \{k \in \mathbb{N}\colon 1 \le k \le n\} \to A$, akkor (kommutativitást és az aszozivitást felhasználva indukvióval belátható) minden ilyen leképzésre $\sum_{k=1}^{n} x_{\varphi(k)}$ ugyan az, ezt a közös értéket jelölhetjük $\sum_{a\in A} x_a$-vel.

108. Fogalmazza meg a maradékos osztás tételét.

Legyen n>0 rögzített természetes szám

$\forall m \in \mathbb{N}$ egyértelműen felírható $m = qn + r$ alakban, ahol $q, r \in \mathbb{N}$ és r<n.

109. Definiálja a hányados és a maradékot természetes számok osztásánál, a páros és a páratlan számokat.

A maradékos osztás tétele szerint $m \in \mathbb{N}$ felírható $m = qn + r$ alakban, ekkor q honyados, r maradék az m szám n el való maradékos osztásánál.

Ha az $m \in \mathbb{N}$ 2 vel való maradékos osztásánál a maradék 0 akkor a szám páros, egyébként páratlan.

110. Fogalmazza meg a számrendszerekre vonatkozó tételt.

Legyen q>1, $q \in \mathbb{N}$

Minden m>0 természetes számhoz, egy és csak egy olyan n természetes szám és $a_0, a_1 \dots a_n \in [0, q[\subset \mathbb{N}$ sorozat létezik, amelyre

$$a_n \neq 0 \text{ és } m = \sum_{i=0}^{n} a_i \cdot q^i$$

111. Mikor mondjuk, hogy egy binér művelet kompatibilis egy osztályozással. Adjon ekvivalens megfogalmazást és definiálja a műveleteket az osztályok között.

Legyen $*$ egy binér művelet X halmazon, és legyen adott X osztályozása és a megfelelő ~ ekvivalencia reláció.

$*$ művelet kompatibilis az osztályozással, illetve ~ -val, ha $x \sim x' \wedge y \sim y' \Rightarrow x * y \sim x' * y'$

Az ekvivalencia reláció tulajdonságai miatt elegendő feltétel: $x * y \sim x' * y \wedge x * y \sim x * y'$

Ha a művelet kompatibilis az osztályozással, akkor az ekvivalencia osztályok terén, $\tilde{X}$-on bevezetünk egy $\tilde{*}$ műveltet az $\tilde{x} \tilde{*} \tilde{y} = \widetilde{x * y}$ definícióval, mert a kompatibilitás miatt az eredmény független a reprezentánsválasztástól.

112. Definiálja a nullgyűrű és a zérógyűrű fogalmát.

A nullgyűrű olyan gyűrű, amely csak egy elemet tartalmaz, ez nyilván a 0.

A zérógyűrűben az alaphalmaz és az összeadás Ábel-csoportot alkot, és bármely két elem szorzata 0.

113. Definiálja a bal és jobboldali nullosztó és a nullosztópár fogalmát.

Ha x,y egy R gyűrű 0-tól különböző elemei, és xy=0, akkor x és y nullosztópár, x bal oldali nullosztó, y jobboldali nullosztó.

114. Definiálja az integritási tartomány fogalmát.

Az integritási tartomány egy kommutatív nullosztómentes gyűrű.

115. Definiálja a rendezett integritási tartomány fogalmát.

R integritási tartomány, rendezett integritási tartomány, ha alaphalmaza rendezett, és

(1) $x, y, z \in R(x \leq y \Rightarrow x + z \leq y + z)$ (Az összeadás monoton)

(2) $x, y \in R(x, y \geq 0 \Rightarrow x \cdot y \geq 0)$ (A szorzás monoton)

116. Forgalmazza meg szükséges és elégséges feltételét arra vonatkozóan, hogy egy intagritási tartomány rendezett integritási tartomány legyen.

R integritási tartomány akkor és csak akkor rendezett integritási tartomány, ha alaphalmaza rendezett és

(1) $x, y, z \in R(x < y \Rightarrow x + z < y + z)$ (Az összeadás szigorúan monoton)

(2) $x, y \in R(x, y > 0 \Rightarrow x \cdot y > 0)$ (A szorzás szigorúan monoton)

117. Fogalmazza meg a rendezett integritási tartományokban az egyenlőtlenségekkel való számolás szabályait leíró tételt.

(1) $x > 0 \Rightarrow -x < 0$ *és* $x < 0 \Rightarrow -x > 0$

(2) $(x < y \ \wedge \ z > 0) \Rightarrow xz < yz$

(3) $(x < y \ \wedge \ z < 0) \Rightarrow xz > yz$

(4) $x \neq 0 \Rightarrow x^2 > 0$; speciálisan ha van egységelem akkor az pozitív

(5) Ha 1 az egységelem, $0 < x < y$ és x-nek van multiplikatív inverze, akkor $0 < \frac{1}{y} < \frac{1}{x}$

118. Definiálja a test fogalmát és adjon 3 példát testre.

Egy T gyűrűt testnek nevezünk, ha a nulelemet 0-val jelölve $T \setminus \{0\}$ a szorzással Ábel-csoportot alkot. Példa:$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

119. Definiálja a rendezett test fogalmát, és adjon példát olyan testre, amely nem tehető rendezett testé.

Egy test rendezett test, ha a test rendezett integritási tartomány.

Például $\mathbb{C}$ nem tehető rendezett testé.

120. Fogalmazza meg az Arkhimédészi tulajdonságot.

Egy F rendezett test arkhimédészien rendezett, ha

$$x, y \in F\big(x > 0 \Rightarrow \exists n \in \mathbb{N}(nx \geq y)\big)$$

121. Mi a kapcsolata az arkhimédészi tulajdonságnak a felső határ tulajdonsággal.

Egy felső határ tulajdonságú rendezett test mindig arkhimédészien rendezett.

122. Fogalmazza meg a racionális számok felső határ tulajdonságára és az arkhimédészi tulajdonságára vonatkozó tételt.

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

123. Fogalmazza meg a valós számok egyértelműségét leíró tételt.

Legyen $\mathbb{R}'$*és* $\mathbb{R}''$ két felső határ tulajdonságú rendezett test.

Ekkor létezik φ kölcsönösen egyértelmű leképzése $\mathbb{R}'$-nek $\mathbb{R}''$-re, amely monoton növekvő, összeadás- és szorzástartó.

124. Definiálja a bővített valós számokat.

A bővített valós számok halmaza:$\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$

$\mathbb{R}$ rendezését úgy terjesztjük ki $\overline{\mathbb{R}}$-re, hogy $\forall x \in \mathbb{R}(-\infty < x < +\infty)$

Ellentett képzés:$-(+\infty) = -\infty$ és $-(-\infty) = +\infty$

Összeadás: $x + (+\infty) = (+\infty) + x = +\infty$,ha $x \in \overline{\mathbb{R}}, x > -\infty$

$x + (-\infty) = (-\infty) + x = -\infty$,ha $x \in \overline{\mathbb{R}}, x < +\infty$

de $(+\infty) + (-\infty)$ és $(-\infty) + (+\infty)$ nincs értelmezve.

125. Fogalmazza meg a valós számok létezését leíró tételt.

Létezik felső határ tulajdonságú rendezett test.

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

Minden x≥0 valós szémhoz és $n \in \mathbb{N}^+$ természetes számhoz pontosan egy olyan y ≥ 0 valós szám található, amely $y^n = x$

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

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

128. Definiálja a komplex számok halmazát a műveletekkel.

A komplex számok halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, azaz 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.

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

Ha $x, x' \in \mathbb{R}$, akkor $(x, 0) + (x', 0) = (x + x', 0)$, $(x, 0) \cdot (x', 0) = (xx', 0)$, így az $x \to (x, 0)$ leképezés kölcsönösen egyértelmű, összeadás és szorzás tartóleképezése $\mathbb{R}$-nek $\mathbb{C}$-be, ezért az összes $(x, 0), x \in \mathbb{R}$ alakú számot azonosítjuk $\mathbb{R}$-rel.

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

Jelölje i a (0,1) komplex számot, ekkor z $\in \mathbb{C}$ egyértelműen felírható z=x+iy alakban ahol $x, y \in \mathbb{R}$, ekkor x-et z valós részének(Jele:$\Re(z)$), y-t z képzetes részének (jele:$\Im(z)$) nevezzük, továbbá z konjugáltja $\bar{z} = x - iy$.

Ha a komplex szám valós része 0, akkor képzetes számnak nevezzük.

131. Fogalmazza meg a komplex konjugálás tulajdonságait.

minden $z, w \in \mathbb{C}$-re igaz:

(1) $\bar{\bar{z}} = z$

(2) $\overline{z + w} = \bar{z} + \bar{w}$

(3) $\overline{zw} = \bar{z} \cdot \bar{w}$

(4) z+$\bar{z} = 2\Re(z)$

(5) z-$\bar{z} = 2i\Im(z)$

(6) $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\bar{z}}$

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

$(x, y) \in \mathbb{C}$ szám abszolút értéke $|(x, y)| = \sqrt{x^2 + y^2}$

Felhasznált tétel: Minden x≥0 valós számhoz és $n \in \mathbb{N}^+$ természetes számhoz pontosan egy olyan y ≥ 0 valós szám található, amely $y^n = x$

133. Fogalmazza meg a komplex számok abszolút értékének tulajdonságait.

minden $z, w \in \mathbb{C}$-re igaz:

(1) $z\bar{z}=|z|^2$

(2) $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$ ha $z \neq 0$

(3) $|(x, 0)| = |x|$

(4) $|0| = 0$ és $z \neq 0$ esetén $|z| > 0$

(5) $|\bar{z}| = |z|$

(6) $|zw| = |z||w|$

(7) $|\Re(z)| \leq |z|$

(8) $|\Im(z)| \leq |z|$

(9) $|z + w| \leq |z| + |w|$

(10) $\big||z| - |w|\big| \leq |z - w|$

134. Definiálja komplex számokra sng függvényt és fogalmazza meg tulajdonságait.

Legyen $sng(0) = 0$ $és$ $legyen$ $sng(z) = \frac{z}{|z|}$, ha $0 \neq \mathbb{C}$.

Ekkor $sng(\bar{z}) = \overline{sgn(z)}$ $és$ $|sgn(z)| = 1,$ ha $z \neq 0$.

135. Definiálja komplex számok trigonometrikus alakját és argumentumát.

Ha $0 \neq$z$\in \mathbb{C}$, akkor van t valós szám, amelyre sng(z)=cost+isint.

Ha az összefüggés igaz, akkor a t+$2k\pi$, k$\in \mathbb{Z}$ számokra is, és csak ezekre.

Ekkor z $=$ |z| cos t + isin t, ez a komplex szám trigonometrikus alakja.

Ha $0 \neq$z$\in \mathbb{C}$, akkor z argumentuma az a t valós szám,
amelyre $-\pi < t \leq \pi$ és z $=$ |z| cos t + isin t.

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

$z, w \in \mathbb{C}$, z $=$ |z| cos t + isin t, w $=$ |w| cos s + isin s,

(1) $zw =$ |zw| cos(t + s) + isin (t + s),

(2) $\frac{z}{w} = \frac{|z|}{|w|}$cos(t − s) + isin (t − s),

137. Ha n $\in \mathrm{N}^+$ és w $\in$ C, írja fel a $z^n = w$ egyenlet összes megoldását.

$w = 0$ esetén $z = 0$, különben ha arg(w)=t akkor a

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

különböző komplex számok, és csak ezek azok, amelyek n-edik hatványa w.

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

Ha $w = 1$, akkor az $\varepsilon^n = 1$ feltételnek az $\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right),\ k = 0,1,\dots,n-1$ komplex számok tesznek eleget. Ezeket n-edik komplex egységgyököknek nevezzük. Bizonyos n-edik egységgyökök hatványaiként az összes többi előáll, ezeket n-edik primitív egységgyököknek nevezzük.

139. Ha $\mathrm{n} \in \mathrm{N}^+$ és $\mathrm{w} \in \mathrm{C}$, írja fel a $\mathrm{z}^{\mathrm{n}} = \mathrm{w}$ egyenlet összes megoldását az n-edig egységgyök segítségével.

$$z\varepsilon_0, z\varepsilon_1, \dots, z\varepsilon_{n-1}$$

140. Fogalmazza meg az algebra alaptételét.

Ha $n \in \mathbb{N}^+, c_0, c_1, \dots, c_n \in \mathbb{C}, c_n \neq 0$, akkor $\exists z \in \mathbb{C}\left(\sum_{k=0}^{n} c_k z^k = 0\right)$

141. Definiálja halmazok ekvivalenciáját és sorolja fel tulajdonságait.

X és Y halmaz ekvivalens, ha létezik X-et Y-ra képző bijekció. (jelölése:X~Y).

Ha X,Y,Z halmazok akkor

(1) $X \sim X$ (reflexivitás)

(2) $X \sim Y \Rightarrow Y \sim X$ (szimmetria)

(3) $(X \sim Y \wedge Y \sim Z) \Rightarrow X \sim Z$ tranzitivitás

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

$X \times Y$ és $X' \times Y'$ is ekvivalensek (speciálisan ekvivalens Y^X és $Y'^{X'}$ is).

143. Definiálja a véges és a végtelen halmazok fogalmát.

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

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

Azt az egyértelműen meghatározott n természetes számot, amelyre egy adott X véges halmaz ekvivalens {1,2,…,n}-nel az X halamz elemei számának nevezzük. Jelölése:$|X|, card(X)$.

Felhasználtuk: Egy véges halmaz csak egy n-re ekvivalens a {1,2…,n} halmazzal.

145. Fogalmazza meg a véges halmok és elemszámuk tulajdonságait leíró tételt.

X és Y halmaz, ekkor

(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) $ha\ X\ és\ Y\ végesek\ és\ diszjuktak, akkor\ X \cup Y\ is\ véges\ és\ |X \cup Y| = |X| + |Y|$

(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) $ha\ X\ véges, akkor\ \wp(X)\ is\ véges, és\ |\wp(X)| = 2^{|X|}$

(8) $ha\ X\ véges, és\ az\ f\ függvény\ X\text{-}et\ Y\text{-}ra\ képezi, akkor\ Y\ is\ véges$
$és\ |Y| \leq |X|, és\ ha\ f\ nem\ kölcsönösen\ egyértelmű\ akkor\ |Y| < |X|$

146. Fogalmazza meg a skatulyaelvet.

Ha X és Y véges halmazok, és $|X| > |Y|$, akkor egy f: X → Y leképezés nem lehet kölcsönösen egyértelmű.

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

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

148. Mit mondhatunk egy véges halmaz összes permutációinak számáról?

Egy véges n elemű halmaz permutációinak száma: $P_n = \prod_{k=1}^{n} k$

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

Az {1,2,…,k}-t A-ba képző kölcsönösen egyértelmű leképzéseket az A halmaz k-ad osztályú variációinak nevezzük.

A véges halmaz k-ad osztályú variációinak száma: $V_n^k = \frac{n!}{(n-k)!}$

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

Az {1,2,…,k}-t A-ba képző leképzéseket az A halmaz k-ad osztályú ismétléses variációinak nevezzük.

A véges halmaz k-ad osztályú variációinak száma: ${}^{i}V_n^k = n^k$

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

Az A halmaz k elemű részhalmazait az A halmaz k-ad osztályú kombinációinak nevezzük.

A véges halmaz k-ad osztályú kombinációinak száma: $C_n^k = \frac{n!}{k!(n-k)!}$

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

A halmaz k-ad osztályú ismétléses kombinációi $f: A \to \mathbb{N}$ függvények, amelyekre igaz $\sum_{a \in A} f(a) = k$.

A véges halmaz k-ad osztályú ismétléses kombinációinak száma: ${}^{i}C_n^k = \binom{n+k-1}{k}$

153. Mit értünk véges halmaz ismétléses permutációin és mit mondhatunk az összes ismétléses permutációk számártól.

$r, i_1 i_2 \dots i_r \in \mathbb{N}$ ekkor

$a_1 a_2 \dots a_r$ elemek $i_1 i_2 \dots i_r$ ismétlődésű ismétléses permutációi az olyan $n = i_1 + i_2 + \cdots + i_r$-tagú sorozatok, amelyekben az a_j elem i_j-szer fordul elő.

Ezek száma: $P_n^{i_1 i_2 \dots i_r} = \frac{n!}{i_1! i_2! \dots i_r!}$

154. Fogalmazza meg a binomiális tételt.

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

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

155. 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

156. Menyi a binomiális együtthatók összege, illetve váltakozó előjellel vett összege.

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

157. Fogalmazza meg a polinomiális tételt.

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

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{\substack{i_1 + i_2 + \cdots + i_r = n \\ i_1 i_2 \dots i_r \in \mathbb{N}}} \mathrm{P}_{\mathrm{n}}^{\mathrm{i}_1, \mathrm{i}_2, \dots, \mathrm{i}_r} \, \mathrm{x}_1^{\mathrm{i}_1} \mathrm{x}_2^{\mathrm{i}_2} \dots \mathrm{x}_{\mathrm{r}}^{\mathrm{i}_r}$$

158. Fogalmazza meg a logikai szita formulát.

Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X-en értelmezett, egy Abel-csoportba képző függvény. Legyen

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

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

és legyen

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

Ekkor

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

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

Az m természetes számot az n természetes szám osztójának, az n-et pedig az m többszörösének nevezzük, illetve azt mondjuk, hogy n osztható m-mel, ha $\exists k \in \mathbb{N}(n = m \cdot k)$

jelölése: m|n

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

$n, m \in \mathbb{N}$

(1) $(m|n \wedge m'|n') \Rightarrow mm'|nn'$

(2) $\forall n \in \mathbb{N}(n|0)$

(3) $0|n \Rightarrow n = 0$

(4) $\forall n(1|n)$

(5) $\forall k \in \mathbb{N}(m|n \Rightarrow mk|nk)$

(6) $(k \in \mathbb{N}^+ \wedge mk|nk) \Rightarrow m|n$

(7) $m|n_i \; és \; k_i \in \mathbb{N}, (i = 1,2, \dots, j), akkor \; m| \sum_{i=1}^{j} k_i n_i$

(8) $(n \neq 0 \wedge m|n) \Rightarrow m \le n$

(9) az oszthatóság reláció részbenrendezés

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

n>1 természetes szám törzs szám, ha csak 1n és n1 alakban írható föl természetes számok szorzata ként.

p>1 természetes szám prím szám, ha p|km esetén p|k vagy p|m teljesül.

Minden prím szám törzsszám is, és ha egy szám törzsszám akkor prím is.

162. Definiálja egységelemes integritási tartományban az oszthatóságot és adja meg a jelölést.

Legyen R egységelemes integritási tartomány. Ha $a, b \in R$, azt mondjuk, hogy b az a osztója, vagy a a b többszöröse, illetve hogy a osztható b-val, ha van olyan $c \in R$, hogy $a = bc$.

Jelölése $b|a$.

163. Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

$a, b \in R$, ahol R egységelemes integritási tartomány

(1) $(b|a \wedge b'|a') \Rightarrow bb'|aa'$

(2) $\forall a \in R(a|0)$

(3) $0|a \Rightarrow a = 0$

(4) $\forall a(1|a)$

(5) $\forall c \in R(b|a \Rightarrow bc|ac)$

(6) $(c \neq 0 \wedge bc|ac) \Rightarrow b|a$

(7) $b|a_i$ *és* $c_i \in R, (i = 1,2, \dots, j), akkor\ b|\sum_{i=1}^{j} c_i a_i$

(8) az oszthatóság reláció reflexív és tranzitív

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

Legyen R egységelmes integritási tartomány. Ha $a|b$ és $b|a$, akkor azt mondjuk, hogy a és b asszociáltak.

Ez a reláció reflexív, szimmetrikus és tranzitív, azaz ekvivalenciareláció, továbbá kompatibilis a szorzással.

A nullának nincs más asszociáltja, csak saját maga.

Az | reláció kompatibilis ezzel az ekvivalenciarelációval,

és az ekvivalenciaosztályokon tekintve részbenrendezést kapunk.

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

Egy R rendezett integritási tartományban 1 asszociáltjait egységeknek nevezzük, azaz az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük.

Az egységek a szorzásra nézve Ábel-csoportot alkotnak.

Az egységek R minden elemének osztói.

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

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

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

$\mathbb{N}$-beli állításokat át fogalmazhatjuk $\mathbb{Z}$-re a következők alapján:

$p, n, m \in \mathbb{Z}$ esetén

(1) $m|n\ pontosan\ akkor, ha\ |m||n|\ az\ \mathbb{N}$-ben

(2) Egészek körében egység ± 1, m asszociáltjai $\pm m$

(3) n pontosan akkor felbonthatatlan, ha |n| felbonthatatlan $\mathbb{N}$-ben

(4) p pontosan akkor prím, ha |p| prím $\mathbb{N}$-ben

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

A $G = \{n + im : n, m \in Z\} \subset C$ úgynevezett Gauss-egészek egységelemes integritási tartományt alkotnak.

Nem igaz, hisz a ± 1 és $\pm i$ is egység.

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

R egységelemes integritási tartomány, egy $0 \neq a \in R$ elem irreducibilis, ha nem egység és csak triviális módon írható fel szorzat ként, azaz

$$(a = bc \ \wedge b, c \in R) \Rightarrow b \ vagy \ c \ egység$$

A $0 \neq p \in R$ elemet prímelemnek nevezzük, ha nem egység és
$p|ab \ (a, b \in R) \Rightarrow (p|a \vee p|b)$.

Minden prím elem irreducibilis.

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

Azt mondjuk, hogy az R egységelmes integritási tartományban az $a_1, a_2, \dots, a_n \in R$ elemeknek a $b \in R$ elem legnagyobb közös osztója,

ha $i = 1,2, \dots, n$ esetén $b|a_i$, és ha $i = 1,2, \dots, n$ esetén $b'|a_i$, akkor $b'|b$.

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

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

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

R egységelemes integritási tartomány. Akkor $b \in R$ az $a_1, a_2, \dots, a_n \in R$ elemek legkisebb közös többszöröse,
ha $i = 1,2, \dots, n$ esetén $a_i|b$, és ha $i = 1,2, \dots, n$ esetén $a_i|b'$, akkor $b|b'$.

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

Nem, de ha létezik az $\mathrm{a}_1, \mathrm{a}_2, \dots, \mathrm{a}_\mathrm{n} \in \mathrm{Z}$ számoknak legnagyobb közös osztója, akkor a legnagyobb közös osztók közül az egyik nemnegatív, ezt $\mathrm{lnko}(\mathrm{a}_1, \mathrm{a}_2, \dots, \mathrm{a}_\mathrm{n})$-nel jelöljük.

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

Nem, de ha létezik az $a_1, a_2, \dots, a_n \in Z$ számoknak legkisebb közös többszöröse, akkor a legkisebb közös többszörösök közül az egyik nemnegatív, ezt $lkkt(a_1, a_2, \dots, a_n)$-jelöli.

175. Ismertesse a bővített euklideszi algoritmust.

Ez az eljárás meghatározza az $a, b \in Z$ egészek egy d legnagyobb közös osztóját, valamint az $x, y \in Z$ egész számokat úgy, hogy $d = ax + by$ teljesüljön.

(1) [inicializálás]

$x_0 \leftarrow 1,$

$y_0 \leftarrow 0,$

$r_0 \leftarrow a,$

$x_1 \leftarrow 0,$

$y_1 \leftarrow 1,$

$r_1 \leftarrow b,$

$n \leftarrow 0$

(2) [vége?]

Ha $r_{n+1} = 0$ akkor

$x \leftarrow x_n,$

$y \leftarrow y_n,$

$d \leftarrow r_n,$

eljárás véget ért.

(3) [ciklus]

$q_{n+1} \leftarrow \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor,$

$r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1},$

$x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1},$

$y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1},$

$n \leftarrow n + 1$

ugrás (2)-re.

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

Bármely $a_1, a_2, \dots, a_n \in Z$ számoknak létezik legnagyobb közös osztója, és kisámítása vissza vezethető két szám legnagyobb közös osztójának kiszámítására, az alábbi módon

$lnko(a_1, a_2, \dots, a_n) = lnko(lnko(a_1, a_2), a_3, a_4, \dots, a_n).$

Így a euklideszi algoritmus ismételt alkalmazásával kiszámíthatjuk véges sok egész szám legnagyobb közös osztóját.

177. Fogalmazza meg a számelmélet alaptételét.

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

178. Definiálja prímtényezős felbontásnál a kanonikus alakot.

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

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

A kanonikus alakból leolvashatók $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ pozitív osztói, ezek a

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \ , ahol\ \beta_j \in \mathbb{N}, \beta_j \leq \alpha_j, ha\ j = 1,2, \dots, k$$

Ha több számunk van pl $a_1, a_2, \dots, a_m$, és mindnek adott a prímtényezős felbontása, akkor ezekből hasonló módon kiolvashatók a legnagyobb közös osztóik, és a legnagyobb közös többszöröseik is a következő módon:

$$a_i = p_1^{\alpha_{i_1}} p_2^{\alpha_{i_2}} \dots p_k^{\alpha_{i_k}}, i = 1,2, \dots, m$$

$$lnko(a_1, a_2, \dots, a_m) = p_1^{min\left(\alpha_{1_1}, \alpha_{2_1}, \dots, \alpha_{m_1}\right)} p_2^{min\left(\alpha_{1_2}, \alpha_{2_2}, \dots, \alpha_{m_2}\right)} \dots p_k^{min\left(\alpha_{1_k}, \alpha_{2_k}, \dots, \alpha_{m_k}\right)}$$

$$lkkt(a_1, a_2, \dots, a_m) = p_1^{max\left(\alpha_{1_1}, \alpha_{2_1}, \dots, \alpha_{m_1}\right)} p_2^{max\left(\alpha_{1_2}, \alpha_{2_2}, \dots, \alpha_{m_2}\right)} \dots p_k^{max\left(\alpha_{1_k}, \alpha_{2_k}, \dots, \alpha_{m_k}\right)}$$

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

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

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

Tetszőleges $a_1, a_2, \dots, a_n \in Z$ számoknak létezik legkisebb közös többszöröse, és $lkkt(a_1, a_2, \dots, a_n) = lkkt(lkkt(a_1, a_2), a_3, a_4, \dots, a_n)$.

182. Erathoszthenész szitáját.

Erathoszthenész szitájával egy adott n-ig az összes prímet tudjuk meg találni,az eljárás a következő:

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.

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

Ha $a, b, m \in Z$ és m osztója $a - b$ -nek, akkor azt mondjuk, hogy a és b kongruensek modulo m, jelölése $a \equiv b\ (mod\ m)$.

184. Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

(1) $(a \equiv b\ (mod\ m) \wedge d|m) \Rightarrow a \equiv b\ (mod\ d)$

(2) $a \equiv b\ (mod\ m) \Leftrightarrow 0 \neq d \in \mathbb{Z}\big(ad \equiv bd\ (mod\ md)\big)$

(3) hogy bármely adott $m \in \mathbb{Z}$-re a kongruencia ekvivalenciareláció $\mathbb{Z}$-ben

(4) $a \equiv b\ (mod\ m) \Leftrightarrow a \equiv b\ (mod - m)$

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

Egy $m \in \mathbb{Z}$ 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.

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

Az $m \in \mathbb{Z}$ modulus szerinti kongruencia kompatibilis az összeadással és a szorzással. A maradékosztályok kommutatív egységelemes gyűrűt alkotnak az összeadással és a szorzással. Ezt a gyűrűt jelöljük $\mathbb{Z}_m$-el.

187. Ismertesse a komlemens ábrázolásokat.

Régen használatos volt az egyes komplemens ábrázolás, amikor egy $0 \leq k \leq 2^{n-1}$ szám esetén úgy tároljuk –k-t hogy bitenként komplementáljuk k-t.

Ma inkább használatos a kettes komplemens ábrázolás, amikor egy $0 \leq k \leq 2^{n-1}$ szám esetén úgy tároljuk –k-t hogy –k mod 2^n ketes számrendszerbeli alakját tároljuk, azaz bitenként komplementáljuk, majd hozzá adunk 1.

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

Legyen $m > 1$ egész. Ha $1 < lnko(a, m) < m$, akkor a maradékosztálya nullosztó Z_m-ben.

Ha $lnko(a, m) = 1$, akkor a maradékosztályának van miltiplikatív inverze Z_m-ben. Speciálisan, ha m prímszám, akkor Z_m test.

189. Ismertesse a diszkrét logaritmus problémát.

$\mathbb{Z}_m$-ben könyű hatványozni, de ha m még prím is , $\mathbb{Z}_m$ invertálható elemeinek multiplikatív csoportjában egy a alap és egy a^khatvány ismeretében nehéz meghatározni a k kitevőt, legalább is, ha m− 1-nek vannak nagy prímtényezői, ez a diszkrét logaritmus probléma.

190. Ismertesse Diffie-Hellmann-Merkle-kulcscserét

A két kommunikáló fél megegyezik:

p prímszámban, amelyre q=2p+1 is prímben és egy 1 < g < p-1-ben

A kommunikáció titkosításához szükséges egy közös kulcs. Ekkor két felhasználó

Bob: választ 1 < a < p véletlen számot, publikálja $g^a \ mod \ q$-t

Aliz: választ 1 < b < p véletlen számot, publikálja $g^b \ mod \ q$-t

Ekkor mindketten ki tudják számolni $g^{ab} \ mod \ q$-t, amit használhatnak közös kulcsnak, a vagy b ismerete nélkül a diszkrét logaritmus problémába ütközünk a közös kulcs meghatározásánál.

191. . Definiálja az Euler-féle φ függvényt.

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

192. Mit mondhatunk az $aa_i + b$ számokról, ha a_i egy maradék rendszer, illetve egy redukált maradék rendszer elemeit futja végig.

Legyen $m > 1$ egész szám, a relatív prím m-hez. Ha $a_1, a_2, \dots, a_m$ teljes maradék rendszer modulo m és $b \in \mathbb{Z}$, akkor $aa_1 + b, aa_2 + b, \dots, aa_m + b$ is teljes maradék rendszer modulo m.

Ha $a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradék rendszer modulo m, akkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradék rendszer modulo m.

193. Fogalmazza meg az Euler Fermat-tételt.

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

194. Fogalmazza meg a Fermat-tételt.

Legyen p prímszám.

Ha $a \in Z$ és $p \nmid a$, akkor $a^{p-1} \equiv 1\ (mod\ p)$.

Ha $a \in Z$ tetszőleges, akkor $a^p \equiv a\ (mod\ p)$.

195. Mit értünk diofantikus problémán?

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

196. Mondjon két példát diofantikus problémára.

$x^2 + y^2 = -4, ahol\ x, y \in \mathbb{Z}$ egyenlet megoldásainak megkeresése, vagy a $x^2 + y^2 = z^2, ahol\ x, y, z \in \mathbb{Z}$ egyenlet megoldásainak megkeresése, amiből a Pithagoraszi szám hármasokat kapunk.

197. Fogalmazza meg a kínai maradéktételt.

Legyenek $m_1, m_2, \dots, m_n$ egynél nagyobb, páronként relatív prím természetes számok, $c_1, c_2, \dots, c_n \in Z$. Az $x \equiv c_j\ (mod\ m_j),\ \ j = 1,2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1 m_2 \dots m_n$.

198. Ismertese az RSA eljárást.

Az eljárás úgynevezett nyilvános kulcsú eljárás, az eljárás a következő:

1.lépés: Válasszunk két nagy $p \neq q$ prímet

2.lépés: legyen n=pq, válszunk egy $1 < e < (p-1)(q-1)$ nyilvános kulcsot, ezt a két értéket fogjuk nyilvánosságra hozni.

3.lépés: d titkos kulcs meg határozása az $ed \equiv 1\ \big(mod\ (p-1)(q-1)\big)$ kongruencia megoldásával, ha nincs megoldása elölről kezdjük.

Ekkor a nyilvános kulcs segítségével kódolt üzenet küldhető nekünk. ha $1 < m < n$ üzenet, akkor anak kódolt formája $c = m^e\ mod\ n$.

Ezt a $m = c^d\ mod\ n$ módon dekódolhatjuk.

199. Ismertesse az RSA eljárás felhasználását digitális aláírásra.

Az RSA felhasználható digitális aláírásra is, hisz a két kulcs szerepe szimmetrikus: Aliz elküldi m üzenet és $m^{d_A}\ mod n_A$ értékét is, ahol d_A, n_A Aliz titkos kulcsa: ez az aláírás, mert csak Aliz volt képes kiszámítani.

200. Ismertesse az RSA eljárás felhasználását bizonyítványok kiállítására.

Az eljárás bizonyítványok kiállítására is használatos. Egy hitelesítő szervezettől – aminek nyilvános kulcsát mindenki ismeri – digitálisan aláírt levélben kapjuk meg Aliz nyilvános kulcsát, így ellenőrizhetjük Aliz digitális aláírását.

Bizonyítások

1) Fogalmazza meg a halmazok uniójának kommutativitását, aszociativitását és idempotenciálját és bizonyítsa be.

   (1) $A \cup B = B \cup A$ (kommutativitás)

   A baloldalnak, akkor eleme x, ha $x \in A \vee x \in B$

   A jobboldalnak, akkor eleme x, ha $x \in B \vee x \in A$

   A két állítás ekvivalens a vagy művelet kommutativitása miatt. ■

   (2) $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás)

   A baloldalnak, akkor eleme x, ha $x \in A \vee (x \in B \vee x \in C)$

   A baloldalnak, akkor eleme x, ha $(x \in A \vee x \in B) \vee x \in C$

   A két állítás ekvivalens a vagy művelet asszociativitása miatt. ■

   (3) $A \cup A = A$ (idempotencia)

   Az egyenlőség mind két oldalán álló halmaznak pontosan akkor eleme x, ha $x \in A$ ■

2) Fogalmazza meg a halmazok metszetének kommutativitását, aszociativitását és idempotenciálját és bizonyítsa be.

   (1) $A \cap B = B \cap A$ (kommutativitás)

   A baloldalnak, akkor eleme x, ha $x \in A \wedge x \in B$

   A jobboldalnak, akkor eleme x, ha $x \in B \wedge x \in A$

   A két állítás ekvivalens az és művelet kommutativitása miatt. ■

   (2) $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás)

   A baloldalnak, akkor eleme x, ha $x \in A \wedge (x \in B \wedge x \in C)$

   A baloldalnak, akkor eleme x, ha $(x \in A \wedge x \in B) \wedge x \in C$

   A két állítás ekvivalens a vagy művelet asszociativitása miatt. ■

   (3) $A \cap A = A$ (idempotencia)

   Az egyenlőség mind két oldalán álló halmaznak pontosan akkor eleme x, ha $x \in A$ ■

3) Fogalmazza meg és bizonyítsa be az unió és a metszet disztributivitását.

   A,B,C halmazok

   <u>A metszet disztributivitása az unióra nézve</u>

   $$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

   Az $A \cap (B \cup C)$ halmaznak x pontosan akkor eleme, ha $x \in A \wedge x \in B \cup C$.

   így $x \in A \cap (B \cup C) \Leftrightarrow x \in A \wedge (x \in B \vee x \in C)$

   Ez viszont ekvivalens azzal, hogy $x \in (A \cap B) \cup (A \cap C)$ ■

   <u>Az unió disztributivitása a metszetre nézve</u>

   $$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

   Az $A \cup (B \cap C)$ halmaznak x pontosan akkor eleme, ha $x \in A \wedge x \in B \cap C$.

   így $x \in A \cup (B \cap C) \Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$

   Ez viszont ekvivalens azzal, hogy $x \in (A \cup B) \cap (A \cup C)$ ■

4) Fogalmazza meg és bizonyítsa be a De Morgan azonosságokat két halmazra.

(1) $(A \cup B)' = A' \cap B'$

x pontosan akkor eleme a baloldalnak, ha nem eleme $A \cup B$

így $x \in (A \cup B)' \Leftrightarrow \neg(x \in A \vee x \in B) \Leftrightarrow \big((\neg\, x \in A) \wedge (\neg x \in B)\big) \Leftrightarrow x \in A' \cap B'$

■

(2) $(A \cap B)' = A' \cup B'$

(3) x pontosan akkor eleme a baloldalnak, ha nem eleme $A \cap B$

(4) így$x \in (A \cap B)' \Leftrightarrow \neg(x \in A \wedge x \in B) \Leftrightarrow \big((\neg\, x \in A) \vee (\neg x \in B)\big) \Leftrightarrow x \in A' \cap B'$

■

5) Bizonyítsa be, hogy binér relációk kompozíciója asszociatív.

Legyen R,S,T binér reláció.

A kompozíció definícióját felhasználva:

$$R \circ (S \circ T) = \Big\{(x,y)\colon \exists z \Big((z,y) \in R \wedge (x,z) \in \big\{(x,z)\colon \exists w\big((w,z) \in S \wedge (x,w) \in T\big)\big\}\Big)\Big\} =$$
$$= \big\{(x,y)\colon \exists z,w\big((z,y) \in R \wedge (w,z) \in S \wedge (x,w) \in T\big)\big\} =$$
$$= \big\{(x,y)\colon \exists w\big((x,w) \in T \wedge (w,y) \in R \circ S\big)\big\} = (R \circ S) \circ T$$

■

6) Fogalmazza meg két binér reláció kompozíciójának inverzére vonatkozó állítást és bizonyítsa be.

Legyen R, S binér reláció, ekkor $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$

$$(R \circ S)^{-1} = \big\{(y,x)\colon \exists z\big((z,y) \in R \wedge (x,z) \in S\big)\big\} = \big\{(y,x)\colon \exists z\big((y,z) \in R^{-1} \wedge (z,x) \in S^{-1}\big)\big\} =$$
$$= S^{-1} \circ R^{-1}$$

■

7) Fogalmazza meg az ekvivalencia reláció és az osztályozás kapcsolatát és bizonyítsa be.

<u>Tétel:</u>

Valamely X halmazon értelmezett ~ ekvivalencia reláció esetén a $\tilde{x} = \{y \in X\colon y \sim x\}, x \in X$ ekvivalenciaosztályok X-nek egy $\tilde{X} = X/\sim$ osztályozását adják.

<u>Megfordítva</u>

az X halmaz bármely $\mathcal{O}$ osztályozása esetén az $\cup \{Y \times Y\colon Y \in \mathcal{O}\}$ reláció ekvivalencia reláció, amelyhez tartozó ekvivalenciaosztályok halmaza $\mathcal{O}$.

Hasonlóan, ha egy ekvivalenciarelációra képezzük az ekvivalenciaosztályokat, majd ebből a hozzátartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza.

Bizonyítás:

Legyen ~ egy X-beli ekvivalencia reláció, és legyen $\tilde{x} = \{y \in X: y \sim x\}$ X halmaz x elemének ekvivalencia osztálya

Bizonyítandó: $\tilde{X} = \{\tilde{x}: x \in X\}$ halmaz az X egy osztályozása

(1) ~ reflexív, így $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az X halmaz minden eleme bene van $\tilde{X}$ valamely elemében.

(2) különböző ekvivalencia osztályok metszete üres.
Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme.
Ekkor $z \sim x \ \wedge \ z \sim y$, ebből a tranzitivitás és a szimmetria miatt $x \sim y$
Így a tranzitivitás miatt $w \in \tilde{x} \Rightarrow w \in \tilde{y}$
Továbbá a tranzitivitás és a szimmetria miatt $w \in \tilde{y} \Rightarrow w \in \tilde{x}$
Tehát $\tilde{x} = \tilde{y}$, azaz $\tilde{x}$ részhalmazok diszjuktak

ezért valóban az X egy osztályozását kapjuk

Megfordítva, legyen az $\mathcal{O}$ az X egy osztályozása, és legyen $R = \cup \{Y \times Y: Y \in \mathcal{O}\}$

Ekkor $(x, y) \in R$, pontosan akkor teljesül, ha x és y $\mathcal{O}$ ugyanazon halmazának elemei.

Ekkor R reflexív, szimmetrikus, és a mivel az osztályok páronként diszjuktak tranzitív is, tehát ekvivalencia reláció.

Nyilván való, hogy ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a megfelelő ekvivalenciaosztályokat, akkor az eredeti osztályozást kapjuk vissza, és fordítva, ha egy ekvivalenciarelációból képezünk a fentiek szerint hozzá tartozó osztályozást, majd abból a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza.

■

8) Fogalmazza meg a szigorú részbenrendezés kapcsolatát a részbenrendezéssel és bizonyítsa be állítását.

Egy $\leq$ részbenrendezés esetén a megfelelő szigorú relációt <-el jelöljük; ez nyilván irreflexív és tranzitív

Ha $x < y$ és $y < z, akkor\ x \leq$ y és y $\leq$ z, ahonnan $x \leq$ z. Ha $x = z$ lenne, akkor teljesülne $y \leq$ x ,így $x = y$ is ellentmondás.

A tranzitivitásból és az irreflexitásból következik a szigorú antiszimetria: $x < y\ esetén\ y > x\ nem\ teljes$ülhet, mert ebből $x < x$ következne.

Megfordítva

ha < egy X-beli szigorú részbenrendezés, amin egy tranzitív és szigorúan antiszimmetrikus (szükség képen irreflexiv) relációt értünk, akkor a megfelelő gyenge reláció egy részben rendezés.

Tehát egy részbenrendezésből kapott szigorú részbenrendezésből ily módon az eredeti részbenrendezést kapjuk vissza, ha pedig egy szigorú részbenrendezésből készítünk egy részben rendezést, majd abból a megfeleő szigorú részbenrendezést, akkor az eredeti szigorú részben rendezést kapjuk vissza.

■

9) Mi a kapcsolat a szigorúan monoton növekvő és a kölcsönösen egyértelmű függvények között? A megfogalmazott állítást bizonyítsa be.

Ha X és Y rendezett, akkor $f: X \to Y$ szigorúan monoton növekvő függvény nyilván kölcsönösen egyértelmű is.

Megfordítva, ha X és Y rendezett, akkor egy $f: X \to Y$ kölcsönösen egyértelmű monoton növő leképzés szigorúan monoton növekvő.

Bizonyítás

f(X)-en:

ha $x < y \; akkor \; f(x) \leq f(y)$, de $f(x) = f(y)$ nem lehetséges

■

10) Mit állíthatunk a monoton növekvő függvények inverz függvényekről? A megfogalmazott állítást bizonyítsa be.

Ha X és Y rendezett, akkor egy $f: X \to Y$ kölcsönösen egyértelmű monoton növő leképzés inverz függvénye szigorúan monoton növekvő.

Bizonyítás

f(X)-en:

ha $x < y \; akkor \; f(x) \leq f(y)$, de $f(x) = f(y)$ nem lehetséges

és ha $u, v \in f(X), u < v, x = f^{-1}(u), y = f^{-1}(v), akkor \; x \geq y \; nem \; lehetséges$, mert ebből $f(x) \geq f(y)$, azaz $u = f(x) > f(y) = v$ következne.

■

11) Fogalmazza meg az indexelt halmazcsaládokra vonatkozó De Morgan szabályokat és bizonyítsa be őket.

$(\cup_{i \in I} X_i)' = \cap_{i \in I} X_i'$

$(\cup_{i \in I} X_i)' = \{x: \exists i \in I(x \in X_i)\}' = \{x: \forall i \in I(x \notin X_i)\} = \{x: \forall i \in I(x \in X_i')\} = \cap_{i \in I} X_i'$

■

$(\cap_{i \in I} X_i)' = \cup_{i \in I} X_i'$

$(\cap_{i \in I} X_i)' = \{x: \forall i \in I(x \in X_i)\}' = \{x: \exists i \in I(x \notin X_i)\} = \{x: \exists i \in I(x \in X_i')\} = \cup_{i \in I} X_i'$

■

12) Bizonyítsa be, hogy a természetes számok halmaza a $\leq$ relációval jól rendezett. Azt, hogy rendezett nem kell bizonyítani.

Legyen $\emptyset \neq A \subset \mathbb{N}$

Legyen $B = \{m \in \mathbb{N}: \forall n \in A(m \leq n)\}$ Nyilván $0 \in B$

Ha $n \in A \; akkor \; n^+ \notin B$

$\exists m \in B, amelyre \; m^+ \notin B$,mert különben indukcióval azt kapnánk, hogy $B = \mathbb{N}$

Bizonyítandó: m az A legkisebb eleme. Az világos hogy alsó korlát, azt kell belátni: $m \in A$

Indirekt bizonyítás

Ha $m \notin A$ akkor minden $n \in A$-ra m<n lenne, amiből $m^+ \leq n$ következne, mert m-et ez ellent mondás mert $m^+ \notin B$

■

13) Fogalmazza meg és bizonyítsa be a maradékos osztás tételét.

Legyen $n > 0$ rögzített természetes szám.

Minden $m \in \mathbb{N}$ egyértelműen felírható $m = qn + r\ alakban, ahol\ q, r \in \mathbb{N}$ és $r < n$

Bizonyítás

Mivel $kn \leq k$, van olyan $k, amelyre\ kn > m$, pl $k = m^+$

Legyen k a legkisebb természetes szám, amelyre $kn > m$. Nyilván $k \neq 0$, így $k = q^+$ valamely $q \in \mathbb{N}$-re. Mivel $qn \leq m$ van olyan r$\in \mathbb{N}$, amelyre $m = qn + r$.

Ha $r \geq n$ lenne, akkor $m \geq qn + n = kn > m$ adódna.

Egyértelműség bizonyítása

Tegyük fel, hogy $m = q'n + r'$, ahol $r' < n$.

Ha például $q' > q$, akkor $m = q'n + r \geq q'n \geq (q+1)n > qn + r = m$ ellentmondás, és hasonlóan $q' < q$ is ellentmondásra vezet.

Így $q = {}'q$, amiből az egyszerűsítési szabály alapján $r = r'$

■

14) Fogalmazza meg és bizonyítsa be a számrendszerekre vonatkozó tételt.

Legyen q>1, $q \in \mathbb{N}$

Minden m>0 természetes számhoz, egy és csak egy olyan n természetes szám és $a_0, a_1 \ldots a_n \in [0, q[\subset \mathbb{N}$ sorozat létezik, amelyre

$$a_n \neq O\ és\ m = \sum_{i=0}^{n} a_i \cdot q^i$$

Bizonyítás:

Osszuk maradékosan m-et q-val

$$m = m'q + r,\ ahol\ m', r \in \mathbb{N}\ és\ r < q$$

Teljes indukció:

kezdő lépés

Ha $m' = 0$, akkor $n = 0,\ a_0 = r$ esetben teljesül

Indukciós lépés

Ha $m' \neq 0$, akkor $m' < m$

Indukciós feltevés: m egyértelműen felírható $\sum_{i=0}^{n} a_i \cdot q^i$ alakban

Az indukciós feltevés alapján m' is felírható egyértelműen
$m' = a_1 + a_2 q + \cdots + a_{n+1} q^n$ alakban.

A maradékos osztásból következik a_0 egyértelműsége, a teljes indukcióból az állítás

■

15) Definiálja a bal és a jobb oldali nullosztó és a nullosztópár fogalmát. Adjon meg két lényegessen különböző, nullosztókkal kapcsolatos állítást, és bizonyítsa be őket.

Ha x,y egy R gyűrű 0-tól különböző elemei, és xy=0, akkor x és y nullosztópár, x bal oldali nullosztó, y jobboldali nullosztó.

(1) Nullosztó mentes gyűrűben lehet nem nulla elemmel szorzásnál jobbról is és balról is egyszerűsíteni.

$ha\ xy = xz, akkor\ x(y - z) = 0, és\ ha\ x \neq 0, akkor\ y - z = 0$
tehát $y = z$

Hasonlóan adódik $yx = zx$ és $x \neq 0\ akkor\ y = z$

■

(2) Ha a gyűrűben van a nullától különböző egységelem, és x-nek van multiplikatív inverze, akkor x nem lehet, sem bal sem jobb oldali nullosztó, hiszen

$xy = 0$-ból, illetve $yx = 0$-ból $x^{-1}xy = y = 0$, $illetve\ yxx^{-1} = y = 0$ adódik.

■

16) Fogalmazza meg szükséges és elégséges feltételét annak, hogy egy integritási tartomány rendezett integritási tartomány legyen, és bizonyítsa be az állítást.

Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fenn állnak.

(1) $x, y, z \in R(x < y \Rightarrow x + z < y + z)$ (Az összeadás szigorúan monoton)

Ha az összeadás monoton és $x < y$, akkor $x \leq y$ *és* $x + z \leq y + z$, de az egyenlőség nem teljesülhet, mert akkor $x = x + z - z = y + z - z = y$ következne.

Az állításból következik, hogy az összeadás monoton, hisz az egyenlőség esete triviális.

(2) $x, y \in R(x, y > 0 \Rightarrow x \cdot y > 0)$ (A szorzás szigorúan monoton)

A szorzás monoton, és $x, y > 0$, akkor $x, y \geq 0$, így $xy \geq 0$. Ha $xy = 0$ lenne, akkor x és y egy nullosztópár lenne, ami lehetetlen.

Az állításból következik a szorzás monotonitása, hisz gyűrűben $x0 = 0y = 0$

17) Fogalmazza meg a rendezett integritási tartományban az egyenlőtlenségekkel való számolás szabályait leíró tételt és bizonyítsa be.

(1) $x > 0 \Rightarrow -x < 0$ *és* $x < 0 \Rightarrow -x > 0$

Ha $x > 0, akkor\ 0 = -x + x$

$$x > 0$$
$$-x + x > -x + 0$$
$$0 > -x$$

Ha $x < 0, akkor\ 0 = -x + x$

$$x < 0$$
$$-x + x < -x + 0$$
$$0 < -x$$

(2) $(x < y \ \wedge \ z > 0) \Rightarrow xz < yz$

$$y - x > x - x$$
$$y - x > 0$$

A szorzás monoton, így

$$(y - x)z > 0$$
$$yz - xz > 0$$
$$yz > xz$$

(3) $(x < y \ \wedge \ z < 0) \Rightarrow xz > yz$

$$-\big((y - x)z\big) > 0$$
$$(y - x)(-z) > 0$$
$$-yz + xz > 0$$
$$xz > yz$$

(4) $x \neq 0 \Rightarrow x^2 > 0$; speciálisan ha van egységelem akkor az pozitív

$$Ha\ x > 0\ akkor\ x^2 > 0$$
$$Ha\ x < 0\ akkor - x >, így\ x^2 = (-x)^2 > 0$$

(5) Ha 1 az egységelem, $0 < x < y$ és x-nek van multiplikatív inverze, akkor $0 < \frac{1}{y} < \frac{1}{x}$

Ha $y > 0$ és $v \leq 0$ $akkor$ $yv \leq 0$

De $y \cdot \frac{1}{y} = 1 > 0$

Ha $x > 0$ és $v \leq 0$ $akkor$ $xv \leq 0$

De $x \cdot \frac{1}{x} = 1 > 0$

$$x < y$$

A (2) állítás alapján szorzunk $\frac{1}{x}\frac{1}{y}$

$$\frac{1}{y} < \frac{1}{x}$$

■

18) Van-e olyan racionális szám, amelynek a négyzete 2? Bizonyítsa be állítását.

Nincs, hisz ha volna, akkor:

Legyen $a, b \in \mathbb{Z}$

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

Következik, hogy a^2 $páros, de$ $akkor$ a $is, tehát$ $legyen$ $a = 2a', ahol$ $a' \in \mathbb{Z}, ekkor$

$$2b^2 = 4a'^2$$

$$b^2 = 2a'^2$$

$$Tehát$$ b is $páros$ $legyen$ $b = 2b', ahol$ $b' \in \mathbb{Z}, ekkor$

$$2 = \frac{a^2}{b^2} = \frac{(2a)'^2}{(2b')^2} = \frac{a'}{b'}$$

Így $a' és b'$ is biztos páros, de ez azt jelentené, hogy az keresett számot akárhányszor el osztjuk 2-vel, akkor is páros számot kapnánk, ami ellent mondás. ■

19) Fogalmazza meg az arkhimédeszi tulajdonságot. Mi a kapcsolata a felső határ tulajdonsággal? Bizonyítsa be állítását.

Egy F rendezett test arkhimédeszien rendezet, ha $x, y \in F, x > 0$ esetén

$$\exists n \in \mathbb{N}(nx \geq y)$$

Egy felső határ tulajdonságú rendezett test mindig arkhimédeszien rendezett.

Indirekt Bizonyítás:

Ellenkező esetben $A = \{nx : n \in \mathbb{N}\}$-nek y a felső korlárja lenne.

Legyen $z = \sup A$

Mivel $z - x < z$ $z - x$ *már nem felső korlát*

így $\exists n \in \mathbb{N}(nx > z - x)$

De ebből $(n+1)x > z$ ami ellentmondás.

■

20) Bizonyítsa be, hogy a racionális számok rendezett teste nem felső határ tulajdonságú.

Legyen A az össze olyan r>0 racionális számok halmaza, amelyre $r^2 < 2$ és legyen B az összes olyan r>0 racionális számok halmaza, amelyre $r^2 > 2$. Legyen

$$s = r - \frac{r^2 - 2}{r + 2} = \frac{2r + 2}{r + 2}$$

Ekkor

$$s^2 - 2 = \frac{2(r^2 - 2)}{(r + 2)^2}$$

$Ha\ r \in A, akkor\ s > r, de\ s^2 < 2, azaz\ s \in A$, így A-nak nincs legnagyobb eleme.

$Ha\ r \in B, akkor\ s < r, de\ s^2 > 2, azaz\ s \in B$, így A-nak nincs legkisebb eleme.

Tehát A-nak nincs $\mathbb{Q}$-ban legkisebb eleme, hisz A-ban nem lehet, hisz nincs legnagyobb eleme, B-ben sem lehet hisz nincs legkisebb eleme.

■

21) Definiálja a valós számok alsó és felső egész részét, és bizonyítsa be ezek létezését.

Legyen $\lfloor x \rfloor, az\ x\ alsó\ egész\ része$ az a legnagyobb eleme $\mathbb{Z}$-nek, amely nem nagyobb mint x, és legyen $\lceil x \rceil$, az x felső egész része az a legkisebb eleme $\mathbb{Z}$-nek, amely nem kisebb, mint x.

Létezés bizonyítása:

$x = 0$ eset triviális (mind kettő 0)

Ha $x > 0$ akkor az arkhimédeszi rendezettségből és a természetes számok jól rendezettségéből adódik, hogy van az x-nél nagyobb vagy egyenlő természetes számok között egy legkisebb n természetes szám, ez a $\lceil x \rceil$.

Nyilván $n > 0$. Ha $n = x$, akkor $\lfloor x \rfloor = \lceil x \rceil = n$, egyébként $\lfloor x \rfloor = n - 1$.

Ha $x < 0$,akkor $\lceil x \rceil = -\lfloor -x \rfloor$ *és* $\lfloor x \rfloor = -\lceil -x \rceil$.

22) Definiálja a komplex számok halmazát a műveletekkel és bizonyítsa be, hogy test.

A komplex számok halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, azaz 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.

Állítás: A komplex számok halmaza testet alkot az összeadással és a szorzással.

Bizonyítás:

A nulelem a (0,0) pár, az (x,y) pár additiv inverze az (-x,-y) pár, egységelem a (1,0) pár, az egységelemtől különböző (x,y) pár multiplikatív inverze az $\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$ pár.

23) Fogalmazza meg a komplex számok abszolút értékének tulajdonságait és bizonyítsa be.

Legyen $z = x + iy$

(1) $z\bar{z}=|z|^2$

$$(x - yi)(x + yi) = x^2 - (iy)^2 = x^2 + y^2 = |x + iy|^2$$

(2) $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$ ha $z \neq 0$

(1)-ből következik

(3) $|(x, 0)| = |x|$

$$|(x, 0)| = \sqrt{x^2 + 0} = |x|$$

(4) $|0| = 0$ és $z \neq 0$ esetén $|z| > 0$

definícióból következik, hisz a négyzet gyök értéke mindig pozitív

(5) $|\bar{z}| = |z|$

$$|\bar{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$$

(6) $|zw| = |z||w|$

Hisz mindkét oldal négyzete $z\bar{z}w\bar{w}$

(7) $|\Re(z)| \leq |z|$

$|x| \leq \sqrt{x^2 + y^2}$ hisz a négyzetgyök függvény monoton növő

(8) $|\Im(z)| \leq |z|$

$|y| \leq \sqrt{x^2 + y^2}$ hisz a négyzetgyök függvény monoton növő

(9) $|z + w| \leq |z| + |w|$

$$|z + w|^2 = (z + w)\overline{(z + w)} = (z + w)(\bar{z} + \bar{w}) = z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} =$$
$$= z\bar{z} + z\bar{w} + \overline{z\bar{w}} + w\bar{w} = |z|^2 + 2\Re(z\bar{w}) + |w|^2$$

$$|z|^2 + \Re(z\bar{w}) + |w|^2 \leq |z|^2 + 2|z\bar{w}| + |w|^2$$

$$|z|^2 + 2|z\bar{w}| + |w|^2 = |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2$$

(10) $\big||z| - |w|\big| \leq |z - w|$

$$|z| \leq |z - w| + |w|$$
$$|z| - |w| \leq |z - w|$$
$$|w| \leq |z - w| + |z|$$
$$|w| - |z| \leq |z - w|$$

■

24) Bizonyítsa be, hogy egyetlen $n \in \mathbb{N}$-re sem létezik ekvivalencia {1,2..n} és egy valódi részhalmaza közt.

Indukcióval:

n=0-ra triviális, hisz az üres halmaznak nincs valódi részhalmaza.

n>0

Tegyük fel, hogy n-re teljesül, de létezik egy f kölcsönösen egyértelmű leképzése {1,2,…,n+1}-nek egy A valódi részhalmazára.

Ha $n+1 \notin A$, akkor f megszorítása {1,2,…,n}-re is létezik egy kölcsönösen egyértelmű leképzés, mégpedig {1,2,..,n}-nek egy valódi részhalmazára, mivel f(n+1) nem lesz az értékkészletben, ami ellent mond az indukciós feltevésnek

Ha $f(k) = n+1 \in A$, akkor viszont úgy kapjuk {1,2,…,n} és A\{n+1} egy ekvivalenciáját, hogy (k,n+1) és az (n+1,l) párokat kihagyjuk a leképezésből és helyettük a (k,l) párt vesszük be. Ez megint ellent mond az indukciós feltevésnek.

25) Fogalmazza meg a véges halmazok és elemszámuk tulajdonságait leíró tételt és bizonyítsa be.

X és Y halmaz, ekkor

(1) $ha\ X\ véges\ és\ Y \subset X, akkor\ Y\ is\ véges\ és\ |Y| \leq |X|$

(2) $ha\ X\ véges\ és\ Y \subsetneq X, akkor\ |Y| < |X|$

$$y = X\ trivi$$

$Y \subsetneq X$, akkor tudjuk, hogy $Y \sim Z \subsetneq \{1,2,\dots,|X|\}$
de tudjuk hogy $Z \sim \{1,2,\dots,m\}$, $ahol\ m < n$

(3) $ha\ X\ és\ Y\ végesek\ és\ diszjuktak, akkor\ X \cup Y\ is\ véges\ és\ |X \cup Y| = |X| + |Y|$

$$X \sim \{1,2,\dots m\}\ és\ Y \sim \{1,2,\dots,n\} \sim \{m+1, m+2, \dots m+n\}$$

(4) $ha\ X\ és\ Y\ végesek, akkor\ |X \cup Y| + |X \cap Y| = |X| + |Y|$

(3) alapján

$$|X \cup Y| = |X \backslash Y| + |X \cap Y| + |Y \backslash X|$$

Írja be az egyenletet ide(3) alapján

$$|X \cup Y| + |X \cap Y| = |X \backslash Y| + |X \cap Y| + |X \cap Y| + |Y \backslash X| = |X| + |Y|$$

(5) $ha\ X\ és\ Y\ végesek, akkor\ X \times Y\ is\ véges, és\ |X \times Y| = |X| \cdot |Y|$

|Y|=0 trivi

indukciós feltevés: ha Y~{1,2,…,n},akkor $|X \times Y| = |X| \cdot |Y|$

ha Y~{1,2,…,n+1}, akkor is igaz, hisz a szorzás definíciója alapján:

$$|X \times \{1,2,\dots,\mathrm{n}+1\}| = |X| \cdot |\{1,2,\dots,\mathrm{n}+1\}|$$

$$bal\ oldal: |X \times \{1,2,\dots,\mathrm{n}+1\}| = |X \times \{1,2,\dots,\mathrm{n}\} \cup X \times \{\mathrm{n}+1\}| = |X \times \{1,2,\dots,\mathrm{n}\}| + |X \times \{\mathrm{n}+1\}| = |X| \cdot |\{1,2,\dots,\mathrm{n}\}| + |X| = |X| \cdot (n+1)$$

■

(6) $ha\ X\ és\ Y\ végesek, akkor\ X^Y\ is\ véges, és\ |X^Y| = |X|^{|Y|}$

|Y|=0 trivi

indukciós feltevés: ha Y~{1,2,…,n},akkor $|X^Y| = |X|^{|Y|}$

ha Y~{1,2,…,n+1}, akkor is igaz, hisz a szorzás definíciója alapján:

$\left|X^{\{1,2,\dots,\mathrm{n}+1\}}\right| = |X|^{|\{1,2,\dots,\mathrm{n}+1\}|}$

$$bal\ oldal: \left|X^{\{1,2,\dots,\mathrm{n}+1\}}\right| = \left|X^{\{1,2,\dots,\mathrm{n}\}} \times X^{\{\mathrm{n}+1\}}\right| = \left|X^{\{1,2,\dots,\mathrm{n}\}}\right| \cdot \left|X^{\{\mathrm{n}+1\}}\right| = |X|^{|\{1,2,\dots,\mathrm{n}\}|} \cdot |X| = |X|^{(n+1)}$$

■

(7) $ha\ X\ véges, akkor\ \wp(X)\ is\ véges, és\ |\wp(X)| = 2^{|X|}$

(6)-ból következik $\wp(X)$-nek a karakterisztikusfüggvények halmazával való ekvivalenciásából.

(8) $ha\ X\ véges, és\ az\ f\ függvény\ X\text{-}et\ Y\text{-}ra\ képezi, akkor\ Y\ is\ véges$
$és\ |Y| \leq |X|, és\ ha\ f\ nem\ kölcsönösen\ egyértelmű\ akkor\ |Y| < |X|$

$$Tegyük\ fel, hogy\ X = \{1,2,\dots,|X|\}$$

$\forall y \in Y$-ra legyen $g(y)$ az $f^{-1}(y)$ halmaz legkisebb eleme. Ekkor g az Y-t kölcsönösen egyértelműen képezi le X egy részhalmazára, ha f nem volt kölcsönösen egyértelmű, akkor nyilván ez a részhalmaz valódi.

26) Fogalmazza meg a skatulya elvet és bizonyítsa be.

Ha X és Y véges halmazok, és $|X| > |Y|$, akkor egy $f: X \to Y$ leképezés nem lehet kölcsönösen egyértelmű.

Bizonyítás: Különben az $|X| > |Y|$, miatt {1,2,…,|X|} egy valódi részhalmaza ekvivalens lenne {1,2,…,|X|}-nel, ami ellent mondás.

27) Mit mondhatunk véges halmazban minimális és maximális elem létezéséről. Bizonyítsa be állítását.

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

A részhalmaz elemeinek száma szerinti indukció:

|A|=1 trivi

Ha |A|=n+1, legyen $a \in A$ és $A' = A\{a\}$

Ekkor, ha $a \leq a', ahol\ a'A' maximáliseleme$, Akkor $a' maximális\ elem$, különben $a\ maximális\ elem$.

28) Mit mondhatunk egy véges halmaz összes permutációinak számáról? Bizonyítsa be állítását.

Egy véges n elemű halmaz permutációinak száma: $P_n = \prod_{k=1}^{n} k = n!$

Indukció:

$P_1 = 1$ teljesül.

Legyen f és g két permutáció.

Legyen $f \sim g$, ha $f(n) = g(n)$, ekkor

Ekvivalencia osztályok száma: n+1

Ekvivalencia osztályok mérete P_n

Így $P_{n+1} = P_n \cdot (n+1) \coloneqq (n+1)!$

29) Mit értünk egy véges halmaz variációin és mit mondhatunk az összes variációk számáról? Bizonyítsa be állítását.

Az {1,2,…,k}-t A-ba képző kölcsönösen egyértelmű leképzéseket az A halmaz k-ad osztályú variációinak nevezzük.

A véges halmaz k-ad osztályú variációinak száma:$V_n^k = \frac{n!}{(n-k)!}$

Legyen f és g két permutáció.

Legyen $f \sim g$, ha {1,2,…,k}-en megegyeznek, ekkor

Ekvivalencia osztályok száma: V_n^k

Ekvivalencia osztályok mérete $(n-k)!$

Össz méret P_n

Így $P_n = P_{n-k} V_n^k$

30) Mit értünk egy véges halmaz kombinációin és mit mondhatunk az összes kombinációk számáról? Bizonyítsa be állítását.

Az A halmaz k elemű részhalmazait az A halmaz k-ad osztályú kombinációinak nevezzük.

A véges halmaz k-ad osztályú kombinációinak száma:$\mathrm{C_n^k} = \frac{\mathrm{n!}}{\mathrm{k!(n-k)!}}$

Legyen f *és* g két variáció.

Legyen $f \sim g$, ha az érték készletük ugyan az, ekkor

Ekvivalencia osztályok száma: C_n^k

Ekvivalencia osztályok mérete $k!$

Össz méret V_n^k

Így $V_n^k = C_n^k k!$

31) Mit értünk egy véges halmaz ismétléses kombinációin és mit mondhatunk az összes ismétléses kombinációk számáról?

A halmaz k-ad osztályú ismétléses kombinációi $f: A \to \mathbb{N}$ függvények, amelyekre igaz $\sum_{a \in A} f(a) = k$.

A véges halmaz k-ad osztályú ismétléses kombinációinak száma: ${}^{i}C_n^k = \binom{n+k-1}{k}$

Legyen

$g: \{1,2, \dots, k\} \to \{1,2, \dots n\}$ monoton növekvő függvényhez definiáljuk h-t

legyen $h(i) = g(i) + i - 1$

Ezzel kölcsönösen egyértelmű megfeleltetést létesíthetünk az $\{1,2, \dots, k\} \to \{1,2, \dots n\}$ monoton növekvő és a $\{1,2, \dots, k\} \to \{1,2, \dots n + k - 1\}$ szigorúan monoton növekvő függvények között.

Utóbbiak megfelelnek k elem kiválasztásának, tehát a megfeleltetés létezéséből következik az állítás.

32) Mit értünk véges halmaz ismétléses permutációin és mit mondhatunk az összes ismétléses permutációk számártól.

$r, i_1 i_2 \dots i_r \in \mathbb{N}$ ekkor

$a_1 a_2 \dots a_r$ 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.

Ezek száma: $P_n^{i_1 i_2 \dots i_r} = \frac{n!}{i_1! i_2! \dots i_r!}$

r=0 és 1 triviális.

Soroljuk egy ekvivalencia osztályba az $a_1 a_2 \dots a_r$ elemek két $i_1 + i_2 + \dots + i_r$ ismétlődésű ismétléses permutációját, ha az a_1 elem kihagyásával, ugyanazt az ismétléses permutációt kapjuk.

ekvivalencia osztályok száma: $P_{n-i_1}^{i_2 \dots i_r}$

ekvivalencia osztályok mérete: ${}^{i}C_{n-i_1+1}^{i_1}$

Össz méret: $P_n^{i_1 i_2 \dots i_r}$

így $P_n^{i_1 i_2 \dots i_r} = {}^{i}C_{n-i_1+1}^{i_1} \cdot P_{n-i_1}^{i_2 \dots i_r} = \frac{n!}{i_1!(n-i_1)!} \frac{(n-i_1)!}{i_2 \dots i_r}$

33) Fogalmazza meg a binomiális tételt és bizonyítsa be.

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

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

Bizonyítás: Indukcióval

n=0,1 re triviális

$$(x+y)^{n+1} = (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} = \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + x^k y^{n-k+1}$$

így csak azt kell belátni, hogy

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+k}{k+1}$$

Ami adódik a bal oldalt közös nevezőre hozva.

34) Fogalmazza meg a polinomiális tételt.

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

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{\substack{i_1+i_2+\cdots+i_r=n \\ i_1 i_2 \dots i_r \in \mathbb{N}}} \mathrm{P}_{\mathrm{n}}^{\mathrm{i}_1,\mathrm{i}_2,\dots,\mathrm{i}_r}\, \mathrm{x}_1^{\mathrm{i}_1}\mathrm{x}_2^{\mathrm{i}_2}\cdots\mathrm{x}_{\mathrm{r}}^{\mathrm{i}_r}$$

Bizonyítás: indukcióval

r=0,r=1 trivi, r=2 binomiális tétel

Ha r-1 re teljesül akkor

Legyen: $y = x_2 + \cdots + x_r$, ekkor az indukciós feltevés és a binomiális tétel alapján

$$(x_1 + x_2 + \cdots + x_r)^n = (x_1 + y)^n = \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}y^{n-i_1} =$$

$$= \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}\sum_{\substack{i_2+\cdots+i_r=n-i_1 \\ i_2\dots i_r\in\mathbb{N}}}\mathrm{P}_{\mathrm{n}}^{\mathrm{i}_2,\dots,\mathrm{i}_r}\,\mathrm{x}_2^{\mathrm{i}_2}\cdots\mathrm{x}_{\mathrm{r}}^{\mathrm{i}_r} =$$

$$= \sum_{i_1=0}^{n}\frac{n!}{i_1!\,(n-i_1)!}x_1^{i_1}\sum_{\substack{i_2+\cdots+i_r=n-i_1 \\ i_2\dots i_r\in\mathbb{N}}}\frac{(\mathrm{n}-i_1)!}{\mathrm{i}_2!\cdots\mathrm{i}_r!}\mathrm{x}_2^{\mathrm{i}_2}\cdots\mathrm{x}_{\mathrm{r}}^{\mathrm{i}_r}$$

$$= \sum_{\substack{i_1+i_2+\cdots+i_r=n \\ i_1 i_2\dots i_r\in\mathbb{N}}}\mathrm{P}_{\mathrm{n}}^{\mathrm{i}_1,\mathrm{i}_2,\dots,\mathrm{i}_r}\,\mathrm{x}_1^{\mathrm{i}_1}\mathrm{x}_2^{\mathrm{i}_2}\cdots\mathrm{x}_{\mathrm{r}}^{\mathrm{i}_r}$$

35) Fogalmazza meg a logikai szita formulát.

Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X-en értelmezett, egy Abel-csoportba képző függvény. Legyen

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

$$S_r = \sum_{1 \le i_1 < i_2 < \dots < i_r \le k} \; \sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} \mathrm{f(x)}$$

és legyen

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

Ekkor

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

Bizonyítás:

Ha $x \in X \setminus \bigcup_{i=0}^{k} X_i$,akkor mind két oldalt egyszer szerepel

Egyébként

Legyen $x \in X_{j_1}, X_{j_2}, \dots, X_{j_t}$

$f(x)$ a bal oldalon nem szerepel.

A jobb oldalon valamely

$$\sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} \mathrm{f(x)}$$

Összegben pontosan akkor lép fel, ha $\{i_1, i_2, \dots, i_r\} \subset \{i_1, i_2, \dots, i_t\}$. Ha $r > t$, akkor nincs ilyen $\{i_1, i_2, \dots, i_r\}$.

Ha $r > t$, akkor pontosan $\binom{t}{r}$ ilyen $\{i_1, i_2, \dots, i_r\}$van, így a jobb oldalon $f(x)$ együtthatója $\sum_{r=0}^{t} \binom{t}{r} (-1)^r = 0$

■

36) Sorolja fel a természetes számok körében az oszthatóság alaptulajdonságait és bizonyítsa be ezeket.

$n, m \in \mathbb{N}$

(1) $(m|n \wedge m'|n') \Rightarrow mm'|nn'$

$$\mathrm{n} = \mathrm{mk} \wedge n' = m'k' akkor\ n'n = m'k'\mathrm{mk} = \mathrm{lmm'}$$

(2) $\forall n \in \mathbb{N}(n|0)$

$$0 = 0n$$

(3) $0|n \Rightarrow n = 0$

$$n = 0k\ mivel\ nincs\ nullosztó\ n\ biztosan\ 0$$

(4) $\forall n(1|n)$

$$n = 1k, ahol\ k = n, hisz\ 1\ egységelem$$

(5) $\forall k \in \mathbb{N}(m|n \Rightarrow mk|nk)$

$$n = ml\ mivel\ nullosztómentes\ bővíthetünk\ k - val\ nk = mkl$$

(6) $(k \in \mathbb{N}^+ \wedge mk|nk) \Rightarrow m|n$

$$nk = mkl\ mivel\ nincs\ nullosztó\ k - val\ egyszerűsíthetünk\ n = ml$$

(7) $m|n_i$ és $k_i \in \mathbb{N}, (i = 1,2, \dots, j), akkor\ m|\sum_{i=1}^{j} k_i n_i$

$$n_i = ml_i\ ekkor\ l\ legyen\ k_i r_i\ így \sum_{i=1}^{j} k_i n_i = m\sum_{i=1}^{j} k_i r_i$$

(8) $(n \neq 0 \wedge m|n) \Rightarrow m \leq n$

hisz n, így n=mk m>n esetén n<mk, egyenlőség nem teljesülhetne

(9) az oszthatóság reláció részbenrendezés

tranzitív: n|m m|kc-nek akkor n|k

reflexív: n=1n

antiszimmetrikus:n|m és m|n-nek akkor m=n (8) miatt

37) Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

$a, b \in R$, ahol R egységelemes integritási tartomány

(1) $(\mathrm{b}|a \wedge b'|a') \Rightarrow bb'|aa'$

(2) $\forall a \in R(a|0)$

(3) $0|a \Rightarrow a = 0$

(4) $\forall a(1|a)$

(5) $\forall c \in R(b|a \Rightarrow bc|ac)$

(6) $(c \neq 0 \wedge \mathrm{bc}|ac) \Rightarrow b|a$

(7) $b|a_i$ és $c_i \in R, (i = 1,2, \dots, j), akkor\ b|\sum_{i=1}^{j} c_i a_i$

(8) az oszthatóság reláció reflexív és tranzitív

Bizonyítást lásd 36)-nál

38) Mi a kapcsolat az egységek és az asszociáltak között?

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

Hisz ha ε egy egység akkor $\varepsilon|\varepsilon$, így valamely $0 \neq e \in R$-re $\varepsilon = e\varepsilon$.

Innen $a\varepsilon = ae\varepsilon$ minden $a \in R$-re, mivel $\varepsilon \neq 0$,így lehet vele egyszerűsíteni, innen következik az állítás.

39) Ismertesse a bővített euklideszi algoritmust.

Ez az eljárás meghatározza az $a, b \in Z$ egészek egy d legnagyobb közös osztóját, valamint az $x, y \in Z$ egész számokat úgy, hogy $d = ax + by$ teljesüljön.

(4) [inicializálás]

$x_0 \leftarrow 1,$

$y_0 \leftarrow 0,$

$r_0 \leftarrow a,$

$x_1 \leftarrow 0,$

$y_1 \leftarrow 1,$

$r_1 \leftarrow b,$

$n \leftarrow 0$

(5) [vége?]

Ha $r_{n+1} = 0$ akkor

$x \leftarrow x_n,$

$y \leftarrow y_n,$

$d \leftarrow r_n,$

eljárás véget ért.

(6) [ciklus]

$q_{n+1} \leftarrow \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor,$

$r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1},$

$x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1},$

$y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1},$

$n \leftarrow n + 1$

ugrás (2)-re.

Bizonyítás:

Véget ér

$|r_n|$ szigorúan monoton csökkenő sorozat és $|r_n| \in \mathbb{N}$, $\mathbb{N}$ jól rendezett.

d=ax+by

indukció

$(d =) r_n = ax_n + by_n$

$n = 0, n = 1$-re teljesül

indukciós lépés

n-re és n+1 re jó akkor n+2-re is

I. $r_n = ax_n + by_n$

II. $r_{n+1} = ax_{n+1} + by_{n+1}$

II. $r_{n+1}q_{n+1} = ax_{n+1}q_{n+1} + by_{n+1}q_{n+1}$

I-II

$$r_n - r_{n+1}q_{n+1} = ax_{n+1} - ax_{n+1}q_{n+1} + by_{n+1} - by_{n+1}q_{n+1}$$

$$r_{n+2} = ax_{n+2} + by_{n+2}$$

d'|a és d'|b akkor d'|d

Innen $d'|a \wedge d'b \Rightarrow d'|ax + by (= d)$

d|a és d|b

Hátulról indukció

$d|r_n (= d)$

$r_{n-1} = r_n q_n + r_{n+1}$ így $d|r_{n-1}$

$r_{n-2} = r_{n-1}q_{n-1} + r_n$ így $d|r_{n-2}$

tehát $d|a_1$ és $d|b_1$

40) Mi a kapcsolat $\mathbb{Z}$-ben a prímelemek és az irreducibilis elemek közt. Bizonyítsa be állítását.

$$ha\ \ p \in \mathbb{Z} (p\ prím\ \Leftrightarrow p\ irreducibilis\ )$$

⇒:

ha $p\ prím\ akkor\ p = xy$ így $p|x$ esetén $x = pz = x(yz)\ \ yz = 1$ ahonnan y és z egységek, x és p asszociáltak.

⇐:

Legyen $p|ab$ de $p \nmid a$

Ekkor $p \nmid a$, miatt $lnko(a, p) = 1$

euklideszi algoritmussal kaphatunk olyan x, y-t, hogy $1 = px + ay$

Innen $b = pbx + aby$, mivel $p|pbx$,így $p|aby$, tehát $p|b$

41) Foglamazza meg és bizonyítsa be a számelemélet alaptételét.

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

∃:

Ha n=1, a felbontás üres sorozat.

Egyébként ha n nem irreducibilis, akkor felírható két nála kisebb, de 1-nél nagyobb szám szorzataként. Indukcióval folytatjuk ezt az eljárást: ha a kapott sorozatnak van nem törzsszám tényezője, akkor a legnagyobb ilyen tényező minden előfordulását helyettesítjük két nála kisebb, de 1-nél nagyobb természetes szám szorzatával.

Az eljárás a természetes számok jólrendezése miatt véges sok lépésben csupa törzsszám tényezőből álló felbontáshoz vezet.

!:

Indirekt bizonyítás:

Legyen n a legkisebb nem egyértelműen felbontható szám

$$n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$$

Mivel $p_1 | n$ azaz $p_1 | q_1 q_2 \cdots q_k$ a p_1 $prímtulajdonsága\ miatt$ $\exists i, hogy\ p_1 | q_i$.

Ekkor $p_1 = q_i$, mert q_i törzs szám.

Egyszerűsítve a kapott közös tényezővel egy kisebb n' számot kapunk, amelynek felbontása nem egyértelmű, ami ellent mondás a feltevés miatt.

42) Fogalmazza meg Eukleidész tételét, és bizonyítsa be.

Végtelen sok prímszám van.

Indirekt bizonyítás

Tegyük fel, hogy csak k prím van, $p_1, p_2, \dots, p_k$ és legyen $n = \prod_{j=1}^{k} p_j$

Ekkor $\forall 1 \leq j \leq k \ \left((n+1) mod\ p_j = 1\right)$, tehát $\forall 1 \leq j \leq k \ \left(p_j \nmid (n+1)\right)$, így $n+1$ prímtényezős felbontásában kell hogy legyen a p_j-ktől különböző prímszám, ami ellentmondás.

43) Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait és bizonyítsa be azokat.

(1) $(a \equiv b\ (mod\ m) \wedge d | m) \Rightarrow a \equiv b\ (mod\ d)$

$$m | a - b\ \wedge d | m\ akkor\ d | a - b\ a\ tranzitivitás\ miatt$$

(2) $a \equiv b\ (mod\ m) \Leftrightarrow 0 \neq d \in \mathbb{Z}\big(ad \equiv bd\ (mod\ md)\big)$

$$m | a - b\ \Leftrightarrow 0 \neq d \in \mathbb{Z}(md | ad - bd)$$

(3) hogy bármely adott $m \in \mathbb{Z}$-re a kongruencia ekvivalenciareláció $\mathbb{Z}$-ben

tranzitív, hisz ha $m | a - b\ \wedge m | b - c\ akkor\ m | a - c - nek$

reflexív, hisz a 0 mindennek többszöröse

szimmetrikus, hisz az $a - b$ asszociáltja $b - a$-nak

(4) $a \equiv b\ (mod\ m) \Leftrightarrow a \equiv b\ (mod -m)$

hisz m és –m egymás asszociáltjai

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

Legyen $m > 1$ egész. Ha $1 < lnko(a,m) < m$, akkor a maradékosztálya nullosztó Z_m-ben.

Bizonyítás

Legyen $d = lnko(a,m), 1 < d < m$

$$a\frac{m}{d} = \frac{a}{d}m \equiv 0\ (mod\ m)$$

ahonnan $x = \frac{m}{d}$ jelöléssel $\tilde{a} \cdot \tilde{x} = \tilde{0}$, azaz $\tilde{a}$ nullosztó Z_m-ben

Ha $lnko(a,m) = 1$, akkor a maradékosztályának van miltiplikatív inverze Z_m-ben. Speciálisan, ha m prímszám, akkor Z_m test.

Bizonyítás

Legyen $d = lnko(a,m) = 1$

Bővített euklideszi algoritmussal olyan x, y egészeket kapunk, amelyekre $ax + my = 1$.

Innen $ax \equiv 1\ (mod\ m)$ azaz $\tilde{a} \cdot \tilde{x} = \tilde{1}$ miatt $\tilde{x}$ az $\tilde{a}$ inverze Z_m-ben.

Így tehát ha m prím és $a \not\equiv 0\ (mod\ m)$, akkor a-nak van multiplikatív inverze.

45) Mit mondhatunk az $aa_i + b$ számokról, ha a_i egy maradék rendszer, illetve egy redukált maradék rendszer elemeit futja végig. Bizonyítsa be állítását.

Legyen $m > 1$ egész szám, a relatív prím m-hez. Ha $a_1, a_2, \dots, a_m$ teljes maradék rendszer modulo m és $b \in \mathbb{Z}$, akkor $aa_1 + b, aa_2 + b, \dots, aa_m + b$ is teljes maradék rendszer modulo m.

Ha $a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradék rendszer modulo m, akkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradék rendszer modulo m.

Bizonyítás

Ha $i \neq j$ estén $aa_i + b \equiv aa_j + b\ (mod\ m)$ teljesülne,
akkor ebből $aa_i \equiv aa_j\ (mod\ m)$, és innen a multiplikatív inverzével szorozva
$a_i \equiv a_j\ (mod\ m)$ következne.

Tehát mivel $aa_1 + b, aa_2 + b, \dots, aa_m + b$ inkongruensek és számuk m- teljes maradék rendszert alkotnak mudulo m.

Bizonyítás

Ha $lnko(aa_i, m) > 1$ akkor $lnko(a_1, m) > 1$

Így az $aa_1, aa_2, \dots, aa_{\varphi(m)}$ számok relatív prímek a modulushoz, és páronként is relatív prímek és számuk $\varphi(m)$, tehát redukált maradékrendszert alkotnak.

46) Fogalmazza meg és bizonyítsa be az Euler Fermat-tételt.

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

Bizonyítás

Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m.

Ekkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradékrendszer modulo m. Innen

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} aa_j \equiv \prod_{j=1}^{\varphi(m)} a_j\ (mod\ m)$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím m-hez, van inverze mudulo m. Ezzel megszorozva kapjuk az állítást.

47) Fogalmazza meg és bizonyítsa be a Fermat-tételt.

Legyen p prímszám.

Ha a ∈ Z és p ∤ a, akkor $\mathrm{a}^{\mathrm{p}-1} \equiv 1\ (\mathrm{mod\ p})$.

Ha a ∈ Z tetszőleges, akkor $\mathrm{a}^{\mathrm{p}} \equiv \mathrm{a}\ (\mathrm{mod\ p})$.

Bizonyítás

Nyilván $\varphi(p) = p - 1$, így az első alak következik a Euler Fermat-tételből.

A második, ha $p \nmid a$ esetben az első alakból következik,
ha pedig $p|a$ akkor mindkét oldal osztható p-vel.

48) Ismertesse a lineáris kongruenciák megoldásának módszerét részletes indoklással.

Legyen $m > 1$ egész szám, $a, b \in \mathbb{Z}$ adottak, keressük $ax \equiv b\ (mod\ m)$ kongruencia megoldásait.

Tehát keresünk x-et amire valamely y egész számmal teljesül: $ax + my = b$.

Legyen $d = lnko(a, m)$, így d|$ax + my$, tehát ha d ∤ b akkor nincs megoldás.

Tegyük fel, hogy $a = a'd, b = b'd, m = m'd\ valamely\ a', b', m' \in \mathbb{Z}$

Azt kapjuk, hogy egyenletünk az $a'x + m'y = b'$ ami ekvivalens $a'x \equiv b'\ (mod\ m')$, ahol a' és m' relatív prímek. A legnagyobb közös osztó kiszámítását a bővített euklideszi algoritmussal végezve, olyan x_0, y_0egészeket is kaphatunk, amelyre $ax_0 + my_0 = 1$.

Szorozva b'-vel, $a'x_1 + m'y_1 = b'$, ahol $x_1 = x_0 b'$.

Vonjuk ki ezt az egyenletet a $a'x + m'y = b'$ egyenletből: $a'(x - x_1) = m'(y_1 - y)$ ahonnan $m' | x - x_1$, azaz $x = x_1 + km$ valamely$k \in \mathbb{Z}$-re.

Minden ilyen x tényleges megoldás, mert $y = y_1 - ka'$-vel $a'x + m'y = b'$

Az összes megoldást $x \equiv x_1\ (mod\ m)$ alakban adható meg.

49) Ismertesse a lineáris kongruenciarendszerek megoldásának módszerét részletes indoklással.

Ha adott lineáris kongruencia, akkor azokat, ha megoldhatók hozzuk $x \equiv a\ (mod\ m)$, illetve $x \equiv b\ (mod\ n)$ alakra, ahol a,b,m,n egészek m,n>0.
Mivel a közös megoldásokra $x = a + my = b + nz\ valamely\ y, z \in \mathbb{Z}$-re az $my - nz = b - a$ egyenlet egész megoldásait keresve, minden x megoldás megtalálható.
Akkor és csak akkor van megoldás, ha $lnko(m,n)|$b − a, ekkor a megoldás $x \equiv x_1\ (mod\ lnko(m,n))$ alakban írható fel valamely $x_1$egésszel.
Ha több kongruencia van az eljárás folytatható.

50) Fogalmazza meg és bizonyítsa be a kínai maradék tételt.

Legyenek $m_1, m_2, \dots, m_n$ egynél nagyobb, páronként relatív prím természetes számok, $c_1, c_2, \dots, c_n \in Z$. Az $x \equiv c_j\ (mod\ m_j),\ \ j = 1,2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1 m_2 \dots m_n$.

Bizonyítás

Legyen $m = m_1 m_2$. A bővített euklideszi algoritmussal olyan x_1, x_2 egéyz számokat kaphatunk, amelyre $m_1 x_1 + m_2 x_2 = 1$
Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1$
Nyilván $c_{1,2} \equiv c_j\ (mod\ m_j)$, ha j=1,2
Ha $x \equiv c_{1,2}\ (mod\ m)$, akkor x az első két kongruencia egy megoldása, és megfordítva, ha x az első két kongruencia egy megoldása, akkor $x - c_{1,2}$ osztható m_1-gyel m_2-vel, tehát a szorzatuk is.
Az eredeti kongruenciarendszer tehát ekvivalens az $x \equiv c_{1,2}\ (mod\ m), x \equiv c_j\ (mod\ m), j = 3,4, \dots, n$ kongruenciarendszerrel.
Így n szerinti indukcióval adódik a bizonyítás.

51) Ismertesse az RSA eljárást részletes indoklással

Az eljárás úgynevezett nyilvános kulcsú eljárás, az eljárás a következő:

1.lépés: Válasszunk két nagy $p \neq q$ prímet

2.lépés: legyen n=pq, válszunk egy $1 < e < (p-1)(q-1)$ nyilvános kulcsot, ezt a két értéket fogjuk nyilvánosságra hozni.

3.lépés: d titkos kulcs meg határozása az $ed \equiv 1 \left(mod\ (p-1)(q-1)\right)$ kongruencia megoldásával, ha nincs megoldása elölről kezdjük.

Ekkor a nyilvános kulcs segítségével kódolt üzenet küldhető nekünk. ha $1 < m < n$ üzenet, akkor annak kódolt formája $c = m^e\ mod\ n$.

Az üzenetet újabb hatványozással kaphatjuk vissza.

valamely k-ra $ed = k(p-1)(q-1)+1$, így

$$c^d = (m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \cdot m \equiv m\ (mod\ m)$$

Ekkor, ha $p|m$, akkor mindkét oldal nullával kongruens, ha $p \nmid m$, akkor a Fermat tétel szerint $m^{p-1} \equiv (1\ mod\ p)$.

Hasonlóan $(m^e)^d \equiv m\ (mod\ q)$

Innen a kínai maradék tétel szerint, mivel $p \neq q$ prímek $m = c^d\ mod\ n$

Így $m = c^d\ mod\ n$ módon dekódolhatjuk az üzenete.

