ELTE IK - Programtervező Informatikus BSc

Záróvizsga tételek

4. Számelmélet, gráfok

Számelmélet, gráfok, kódoláselmélet

Halmazok, relációk, függvények és műveletek. Komplex számok. Leszámlálások véges halmazokon. Irányítatlan és irányított gráfok, fák, Euler-és Hamilton-gráfok, gráfok adatszerkezetei. Számelméleti alapfogalmak, oszthatóság, kongruencia, prímek. Polinomok és műveleteik, maradékos osztás.

1 Számelmélet

1.1 Halmazok

A halmaz (rendszer, osztály, összesség, ...) elemeinek gondolati burka. Egy halmazt az elemei egyértelműen meghatároznak.

Alapfogalmak

- Üres halmaz
  Az a halmaz, amelynek nincs eleme az Üres halmaz. Jele: $\emptyset$. A meghatározottsági axióma alapján ez egyértelmű
- Részhalmaz
  (x, y) rendezett pár, ha $(x, y) = (u, v) \iff x = u \wedge y = v$. Ezt a tulajdonságot halmazokkal definiáljuk:
  $$(x, y) := \{\{x\}, \{x, y\}\}$$
- Hatvány halmaz
  Ha A egy halmaz, akkor azt a halmazrendszert, melynek elemei pontosan az A halmaz részhalmazai az A hatványhalmazának mondjuk, és 2^A-val jelöljük.
  - $A = \emptyset, 2^\emptyset = \emptyset$
  - $A = \{a\}, 2^{\{a\}} = \{\emptyset, \{a\}\}$
  - $A = \{a, b\}, 2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
  - $|2^A| = 2^{|A|}$

Műveletek

- Unió
  Az A és B halmazok uniója: $A \cup B$ az a halmaz, mely pontosan az A és a B elemeit tartalmazza.
- Metszet
  Az A és B halmazok metszete: $A \cap B$ az a halmaz, mely pontosan az A és a B közös elemeit tartalmazza: $A \cap B = \{x \in A : x \in B\}$
- Diszjunkt
  Ha $A \cap B = \emptyset$, akkor A és B diszjunktak.

- Különbség
  Az A és B halmazok különbsége az $A \setminus B = \{x \in A : x \notin B\}$
- Komplementer
  Egy rögzített X alaphalmaz és $A \subseteq X$ részhalmaz esetén az A halmaz komplementere az $\overline{A} = A' = X \setminus A$
- Szimmetrikus differencia
  $A \triangle B = (A \setminus B) \cup (B \setminus A)$

Tulajdonságok

- Unió
  - $A \cup \emptyset = A$
  - $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás)
  - $A \cup B = B \cup A$ (kommutativitás)
  - $A \cup A = A$ (idempotencia)
  - $A \subseteq B \iff A \cup B = B$
- Metszet
  - $A \cap \emptyset = \emptyset$
  - $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás)
  - $A \cap B = B \cap A$ (kommutativitás)
  - $A \cap A = A$ (idempotencia)
  - $A \subseteq B \iff A \cap B = A$
- Unió és Metszet disztributivitási tulajdonságai
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Különbség
  - $A \setminus B = A \cap \overline{B}$
- Komplementer
  - $\overline{\overline{B}} = A$
  - $\overline{\emptyset} = X$
  - $\overline{X} = \emptyset$
  - $A \cap \overline{A} = \emptyset$
  - $A \cup \overline{A} = X$
  - $A \subseteq B \iff \overline{B} \subseteq \overline{A}$
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- Szimmetrikus differencia
  - $A \triangle B = (A \cup B) \setminus (B \cap A)$

1.2 Relációk, rendezések

Alapfogalmak

- Rendezett pár
  (x, y) rendezett pár, ha $(x, y) = (u, v) \iff x = u \wedge y = v$. Ezt a tulajdonságot halmazokkal definiáljuk:

$$(x, y) := \{\{x\}, \{x, y\}\}$$

- Descartes-szorzat
  X, Y halmazok Descartes-szorzata vagy direkt szorzata:
  $$X \times Y := \{(x, y) : x \in X, y \in Y\}$$
- Binér reláció
  Egy halmazt binér relációnak nevezünk, ha minden eleme rendezett pár. Ha R binér reláció és $(x, y) \in R$, akkor gyakran írjuk: xRy
- Reláció
  Ha X, Y halmazokra $R \subset X \times Y$, akkor R reláció X és Y között.
- Értelmezési tartomány
  Az R binér reláció értelmezési tartománya:
  $$\mathrm{dmn}(R) := \{x \mid \exists y : (x, y) \in R\}$$
- Érték készlet
  Az R binér reláció érték készlete:
  $$\mathrm{rng}(R) := \{y \mid \exists x : (x, y) \in R\}$$
- Inverz
  Egy R binér reláció inverze:
  $$R^{-1} := \{(a, b) : (b, a) \in R\}$$
- Halmaz képe
  Legyen R binér reláció, és A halmaz. Az A halmaz képe:
  $$R(A) := \{y \mid \exists x \in A : (x, y) \in R\}$$
- Kompozíció
  R és S binér relációk kompozíciója:
  $$R \circ S := \{(x, y) \mid \exists z : (x, z) \in S \ \wedge \ (z, y) \in R \}$$

Tulajdonságok

Az R egy X-beli binér reláció (azaz $R \subset X \times X$)

1. tranzitív
   $$\forall x, y, z : (x, y) \in R \ \wedge \ (y, z) \in R \Longrightarrow (x, z) \in R$$
2. szimmetrikus
   $$\forall x, y : (x, y) \in R \Longrightarrow (y, x) \in R$$
3. antiszimmetrikus
   $$\forall x, y : (x, y) \in R \ \wedge \ (y, x) \in R \Longrightarrow x = y$$
4. szigorúan antiszimmetrikus
   $$\forall x, y : (x, y) \in R \Longrightarrow (y, x) \notin R$$

5. reflexív

$$\forall x \in X : (x, x) \in R$$

6. irreflexív

$$\forall x \in X : (x, x) \notin R$$

7. trichotóm
   Ha minden $x, y \in X$ esetén az alábbiak közül pontosan egy teljesül
   a) $x = y$
   b) $(x, y) \in R$
   c) $(y, x) \in R$
8. dichotóm

$$\forall x, y \in X : (x, y) \in R \ \vee \ (y, x) \in R$$

   Más néven az elemek összehasonlíthatóak.

Rendezések

- Ekvivalenciareláció, osztályozás
  X halmaz, R X-beli binér reláció ekvivalenciareláció, ha
  - Reflexív
  - Tranzitív
  - Szimmetrikus

  X részhalmazainak egy $\mathcal{O}$ rendszerét osztályozásnak hívjuk, ha $\mathcal{O}$ páronként diszjunkt nemüres halmazokból álló halmazrendszer, melyre $\cup\mathcal{O} = X$

  Tétel:
  Egy ekvivalenciareláció meghatároz egy osztályozást. Fordítva: $\mathcal{O}$ osztályozásra
  $R = \cup\{Y \times Y : Y \in \mathcal{O}\}$ ekvivalenciareláció.
- Részbenrendezés
  X halmaz, R X-beli binér reláció részbenrendezés, ha
  - Reflexív
  - Tranzitív
  - Antiszimmetrikus
- Teljes rendezés
  X halmaz, R X-beli binér reláció (teljes) rendezés, ha
  - Reflexív
  - Tranzitív
  - Antiszimmetrikus
  - Dichotóm

  Magyarul ha egy részbenrendezés dichotóm (tehát minden eleme összehasonlítható), akkor (teljes) rendezés.
- Szigorú és gyenge reláció, rendezés
  X halmaz, R,S relációk X-beliek. Ha

$$xRy \ \wedge \ x \neq y \Rightarrow xSy$$

akkor S-et az R szigorításának nevezzük.
Megfordítva, ha

$$xRy \ \vee \ x = y \Rightarrow xTy$$

akkor T az R-hez megfelelő gyenge reláció.

Megjegyzés: Tulajdonképpen a reflexívitás elvételéről és hozzáadásáról van szó. Egy részbenrendezés esetén a megfelelő szigorú reláció (szigorú részbenrendezés) tehát irreflexív, következésképpen szigorúan antiszimmetrikus is. Megfordítva: Egy X-beli szigorú részbenrendezés (tran., irrefl., szig. ant.) megfelelő gyenge relációja részbenrendezés.

Korlátok

- Legkisebb, legnagyobb, minimális, maximális elem
  X halmazbeli részbenrendezés ($\preccurlyeq$) legkisebb (legelső) elemén egy olyan $x \in X$ elemet értünk, melyre: $\forall y \in X : x \preccurlyeq y$. (Ilyen nem biztos, hogy létezik, de ha igen, akkor egyértelmű).
  Hasonlóan a legnagyobb (utolsó) elem olyan $x \in X$, hogy $\forall y \in X : y \preccurlyeq x$.

  x-et minimálisnak nevezzük, ha nincs nála kisebb elem, maximálisnak, ha nincs nála nagyobb elem. (Szemben a legkisebb/legnagyobb elemekkel, minimális/maximális elemből több is lehet. Ha viszont X rendezett, akkor legkisebb=minimális, legnagyobb=maximális.)
- Alsó, felső korlát
  X részbenrendezett halmaz, $Y \subset X$. Az $x \in X$ elem az Y alsó korlátja $\forall y \in Y : x \preccurlyeq y$. (felső korlátja: $\forall y \in Y : y \preccurlyeq x$). Látható, hogy x nem feltétlenül eleme Y-nak, sőt az is lehet, hogy Y-nak nincs alsó/felső korlátja, vagy akár több is van. Ha azonban $x \in Y$, akkor egyértelmű és ez Y legkisebb eleme.
- Infimum, szuprémum
  Ha az alsó korlátok között van legnagyobb elem, azt Y alsó határának, infimumának nevezzük. (Jele: $\inf Y$)
  Ha a felső korlátok között van legnagyobb elem, azt Y felső határának, szuprémumának nevezzük. (Jele: $\sup Y$)
- Alsó, felső határ tulajdonság
  X részbenrendezett halmaz. Ha $\forall \emptyset \neq Y \subset X : Y$ felülről korlátos és van szuprémuma, akkor felső határ tulajdonságú. Illetve ha $\forall \emptyset \neq Y \subset X : Y$ alulról korlátos és van infimuma, akkor alsó határ tulajdonságú.

1.3 Függvények és műveletek

1.3.1 Függvények

Definíció

Egy f reláció függvény, ha

$$(x, y) \in f \ \wedge (x, y') \ \in f \Longrightarrow y = y'$$

Más szóval minden x-hez legfeljebb egy olyan y létezik, hogy $(x, y) \in f$

Így minden $x \in \mathrm{dmn}(f)$-re az $f(x) = \{y\}$, melyet $f(x) = y$ vagy $f : x \mapsto y$ vagy $f_x = y$ is szoktunk jelölni.

Értelmezési tartomány, értékkészlet

Az $f : X \to Y$ jelölést használjuk, ha $\mathrm{dmn}(f) = X$.
Az $f \in X \to Y$ jelölést használjuk, ha $\mathrm{dmn}(f) \subset X$ (amikor $\mathrm{dmn}(f) \subsetneq X$ is előfordulhat).
Mindkét esetben $\mathrm{rng}(f) \subset Y$.

Injektív

f függvény kölcsönösen egyértelmű/injektív, ha

$$f(x) = y \;\wedge\; f(x') = y \implies x = x'$$

Ez azzal ekvivalens, hogy f^{-1} reláció is függvény.

Szürjektív

Az f függvény szürjektív, ha

$$\forall y \in Y : \exists x \in X : f(x) = y$$

Azaz $\mathrm{rng}(f) = Y$. Magyarul az f függvény az egész Y-ra képez.

Bijektív

Ha az f függvény injektív és szürjektív, akkor bijektív.

Indexelt család

Az x függvény i helyen felvett értékét x_i-vel is szoktuk jelölni. Ilyenkor gyakran $\mathrm{dmn}(f) = I$ értelmezési tartományt indexhalmaznak, elemeit indexeknek, $\mathrm{rng}(f)$-et indexelt halmaznak, és magát az x függvényt indexelt családnak szoktuk nevezni.

1.3.2 Műveletek

Definíciók

- Binér művelet
  X halmazon egy $f : X \times X \to X$ függvény binér művelet.
- Unér művelet
  X halmazon egy $f : X \to X$ függvény unér művelet.
- Nullér művelet
  X halmaz, $f : \{\emptyset\} \to X$ nullér művelet. (Gyakorlatilag elemkiválasztás)

Tulajdonságok

- Legyen $\spadesuit$, © binér műveletek X-en.
  1. $\spadesuit$ asszociatív, ha
  $$\forall x, y, z \in X : \quad (x \spadesuit y) \spadesuit z = x \spadesuit (y \spadesuit z)$$
  2. $\spadesuit$ kommutatív, ha
  $$\forall x, y \in X : \quad x \spadesuit y = y \spadesuit x$$
  3. $\spadesuit$ disztributív a ©-ra, ha $\forall x, y, z \in X$:
  $$x \spadesuit (y \copyright z) = (x \spadesuit y) \copyright (x \spadesuit z) \quad \text{- baloldali}$$
  $$(y \copyright z) \spadesuit x = (y \spadesuit x) \copyright (z \spadesuit x) \quad \text{- jobboldali}$$
- Legyen $\heartsuit$ binér művelet X-en és § binér művelet Y-on $f : X \to Y$ művelettartó ha:
$$\forall x_1, x_2 \in X : f(x_1 \heartsuit x_2) = f(x_1) \; \S \; f(x_2)$$

1.4 Számfogalom, komplex számok

1.4.1 Számfogalom

Algebrai Struktúrák

1. Grupoid
   G halmaz egy $\star$ művelettel, azaz a $(G, \star)$ párt grupoidnak nevezzük.
2. Félcsoport
   Ha egy grupoidban a $\star$ művelet asszociatív, akkor a grupoid félcsoport.
3. Monoid
   Semleges elemes félcsoportot monoidnak nevezzük.
   Megyjegyzés: $a \in G$ *semeleges elem, ha* $\forall g \in G : a \star g = g \star a = g$
4. Csoport
   Ha egy monoidban minden elemnek van inverze, akkor csoportról beszélünk.
   Megyjegyzés: $g, g^{-1} \in G$ *és* $\xi \in G$ *semleges elem, akkor a* g^{-1} *a* g *inverze, ha* $g \star g^{-1} = \xi$ *és* $g^{-1} \star g = \xi$
5. Ábel-csoport
   Ha egy csoportban a művelet kommutatív, akkor Abel-csoport.
6. Gyűrű
   $(R, +, \cdot)$ gyűrű, ha az összeadással Abel-csoport, a szorzással félcsoport és teljesül mindkét oldali disztributivitás.

   Ha a szorzás kommutatív, akkor kommutatív gyűrű.

   Ha a szorzásnak van egységeleme, akkor egységelemes gyűrű.
7. Integritási tartomány
   Nullosztó mentes kommutatív gyűrű.

   Nullosztó: x, y *nullátók különböző elemek, de* $x \cdot y = 0$
8. Rendezett integritási tartomány
   R integritási tartomány rendezett integritási tartomány, ha rendezett halmaz, továbbá az összeadás és szorzás monoton.

   Összeadás monoton: $x, y, z \in R$ *és* $x \leq y \;\Rightarrow\; x + z \leq y + z$
   Szorzás monoton: $x, y \in R$ *és* $x, y \geq 0 \;\Rightarrow\; x \cdot y \geq 0$
9. Test
   Egy R gyűrűt, ha $R \setminus \{0\}$ szorzással Abel-csoport, akkor test.
10. Rendezett test
    Ha egy test rendezett integritási tartomány, akkor rendezett test.

Természetes számok

- Peano-axiómák
  Legyen $\mathbb{N}$ egy halmaz és a $^+$ egy $\mathbb{N}$-en értelmezett függvény. Az alábbi feltételeket Peano-axiómáknak nevezzük:
  1. $0 \in \mathbb{N}$ - 0 egy nullér művelet $\mathbb{N}$-en
  2. ha $n \in \mathbb{N}$, akkor $n^+ \in N$ - $^+$ egy unér művelet $\mathbb{N}$-en
  3. ha $n \in \mathbb{N}$, akkor $n^+ \neq 0$ - 0 nincs a $^+$ értékkészletében
  4. ha $n, m \in \mathbb{N}$, és $m^+ = n^+$, akkor $n = m$ - $^+$ injektív
  5. ha $S \subset \mathbb{N}, 0 \in S$, továbbá $n \in S : n^+ \in S$, akkor $S = \mathbb{N}$ - a matematikai indukció elve
- Műveletek
  - összeadás
    $k, m, n \in \mathbb{N}$, akkor:
    1. $(k + m) + n = k + (m + n)$ - *asszociativitás*
    2. $n + 0 = 0 + n = n$ - *0 a nullelem (additív semleges elem)*
    3. $n + k = k + n$ - *kommutativitás*

4. $n + k = m + k$ vagy $k + n = k + m$, akkor $m = n$ - *egyszerűsítési szabály*

– szorzás

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

1. $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ - *asszociativitás*
2. $0 \cdot n = n \cdot 0 = 0$
3. $n \cdot 1 = 1 \cdot n = n$ - *1 az egységelem (multiplikatív semleges elem)*
4. $n \cdot k = k \cdot n$ - *kommutativitás*
5. $k \cdot (m + n) = k \cdot m + \cdot n$, illetve $(m + n) \cdot k = m \cdot k + n \cdot k$ - *disztributivitás*
6. $k \neq 0$ esetén: $n \cdot k = m \cdot k$, akkor $m = n$ - *egyszerűsítési szabály*

Egész számok

Természetes számok körében az összeadásra nézve csak a nullának van inverze, másként szólva, a kivonás általában nem végezhető el.

Tekintsük a $\sim \subset \mathbb{N} \times \mathbb{N}$ relációt, melyre $(m, n) \sim (m', n')$, ha $m+n' = m'+n$. És vegyük az $(m, n)+(m', n') = (m+m', n+n')$ összeadást. A $\sim$ reláció ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelöljük $\mathbb{Z}$-vel. $\mathbb{Z}$ elemeit egész számoknak nevezzük.

Az összeadás kompatibilis az ekvivalenciával, így az egész számok között értelmezve van, és $(\mathbb{Z}, +)$ Ábel-csoport.

Tehát $(\mathbb{Z}, +, \cdot)$ gyűrű.

Megjegyzés: $*$ művelet kompatibilis a $\asymp$ ekvivalenciarelációval, ha teljesül: $x \asymp x' \wedge y \asymp y' \implies x*y \asymp x'*y'$

Racionális számok

Az egész számok körében a nem nulla elemek közül csak az 1-nek és a -1-nek van multiplikatív inverze, másként szólva az osztás általában nem végezhető el.

Tekintsük a $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$-n a $\sim$ relációt, melyre $(m, n) \sim (m', n')$, ha $mn' = nm'$. És vegyük az $(m, n) + (m', n') = (mn' + nm', nn')$ összeadást és az $(m, n) \cdot (m', n') = (mm', nn')$ szorzást. A $\sim$ reláció ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelöljük $\mathbb{Q}$-val. $\mathbb{Q}$ elemeit racionális számoknak nevezzük.

$(\mathbb{Q}, +, \cdot)$ rendezett test.

Valós számok

Nincs olyan $a \in \mathbb{Q}$ szám, melynek négyzete 2. Tehát nem minden szám írható fel m/n $(m, n \in \mathbb{N}^+)$ alakban.

Archimédeszi rendezettség:
Egy F rendezett testet archimédeszien rendezett, ha $x, y \in F : \exists n \in \mathbb{N} : nx \geq y \quad (x > 0)$

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

Egy felső határ tulajdonságú rendezett testet a valós számok testének nevezünk, és $\mathbb{R}$-rel jelöljük. $(\exists!\mathbb{R})$

1.4.2 Komplex számok

A komplex számok szükségét a harmadfokú egyenletek megoldására való Cardano-képlet szülte. Ugyanis abban az esetben, amikor az egyenletnek három különböző valós gyöke van, a képletben a gyökjel alá negatív szám kerül. Fokozatosan tisztult a "képzetes" számokkal való számolás szabályai, és a trigonometrikus függvényekkel való kapcsolat.

Definíció

A komplex számok halmaza $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. $\mathbb{C}$ az $(x, y)+(x', y') = (x+x', y+y')$ összeadással és az $(x, y) \cdot (x', y') = (xx' - yy', y'x + yx')$ szorzással test. A komplex számok halmaza nem rendezett test, mivel (tétel alapján) egy rendezett integritási tartományban $x \neq 0 \Rightarrow x^2 > 0$. (Ez azonban $(0, 1)^2 = i^2 = -1$-re nem teljesül).

[A komplex számok körében (0,0) a nullelem, $(1, 0)$ egységelem, (x, y) additív inverze $(-x, -y)$, és $(0, 0) \neq (x, y)$ pár multiplikatív inverze az $(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$ pár.]

Valós számok azonosítása

Mivel $(x,0)+(x',0)=(x+x',0)$ és $(x,0)\cdot(x',0)=(xx',0)$ így az összes $(x,0), x\in\mathbb{R}$ komplex számot azonosíthatjuk $\mathbb{R}$-rel.

Komplex számok algebrai alakja

Mivel

$$(x,y)=(x,0)+(y,0)\cdot i=x+yi$$

így a komplex számokat $a+bi$ algebrai alakban is írhatjuk.

Ekkor az $\mathrm{Re}(z)=x$ valós számot a $z=(x,y)$ komplex szám valós részének, az $\mathrm{Im}(z)=y$ valós számot pedig a képzetes részének nevezzük.

Konjugált

$z=x+yi$ komplex szám konjugáltja: $\overline{z}=x-yi$

Tulajdonságai:

1. $\overline{z+w}=\overline{z}+\overline{w}$
2. $\overline{z\cdot w}=\overline{z}\cdot\overline{w}$
3. $\overline{\overline{z}}=z$
4. $z+\overline{z}=2\mathrm{Re}(z)$
5. $z-\overline{z}=i\cdot 2\mathrm{Im}(z)$

Abszolút érték

A $z=(x,y)$ komplex szám abszolút értéke: $|z|=\sqrt{x^2+y^2}$

Tulajdonságai:

1. $z\cdot\overline{z}=|z|^2$
2. $\frac{1}{z}=\frac{\overline{z}}{|z|^2}$
3. $|z|=\overline{|z|}$
4. $|z\cdot w|=|z|\cdot|w|$
5. $|z+w|\leq|z|+|w|$

Trigonometrikus alak

- Argumentum
  $z\neq 0$ esetén az a z argumentuma $\forall t\in\mathbb{R}$, melyre $\mathrm{Re}(z)=|z|\cos(t)$, és $\mathrm{Im}(z)=|z|\sin(t)$. Más szóval a z argumentuma az origóból a z-be mutató vektor és a pozitív valós tengellyel bezárt szöge.
- Trigonometrikus alak
  A z komplex szám trigonometrikus alakja: $z=|z|(\cos(t)+i\cdot\sin(t)$
- Moivre-azonosságok
  Legyen $z=|z|(\cos(t)+i\cdot\sin(t))$, és $w=|w|(\cos(s)+i\cdot\sin(s))$. Ekkor

$$z\cdot w=|z||w|(\cos(t+s)+i\cdot\sin(t+s))$$

$$\frac{z}{w}=\frac{|z|}{|w|}(\cos(t-s)+i\cdot\sin(t-s))\quad(w\neq 0)$$

$$z^n=|z|^n(\cos(nt)+i\cdot\sin(nt))\quad(n\in\mathbb{Z})$$

- Gyökvonás
  Legyen $z^n=w$ ekkor:

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

De mivel ez a jelöltés összetéveszthető a valósak között (egyértelművé tett) valós gyökvonással. így ezt a jelölést nem használjuk. Vezessük be helyette a n-edik komplex egységgyök fogalmát:

$$\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i \cdot \sin\left(\frac{2k\pi}{n}\right), \quad k = 0, ..., n-1$$

Ezek után a w gyökeit a z és az n-edik komplex egységgyökök segítségével kaphatjuk meg: $z\varepsilon_0, ..., z\varepsilon_{n-1}$

1.5 Leszámlálások véges halmazokon

Véges halmazok

- Halmazok ekvivalenciája
  X, Y halmazok ekvivalensek, ha létezik X-et Y-ra képező bijekció.
  Jele: $X \sim Y$
- Véges és végtelen halmazok
  X halmaz véges, ha $\exists n \in \mathbb{N} : X \sim \{1, 2, ..., n\}$, egyébként végtelen. Ha létezik n, akkor az egyértelmű, és ekkor a halmaz elemszámának/számosságának nevezzük. Jele: $\#(X)$

Skatulya elv

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

Leszámolások

- Permutáció
  A halmaz egy permutációja az önmagára való kölcsönösen egyértelmű leképezése. Az A halmaz összes permutációjának száma:
  $$P_n = \prod_{k=1}^{n} k \;=\; n!$$
- Variáció
  Az A halmaz elemeiből készíthető, különböző tagokból álló $a_1, a_2, ..., a_k$ sorozatokat az A halmaz k-ad osztályú variációinak nevezzük. Ha A véges ($\#(A) = n$), akkor V_n^k száma megegyezik az $\{1, 2, ..., k\}$-t $\{1, 2, ..., n\}$-be képező kölcsönösen egyértelmű leképezések számával:
  $$V_n^k = \frac{n!}{(n-k)!}$$
- Kombináció
  Ha A halmaz $k \in \mathbb{N}$ elemű részhalmazait k-ad osztályú kombinációinak nevezzük. Ha A véges, akkor C_n^k száma megegyezik $\{1, 2, ..., n\}$ k elemű részhalmazainak számával.
  $$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$
- Ismétléses permutáció
  $A = \{a_1, \ldots, a_r\}$ halmaz elemeinek ismétlődései $i_1, \ldots, i_r$. (Az elemek ismétléses permutációi olyan $i_1 + \cdots + i_r = n$ tagú sorozatok, melyben az a_j elem i_j-szer fordul elő.)
  $$P_n^{i_1,\ldots,i_r} = \frac{n!}{i_1!i_2!\cdots i_r!}$$
- Ismétléses variáció
  Az A véges halmaz elemeiből készíthető (nem feltétlenül különböző) $a_1, \cdots, a_k$ sorozatokat, az A halmaz

k-ad osztályú ismétléses variációinak nevezzük.

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

- Ismétléses kombináció
  Az A véges halmaz. A halmazból k elemet kiválasztva, ismétléseket megengedve, de a sorrend figyelmen kívül hagyva, az A halmaz k-ad osztályú ismétléses kombinációit kapjuk.

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

Tételek

- Binomiális tétel
  $x, y \in R$ (kommutatív egységelemes gyűrű), $n \in \mathbb{R}$. Ekkor

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

- Polinomiális tétel
  $r, n \in \mathbb{N}$ és $x_1, x_2, \cdots, x_r \in R$ (kommutatív egységelemes gyűrű), ekkor

$$(x_1 + \cdots + x_r)^n = \sum_{i_1+\cdots+i_r=n} P_n^{i_1,\cdots,i_r} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} \qquad (i_1, \cdots, i_r \in \mathbb{N})$$

- Szita formula
  $X_1, \cdots, X_k \subset X$ (véges halmaz). f az X-en értelmezett, egy Abel-csoportba képző függvény. Legyen:

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

$$S_r = \sum_{1 \leq i_1 \leq \cdots \leq i_r \leq k} \left(\sum_{x \in X_{i_1} \cap \cdots \cap X_{i_r}} f(x) \right)$$

  és

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

  Ekkor

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

1.6 Számelméleti alapfogalmak, maradékos osztás, lineáris kongruencia-egyenletek

1.6.1 Számelméleti alapfogalmak

Oszthatóság egységelemes integritási tartományban

R egységelemes integritási tartomány, $a, b \in R$. Ha $\exists c \in R : a = bc$, akkor b osztója a-nak (a a b többszöröse). Jele: $b|a$

A $b = 0$-t kivéve legfeljebb egy ilyen c létezik.

Az oszthatóság tulajdonságai egységelemes integritási tartományban.

- Ha $b|a$ és $b'|a'$, akkor $bb'|aa'$
- $\forall a \in R : a|0$ (a nullának minden elem osztója)
- $0|a \Leftrightarrow a = 0$ (a null csak saját magának osztója)

- $\forall a \in R : 1|a$ (az egységelem minden elem osztója)
- $b|a \Rightarrow \forall c \in R : bc|ac$
- $bc|ac$ és $c \neq 0 \Rightarrow b|a$
- $b|a_i$ és $c_i \in R,\ (i = 1, \cdots, j) \ \Rightarrow\ b| \sum_{i=1}^{j} a_i c_i$
- az $|$ reláció reflexív és tranzitív

Felbonthatatlan elem és prímelem

$0, 1 \neq a \in R$ felbonthatatlan (irreducibilis), ha $a = bc$ esetén b vagy c egység ($b, c \in R$).

$0, 1 \neq p \in R$ prím, ha $\forall a, b \in R : p|ab$ esetén $p|a$ vagy $p|b$

Legnagyobb közös osztó, legkisebb közös többszörös, relatív prím

R egységelemes integritási tartomány. $a_1, \cdots, a_n \in R$ elemeknek $b \in R$ legnagyobb közös osztója, ha $b|a_i$ és $b'|a_i$ esetén $b'|b$. Ha b egység, akkor $a_1, \cdots, a_n$ relatív prímek.

$a_1, \cdots, a_n \in R$ elemeknek legkisebb közös többszöröse $b \in R$, ha $a_i|b$ és $a_i|b'$ esetén $b|b'$.

Bővített euklideszi algoritmus

Az eljárás meghatározza az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztóját ($d \in \mathbb{Z}$), valamint $x, y \in \mathbb{Z}$ számokat úgy, hogy $d = ax + by$

A számelmélet alaptétele

Minden pozitív természetes szám (sorrendtől eltekintve) egyértelműen felbontható prímszámok szorzataként.

Erathoszthenész szitája

Adott n-ig a prímek meghatározásához: Írjuk fel a számokat 2-től n-ig. Az első szám (2) prím, összes többszöröse összetett, ezeket húzzuk ki. A fennmaradó számok közül az első (3) ugyancsak prím, stb. Az eljárás végén az n-nél nem nagyobb prímek maradnak.

1.6.2 Maradékos osztás

Legyen R egységelemes integritási tartomány, $f, g \in R[x], g \neq 0$ és tegyük fel, hogy g főegyütthatója egység R-ben. Ekkor

$$\exists! q, r \in R[x] : f = g \cdot q + r \qquad (\deg(r) < \deg(g))$$

1.6.3 Horner-séma

A Horner-módszer egy polinom helyettesítési értékének kiszámítására alkalmas. (Ezzel együtt természetesen az is eldönthető, hogy adott c érték a polinom gyöke-e vagy nem. 4-ed fok felett erre még analitikus megoldás sincs.)

A módszer lényege, hogy az egyébként $f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$ polinom helyettesítési értékének kiszámolásához rendkívül sok szorzásra és összeadásra lenne szükség. A polinom átalakításával azonban a műveletek számát lecsökkenthetjük. A maradékos osztást alkalmazva:

$$f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0 = (f_n x^{n-1} + f_{n-1} x^{n-2} + \cdots)x + f_0$$

Ezt rekurzívan folytatva a következő alakra jutunk:

$$(((f_n x + f_n - 1)x + f_n - 2)x + \cdots)x + f_0$$

A helyettesítési érték kiszámítását egy táblázatban könnyebben elvégezhetjük.

	f_n	f_{n-1}	f_{n-2}	$\cdots$	f_0
c	f_n	$f_n c + f_{n-1}$	$(f_n c + f_{n-1})c + f_{n-2}$	$\cdots$	$f(c)$

A táblázat kitöltése a következőképp zajlik:

1. Az első sorba felírjuk a polinom együtthatóit
2. A második sor első cellájába beírjuk az argumentum értékét.
3. A főegyüttható alá beírjuk önmagát.
4. A második sor celláinak kitöltésével folytatjuk
5. Az előző cella elemét megszorozzuk az argumentummal
6. A szorzathoz adjuk hozzá az aktuális együtthatót
7. Az összeget írjuk be az aktuális cellába
8. Folytassuk az 5. ponttal, míg el nem jutunk az utolsó celláig

Az utolsó cellába a polinom helyettesítési értéke kerül. (Ha ez nulla, akkor az argumentum a polinom gyöke.)

1.6.4 Lineáris kongruencia egyenletek

Kongruencia

Ha $a, b, m \in \mathbb{Z}$ és $m|(a-b)$, akkor azt mondjuk, hogy a és b kongruensek modulo m (Jele: $a \equiv b \mod m$).

A kongruencia ekvivalenciareláció bármely m-re. Ha $a \in \mathbb{Z}$ akkor az ekvivalenciaosztály elemei $a+km, k \in \mathbb{Z}$ alakúak.

Maradékosztályok

Az $m \in \mathbb{Z}$ modulus szerinti ekvivalenciaosztályoknak nevezzük. A maradékosztályokat elemeikkel reprezentáljuk. (Az a elem által reprezentált maradékosztály $\widetilde{a} \mod m$).

Ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor mindegyik az és a maradékosztályt redukált maradékosztálynak nevezzük.

Páronként inkongruens egészek egy rendszerét maradékrendszernek nevezzük.

Ha egy maradékrendszer minden maradékosztályból tartalmaz elemet, akkor teljes maradékrendszer.

Ha maradékrendszer pontosan a redukált maradékosztályokból tartalmaz elemet, akkor redukált maradékrendszer.

Euler-féle φ függvény

$m > 0$ egész szám. Az Euler-féle $\varphi(m)$ függvény a modulo m redukált maradékosztályok számát adja meg. Ez nyilván megegyezik a $0, 1, \cdots, m-1$ számok közötti, m-hez relatív prímek számával.

Euler-Fermat tétel

$m > 1$ egész, a relatív prím m-hez, ekkor:

$$a^{\varphi(m)} \equiv 1 \mod m$$

Fermat tétel

Legyen p prím, és $a \in \mathbb{Z} : p \nmid a$, ekkor

$$a^{p-1} \equiv 1 \mod p$$

Lineáris kongruencia megoldása

Keressük az $ax \equiv b \mod m$ kongruencia megoldásait ($a, b, m \in \mathbb{Z}$ ismert). Ez ekvivalens azzal, hogy keressünk olyan x-et, melyre (valamely y-nal) $ax + my = b$.

Legyen $d = \text{lnko}(a, m)$. Mivel d osztója $ax + my$-nak, b-t is osztania kell, különben nincs megoldás. Így $\frac{a}{d}x + \frac{m}{d}y = \frac{b}{d}$. Ekkor $a'x + m'y = 1$. A bővített euklideszi algoritmus segítségével olyan u, v számokat kapunk, melyekkel $a'u + m'v = 1$ (ui.: a', m' relatív prímek). Az egyenletet b'-vel beszorozva $a'ub' + m'vb' = b' \Rightarrow x \equiv ub' \mod m'$

Lineáris kongruenciarendszer megoldása

Két lineáris kongruencia esetén a megoldások $x \equiv a \mod m$ és $x \equiv b \mod n$. A közös megoldáshoz $x = a + my = b + nz \Leftrightarrow my - nz = b - a$ egyenletet kell megoldani. Akkor és csak akkor van megoldás, ha $d = \text{lnko}(m, n)$ osztója $b - a$-nak. Ekkor a megoldás valamely x_1 egésszel $x \equiv x_1 \mod \text{lkkt}(m, n)$ alakban írható. (Több kongruencia esetén az eljárás folytatható.)

Kínai maradéktétel

$1 < m_1, \cdots, m_n \in \mathbb{N}$ páronként relatív prímek, és $c_1, \cdots, c_n \in \mathbb{Z}$. Az $x \equiv c_j \mod m_j$ $(j = 1, \cdots, n)$ kongruenciarendszer megoldható, és bármely két megoldása kongruens $\mod m_1 m_2 \cdots m_n$

2 Polinomok és műveleteik

Definíció

Legyen R gyűrű. Egy polinomot egy $\sum_{i=0}^{n} f_i x^i$ alakú véges összegnek tekintünk, ahol $n \in \mathbb{N}, f_i \in R$.

Az f_n tagot a polinom főegyütthatójának nevezzük.

Műveletek

Legyen $R[x]$ az $f = (f_0, f_1, \cdots)$ végtelen sorozatok feletti gyűrű (polinomok gyűrűje), ahol $f_i \in R$. Ekkor az $R[x]$-beli műveletek:

- Összeadás:

$$f + g = (f_0 + g_0, f_1 + g_1, \cdots) \qquad (f, g \in R[x])$$

- Szorzás:

$$f \cdot g = h = (h_0, h_1, \cdots) \qquad (f, g, h \in R[x]), \text{ ahol}$$
$$h_k = \sum_{i+j=k} f_i g_j$$

Megjegyzés: Ha R kommutatív, akkor $R[x]$ is az. Ha R egységelemes az 1 egységelemmel, akkor $R[x]$ is az az $(1, 0, 0, \cdots)$ egységelemmel.

3 Gráfok

3.1 Általános és síkgráfok

Alapfogalmak

- Irányítatlan gráf
  Egy irányítatlan gráf a $G = (V, E, \varphi)$ rendezett 3-as, ahol:
  V - a csúcsok halmaza
  E - élek halmaza
  φ - illeszkedési reláció $(\varphi \in E \times V)$
  Ha $v \in \varphi(e)$, akkor v illeszkedik az e élre. $(v \in V, e \in E)$. Egy élnek mindig két vége van
- Él-, és csúcstípusok
  - Izolált csúcs
    $v \in V$ izolált csúcs, ha $\nexists e \in E : v \in \varphi(e)$
  - Párhuzamos él
    $e, e' \in E$ élek párhuzamos élek, ha $\varphi(e) = \varphi(e')$
  - Hurokél
    $e \in E$ hurokél, ha $|\varphi(e)| = 1$

- Irányított gráf
  Egy irányítatott gráf a $G = (V, E, \psi)$ rendezett 3-as, ahol:
  V - a csúcsok halmaza
  E - élek halmaza
  ψ - illeszkedési reláció ($\psi \in E \to V \times V$)
  $\psi(e) = (v, v')$, *ahol* v *az* e *él kezdőpontja,* v' *a végpontja.*

Véges, egyszerű gráfok - alapfogalmak

- Egyszerű gráf
  G gráf egyszerű, ha nem tartalmaz párhuzamos vagy hurokéleket
- Véges gráf $G = (V, E, \varphi)$ gráf véges, ha V, E véges halmazok.
- Szomszédság, fok
  Két él szomszédos, ha van közös pontjuk.
  Két csúcs szomszédos, ha van közös élük.
  $v \in V$ szomszédjainak száma a v foka. [Jele: $\deg(v) = \mathrm{d}(v)$]
- r-reguláris gráfok
  G gráf r-reguláris, ha minden pont foka r
- Teljes gráf
  G gráf teljes gráf, ha minden él be van húzva, más szóval $(|V| - 1)$-reguláris. (Jele: $K_{|V|}$)
- Páros gráf
  G páros gráf, ha $V = V' \cup V''$ és $V' \cap V'' = \emptyset$ (diszjunkt), valamint él csak V' és V'' között fut.
  Ha viszont így V' *és* V'' *között minden él be húzva, akkor teljes páros gráf. (Jele:* $K_{n,m}$*, ahol* $n = |V'|, m = |V''|$*)*
- Részgráf
  $G = (V, E, \varphi)$ részgráfja $G' = (V', G', \varphi')$-nek, ha $V \subset V \ \wedge \ E \subset E' \ \wedge \ \varphi \subset \varphi'$
- Séta, vonal, út
  G gráfban egy n hosszú séta v-ből v'-be egy olyan

  $$v_0, e_1, v_1, \cdots, v_{n-1}, e_n, v_n$$

  sorozat, melyre $v = v_1, v' = v_n$ és $v_{i-1}, v_i \in \varphi(e_i)$

  Egy séta vonal, ha minden él legfeljebb egyszer szerepel a sorozatban.

  Egy vonal út, ha minden csúcs legfeljebb egyszer szerepel a sorozatban.

  Egy séta/vonal/út zárt, ha kezdő és végpontja megegyezik, egyébként nyílt.
- Összefüggő gráf Egy gráf összefüggő, ha bármely két csúcs közt van út.
  Ez a reláció ekvivalenciareláció, melynek ekvivalenciaosztályait komponenseknek nevezzük.
- Címkézett, Súlyozott gráf
  $G = V, E, \varphi, C_e, c_e, C_v, c_v)$ rendezett 7-es címkézett gráfot jelöl, ahol C_e, C_v tetszőleges halmazok, és

  $$c_e : E \to C_e$$

  $$c_v : E \to C_v$$

  Ha $C_e = C_v = \mathbb{R}^+$, akkor a gráfot súlyozott gráfnak nevezzük, és w a csúcs/él súlya. $(w(e) = c_e(e),\ w(v) = c_v(v))$

Síkba rajzolhatóság

Fogalmak

- Síkba rajzolhatóság
  Egy gráf síkba rajzolható, ha lerajzolható úgy, hogy az elei nem keresztezik egymást.
- Topologikus izomorfia
  Két gráf topologikusan izomorf, ha a következő lépést illetve fordítottját véges sok ismétlésével egyikből a másikat kapjuk: Egy másodfokú csúcsot elhagyunk, és a szomszédjait összekötjük.
- Tartomány
  Ha G gráf síkba rajzolható, akkor a tartományok az élek által határolt síkidomok. (A nem korlátolt síkidom is tartomány.)

Tételek

1. Minden véges gráf $\mathbb{R}^3$-ban lerajzolható.
2. Ha egy véges gráf síkba rajzolható $\Longleftrightarrow$ gömbre rajzolható
3. Euler-tétel:
   Ha a G véges gráf összefüggő, síkba rajzolható gráf, akkor:
   $$|E| + 2 = |V| + |T|$$
4. Kuratowsky-tétel:
   Egy véges gráf pontosan akkor síkba rajzolható, ha nem tartalmaz K_5-tel, vagy $K_{3,3}$-mal topologikusan izomorf részgráfot.

3.2 Fák

Fa

Egy gráfot fának nevezünk, ha összefüggő és körmentes.

Feszítőfa

F részgráfja G-nek. Ha F fa és csúcsainak halmaza megegyezik G csúcsainak halmazával, akkor F-et a G feszítőfájának nevezzük.

Tételek

- Ha G egyszerű gráf, akkor a következő feltételek ekvivalensek:
  1. G fa
  2. G összefüggő, de bármely él törlésével már nem az
  3. Két különböző csúcs között csak egy út van
  4. G körmentes, de egy él hozzáadásával már nem az
- Ha G egyszerű véges gráf, akkor a következő feltételek ekvivalensek:
  1. G fa
  2. G-ben nincs kör és $n-1$ éle van
  3. G összefüggő és $n-1$ éle van

Irányított fa

Olyan fa, melyre: $\exists v \in V : d^-(v) = 0$ és $\forall v' \neq v : d^-(v') = 1$ (Egy csúscs befoka 0, a többié 1)

További fogalmak:

- $r \in V, d^-(r) = 0$ csúcsot gyökérnek nevezzük
- v' csúcs szintje a r, v' út hossza
- $(v, v') \in \psi(e)$, a v szülője v'-nek, v' gyereke, v-nek.
- v levél, ha $d^+(v) = 0$

3.3 Euler- és Hamilton-gráfok

3.3.1 Euler-gráf

Euler-vonal

Az Euler-vonal olyan vonal v-ből v'-be a gráfban, amelyben minden él szerepel. Ha $v = v'$ akkor ezt a vonalat Euler-körvonalnak is szokás nevezni. Euler-vonallal rendelkező gráfot Euler-gráfnak nevezik.

Tétel

Egy összefüggő véges gráfban pontosan akkor létezik Euler-körvonal, ha minden csúcs páros fokú.

3.3.2 Hamilton-gráf

A Hamilton-út egy olyan út v-ből v'-be a gráfban, mely minden csúcsot tartalmat. Ha $v = v'$ akkor ezt az utat Hamilton-körnek is szokás nevezni. Hamilton-úttal rendelkező gráfot Hamilton-gráfnak nevezik.

3.4 Gráfok adatszerkezetei

Gráfok számítógépes reprezentációjához legtöbbször láncolt listákat, vagy mátrixokat szoktak használni. A láncolt listák inkább ritka gráfokra, míg a mátrixok sűrű gráfok esetén gazdaságosak.

Illeszkedési mátrix

$G = (V, E, \psi)$ irányított gráf esetén a gráfot egy $A = \{0, 1, -1\}^{n \times m}$ mátrix segítségével tudjuk reprezentálni, ahol $V = \{v_1, \cdots, v_n\}$, és $E = \{e_1, \cdots, e_m\}$. Ekkor a mátrix egyes elemei:

$$a_{ij} = \begin{cases} 1 & \text{ha } v_i \text{ kezdőpontja } e_j\text{-nek} \\ -1 & \text{ha } v_i \text{ végpontja } e_j\text{-nek} \\ 0 & \text{különben} \end{cases}$$

Ha G nem irányított, akkor $a_{ij} = |a_{i,j}|$

Csúcsmátrix

A fenti jelölésekkel irányított esetben $B \in \mathbb{Z}^{n \times n}$, ahol b_{ij} a v_i-ből v_j-be menő élek számát jelöli.

Ha G irányítatlan, akkor b_{ii} v_i hurokéleinek száma, egyébként b_{ij} a v_i és v_j csúcsok közötti élek száma.