DEFINICIÓK

1. Mondjon legalább három példát predikátumra.

Predikátummal egy matematikai tulajdonságot jelentünk ki, általában nagy betűvel jelöljük, és ehhez a jelöléshez társítjuk azt a tulajdonságot, jelentést. Értékük lehet igaz vagy hamis.
Például a síkgeometriában predikátumok: $\mathrm{E(x)}$ („x egyenes”), $\mathrm{P(x)}$ („x pont”), $\mathrm{I(x, y)}$ („x illeszkedik y-ra”).

2. Sorolja fel a logikai jeleket.

A logikai formulák alkothatók velük, ha predikátumokat kapcsolunk össze: ¬(„nem”), ∧ („és”), ∨ („vagy”), ⊕ („kizáró vagy”) ⇒(„ha ... akkor ...”) , ⇔(„akkor és csak akkor” vagy „pontosan akkor”).

3. Milyen kvantorokat ismer? Mi a jelük?

Az elsőrendű formulák alkotóelemei: ∃(„létezik” vagy „van olyan”) egzisztenciális kvantor és a ∀ („minden” vagy „bármely”) univerzális kvantor.

4. Hogyan kapjuk a logikai formulákat?

Nulladrendű nyelv esetén a logikai formulákat a predikátumokból és a logikai jelekből épülnek fel, elsőrendű nyelv esetén a két kvantort is felhasználjuk.
Pl. Nulladrendű: A ∨ ¬B ; Elsőrendű: ∀x ∃y (P(x,y))

5. Mikor van egy változó egy kvantor hatáskörében?

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

6. Mik a nyitott és mik a zárt formulák?

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

Röviden: Minden változó a formulában kvantált. Pl.: ∀x∀y∀z(¬P(x,y) ∨ P(y,z))- ez zárt, egyik változó sem szabad, mindegyik kvantált. ∀x∀y(¬P(x,y) ∨ P(y,z)) – ez nyitott, z változó szabad, nem kvantált, nincs kvantor hatáskörében
Ez a következő kettőnél szintén felhasználható

7. Mondjon két példát nyitott formulára.

A síkgeometria példájánál maradva, az $((E(x) \wedge P(y)) \wedge I(x, y))$ és a $((P(x) \wedge P(y)) \wedge \neg x = y)$ formulában x és y szabad változók, mert nem kvantáltak, így ezek a kifejezések nyitott formulák.

8. Mondjon egy példát zárt formulára.

A $\forall x(E(x) \Rightarrow \exists y(P(y) \wedge I(x, y)))$ zárt formula, mert nincs szabad változója.

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

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

10. Milyen tulajdonságokkal rendelkezik a „részhalmaz” fogalom?

Minden halmaz részhalmaza saját magának (reflexivitás), és ha $A \subset B$, $B \subset C$, akkor $A \subset C$ (tranzitivitás). Ha $A \subset B$ és $B \subset A$, akkor a meghatározottsági axioma szerint az is teljesül, hogy $A = B$ (antiszimmetria).

11. Milyen tulajdonságokkal rendelkezik a halmazok egyelősége?

A halmazok egyenlősége ekvivalencia reláció: reflexív, tranzitív, szimmetrikus.
reflexív: $\forall$ x $\in$ X x = x
tranzitív: $\forall$ x $\forall$ y $\forall$ z $\in$ X (x = y $\wedge$ y = z $\Rightarrow$ x = z)
szimmetrikus: $\forall$ x $\forall$ y $\in$ X (x = y $\Rightarrow$ y =x)

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

Akkor mondjuk, hogy *A* halmaz részhalmaza a *B* halmaznak, ha *A* minden eleme a *B* halmaznak is eleme.
Jele: *A*$\subset$*B* vagy *B*$\supset$*A*.
Ha *A* részhalmaza *B*-nek, de nem egyenlő vele, akkor azt mondjuk, hogy *A* valódi részhalmaza *B*-nek.
Jele: $A \subsetneq B$ vagy $B \supsetneq A$ (más jelölések részhalmazra: *A*$\subseteq$*B* vagy *B*$\supseteq$*A*, és valódi részhalmazra: *A*$\subset$*B* vagy *B*$\supset$*A*).

13. Írja le az üres halmaz fogalmát.

Egy olyan halmazt, amelynek nincs eleme, üres halmaznak nevezünk. jele: $\emptyset$

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

Igen, mivel bármely üres halmaznak ugyanazok az elemei (hiszen nincs elemük), az üres halmazok egyenlők, azaz csak egyetlen üres halmaz létezik; meghatározottság axiómája miatt csak egy üres halmaz van.

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

Ha *A* és *B* halmazok, akkor azt a halmazt, amelynek pontosan azok az elemei, melyek elemei *A*-nak vagy *B*-nek (vagy mindkettőnek), *A*∪*B*-vel jelöljük és két halmaz uniójának nevezzük.

A∪B := {x | x $\in$ A $\vee$ x $\in$ B}

16. Írja le halmazrendszer unióját és a megfelelő jelöléseket.

Ha A egy halmaz, amelynek elemei mind halmazok, akkor azt a halmazt, amely pontosan azokat a elemeket tartalmazza, amelyek A valamely elemének az elemei, az A uniójának nevezzük. Ennek jelölése: ∪A vagy $\cup_{A \in \mathrm{A}} A$.   ∪ A := { x | $\exists$ A $\in$ A (x $\in$ A) } !!!Fontos: A ≠ A (nyomtatott A: A, írott A: A) !!!

17. Fogalmazza meg a halmazok uniójának alaptulajdonságait.

Ha A, B , C halmazok, akkor:

(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) $A \subset B$ akkor és csak akkor, ha $A \cup B = B$.

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

Ha A és B halmazok, legyen $A \cap B \coloneqq \{x \mid x \in A \ \wedge \ x \in B\}$. Általánosan, ha A halmazok egy nem üres rendszere, akkor a halmazrendszer metszetét a ∩ A := { x | ∀ A ∈ A (x ∈ A) } összefüggéssel definiáljuk. !!!Fontos: A ≠ A (nyomtatott A, írott A pl.) !!!

19. Definiálja a diszjunktság és a páronként diszjunktság fogalmát.

Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B diszjunktak (vagy idegenek). Általánosabban, ha egy nem üres A halmazrendszer metszete az üres halmaz, akkor azt mondjuk, hogy a halmazrendszer diszjunkt. Ha a halmazrendszer bármely két halmazának metszete üres, akkor azt mondjuk, hogy elemei páronként diszjunktak. (Más szóhasználatban a páronként diszjunkt halmazokból álló halmazrendszert nevezzük diszjunktnak.)

20. Fogalmazza meg a halmazok metszetének alaptulajdonságait.

Ha A, B, C halmazok, akkor:

(1) $A \cap \emptyset = \emptyset$;
(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) $A \subset B$ akkor és csak akkor, ha $A \cap B = A$.

21. Fogalmazza meg az unió és a metszet disztributivitását.

Ha A, B, C halmazok, akkor
(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (a metszet disztributivitása az unióra nézve)
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (az unió disztributivitása a metszetre nézve)

22. Definiálja a halmazok különbségét, szimmetrikus differenciálját és komplementerét.

Az A és B halmazok különbségét (vagy differenciálját) az $A \backslash B := \{x \mid x \in A \ \wedge \ x \notin B\}$ összefüggéssel definiáljuk. A két halmaz szimmetrikus differenciálját az $A \vartriangle B := (A \backslash B) \ \cup (B \backslash A)$ vagy (A∪B)\(A∩B) összefüggéssel definiáljuk. Ha $A \subset X$, akkor az $X \backslash A$ halmazt néha A'-val jelöljük, és az A halmaz X-re vonatkozó komplementerének nevezzük. Ez természetesen nem csak A-tól, hanem az X „alaphalmaztól" is függ, ami az A' jelölésben nem jut kifejezésre.

23. Fogalmazza meg a halmazok komplementerének alaptulajdonságait.

Ha $A, B \subset X$, akkor

(1) $(A')' = A$
(2) $\emptyset' = X$
(3) $X' = \emptyset$
(4) $A \cap A' = \emptyset$
(5) $A \cup A' = X$
(6) $A \subset B$ akkor és csak akkor, ha $B' \subset A'$
(7) $(A \cup B)' = A' \cap B'$
(8) $(A \cap B)' = A' \cup B'$

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

Egy halmaz hatványhalmazának nevezzük az adott halmaz összes részhalmazainak a halmazát.
$\wp$(A) := {B | B ⊂ A}

25. Definiálja a rendezett pár fogalmát és koordinátáit.

x, y esetén legyen $(x, y) := \{\{x\}, \{x, y\}\}$. Fontos a sorrend, x = y esetén $(x, y) := \{\{x\}\}$

26. Definiálja két halmaz Descartes-szorzatát.

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

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

Egy halmazt binér relációnak (vagy kétváltozós relációnak) nevezünk, ha minden eleme rendezett pár.
Ha R egy binér reláció, akkor $(x, y) \in R$ helyett gyakran azt írjuk, hogy xRy, és azt mondjuk, hogy x és y között fennáll az R reláció.

28.Adjon három példát binér relációra.

halmazokra tekintve a részhalmazság egy binér reláció, egyenesekre tekintve a merőlegesség, vagy a párhuzamosság szintén

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

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

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

Az R binér reláció értelmezési tartományát a: $\mathrm{dmn}(R) \coloneqq \{x \mid \exists\ y\ (x, y) \in R\}$,
értékkészletét pedig a: $\mathrm{rng}(R) \coloneqq \{y \mid \exists\ x\ (x, y) \in R\}$
összefüggéssel értelmezzük. A jelölések a „domain”, illetve a „range” szóra utalnak; dom vagy $\mathcal{D}$, illetve ran, $\mathcal{R}$ vagy Im (az „image” szóból) is szokásosak.

R ⊆ A × B reláció
$\mathcal{D}_R$:= { a ∈ A ∃ b ∈ B : (a,b) ∈ R} ; $\mathcal{R}_R$:= { b ∈ B ∃ a ∈ A : (a,b) ∈ R }

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

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

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

Egy R binér reláció inverzén az $R^{-1} \coloneqq \{(b, a) \colon (a, b) \in R\}$ binér relációt értjük.

(1) $(R^{-1})^{-1} = R$; (involúció)

(2) ha R reláció X és Y között, akkor R^{-1} reláció Y és X között;

(3)$\mathcal{D}(R^{-1}) = \mathcal{R}(R)$ és $\mathcal{R}(R^{-1}) = \mathcal{D}(R)$

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

Legyen $R \subseteq \mathrm{X} \times \mathrm{Y}$ egy binér reláció és A egy halmaz. Az A halmaz képe az $R(A) \coloneqq \{y \mid \exists \mathrm{x} \in \mathrm{A} \colon (\mathrm{x}, \mathrm{y}) \in R\}$ halmaz. $R(A)$ pontosan akkor üres, ha A és $dmn(R)$ diszjunktak vagyis $R(A) = \emptyset \Leftrightarrow A \cap dmn(R) = \emptyset$. Az A halmaz inverz képe az R relációnál $R^{-1}(A) \coloneqq \{x \mid \exists \mathrm{y} \in \mathrm{A} \colon (\mathrm{x}, \mathrm{y}) \in R\}$. $R^{-1} \subseteq Y \times X$ Ha $A = \{a\}$, akkor $R(\{a\})$ helyett $R(a)$-t írunk.

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

Az R és Q binér relációk összetételén (kompozícióján, szorzatán) az $Q \circ R \coloneqq \{(x, z) \colon \exists y \colon (x, y) \in R \text{ és } (y, z) \in Q\}$ relációt értjük. Két reláció kompozíciója lehet üres: ha $rng(R)$ és $dmn(Q)$ halmazok diszjunktak.

R ⊆ A × B , Q ⊆ B × C

Q ∘ R = {(a,c) | ∃ b ⊆ B : aRb ∧ bRc } a ∈ A , c ∈ C

A = { a, b} C = {(a, b)} Q := R ⇒ Q ∘ R = ∅ (üres)

35. Fogalmazzon meg két (régiben három), binér relációk kompozíciójára vonatkozó állítást.

Legyenek R, Q és P binér relációk. Ekkor

(1)ha $rng(R) \supset dmn(Q)$, akkor $rng(Q \circ R) = rng(Q)$;

(2)$P \circ (Q \circ R) = (P \circ Q) \circ R$ (asszociativitás);

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

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

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1)tranzitív, ha minden x, y, z-re $(x, y) \in R$ és $(y, z) \in R$ esetén $(x, z) \in R$;
∀ x ∀ y ∀ z ∈ X (xR y ∧ yRz ⇒ xRz)

(2)szimmetrikus, ha minden x, y-ra $(x, y) \in R$ esetén $(y, x) \in R$;
∀ x ∀ y ∈ X (xRy ⇒ yRx)

(3)dichotom, ha minden $x, y \in X$ esetén $(x, y) \in R$ vagy $(y, x) \in R$ (esetleg mindkettő), azaz bármely két elem összehasonlítható.

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

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

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) intranzitív, ha minden x, y, z-re $(x, y) \in R$ *és* $(y, z) \in R$ esetén $(x, z) \notin R$;
(2) antiszimmetrikus, ha minden x, y-ra $(x, y) \in R$ és $(y, x) \in R$ esetén $x = y$;
(3) trichotom, ha minden $x, y \in X$ esetén $x = y, (x, y) \in R$ vagy $(y, x) \in R$ közül pontosan egy teljesül.

Ezek közül az intranzitivitás és az antiszimmetrikusság függ csak a relációtól.

38. Mint jelent az, hogy egy reláció szigorúan antiszimmetrikus, reflexív illetve irreflexív? Ezek közül mi az, ami csak a reláción múlik?

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) reflexív, ha minden $x \in X$ esetén $(x, x) \in R$;
(2) irreflexív, ha minden $x \in X$ esetén $(x, x) \notin R$;
(3) szigorúan antiszimmetrikus, ha minden x, y-ra $(x, y) \in R$ és $(y, x) \notin R$;

Ezek közül a szigorúan antiszimmetrikusság függ csak a relációtól.

39. Definiálja az ekvivalenciarelációt, illetve az osztályozás fogalmát.

Legyen X egy halmaz. Az X-beli binér relációt ekvivalenciarelációnak nevezzük, ha reflexív, szimmetrikus és tranzitív. Az X részhalmazainak egy O rendszerét X osztályozásának nevezzük, ha O páronként diszjunkt nem üres halmazokból álló halmazrendszer, amelyre $\cup\, O = X$.

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

Valamely X halmazon értelmezett $\sim$ ekvivalenciareláció X-nek egy osztályfelbontását adja. Megfordítva, az X halmaz minden osztályfelbontása egy $\sim$ ekvivalenciarelációt hoz létre.

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

Egy X halmazbeli részbenrendezés egy tranzitív, reflexív, és antiszimmetrikus X-beli reláció. Egy X részbenrendezett halmaz, illetve rendezett halmaz tulajdonképpen az $(X, \leq)$ pár. Egy X részbenrendezett halmaz minden Y részhalmaza is részbenrendezett, ha a $\leq$ relációt csak ennek az elemei között tekintjük, azaz a $\leq \cap\ (\mathrm{Y} \times \mathrm{Y})$ relációval.

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

A reláció (teljes) rendezés, ha refl., antiszimm., tr., és dichotom.
Egy halmaz rendezett, ha ezt a relációt értelmezzük rajta. Jele: (X, ≤)
Egy részben rendezett halmaz(nem dichotom, de a többi tulajdonság teljesül), részhalmaza, ha (teljesen) rendezett akkor az egy láncot alkot.

43. Mondjon példát részbenrendezett de nem rendezett halmazra.

A természetes számok körében az „n osztja m-et” reláció részbenrendezés, de nem (teljes) rendezés, mivel nem bármely két elem eseté áll fenn a reláció, nem dichotom.

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

R ⊆ X × X binér reláció:
szigorú, ha irreflexív, ∀ x ∈ X¬xRx
gyenge, ha reflexív ∀ x ∈ X xRx

szigorú és gyenge reláció között a reflexivitási tulajdonság dönt: ha egy reláció irreflexív, vagyis egy elem önmagával nem állhat relációban, akkor a reláció szigorú, amennyiben a reflexivitás megengedett, bármely elem önmagával is relációban áll, akkor gyenge reláció

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

R ⊆ X × X binér reláció szigorú részben rendezés:
irreflexív: ∀x ¬xRx ; (x,x) ∉ R
antiszimetrikus: ∀x ∀y (x ≠ y ∧ R(x,y) ⇒ ¬R(y,x))
tranzitív: ∀x∀y∀z (R(x,y) ∧ R(y,z) ⇒R(x,z))

(gyenge) részben rendezés esetén a reflexivitás megengedett: ∀x xRx ; (x,x) ∈ R

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

A rendezés relációit használva egy halmazon, az elemek kapcsolatát fogalmazhatjuk meg ilyen módon: Ha $x < y$, akkor azt mondjuk, hogy x kisebb, mint y vagy y nagyobb, mint x, (szigorú reláció) illetve hogy x megelőzi y-t vagy y követi x-et. A gyenge reláció esetén hozzátesszük, hogy „vagy egyenlő”.

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

Legyen X egy részbenrendezett halmaz. Ha $x \leq z$ és $z \leq y$, akkor azt mondjuk, hogy z az x és y közé esik, ha pedig $x < z$ és $z < y$, akkor azt mondjuk, hogy z szigorúan x és y közé esik. Az összes ilyen elemek halmazát $[x, y]$, illetve $]x, y[$ jelöli. Ily módon definiált elemek halmazát intervallumnak nevezünk.

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

Egy X halmazon, ha értelmeztünk szigorú rendezést (X, <): és x < y
x közvetlenül megelőzi y-t, vagy y közvetlenül követi x-t jelentse azt, hogy:
¬∃ z (x < z ∧ z< y)

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

Legyen X egy részbenrendezett halmaz. Egy x elemhez tartozó kezdőszeletnek a $\{y \in X : y < x\}$ részhalmazt nevezzük. A kezdőszelet logikus, de nem elterjedt jelölése $]\leftarrow, x[$.

50. Definiálja a legkisebb és a legnagyobb elem fogalmát.

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

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

Legyen x eleme X. Az x-et minimálisnak nevezzük, ha nincs nála kisebb elem, maximálisnak pedig akkor, ha nincs nála nagyobb elem. Maximális és minimális elem lehet több is. Jelölések: $\min X$, $\max X$; abban az esetben, ha ezek egyértelműek

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

Ha az A halmaz a {2, 3, 6} elemekből áll, és a reláció az oszthatóság, akkor a 2 és a 3 is minimális elem.

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

A természetes számok halmaza ilyen a szokásos rendezéssel.

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

Igen. Minimális és maximális elem több is lehet, és hogy ha X rendezett, akkor a legkisebb és a minimális elem fogalma, illetve a legnagyobb és a maximális elem fogalma egybeesik.

55. Definiálja az alsó és a felső korlát fogalmát.

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

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

Ha egy Y részhalmaznak van egy vagy több alsó korlátja, akkor is előfordulhat, hogy egyik sem eleme Y-nak. Ha mégis, van az alsó korlátok között eleme Y-nak, akkor csak egy van és ez az Y legkisebb eleme.

57. Definiálja az alsó és a felső határ tulajdonságot.

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

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

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

59. Definiálja az infimum és suprémum fogalmát.

Ha az alsó korlátok halmazában van legnagyobb elem, akkor azt Y legnagyobb alsó korlátjának, pontos alsó korlátjának, vagy alsó határának, idegen szóval infimumának nevezzük és inf Y-nal jelöljük.
Ha Y felső korlátjai halmazában van legkisebb elem, akkor azt Y legkisebb felső korlátjának, pontos felső korlátjának, vagy felső határának, idegen szóval suprémumának nevezzük, és supY-nal jelöljük.

60. Definiálja a jólrendezés és jólrendezett halmaz fogalmát.

Egy X (teljesen) rendezett halmazt jólrendezettnek, (teljes) rendezését pedig jólrendezésnek nevezzük, ha X bármely nem üres részhalmazának van legkisebb eleme.

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

Az egész, racionális és valós számok halmaza nem jólrendezett de rendezett a szokásos rendezéssel.

62. Adjon példát jólrendezett halmazra.

A természetes számok halmaza jólrendezett a szokásos rendezéssel.

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

Az X és Y részbenrendezett halmazok Descartes-szorzatán értelmezzük az alábbi részbenrendezéseket:
$R1 := \{((x,y) \in X \times Y, (x',y') \in X \times Y): x \leq x' \land y \leq y'\}$
$R2 := \{((x,y) \in X \times Y, (x' y') \in X \times Y): x \leq x' \lor (x=x' \land y \leq y')\}$

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

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

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

Egy függvény egy olyan f reláció, amelyre ha $(x, y) \in f$ és $(x, y^{'}) \in f, akkor\ y = y'$, másszóval minden x-hez legfeljebb egy olyan y létezik, amelyre $(x, y) \in f$. Jelölések: $f(x) = y$. Az y elemet az f függvény x helyén (argumentumában) felvett értékének nevezzük. Egyéb jelölés: $f : x \mapsto y$.

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

Annak kifejezésére, hogy az f függvény értelmezési tartománya a teljes X halmaz, értékkészlete pedig az Y halmaznak részhalmaza az $f : X \to Y$ jelölés szolgál, amit úgy olvasunk ki, hogy f az X-et Y-ba képező függvény. Ez nem ugyanaz, mint $f \in X \to Y$, mert utóbbi esetben $\boldsymbol{D}(f) \subsetneq X$ is lehetséges.

67. Mikor nevezünk egy függvényt kölcsönösen egyértelműnek?

Az f függvényt kölcsönösen egyértelműnek nevezzük, ha f(x)=y és f(x')=y esetén x=x'.
Ez azzal ekvivalens, hogy az f^{-1} reláció egy függvény.
Szokás a kölcsönösen egyértelmű függvényeket injektívnek is nevezni.

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

Igen. Ezt I_X-ként jelöljük, és X-nek X-re való identikus leképezésének nevezünk.
$f \subseteq A \times B$ függvény szürjektív, ha rng(f) = B

69. Definiálja a permutáció fogalmat.

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

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

Igen, ha f és g függvények akkor g∘f is. Ha f és g kölcsönösen egyértelmű függvény, akkor g∘f is az. Ha az f függvény X-et Y-ra , a g függvény pedit Y-t Z-re képezi le, akkor g∘f az X-et Z-re képezi le.

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

$f \subseteq A \times B$ függvény
injektív, ha $\forall\, a_1, a_2 \in A\; a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$
szürjektív, ha rng(f) = B
bijektív, ha injektív és szürjektív

Pl.:Legyen A a teljes R, és B a nem 0 valósak halmaza, C pedig a pozitív valós számok halmaza. Ha $f\colon B \to C$ a négyzet-, $g\colon A \to B$ az exp. függvény, akkor külön külön nem bijektívek (f nem inj., g nem szürj.), de összetételük az.

72. Mi a kapcsolat függvények és ekvivalenciarelációk között?

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

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

Legyenek X és Y részbenrendezett halmazok. Az $f : X \to Y$ függvényt monoton növekedőnek nevezzük, ha $x, y \in X,\ x \leq y\ esetén\ f(x) \leq f(y),$ illetve monoton csökkenőnek nevezzük, ha $x, y \in X,\ x \leq y\ esetén\ f(x) \geq f(y)$.

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

Legyenek X és Y részbenrendezett halmazok. Az $f : X \to Y$ függvényt szigorúan monoton növekedőnek nevezzük, ha $x, y \in X,\ x < y\ esetén\ f(x) < f(y),$ illetve szigorúan monoton csökkenőnek nevezzük, ha $x, y \in X,\ x < y\ esetén\ f(x) > f(y)$.

75. Mi a kapcsolat szigorúan monoton növekedő függvények, a kölcsönösen egyértelmű függvények (és az inverz függvények) között?

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

76. Mit állíthatunk a monoton növekedő függvények inverz függvényéről?

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

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

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

Burcsi órai jegyzet:
Ha x: I → ? egy ún. indexhalmazból képez, ilyenkor x(i) helyett x_i-t írunk, I elemei az indexek, az rng(x) pedig rendezett indexhalmaz, rendezett család.

78. Definiálja indexelt halmazcsaládok unióját és metszetét.

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

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

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

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

Ha az $(x_1, x_2, \dots, x_n)$ elem n-eseket az {1,2,...,n} halmaz, azaz N^+-nak az $n \in N^+$-nál nem nagyobb elemei által indexelt családokkal azonosítjuk, akkor az $X_1 \times X_2 \times \dots \times X_n$ Descartes-szorzatot mint az összes olyan $x_i,\ i \in \{1,2, \dots, n\}$ családok halmazát definiálhatjuk, amelyekre $x_i \in X_i, ha\ i \in \{1,2, \dots, n\}$.

Véges sok, n darab halmaz Descartes – szorzatát formálisan így definiáljuk:
X1 × X2 × … × Xn :={(x1,x2,...,xn):x1 ∈ X1, x2 ∈X2, … xn ∈ Xn}
Ha X1 = X2 = … = Xn := X1 × X2 × … × Xn helyett egyszerűen Xn-t szokás írni.

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

Ha az $(\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_\mathrm{n})$ elem n-eseket az $\{1,2, \dots, \mathrm{n}\}$ halmaz, azaz N^+-nak az $\mathrm{n} \in \mathrm{N}^+$-nál nem nagyobb elemei által indexelt családokkal azonosítjuk, akkor az $X_1 \times X_2 \times \dots \times X_n$ Descartes-szorzatot mint az összes olyan $x_i,\ i \in \{1,2, \dots, n\}$ családok halmazát definiálhatjuk, amelyekre $x_i \in X_i$, ha $i \in \{1,2, \dots, n\}$.
Ilyen szorzathalmazok részhalmazait n-változós relációknak nevezzük.

Véges sok, n darab halmazon értelmezett reláció:
R ⊆ X1 × X2 × … × Xn (x1,x2,...,xn) ∈ R :x1 ∈ X1, x2 ∈X2, … xn ∈ Xn
Ha X1 = X2 = … = Xn akkor homogén reláció.

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

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

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

Legyen X egy halmaz. Egy X-beli binér műveleten egy $*: X \times X \to X$ leképezést értünk. Ha $x, y \in X$, akkor $*(x, y)$ a művelet eredménye, x és y pedig az operandusai. Rendszerint a binér művelet jelét az operandusok közé írjuk: $x * y$.
Egy X-beli unér művelet egy $* : X \to X$ leképezés.
Mivel $X^0 = \{\emptyset\}$, egy nullér művelet egy $* : \{\emptyset\} \to X$ leképezés, ami tulajdonképpen X egy elemének a kijelölését jelenti, operandusa nincs, csak eredménye.

binér: 2 operandus, 1 operátor, jele: ℝ x ℝ → ℝ pl: összeadás, metszet, stb.

unér: 1 operandus, 1 operátor, jele: ℝ → ℝ pl: negáció

nullér: nincs operandus, nincs operátor, jele: → L pl: egy kifejezés logikai kiértékelése

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

binér

∧ ↑ ↓
↑ ↑ ↓
↓ ↓ ↓

unér

¬ ↑ ↓
↓ ↑

85. Hogyan definiálunk műveleteket függvénytereken?

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

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

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

86. Adjon példát műveletekre függvények között.

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

87. Definiálja a művelettartó leképezés fogalmát.

Legyen $*$ binér művelet az X, és legyen $*'$ binér művelet az X' halmazon. Egy $\varphi : X \to X'$ leképezést művelettartónak nevetünk, ha $\varphi(x * y) = \varphi(x) *' \varphi(y)$ $minden$ $x, y \in X$-re. Hasonlóan értelmezzük a művelettartást unér és nullér műveletre is.

88. Adjon példát műveletttartó leképzésre.

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

89. Fogalmazza meg a rekurziótételt.

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

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

H az alaphalmaz $A \subseteq H$, $\chi_A : H \to \{0,1\}$ ((hamis, igaz))
$\chi_A(x) := \{ 1, \text{ha } x \in A ; 0, \text{ha } x \notin A\}$

(($A,B \subseteq H$
$\chi_{A \cup B} = \chi_A + \chi_B - \chi_A\chi_B$
$\chi_{A \cap B} = \chi_A\chi_B$
$\chi_{A \setminus B} = \chi_A - \chi_A\chi_B$
$\chi_{A \triangle B} = \chi_A + \chi_B - 2\chi_A\chi_B$
$\chi_{A'} = 1 - \chi_A$))

91. Definiálja a baloldali semleges elem, a jobboldali semleges elem és a semleges elem fogalmát.
Legyen $*$ egy binér művelet a G halmazon. A G halmazt a $*$ művelettel, (azaz, ha pontosak akarunk lenne, a $(G,*)$ párt) szokás grupoidnak is nevezni. A G egy s elemét bal, illetve jobb oldali semleges elemnek nevezzük, ha $s * g = g$, illetve $g * s = g$ minden $g \in G$-re. Ha s bal és jobb oldali semleges elem is, akkor semleges elemnek nevezzük.

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

Ha a $*$ binér művelet a G halmazon asszociatív, azaz $x, y, z \in X$ esetén $(x * y) * z = x * (y * z)$, akkor a G-t (pontosabban a $(G,*)$ párt) félcsoportnak nevezzük. Ha a G félcsoportban s semleges elem, és $g, g^* \in G$-re $g * g^* = s$, akkor azt mondjuk, hogy g a g^* balinverze, g^* pedig a g jobbinverze. Ha a g^* a g bal- és jobbinverze is, akkor azt mondjuk, hogy a g inverze. Ekkor nyilván g meg a g^* inverze.

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

Igen. Ha g-nek g^{-1} az inverze, és h-nak h^{-1} az inverze, akkor a $g * h$ inverze $h^{-1} * g^{-1}$.

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

Csoport olyan matematikai struktúra, amelyben definiálva van egy kétváltozós, asszociatív, invertálható művelet és ∃ egység elem. Jele pl: (G, *) ((halmaz, művelet))
Amennyiben a művelet kommutatív is akkor Abel-csoportról beszélünk.

95. Igaz-e, hogy ha X tetszőleges halmaz, akkor ($\wp(\mathbf{X})$,∩) egy egységelemes félcsoport?

Egy struktúrát, egy kétváltozós művelettel félcsoportnak nevezzük, ha az asszociatív tulajdonság teljesül. Asszociatívitás (csoportosíthatóság): pl. (a ∩ b) ∩ c = a ∩ (b ∩ c) Az egységeleme az X halmaz a teljes halmaz: A ∩ X = A

96. Igaz-e, hogy ha X tetszőleges halmaz, akkor ($\wp(\mathbf{X})$,∪) egy csoport?

Nem, az egységelem az üres halmaz, de rajta kívül senkinek nincs inverze, ha X nem üres.
($\wp(X)$,∪) kommutatív egységelemes félcsoport.

97. Igaz-e, hogy ha X tetszőleges halmaz, akkor ($\wp(\mathbf{X})$,\) egy félcsoport?

Nem. ($\wp(X)$,\)-ben általában nincs egységelem, a művelet nem asszociatív és nem is kommutatív.
(A\B)\C ≠ A\(B\C)

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

Igaz. Az identitás az egységelem; ez általában nem kommutatív és nem is csoport, bár vannak invertálható elemei.

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

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

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

Legyen $k, m, n \in N$. Ekkor

(1) n^+ közvetlenül követi n-et;
(2) $m \leq n \Leftrightarrow$, ha $m + k \leq n + k$;
(3) $k \neq 0$ esetén $m \leq n \Leftrightarrow$, ha $m \cdot k \leq n \cdot k$;
(4) $m < n \Leftrightarrow$, ha $m + k < n + k$;
(5) $k \neq 0$ esetén $m < n \Leftrightarrow$, ha $m \cdot k < n \cdot k$;
(6) $ha\ m \cdot k = n \cdot k$ és $k \neq 0$, akkor $m = n$ (egyszerűsítési szabály vagy törlési szabály $k \neq 0$-ra).

101. Definiálja a véges sorozatokat.

Ha $n \in \mathbb{N}$, akkor a [0,n]⊂ ℕ vagy [1,n]⊂$\mathbb{N}^+$ halmazon értelmezett függvényeket véges sorozatnak nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0, x_1, \dots, x_n$ vagy $x_i,\ i = 0,1,2, \dots, n$, illetve $x_1, x_2, \dots, x_n$ vagy $x_i,\ i = 1,2, \dots, n$.

102. Fogalmazza meg az általános rekurziótételt.

Legyen X egy halmaz, a ∈ X és f: X → X ekkor egy és csak egy g : ℕ → X létezik, hogy $g(0) = a$ és $g(n^+) = f(g(n))$

((Egy X halmazból ugyanoda képező f függvény esetén pontosan egy olyan függvény van, amely a természetes számokból a halmazba képezve, a 0-ra a-t, és n rákövetkezőjére a n f szerinti képét adja. Ez gyakorlatilag a rekurzív sorozat általános megadása függvénnyel.))

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

A Fibonacci számok esetén g : $\mathbb{N} \to X$
g(0) = 1 , g(1)=1 és n ≥ 1 –re $g(n^+) = g(n) + g(n\text{-}1)$

((A fenti képletbe beírva azt, hogy az első elem: 0, a második 1, és onnantól kezdve a következő elem az előző kettő összege.))

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

Ha G egy félcsoport, $x : N^+ \to G$ egy sorozat, akkor az általános rekurziótételt alkalmazva definiálhatjuk a $\Pi_{k=1}^{n} x_k,\ n \in N^+$ szorzatokat úgy, hogy $\Pi_{k=1}^{1} x_k = x_1$ és $\Pi_{k=1}^{n+1} x_k = (\Pi_{k=1}^{n} x_k) \cdot x_{n+1}$. Ha G egységelemes félcsoport e egységelemmel, akkor $\Pi_{k=1}^{0} x_k = e$.

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

A sorozatok tulajdonságaiból következik, vagy indukcióval bizonyítható, hogy $g^{m+n} = g^m \cdot g^n$ és $(g^m)^n = g^{mn}$ minden $m, n \in N^+$-ra, ha G egységelemes félcsoport, akkor minden $m, n \in N$-re.

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

Ha g, h a G félcsoport felcseréhető elemei, akkor indukcióval $(gh)^n = g^n h^n$ minden $n \in N^+$-ra, ha G egységelemes félcsoport, akkor minden $n \in N$-re.

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

Ha G kommutatív, akkor additív írásmódot is használhatunk, ilyenkor a szorzat helyett $\sum_{k=1}^{n} x_k$ összeget írunk. Ha G kommutatív félcsoport 0 nullelemmel, akkor $\sum_{k=1}^{0} x_k = 0$. Ha $x_k = g$ minden n-re, akkor $\sum_{k=1}^{n} x_k$ helyett ng-t írunk, n az együttható. Gyakran $\sum_{k=1}^{n} x_k$ helyett azt írjuk, hogy $x_1 + x_2 + \cdots + x_n$. Ha $x : A \to G$ egy tetszőleges függvény, és van olyan $\varphi : \{k \in N : 1 \leq k \leq n\} \to A$ kölcsönösen egyértelmű leképezés, amely A-ra képez, akkor a kommutativitást és asszociativitást felhasználva indukcióval belátható, hogy minden ilyen leképezésre $\sum_{k=1}^{n} x_{\varphi(k)}$ ugyanaz. (Ez az általános kommutativitás tétele.) Ezt a közös értéket $\sum_{a\in A} x_a$-val is jelöljük.

111. Mit értünk azon, hogy az összeadás és a szorzás kompatibilis a maradékosztályozással?

Legyen $*$ egy binér művelet X-en, és legyen adott X egy osztályozása, illetve a megfelelő $\sim$ ekvivalencia-reláció. Azt mondjuk, hogy a $*$ művelet kompatibilis az osztályozással, illetve az ekvivalenciarelációval, ha $x \sim x'$ és $y \sim y'$ esetén $x * y \sim x' * y'$. Az ekvivalenciareláció tulajdonságai miatt elég azt megkövetelni, hogy $x * y \sim x' * y$ és $x * y \sim x * y'$ teljesüljön.
Ha a művelet kompatibilis az osztályozással, akkor az ekvivalenciaosztályok terén, $X^\sim$-on bevezethetünk egy $*^\sim$ műveletet a $x^\sim *^\sim y^\sim = (x * y)^\sim$ definícióval.

112. Definiálja a nullgyűrű és a zérógyűrű fogalmát.

Egy R halmazt egy $(+,\cdot)$ binér műveletekből álló párral gyűrűnek nevezünk, ha az összeadással Abel-csoport (a nullelemet 0 fogja jelölni), a szorzással félcsoport, és teljesül mindkét oldali disztributivitás.
A nullgyűrű csak egy elemet tartalmaz, ez pedig a 0.
A zérógyűrű olyan Abel-csoport, melyben bármely két elem szorzatát nullának értelmezzük.

Pl: Bármely X halmazra $\wp$(X) a (Δ,∩) műveletekkel kommutativ egységelemes gyűrű (∅ a nulla), amelyben X≠∅ esetén két nem nulla elem "szorzata" lehet nulla

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

Ha x, y egy R gyűrű nullától különböző elemei, és $xy = 0$, akkor azt mondjuk, hogy x és y egy nullosztópár, x bal oldali nullosztó, y pedig jobb oldali nullosztó.

114. Definiálja az integritási tartomány fogalmát.

Kommutatív, nullosztómentes, legalább kételemű gyűrűt integritási tartománynak nevezzük.

115. Definiálja a rendezett integritási tartomány fogalmát.

Az R-et rendezett integritási tartománynak nevezzük, ha rendezett halmaz, integritási tartomány, és
(1) ha $x, y, z \in R$ és $x \leq y$, akkor $x + z \leq y + z$ (az összeadás monoton);
(2) ha $x, y \in R$ és $x, y \geq 0$, akkor $x \cdot y \geq 0$ (a szorzás monoton).

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

Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fennállnak:
(1’) ha $x, y, z \in R$ és $x < y$, akkor $x + z < y + z$ (az összeadás szigorúan monoton);
(2’) ha $x, y \in R$ és $x, y > 0$, akkor $x \cdot y > 0$ (a szorzás szigorúan monoton).

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

Legyen R rendezett integritási tartomány. Ekkor
(1) ha $x > 0$, akkor $-x < 0$, és ha $x < 0$, akkor $-x > 0$;
(2) ha $\mathrm{x} < y$ és $\mathrm{z} > 0$, akkor $\mathrm{xz} < yz$;
(3) ha $\mathrm{x} < y$ és $\mathrm{z} < 0$, akkor $\mathrm{xz} > yz$;
(4) ha $\mathrm{x} \neq 0$, akkor $\mathrm{x}^2 > 0$; speciálisan, ha van egységelem, akkor az pozitív;
(5) ha 1 az egységelem, $0 < \mathrm{x} < y$, és x-nek is, y-nak is van multiplikatív inverze, akkor $0 < \frac{1}{\mathrm{y}} < \frac{1}{\mathrm{x}}$.

118. Definiálja a test és a ferdetest fogalmát és adjon három példát testre.

(T, +, *) Olyan alg. strukt. amely (T, +): összeadásra Abel-csoport, (T, *): szorzásra komm. és assz., minden nem null elemnek van inverze, disztributivitás teljesül mindkét műveletre, létezik egység elem

Ferdetest estén (T, *): szorzásra csak assz., (nem komm.)

pl.: valós számok, komplex számok

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

Egy testet rendezett testnek nevezünk, ha test és rendezett integritási tartomány.
Például a kételemű testen nincs olyan rendezés, amellyel rendezett test, mert rendezett testben $1 > 0$ és $-1 < 0$, de a kételemű testben $-1 = 1$.

120. Fogalmazza meg az arkhimédeszi tulajdonságot.

Egy F rendezett testet archimédeszi tulajdonságúnak nevezünk, ha $x, y \in F$, x>0 esetén van olyan $n \in \mathbb{N}$, amelyre $nx \geq y$

121. Mi a kapcsolata az Arkhimédészi tulajdonságnak a felső határ tulajdonsággal?

Egy F rendezett testet felső határ tulajdonságúnak nevezünk, ha minden nem üres felülről korlátos részhalmazának létezik legkisebb felső korlátja. Egy felső határ tulajdonságú test mindig arkhimédészi tulajdonságú is.

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

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

123. Fogalmazza meg a valós számok egyértelműségét leíró tételt.

Létezik felső határ tulajdonságú test. Egy felső határ tulajdonságú testet valós számoknak nevezünk. Legyen R' és R'' két felsőhatár tulajdonságú test. Ekkor létezik egy φ kölcsönösen egyértelmű leképezése R'-nak R''-re, amely monoton növekedő, összeadás és szorzástartó.

124. Definiálja a bővített valós számokat.

A bővített valós számok halmaza: $\overline{\mathbb{R}}$:=ℝ∪{+∞,-∞}. ((szóval az első ℝ felett van egy felülvonás))

125. Fogalmazza meg a valós számok létezését leíró tételt.

Létezik felsőhatár tulajdonságú rendezett test, amelyet valós számoknak nevezünk.

126.Fogalmazza meg a gyökvonásra vonatkozó tételt.

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

127. Fogalmazza meg a szorzat gyökére vonatkozó állítást.

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

128. Definiálja a komplex számok halmazát a műveletekkel.

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

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 $x \mapsto (x,0)$ leképezés kölcsönösen egyértelmű, összeadás- és szorzástartó leképezése $\mathbb{R}$-nek $\mathbb{C}$-be, ezért az összes $(x,0), x \in \mathbb{R}$ alakú komplex számok halmazát azonosíthatjuk $\mathbb{R}$-el.

Definiálunk egy i számot, amelyre az igaz, hogy i * i = -1
$\mathbb{C}$:= $\mathbb{R}$ + i * $\mathbb{R}$
műveleteket ki kell terjeszteni, hogy az asszociativitás megmaradjon
ha volt kommutativitás a struktúrán akkor az is
új művelet leszűkítése ugyanaz legyen mint ami az eredetiben volt

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

Jelölje i a $(0,1)$ komplex számot. Az $i^2=-1$, az i segítségével az (x,y) komplex számot $x+iy$ alakban írhatjuk, és ez a felírás természetesen egyértelmű. Ezt a szám algebrai alakjának nevezzük. Ha $z=x+iy \in \mathbb{C}$, ahol $x, y \in \mathbb{R}$, akkor x-et a z valós részének, az y-t pedig a z képzetes részének nevettük. A z konjugáltja a z' $=x-iy$ komplex szám. Egy komplex szám pontosan akkor valós, ha megegyezik a konjugáltjával, vagyis képzetes része 0. Ha egy komplex szám valós része nulla, akkor képzetesnek nevezzük.

131. Fogalmazza meg a komplex konjugálás tulajdonságait.

Legyen $z=x+iy \in \mathbb{C}$ és $x, y \in \mathbb{R}$. z konjugáltja: z' $=x-iy$
$z, w \in \mathbb{C}$:
(z')'=z,
(z+w)'=z'+w',
(zw)'=z'w',
z+z'=2$\boldsymbol{\mathcal{Re}}$(z),
z-z'=2i$\boldsymbol{\mathcal{Im}}$(z)

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

Legyen az $(x,y) \in R \times R$ komplex szám abszolút értéke $|(x,y)|=\sqrt{x^2+y^2}$.
Felhasznált tétel: ha $x \in R, x \geq 0, n \in N^+$, akkor egy és csak egy olyan y nem negatív valós szám létezik, amelyre $y^n=x$. Az y számot az x szám n-edik gyökének nevezzük, és $\sqrt[n]{x}$ -szel jelöljük.

133. Fogalmazza meg komplex számok abszolút értékének tulajdonságait.

z,w ∈ $\mathbb{C}$
zz'=|z|^2,
|0|=0, és
z≠0 esetén |z|>0,
|z'|=|z|,
|zw|=|z||w|,
|z+w| ≤ |z| + |w|,
|($\boldsymbol{\mathcal{Re}}$(z))|≤|z|,
|$\boldsymbol{\mathcal{Im}}$(z)|≤|z|,
|z|≤|$\boldsymbol{\mathcal{Re}}$(z)|+|$\boldsymbol{\mathcal{Im}}$(z)|.

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

Legyen $z \in \mathbb{C}$, $sgn(z) = 0$, ha z = 0 és $sgn(z) = \frac{z}{|z|}$ egyébként.

135. Definiálja komplex számok trigonometrikus alakját és argumentumát.

A pozitív x féltengellyel bezárt φ (irányított) szög a $\mathbb{C}$ szám argumentuma, jele: $\arg z$

$\arg z = \varphi$ esetén $\operatorname{sgn}(z) = \cos\varphi + i\sin\varphi$

Ekkor a $z = |z|(\cos\varphi + i\sin\varphi)$ alakot a z $\mathbb{C}$ szám trigonometrikus alakjának nevezzük.

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

Legyen $z, w \in \mathbb{C}$, $z = |z|(\cos\varphi + i\sin\varphi)$ és $w = |w|(\cos\psi + i\sin\psi)$ ahol $\varphi = \arg z$, $\psi = \arg w$.
Ekkor zw trigonometrikus alakja $zw = |zw|(\cos(\varphi+\psi) + i\sin(\varphi+\psi))$.
Ha $w \neq 0$, akkor $\frac{1}{w} = \frac{w}{|w^2|}$, ebből $\frac{z}{w} = \frac{|z|}{|w|}(\cos(\varphi-\psi) + i\sin(\varphi-\psi))$.

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

Indukcióval $|w| = |z|^n$. Ebből $w = 0$ esetén $z = 0$. Egyébként, ha $\varphi = \arg(w)$, akkor a $z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{\varphi+2k\pi}{n}\right) + i\,sin\left(\frac{\varphi+2k\pi}{n}\right)\right)$, $k = 0,1,\dots,n-1$ különböző komplex számok, és csak ezek azok, amelyek n-edik hatványa w.

138. Írja fel az $\mathbf{n}$-edik komplex egységgyököket. Mit értünk primitív $\mathbf{n}$-edik egységgyök alatt?

Ha $w = 1$, akkor az $\epsilon^n = 1$ feltételnek az $\epsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$, $k = 0,1,\dots,n-1$ komplex számok tesznek eleget. Ezeket n-edik komplex egységgyököknek nevezzük. Bizonyos n-edik egységgyökök hatványaiként az összes többi előáll (például $\epsilon_k = \epsilon_1^k$, $k = 0,1,\dots,k-1$), ezeket n-edik primitív egységgyököknek nevezzük.
Primitív n-edik egységgyök fogalamát úgy is értelmezhetjük hogy n-edik hatványa 1, de semmilyen kisebb pozitív egész kitevőjú hatványa nem 1.

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

Ezek $z\epsilon_0, z\epsilon_1, \dots, z\epsilon_{n-1}$.

140. Fogalmazza meg az algebra alaptételét.

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

141. Definiálja halmazok ekvivalenciáját és sorolja fel tulajdonságait.

Az X és Y halmazokat ekvivalensnek nevezzük, ha lézetik X-et Y-ra leképező kölcsönösen egyértelmű leképezés. Jelölése: $X \sim Y$.
Legyenek $X, Y\ és\ Z$ halmazok. Ekkor
(1) $X \sim X$ (reflexivitás);
(2) ha $X \sim Y$, akkor $Y \sim X$ (szimmetria);
(3) ha $X \sim Y$ és $Y \sim Z$, akkor $X \sim Z$ (tranzitivitás).

142. Ha az $\mathbf{X}$ és $\mathbf{X}'$ illetve $\mathbf{Y}$ és $\mathbf{Y}'$ halmazok ekvivalensek, milyen más halmazok ekvivalenciájára következtethetünk még ebből?

Hogy Y^X és ${Y'}^{X'}$ ekvivalensek illetve $X \times Y$ és $X' \times Y'$ is ekvivalnesek.

143. Definiálja a véges és a végtelen halmazok fogalmát.

Egy X halmazt végesnek nevezünk, ha valamely n természetes számra ekvivalens a $\{1,2, \dots, n\}$ halmazzal vagy ha a halmaz üres, egyébként végtelennek nevezzük.

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

Azt az egyértelműen meghatározott természetes számot, amelyre egy adott X véges halmaz ekvivalens $\{1,2, \dots, n\}$-nel, az X halmaz elemei számának vagy számosságának nevezzük, és $card(A)$-val jelöljük.

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

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

146. Fogalmazza meg a skatulyaelvet.

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

((amennyiben a fv. értelmezési tartománya nagyobb elemszámú akkor nem lehet injektív. A függvény többértelmű mivel $\exists\ x_1, x_2 \in X$, hogy $x_1 \neq x_2$, de $f(x_1) = f(x_2)$))

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?

X → X bijekció: X permutációja, Jele: P_n = {1,2,…,n}
A permutáció elemszáma csak az card(X)-től függ
$P_n = n! = \prod_{k=1}^{n} k = 1 * 2 * \ldots * n$

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

Az A halmaz elemeiből készíthető, különböző tagokból álló $a_1, a_2, \ldots, a_k$ sorozatokat, az A halmaz k-ad osztályú variációinak nevezzük. Ha a sorozat elemei különbözőek akkor {1,2,…,k} → A injektív fv.
Az összes elem száma: n! , az osztályok mérete: (n-k)!

$$V_n^k = \frac{n\,!}{(n-k)!} = n * (n-1) * \ldots * (n-k+1)$$

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

Az A halmaz elemeiből készíthető, különböző tagokból álló $a_1, a_2, \ldots, a_k$ sorozatokat, az A halmaz k-ad osztályú variációinak nevezzük. Az összes elem száma n, az elemek ismétlődhetnek, ekkor:

$${}^{i}V_n^k = n^k$$

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

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

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

Legyen f:A→ℕ olyan függvény, amire $\sum_{a \in A} f(a) = k$. Ezeket az A k-ad osztályú ismétléses kombinációjának nevezzük.

$${}^{i}C_n^k = \binom{n+k-1}{k}$$

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

Ha $r, i_1, i_2, \ldots, i_r \in \mathbb{N}$, akkor az $a_1, a_2, \ldots, a_r$ (különböző) elemek $i_1, i_2, \ldots, i_r$ ismétlődésű ismétléses permutációi az olyan $n = i_1 + i_2 + \ldots + i_r$-tagú sorozatok, amelyekben az a_j elem i_j-szer fordul elő.

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

154. Fogalmazza meg a binomiális tételt.

Legyenek x, y egy R kommutatív egységelemes gyűrű elemei, $n \in N$. Ekkor
$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.
Ha a gyűrű nem egységelemes, akkor is igaz az állítás n eleme $\mathbb{N}^+$ esetén, ha formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk

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
1 8 28 56 70 56 28 8 1

156. Mennyi a binomiális együtthatok összege, illetve váltakozó előjellel vett összege?

$\sum_{k=0}^{n}\binom{n}{k} = 2^{\mathrm{n}}$ és $\sum_{k=0}^{n}\binom{n}{k}(-1)^{\mathrm{k}} = 0$ (csak akkor ha $n \neq 0$, mert ha igen, akkor az eredmény 1)

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

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

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, értékeket egy Abel-csoportban felvevő függvény.
Ha $1 \leq i_1 < i_2 < \cdots < i_r \leq k$, akkor legyen

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

Legyen továbbá

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

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

és legyen

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

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 m többszörösének nevezzük, illetve azt mondjuk, hogy n osztható m-el, ha van olyan k természetes szám, hogy $n = mk$; jelölése $m|n$.

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

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

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

Ha egy $n > 1$ természetes szám csak $1 \cdot n = n \cdot 1$ alakban írható fel természetes számok szorzataként, akkor törzsszámnak (vagy felbonthatatlannak, illetve irreducibilisnek) nevezzük. Ekkor n-nek nincs más osztója, mint 1 és saját maga. A $p > 1$ természetes számot prímszámnak nevezzük, ha $p|km$ $(k, m \in N)$ esetén $p|k$ vagy $p|m$. ((Kapcsolat:)) Minden prímszám törzsszám.

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

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.

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

Az 1 asszociáltjai nem mások, mint 1 osztói, hiszen 1 bárminek osztója; ezeket egységeknek nevezzük. Alapjában véve egységnek azt az elemet nevezzük, amivel minden elem osztható. Az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját. Az egységek bármely $a \in R$-nak osztói, mert $1a$-nak osztói.

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

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység. Egy elemnek az asszociáltjaitól különböző osztóit az elem valódi osztóinak nevezzük. Egy nem nulla elemnek az asszociáltjai és az egységek triviális osztói.

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

Mivel ha k,m∈ℤ, akkor |km|=|k|*|m|, az egész számok körében m|n pontosan akkor teljesül, ha |m|||n| az ℕ-ben.

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

Legyen R egységelemes integritási tartomány. Egy $0 \neq a \in R$ elemet felbonthatatlannak (törzsszám, igen 3 különböző neve is van) nevezünk, ha nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc,\ \ b, c \in R$ esetén b vagy c egység.
A $0 \neq p \in R$ elemet prímelemnek nevezzük, ha nem egység és $p|ab\ (a, b \in R)$ esetén $p|a$ vagy $p|b$.
Kapcsolat: minden prímelem felbonthatatlan, mert ha $p = xy$, akkor $p|x$ esetén $x = pz = x(yz)$ miatt $yz = 1$, ahonnan y és z egységek, x és p pedig asszociáltak, és hasonlóan $p|y$ esetén x egység, y és p pedig asszociáltak.

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, és az $a_1, a_2, \dots, a_n \in R$. Ha az $a_1, a_2, \dots, a_n$ elemek legnagyobb közös osztói egységek, akkor azt mondjuk, hogy $a_1, a_2, \dots, a_n$ relatív prímek.

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

R egységelemes integritási tartomány. Azt mondjuk, hogy $b \in R$ 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.

Ha létezik az $a_1, a_2, \dots, a_n \in Z$ számoknak legnagyobb közös osztója, akkor a legnagyobb közös osztók közül az egyik nemnegatív, ezt $lnko(a_1, a_2, \dots, a_n)$-nel jelöljük.

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

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, jelölje ezt $lkkt(a_1, a_2, \dots, a_n)$-nel jelöljük.

175. Ismertesse a bővített euklidészi 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] Legyen $x_0 \leftarrow 1, y_0 \leftarrow 0,\ r_0 \leftarrow a, x_1 \leftarrow 0,\ y_1 \leftarrow 1,\ r_1 \leftarrow b,\ n \leftarrow 0.$

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

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

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

Bármely $a_1, a_2, \ldots, a_n \in Z$ számoknak létezik legnagyobb közös osztója, és $lnko(a_1, a_2, \ldots, a_n) = lnko(lnko(a_1, a_2), a_3, a_4, \ldots, a_n)$.

177. Fogalmazza meg a számelmélet alaptételét.

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

178. Definiálja prímtényezős felbontásnál a kanonikus alakot.

A számelmélet alaptételében szereplő prímtényezős felbontást gyakran $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ alakban írjuk, ahol $p_1, p_2, \ldots, p_k$ 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?

Ha mindnek adott a primétényezős felbontása, akkor közös osztóik, valamint hasonlóan közös többszöröseik is leolvashatóak. Ez a kanonikus alak: $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ ahol $p_1, p_2, \ldots, p_k$ különböző prímek, a kitevők pedig N^+ elemei.

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

Tetszőleges $a, b \in Z$ számoknak létezik legkisebb közös többszöröse, és $lnko(a, b) \cdot lkkt(a, b) = |ab|$.

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

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

182.. Ismertesse Erathoszthenész szitáját.

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

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; ezt úgy jelöljük, hogy $a \equiv b \ (mod\ m)$.
((Más szavakkal **a**-t **m**-mel osztva a maradék **b**.))

184. Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

Ha a és b nem kongruensek modulo m, akkor azt mondjuk, hogy inkongruensek modulo m, és azt írjuk, hogy $a \not\equiv b \ (mod\ m)$. Nyilván, ha $a \equiv b \ (mod\ m)$ és $d|m$, akkor $a \equiv b \ (mod\ d)$ is teljesül. Ha $0 \neq d \in Z$, akkor $a \equiv b \ (mod\ m)$ ekivalens azzal, hogy $ad \equiv bd \ (mod\ md)$.
Az oszthatóság tulajdonságaiból következik, hogy bármely adott $m \in Z$-re a kongruencia ekvivalenciareláció Z-ben. Az m és a $-m$ szerinti kongruencia ugyanazt jelenti.

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

Egy $m \in Z$ 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 $\mathrm{Z_m}$-et. Milyen algebrai struktúra $\mathrm{Z_m}$?

Egy $m \in Z$ modulus szerinti kongruencia ekvivalenciaosztályait maradékosztályoknak nevezzük.
A kongruencia kompatibilis az összeadással és a szorzással. A kongruencia ekvivalenciaosztályok kommutatív egységelemes gyűrűt alkotnak az összeadással és a szorzással. Ezt a gyűrűt Z_m-el jelöljük.

187. Ismertesse a komplemens ábrázolásokat.

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

188. Fogalmazza meg a $\mathrm{Z_m}$ 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.

A diszkrét logaritmus az alap és a hatványozás végeredményének ismerete mellett keresi a hatvány kitevőt. A diszkrét logaritmus probléma ennek a megoldhatósága, maga az algoritmus értelmezett több féle struktúra felett, z legnehezebb megoldhatósági problémát a véges csoportok felett jelenti.

190. Ismertesse a Diffie-Hellmann-Merkle kulcscserét.

Legyen p olyan prím, amire q = 2p+1 is prím (Sophie Germain prím)
1<g<p-1 „alap"
Ha a két felhasználó választ A felh.: 1<a<p illetve B felh.: 1<b<p véletlen kitevőt, majd kiszámoljak, és közzéteszik a g^a mod q illetve g^b mod q értékeket. Mindketten ki tudják számolni g^{ab} mod q érteket, ez lesz a titkos kulcs. Más nem tudja ezt kiszámolni.

191. Definiálja az Euler-féle φ függvényt.

$\varphi: \mathbb{N} \to \mathbb{N}$
$\varphi(m) = |\{j: 1 \leq j \leq m \wedge \text{LNKO}(j,m)=1\}|$

((Magyarul visszaadja azon halmaz elemszámát, amely számok az [1,m] intervallumon relatív prímek m-mel.))

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

Legyen m>1 egész szám, a relatív prím m-hez. Ha $a_1,a_2,...,a_m$ teljes maradékrendszer modulo m és $b\in\mathbb{Z}$, akkor $aa_1+b,aa_2+b,...,aa_m+b$ is teljes maradékrendszer modulo m. Ha $a_1,a_2,...,a(m)$ redukált maradékrendszer modulo m, akkor $aa_1,aa2,...,aa\,\varphi_{(m)}$ is redukált maradékrendszer 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.

Például az $x^2 + y^2 = -4$ problémának valós megoldása nincs, az $x^4 - 4y^4 = 3$ egyenlet egyik oldala pedig modulo 4 kongruens 0-val vagy 1-el, a másik oldala pedig 3-mal, emiatt az egyenletnek nincs egész megoldása. Az $x^2 + y^2 = z^2$ egyenlet megoldásai a pitagoraszi számhármasok, míg ha $n > 2$ egész, akkor a Fermat-sejtés szerint az $x^n + y^n = z^n$ egyenletnek nincsenek nem triviális egész megoldásai.

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 $x \equiv c_j \left(mod\ m_j\right),\ \ j = 1,2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1 m_2 \dots m_n$.

TÉTELEK

1. Fogalmazza meg a halmazok uniójának kommutativitását, asszociativitását és idempotenciáját és bizonyítsa be.

Állítás:
1. kommutativitás: $A \cup B = B \cup A$
2. assziciativitás: $A \cup (B \cup C) = (A \cup B) \cup C$
3. idempotencia: $A \cup A = A$

Bizonyítás:
1. $x \in A \cup B \Leftrightarrow x \in A\, vagy\, x \in B \Leftrightarrow x \in B\, vagy\, x \in A \Leftrightarrow x \in B \cup A$
2. $x \in (A \cup B) \cup C \Leftrightarrow x \in (A \cup B) vagy\, x \in C \Leftrightarrow (x \in A\, vagy\, x \in B) vagy\, x \in C \Leftrightarrow x \in A\, vagy\, (x \in B\, vagy\, x \in C) \Leftrightarrow\ x \in A\, vagy\, x \in (B \cup C) \Leftrightarrow x \in A \cup (B \cup C)$
3. $x \in (A \cup A) \Leftrightarrow x \in A\, vagy\, x \in A \Leftrightarrow x \in A$

2. Fogalmazza meg a halmazok metszetének kommutativitását, asszociativitását és idempotenciáját és bizonyítsa be.

Állítás:
1. kommutativitás: $A \cap B = B \cap A$
2. assziciativitás: $A \cap (B \cap C) = (A \cap B) \cap C$
3. idempotencia: $A \cap A = A$

Bizonyítás
1. $x \in A \cap B \Leftrightarrow x \in A \text{ és } x \in B \Leftrightarrow x \in B \text{ és } x \in A \Leftrightarrow x \in B \cap A$
2. $x \in A \cap (B \cap C) \Leftrightarrow x \in A \text{ és } x \in (B \cap C) \Leftrightarrow x \in A \text{ és } (x \in B \text{ és } x \in C) \Leftrightarrow (x \in A \text{ és } x \in B\, és\, x{\in}C{\Leftrightarrow}\, x{\in}A{\cap}B\, és\, x{\in}C{\Leftrightarrow}x{\in}A{\cap}B{\cap}C$
3. $x \in (A \cap A) \Leftrightarrow x \in A \text{ és } x \in A \Leftrightarrow x \in A$

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

Állítás:
Ha A, B, C halmazok, akkor
(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (a metszet disztributivitása az unióra nézve)
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (az unió disztributivitása a metszetre nézve)
Bizonyítás:
1,

$$x \in A \cap (B \cup C) \Leftrightarrow x \in A \text{ és } x \in (B \cup C) \Leftrightarrow x \in A \text{ és } (x \in B\, vagy\, x \in C)$$
$$\Leftrightarrow (x \in A \text{ és } x \in B)\, vagy\, (x \in A \text{ és } x \in C)$$
$$\Leftrightarrow x \in (A \cap B)\, vagy\, x \in (A \cap C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$$

2,

$$x \in A \cup (B \cap C) \Leftrightarrow x \in A\, vagy\, x \in (B \cap C) \Leftrightarrow x \in A\, vagy\, (x \in B \text{ és } x \in C)$$
$$\Leftrightarrow (x \in A\, vagy\, x \in B) \text{ és } (x \in A\, vagy\, x \in C)$$
$$\Leftrightarrow x \in (A \cup B) \text{ és } x \in (A \cup C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

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

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$
    1. $X \in (A \cup B)' \leftrightarrow x \notin (A \cup B) \Leftrightarrow x \notin A \text{ és } x \notin B \Leftrightarrow x \in A' \text{és } x \in B' \Leftrightarrow x \in A' \cap B'$
    2. $X \in (A \cap B)' \leftrightarrow x \notin (A \cap B) \Leftrightarrow x \notin A\, vagy\, x \notin B \Leftrightarrow x \in A' vagy\, x \in B' \Leftrightarrow x \in A' \cup B'$

5. Bizonyítsa be, hogy binér relációk kompozzíciója asszociatív.

Legyenek A,B,C,D adott halmazok, $f \subset A\ x\ B,\ g \subset B\ x\ C, h \subset C\ x\ D$, ekkor
$f \circ (g \circ h) = (f \circ g) \circ h$ fenáll.
$(x,y) \in (f \circ g) \circ h \Leftrightarrow\ \exists\ z\ \in D_g \cap R_h\ \supset\ D_{f \circ g} \cap R_h$ úgy, hogy $(x,y) \in h$ és $(z,y) \in f \circ g \Leftrightarrow \exists\ z\ \in D_g \cap R_h$ úgy, hogy $(x,y) \in h$ és $\exists\ n\ \in D_f \cap R_g$ úgy, hogy $(z,n) \in g$ és $(n,y) \in f\ \ \Leftrightarrow \exists\ n\ \in D_f \cap R_g \supset D_f \cap R_{g \circ h}$ úgy, hogy $(x,n) \in g \circ h$ és $(n,y) \in f\ \ \Leftrightarrow$ ha $(x,y) \in\ f \circ (g \circ h)$

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

Legyenek A,B,C adott halmazok $f \subset A\ x\ B,\ \ g \subset B\ x\ C$, ekkor $(f \circ g)^{-1} =\ g^{-1} \circ f^{-1}$ fennáll
$(x,y) \in (f \circ g)^{-1} \Leftrightarrow (y,x) \in f \circ g \Leftrightarrow \exists\ z\ \in D_f \cap R_g$ úgy, hogy $(y,z) \in g$ és
$(z,x) \in f \Leftrightarrow \exists\ z \in {R_f}^{-1} \cap {D_g}^{-1}$ úgy, hogy $(x,z) \in f^{-1} \Leftrightarrow (x,y) \in g^{-1} \circ f^{-1}$

7. Fogalmazza meg az ekvivalenciareláció és az osztályozás kapcsolatát és bizonyítsa be.

Állítás: Valamely *X* halmazon értelmezett ~ ekvivalenciareláció *X*-nek egy osztályfelbontását adja. Megfordítva, az *X* halmaz minden osztályfelbontása egy ~ ekvivalenciarelációt hoz létre.
Bizonyítás: Legyen ~ egy *X*-beli ekvivalenciareláció, és legyen $\tilde{x}=\{y \in X : y \sim x\}$ az *X* halmaz *x* eleme segítségével definiált részhalmaza. Megmutatjuk, hogy az $\tilde{X}=\{\tilde{x} : x \in X\}$ halmaz az *X* egy osztályozása. Mivel ~ reflexív, $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az *X* halmaz minden *x* eleme benne van a $\tilde{X}$ valamely elemében, például $\tilde{x}$ -ban. Csak azt kell belátnunk, hogy a különböző részhalmazok metszete üres. Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen *z* a metszet egy eleme. Ekkor *z* ~ *x* és *z* ~ *y*, amiből a szimmetria és a tranzitivitás miatt *x* ~ *y*. Ha most $w \in \tilde{x}$, akkor a tranzitivitás miatt $w \in \tilde{y}$. Hasonlóan, a szimmetria és a tranzitivitás miatt, ha $w \in \tilde{y}$, akkor $w \in \tilde{x}$. Azt kaptuk tehát, hogy $\tilde{x} = \tilde{y}$, azaz ha két részhalmaznak van közös eleme, akkor azonosak, vagyis különböző $\tilde{x}$ részhalmazok diszjunktak, ezért valóban az *X* egy osztályfelbontását kaptuk, és $\tilde{x}$ az *x*-et tartalmazó osztály.
Megfordítva, legyen *O* az *X* egy osztályozása. Legyen
R={(x,y) ∈ *X* × *X : x* és *y* az *O* ugyanazon halmazának elemei*}*.
Ez az *R* nyilván reflexív, szimmetrikus és mivel az osztályok páronként diszjunktak, tranzitív is, tehát ekvivalenciareláció.

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

Állítás: Ha R részbenrendezés és S szigorú részbenrendezés az A halmazon, akkor:
(1) R\$\mathbf{I_x}$ szigorú részbenrendezés,
(2) SU $\mathbf{I_x}$ részbenrendezés, és
(3) S= R\ $\mathbf{I_x}$ pontosan akkor, ha SU $\mathbf{I_x}$ =R.
Bizonyítás:
(1) R\$\mathbf{I_x}$ nyilván irreflexív. Ha (a,b)∈ R\$\mathbf{I_x}$, akkor a≠b, amiből a R antiszimmetriája miatt (b,a)∉R. Ezért (b,a)∉ R\$\mathbf{I_x}$, amiből a szigorú antiszimmetria adódik. Tegyük most fel, hogy (a,b),(b,c)∈ R\$\mathbf{I_x}$. Ekkor R tranzitivitásából (a,c)∈R. Mivel R\$\mathbf{I_x}$ szigorúan antiszimmetrikus, ezért c≠a, így (a,c)∈ R\$\mathbf{I_x}$. Ezzel R\$\mathbf{I_x}$ tranzitiviását is bebizonyítottuk.
(2) SU $\mathbf{I_x}$ reflexívitása a diagonális reláció ($\mathbf{I_x}$) definíciójából következik. Ha (a,b)∈S, akkor (b,a)∉S.Vagyis (a,b),(b,a)∈ SU $\mathbf{I_x}$ csak akkor lehetséges, ha (a,b),(b,a)∈ $\mathbf{I_x}$. Ez pedig SU $\mathbf{I_x}$ antiszimmetriáját jelenti. Tegyük fel, hogy (a,b),(b,c)∈ SU $\mathbf{I_x}$. Ha (a,b),(b,c)∈S, akkor a tranzitivitás miatt (a,c)∈S. Ha egyikük S-nek eleme, a másik pedig $\mathbf{I_x}$ -beli, akkor (a,c) megegyezik (a,b) és (b,c) valamelyikével, és így

ugyancsak S-beli. Amennyiben pedig (a,b),(b,c)∈ $\mathbf{I_x}$, akkor (a,c) is az. Vagyis (a,c) mindig ∈ S∪ $\mathbf{I_x}$ -nak, ami bizonyítja a tranzitivitást.

(3) következik (1)-ből és (2)-ből.

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

Legyenek X és Y részbenrendezett halmazok. Az F:y—>y függvényt monoton növekedőnek nevezzük ha x,y€X, x<y esetén f(x) ≤f(y) és szigorúan monoton növekedőnek nevezzük, ha x,y€X, x<y esetén f(x)<f(y). Szigorúan monoton növekedő fv monoton növekedő is.
Ha X,Y rendezettek, akkor szigorúan monoton növekedő függvény nyilván kölcsönösen egyértelmű is. Megfordítva, ha X és Y rendezettek, akkor egy F:Y—>Y kölcsönösen egyértelmű monoton növekedő leképezés szigorúan monoton növekedő is és az inverze is monoton növekedő f(x)-en. Valóban, ha x<y, akkor f(x)<=f(y), de f(x)=f(y) nem lehetséges, és ha u,v ∈ f(x), u<=v, x=f^{-1}(u), y=f^{-1}(v), akkor x>y nem lehetséges, mert ebből x>=y és x!=y miatt f(x)>=f(y), de f(x)!=f(y), azaz u=f(x)>f(y)=v következménye. A másik eset hasonló módon bizonyítható.

10. Mit állíthatunk a monoton növekedő függvények inverz függvényéről? A megfogalmazott állítást bizonyítsa be.

1. Monoton növekedő függvény inverze (ha van) is monoton növekedő f(x)-en.
2. Ha $n, v \in f(x); n \leq v; x = f^{-1}(n); y = f^{-1}(v)$
   ekkor $x > y$ nem lehetséges, mert $x \geq y$ és $x \neq y$-ból $f(x) \geq f(y)$ de $f(x) \neq f(y)$
   következik, azaz $n = f(x) > f(y) = v$, ami ellentmondás
   Tehát, ha $n, v \in f(x);\ n < v$ akkor $f^{-1}(n) \leq f^{-1}(v)$, sőt $f^{-1}(n) < f^{-1}(v)$

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

Állítás:
Legyen $I \neq \emptyset$ indexhalmaz, X halmaz, $\{X_i \subset X \mid i \in I\}$ indexelt halmazrendszer. Ekkor
1. $(\cap_{i\in I}\ X_i)' = \cup_{i\in I} X_i{}'$
2. $(\cup_{i\in I}\ X_i)' = \cap_{i\in I} X_i'$

Bizonyítás:
1. $x \in (\cap_{i\in I}\ X_i)' \Leftrightarrow x\ \notin \cap_{i\in I} X_i \Leftrightarrow \exists i \in I$ úgy, hogy $x \notin X_i \Leftrightarrow \exists i \in I$ úgy, hogy $x \in X_i' \Leftrightarrow x \in \cup_{i\in I}\ X_i{}'$
2. $x \in (\cup_{i\in I}\ X_i)' \Leftrightarrow x\ \notin \cup_{i\in I} X_i \Leftrightarrow \forall i \in I$ esetén $x \notin X_i \Leftrightarrow \forall i \in I$ esetén $x \in X_i' \Leftrightarrow x \in \cap_{i\in I}\ X_i{}'$

12. Bizonyítsa be, hogy a természetes számok halmaza a ≤ relációval jólrendezett. Azt, hogy rendezett, nem kell bizonyítania.

Legyen $A \subset \mathbb{N}$ nem üres halmaz. Legyen $B = \{m \in \mathbb{N} \mid m \leq n\ \forall\ n \in A\}$.
Nyilván $O \in B$. Ha $n \in A$, akkor $n^+ \notin B$. Tehát van olyan $m \in B$, amelyben $m^+ \notin B$, mert egyébként teljes indukcióval azt kapnánk, hogy $B = \mathbb{N}$. Megmutatjuk, hogy m az A legkisebb eleme. Az világos, hogy alsó korlát, csak azt kell belátnunk, hogy $m \in A$. Ha $m \notin A$ teljesül, akkor minden $n \notin A$-ra $m < n$ lenne, amiből $m^+ \notin B$következne, mer tm^+ közvetlenül követi m-et, ez azonban ellentmondás.

16. Fogalmazzon meg szükséges és elégséges feltételt arra vonatkozóan, hogy egy integritási tartomány rendezett integritási tartomány legyen, és bizonyítsa be az állítást.

- R rendezett integritási tartomány ⇔ R integritási tartomány, R rendezett halmaz,
a) Ha $x, y, z\ \in R$ és $x < y$ akkor $x + z < y + z$

b) Ha $x, y \in R$ és $x, y > 0$ akkor $x * y > 0$
- Ha R rendezett integritási tartomány $\Longrightarrow x \leq y \Leftrightarrow x+z \leq y+z$
tehát ha $x < y \Leftrightarrow x+z \leq y+z$ de $x+z \neq y+z$
mert $x+z = y+z \Leftrightarrow x = z$ ↯
tehát $x < y \Leftrightarrow x+z < y+z$
ha a) $\Longrightarrow$ $x < y \Leftrightarrow x+z < y+z \Rightarrow x+z \leq y+z$
$x = y \Leftrightarrow x+z = y+z \Rightarrow x+z \leq y+z \Longrightarrow$ R r.i.t
- Ha R rendezett integritásitartomány $\Longrightarrow x, y \geq 0 \Leftrightarrow xy \geq 0$
tehát ha $x, y \geq 0 \Longrightarrow xy \geq 0$ de $xy \neq 0$ mert $x, y \neq 0$ ↯
tehát $x, y > 0 \Leftrightarrow xy > 0$
ha b) $\Longrightarrow$ $x, y > 0 \Leftrightarrow xy > 0 \Longrightarrow xy \geq 0$
$x, y = 0 \Leftrightarrow xy = 0 \Longrightarrow xy \geq 0 \Longrightarrow$ R r.i.t

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

a) Ha $x > 0$ akkor $-x < 0$; ha $x < 0$ akkor $-x > 0$
Ha $x > 0 \Longrightarrow 0 = -x + x > -x + 0 = -x$
Ha $x < 0 \Longrightarrow 0 = -x + x < -x + 0 = -x$
b) Ha $x > 0$ és $z > 0$ akkor $x > 0\ xz < yz$
$y - x > y - y = 0 \Longrightarrow (y-x)z > 0 \Longrightarrow yz = (y-x)z + xz > 0 + xz = xz$
c) Ha $x < y$ és $z < 0$ akkor $xz > yz$
$-\big((y-x)z\big) = (y-x)(-z) > 0 \Longrightarrow (y-x)z < 0 \Longrightarrow yz < xz$
d) Ha $x \neq 0$ akkor $x^2 > 0$; spec: ha van egységelem, akkor az pozitív
Ha $x > 0 \Longrightarrow x^2 = x * x > 0$
Ha $x < 0 \Longrightarrow -x > 0 \Longrightarrow x^2 = xx = (-x)(-x) = (-x)^2 > 0$
Spec: $1^2 = 1 > 0$
e) Ha 1 az egységelem, $0 < x < y$ és x,y is multiplikatív invertálható,akkor

$$0 < y^{-1} < x^{-1}, 0 < \frac{1}{y} < \frac{1}{x}$$

Ha $y > 0$ és $v \leq 0$ akkor $yv \leq 0$ de $y\left(\frac{1}{y}\right) = 1 > 0$
Ezért $\frac{1}{y} > 0$. Hasonlóképp $\frac{1}{x} > 0$
Ha $x < 0$, $\left(\frac{1}{x}\right)\left(\frac{1}{y}\right) > 0 \Longrightarrow \frac{1}{y} < \frac{1}{x}$

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

Állítás: Nincs olyan racionális szám melynek négyzete 2.
Bizonyítás:
Ha lenne, akkor lenne olyan is amely felírható m/n alakban, ahol m,n ∈ N^+. Válasszuk azt a felírást melyre a számláló minimális. Mivel $m^2=2n^2$, m páros kell, hogy legyen. Legyen m = 2k ∈ N^+. Ekkor $4k^2=2n^2$, ahonnan $2k^2 = n^2$. Innen n is páros. Ez ellentmond annak, hogy a számláló minimális.

19. Fogalmazza meg az arkhimédeszi tulajdonságot. Mi a kapcsolata a felsőhatár tulajdonsággal? Bizonyítsa be állítását.

Arkhimédeszi tulajdonság: Egy T(+;*;≤) rendezett test arkhimédeszi tulajdonságú, ha minden x,y ∈ T : x > 0 esetén létezik n ∈ N : nx > y. Ekkor T arkhimédeszien rendezett.
Állítás:
Ha T felsőhatár tulajdonságú,rendezett test akkor T arkhimédeszi tulajdonságú.

Bizonyítás:
T.F.H. nem ekkor y felső korlátja: A = {nx | n ∈ N}
Legyen z = sup(A) ekkor z-x < z nem felső korlát ekkor létezik n : nx > z-x ℘
amiből (n+1)x > z. ez ellentmond a feltevésnek!

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

Állítás:
A racionális számok rendezett teste arkhimédészi tulajdonságú de nem felsőhatár tulajdonságú.
Bizonyítás:
Legyen x > 0. Ha y ≤ 0, akkor n = 0 választással, ha pedig x = i/j, y = k/m, i,j,k,m $\in$ N^+, akkor n $\geq$ kj választással nx $\geq$ y, így kapjuk, hogy Q arkhimédészi tulajdonságú.
Legyen A az összes olyan r > 0 racionális számok halmaza amelyekre r2 < 2, és legyen B az összes olyan r > 0 racionális számok halmaza r2 > 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, így A-nak nincs legnagyobb eleme. Ha r $\in$ B, akkor s < r, de s^2 > 2, így B-nek nincs legkissebb eleme. Innen következik, hogy A-nak nincs legkisebb felső korlátja: ha lenne, nem lehetne A-ban, mert akkor A legnagyobb eleme lenne, így B-ben kell lennie, de B-nek nincs legkisebb eleme.

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

A kompelx számok halmaza ℂ = ℝ × ℝ, a valós számpárok halmaz, az
(x,y) + (x',y') = (x+x',y+y') összeadással és
(x,y) * (x',y') = (xx' - yy', y'x + yx') szorzással mint műveletekkel.
Bizonyítás:
Egyszerű számolás mutatja, hogy ℂ test a fenti műveletekkel: nullelem a (0,0) pár, az (x,y) pár additív inverze a (-x,-y) pár, egységelem az (1,0) pár, és a nullelemtől különböző (x,y) pár multiplikatív inverze az $(x/(x^2+y^2), -y/(x^2+y^2))$ pár.

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

- $z * \overline{z} = |z|^2$
Ha $z = (a;b) \Longrightarrow (a;b) * (a;-b) = (a^2+b^2; ab-ab) = (a^2+b^2;0) = |z|^2$
- |0|=0; ha $z \neq 0$ akkor |z|>0
$|0| = 0^2 + 0^2 = 0$
Ha z=a+bi ⟹ $a^2; b^2 \geq 0 \Longrightarrow a^2+b^2 \geq 0$ Ha $a \neq 0 \neq b$ akkor $a^2+b^2 > 0$
- $|\overline{z}| = |z|$
$|\overline{z}| = \sqrt{a^2 + -b^2} = \sqrt{a^2+b^2} = |z|$
-$|zw| = |z||w|$
$|zw|^2 = z\overline{z}w\overline{w} = |z|^2|w|^2$
-$|Re(z)| \leq |z|; |Im(z) \leq |z||$
$\sqrt{a^2} \leq \sqrt{a^2+b^2} \Longleftarrow a^2 \leq a^2+b^2 \Longleftarrow 0 \leq b^2$ ami mindig igaz
$\sqrt{b^2} \leq \sqrt{a^2+b^2} \Longleftarrow b^2 \leq a^2+b^2 \Longleftarrow 0 \leq a^2$

-$|z| \leq |Re(z)| + |Im(z)|$
$\sqrt{a^2+b^2} \leq \sqrt{a^2} + \sqrt{b^2} \Leftarrow a^2+b^2 \leq a^2+b^2+2\sqrt{a}\sqrt{b}$
-$|z+w| \leq |z| + |w|$

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

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

$$\left.\begin{array}{r} |z| \leq |z-w| + |w| \Rightarrow |z| - |w| \leq |z-w| \\ |w| \leq |w-z| + |z| \Rightarrow |w| - |z| \leq |w-z| = |z-w| \end{array}\right\} \Rightarrow ||z|-|w|| \leq |z-w|$$

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

Teljes indukcióval: n=0-ra világos.
Tfh n-re teljesül, de n+1-re létezik f kölcsönösen egyértelmű leképezés {1,2,…,n+1}-nek és A valódi részhalmazának.
Ha $n+1 \notin A$ akkor f|{1,2,…,n} kölcsönösen egyértelmű leképezése {1,2,…,n}-nek egy valódi részhalmazára, mivel $n+1 \notin rrg(f)$ de ez ↯
Ha $n+1 \in A$, akkor $\{1,2,\dots,n\} \sim A\{n+1\}$ hogy (k;n+1) és az (n+1;l) párokat kihagyjuk a leképezésből, helyettük a (k;l) párt vesszük be, ha k=1=n+1 nem áll fenn. Ez megint ellentmondás.
35. Fogalmazza meg a logikai szita formulást és bizonyítsa be.
$X_1; X_2; \dots; X_k \subset X$ (véges); $f\colon X \to A$ ((A;X)Abel-csoport); $1 \leq i_1 < i_2 <..< i_r \leq k$
Legyen $Y_{i1;i2;..;ir} = X_{i1} \cap X_{i2} \cap..\cap X_{ir}$; Legyen $S = \sum_{x\in x} f(x)$
Legyen $S_r = \sum_{i\leq i_1<i_2<..<i_r\leq k}(\sum_{x\in Y_{i_1;i_2;..;i_k}} f(x))$; Legyen $S_0 = \sum_{x\in X\setminus\cup_{i=1}^{k} x_i} f(x)$
Ekkor $S_0 = S - S_1 + S_2 - S_3 +..+ (-1)^k S_k$
Ha $x \in X\setminus\cup_{i=1}^{k} X_i$ akkor mindkét oldalon egyszerre szerepel f(x) (S;S_0)
Egyébként legyen $X_{j1}; X_{j2}; ..; X_{jt}$ azok a részhalmazok, amiben szerepel x.
bal oldalon ekkor nincs f(x).
jobb oldalon f(x) akkor lép fel valami $\sum_{x\in Y_{i_1;i_2;..;i_r}} f(x)$ összegben, ha $\{i_1; i_2; ..; i_r\} \leq \{j_1; j_2; ..; j_t\}$. Ha r>t akkor nincsen ilyen, ha $r \leq t$ akkor pontosan $\binom{t}{r}$ ilyen van, így a jobb oldalon f(x) együtthatója $\sum_{r=0}^{t}\binom{t}{r}(-1)^r = 0$

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

Állítás: Legyenek X és Y halmazok. Ekkor:
1) ha X véges és Y $\subseteq$ X, akkor Y is véges, és #(Y) ≤ #(X);
2) ha X véges és Y $\subset$ X, akkor #(Y) < #(X);
3) ha X és Y végesek és diszjunktak, akkor X $\cup$ Y is véges, és #(X $\cup$ Y) = #(X) + #(Y);
4) ha X és Y végesek, akkor #(X $\cup$ Y) + # (X ∩ Y) = #(X) + #(Y);
5) ha X és Y végesek, akkor X × Y is véges, és #(X × Y) = #(X) * #(Y);
6) ha X és Y végesek, akkor X^Y is véges, és $\#(X^Y) = \#(X)^{\#(Y)}$;
7) ha X véges halmaz, akkor $\wp$ (X) is véges, és #($\wp$ (X)) = $2^{\#(X)}$;
8) ha X véges, és az f függvény X-et Y-ra képzi, akkor Y is véges, #(Y) ≤ #(X), és ha f nem kölcsönösen egyértelmű, akkor #(Y) < #(X);

Bizonyítás:
1) nyilvánvaló, ha Y = X, ha viszont Y $\subset$ X, akkor ekvivalens {1,2,...#(X)} egy valódi részhalmazával, amiről tudjuk, hogy ekvivalens {1,2,...,m}-mel valamely m < n-re. Ezzel 2)-t is beláttuk. 3) azon múlik, hogy {m + 1, m + 2, ..., m + n} ekvivalens {1,2,...,n}-nel ami n szerinti indukcióval következik. 3) #(X $\cup$ Y) = #(X \ Y)

+ #(X ∩ Y) + #(Y \ X); mindkét oldalhoz hozzáadva #(X ∩ Y)-t és ujra felhasználva 3)-at kapjuk 4)-et. 5) és 6) az Y elemeinek száma szerinti teljes indukcióval következnek. 7)következik 6)-ból és $\wp$ (X)-nek a karakterisztikus függvények halmazával való ekvivalenciájából. 8) bizonyításához feltehetjük, hogy X = {1,2,...,#(X)}. Minden y ∈ Y-ra legyen g(y) az $f^{-1}(y)$ halmaz legkisebb eleme. Ekkor g az Y-t kölcsönösen egyértelműen képzi le X egy részhalmazára, és ha f nem volt kölcsönösen egyértelmű , akkor ez a részhalmaz valódi.

26. Fogalmazza meg a skatulyaelvet és bizonyítsa be.

Állítás: Ha X és Y véges halmazok, és #(X) > #(Y) akkor egy f: X $\rightarrow$ Y leképezés nem lehet kölcsönösen egyértelmű.
Bizonyítás: Egyébként {1,2,...,#(Y)} egy részhalmaza, azaz #(Y) < # (X) miatt {1,2,...,#(X)} egy valódi részhalmaza ekvivalens lenne {1,2,...., #(X)}-nel.

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

Állítás: Részben rendezett halmaz bármely nem üres véges részhalmazának van maximális és minimális eleme.
Bizonyítás: A halmaz elemeinek száma szerinti teljes indukcióval. Ha #(A) = 1, akkor nyilvánvaló. Ha #(A) = n + 1, legyen a $\in$ A és A' = A \ {a}. Ha a nem nagyobb, mint A' egy adott a' maximális eleme, akkor a' maximális elem, egyébként a maximális elem. Minimális elemre a bizonyítás hasonló.

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

Ha egy A halmaz ekvivalens $\{1,2, \dots, n\}$-nel, akkor tudjuk, hogy permutációinak halmaza ekvivalens $\{1,2, \dots, n\}$ permutációinak halmazával. Ha $A = \{a_1, a_2, \dots, a_n\}$ és p_1, p_2, …, p_n az $\{1,2, \dots, n\}$ egy permutációja, akkor az A megfelelő permutációja az $a_i \longmapsto a_{p_i}$ leképezés. Így A permutációinak száma csak $n = ?\,(A)$-tól függ. Jelölje ezt a számot P_n.
Teljes indukcióval megmutatjuk, hogy $P_n = \prod_{k=1}^{n} k$. Feltéve, hogy n-re igaz az állítás, tekintsük ekvivalensnek, $\{1,2, \dots, n+1\}$ két permutációját, ha mindkettőnél az 1 képe ugyanaz. Világos, hogy n+1 ekvivalenciaosztály van, és egy ekvivalenciaosztály elemei megfeleltethetők egy n elemű halmaz permutációinak. Így minden ekvivalenciaosztálynak P_n eleme van, ahonnan

$$P_{n+1} = \left(\prod_{k=1}^{n} k\right) \cdot (n+1) = \prod_{k=1}^{n+1} k$$

A $P_n = \prod_{k=1}^{n} k$ szorzatot n!-sal is jelöljük.

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

Az A halmaz elemeiből készíthető, különböző tagokból álló a1, a2, …, ak sorozatokat, azaz $\{1,2, \dots, k\}$-t A-ba képző kölcsönösen egyértelmű leképezéseket az A halmaz k-ad osztályú variációinak nevezzük. Ha A véges halmaz, $?\,(A) = n$, akkor ezek V_n^kszáma megegyezik az $\{1,2, \dots, k\}$-t $\{1,2, \dots, n\}$-be képező kölcsönösen egyértelmű leképezések számával.
Megmutatjuk, hogy

$$\bigvee_{n}^{k} = \frac{n!}{(n-k)!} = n(n-1) \dots (n-k+1)$$

ha $k \leq n$. Soroljuk $\{1,2, \dots n\}$ két permutációját egy osztályba, ha $\{1,2, \dots k\}$-n megegyeznek. Minden osztálynak $(n-k)!$ elme van, az osztályok száma pedig V_n^k, ahonnan kapjuk az állítást.

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

Ha $k \in \mathbb{N}$, akkor az A halmaz k elemű részhalmazait az A halmaz k-ad osztályú kombinációinak nevezzük. Ha A véges halmaz, $?\,(A) = n$, akkor ezek C_n^k száma megegyezik a $\{1,2,\ldots,n\}$ halmaz k elemű részhalmazainak számával.
Megmutatjuk, hogy

$$C_n^k = \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\cdot\ldots\cdot k}$$

ha $k \leq n$. Soroljuk $\{1,2,\ldots n\}$ két variációját egy osztályba, ha értékkészlete ugyanaz. Minden osztálynak k! eleme van, az osztályok száma pedig C_n^k, ahonnnan kapjuk az állítást.
Szokásos C_n^k helyett az

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{1\cdot 2\cdot\ldots\cdot k}$$

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

Ha $k \in \mathbb{N}$, akkor az A halmazból k elemet kiválasztva ismétléseket is megengedve de tekintet nélkül a sorrendre, az A halmaz k-ad osztályú ismétléses kombinációját kapjuk. Pontosabban, tekintsük mindazokat az $f\colon A \longrightarrow \mathbb{N}$ függvényeket, amelyek csak véges sok helyen vesznek fel nem nulla értéket, és ezen értékek összege k; ezek az A halmaz ismétléses kombinációi.
Megmutatjuk, hogy

$${}^{i}C_n^k = \binom{n+k-1}{k}$$

Egy $g\colon\{1,2,\ldots k\} \longrightarrow \{1,2,\ldots n\}$ monoton növekvő függvényhez definiáljuk a h függvényt a h(j)=g(j)+j-1 összefüggéssel. Ezzel kölcsönösen egyértelmű megfeleltetést létesítettünk az $\{1,2,\ldots,k\}$-t $\{1,2,\ldots n\}$-be képző monoton növekvő függvények és az $\{1,2,\ldots k\}$-t $\{1,2,\ldots,n+k-1\}$-be képző szigorúan monoton növekvő függvények között, aminek létezéséből következik az állítás.

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

Ha $r, i_1, i_2, \ldots, i_r \in \mathbb{N}$, akkor az $a_1, a_2, \ldots a_r$ (különböző) elemek $i_1, i_2, \ldots, i_r$ ismétlődésű ismétléses permutációi az olyan $n = i_1 + i_2 + \cdots + i_r$ tagú sorozatok, amelyekben az a_j elem i_j-szer forul elő.
Megmutatjuk, hogy ezek száma

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

Ha r=0 és ha r=1, akkor igaz az állítás. Egyébként soroljuk az $a_1, a_2, \ldots a_r$ elemek két $i_1, i_2, \ldots i_r$ ismétlődésű ismétléses permutációját egy osztályba, ha az a_1 elem összes előfordulását kihagyva a sorozatból ugyanazt a $b_1, b_2, \ldots b_{n-i_1}$ ismétléses permutációt kapjuk.

33. Fogalmazza meg a binominális tételt és bizonyítsa be.

Állítás:
Legyenek x,y egy R kommutatív egységelemes gyűrű elemei, $n \in \mathbb{N}$. Ekkor

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

Ha a gyűrű nem egységelemes, akkor is igaz az állítás $n \in \mathbb{N}^+$ esetén, ha a formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk.
Az $\binom{n}{k}$ együtthatókat binominális együtthatóknak is nevezik. Szokásos elrendezésük a Pascal-háromszög: az n indexű sorban az $(x+y)^n$-ben fellépő együtthatók vannak.
Bizonyítás:
Indukcióval: n=0, 1-re igaz az állítás nyilvánvaló. Ha n-re teljesül, akkor a disztributivitást felhasználva,

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

így csak azt kell belátnunk, hogy

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

ha $0 \le k < n$, ami a bal oldalt közös nevezőre hozva adódik.
Következmény:

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

Bizonyítás:
A binominális tételből x=1, y=1, illetve az x=1, y=-1 helyettesítéssel adódik.

34. Fogalmazza meg a polinomiális tételt és bizonyítsa be.

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

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

Ha a gyűrű nem egységelemes, akkor is igaz az állítás $r, n \in \mathbb{N}^+$, $i_1, \dots i_r \in \mathbb{N}$ esetén, ha a formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk.
A tételben játszott szerepük miatt szokás a $P_n^{i_1,i_2,\dots,i_r}$ számokat polinomiális együtthatóknak is nevezni.
Bizonyítás: Indukcióval: r=0, 1-re az állítás nyilvánvaló, az r=2 esetet már láttuk. Ha r-1-re teljesül, akkor $y=x_2+\dots+x_r$ jelöléssel, a binomiális tételt és az indukciós feltevést használva,

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

$$= \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}\sum_{i_1+\cdots+i_r=n-i_1} P_{n-i_1}^{i_2,\dots,i_r}x_2^{i_2}\dots x_r^{i_r}$$

$$= \sum_{i_1=0}^{n}\frac{n!}{i_1!\,(n-i_1)!}x_1^{i_1}\sum_{i_1+\cdots+i_r=n-i_1}\frac{(n-i_1)!}{i_2!\dots i_r!}x_2^{i_2}\dots x_r^{i_r}$$

$$= \sum_{i_1+i_2+\cdots+i_r=n} P_{n-i_1}^{i_1,i_2,\dots,i_r}x_1^{i_1}x_2^{i_2}\dots x_r^{i_r}$$

35. Fogalmazza meg a logikai szita formulást és bizonyítsa be.

$X_1; X_2; \dots; X_k \subset X$ (véges); $f: X \to A$ ((A;X)Abel-csoport); $1 \le i_1 < i_2 <..< i_r \le k$
Legyen $Y_{i1;i2;..;ir} = X_{i1} \cap X_{i2} \cap..\cap X_{ir}$; Legyen $S = \sum_{x\in x} f(x)$
Legyen $S_r = \sum_{i\le i_1<i_2<..<i_r\le k}(\sum_{x\in Y_{i_1;i_2;..;i_k}} f(x))$; Legyen $S_0 = \sum_{x\in X\setminus\cup_{i=1}^{k}x_i} f(x)$
Ekkor $S_0 = S - S_1 + S_2 - S_3 +..+(-1)^k S_k$

Ha $x \in X \setminus \cup_{i=1}^{k} X_i$ akkor mindkét oldalon egyszerre szerepel f(x) ($S;S_0$)
Egyébként legyen $X_{j1}; X_{j2}; ..; X_{jt}$ azok a részhalmazok, amiben szerepel x.
bal oldalon ekkor nincs f(x).
jobb oldalon f(x) akkor lép fel valami $\sum_{x \in Y_{i_1;i_2;..;i_r}} f(x)$ összegben, ha $\{i_1; i_2; ..; i_r\} \leq \{j_1; j_2; ..; j_t\}$. Ha r>t akkor nincsen ilyen, ha $r \leq t$ akkor pontosan $\binom{t}{r}$ ilyen 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.

Állítás:

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

Bizonyítás: A bizonyítások a definíció alapján triviálisak

37. Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait és bizonyítsa be ezeket.

Egy egységelemes integritási tartomány elemei körében

(1) ha $b|a$ és $b'|a'$, akkor $bb'|aa'$;
(2) a nullának minden természetes szám osztója;
(3) a nulla csak saját magának osztója;
(4) az 1 minden elemnek az osztója;
(5) ha $b|a$, akkor $bc|ac$ minden $c \in R$-re;
(6) ha $bc|ac$;s $c \neq 0$, akkor $b|a$;
(7) ha $b|a_i$ és $c_i \in R, (i = 1,2, \dots, j)$, akkor $b| \sum_{i=1}^{j} c_i a_i$;
(8) az $|$ reláció reflexív és tranzitív.

38. Mi a kapcsolat az egységek és az asszociáltak között? Bizonyítsa be állítását.

Egy elem asszociáltjait létrehozhatjuk az 1 asszociáltjai segítségével, amelyek nem mások, mint az 1 osztói, hiszen 1 bárminek az osztója, ezeket egységeknek nevezzük. Az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját. Az egységek bármely $a \in \mathbb{R}$-nek osztói, mert 1a-nak osztói. Megfordítva nyilvánvaló. Ha egy elem minden $a \in \mathbb{R}$-nek osztója, akkor egység. Az $a \in \mathbb{R}$ asszociáltján az εa alakú elemek, ahol ε egység.

39. Ismertesse a bővítettbővített euklideszi algoritmust. Bizonyítsa be, hogy működik.

Állítás:
A következő eljárás egy R euklideszi gyűrűben meghatározza az a,b ∈ R elemek egy d legnagyobb közös osztóját, valamint az x,y ∈ R elemeket úgy, hogy d = ax + by teljesüljön.(Az eljárás során végig $ax_n + by_n = r_n$, n = 0,1,....)

(1) [Inicializálás] Legyen $x_0 \leftarrow e$ (a gyűrű egységeleme), $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow e$, $r_1 \leftarrow b$, $n \leftarrow 0$.
(2) [Vége?] Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.
(3) [Ciklus] Legyen $r_n = q_{n+1}r_{n+1} + r_{n+2}$, ahol $r_{n+2} = 0$ vagy $\phi(r_{n+2}) < \phi(r_{n+1})$, legyen $x_{n+2} \leftarrow x_n - q_{n+1}x_{n+1}$, $y_{n+2} \leftarrow y_n - q_{n+1}y_{n+1}$, $n \leftarrow n + 1$, és menjünk (2)-re.
Bizonyítás:
Mivel a $\phi(r1)$, $\phi(r2)$,... természetes számok szigorúan monoton csökkenő sorozata, az eljárás véget ér, mert egyébként N nem lenne jólrendezett. Teljes indukcióval $ax_n + by_n = r_n$, így $d = ax + by$. Innen a és b közös osztói mind osztói d-nek. Mivel $r_{n+1} = 0$ vagy $n = 0$ ekkor $d = a$ és $b = 0$ vagy pedig $n > 0$, és $r_0, r_1, \ldots, r_{n-1}$ mind többszörösei r_n-nek, mert $r_{n-1} = q_n r_n$, $r_{n-2} = q_{n-1}r_{n-1} + r_n$, és így tovább, speciálisan $a = r_0$ és $b = r_1$ többszörösei d-nek.

40. Mi a kapcsolat $\mathbb{Z}$-ben a prímelemek és az irreducibilis elemek között? Bizonyítsa állítását.

Állítás:
A Z egy elem pontosan akkor felbonthatatlan(irreducibilis) ha prímelem.
A természetes számokra megfogalmazva az állítást, egy természetes szám akkor prímszám ha törzsszám.
Bizonyítás:
Azt már beláttuk, hogy prímelem felbonthatatlan. Tegyük fel, hogy p felbonthatatlan, és legyen $p|mn$. Tegyük fel, hogy p nem osztója m-nek. Ekkor p és m relatív prímek. A bővített Euklideszi algoritmussal kaphatunk olyan x,y egészeket, hogy $px + my = 1$. Innen $pnx + mny = n$. Mivel p osztója a bal oldalnak, a jobb oldalnak is.

41. Fogalmazza meg és bizonyítsa be a számelmélet alaptételét.

Állítás:
Minden pozitív természetes szám a sorrendtől eltekintve egyértelműen felírható prímszámok szorzataként
Egész számokra fogalmazva az állítást, minden nem 0 és nem egység egész szám előáll prímelemek szorzataként, és az előállítás sorrendtől és asszociáltaktól eltekintve egyértelmű.
Bizonyítás:
Ha $n = 1$, a felbontás az 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 szorzatnak 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 jólrendezettsége miatt véges sok lépésben csupa törzsszám tényezőből álló felbontáshoz vezet.
A felbontás egyértalműségének bizonyításához tegyük fel indirekt, hogy van olyan természetes szám, amely két lényegesen különböző módon bontható fel és legyen n a legkisebb ilyen:
$n = p_1p_2 \ldots p_j = q_1q_2 \ldots q_k$.
Mivel $p_1|n$ azaz $p_1|q_1q_2 \ldots q_k$ a p_1 prímtulajdonsága miatt van olyan i, hogy $p_1|q_i$. Ekkor viszont $p_1 = q_i$, mert qi törzsszám. Egyszerűsítve a közös tényezővel egy kisebb n' számot kapunk, amelynek felbontása nem egyértelmű, ami ellentmondás.

42. Fogalmazza meg Eukleidész tételét, és bizonyítsa be.

Állítás:
Végtelen sok prímszám van.
Bizonyítás:
Tegyük fel indirekt, hogy véges sok prímszám van, $p_1, p_2, \ldots, p_k$, és legyen $n = \prod^{k}_{j=1} p_j$. Ekkor $n + 1$ minden p_j-vel osztva 1-et ad maradékként, tehát nem osztható egyetlen p_j-vel sem. Így 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.

Állítás:
Ha a $\equiv$ b (m) és d|m, akkor a $\equiv$ b (d) is teljesül.
Ha 0 $\neq$ d $\in$ Z, akkor a $\equiv$ b (m) ekvivalens azzal, hogy ad $\equiv$ bd (md)
Az oszthatóság tulajdonságaiból azonnal következik, hogy bármely adott m $\in$ Z-re a kongruencia ekvivalenciareláció Z-ben
Bizonyítás:-

44. Fogalmazza meg a Z_m gyűrű tulajdonságait leíró tételt és bizonyítsa be.

Állítás:
Legyen 1 < m ∈ Z. Ha 1 < lnko(a,m) < m, akkor *a* maradékosztálya nullosztó Z_m.-ben. Ha lnko(a,m) = 1, akkor *a* maradékosztályának van multiplikatív inverze Z_m.-ben. Speciálisan, ha *m* prímszám, akkor Z_m. test.
Bizonyítás:-

45. Mit mondhatunk az aa_i+b számokról, ha a_i egy maradékrendszer, illetve egy redukált maradékrendszer elemeit futja be? Bizonyítsa be állítását.

Állítás:
Legyen m>1 egész szám, a relatív prím m-hez. ha $a_1, a_2, \dots, a_m$ teljes maradékrendszer modulo m és $b \in \mathbb{Z}$, akkor $aa_1 + b, aa_2 + b, \dots, aa_m + b$ is teljes maradékrendszer modulo m. Ha $a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradékrendszer modulo m, akkor $aa_1, aa_2, \dots, aa_{\varphi(m)}$ is redukált maradékrendszer modulo m.
Bizonyítás:
Ha $i \neq j$ esetén $aa_i + b \equiv aa_j + b$ (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 az $aa_i + b, i = 1,2, \dots m$ számok páronként inkongruensek, és – mivel számuk m – teljes maradékrendszert alkotnak modulo m. A másik állítás bizonyításához vegyük észre, hogy ha $lnko(aa_i, m) > 1$, akkor $lnko(a_i, m) > 1$. Így az $aa_i, i = 1,2, \dots \varphi(m)$ számok páronként relatív prímek, a modulushoz is relatív prímek és számuk $\varphi(m)$, tehát redukált maradékrendszert alkotnak.

46. Fogalmazza meg és bizonyítsa be az Euler-Fermat tételt.

Állítás:
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

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} (aa_j) \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod m$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím *m*-hez, van inverze modulo *m*. Ezzel megszorozva mindkét oldalt, kapjuk az állítást.

47. Fogalmazza meg és bizonyítsa be a Fermat-tételt.

Állítás:

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 $a^p \equiv a\ (mod\ p)$.
Bizonyítás:
Nyilván $\varphi(p) = p - 1$, így az első alak következik az előző tételből. A második alak a $p \nmid a$ 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 az $ax \equiv b$ (mod m) kongruencia megoldásait. A probléma nyilván azzal ekvivalens, hogy találjunk olyan x egész számot, amelyre valamely y egész számmal $ax + my = b$ teljesül. Legyen $d = lnko(a, m)$. Mivel d osztója ax+my-nak, osztója kell legyen b-nek, egyébként nincs megoldás.
Tegyük fel, hogy a=a'd, b=b'd, m=m'd valamely a', b', m'∈$\mathbb{Z}$-re. Azt kapjuk, hogy az egyenletünk az a'x+m'y=b', illetve az a'x≡b' (mod m') egyenlettel ekvivalens, ahol a' és m' relatív prímek. A legnagyobb közös osztó kiszámítását a bővített euklideszi algoritmussal végezve, olyan x_0, y_0 egészeket is kapunk, amelyre $ax_0+my_0=d$, azaz $a'x_0+m'y_0=1$. Szorozva b'-vel, $a'x_1+m'y_1=b'$, ahol $x_1=x_0b'$ és $y_1=y_0b'$. Az általános megoldáshoz vonjuk ki ezt az egyenletet az 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∈$\mathbb{Z}$-re.
Minden ilyen x ténylegesen megoldás, mert $y=y_1-ka'$-vel a'x+m'y=b'.

50. Fogalmazza meg és bizonyítsa be a kínai maradéktételt.

Legyenek $m_1, m_2, .., m_n$ egynél nagyobb páronként relatív prím természetes számok, $c_1, c_2, .., c_n \in \mathbb{Z}$. Az $x \equiv c_j(mod\ m_j)$, j=1,2,..,n kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1, m_2, .., m_n$
Legyen $m = m_1 m_2$. A bővített euklideszi algoritmussal olyan x_1, x_2 egész számokat kaphatunk, amelyekre $m_1x_1 + m_2x_2 = 1$. Legyen $c_{1.2} = m_1x_1c_2 + m_2x_2c_1$. 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 másik megoldása, akkor $x - c_{1,2}$ osztható m_1-el és m_2-vel, tehát a szorzatukkal is. Az eredeti kongruenciarendszer tehát ekvivalens az $x \equiv c_{1,2j}(mod\ m)$, $x \equiv c_j(mod\ m_j)$, ha j=3,4,…,n kongruenciarendszerrel. Így n szerinti indukcióval adódik a bizonyítás.