Bizonyítások

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

Állítás:

(1) $A \cup B = B \cup A$ (kommutativitás),
(2) $(A \cup B) \cup C = A \cup (B \cup C)$ (asszociativitás),
(3) $A \cup A = A$ (idempotencia).

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) $A \cap B = B \cap A$ (kommutativitás),
(2) $(A \cap B) \cap C = A \cap (B \cap C)$ (asszociativitás),
(3) $A \cap A = A$ (idempotencia).

Bizonyítás:

(1) $x \in A \cap B \Leftrightarrow x \in A$ és $x \in B \Leftrightarrow x \in B$ és $x \in A \Leftrightarrow x \in B \cap A$
(2) $x \in (A \cap B) \cap C \Leftrightarrow x \in (A \cap B)$ és $x \in C \Leftrightarrow (x \in A$ és $x \in B)$ és $x \in C \Leftrightarrow x \in A$ és $(x \in B$ és $x \in C) \Leftrightarrow x \in A$ és $x \in (B \cap C) \Leftrightarrow x \in A \cap (B \cap C)$
(3) $x \in (A \cap A) \Leftrightarrow x \in A$ és $x \in A \Leftrightarrow x \in A$

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

Állítás:

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

Bizonyítás:

(1) $x \in A \cup (B \cap C) \Leftrightarrow x \in A$ vagy $x \in (B \cap C) \Leftrightarrow x \in A$ vagy $(x \in B$ és $x \in C) \Leftrightarrow (x \in A$ vagy $x \in B)$ és $(x \in A$ vagy $x \in C) \Leftrightarrow x \in (A \cup B)$ és $x \in (A \cup C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$.
(2) $x \in A \cap (B \cup C) \Leftrightarrow x \in A$ és $x \in (B \cup C) \Leftrightarrow x \in A$ és $(x \in B$ vagy $x \in C) \Leftrightarrow (x \in A$ és $x \in B)$ vagy $(x \in A$ és $x \in C) \Leftrightarrow x \in (A \cap B)$ vagy $x \in (A \cap C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$.

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

Állítás:

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

Bizonyítás:

(1) $x \in (A \cup B)' \Leftrightarrow x \notin (A \cup B) \Leftrightarrow x \notin A$ és $x \notin B \Leftrightarrow x \in A'$ 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 a binér relációk kompozíciója asszociatív.

Állítás:

Legyenek A,B,C,D,E,F adott halmazok, $f \subset A \times B$, $g \subset C \times D$, $h \subset E \times F$, ekkor $f \circ (g \circ h) = (f \circ g) \circ h$ fennáll.

Bizonyítás:

$(x,y) \in f \circ (g \circ h) \Leftrightarrow \exists z \in \mathbf{D}g \cap \mathbf{R}h \supset \mathbf{D}f \cap g \cap \mathbf{R}h$ úgy, hogy $(x,z) \in h$ és $(z,y) \in f \circ g \Leftrightarrow \exists z \in \mathbf{D}g \cap \mathbf{R}h$ úgy,hogy $(x,z) \in h$ és $\exists u \in \mathbf{D}f \cap \mathbf{R}g$ úgy, hogy $(z,u) \in g$ és $(u,y) \in f \Leftrightarrow$ ha $\exists u \in \mathbf{D}f \cap \mathbf{R}g \supset \mathbf{D}f \cap \mathbf{R}g \circ h$ úgy, hogy $(x,u) \in g \circ h$ és $(u,y) \in f \Leftrightarrow$ ha $(x,y) \in (f \circ g) \circ h$.

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

Állítás:

Legyenek A,B,C,D adott halmazok, $f \subset A \times B$, $g \subset C \times D$, ekkor $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ fennáll.

Bizonyítás:

$(x,y) \in (f \circ g)^{-1} \Leftrightarrow (y,x) \in f \circ g \Leftrightarrow \exists z \in \mathbf{D}f \cap \mathbf{R}g$ úgy, hogy $(y,z) \in g$ és $(z,x) \in f \Leftrightarrow \exists z \in \mathbf{R}f^{-1} \cap \mathbf{D}g^{-1}$ úgy, hogy $(z,y) \in g^{-1}$ és $(x,z) \in f^{-1} \Leftrightarrow (x,y) \in g^{-1} \circ f^{-1}$.

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

Állítás:

X egy halmaz $\sim \subseteq X \times X$ egy ekvivalenciareláció. Ekkor $\mathcal{O} = \{\tilde{x} \mid x \in X\}$ az X osztályozását adják, ahol $\tilde{x} = \{y \in X \mid y \sim x\}$. Fordítva, ha $\mathcal{O}$ egy osztályozás, akkor az $\cup\{Y \times Y \mid Y \in \mathcal{O}\}$ egy ekvivalenciareláció. Továbbá egy ekvivalenciaosztályhoz tartozó osztályhoz tartozó ekvivalenciareláció az az eredeti ekvivalenciareláció (és fordítva).

Bizonyítás:

Legyen $\sim$ egy X-beli ekvivalenciareláció, és legyen $\tilde{x} = \{y \in X \mid y \sim x\}$ az X halmaz x eleme segítségével definiált részhalmaza. Megmutatjuk, hogy az $\tilde{X} = \tilde{x} : x \in X\}$ halmaz az X egy osztályozása.

Mivel $\sim$ reflexív, $\tilde{x} \ni x$, vagyis az $\tilde{x}$ részhalmaz nem ürés, 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 ekvivalenciarelációk metszete ürés. Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme. Ekkor $z \sim x$ és $z \sim y$, amiből a szimmetria és a tranzitivitás miatt $x \sim y$. 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 tehat, 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 $\mathcal{O}$ az X egy osztályozása. Legyen $R \cup \{Y \times Y : Y \in \mathcal{O}\}$. Nyilván $(x,y) \in \mathbb{R}$ pontosan akkor teljesül, ha x és y az $\mathcal{O}$ ugyanazon halmazának elemei. Ez az R nyilván reflexív, szimmetrikus és mivel az osztályok páronként diszjunktak, tranzitív is, tehát ekvivalenciareláció. Az is nyilvánvaló, hogy ha egy osztályozásból képezzük a hozzá tartozó ekvivalenciarelációt, majd ebből a megfelelő ekvivalenciaosztályokat, akkor az eredeti osztályozást kapjuk vissza, és fordítva, ha egy ekvivalenciarelációból képezzük a fentiek szerint hozzá tartozó osztályozást, majd abból a hozzá tartozó ekvivalenciarelációt, akkor az eredeti relációt kapjuk vissza.

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

Állítás:

Ha R részbenrendezés és S szigorú részbenrendezés az A halmazon, akkor:

(1) R\Ix szigorú részbenrendezés,

(2) S∪Ix részbenrendezés, és

(3) S=R\Ix pontosan akkor, ha S∪Ix=R.

Bizonyítás:

(1) R\Ix nyilván irreflexív. Ha (a,b)∈R\Ix, akkor a≠b, amiből a R antiszimmetriája miatt (b,a)∉R. Ezért (b,a)∉R\Ix, amiből a szigorú antiszimmetria adódik. Tegyük most fel, hogy (a,b),(b,c)∈R\Ix. Ekkor R tranzitivitásából (a,c)∈R. Mivel R\Ix szigorúan antiszimmetrikus, ezért c≠a, így (a,c)∈R\Ix. Ezzel R\Ix tranzitivitását is bebizonyítottuk.

(2) S∪Ix reflexivitása a diagonális reláció (Ix) definíciójából következik. Ha (a,b)∈S, akkor (b,a)∉S. Vagyis (a,b),(b,a)∈S∪Ix csak akkor lehetséges, ha (a,b),(b,a)∈Ix. Ez pedig S∪Ix antiszimmetriáját jelenti. Tegyük fel, hogy (a,b),(b,c)∈S∪Ix. Ha (a,b),(b,c)∈S, akkor a tranzitivitás miatt (a,c)∈S. Ha egyikük S-nek eleme, a másik pedig Ix-beli, akkor (a,c) megegyezik (a,b) és (b,c) valamelyikével, és így ugyancsak S-beli. Amennyiben pedig (a,b),(b,c)∈Ix, akkor (a,c) is az. Vagyis mindig (a,c)∈S∪Ix-nak, ami bizonyítja a tranzitivitást.

(3) következik (1)-ből és (2)-ből.

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

Állítás:

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

Bizonyítás:

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 f(x)≥f(y), de f(x)≠f(y), azaz u=f(x)>f(y)=v következne. A másik eset hasonlóan bizonyítható.

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

Állítás:

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

Bizonyítás:

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 következne.

11. Fogalmazza meg a halmazcsaládokra vonatkozó De Morgan-szabályokat, és bizonyítsa be őket.

Állítás:

Ha Xi, i∈I az X halmaz részhalmazainak egy nem üres családja (azaz I≠∅), akkor az X-re vonatkozó komplementert vesszővel jelölve,

1. (∪i∈IXi)'=∩i∈IXi';
2. (∩i∈IXi)'=∪i∈IXi'.

Bizonyítás:

1. x∈(∩i∈IXi)' ⇔ x∉(∩i∈IXi) ⇔ ∃i∈I:x∉Xi ⇔ ∃i∈I:x∈Xi' ⇔ x∈∪i∈IXi';
2. x∈(∪i∈IXi)' ⇔ x∉(∪i∈IXi) ⇔ ∀i∈I:x∉Xi ⇔ ∀i∈I:x∈Xi' ⇔ x∈∩i∈IXi'.

12. Bizonyítsa be, hogy a természetes számok halmaza a ≤ relációval rendezett.

Állítás:

A természetes számok halmaza a ≤ relációval rendezett.

Bizonyítás:

Nyilvánvaló, hogy £ reflexív és tranzitív. Megmutatjuk, hogy antiszimmetrikus. Ha m£ n és n£ m, akkor n=m+x és m=n+y valamely x,y∈ℕ-re. De ebből n+0=n=m+x=(n+y)+x=n+(y+x). Az egyszerűsítési szabály szerint y+x=0. Ha x¹ 0, az összeg definíciója szerint rákövetkezője valaminek, így nem lehet 0. Tehát x=0. Innen m=n.

Meg kell meg mutatnunk, ℕ bármely két eleme összehasonlítható. Jelölje S(n) azon elemek halmazat, amelyek egy adott n∈ℕ-nél összehasonlíthatok, S pedig azon n∈ℕ-ek halmazat, amelyekre S(n)=ℕ. Azt kell megmutatnunk, hogy S=ℕ. Először megmutatjuk, hogy S(0)=ℕ, azaz 0∈S. Valóban m=0+m, így 0≤ m minden ℕ-re. Most feltéve, hogy S(n)=ℕ megmutatjuk, hogy S(n^+)=ℕ. Legyen m∈ℕ, ha m≤ n, akkor n=m+k, így n^+=m+k^+, tehát m£ n^+, azaz mÎS(n^+). Ha m>n, akkor m=n+k valamely egyértelműsítési szabály szerint meghatározott k∈ℕ-re, amelyre k≠0.Legyen k=j^+, akkor m=n+k=n+j^+=n^++j, így m≥ n^+. Ezzel beláttuk, hogy S(n^+)=ℕ, így ha n∈S, akkor n^+∈S. Indukcióval kapjuk, hogy S=ℕ.

13. Fogalmazza meg es bizonyítsa be a maradékos osztás tételét.

Állítás:

Legyen n>0 természetes szám. Minden m természetes szám egyértelműen felírható m=qn+r alakban, ahol q,r∈ℕ es r<n.

Bizonyítás:

Mivel kn≥k, van olyan k, amelyre kn>m, például k=m^+. Legyen k a legkisebb természetes szám, amelyre kn>m. Nyilván k≠0, így k=q+ valamely q∈ℕ-re. Mivel qn≤m, van olyan r természetes szám, amelyre m=qn+r. Ha r≥n lenne, akkor m≥qn+n=kn>m adódna. Az egyértelműség bizonyításához tegyük fel, hogy m=q'n+r', ahol r'<n. Ha például q'>q, akkor m=q'n+r'≥q'n≥(q+1)n>qn+r=m, ellentmondás, es hasonlóan q'<1 is ellentmondásra vezet. Így q=q', amiből már r=r' következik.

14. Fogalmazza meg es bizonyítsa be a számrendszerekre vonatkozó tételt.

Állítás:

Legyen q>1 természetes szám. Minden m>0 természetes számhoz egy es csak egy olyan n természetes szám és $a_0,a_1,...a_n$∈[0,q[⊂ℕ sorozat létezik, amelyre a_n≠0 es m = $\sum_{i=0}^{n} a_i \cdot q^i$.

Bizonyítás:

Teljes indukcióval bizonyítunk: feltesszük, hogy 0<m'<m eseten igaz az állítás, és bebizonyítjuk, hogy m-re is. Ebből következik, hogy az álltás minden pozitív természetes számra teljesül. Osszuk maradékosan m-et q-val, azaz írjuk fel m=m'+r alakban, ahol m',r∈ℕ és r<q. Ha m'=0, akkor n=0, a_0=r választással készen is vagyunk (az egyértelműség a maradékos osztás egyértelműségéből következik). Ha m'≠0, akkor m'<m, és az indukciós feltevés szerint egyértelműen felírható m'=a_1+a_2q+...+$a_{n+1}q^n$ alakban. A maradékos osztás egyértelműségéből következik a_0 egyértelműsége, és teljes indukcióval az állítás.

15. Definiálja a bal es jobb oldali nullosztó es nullosztópár fogalmat. Adjon meg két lényegesen különböző, nullosztókkal kapcsolatos állítást, es bizonyítsa be őket.

Állítás:

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. (Egy legalább kételemű gyűrűt nullosztómentesnek nevezünk, ha nincsenek benne nullosztópárok.)

(1) Nullosztómentes gyűrűben nem nulla elemmel való szorzásnál lehet balról is, jobbról is egyszerűsíteni.

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

Bizonyítás:

(1) Ha xy=xz és x≠0. akkor x(y-z)=0, és ha x≠0 így y-z=0, tehát y=z. Hasonlóan adódik, hogy ha yx=zx és x≠0, akkor y=z. Az nyilvánvaló, hogy ha van nullosztópár, akkor a bal oldali nullosztóval balról, ja jobb oldali nullosztóval jobbról nem lehet egyszerűsíteni.

(2) Mivel xy=0-ból illetve xy=0-ból $x^{-1}xy=y=0$ illetve $yxx^{-1}=y=0$ következik.

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

Állítás:

Segéd def.:

Definiálja a rendezett integritási tartomány fogalmat. Az R-et rendezett integritási tartománynak nevezzük, ha rendezett halmaz, integritási tartomány, és

(1) ha x,y,z∈R és x≤y, akkor x+z≤y+z (az összeadás monoton);

(2) ha x,y∈R és x,y≥0, akkor x·y≥0 (a szorzás monoton).

Rendezett integritási tartományban ha x>0, akkor x-et pozitívnak, ha x<0, akkor x-et negatívnak nevezzük. Az egész számok tulajdonságait röviden úgy foglalhatjuk össze, hogy ℤ rendezett integritási tartomány.

Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fennállnak:

(1') ha x,y,z∈R es x<y, akkor x+z<y+z (az összeadás szigorúan monoton);

(2') ha x,y∈R es x,y>0, akkor x·y>0 (a szorzás szigorúan monoton).

Bizonyítás:

Ha a definícióból (1) teljesül, x<y, akkor x≤y és így x+z≤y+z, de egyenlőség nem teljesülhet, mert akkor x=x+z-z=y+z-z=y következne, így kapjuk (1')-t. (1')-ből nyilván következik (1), mert az egyenlőség esete triviális.

Ha a definícióból (2) teljesül és x,y>0, akkor x,y≥0, így xy≥0. Ha xy=0 lenne, akkor x és y egy nullosztópár lenne, ami lehetetlen, így kapjuk (2')-t. (2')-ből nyilván következik (2), mert gyűrűben x0=0y=0.

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

Állítás:

Legyen R rendezett integritási tartomány. Ekkor teljesülnek a szokásos „egyenlőtlenségekkel való számolási szabályok”:

1. *ha $x>0$, akkor $-x<0$, és ha $x<0$, akkor $-x>0$;*
2. *ha $x<y$ és $z>0$, akkor $xz<yz$;*
3. *ha $x<y$ és $z<0$, akkor $xz>yz$;*
4. *ha $x\neq 0$, akkor $x^2>0$; speciálisan, ha van egységelem, akkor az pozitív;*
5. *ha 1 az egységelem, $0<x<y$,és x-nek is, y-nak is van multiplikatív inverze, akkor $0<1/y<1/x$.*

Bizonyítás:

(1) Ha $x>0$, akkor $0=-x+x>-x+0=-x$. Ha $x<0$, akkor $0=-x+x<-x+0=-x$.

(2) Abból következik, hogy $y-x>x-x=0$, így $(y-x)z>0$, amiből $yz-xz>0$, így $yz>xz$.

(3) Megkapjuk (1)-ből és (2)-ből, mert $-((y-x)z)=(y-x)(-z)>0$, így $(y-x)z<0$, tehát $yz<xz$.

(4) Ha $x>0$, akkor $x^2>0$, ha viszont $x<0$, akkor $-x>0$, így $x^2=(-x)^2>0$. Speciálisan, $1^2=1>0$.

(5) Ha $y>0$ és $v\leq 0$, akkor $yv\leq 0$. De $y(1/y)=1>0$. Ezért $1/y>0$, és hasonlóan $1/x>0$. Ha az $x<y$ egyenlőtlenség mindkét oldalát megszorozzuk a pozitív $(1/x)(1/y)$-nal, akkor azt kapjuk, hogy $1/y<1/x$.

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

Állítás:

Nincs olyan racionális szám, amelynek négyzete 2.

Bizonyítás:

Ha lenne, akkor $(-m/n)2=(m/n)2$ miatt lenne olyan is, amely felírható m/n alakban, ahol $m, n\in\mathbb{N}^+$. Válasszuk azt a felírást, amelyre a számláló minimális. Mivel $m^2=2n^2$, m páros kell legyen. Legyen $m=2k$, $k\in\mathbb{N}^+$. Ekkor $4k^2=2k^2$, ahonnan $2k^2=n^2$. Innen n is páros. Ez ellentmond annak, hogy a számláló minimális.

19. Fogalmazza meg az Arkhimédészi tulajdonságot. Mi a kapcsolata a felső határ tulajdonsággal? Bizonyítsa be álltását.

Állítás:

Arkhimédészi tulajdonság:

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

Egy felső határ tulajdonságú rendezett test mindig arkhimédészien rendezett.

Bizonyítás:

Egy felső határ tulajdonságú test mindig arkhimédészi tulajdonságú is, ellenkező esetben $A=\{nx:n\in\mathbb{N}\}$-nek az y felső korlátja lenne. Legyen $z=\sup A$. Mivel $z-x<z$, a $z-x$ már nem felső korlát, így van olyan $n\in\mathbb{N}$, amelyre $nx>z-x$. De ebből $(n+1)x>z$, ami ellentmondás.

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

Állítás:

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

Bizonyítás:

Legyen $x>0$. Ha $y\leq 0$, akkor $n=0$ választással, ha pedig $x=i/j$, $y=k/m$, $i,j,k,m\in\mathbb{N}^+$, akkor $n\geq kj$ választással $nx\geq y$ így kapjuk, hogy $\mathbb{Q}$ arkhimédészien rendezett.

Legyen A az összes olyan $r>0$ racionális számok halmaza, amelyekre $r^2<2$, és legyen B az összes olyan $r>0$ racionális számok halmaza, amelyekre $r^2>2$. Legyen $s=r-\frac{r^2-2}{r+2}=\frac{2r+2}{r+2}$. Ekkor $s^2-2=\frac{2(r^2-2)}{(r+2)^2}$. Ha $r\in A$, akkor $s>r$, de $s^2<2$, azaz $s\in A$, így A-nak nincs legnagyobb eleme. Ha $r\in B$, akkor $s<r$, de $s^2>2$, azaz $s\in B$, így B-nek nincs legkisebb eleme. Innen következik, hogy A-nak nincs $\mathbb{Q}$-ban legkisebb felső korlátja: ha lenne, nem lehetne A-ban, mert akkor A legnagyobb eleme lenne, így B-nek kellene lennie, de B-nek nincs legkisebb eleme. (Hasonlóan adódik, hogy B-nek nincs legnagyobb alsó korlátja $\mathbb{Q}$-ban.)

21. Definiálja valós szám alsó, és felső egész részét, és bizonyítsa be ezek létezését.

Állítás:

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

Bizonyítás:

Ha x=0, akkor nyilvánvaló, hogy ezek léteznek (ekkor mindkettő 0). Ha x>0, az arkhimédészi rendezettségből és $\mathbb{N}$ jólrendezettségéből következik, hogy van az x-nél nagyobb vagy egyenlő természetes számok között egy legkisebb n természetes szám, ez éppen $\lceil x \rceil$. Nyilván n>0. Ha n=x, akkor $\lfloor x \rfloor = \lceil x \rceil = n$, egyébként $\lfloor x \rfloor = n-1$. Végül, ha x<0, akkor $\lceil x \rceil = -\lfloor -x \rfloor$ és $\lfloor x \rfloor = -\lceil -x \rceil$.

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

Állítás:

Bizonyítás:

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

Állítás:

Bizonyítás:

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

Állítás:

Ha n természetes szám, akkor nem létezik ekvivalencia {1,2,…,n} és egy valódi részhalmaza között.

Bizonyítás:

Indukcióval bizonyítjuk: 0-ra az állítás világos, mert az üres halmaznak nincs valódi részhalmaza. Tegyük fel, hogy n-re teljesül, de létezik egy f kölcsönösen egyértelmű leképezése {1,2,…,n+1}-nek egy A valódi részhalmazára. Ha $n+1 \notin A$, akkor f megszorítása {1,2,…,n}-re is kölcsönösen egyértelmű leképezés, mégpedig {1,2,…,n}-nek egy valódi részhalmazára, mivel f(n+1) nem lesz az értékkészletben, ami ellentmond az indukciós feltevésnek. Ha $f(k)=n+1 \in A$, akkor viszont úgy kapjuk {1,2,…,n} és A\{n+1} egy ekvivalenciáját, hogy – hacsak nem k=n+1 – a (k,n+1) és az (n+1,l) párokat kihagyjuk a leképezésből, és helyettük a (k,l) párt vesszük be. Ez megint ellentmond az indukciós feltevésnek.

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

Állítás:

Legyen 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 $card(X \times X) = card(X) \cdot card(Y)$;*
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 $card(Y)<card(X)$.*

Bizonyítás:

1. *nyilvánvaló, ha Y=X, ha viszont $Y \subsetneq X$, akkor ekvivalens {1,2,…,card(X)} egy valódi részhalmazával, amiről tudjuk, hogy ekvivalens {1,2,…,m}-mel valamely m<n-re. Ezzel beláttuk (2)-t is.*
2. *azon múlik, hogy {1,2,…,n} ekvivalens {m+1,m+2,…,m+n}-nel. (3) szerint $card(X \cup Y) = card(X\setminus Y)+card(X \cap Y)+card(Y\setminus X)$, mindkét oldalhoz hozzáadva $card(X \cap Y)$-t, és újra felhasználva (3)-mat kapjuk (4)-et.*
3. *(6) az Y elemeinek száma szerinti indukcióval következnek, felhasználva a szorzást, és a hatványozás definícióját.*
4. *következik (6)-ból és $\wp(X)$-nek a karakterisztikus függvények halmazával való ekvivalenciájából.*
5. *bizonyításához feltehetjük, hogy $X = \{1,2,…,card(X)\}$. Minden $y \in Y$-ra legyen $g(y)$ az $f^{-1}(y)$ halmaz legkisebb eleme. Ekkor g az Y-t kölcsönösen egyértelműen képezi le X egy részhalmazára, 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 $card(X) > card(Y)$, akkor egy $f: X \to Y$ leképezés nem lehet kölcsönösen egyértelmű.

Bizonyítás:

Egyébként {1,2,…,card(Y)} egy részhalmaza azaz $card(Y) < card(X)$ miatt {1,2,…,card(X)} egy valódi részhalmaza ekvivalens lenne {1,2,…,card(X)}-el.

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

Állítás:

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

Bizonyítás:

A részhalmaz elemeinek száma szerinti indukcióval: Ha card(A)=1, akkor nyilvánvaló. Ha $card(A) = n+1$, legyen $a \in A$ és $A'=A\setminus\{a\}$. Ha a nem nagyobb, mint A' (egy adott) a' maximális eleme, akkor az a' maximális elem, egyébként a maximális elem. Minimális elemre a bizonyítás hasonló.

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

Állítás:

Egy A halmaz permutációinak száma csak n=card(A)-tól függ. Ez a szám a P_n.

Bizonyítás:

Meg akarjuk határozni véges halmazok permutációinak számát. Ha egy A halmaz ekvivalens {1,2,…,n}-nel, akkor tudjuk, hogy permutációinak halmaza ekvivalens {1,2,…,n} permutációinak halmazával. Ha $A=\{a_1,a_2,…,a_n\}$ és $p_1,p_2,…,p_n$ az {1,2,…,n} egy permutációja, akkor az A megfelelő permutációja az $a_i \mapsto a_{pi}$ leképezés (az $a_i \mapsto i, i \mapsto p_i$, $j \mapsto a_j$ leképezések összetétele). Így A permutációinak száma csak n=card(A)-tól függ. Ez a szám a P_n.

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

Állítás:

Legyen A egy halmaz. Az A elemeiből képezhető $a_1,a_2,\dots,a_k$ sorozatot (vagyis $\{1,2,\dots,k\} \to A$ függvényeket) A k-ad osztályú ismétléses variációinak hívjuk. Ha kikötjük, hogy a sorozat elemei különbözők, akkor ismétlés nélküli variáció. ($\{1,2,\dots,k\} \to A$ injektív).

Ezek száma csak |A|-tól függ.

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

Bizonyítás:

2 permutációt tekintsünk ekvivalensnek, ha {1,2,…,k}-n megegyeznek.

Ekvivalens osztályok száma: V_n^k
Ekvivalens osztályok mérete: P_{n-k}
Összes osztály mérete: P_n

$$V_n^k \cdot P_{n-k} = P_n$$

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

Állítás:

A halmaz k-ad elemű részhalmazait az A k-ad osztályú kombinációinak hívjuk. Ha A n elemű, akkor |A|=n, ezek száma C_n^k

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

Bizonyítás:

Két variáció legyen ekvivalens, ha az értékkészletük ugyanaz. (pl.: ACDF ~ FDCA)

Ekvivalens osztályok száma: C_n^k
Ekvivalens osztályok mérete: $k!$
Összes osztály mérete: V_n^k

$$V_n^k = C_n^k \cdot k!$$

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

Állítás:

A halmaz k-ad osztályú ismétléses kombinációja: f: A→ℕ, melyre: $\sum_{a\in A} f(a) = k$

$C_n^{k,i}$ *legyen az n elem k-ad osztályú ismétléses kombinációk száma.*

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

Bizonyítás:

Az kell, hogy a g:{1,2,…,k}→{1,2,…,n} monoton növekvő függvények száma.

h:{1,2,…,k}→{1,2,…,n+k-1} szigorúan monoton függvények száma.

Megfeleltetés: Ha g adott. Legyen h(i)=g(i)+i-1 bijekció a lehetséges g-k és k-k között.

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

Állítás:

Legyen $r,i_1,i_2,\dots,i_r\in\mathbb{N}$. Ekkor az $a_1,a_2,\dots,a_r$ elemek egy $i_1,i_2,\dots,i_r$ ismétlődésű ismétléses permutációja egy olyan $n=i_1+i_2+\dots+i_r$ hosszú sorozat, melyben a_j pontosan i_j-szer fordul elő. Számuk: $P_n^{i_1,i_2,\dots i_r}$

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

Bizonyítás:

r szerinti indukció. r=0, 1 könnyen látható. r≥2 esetén soroljuk most ekvivalencia osztályokba azokat az ismétléses permutációkat, melyekből törölve a_i-k ugyanazt az $(n\text{-}i_1)$ hosszú sorozatot kapjuk.

Ekvivalencia osztályok száma: $P_{n-i_n}^{i_2,i_3,\dots i_r}$ (indukciós feltevés).

Ekvivalencia osztályok mérete: Hányféleképpen lehet i1 db a1-et beszúrni n-i1+1 helyre ismétléssel?

$$C_{n-i_1+1}^{i_1,i}=\binom{n-i_1+1+i_1-1}{i_1}=\binom{n}{i_1}$$

Összméret: $P_n^{i_1,i_2,\dots,i_r}$

Tehát $P_n^{i_1,i_2,\dots,i_r}=P_{n-i_1}^{i_2,i_3,\dots,i_r}\cdot\binom{n}{i_1}$ …… számolás…

33. Fogalmazza meg a binomiális tételt és bizonyítsa be.

Állítás:

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

Bizonyítás:

Indukcióval: n=0,1-re az állítás nyilvánvaló. Ha n-re teljesül, akkor a disztributivitást felhasználva: $(x+y)^{n+1}=(x+y)\sum_{k=0}^n\binom{n}{k}x^ky^{n-k}=\sum_{k=0}^n\binom{n}{k}(x^{k+1}y^{n-k}+x^ky^{n-k+1})$, 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.

34. Fogalmazza meg a polinomiális tételt és bizonyítsa be.

Állítás:

Legyen $r\in\mathbb{N}$, x1,x2,…,xr egy R kommutatív egységelemes gyűrű elemei, $n\in\mathbb{N}$. Ekkor $(x_1+x_2+\dots++x_r)^n=\sum_{\substack{i_1+i_2+\dots+i_r=n\\ i_1,i_2,\dots,i_r\in\mathbb{N}}}P_n^{i_1+i_2+\dots+i_r}\,{x_1}^{i_1}{x_2}^{i_2}\cdot\dots\cdot{x_r}^{i_r}$. Ha gyűrű nem egységelemes, akkor is igaz az állítás $n,r\in\mathbb{N}^+$, $i_1,i_2,\dots,i_r\in\mathbb{N}$ esetén, ha a formailag szereplő, de nem létező nulladik hatványokat egyszerűen kihagyjuk.

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,

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

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

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

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

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

Állítás:

Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X-en értelmezett, értékeket egy Abel-csoportban felvevő függvény.

Ha $1 \le i_1 < i_2 < \dots < i_r \le k$, akkor legyen

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

Legyen továbbá

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

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

és legyen

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

Ekkor

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

Bizonyítás:

Ha $x \in X | \cup_{i=1}^{k} X_i$, akkor f(x) mindkét oldalon egyszer szerepel, a jobb oldalon csak S-ben. Egyébként legyenek $X_{j_1}, X_{j_2}, \dots, X_{j_t}$, azok a részhalmazok, amelyek tartalmazzák x-et. A bal oldalon f(x) nem szerepel. A jobb oldalon valamely $\sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} f(x)$ összegben f(x) pontosan akkor lép fel, ha $\{i_1,i_2,\dots i_r\} \subset \{j_1,j_2,\dots,j_t\}$. Ha $r > t$, akkor nincs ilyen $\{i_1,i_2,\dots,i_r\}$. Ha $r \le t$, akkor pontosan $\binom{t}{r}$ ilyen $\{i_1,i_2,\dots,i_r\}$ van, így a jobb oldalon f(x) együtthatója $\sum_{r=0}^{t} \binom{t}{r} (-1)^r = 0$.

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

Állítás:

Az oszthatóság tulajdonságai $\mathbb{N}$-ben. 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 az osztója;
(4) az 1 minden természetes számnak osztója;
(5) ha $m|n$, akkor $mk|nk$ minden $k \in \mathbb{N}$-re;
(6) ha $k \in \mathbb{N}^+$ és $mk|nk$, akkor $m|n$;
(7) ha $m|n_i$ és $k_i \in \mathbb{N}$, $(i=1,2,\dots,j)$, akkor $m|\sum_{i=1}^{j} k_i n_i$;
(8) bármely nem nulla természetes szám osztója kisebb vagy egyenlő, mint a szám;
(9) az $|$ 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.

Állítás:

Egy egységelemes integritási tartomány elemei körében

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

Bizonyítás:

A bizonyítások a definíció alapján triviálisak.

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

Állítás:

Egy elem asszociáltjait leírhatjuk az 1 asszociáltjai segítségével, amelyek nem mások, mint 1 osztói, hiszen 1 bárminek osztója; ezeket egységeknek nevezzük. Az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük. (Így egy egységelemes integritási tartomány pontosan akkor test, ha minden nem nulla eleme egység.)

Bizonyítás:

Az egységek a szorzatra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját. Az egységek bármely $a \in R$-nek osztói mert $a = 1a$-nak osztói. Megfordítva nyilvánvaló: ha egy elem minden $a \in R$-nek osztója, akkor egység. Az egységeket ezzel a tulajdonsággal tetszőleges $R \neq \{0\}$ integritási tartományban is lehet definiálni, de könnyen adódik, hogy ha van egység, akkor R egységelemes: ha ε egy egység, akkor $\varepsilon \mid \varepsilon$, így valamely $0 \neq e \in \mathbb{R}$-re $\varepsilon = e\varepsilon$. Innen $a\varepsilon = ae\varepsilon$ minden $a \in \mathbb{R}$-re. Mivel $\varepsilon \neq 0$, lehet vele egyszerűsíteni. 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 a triviális osztói.

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

Állítás:

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

(1) [Inicializálás.] Legyen $x_0 \leftarrow 1$, $y_0 \leftarrow 0$, $r0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow 1$, $r_1 \leftarrow b$, $n \leftarrow 0$.
(2) [Vége?] Ha $r_{n+1}=0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ér.
(3) [Ciklus.] Legyen $q_{n+1} \leftarrow \lfloor r_n / r_{n+1} \rfloor$, $r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1}$, $x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1}$, $y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1}$, $n \leftarrow n+1$ és menjünk (2)-re.

Bizonyítás:

Az |r1|, |r2|,… természetes számok – mivel r_{n+2} az r_{n+1}-gyel való osztás maradéka – szigorúan monoton csökkenő sorozatot alkotnak, így az eljárás véges sok lépésben véget ér, mert egyébként $\mathbb{N}$ nem lenne jólrendezett. Indukcióval, ha $ax_n+by_n=r_n$ és $ax_{n+1}+by_{n+1}=r_{n+1}$, akkor a második összefüggést szorozva q_{n+1}-gyel és kivonva az elsőből, $ax_{n+2}+by_{n+2}=r_{n+2}$, így végül $d=ax+by$. Innen a és b közös osztói mind osztói d-nek. Kilépéskor $r_{n+1}=0$, és két eset van: Ha n=0, akkor $d=a$ és $b=0$. Ha $n>0$, akkor $r_0, r_1, \ldots, r_{n-1}$ mind többszörösei r_n=d-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 $b=r_1$ is többszörösei d-nek. Így d egy legnagyobb közös osztó.

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

Állítás:

A $\mathbb{Z}$ egy eleme pontosan akkor felbonthatatlan, ha prímelem.

Bizonyítás:

Azt már beláttuk, hogy prímelem felbonthatatlan. Tegyük fel, hogy p felbonthatatlan, és legyen $p|mn$. Tegyük fel, hogy $p\nmid m$. 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 egyszerűen felírható prímszámok szorzataként.

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 helyettesítsük 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 egyértelműségének bizonyításához tegyük fel indirekt, hogy van olyan természetes szám, amely két lényegesen különböző módon bontható fel, és legyen ne a legkisebb ilyen: $n=p_1p_2\cdot\ldots\cdot p_j=q_1q_2\cdot\ldots\cdot q_k$

42. Fogalmazza meg Eukleidész tételét, és bizonyítsa be.

Állítás:

Végtelen sok prímszám van.

Bizonyítás:

Mutatunk egy módszert újabb és újabb prímek előállítására:

Ha ismerünk n különböző prímet, $p_1,p_2,\ldots,p_n$-t, akkor legyen $X=p_1p_2\cdot\ldots\cdot p_{n+1}$. X prímfelbontásában milyen prímek vannak? Biztos nincs benne $p_1,p_2,\ldots,p_n$, mert ezekre $p_i|x-1 \Longrightarrow p_i \nmid x$.

43. Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait és bizonyítsa be azokat.

Állítás:

Ha $a,b,m\in\mathbb{Z}$ és m osztója a-b-nek, akkor azt mondjuk, hogy a és b kongruensek modulo m; ezt úgy jelöljük, hogy $a \equiv b \pmod m$. Ha a és b nem kongruensek modulo m, akkor azt mondjuk, hogy inkongruensek modulo m, és azt írjuk, hogy $a \not\equiv b \pmod m$. Vagy rövidebben: $a\equiv b\ (m)$, illetve $a \not\equiv b\ (m)$. Nyilván, ha $a \equiv b \pmod m$ és $d \mid m$, akkor $a \equiv b \pmod d$ is teljesül. Ha $0 \neq d \in \mathbb{Z}$, akkor $a \equiv b \pmod m$ ekvivalens azzal, hogy $ad \equiv bd \pmod{md}$.

Bizonyítás:

Az oszthatóság tulajdonságából azonnal következik, hogy bármely adott $m \in \mathbb{Z}$-re a kongruencia ekvivalenciareláció $\mathbb{Z}$-ben. Az m és a –m szerinti kongruencia ugyanazt jelenti, így legtőbbször feltesszük, hogy $m \in \mathbb{N}$. Ha $a \in \mathbb{Z}$, akkor az ekvivalencia osztálynak elemei az $a+km$, $k \in \mathbb{Z}$ alakú egészek; valóban, ezek nyilván kongruensek a-val, és ha $a' \equiv a \pmod m$, akkor $a' - a = km$ valamely $k \in \mathbb{Z}$-re. Az, hogy $a' \equiv a \pmod m$, pontosan akkor teljesül, ha $a' = a + km$, akkor $\lfloor a'/m \rfloor = \lfloor a/m \rfloor + k$, ahonnan $a' \bmod m = a \bmod m$ következik, és megfordítva, ha $m' \bmod m = a \bmod m$, akkor $a' - a' - \lfloor a'/m \rfloor m = a - \lfloor a/m \rfloor m$, ahonnan $k = \lfloor a'/m \rfloor - \lfloor a/m \rfloor$-szel $a' = a + km$.

Megjegyezzük, hogy ha $a' \equiv a \pmod m$, akkor $lnko(a,m) = lnko(a',m)$, mert $a' = a + km$, illetve $a = a' - km$ miatt a' és m közös osztói osztói a-nak is és megfordítva, a és m közös osztói osztói a'-nek is.

44. Fogalmazza meg a $\mathbb{Z}_m$ gyűrű tulajdonságait leíró tételt és bizonyítsa be.

Állítás:

Bizonyítás:

45. Mit mondhatunk az aa_j+b számokról, ha a_j 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 $aa_i+b\equiv aa_j+b \pmod m$ teljesülne, akkor ebből $aa_i\equiv aa_j \pmod m$, és innen a multiplikatív inverzével szorozva $a_i\equiv a_j \pmod m$ 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 $\text{lnko}(aa_i,m)>1$, akkor $\text{lnko}(a_i,m)>1$. Így az aa_i, $i=1,2,\dots,\varphi(m)$ számuk 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 $a^{\varphi(m)}\equiv 1 \pmod m$.

Bizonyítás:

Legyen $a_1,a_2,\dots,a_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Ekkor $aa_1,aa_2,\dots,aa_{\varphi(m)}$ is redukált maradékrendszer modulo m. Innen

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

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

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

Állítás:

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

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 kövétezik, ha pedig $p\mid a$, akkor mindkét oldal osztható p-vel.

48. Ismertesse a lineáris kongruenciák megoldásának módszerét részletes indoklással.

Állítás:

Legyen $m>1$ egész szám, $a,b\in\mathbb{Z}$ adottak. Keressük az $ax\equiv b \pmod m$ kongruencia megoldásait. A probléma nyilván azzal ekvivalens, hogy találjunk olyan x egész számot, amelyre valamely y egész számmal $ax+my = b$ teljesül. (Ha x-et megtaláljuk, y már adódik.)

Bizonyítás:

Legyen $d=\text{lnko}(a,m)$. 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 $a',b',m'\in\mathbb{Z}$-re. Azt kapjuk, hogy az egyenletünk az $a'x+m'y=b'$, illetve az $a'x\equiv b' \pmod m$ 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, amelyekre $ax_0+my_0=y_0b'$. Az általános megoldáshoz vonjuk ki ezt az egyenletet az $a'x+m'y=b$ egyenletekből: $a'(x-x_1)=m'(y_1-y)$, ahonnan $m' \mid x-x_1$, azaz $x=x_1+km'$ valamely $k\in\mathbb{Z}$-re. Minden ilyen x ténylegesen megoldás, mert $y=y_1-ka'$-vel $a'x+m'y=b'$.

Összefoglalva, ha van megoldás, akkor az összes megoldás $x\equiv x_1 \pmod{m'}$ alakban adható meg. Ez a halmaz $x_1,x_1+m',\dots,x_1+(d-1)m'$ számok modulo m vett maradékosztályainak egyesítése.

49. Ismertesse a lineáris kongruencia rendszerek megoldásának módszerét részletes indoklással.

Állítás:

Ha két lineáris kongruencia adott, akkor azokat (ha megoldhatóak) $x \equiv a \pmod m$, illetve $x \equiv b \pmod n$ alakra hozhatjuk (a,b,m,n egészek, $m,n>0$).

Bizonyítás:

Mivel közös megoldásokra $x=a+my=b+nz$ valamely $y,z\in\mathbb{Z}$-re, az $my-nz=b-a$ egyenlet egész megoldásait megkeresve, minden x megoldás megtalálható. Akkor és csak akkor van megoldás, ha $d=\text{lnko}(m,n)$ osztója $b-a$-nak, és ekkor a megoldás $x\equiv x_1 \pmod{\text{lkkt}(m,n)}$ alakban írható valamely x_1 egésszel. Ha több kongruencia van, az eljárás folytatható.

50. Fogalmazza meg és bizonyítsa be a kínai maradéktételt.

Állítás:

Legyenek $m_1,m_2,\dots,m_n$ egynél nagyobb, páronként relatív prím természetes számok, $c_1,c_2,\dots,c_n\in\mathbb{Z}$. Az $x\equiv c_j \pmod{m_j}$, $j=1,2,\dots,n$ kongruenciarendszer megoldható, és bármely két megoldás kongruens modulo $m_1m_2\cdot\dots\cdot m_n$.

Bizonyítás:

Legyen $m=m_1m_2$. 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 $c_{1,2}\equiv c_j \pmod{m_j}$, ha $j=1,2$. Ha $x\equiv c_{1,2} \pmod m$, akkor x az első két kongruencia egy megoldása, és megfordítva, ha x az első két kongruencia egy megoldása, akkor $x-c_{1,2}$ osztható m_1-el és m_2-vel, tehát szorzatuk is. Az eredeti kongruenciarendszer tehát ekvivalens az $x\equiv c_{1,2} \pmod m$, $x\equiv c_j \pmod{m_j}$, $j=3,4,\dots,n$ kongruenciarendszerrel. Így n szerinti indukcióval adódik a bizonyítás.

Megjegyezzük, hogy a gyakorlatban érdemesebb $c_{1,2}$ helyett $c_{1,2} \pmod m$-et használni, és mindig azt a két kongruenciát összevonni, amelyek modulusa a legkisebb.

51. Ismertesse az RSA eljárást részletes indoklással.

Állítás:

Bizonyítás: