EÖTVÖS LORÁND TUDOMÁNYEGYETEM – INFORMATIKAI KAR

Diszkrét matematika I.

Vizsgaanyag

Készítette: Nyilas Árpád

Bizonyítások

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

(1) $A \cup B = B \cup A$ (kommutativitás)
A baloldalnak, akkor eleme x, ha $x \in A \vee x \in B$
A jobboldalnak, akkor eleme x, ha $x \in B \vee x \in A$
A két állítás ekvivalens a vagy művelet kommutativitása miatt. ■

(2) $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás)
A baloldalnak, akkor eleme x, ha $x \in A \vee (x \in B \vee x \in C)$
A baloldalnak, akkor eleme x, ha $(x \in A \vee x \in B) \vee x \in C$
A két állítás ekvivalens a vagy művelet asszociativitása miatt. ■

(3) $A \cup A = A$ (idempotencia)
Az egyenlőség mind két oldalán álló halmaznak pontosan akkor eleme x, ha $x \in A$■

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

(1) $A \cap B = B \cap A$ (kommutativitás)
A baloldalnak, akkor eleme x, ha $x \in A \wedge x \in B$
A jobboldalnak, akkor eleme x, ha $x \in B \wedge x \in A$
A két állítás ekvivalens az és művelet kommutativitása miatt. ■

(2) $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás)
A baloldalnak, akkor eleme x, ha $x \in A \wedge (x \in B \wedge x \in C)$
A baloldalnak, akkor eleme x, ha $(x \in A \wedge x \in B) \wedge x \in C$
A két állítás ekvivalens az és művelet asszociativitása miatt.■

(3) $A \cap A = A$ (idempotencia)
Az egyenlőség mind két oldalán álló halmaznak pontosan akkor eleme x, ha $x \in A$■

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

A,B,C halmazok

A metszet disztributivitása az unióra nézve

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

Az $A \cap (B \cup C)$ halmaznak x pontosan akkor eleme, ha $x \in A$ *és* $x \in B \cup C$. Ez utóbbi pontosan akkor teljesül, ha $x \in B$ vagy $x \in C$.

Így x pontosan akkor eleme az $A \cap (B \cup C)$ halmaznak , ha $x \in A$ és $x \in B$ vagy pedig $x \in A$ és $x \in C$.

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

Az unió disztributivitása a metszetre nézve

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

Az $A \cup (B \cap C)$ halmaznak x pontosan akkor eleme, ha $x \in A$ $vagy$ $x \in B \cap C$. Ez utóbbi pontosan akkor teljesül, ha $x \in B$ és $x \in C$.

Így x pontosan akkor eleme az $A \cup (B \cup C)$ halmaznak , ha $x \in A$ $vagy$ $x \in B$ vagy pedig $x \in A$ vagy $x \in C$.

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

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

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

$x \in (A \cup B)' \iff x \notin (A \cup B) \iff x \notin A$ és $x \notin B \iff x \in A'$ és $x \in B' \iff x \in A' \cap B'$

■

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

$x \in (A \cap B)' \iff x \notin (A \cap B) \iff x \notin A \; vagy \; x \notin B \iff x \in A' \; vagy \; x \in B' \iff x \in A' \cup B'$

■

5) Bizonyítsa be, hogy binér relációk kompozíciója asszociatív.

Legyen R,S,T binér reláció.

A kompozíció definícióját felhasználva:

$$R \circ (S \circ T) = \{(x,y): \exists z \left((z,y) \in R \wedge (x,z) \in \{(x,z): \exists w((w,z) \in S \wedge (x,w) \in T)\}\right)\} =$$
$$= \{(x,y): \exists z,w((z,y) \in R \wedge (w,z) \in S \wedge (x,w) \in T)\} =$$
$$= \{(x,y): \exists w((x,w) \in T \wedge (w,y) \in R \circ S)\} = (R \circ S) \circ T$$

■

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

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

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

■

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

<u>Tétel:</u>

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

<u>Megfordítva</u>

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

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

<u>Bizonyítás:</u>

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

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

~ reflexív, így $x \in \tilde{x}$, vagyis az $\tilde{x}$ részhalmaz nem üres, és az X halmaz minden eleme bene van $\tilde{X}$ valamely elemében, pl: $\tilde{x}$ -ban.

Különböző ekvivalencia osztályok metszete üres:

Ha $\tilde{x} \cap \tilde{y} \neq \emptyset$, akkor legyen z a metszet egy eleme.
Ekkor $z \sim x \wedge z \sim y$, ebből a tranzitivitás és a szimmetria miatt $x \sim y$

Így a tranzitivitás miatt $w \in \tilde{x} \Rightarrow w \in \tilde{y}$
Továbbá a tranzitivitás és a szimmetria miatt $w \in \tilde{y} \Rightarrow w \in \tilde{x}$
Tehát $\tilde{x} = \tilde{y}$, azaz $\tilde{x}$ részhalmazok diszjunktak,

ezért valóban az X egy osztályozását kapjuk

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

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

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

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

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

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

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

A tranzitivitásból és az irreflexivitásból következik a szigorú antiszimmetria: $x < y$ *esetén* $y > x$ *nem teljesülhet*, mert ebből $x < x$ következne.

Megfordítva

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

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

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

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

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

Bizonyítás

f(X)-en:

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

■

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

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

Bizonyítás

f(X)-en:

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

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

■

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

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

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

■

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

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

■

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

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

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

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

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

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

Indirekt bizonyítás

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

■

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

Legyen $n > 0$ rögzített természetes szám.

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

Bizonyítás

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

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

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

Egyértelműség bizonyítása

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

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

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

■

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

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

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

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

Bizonyítás:

Osszuk maradékosan m-et q-val

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

Teljes indukció:

kezdő lépés

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

Indukciós lépés

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

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

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

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

■

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

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

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

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

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

■

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

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

■

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

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

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

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

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

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

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

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

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

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

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

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

(2) ha $x < y$ *és* $z > 0, \ akkor\ xz < yz$

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

(3) ha $x < y$ *és* $z < 0, \ akkor\ xz > yz$

(1) és (2)– ből: $-\big((y - x)z\big) = \ (y - x)(-z) > 0$, így $(y - x)z < 0$, tehát $yz < xz.$

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

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

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

Ha $y > 0$ *és* $v \leq 0\ akkor\ yv \leq 0$. De $y \cdot \frac{1}{y} = 1 > 0$. Ezért $\frac{1}{y} > \ 0$, és hasonlóan $\frac{1}{x} > \ 0$

Ha az $x < y$ egyenlőtlenség mindkét oldalát megszorozzuk a pozitív $\frac{1}{x} \cdot \frac{1}{y}$ –nal, akkor azt kapjuk, hogy $\frac{1}{y} < \frac{1}{x}$.

■

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

Nincs, hisz 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, hogy legyen. Legyen $m = 2k, k \in \mathbb{N}^+$. 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 arkhimédészi tulajdonságot. Mi a kapcsolata a felső határ tulajdonsággal? Bizonyítsa be állítását.

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

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

Egy felső határ tulajdonságú rendezett test mindig arkhimédészien rendezett.

Indirekt Bizonyítás:

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

Legyen $z = \sup A$

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

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

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

SZÜRKÍTÉS

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

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

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

Ekkor

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

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

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

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

■

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

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

Létezés bizonyítása:

$x = 0$ eset triviális (mind kettő 0)

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

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

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

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

A komplex számok halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, azaz a valós számpárok halmaza,

az $(x, y) + (x', y) = (x + x', y + y')$ összeadással

és az $(x, y) \cdot (x', y') = (xx' - y'y, y'x + yx')$ szorzással mint műveletekkel.

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

Bizonyítás:

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

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

Legyen $z = x + iy$

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

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

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

(1)-ből következik

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

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

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

definícióból következik, hisz a négyzet gyök értéke mindig pozitív

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

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

Indukcióval:

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

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

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

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

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

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 $\rho(X)$ is véges, és $card\big(\rho(X)\big) = 2^{card(X)}$;
(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 $\{1, 2, \dots, card(X)\}$ egy valódi részhalmazával, amiről tudjuk, hogy ekvivalens $\{1, 2, \dots, m\}$ –mel valamely $m < n$ –re.
Ezzel (2) –t i beláttuk.
(3) azon múlik, hogy $\{1, \dots, n\}$ ekvivalens $\{m + 1, m + 2, \dots, m + n\}$ –nel.
(3) szerint $card(X \cup Y) = card(X \backslash Y) + card(X \cap Y) + card(Y \backslash X)$; mindkét oldalhoz hozzáadva $card(X \cap Y)$ –t, és újra felhasználva (3)-at kapjuk (4)-et.
(5) és (6) az Y elemeinek száma szerinti indukcióval következnek, felhasználva a szorzás és a hatványozás definícióját.
(7) következik (6)-ból és $\wp(X)$-nek a karakterisztikus függvények halmazával való ekvivalenciájából.

(8) bizonyításához feltehetjük, hogy $X = \{1, 2, \dots, card(X)\}$. 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 skatulya elvet és bizonyítsa be.

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

Bizonyítás: Egyébként $\{1, 2, \dots, card(Y)\}$ egy részhalmaza, azaz $card(Y) < card(X)$ miatt $\{1, 2, \dots, card(X)\}$ egy valódi részhalmaza ekvivalens lenne $\{1, 2, \dots, card(X)\}$ –el.

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

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

A részhalmaz elemeinek száma szerinti indukcióval: Ha $card(A) = 1$, akkor nyilvánvaló. Ha $card(A) = n + 1$, legyen $a \in A$ és $A' = A \backslash \{a\}$. 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 egy véges halmaz összes permutációinak számáról? Bizonyítsa be állítását.

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

Indukció:

$P_1 = 1$ teljesül.

Legyen f $és$ g két permutáció.

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

Ekvivalencia osztályok száma: n+1

Ekvivalencia osztályok mérete P_n

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

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

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

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

Legyen f $és$ g két permutáció.

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

Ekvivalencia osztályok száma: V_n^k

Ekvivalencia osztályok mérete $(n - k)!$

Össz méret P_n

Így $P_n = P_{n-k} V_n^k$

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

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

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

Legyen f és g két variáció.

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

Ekvivalencia osztályok száma: C_n^k

Ekvivalencia osztályok mérete $k!$

Össz méret V_n^k

Így $V_n^k = C_n^k k!$

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

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

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

Legyen

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

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

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

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

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

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

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

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

r=0 és 1 triviális.

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

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

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

Össz méret: $P_n^{i_1 i_2 \dots i_r}$

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

33) Fogalmazza meg a binomiális tételt és bizonyítsa be.

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

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

Bizonyítás: Indukcióval

n=0,1 re triviális

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

így csak azt kell belátni, hogy

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+k}{k+1}, \text{ ha } 0 \le k < n.$$

Ami adódik a bal oldalt közös nevezőre hozva.

34) Fogalmazza meg a polinomiális tételt.

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

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

Bizonyítás: indukcióval

r=0,r=1 trivi, r=2 binomiális tétel

Ha r-1 re teljesül akkor

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

$$(x_1 + x_2 + \cdots + x_r)^n = (x_1+y)^n = \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}y^{n-i_1} = \sum_{i_1=0}^{n}\binom{n}{i_1}x_1^{i_1}\sum_{i_2+\cdots+i_r=n-i_1}\mathrm{P}_n^{i_2,\dots,i_r}\,\mathrm{x}_2^{i_2}\cdots\mathrm{x}_r^{i_r} =$$

$$= \sum_{i_1=0}^{n}\frac{n!}{i_1!\,(n-i_1)!}x_1^{i_1}\sum_{i_2+\cdots+i_r=n-i_1}\frac{(n-i_1)!}{i_2!\cdots i_r!}\mathrm{x}_2^{i_2}\cdots\mathrm{x}_r^{i_r} = \sum_{i_1+i_2+\cdots+i_r=n}\mathrm{P}_n^{i_1,i_2,\dots,i_r}\,\mathrm{x}_1^{i_1}\mathrm{x}_2^{i_2}\cdots\mathrm{x}_r^{i_r}$$

35) Fogalmazza meg a logikai szita formulát.

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

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

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

és legyen

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

Ekkor

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

Bizonyítás:

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

Egyébként

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

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

A jobb oldalon valamely

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

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

Ha $r \le t$, 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.

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

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

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

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

$$0 = 0n$$

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

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

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

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

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

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

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

$$nk = mkl\ mivel\ nincs\ nullosztó\ k - val\ egyszerűsíthetünk\ n = ml$$

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

$$n_i = ml_i\ ekkor\ l\ legyen\ k_i r_i\ így \sum_{i=1}^{j} k_i n_i = m\sum_{i=1}^{j} k_i r_i$$

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

hisz n, így n=mk m>n esetén n<mk, egyenlőség nem teljesülhetne

(9) az oszthatóság reláció részbenrendezés

tranzitív: n|m m|kc-nek akkor n|k

reflexív: n=1n

antiszimmetrikus:n|m és m|n-nek akkor m=n (8) miatt

37) Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

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

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

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

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

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

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

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

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

(8) az oszthatóság reláció reflexív és tranzitív

Bizonyítást lásd 36)-nál

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

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

Hisz ha ε egy egység akkor $\varepsilon|\varepsilon$, így valamely $0 \neq e \in R$-re $\varepsilon = e\varepsilon$.

Innen $a\varepsilon = ae\varepsilon$ minden $a \in R$-re, mivel $\varepsilon \neq 0$,így lehet vele egyszerűsíteni, innen következik az állítás.

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

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 ugrás (2)-re.

Bizonyítás:

Az $|r_1|, |r_2|, \ldots$ természetes számok 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 közt. Bizonyítsa be állítását.

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

Bizonyítás:

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.

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

∃:

Ha n=1, a felbontás üres sorozat.

Egyébként ha n nem irreducibilis, akkor felírható két nála kisebb, de 1-nél nagyobb szám szorzataként. Indukcióval folytatjuk ezt az eljárást: ha a kapott sorozatnak van nem törzsszám tényezője, akkor a legnagyobb ilyen tényező minden előfordulását helyettesítjük két nála kisebb, de 1-nél nagyobb természetes szám szorzatával.

Az eljárás a természetes számok jólrendezése miatt véges sok lépésben csupa törzsszám tényezőből álló felbontáshoz vezet.

!: A felbontás egyértelműségének bizonyítása

Indirekt módon:

Legyen n a legkisebb nem egyértelműen felbontható szám

$$n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$$

Mivel $p_1 | n$ azaz $p_1 | q_1 q_2 \cdots q_k$ a p_1 prímtulajdonsága miatt $\exists i$, hogy $p_1 | q_i$.

Ekkor $p_1 = q_i$, mert q_i törzs szám.

Egyszerűsítve a kapott közös tényezővel egy kisebb n' számot kapunk, amelynek felbontása nem egyértelmű, ami ellent mondás a feltevés miatt.

42) Fogalmazza meg Eukleidész tételét, és bizonyítsa be.

Végtelen sok prímszám van.

Indirekt bizonyítás:

Tegyük fel, hogy csak véges sok prímszám van, $p_1, p_2, \dots, p_k$ és legyen $n = \prod_{j=1}^{k} p_j$.

Ekkor $n + 1$ minden p_j-vel osztva 1-et ad maradékként, tehát nem osztható egyetlen p_j-vel sem. Így prímtényezős felbontásban kell hogy legyen a p_j-től különböző prímszám, ami ellentmondás.

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

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

$$m | a - b \ \wedge d | m \ akkor \ d | a - b \ a \ tranzitivitás \ miatt$$

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

$$m | a - b \ \Leftrightarrow 0 \neq d \in \mathbb{Z}(md | ad - bd)$$

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

tranzitív, hisz ha $m | a - b \ \wedge m | b - c \ akkor \ m | a - c - nek$

reflexív, hisz a 0 mindennek többszöröse

szimmetrikus, hisz az $a - b$ asszociáltja $b - a$-nak

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

hisz m és –m egymás asszociáltjai

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

Legyen $m > 1$ egész. Ha $1 < lnko(a, m) < m$, akkor a maradékosztálya nullosztó $\mathbb{Z}_m$-ben.

Ha $lnko(a, m) = 1$, akkor a maradékosztályának van miltiplikatív inverze $\mathbb{Z}_m$-ben. Speciálisan, ha m prímszám, akkor $\mathbb{Z}_m$test.

Bizonyítás:

Legyen $d = lnko(a, m)$. Ha $1 < d < m$, akkor $a \cdot (m/d) = (a/d) \cdot m \equiv 0 \ (mod\ m)$, ahonnan $x = m/d$ jelöléssel $\tilde{a} \cdot \tilde{x} = \tilde{0}$, azaz $\tilde{a}$ nullosztó $\mathbb{Z}_m$ -ben.

Ha $d = 1$, akkor a bővített euklideszi algoritmussal olyan $x, y \in \mathbb{Z}$ egészeket kaphatunk, amelyekre $ax + my = 1$. Innen $ax \equiv 1 \ (mod\ m)$, azaz $\tilde{a} \cdot \tilde{x} = \tilde{1}$ miatt $\tilde{x}$ az $\tilde{a}$ inverze $\mathbb{Z}_m$ –ben.

Speciálisan, ha m prím, és $a \not\equiv 0 \ (mod\ m)$, akkor a-nak van multiplikatív inverze.

45) Mit mondhatunk az $aa_i + b$ számokról, ha a_i egy maradék rendszer, illetve egy redukált maradék rendszer elemeit futja végig. Bizonyítsa be állítását.

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

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

Bizonyítás

Ha $i \neq j$ estén $aa_i + b \equiv aa_j + b \ (mod\ m)$ teljesülne,
akkor ebből $aa_i \equiv aa_j \ (mod\ m)$, és innen a multiplikatív inverzével szorozva $a_i \equiv a_j \ (mod\ m)$ következne.

Tehát az $aa_1 + b, i = 1, 2, \dots, m$ számok páronként inkongruensek, és mivel számuk m, teljes maradék rendszert alkotnak modulo m.

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.

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

Bizonyítás

Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m.

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

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

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

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

Legyen p prímszám.

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

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

Bizonyítás

Nyilván $\varphi(p) = p - 1$, így az első alak következik a Euler Fermat-tételből.

A második, ha $p \nmid a$ esetben az első alakból következik,
ha pedig $p|a$ akkor mindkét oldal osztható p-vel.

48) Ismertesse a lineáris kongruenciák megoldásának módszerét részletes indoklással.

Legyen $m > 1$ egész szám, $a, b \in \mathbb{Z}$ adottak, keressük $ax \equiv b \ (mod\ m)$ kongruencia megoldásait.

Tehát keresünk x-et amire valamely y egész számmal teljesül: $ax + my = b$.

Legyen $d = lnko(a, m)$, így d|$ax + my$, tehát ha d ł b akkor nincs megoldás.

Tegyük fel, hogy $a = a'd, b = b'd,\ m = m'd\ valamely\ a', b', m' \in \mathbb{Z}$

Azt kapjuk, hogy egyenletünk az $a'x + m'y = b'$ ami ekvivalens $a'x \equiv b'\ (mod\ m')$, ahol a' és m' relatív prímek. A legnagyobb közös osztó kiszámítását a bővített euklideszi algoritmussal végezve, olyan x_0, y_0egészeket is kaphatunk, amelyre $ax_0 + my_0 = d$, 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 a $a'x + m'y = b'$ egyenletből: $a'(x - x_1) = m'(y_1 - y)$ ahonnan $m' | x - x_1$, azaz $x = x_1 + km$ valamely$k \in \mathbb{Z}$-re.

Minden ilyen x tényleges megoldás, mert $y = y_1 - ka'$-vel $a'x + m'y = b'$

Az összes megoldást $x \equiv x_1\ (mod\ m)$ alakban adható meg.

49) Ismertesse a lineáris kongruenciarendszerek megoldásának módszerét részletes indoklással.

Ha adott lineáris kongruencia, akkor azokat, ha megoldhatók hozzuk $x \equiv a\ (mod\ m)$, illetve $x \equiv b\ (mod\ n)$ alakra, ahol a,b,m,n egészek m,n>0.
Mivel a közös megoldásokra $x = a + my = b + nz\ valamely\ y, z \in \mathbb{Z}$-re az
$my - nz = b - a$ egyenlet egész megoldásait keresve, minden x megoldás megtalálható.
Akkor és csak akkor van megoldás, ha $lnko(m, n)$|b − a, ekkor a megoldás
$x \equiv x_1\ (mod\ lnko(m, n))$ alakban írható fel valamely $x_1$egésszel.
Ha több kongruencia van az eljárás folytatható.

50) Fogalmazza meg és bizonyítsa be a kínai maradék tételt.

Legyenek $m_1, m_2, \dots, m_n$ egynél nagyobb, páronként relatív prím természetes számok, $c_1, c_2, \dots, c_n \in Z$. Az $x \equiv c_j\ (mod\ m_j),\ \ j = 1,2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1m_2 \dots m_n$.

Bizonyítás

Legyen $m = m_1m_2$. A bővített euklideszi algoritmussal olyan x_1, x_2 egész számokat kaphatunk, amelyre $m_1x_1 + m_2x_2 = 1$
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 megoldása, és megfordítva, ha x az első két kongruencia egy megoldása, akkor $x - c_{1,2}$ osztható m_1-gyel m_2-vel, tehát a szorzatukkal is.
Az eredeti kongruenciarendszer tehát ekvivalens az $x \equiv c_{1,2}\ (mod\ m), x \equiv c_j\ (mod\ m_j), j = 3,4, \dots, n$ kongruenciarendszerrel.
Így n szerinti indukcióval adódik a bizonyítás.

51) Ismertesse az RSA eljárást részletes indoklással

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

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

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

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

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

Az üzenetet újabb hatványozással kaphatjuk vissza.

valamely k-ra $ed = k(p-1)(q-1)+1$, így

$$c^d = (m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \cdot m \equiv m\ (mod\ m)$$

Ekkor, ha $p|m$, akkor mindkét oldal nullával kongruens, ha $p \nmid m$, akkor a Fermat tétel szerint $m^{p-1} \equiv (1\ mod\ p)$.

Hasonlóan $(m^e)^d \equiv m\ (mod\ q)$

Innen a kínai maradék tétel szerint, mivel $p \neq q$ prímek $m = c^d\ mod\ n$

Így $m = c^d\ mod\ n$ módon dekódolhatjuk az üzenete.