УНИВЕРЗИТЕТ У КРАГУЈЕВЦУ
ПРИРОДНО–МАТЕМАТИЧКИ ФАКУЛТЕТ

Бојана Боровићанин

ДИСКРЕТНА МАТЕМАТИКА

Теорија бројева, комбинаторика и теорија графова

КРАГУЈЕВАЦ, 2019.

Дискретна математика

Теорија бројева, комбинаторика и теорија графова

Аутор:
др Бојана Боровићанин, доцент ПМФ-а у Крагујевцу

Рецензенти:
Академик др Иван Гутман,
професор емеритус ПМФ-а у Крагујевцу, редовни члан САНУ
др Мирослав Петровић,
редовни професор у пензији ПМФ-а у Крагујевцу
др Игор Миловановић,
редовни професор Електронског факултета у Нишу

Издавач:	Природно-математички факултет у Крагујевцу `www.pmf.kg.ac.rs`
За издавача:	*Проф. др Срећко Трифуновић*, декан
Слог:	*др Бојана Боровићанин*
Цртежи:	*др Бојана Боровићанин*
Корице:	*Агенција „Круг“, Крагујевац*
Штампа:	„ *InterPrint* “, Крагујевац
Тираж:	150 примерака

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

ДИСКРЕТНА математика Теорија бројева, комбинаторика и теорија графова : уџбеник / Б. [Бојана] Боровићанин . . . ; [цртежи Бојана Боровићанин]. – Крагујевац : Природно-математички факултет, 2019 (Крагујевац :). – 144 стр. : граф. прикази ; 24 цм

На врху насл. стр. : Универзитет у Крагујевцу. – Тираж 150. – Библиографија: стр. 142–144.

ISBN 978–86–6009–064–7

1. Боровићанин, Бојана
а) Боровићанин Бојана – Уџбеник
COBISS. SR-ID

ISBN 978–86–6009–064–7

Садржај

Предговор

Ова књига је настала као плод вишегодишњег рада у оквиру предмета *Дискретна математика* у Институту за математику и информатику Природно-математичког факултета у Крагујевцу и има за циљ да студентима обезбеди што адекватнију литературу за припремање испита из поменутог предмета.

Садржај књиге одговара у потпуности наставном плану и програму предмета *Дискретна математика*, уз додатно проширење појединих садржаја. Књига садржи три поглавља: Теорија бројева, Комбинаторика и Теорија графова. За разумевање изложених садржаја од читаоца се захтева минимално претходно знање из математичке логике, анализе и линеарне алгебре.

Области обрађене у оквиру књиге су разматране у литератури на енглеском језику, као и у оквиру неколико издања на српском језику, али ни у једном од њих нису обједињене све области садржане у књизи. Надам се да ће њоме бити направљен корак напред у односу на постојећу литературу на српском језику која се односи на теме обрађене у књизи. Верујем да она може бити од користи не само студентима математике у оквиру курса Дискретна математика, већ и у разним другим курсевима.

Захваљујем се рецензентима академику др Ивану Гутману, др Мирославу Петровићу и др Игору Миловановићу на корисним сугестијама и указаним грешкама, чиме су значајно побољшали квалитет ове књиге. Такође, захваљујем се на помоћи колегиницама др Марији Станић, др Сузани Алексић и др Мирјани Лазић. Осим тога, бићу захвална и на свакој аргументованој примедби, јер и поред све пажње и уложеног напора, вероватно има и недостатака.

Глава 1

Теорија бројева

1.1 Увод

Теорија бројева је једна од најстаријих грана математике чијем су развоју значајан допринос дали антички математичари Диофант[1] и Еуклид[2], а касније и неки од најзначајнијих математичара у историји, као што су Ојлер[3] и Гаус[4]. Теорија бројева је углавном током историје посматрана као област тзв. чисте, односно теоријске математике, која нема значајну практичну примену. Међутим, од средине 70-тих година 20. века долази до битне промене оваквог гледишта, да би данас ова математичка дисциплина постала једна од најзначајнијих у области криптографије и безбедне размене информација.

1.2 Дељивост

Теорија бројева се углавном бави проучавањем особина целих бројева. У овом поглављу, користићемо, без доказивања, нека својства скупа $\mathbb{N} = \{1, 2, \ldots\}$ природних бројева, као и скупа $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ целих бројева. Осим тога, скуп $\mathbb{N} \cup \{0\}$ означаваћемо са $\mathbb{N}_0$.

Појам дељивости је један од најједноставнијих, али истовремено и најважнијих појмова у теорији бројева. Скуп $\mathbb{Z}$ је затворен за операције сабирања, одузимања и множења, тј. збир, разлика или производ два

[1] Diophantus (око 200–280 н. е.) старогрчки математичар
[2] Euclid (око 330–275 п. н. е.), старогрчки математичар
[3] Leonhard Euler (1707–1783), швајцарски математичар
[4] Johann Carl Friedrich Gauss (1777–1855), немачки математичар

цела броја је такође цео број. Међутим, са операцијом дељења то није случај. Питање дељивости у скупу $\mathbb{Z}$ је веома значајно у теорији бројева.

Дефиниција 1.1. *Цео број a **дељив** је целим бројем b $(b \neq 0)$ ако постоји цео број q такав да је $a = bq$.*

Ако је број a дељив бројем b, пишемо $b \mid a$ (b дели a) и кажемо да је број b **делилац** броја a, односно да је број a **садржалац** броја b. Ако број a није дељив бројем b, пишемо $b \nmid a$ (b не дели a).

Основна својства релације дељивости изложена су у следећој теореми.

Теорема 1.1. 1° *$a \mid a$, за свако $a \in \mathbb{Z} \setminus \{0\}$.*

2° *Ако $b \mid a$, тада $b \mid ac$ за свако $c \in \mathbb{Z}$.*

3° *Ако $b \mid a$ и $b \mid c$, тада $b \mid ax + cy$ за све $x, y \in \mathbb{Z}$.*

4° *Ако $b \mid a$ и $a \mid b$, тада је $a = b$ или $a = -b$, за $a, b \in \mathbb{Z} \setminus \{0\}$.*

5° *Ако $b \mid a$ и $a \mid c$, тада $b \mid c$.*

6° *Ако $b \mid a$ и $a \neq 0$, тада је $|b| \leqslant |a|$.*

Доказ. 1° Како је $a = 1 \cdot a$ и $1 \in \mathbb{Z}$, тврђење следи.

2° Ако $b \mid a$, тада постоји цео број q такав да је $a = bq$. Тада за свако $c \in \mathbb{Z}$ важи да је $ac = (bq)c = bq_1$, где је $q_1 = qc \in \mathbb{Z}$, одакле следи да $b \mid ac$.

3° Ако $b \mid a$ и $b \mid c$, тада постоје цели бројеви q_1 и q_2 такви да је $a = bq_1$ и $c = bq_2$. За произвољне целе бројеве x и y важи да је $ax + cy = b(q_1x + q_2y) = bz$, где је $z = q_1x + q_2y \in \mathbb{Z}$. Према дефиницији релације дељивости следи да $b \mid ax + cy$.

4° Ако $b \mid a$ и $a \mid b$, тада постоје цели бројеви q_1 и q_2 такви да је $a = bq_1$ и $b = aq_2$, одакле је $a = aq_1q_2$, тј. $a(1 - q_1q_2) = 0$. Одавде, с обзиром на то да је $a \neq 0$, следи да је $q_1q_2 = 1$. Како су q_1 и q_2 цели бројеви, то је $q_1 = q_2 = 1$ или $q_1 = q_2 = -1$, односно $a = b$ или $a = -b$.

5° Ако $b \mid a$ и $a \mid c$, онда постоје цели бројеви q_1 и q_2 такви да је $a = bq_1$ и $c = aq_2$. Тада је $c = bq_1q_2 = bq$, при чему је $q = q_1q_2 \in \mathbb{Z}$, одакле следи да $b \mid c$.

6° Како $b \mid a$, постоји цео број q такав да је $a = bq$. Одавде следи да је $|a| = |b||q|$, а како је $a \neq 0$, то је $|q| \geqslant 1$, одакле следи тврђење. □

Уочимо да је релација дељивости релација поретка на скупу $\mathbb{N}$, али не и на скупу $\mathbb{Z}$ (теорема 1.1, 1° и 4°).

Теорема 1.2. *Ако је у збиру од n сабирака $a_1 + a_2 + \cdots + a_n = 0$, њих $n-1$ дељиво целим бројем b, тада су сви сабирци дељиви са b.*

Доказ. Нека су у датом збиру сви сабирци осим a_i, $1 \leqslant i \leqslant n$, дељиви целим бројем b. Тада, према дефиницији 1.1, постоје цели бројеви $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n$ такви да је

$$a_1 = bq_1,\ a_2 = bq_2,\ \ldots, a_{i-1} = bq_{i-1},\ a_{i+1} = bq_{i+1},\ \ldots, a_n = bq_n.$$

Сада из дате једнакости добијамо

$$a_i = -b(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_n) = bq_i,$$

где је $q_i = -(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_n) \in \mathbb{Z}$. Дакле, $b \mid a_i$. □

У скупу $\mathbb{Z}$ операција дељења није увек изводљива. Међутим, увек је могуће тзв. „дељење са остатком“, тј. важи следећа теорема.

Теорема 1.3. (**Теорема о остатку**) *За сваки цео број a и природан број b постоје јединствени цели бројеви q и r такви да је*

$$a = bq + r, \quad 0 \leqslant r < b.$$

*При том се број q назива **количник**, а r **остатак** при дељењу броја a бројем b.*

Доказ. Посматрајмо скуп целих бројева $\{a - kb \mid k \in \mathbb{Z}\}$ и изаберимо у њему најмањи број који припада скупу $\mathbb{N}_0$ (егзистенција таквог броја следи из чињенице да је скуп природних бројева добро уређен). Нека је то број $a - qb$ и обележимо га са r. Тада је

$$a = bq + r, \quad 0 \leqslant r < b, \tag{1.1}$$

јер би у случају $r \geqslant b$ и број $a-(q+1)b = r-b < r$ припадао скупу $\mathbb{N}_0$, што је у контрадикцији са избором броја r. Тиме је доказана егзистенција бројева q и r. Докажимо још њихову јединственост. Претпоставимо да постоје и бројеви q_1 и r_1 такви да је

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b. \tag{1.2}$$

Одузимањем (1.2) од (1.1) добијамо

$$0 = b(q - q_1) + (r - r_1),$$

одакле, на основу теореме 1.2, следи да $b \mid r - r_1$. Како је $\mid r - r_1 \mid < b$, мора бити $r - r_1 = 0$, тј. $r = r_1$, па је и $q = q_1$. □

Претпоставка да је b природан број у претходној теореми може се заменити захтевом да је b цео број различит од 0 и условом $0 \leqslant r < \mid b \mid$.

ПРИМЕР 1.1. Одредити највећи природан број који подељен са 31 даје количник 17.

Решење. Тражени број a, чији је количник при дељењу са 31 једнак 17, према претходној теореми може се написати у облику $a = 31 \cdot 17 + r$, при чему је $0 \leqslant r < 31$. Највећи природан број описаног облика је $a = 31 \cdot 17 + 30 = 557$. △

ПРИМЕР 1.2. Ако број a при дељењу са $3, 5, 7$ даје остатке r_1, r_2, r_3, респективно, доказати да је број $70r_1 + 21r_2 + 15r_3 - a$ дељив са 105.

Решење. Из услова задатка следи да је $a = 3k + r_1 = 5\ell + r_2 = 7m + r_3$, $k, \ell, m \in \mathbb{Z}$, тј. важи да је $r_1 = a - 3k$, $r_2 = a - 5\ell$, $r_3 = a - 7m$. Одавде је

$$\begin{aligned} 70r_1 + 21r_2 + 15r_3 - a &= 70(a - 3k) + 21(a - 5\ell) + 15(a - 7m) - a \\ &= 105(a - 2k - \ell - m), \end{aligned}$$

одакле произилази да $105 \mid 70r_1 + 21r_2 + 15r_3 - a$. △

Дефиниција 1.2. *Цео број d је **заједнички делилац** бројева a и b ако $d \mid a$ и $d \mid b$.*

Сваки цео број различит од 0 има коначно много делилаца, па је скуп заједничких делилаца два цела броја, од којих је бар један различит од 0, коначан и у њему постоји највећи број.

Дефиниција 1.3. *Највећи међу заједничким делиоцима бројева a и b, од којих је бар један различит од 0, је **највећи заједнички делилац** бројева a и b. Обележавамо га са (a, b), $NZD(a, b)$ или $D(a, b)$.*

У књизи ће, осим ако не назначимо другачије, бити коришћена ознака (a, b) за највећи заједнички делилац бројева a и b.

Дефиниција 1.4. *За бројеве a и b кажемо да су **узајамно** (**релативно**) **прости** ако је $(a, b) = 1$.*

Теорема 1.4. *Ако је d највећи заједнички делилац целих бројева a и b, онда постоје цели бројеви α и β такви да је $\alpha a + \beta b = d$.*

Доказ. Посматрајмо скуп целих бројева $A = \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$ и изаберимо најмањи позитиван елемент тог скупа. Нека је то број $c = \alpha a + \beta b$. Доказаћемо да је c највећи заједнички делилац бројева a

и b. Докажимо најпре да $c \mid a$ и $c \mid b$. Ако $c \nmid a$, тада постоје, према теореми 1.3, цели бројеви q и r такви да је $a = cq + r$ и $0 < r < c$. Тада је

$$r = a - cq = a - (\alpha a + \beta b)q = (1 - \alpha q)a - \beta q b,$$

тј. r је позитиван број мањи од c и припада скупу A, супротно претпоставци да је c најмањи такав број. Дакле, $c \mid a$. Аналогно се доказује да $c \mid b$.

Докажимо још да је c највећи заједнички делилац бројева a и b, тј. да је $d = c$. Како је $d = (a, b)$, то $d \mid a$ и $d \mid b$, тј. $a = dq_1$ и $b = dq_2$, за неке целе бројеве q_1 и q_2. Тада је $c = \alpha d q_1 + \beta d q_2 = d(\alpha q_1 + \beta q_2)$, одакле следи да $d \mid c$. Имајући у виду да су d и c позитивни бројеви, према теореми 1.1 6° следи да је $d \leqslant c$. Како је d највећи заједнички делилац бројева a и b, мора бити $d = c$, односно $d = \alpha a + \beta b$. □

На основу доказа претходне теореме очигледно важи следеће тврђење.

Последица 1.1. *Највећи заједнички делилац целих бројева a и b је најмањи позитиван број облика $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$.*

Теорема 1.5. *Ако се цели број d може приказати у облику $d = \alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$, онда $(a, b) \mid d$. Специјално, ако је $\alpha a + \beta b = 1$, онда су бројеви a и b узајамно прости.*

Доказ. Нека је $D = (a, b)$. Тада постоје цели бројеви q_1 и q_2 такви да је $a = Dq_1$ и $b = Dq_2$, па је $d = \alpha a + \beta b = \alpha D q_1 + \beta D q_2 = D(\alpha q_1 + \beta q_2)$, одакле следи да $D = (a, b) \mid d$.

Ако је $\alpha a + \beta b = 1$, тада $(a, b) \mid 1$, одакле следи да је $(a, b) = 1$, тј. бројеви a и b су узајамно прости. □

Теорема 1.6. 1° *Ако је $k > 0$, тада је $(ka, kb) = k(a, b)$.*

2° *Ако је $a = bq$ и $b > 0$, онда је $(a, b) = b$.*

3° *Ако $c \mid ab$ и при томе је $(c, a) = 1$, тада $c \mid b$.*

4° $(ab, c) = 1$ *ако и само ако је* $(a, c) = 1$ *и* $(b, c) = 1$.

5° *Ако је $a = bq + r$, тада је $(a, b) = (b, r)$.*

Доказ. 1° Према последици 1.1 највећи заједнички делилац бројева a и b је најмањи позитиван број облика $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$, а највећи делилац бројева ka и kb је најмањи позитиван број облика $\alpha k a + \beta k b$, $\alpha, \beta \in \mathbb{Z}$, одакле због услова $k > 0$ непосредно следи тврђење.

2° Како $b \mid a$ и $b \mid b$, следи да је b заједнички делилац бројева a и b. Број $b > 0$ не може имати ниједан делилац $c > b$, одакле следи да је $(a, b) = b$.

3° Како је $(c, a) = 1$, према теореми 1.4 следи да постоје цели бројеви γ и α такви да је $\gamma c + \alpha a = 1$, па је $\gamma cb + \alpha ab = b$. Како по претпоставци $c \mid ab$ и важи да $c \mid cb$, следи, према теореми 1.2, да $c \mid b$.

4° Ако је $(a, c) = 1$ и $(b, c) = 1$, онда постоје $\alpha, \beta, \gamma_1, \gamma_2 \in \mathbb{Z}$ такви да је $\alpha a + \gamma_1 c = 1$ и $\beta b + \gamma_2 c = 1$. Одавде је

$$\alpha a \beta b = (1 - \gamma_1 c)(1 - \gamma_2 c) = 1 - \gamma c,$$

где је $\gamma = \gamma_1 + \gamma_2 - \gamma_1 \gamma_2 c$. Сада из услова $\alpha\beta ab + \gamma c = 1$ следи да је $(ab, c) = 1$.

Обрнуто, ако је $(ab, c) = 1$, тада постоје $\alpha, \gamma \in \mathbb{Z}$ такви да је $\alpha ab + \gamma c = 1$, одакле због $(\alpha b)a + \gamma c = 1$ следи да је $(a, c) = 1$, односно, због $(\alpha a)b + \gamma c = 1$ следи да је $(b, c) = 1$.

5° Нека је $d_1 = (a, b)$ и $d_2 = (b, r)$. Тада из услова $a = bq + r$ следи да $d_1 \mid r$, тј. d_1 је заједнички делилац бројева b и r, па је $d_1 \leqslant d_2$. Осим тога, из услова $a = bq + r$ следи да $d_2 \mid a$, тј. d_2 је заједнички делилац бројева a и b, па је $d_2 \leqslant d_1$. Како је $d_1 \leqslant d_2$ и $d_2 \leqslant d_1$, то је $d_1 = d_2$, тј. $(a, b) = (b, r)$. □

Нагласимо да из услова $c \mid ab$, без додатне претпоставке $(c, a) = 1$, не следи да $c \mid b$ (тврђење 3°). На пример, $10 \mid 4 \cdot 15$, али $10 \nmid 4$ и $10 \nmid 15$.

ПРИМЕР 1.3. Доказати да из услова $7 \mid \overline{abb}$ следи да $7 \mid a + 2b$, при чему је $\overline{abb} = 100a + 10b + b$.

Решење. Важи да је

$$\begin{aligned}\overline{abb} &= 100a + 10b + b = 98a + 7b + 2a + 4b \\ &= 7(14a + b) + 2(a + 2b),\end{aligned}$$

одакле, како $7 \mid \overline{abb}$ и $7 \mid 7(14a + b)$, према теореми 1.2 произилази да $7 \mid 2(a + 2b)$, односно, према теореми 1.6 3°, $7 \mid a + 2b$. △

Питање дељивости целих бројева не зависи од њиховог знака, па се можемо ограничити на дељивост природних бројева. У наставку ћемо изложити поступак за одређивање највећег заједничког делиоца два природна броја, познат као **Еуклидов алгоритам**. На основу теореме 1.3

можемо записати следећи низ једнакости

$$\begin{aligned} a &= bq_1 + r_1, && 0 \leqslant r_1 < b, \\ b &= r_1q_2 + r_2, && 0 \leqslant r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, && 0 \leqslant r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, && 0 \leqslant r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned} \tag{1.3}$$

Како бројеви r_n чине строго опадајући низ природних бројева, након коначно много корака долазимо до $r_{n+1} = 0$, тј. до једнакости $r_{n-1} = r_nq_{n+1}$, која говори о дељивости два узастопна остатка.

Теорема 1.7. *Последњи остатак r_n који је различит од нуле у једнакостима* (1.3) *представља највећи заједнички делилац бројева a и b.*

Доказ. На основу теореме 1.6 5° важе следеће једнакости

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n).$$

Како је $r_{n-1} = r_nq_{n+1}$, то према теореми 1.62° важи да је $(r_{n-1}, r_n) = r_n$, па је $(a, b) = r_n$. □

ПРИМЕР 1.4. Применом Еуклидовог алгоритма одредити $(252, 198)$.

Решење. Како је

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2, \end{aligned}$$

следи да је $(252, 198) = 18$. △

Према теореми 1.4 највећи заједнички делилац целих бројева a и b може се приказати као њихова линеарна комбинација, тј. у облику $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$. Бројеве α и β можемо ефективно одредити применом Еуклидовог алгоритма, што ће бити показано у следећем примеру.

ПРИМЕР 1.5. Одредити целе бројеве α и β такве да је $\alpha \cdot 252 + \beta \cdot 198 = (252, 198)$.

Решење. На основу претходног примера важи да је $(252, 198) = 18$, као и

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

△

ПРИМЕР 1.6. Одредити $(2n + 3, n + 7)$, $n \in \mathbb{N}$.

Решење. Нека је $d = (2n + 3, n + 7)$. Тада $d \mid 2(n + 7) - (2n + 3)$, тј. $d \mid 11$, одакле следи да је $d = 1$ или $d = 11$.

Нека је $n = 11q + r$, $0 \leqslant r < 11$. Ако је $d = 11$, тада из услова $11 \mid n + 7$ следи да $11 \mid 11q + r + 7$, одакле произилази да је $r = 4$. Како је сада $2n + 3 = 2(11q + 4) + 3 = 11(2q + 1)$, следи да $11 \mid 2n + 3$. Дакле, ако је природан број n облика $11q + 4$, $q \in \mathbb{N}$, тада је $d = 11$, док за $n = 11q + r$, $r \neq 4$, важи да је $d = 1$. △

Дефиницију највећег заједничког делиоца можемо проширити и на скуп од n произвољних целих бројева.

Дефиниција 1.5. *Највећи заједнички делилац n целих бројева $a_1, a_2, \ldots, a_n$, од којих је бар један различит од нуле, је највећи од заједничких делилаца ових бројева и обележавамо га са $(a_1, a_2, \ldots, a_n)$. Ако је $(a_1, a_2, \ldots, a_n) = 1$, бројеви $a_1, a_2, \ldots, a_n$ су **узајамно (релативно) прости.***

*Бројеви $a_1, a_2, \ldots, a_n$ су **узајамно (релативно) прости у паровима** ако је $(a_i, a_j) = 1$ за $i, j = 1, 2, \ldots, n$, $i \neq j$.*

ПРИМЕР 1.7. Бројеви $5, 11, 15$ су узајамно прости, тј. $(5, 11, 15) = 1$, али нису узајамно прости у паровима, јер је $(5, 15) = 5$.

Дефиниција 1.6. *Заједнички садржалац n целих бројева $a_1, a_2, \ldots, a_n$, различитих од нуле, је број који је дељив сваким од бројева $a_1, a_2, \ldots, a_n$. Најмањи међу позитивним заједничким садржаоцима бројева $a_1, a_2, \ldots, a_n$ зове се најмањи заједнички садржалац бројева $a_1, a_2, \ldots, a_n$ и обележава са $[a_1, a_2, \ldots, a_n]$.*

Теорема 1.8. *Потребан и довољан услов да произвољан број буде дељив производом више чинилаца, који су релативно прости у паровима, је да тај број буде дељив сваким чиниоцем производа.*

Доказ. Доказ изводимо индукцијом по броју чинилаца. Докажимо најпре да тврђење важи у случају производа два чиниоца. Нека је број

n дељив сваким од бројева a и b, таквих да је $(a,b)=1$. Из услова $a \mid n$ следи да постоји цео број q такав да је $n=aq$. Како $b \mid n$, тј. $b \mid aq$ и при том је $(a,b)=1$, према теореми 1.6 3° следи да $b \mid q$, односно $q=bq_1$, $q_1 \in \mathbb{Z}$. Дакле, $n=aq=abq_1$, тј. $ab \mid n$. Обрнуто, ако $ab \mid n$, тада је $n=abq$, $q \in \mathbb{Z}$, одакле следи да $a \mid n$ и $b \mid n$.

Претпоставимо да тврђење важи за производ k чинилаца који су релативно прости у паровима и посматрајмо број n дељив сваким од бројева $a_1, a_2, \ldots, a_{k+1}$ који су релативно прости у паровима. Како $a_{k+1} \mid n$, важи да је $n=a_{k+1}q$, $q \in \mathbb{Z}$. Из услова $a_i \mid n$, тј. $a_i \mid a_{k+1}q$, како је $(a_i, a_{k+1})=1$, $i=1,2,\ldots,k$, следи, према теореми 1.6 3°, да $a_i \mid q$, $i=1,2,\ldots,k$. Одавде, према индуктивној претпоставци важи да $a_1a_2\cdots a_k \mid q$, тј. $q=a_1a_2\cdots a_kq_1$, за неко $q_1 \in \mathbb{Z}$. Сада је $n=a_1a_2\cdots a_ka_{k+1}q_1$, тј. $a_1a_2\cdots a_ka_{k+1} \mid n$. Обрнуто, ако $a_1a_2\cdots a_ka_{k+1} \mid n$, тада је $n=a_1a_2\cdots a_ka_{k+1}q$, $q \in \mathbb{Z}$, одакле следи да $a_i \mid n$, $i=1,2,\ldots,k+1$. □

Применом претходне теореме добијамо критеријуме дељивости производима више чинилаца који су релативно прости у паровима. На пример, број је дељив са 15 ако и само ако је дељив са 3 и 5, број је дељив са 120 ако и само ако је дељив са 3, 5 и 8, итд.

1.3 Прости бројеви

Дефиниција 1.7. *Цео број $p>1$ је **прост** ако нема ниједан делилац d такав да је $1<d<p$. Цео број $m>1$ који није прост је **сложен** број.*

Прости бројеви су $2,3,5,7,11,13,17,\ldots$, а сложени $4,6,8,9,10,\ldots$

Теорема 1.9. *Природан број $n>1$ је сложен ако и само ако има прост фактор p, такав да је $p \leqslant \sqrt{n}$.*

Доказ. Ако број $n>1$ има прост фактор $p \leqslant \sqrt{n}$, онда је он према дефиницији 1.7 сложен број. Обрнуто, нека је p најмањи прост фактор сложеног броја n. Тада постоји природан број m такав да је $n=pm$, при чему је $m \geqslant p$. Одавде је $n=pm \geqslant p^2$, тј. $p \leqslant \sqrt{n}$. □

Претходну теорему можемо искористити при налажењу свих простих бројева мањих од датог природног броја n поступком који је познат као **Ератостеново сито**. Најпре исписујемо све природне бројеве од 1 до n.

$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \ldots, n.$

Затим, прецртамо број 1. Како је 2 први прост број, прецртамо све бројеве дељиве са 2 и веће од 2 (они су сложени). Следећи прост број је 3. Прецртамо све бројеве веће од 3 који су дељиви са 3. Следећи непрецртан број је 5, па је он прост, јер би у супротном већ био прецртан. Први непрецртани садржалац броја 5 је $25 = 5^2$. Настављајући описани поступак издвојићемо („кроз сито ће проћи“) све просте бројеве мање од n. Имајући у виду теорему 1.9 закључујемо да се поступак прекида када прецртамо све сложене бројеве који су садржаоци простих бројева не већих од $\sqrt{n}$.

ПРИМЕР 1.8. Сваки прост број већи од 2 је облика $4k+1$ или $4k-1$, за неко $k \in \mathbb{N}$.

Решење. Како је сваки прост број већи од 2 непаран, он при дељењу са 4 даје остатак 1 или 3, одакле следи тврђење. △

Теорема 1.10. (**Еуклид**) *Од сваког простог броја постоји већи прост број, тј. постоји бесконачно много простих бројева.*

Доказ. Претпоставимо супротно, тј. да постоји коначно много простих бројева. Нека су то бројеви $p_1, p_2, \ldots, p_k$, а сви остали природни бројеви већи од 1 су сложени. Број

$$n = p_1 p_2 \cdots p_k + 1$$

је сложен према претпоставци, па мора бити дељив неким простим бројем. Међутим, то је немогуће, јер при дељењу било којим од простих бројева $p_1, p_2, \ldots, p_k$ даје остатак 1, одакле следи да је тврђење теореме истинито. □

ПРИМЕР 1.9. Простих бројева облика $4k-1$, $k \in \mathbb{N}$, има бесконачно много.

Решење. Претпоставимо да су $p_1, p_2, \ldots, p_\ell$ једини прости бројеви облика $4k-1$, $k \in \mathbb{N}$, и посматрајмо број

$$N = 4p_1 p_2 \cdots p_\ell - 1.$$

Број N је већи од свих наведених простих бројева и облика је $4k-1$, $k \in \mathbb{N}$, па мора бити сложен. Како је N непаран број, његови прости фактори су облика $4k-1$ или $4k+1$, $k \in \mathbb{N}$. Производ два броја облика $4k+1$, $k \in \mathbb{N}$, је број тог истог облика, тј.

$$(4k_1+1)(4k_2+1) = 4(4k_1k_2 + k_1 + k_2) + 1,$$

па број N мора имати прост фактор облика $4k-1$, $k \in \mathbb{N}$. Међутим, како је

$$N+1 = 4p_1p_2\cdots p_\ell$$

и $(N, N+1) = 1$, то је број N узајамно прост са свим простим бројевима облика $4k-1$. Дакле, простих бројева облика $4k-1$, $k \in \mathbb{N}$, има бесконачно много. △

Напомена. Простих бројева облика $4k+1$, $k \in \mathbb{N}$, такође има бесконачно много, о чему ће бити речи нешто касније.

Иако простих бројева има бесконачно много, они су „ретки“ у скупу природних бројева, о чему говори следећа теорема.

Теорема 1.11. *Ако је дат произвољан природан број n, увек се може наћи n узастопних сложених бројева.*

Доказ. Посматрајмо n узастопних природних бројева

$$\begin{aligned} m_1 &= (n+1)n(n-1)\cdots 3\cdot 2\cdot 1+2,\\ m_2 &= (n+1)n(n-1)\cdots 3\cdot 2\cdot 1+3,\\ &\vdots\\ m_n &= (n+1)n(n-1)\cdots 3\cdot 2\cdot 1+n+1. \end{aligned}$$

Како је број m_1 дељив са 2, m_2 са 3, ..., m_n са $n+1$, свих n бројева су сложени. □

ПРИМЕР 1.10. Ако је p прост број, доказати да је број p^4+p^2+1 сложен.

Решење. Ако је $p=2$, тада је $p^4+p^2+1 = 21 = 3\cdot 7$, што је сложен број. За $p=3$ је $p^4+p^2+1 = 91 = 7\cdot 13$, што је такође сложен број.

Докажимо да је сваки прост број p већи од 3 облика $6k\pm 1$, $k \in \mathbb{N}$. Наиме, ако број p напишемо у облику $p = 6k+r$, $0 \leqslant r < 6$, тада из услова да је p прост следи да може бити $r=1$ или $r=5$, одакле произилази тражени закључак. Ако је p прост број облика $6k\pm 1$, тада је број p^4+p^2+1 облика $3m$, $m \in \mathbb{N}$, односно то је сложен број. Дакле, за сваки прост број p, број p^4+p^2+1 је сложен. △

Теорема 1.12. (**Еуклидова лема**) *Ако је p прост број и $p \mid ab$, тада $p \mid a$ или $p \mid b$. Важи и општије, ако $p \mid a_1a_2\cdots a_n$, тада $p \mid a_i$, за неко $i = 1, 2, \ldots, n$.*

Доказ. Нека $p \mid ab$ и претпоставимо да $p \nmid a$. Како су једини делиоци простог броја p бројеви 1 и p, следи да је $(p, a) = 1$, па према теореми 1.6 3° важи да $p \mid b$.

Општије тврђење доказујемо индукцијом по броју чинилаца n. За $n = 2$ тврђење је доказано. Претпоставимо да тврђење важи за производе са мање од n чинилаца. Ако $p \mid a_1 \cdot (a_2 \cdots a_n)$, онда, на основу случаја $n = 2$, $p \mid a_1$ или $p \mid a_2 \cdots a_n$. Ако $p \mid a_1$, тврђење је доказано. У супротном, како $p \mid a_2 \cdots a_n$, по индуктивној претпоставци следи да $p \mid a_i$, за неко $i = 2, \ldots, n$. □

Користећи претходну теорему доказаћемо следећу, веома важну теорему теорије бројева.

Теорема 1.13. (**Основни став аритметике**) *Сваки природан број $n > 1$ може се на јединствен начин представити у облику производа простих чинилаца (са тачношћу до њиховог поретка), тј. за сваки природан број $n > 1$ постоје јединствени прости бројеви $p_1, p_2, \ldots, p_k$, такви да је $p_1 < p_2 < \cdots < p_k$, и јединствени цели бројеви $\alpha_1, \alpha_2, \ldots, \alpha_k$, тако да је*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Доказ. Ако је n прост број, тврђење очигледно важи. Претпоставимо да тврђење важи за сваки сложен број мањи од n. Ако је n сложен број, тада се n може написати у облику $n = n_1 n_2$, при чему $1 < n_1, n_2 < n$. Бројеви n_1 и n_2 су или прости или се по индуктивној претпоставци могу приказати као производ простих чинилаца, одакле следи да и број n има то својство. Групишући једнаке просте факторе броја n, закључујемо да се сваки природан број $n > 1$ може представити у облику

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{1.4}$$

где су $p_1 < p_2 < \cdots < p_k$ прости бројеви и $\alpha_1, \alpha_2, \ldots, \alpha_k$ природни бројеви.

Представљање броја $n > 1$ у облику (1.4) познато је као **канонска факторизација** броја n.

Докажимо да је представљање броја n у облику (1.4) јединствено. Препоставимо супротно, тј. да број $n > 1$ има две такве факторизације

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad p_1 < p_2 < \cdots < p_k, \quad \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N},$$

и

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}, \quad q_1 < p_2 < \cdots < q_s, \quad \beta_1, \beta_2, \ldots, \beta_s \in \mathbb{N}. \tag{1.5}$$

Како $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, $1 \leqslant i \leqslant k$, према теореми 1.12 постоји индекс j, $1 \leqslant j \leqslant s$, такав да $p_i \mid q_j$, одакле, пошто су p_i и q_j прости бројеви, следи да је $p_i = q_j$. Дакле, $\{p_1, p_2, \ldots, p_k\} \subseteq \{q_1, q_2, \ldots, q_s\}$. Аналогно се показује да је и $\{q_1, q_2, \ldots, q_s\} \subseteq \{p_1, p_2, \ldots, p_k\}$, па је $\{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_s\}$. Закључујемо да је $k = s$, а како су низови $p_1, p_2, \ldots, p_k$ и $q_1, q_2, \ldots, q_s$ растући, важи да је $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$, одакле следи да се једнакост (1.5) може написати у облику

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}. \tag{1.6}$$

Докажимо још да је $\alpha_i = \beta_i$, $1 \leqslant i \leqslant k$. Претпоставимо да је $\alpha_1 \neq \beta_1$ и нека је, на пример, $\alpha_1 < \beta_1$, тј. $\beta_1 = \alpha_1 + \gamma$, $\gamma > 0$. Ако поделимо израз на десној страни сваке од једнакости (1.4) и (1.6) са $p_1^{\alpha_1}$ добијамо

$$p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\gamma} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

одакле следи да p_1 дели десну, а не дели леву страну последње једнакости, што је немогуће, па мора бити $\alpha_1 = \beta_1$. Аналогно се доказује да је $\alpha_i = \beta_i$, $i = 2, \ldots, k$, одакле следи јединственост факторизације. □

Помоћу канонске факторизације датих бројева a и b лако се одређује њихов највећи заједнички делилац и најмањи заједнички садржалац.

Теорема 1.14. *Нека су* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *и* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geqslant 0$, $i = 1, 2, \ldots, k$, *канонске факторизације природних бројева* a *и* b. *Тада*

$$b \mid a \Leftrightarrow \beta_i \leqslant \alpha_i, \quad i = 1, 2, \ldots, k. \tag{1.7}$$

Доказ. Ако $b \mid a$, онда постоји природан број $q = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, $\gamma_i \geqslant 0$, $i = 1, 2, \ldots, k$, такав да је $a = bq$. Из последње једнакости следи да је

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1 + \gamma_1} p_2^{\beta_2 + \gamma_2} \cdots p_k^{\beta_k + \gamma_k},$$

односно, због јединствености канонске факторизације броја a важи да је

$$\alpha_i = \beta_i + \gamma_i, \quad i = 1, 2, \ldots, k,$$

одакле следи да је $\beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$.

Обрнуто, ако је $\beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$, тада је $\gamma_i = \alpha_i - \beta_i \geqslant 0$, $i = 1, 2, \ldots, k$, и природан број $q = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ задовољава једнакост $a = bq$, одакле следи да $b \mid a$. □

Теорема 1.15. *Нека су* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *и* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geqslant 0$, $i = 1, 2, \ldots, k$, *канонске факторизације природних бројева* a *и* b. *Тада је*

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \quad \gamma_i = \min\{\alpha_i, \beta_i\}, \quad i = 1, 2, \ldots, k, \tag{1.8}$$

и

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \quad \delta_i = \max\{\alpha_i, \beta_i\}, \quad i = 1, 2, \ldots, k. \tag{1.9}$$

Доказ. Нека је $D = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, при чему је $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, k$. Како је $\gamma_i \leqslant \alpha_i$ и $\gamma_i \leqslant \beta_i$, $i = 1, 2, \ldots, k$, на основу теореме 1.14 следи да $D \mid a$ и $D \mid b$, тј. D је заједнички делилац бројева a и b. Докажимо још да је D највећи заједнички делилац бројева a и b. Нека је број $d = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}$, $\mu_i \geqslant 0$, $i = 1, 2, \ldots, k$, произвољан заједнички делилац бројева a и b. Тада, према теореми 1.14, важи да је $\mu_i \leqslant \alpha_i$ и $\mu_i \leqslant \beta_i$, $i = 1, 2, \ldots, k$, одакле следи да је $\mu_i \leqslant \min\{\alpha_i, \beta_i\} = \gamma_i$, $i = 1, 2, \ldots, k$. Према теореми 1.14 сада важи да $d \mid D$, одакле, на основу теореме 1.1 6°, следи да је $d \leqslant D$. Дакле, доказали смо да је

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}.$$

Нека је $S = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, при чему је $\delta_i = \max\{\alpha_i, \beta_i\}$, $i = 1, 2, \ldots, k$. Како је $\alpha_i \leqslant \delta_i$ и $\beta_i \leqslant \delta_i$, $i = 1, 2, \ldots, k$, на основу теореме 1.14 следи да $a \mid S$ и $b \mid S$, тј. S је заједнички садржалац бројева a и b. Докажимо да је S најмањи заједнички садржалац бројева a и b. Нека је број $s = p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k}$, $\nu_i \geqslant 0$, $i = 1, 2, \ldots, k$, произвољан заједнички садржалац бројева a и b. Тада према теореми 1.14 важи да је $\nu_i \geqslant \alpha_i$ и $\nu_i \geqslant \beta_i$, $i = 1, 2, \ldots, k$, одакле следи да је $\nu_i \geqslant \max\{\alpha_i, \beta_i\} = \delta_i$, $i = 1, 2, \ldots, k$. Сада важи да $S \mid s$, одакле, према теореми 1.1 6°, следи да је $S \leqslant s$, чиме је доказано да је

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}.$$

□

На основу доказа претходне теореме закључујемо да важе следећа тврђења.

Последица 1.2. *Ако је* d *произвољан заједнички делилац бројева* a *и* b, *тада* $d \mid (a, b)$.

Последица 1.3. *Ако је s произвољан заједнички садржалац бројева a и b, тада $[a,b] \mid s$.*

Последица 1.4. *За целе бројеве a и b важи*

1° $(a,b)\cdot[a,b] = |a\,b|$,

2° $[ka,kb] = k[a,b], \quad k \in \mathbb{N}$.

Доказ. 1° Како је $\min\{\alpha,\beta\} + \max\{\alpha,\beta\} = \alpha+\beta$, тврђење следи непосредно.

2° Према 1° важи да је $[ka,kb] = \dfrac{k^2\,|a\,b|}{(ka,kb)}$, а како је $(ka,kb) = k\,(a,b)$, тврђење следи. □

ПРИМЕР 1.11. Одредити све природне бројеве a и b, такве да је $(a,b) = 6$ и $[a,b] = 36$.

Решење. Из услова $(a,b) = 6$, следи да је $a = 6m$, $b = 6n$, $m,n \in \mathbb{N}$, при чему је $(m,n) = 1$. Према последици 1.4 важи да је $36 = [a,b] = [6m,6n] = 6\,[m,n] = 6mn$, тј. $mn = 6$. Како је $(m,n) = 1$, закључујемо да бројеви m и n узимају вредности из следеће табеле.

m	1	6	2	3
n	6	1	3	2

Одавде произилази да су вредности бројева a и b дате у табели испод.

a	6	36	12	18
b	36	6	18	12

△

Теорема 1.16. *Ако је производ два узајамно проста природна броја a и b квадрат целог броја, тј. ако је $ab = c^2$, $c \in \mathbb{Z}$, тада су и a и b квадрати целих бројева.*

Доказ. Природан број је квадрат целог броја ако и само ако су му сви експоненти у канонској факторизацији парни бројеви. Како су бројеви a и b узајамно прости, сваки прост делилац броја c^2 је или делилац броја a или делилац броја b, али не и делилац оба ова броја. Због тога сви прости фактори у канонској факторизацији бројева a и b морају имати парне експоненте, одакле следи да су бројеви a и b квадрати целих бројева. □

Коришћењем канонске факторизације природног броја могуће је одредити укупан број позитивних делилаца, као и збир свих позитивних делилаца тог броја.

Теорема 1.17. *Нека је* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *канонска факторизација природног броја* a. *Тада*

1° *укупан број свих позитивних делилаца броја* a (*укључујући* 1 *и* a), *у ознаци* $\tau(a)$, *одређен је са*

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1), \tag{1.10}$$

2° *збир свих позитивних делилаца броја* a, *у ознаци* $\sigma(a)$, *одређен је са*

$$\sigma(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{1.11}$$

Доказ. 1° На основу теореме 1.14, сви позитивни делиоци броја a су облика $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, при чему је $0 \leqslant \beta_i \leqslant \alpha_i$. Дакле, код произвољног позитивног делиоца d броја a, експонент β_i, $i = 1, 2, \ldots, k$, са којим се прост фактор p_i појављује у канонској факторизацији броја d може се изабрати на $\alpha_i + 1$ начина, одакле следи да је број $\tau(a)$ одређен помоћу једнакости (1.10).

2° Формулу за збир свих позитивних делилаца броја a одређујемо индукцијом по броју (различитих) простих делилаца броја a.

Ако је $a = p_1^{\alpha_1}$, за неки прост број p_1 и неко $\alpha_1 \in \mathbb{N}$, тада су бројеви $1, p_1, p_1^2, \ldots, p_1^{\alpha_1}$ сви позитивни делиоци броја a, па је њихов збир

$$\sigma(a) = 1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.$$

Претпоставимо да једнакост (1.11) важи за све природне бројеве који имају k (различитих) простих делилаца.

Нека је $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}$ број са $k+1$ различитих простих делилаца. Ако је $a_0 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, тада су сви позитивни делиоци броја a дати са

$$\begin{array}{llll} d_1, & d_1 \cdot p_{k+1}, & \ldots, & d_1 \cdot p_{k+1}^{\alpha_{k+1}} \\ d_2, & d_2 \cdot p_{k+1}, & \ldots, & d_2 \cdot p_{k+1}^{\alpha_{k+1}} \\ \vdots & & & \end{array}$$

где су $d_1, d_2, \ldots$ сви позитивни делиоци броја a_0. Одавде, коришћењем

индуктивне претпоставке, добијамо

$$\begin{aligned}\sigma(a)=\sum_{d|a} d &= \sum_{d|a_0}\left(d+d\cdot p_{k+1}+\cdots+d\cdot p_{k+1}^{\alpha_{k+1}}\right)\\ &= \left(1+p_{k+1}+\cdots+p_{k+1}^{\alpha_{k+1}}\right)\sum_{d|a_0} d\\ &= \frac{p_{k+1}^{\alpha_{k+1}+1}-1}{p_{k+1}-1}\cdot\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.\end{aligned}$$

□

Дефиниција 1.8. *Функција $f:\mathbb{N}\to\mathbb{Z}$ је **мултипликативна** ако су испуњени услови:*

(1) $f(n_0)\neq 0$, *за неко* $n_0\in\mathbb{N}$,

(2) *ако је* $(m,n)=1$, *тада је* $f(mn)=f(m)f(n)$.

Теорема 1.18. *Функције τ и σ су мултипликативне.*

Доказ. Како је $\tau(1)=\sigma(1)=1$, услов (1) из дефиниције 1.8 је задовољен.

Ако су m и n два узајамно проста броја чије су канонске факторизације дате са

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\quad n=q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s},$$

при чему се ниједан од бројева p_i, $i=1,2,\ldots,k$, не поклапа ни са једним од бројева q_j, $j=1,2,\ldots,s$, тада је

$$mn=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$$

канонска факторизација броја mn, одакле према теореми 1.17 следи да је

$$\tau(mn)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)(\beta_1+1)(\beta_2+1)\cdots(\beta_s+1)=\tau(m)\tau(n)$$

и

$$\begin{aligned}\sigma(mn) &= \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}\\ &\quad\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdot\frac{q_2^{\beta_2+1}-1}{q_2-1}\cdots\frac{q_s^{\beta_s+1}-1}{q_s-1}\\ &= \sigma(m)\sigma(n),\end{aligned}$$

тј. функције τ и σ су мултипликативне. □

ПРИМЕР 1.12. Наћи најмањи природан број n који има исти број делилаца као број 1998.

Решење. Како је $1998 = 2 \cdot 3^3 \cdot 37$, укупан број делилаца броја 1998 једнак је $\tau(1998) = 2 \cdot 4 \cdot 2 = 16$. Имајући у виду да је $16 = 1 \cdot 16 = 2 \cdot 8 = 4 \cdot 4 = 2 \cdot 2 \cdot 4 = 2 \cdot 2 \cdot 2 \cdot 2$, закључујемо да је број n један од бројева $2^{15}, 2^7 \cdot 3, 2^3 \cdot 3^3, 2^3 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 5 \cdot 7$ (сваки од бројева је, због услова минималности броја n, добијен множењем најмањих могућих простих бројева). Од наведених бројева најмањи је број $2^3 \cdot 3 \cdot 5 = 120$ и то је тражени број. △

1.3.1 Дистрибуција простих бројева

Нека је са $\pi(n)$ означен број простих бројева који нису већи од датог природног броја n. Прости бројеви су веома неправилно распоређени у скупу природних бројева, па је проблем испитивања понашања функције π веома тежак. Један од основних резултата у теорији бројева представља асимптотски закон расподеле простих бројева о коме говори следећа теорема.

Теорема 1.19. (**Теорема о простим бројевима**) *Важи да је*

$$\pi(n) \sim \frac{n}{\ln n}$$

(*чита се* $\pi(n)$ *је асимптотски једнако са* $\frac{n}{\ln n}$).

Доказ ове теореме ће због сложености бити изостављен. Ова теорема заправо тврди да за сваки произвољно мали реалан број $\varepsilon > 0$ постоји природан број n_0, који зависи од ε, такав да је за све природне бројеве $n > n_0$ испуњено

$$1 - \varepsilon < \frac{\pi(n)}{\frac{n}{\ln n}} < 1 + \varepsilon.$$

Ово тврђење је као хипотезу изнео Гаус 1840. године, а доказали су је независно Вале-Пусен[5] и Адамар[6] 1896. године. Чебишев[7] је 1850. године доказао да за сваки природан број $n > 1$ важи

$$\frac{7}{8} \cdot \frac{n}{\ln n} < \pi(n) < \frac{9}{8} \cdot \frac{n}{\ln n}.$$

[5] Charles Jean de la Valée-Poussin (1866–1962), белгијски математичар
[6] Jacques Salomon Hadamard (1865–1963), француски математичар
[7] Pafnuty Lvovich Chebyshev (1821–1894), руски математичар

Ова процена, иако лошија од Гаусове, је значајна, јер важи за сваки природан број $n > 1$.

Навешћемо, такође без доказа због сложености, и Дирихлеову[8] теорему која говори о дистрибуцији простих бројева.

Теорема 1.20. (**Дирихле**) *Ако су a и m узајамно прости природни бројеви, тада аритметички низ $a + km$, $k \in \mathbb{N}_0$, садржи бесконачно много простих бројева.*

Користећи претходни резултат закључујемо да простих бројева облика $4k + 1$, $k \in \mathbb{N}$, има бесконачно много, о чему је било речи раније.

1.4 Конгруенције

Дефиниција 1.9. *Нека је $m > 1$ природан број. Цели бројеви a и b су конгруентни по модулу m ако $m \mid a - b$. Пише се $a \equiv b \pmod{m}$.*

Пример 1.13. $17 \equiv 5 \pmod{12}$, $7 \equiv 7 \pmod{12}$ и $36 \equiv 0 \pmod{12}$. Слично, $6 \equiv -14 \pmod{20}$.

Теорема 1.21. 1° *$a \equiv b \pmod{m}$ ако и само ако је $a = mk + b$ за неки цео број k.*

2° *$a \equiv b \pmod{m}$ ако и само ако бројеви a и b дају исти остатак при дељењу са m.*

3° *Бити конгруентан по датом модулу је релација еквиваленције у скупу $\mathbb{Z}$.*

Доказ. 1° Ако је $a \equiv b \pmod{m}$, тада $m \mid a - b$, тј. $a - b = mk$, за неки цео број k, па је $a = mk + b$. Обратно, ако је $a = mk + b$, за неки цео број k, тада је $a - b = mk$, односно $m \mid a - b$, одакле је $a \equiv b \pmod{m}$.

2° Ако је $a \equiv b \pmod{m}$, тада $m \mid a - b$. Применом теореме о остатку (теорема 1.3) добијамо да је $a = mq_1 + r_1$ и $b = mq_2 + r_2$, при чему је $0 \leqslant r_1, r_2 < m$, па је $a - b = m(q_1 - q_2) + r_1 - r_2$. Како $m \mid a - b$, следи да $m \mid r_1 - r_2$, одакле, из $0 \leqslant | r_1 - r_2 | < m$, следи да је $r_1 - r_2 = 0$, тј. $r_1 = r_2$.

Обрнуто, ако је $r_1 = r_2$, тада је $r_1 - r_2 = 0$, па је $a - b = m(q_1 - q_2)$, тј. $m \mid a - b$, односно $a \equiv b \pmod{m}$.

[8] Peter Gustav Lejeune Dirichlet (1805–1859), немачки математичар

3° Према претходно доказаном очигледно је $a \equiv a \pmod{m}$. Осим тога, како $m \mid a-b$ ако и само ако $m \mid b-a$, важи да је $a \equiv b \pmod{m}$ ако и само ако је $b \equiv a \pmod{m}$.

Докажимо још транзитивност релације $\equiv \pmod{m}$. Нека су a, b, c цели бројеви такви да је $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$. Тада $m \mid a-b$ и $m \mid b-c$, па $m \mid (a-b)+(b-c)$, тј. $m \mid a-c$, одакле је $a \equiv c \pmod{m}$. □

Неке особине конгруенција дате су у следећим теоремама.

Теорема 1.22. 1° *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *тада је* $ax+cy \equiv bx+dy \pmod{m}$, *за свака два цела броја* x *и* y.

2° *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *тада је* $ac \equiv bd \pmod{m}$.

3° *Ако је* $a \equiv b \pmod{m}$ *и* $m = kd$, $d > 1$, *тада је* $a \equiv b \pmod{d}$.

4° *Ако је* $a \equiv b \pmod{m}$, *онда је* $P(a) \equiv P(b) \pmod{m}$, *где је* $P(x)$ *полином са целобројним коефицијентима.*

Доказ. 1° Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, тада $m \mid a-b$ и $m \mid c-d$. Одавде, према теореми 1.1 2°, следи да $m \mid (a-b)x$ и $m \mid (c-d)y$, за произвољне целе бројеве x и y. Према теореми 1.1 3° важи

$$m \mid (a-b)x + (c-d)y,$$

тј.

$$m \mid (ax+cy) - (bx+dy),$$

одакле следи да је $ax+cy \equiv bx+dy \pmod{m}$.

2° Из $a \equiv b \pmod{m}$ следи да $m \mid a-b$, па $m \mid (a-b)c$. Осим тога, из $c \equiv d \pmod{m}$, следи да $m \mid c-d$, односно $m \mid (c-d)b$. Према претходном, важи

$$m \mid (a-b)c + (c-d)b,$$

тј.

$$m \mid ac - bd,$$

одакле произилази да је $ac \equiv bd \pmod{m}$.

3° Ако је $a \equiv b \pmod{m}$, тада $m \mid a-b$. Како је $m = kd$, $d > 1$, то $d \mid m$, одакле, због транзитивности релације дељивости, следи да $d \mid a-b$, тј $a \equiv b \pmod{d}$.

4° Нека је $P(x) = \sum_{k=0}^{n} c_k x^k$ произвољан полином са целобројним коефицијентима. На основу тврђења 2°, из $a \equiv b \pmod{m}$ следи да је $a^k \equiv b^k \pmod{m}$ за свако $k \in \mathbb{N}_0$. Осим тога, како је $c_k \equiv c_k \pmod{m}$,

за свако $k = 0, 1, \ldots, n$, то је, према тврђењу 2°, $c_k a^k \equiv c_k b^k \pmod{m}$, за свако $k = 0, 1, \ldots, n$. Сада на основу тврђења 1° важи да је

$$\sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod{m},$$

тј.

$$P(a) \equiv P(b) \pmod{m}.$$

□

Теорема 1.23. 1° *Ако је* $ax \equiv ay \pmod{m}$ *и при томе је* $(a, m) = 1$, *тада је* $x \equiv y \pmod{m}$.

2° $ax \equiv ay \pmod{m}$ *ако и само ако је* $x \equiv y \left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$.

3° $x \equiv y \pmod{a}$ *и* $x \equiv y \pmod{b}$ *ако и само ако је* $x \equiv y \left(\mathrm{mod}\ [a, b]\right)$.

Доказ. 1° Ако је $ax \equiv ay \pmod{m}$, онда $m \mid ax - ay$, тј. $m \mid a(x - y)$. Како је $(a, m) = 1$, следи да $m \mid x - y$, тј. $x \equiv y \pmod{m}$.

2° Из $ax \equiv ay \pmod{m}$ следи да $m \mid ax - ay$, па је $a(x - y) = km$, за неки цео број k. Одавде добијамо да је $\frac{a}{(a,m)}(x - y) = k\frac{m}{(a,m)}$, па $\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x - y)$. Како је $\left(\frac{m}{(a,m)}, \frac{a}{(a,m)}\right) = 1$, следи да $\frac{m}{(a,m)} \mid x - y$, тј. $x \equiv y \left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$.

Обрнуто, ако је $x \equiv y \left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$, тј. $\frac{m}{(a,m)} \mid x - y$, тада је $x - y = k\frac{m}{(a,m)}$, за неки цео број k, па је и $a(x - y) = \frac{ak}{(a,m)}m$. Дакле, $m \mid ax - ay$, тј. $ax \equiv ay \pmod{m}$.

3° Ако је $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$, тада $a \mid x - y$ и $b \mid x - y$, па је $x - y$ заједнички садржалац бројева a и b, одакле следи да $[a, b] \mid x - y$, тј. $x \equiv y \left(\mathrm{mod}\ [a, b]\right)$.

Обрнуто, ако је $x \equiv y \left(\mathrm{mod}\ [a, b]\right)$, тада $[a, b] \mid x - y$. Како $a \mid [a, b]$ и $b \mid [a, b]$, из транзитивности релације дељивости следи да $a \mid x - y$ и $b \mid x - y$, тј. $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$. □

Тврђење 1° познато је као закон канцелације (скраћивања) и не важи без претпоставке да је $(a, m) = 1$.

1.4.1 Системи остатака

Дефиниција 1.10. *Нека је* $m > 1$ *природан број. Скуп од* m *целих бројева у коме не постоји ниједан пар бројева конгруентних по модулу* m *назива се* ***потпуни систем остатака по модулу*** m.

Релација $\equiv \pmod m$ је релација еквиваленције у скупу целих бројева, па сви цели бројеви који су конгруентни по датом модулу m, тј. дају исти остатак при дељењу са m, припадају истој класи еквиваленције ове релације. Како су $0, 1, \ldots, m-1$ могући остаци при дељењу са m произвољног целог броја, следи да постоји тачно m класа еквиваленције ове релације. Дакле, потпуни систем остатака по модулу m чини произвољних m бројева изабраних тачно по један из сваке од m класа еквиваленције ове релације.

Теорема 1.24. 1° *Скуп* $\{0, 1, \ldots, m-1\}$ *је потпуни систем остатака по модулу* m.

2° *Ако је* $\{x_1, x_2, \ldots, x_m\}$ *потпуни систем остатака по модулу* m *и* $(a, m) = 1$, *тада је и скуп* $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ *потпуни систем остатака по модулу* m, *за сваки цео број* b.

Доказ. Тврђење 1° је очигледно тачно на основу дефиниције потпуног система остатака по модулу m.

2° Довољно је доказати да међу елементима скупа $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ не постоји ниједан пар бројева конгруентних по модулу m. Ако за неке i и j, $i \neq j$, $i, j = 1, 2, \ldots, m$, важи $ax_i + b \equiv ax_j + b \pmod m$, тада је $ax_i \equiv ax_j \pmod m$, одакле, због $(a, m) = 1$, следи да је $x_i \equiv x_j \pmod m$, што је немогуће, јер је $\{x_1, x_2, \ldots, x_m\}$ потпуни систем остатака по модулу m. □

Скуп $\{0, 1, \ldots, m-1\}$ зове се и систем најмањих ненегативних остатака. Осим њега, користи се и тзв. систем остатака најмањих по модулу, који за непаран број m чине бројеви

$$-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2},$$

а за паран број m бројеви

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2} \quad \text{или} \quad -\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1.$$

ПРИМЕР 1.14. Скупови $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ и $\{20, 11, -8, 3, 14, -15, 26, -3, 8, -11\}$ су потпуни системи остатака по модулу 10.

Дефиниција 1.11. *Скуп свих елемената потпуног система остатака по модулу* m *који су релативно прости са* m *назива се* ***сведени*** (***редуковани***) ***систем остатака по модулу*** m.

ПРИМЕР 1.15. Скупови $\{1, 3, 7, 9\}$ и $\{11, 3, -3, -11\}$ су сведени системи остатака по модулу 10.

Теорема 1.25. *Ако је* $a \equiv b \pmod{m}$ *и* $(a, m) = 1$, *тада је и* $(b, m) = 1$.

Доказ. Ако је $a \equiv b \pmod{m}$, онда је $a = mk + b$, за неки цео број k. Како је $(a, m) = 1$, постоје цели бројеви α и β, такви да је $\alpha a + \beta m = 1$, одакле је $\alpha(mk+b)+\beta m = 1$, тј. $\alpha b+(\alpha k+\beta)m = 1$, па је $(b, m) = 1$. □

На основу претходне теореме закључујемо да су или сви или ниједан елемент из произвољне класе еквиваленције релације $\equiv \pmod{m}$ релативно прости са m, па ће у сведеном систему остатака по датом модулу m увек бити исти број елемента, без обзира од ког потпуног система остатака полазимо.

Дефиниција 1.12. *Број природних бројева који нису већи од датог природног броја* m *и релативно су прости са њим, тј. број елемената произвољног сведеног система остатака по модулу* m *означава се са* $\varphi(m)$. *Функција* φ *зове се* ***Ојлерова функција***.

Ако је p прост број, тада је $\varphi(p) = p - 1$.

Теорема 1.26. *Ако је* $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ *сведени систем остатака по модулу* m *и* $(a, m) = 1$, *тада је и скуп* $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ *сведени систем остатака по модулу* m.

Доказ. Скуп $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ садржи $\varphi(m)$ целих бројева међу којима нема конгруентних по модулу m. Осим тога, како је $(a, m) = 1$ и $(x_i, m) = 1$, за свако $i = 1, 2, \ldots, \varphi(m)$, то је и $(ax_i, m) = 1$, за свако $i = 1, 2, \ldots, \varphi(m)$, одакле следи да скуп $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ представља сведени систем остатака по модулу m. □

ПРИМЕР 1.16. Нека је $m = 10$ и $a = 7$. Тада је $(a, m) = 1$, па је скуп $\{7 \cdot 1, 7 \cdot 3, 7 \cdot 7, 7 \cdot 9\} = \{7, 21, 49, 63\}$ сведени систем остатака по модулу 10.

Теорема 1.27. *Ојлерова функција* φ *је мултипликативна.*

Доказ. Важи да је $\varphi(2) = 1 \neq 0$. Нека су m и n узајамно прости бројеви, тј. $(m, n) = 1$. Докажимо да је $\varphi(mn) = \varphi(m)\varphi(n)$.

Распоредимо бројеве од 1 до mn у следећу табелу.

1	2	$\cdots$	k	$\cdots$	m
$m+1$	$m+2$	$\cdots$	$m+k$	$\cdots$	$2m$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(n-1)m+1$	$(n-1)m+2$	$\cdots$	$(n-1)m+k$	$\cdots$	mn

Како је неки број узајамно прост са mn ако и само ако је узајамно прост и са m и са n, доказ ћемо извести тако што ћемо најпре пребројати колико у табели има бројева узајамно простих са m, а затим колико међу њима има бројева узајамно простих са n.

Бројеви сваке колоне у табели припадају истој класи еквиваленције релације $\equiv \pmod m$, одакле, на основу теореме 1.25, следи да су или сви или ниједан елемент произвољне колоне узајамно прости са m. Ово нам омогућава да говоримо о „колонама узајамно простим са m“. Таквих колона има $\varphi(m)$.

Посматрајмо произвољну колону $k, m+k, 2m+k, \ldots, (n-1)m+k$ бројева узајамно простих са m. Бројеви ове колоне су облика $mi+k$, $i = 0, 1, \ldots, n-1$. Како је $(m, n) = 1$, према теореми 1.24 2°, бројеви ове колоне образују потпуни систем остатака по модулу n, па међу њима постоји тачно $\varphi(n)$ бројева узајамно простих са n.

Свака од $\varphi(m)$ колона бројева узајамно простих са m садржи $\varphi(n)$ бројева узајамно простих са n, па цела табела садржи $\varphi(m)\varphi(n)$ бројева узајамно простих и са m и са n, а тиме и са mn, чиме је доказано да је $\varphi(mn) = \varphi(m)\varphi(n)$. □

Теорема 1.28. *Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n, тада је*

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

Доказ. Претпоставимо најпре да број n има један прост делилац, тј. да је $n = p^\alpha$, за неки прост број p и неки природан број α. Међу природним бројевима од 1 до p^α има $p^{\alpha-1}$ бројева дељивих са p, тј. бројева који нису узајамно прости са p^α. То су бројеви $p, 2p, \ldots, p^\alpha$. Следи да је

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right). \tag{1.12}$$

Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, тада на основу (1.12) и претходне теореме добијамо

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})\\ &= p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)\\ &= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

□

ПРИМЕР 1.17. Доказати да је $\sum_{d|n} \varphi(d) = n$.

Решење. Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n. Тада се према теореми 1.14 произвољан делилац d броја n може написати у облику $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, при чему је $0 \leqslant \beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$. Због мултипликативности функције φ важи

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} \left(1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})\right). \tag{1.13}$$

Наиме, множењем фактора на десној страни релације (1.13) добијамо суму фактора облика $\varphi(p_1^{\beta_1})\varphi(p_2^{\beta_2}) \cdots \varphi(p_k^{\beta_k}) = \varphi\big(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\big)$, при чему је $0 \leqslant \beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$, а то је управо лева страна релације (1.13).

Сада је

$$\begin{aligned}\sum_{d|n} \varphi(d) &= \prod_{i=1}^{k} \left(1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})\right) \\ &= \prod_{i=1}^{k} p_i^{\alpha_i} = n.\end{aligned}$$

△

Теорема 1.29. (**Ојлер**) *Ако је* $(a, m) = 1$, *тада је* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказ. Нека је $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ сведени систем остатака по модулу m. Како је $(a, m) = 1$, то је и скуп $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ сведени систем остатака по модулу m. Дакле, за сваки елемент x_i првог скупа постоји тачно један елемент ax_j другог скупа, такав да је $x_i \equiv ax_j \pmod{m}$, па је

$$(ax_1)(ax_2) \cdots (ax_{\varphi(m)}) \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod{m},$$

тј.

$$a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)} \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod{m}. \tag{1.14}$$

Како бројеви $x_1, x_2, \ldots, x_{\varphi(m)}$ образују сведени систем остатака по модулу m, то је $(x_1 x_2 \cdots x_{\varphi(m)}, m) = 1$, па релација (1.14) након скраћивања постаје

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

□

Теорема 1.30. (**Мала Фермаова**[9] **теорема**) *Ако је p прост број и $p \nmid a$, онда је $a^{p-1} \equiv 1 \pmod{p}$.*

Доказ. Ако је p прост број и $p \nmid a$, тада је $(a, p) = 1$, па према Ојлеровој теореми важи да је $a^{\varphi(p)} \equiv 1 \pmod{p}$. За прост број p је $\varphi(p) = p - 1$, одакле следи тврђење. □

Последица 1.5. *Ако је p прост број и a произвољан цео број, тада је $a^p \equiv a \pmod{p}$.*

Доказ. Ако $p \nmid a$, тада је према претходној теореми $a^{p-1} \equiv 1 \pmod{p}$, одакле следи да је $a^p \equiv a \pmod{p}$. Ако $p \mid a$, тада $p \mid a^p - a$, тј. $a^p \equiv a \pmod{p}$. □

ПРИМЕР 1.18. Доказати да је број $2222^{5555} + 5555^{2222}$ дељив са 7.

Решење. Важи да је $2222 \equiv 3 (\mathrm{mod}\ 7)$ и $5555 \equiv 4 (\mathrm{mod}\ 7)$. Из услова $3^3 \equiv -1 (\mathrm{mod}\ 7)$ следи да је $3^6 \equiv 1 (\mathrm{mod}\ 7)$, па је

$$2222^{5555} \equiv 3^{5555} \equiv 3^{6 \cdot 925 + 5} \equiv 1^{925} \cdot 3^5 \equiv 3^3 \cdot 3^2 \equiv (-1) \cdot 9 \equiv 5 (\mathrm{mod}\ 7).$$

Аналогно се показује да је $4^3 \equiv 1 (\mathrm{mod}\ 7)$ и $5555^{2222} \equiv 2 (\mathrm{mod}\ 7)$, одакле следи да је

$$2222^{5555} + 5555^{2222} \equiv 0 (\mathrm{mod}\ 7),$$

односно $7 \mid 2222^{5555} + 5555^{2222}$. △

ПРИМЕР 1.19. Одредити две последње цифре броја 3^{400}.

Решење. Како је $\varphi(25) = 20$, следи да је $3^{20} \equiv 1 (\mathrm{mod}\ 25)$, па је $3^{400} \equiv 1 (\mathrm{mod}\ 25)$. Такође је $3^2 \equiv 1 (\mathrm{mod}\ 4)$, па је $3^{400} \equiv 1 (\mathrm{mod}\ 4)$. Дакле, $3^{400} \equiv 1 (\mathrm{mod}\ 100)$, па су последње две цифре 01. △

1.4.2 Поредак броја по датом модулу

Дефиниција 1.13. ***Поредак броја*** *a* ***по модулу*** *m је најмањи природан број t за који важи $a^t \equiv 1 \pmod{m}$.*

ПРИМЕР 1.20. Поредак броја 3 по модулу 11 је 5, јер $3^1, 3^2, 3^3, 3^4 \not\equiv 1 \pmod{11}$, а $3^5 \equiv 1 \pmod{11}$.

[9] Pierre de Fermat (1601–1665), француски математичар

На основу Ојлерове теореме закључујемо да поредак броја a по модулу m постоји ако су бројеви a и m узајамно прости. Међутим, важи и обрнуто. Наиме, ако је за неки природан број t испуњено $a^t \equiv 1(\mathrm{mod}\ m)$, тада је $a^t - mk = 1$, за неко $k \in \mathbb{Z}$, одакле следи да је $(a, m) = 1$.

Теорема 1.31. *Ако је t поредак броја a по модулу m и $a^s \equiv 1\,(\mathrm{mod}\ m)$, тада $t \mid s$. Специјално, $t \mid \varphi(m)$.*

Доказ. Претпоставимо да $t \nmid s$. Тада је $s = qt + r$, за неке целе бројеве q и r, такве да је $0 < r < t$, па је $a^s = a^{qt+r} = (a^t)^q \cdot a^r$. Имајући у виду да је $a^t \equiv 1(\mathrm{mod}\ m)$ и $a^s \equiv 1(\mathrm{mod}\ m)$, закључујемо да је $a^r \equiv 1(\mathrm{mod}\ m)$. Међутим, како је $0 < r < t$, ово је у супротности са чињеницом да је t најмањи природан број са особином $a^t \equiv 1(\mathrm{mod}\ m)$. □

Дефиниција 1.14. *Ако је поредак броја a по модулу m једнак $\varphi(m)$, број a се назива* ***примитиван корен по модулу*** *m.*

Теорема 1.32. *Ако је a примитиван корен по модулу m, тада бројеви*

$$1 = a^0, a^1, \ldots, a^{\varphi(m)-1}$$

образују сведени систем остатака по модулу m.

Доказ. Како је a примитиван корен по модулу m, следи да је $(a, m) = 1$, одакле следи да је $(a^i, m) = 1$, за свако $i = 0, 1, \ldots, \varphi(m) - 1$. Осим тога, наведених бројева има тачно $\varphi(m)$, па је довољно доказати да међу њима не постоје два која су конгруентна по модулу m. Претпоставимо супротно, да постоје i и j, $0 \leqslant i < j < \varphi(m)$, такви да је $a^i \equiv a^j\ (\mathrm{mod}\ m)$. Тада је $a^{j-i} \equiv 1(\mathrm{mod}\ m)$, при чему је $0 < j - i < \varphi(m)$, што је супротно претпоставци да је a примитиван корен по модулу m. □

Последица 1.6. *Ако је p прост број и a примитиван корен по модулу p, тада бројеви $1, a, \ldots, a^{p-2}$ образују сведени систем остатака по модулу p.*

Теорема 1.33. (**Вилсон**[10]) *Ако је p прост број, тада је $(p-1)! \equiv -1(\mathrm{mod}\ p)$.*

Доказ. Тврђење очигледно важи за $p = 2$ и $p = 3$. Претпоставимо да је p прост број већи од 3. Важи да је $1 \equiv 1(\mathrm{mod}\ p)$ и $p - 1 \equiv -1(\mathrm{mod}\ p)$. Доказаћемо да је могуће груписати елементе скупа $A = \{2, 3, \ldots, p-2\}$ у парове (i, j) за које важи $i \cdot j \equiv 1(\mathrm{mod}\ p)$, односно доказаћемо да за

[10] John Wilson (1741–1793), енглески математичар

сваки број $i \in A$ постоји тачно један број $j \in A$, $j \neq i$, такав да је $i \cdot j \equiv 1 (\mathrm{mod}\ p)$.

Имајући у виду да је $2 \leqslant i \leqslant p-2$, при чему је p прост број, закључујемо да је $(i,p) = 1$, одакле, према теореми 1.24, следи да је скуп $\{0, i, 2i, \ldots, (p-1)i\}$ потпуни систем остатака по модулу p, па је тачно један елемент овог скупа (који је различит од 0) конгруентан са 1 по модулу p. Нека је то елемент $j \cdot i$, $1 \leqslant j \leqslant p-1$.

Ако би било $j = 1$, тада је $i \equiv 1 (\mathrm{mod}\ p)$, што је немогуће. Аналогно, не може бити ни $j = p-1$.

Докажимо још да је $j \neq i$. У супротном, важи да је $i^2 \equiv 1 (\mathrm{mod}\ p)$, тј. $p \mid (i-1)(i+1)$. Како је p прост број, следи да $p \mid i-1$ или $p \mid i+1$, што је немогуће, јер је $2 \leqslant i \leqslant p-2$. □

Важи и обрнуто тврђење Вилсонове теореме.

Теорема 1.34. *Ако је* $(p-1)! \equiv -1 (\mathrm{mod}\ p)$, *тада је* p *прост број.*

Доказ. Ако би p био сложен број, тада би p имао делилац q, такав да је $1 < q < p$, одакле следи да $q \mid (p-1)!$, па $q \nmid (p-1)! + 1$, а самим тим и $p \nmid (p-1)! + 1$. Контрадикција. □

ПРИМЕР 1.21. Нека је p прост број. Тада конгруенција $x^2 \equiv -1 (\mathrm{mod}\ p)$ има решење ако и само ако је $p = 2$ или $p \equiv 1 (\mathrm{mod}\ 4)$. Доказати.

Решење. Ако је $p = 2$, тада је $x = 1$ једно решење. Ако је $p \equiv 1 (\mathrm{mod}\ 4)$, тада на основу Вилсонове теореме важи

$$1 \cdot 2 \cdots \frac{p-1}{2} \cdot (p-1)(p-2) \cdots \left(p - \frac{p-1}{2}\right) \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 (\mathrm{mod}\ p)$$
$$\equiv -1 (\mathrm{mod}\ p),$$

па је $x = \left(\frac{p-1}{2}\right)!$ једно решење.

Нека је $p \equiv 3 \,(\mathrm{mod}\ 4)$. Претпоставимо да постоји цео број x, такав да је $x^2 \equiv -1 (\mathrm{mod}\ p)$. Тада је $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$, што је у супротности са теоремом 1.30. △

1.4.3 Критеријуми дељивости - Паскалов метод

Применом теорије конгруенција могу се добити неки критеријуми дељивости. Како се сваки природан број може представити у облику

производа степена простих бројева, од интереса је одредити критеријуме дељивости степенима простих бројева.

Један од начина добијања критеријума дељивости је тзв. ***Паскалов***[11] ***метод***.

Теорема 1.35. *Број* $a = \overline{a_n a_{n-1} \cdots a_1 a_0} = \sum_{i=0}^{n} a_i \cdot 10^i$ *је дељив природним бројем* m *ако и само ако је са* m *дељив збир* $\sum_{i=0}^{n} a_i r_i$, *где су* r_i *цели бројеви за које важи* $10^i \equiv r_i \pmod{m}$, $i = 0, 1, \ldots, m$.

Доказ. Користећи особине конгруенција добијамо

$$a = \overline{a_n a_{n-1} \cdots a_1 a_0} = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i r_i \pmod{m},$$

одакле следи тврђење. □

Бирајући на одговарајуће начине бројеве r_i, добијају се различити критеријуми дељивости.

Последица 1.7. *Број* $a = \overline{a_n a_{n-1} \cdots a_1 a_0}$ *је дељив са* 2^t (*односно са* 5^t) *ако и само ако је са* 2^t (*односно са* 5^t) *дељив број* $\overline{a_{t-1} \ldots a_1 a_0}$, *где је* t *произвољан природан број.*

Доказ. Довољно је у теореми 1.35 узети $r_i = 10^i$ за $i = 0, 1, \ldots, t-1$ и $r_i = 0$ за $i \geqslant t$. □

Применом последице 1.7 добијамо познате критеријуме дељивости са 2, 5, 4, 25, 8, 125, итд. Број је дељив са 2 (односно са 5) ако се завршава неком од цифара $0, 2, 4, 6, 8$ (односно са 0 или 5); број је дељив са $4 = 2^2$ (односно са $25 = 5^2$) ако је његов двоцифрени завршетак дељив са 4 (са 25), итд.

Последица 1.8. *Нека је* t *природан број, такав да је* $10^t \equiv 1 \pmod{m}$. *Број* $a = \overline{a_n a_{n-1} \cdots a_1 a_0}$ *је дељив природним бројем* m *ако и само ако је са* m *дељив збир бројева који се добијају поделом здесна налево броја* a *на групе по* t *цифара.*

Доказ. У теореми 1.35 треба узети да је $r_i = 10^i$, за $i = 0, 1, \ldots, t-1$ и $r_{tq+i} = 10^i$, $q \in \mathbb{N}$, јер је $10^{tq+i} \equiv 10^i \pmod{m}$. □

[11] Blaise Pascal (1623–1662), француски математичар

Специјално, одавде добијамо критеријуме дељивости са 3, 9 и 11.

$$\begin{aligned}
3 \mid a &= \sum_{i=0}^{n} a_i \cdot 10^i \iff 3 \mid \sum_{i=0}^{n} a_i \qquad (t=1),\\
9 \mid a &= \sum_{i=0}^{n} a_i \cdot 10^i \iff 9 \mid \sum_{i=0}^{n} a_i \qquad (t=1),\\
11 \mid a &= \sum_{i=0}^{n} b_i \cdot 100^i \iff 11 \mid \sum_{i=0}^{n} b_i \qquad (t=2).
\end{aligned}$$

ПРИМЕР 1.22. $11 \mid 276507$, јер $11 \mid 99 = 7 + 65 + 27$.

Последица 1.9. *Нека је t природан број, такав да је $10^t \equiv -1 \pmod{m}$. Број $a = \overline{a_n a_{n-1} \cdots a_1 a_0}$ је дељив природним бројем m ако и само ако је са m дељив збир бројева који се добијају поделом здесна налево броја a на групе по t цифара, при чему им се наизменично промени знак.*

Доказ. У теореми 1.35 треба узети да је $r_i = 10^i$, $i = 0, 1, \ldots, t-1$, затим $r_{t+i} = -10^i$, $i = 0, 1, \ldots, t-1$, па онда опет $r_{2t+i} = 10^i$, $i = 0, 1, \ldots, t-1$, тј. $r_{tq+i} = (-1)^q \cdot 10^i$, $i = 0, 1, \ldots, t-1$, $q \in \mathbb{N}$. □

Специјално,

$$\begin{aligned}
11 \mid a &= \sum_{i=0}^{n} a_i \cdot 10^i \iff 11 \mid \sum_{i=0}^{n} (-1)^i a_i \qquad (t=1),\\
101 \mid a &= \sum_{i=0}^{n} b_i \cdot 100^i \iff 101 \mid \sum_{i=0}^{n} (-1)^i b_i \qquad (t=2),\\
7 \mid a &= \sum_{i=0}^{n} c_i \cdot 1000^i \iff 7 \mid \sum_{i=0}^{n} (-1)^i c_i \qquad (t=3),\\
13 \mid a &= \sum_{i=0}^{n} c_i \cdot 1000^i \iff 13 \mid \sum_{i=0}^{n} (-1)^i c_i \qquad (t=3).
\end{aligned}$$

ПРИМЕР 1.23. $11 \mid 2843269$, јер је $9-6+2-3+4-8+2 = 0 \equiv 0 \pmod{11}$.

ПРИМЕР 1.24. $101 \mid 604307947$, јер је $47 - 79 + 30 - 4 + 6 = 0 \equiv 0 \pmod{101}$.

ПРИМЕР 1.25. $7 \mid 2232706$, јер је $706 - 232 + 2 = 476 \equiv 0 \pmod{7}$.

ПРИМЕР 1.26. $13 \mid 7057219$, јер је $219 - 57 + 7 = 169 \equiv 0 \pmod{13}$.

ПРИМЕР 1.27. Одредити све троцифрене бројеве који су 5 пута већи од производа својих цифара.

Решење. Тражени број $\overline{abc}$ задовољава услов $\overline{abc} = 5abc$, тј. дељив је са 5, одакле следи да $c \in \{0, 5\}$. У случају да је $c = 0$, производ abc једнак је 0, што је немогуће, па је $c = 5$. Сада је $\overline{ab5} = 25ab$, тј. број $\overline{ab5}$ је дељив са 25, одакле следи да $b \in \{2, 7\}$. У случају да је $b = 2$ добијамо да је $\overline{a25} = 50a$, што је немогуће, јер је у овом случају последња цифра c једнака 0. Дакле, мора бити $b = 7$, одакле непосредно произилази да је $a = 1$, тј. тражени број је 175. △

ПРИМЕР 1.28. Одредити цифре a и b тако да је број $n = \overline{a1995} + \overline{1995b}$ дељив са 44.

Решење. Како је $44 = 4 \cdot 11$ и $(4, 11) = 1$, закључујемо да број n мора бити дељив са 4 и са 11. Како је $\overline{a1995} \equiv 3 \pmod 4$, следи да мора бити $\overline{1995b} \equiv 1 \pmod 4$, одакле произилази да $b \in \{3, 7\}$.

Претпоставимо најпре да је $b = 3$. Тада је $19953 \equiv 10 \pmod{11}$, па мора бити $\overline{a1995} \equiv 1 \pmod{11}$, одакле следи да је $a + 4 \equiv 1 \pmod{11}$, тј. $a = 8$.

Нека је сада $b = 7$. Слично као у претходном случају закључује се да мора бити $a = 4$. △

1.4.4 Неке примене конгруенција

Теорија конгруенција има различите и занимљиве примене, како у математици, тако и у другим областима. Размотрићемо примену конгруенција за једнозначно означавање књига, као и за прављење распореда учесника одређених турнира.

Означавање књига

Свака књига је једнозначно одређена својим ISBN бројем (*International Standard Book Number*) који представља низ од 10 цифара, $a_1, a_2, \ldots, a_{10}$ (нпр. $86 - 18 - 12341 - 8$), подељених у четири групе, од којих прва означава где је књига издата, друга издавача, а трећа наслов и редни број издања. Последња цифра, a_{10}, назива се контролна цифра и она се одређује на основу претходних девет цифара коришћењем релације

$$a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \pmod{11},$$

при чему се у случају да је $a_{10} \equiv 10 \pmod{11}$ на последњу позицију уписује X. Контролна цифра је уведена у циљу корекције грешака које настају при преписивању ISBN бројева, било заменом места две цифре или погрешним преписивањем неке од цифара.

Показаћемо како се применом конгруенција и коришћењем контролне цифре може проверити да ли је написани ISBN број исправан. Претпоставимо да је низ $b_1, b_2, \ldots, b_{10}$ добијен преписивањем ISBN броја формираног од цифара $a_1, a_2, \ldots, a_{10}$, при чему је тачно једна од цифара a_k погрешно преписана. Дакле, важи да је $a_k \neq b_k$, док је $a_i = b_i$ за $i \neq k$. У овом случају низ састављен од цифара $b_1, b_2, \ldots, b_{10}$ не представља исправан ISBN број, што произилази из следећег разматрања.

Конгруенција $a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \pmod{11}$ еквивалентна је са $\sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11}$, одакле произилази да је

$$\sum_{i=1}^{10} i \cdot b_i \equiv \sum_{i=1}^{10} i \cdot b_i - \sum_{i=1}^{10} i \cdot a_i \pmod{11}.$$

Последња конгруенција је еквивалентна са $\sum_{i=1}^{10} i \cdot b_i \equiv k\,(b_k - a_k) \pmod{11}$. Како је $b_k \neq a_k$, десна страна последње конгруенције не може бити једнака нули, одакле следи да низ $b_1, b_2, \ldots, b_{10}$ не представља исправан ISBN број.

Једноставно се показује да аналогно важи и у случају када је низ $b_1, b_2, \ldots, b_{10}$ добијен заменом места две цифре исправног ISBN броја.

Распоред турнира

Конгруенције се могу применити при састављању распореда турнира на коме учествује n играча, при чему сваки од играча одиграва тачно један меч против сваког од преосталих учесника турнира. Ако је n паран број, овакав турнир се састоји од укупно $n - 1$ кола, тако да сваки од играча има меч у сваком колу. Уколико је n непаран број, тада се у сваком колу састаје $\frac{n-1}{2}$ парова, па један играч мора бити слободан. У том случају додајемо још једног, фиктивног играча, па можемо претпоставити да је n паран број. Играч који се састаје са фиктивним играчем је у ствари у том колу слободан. У овом случају турнир се састоји од n кола.

Нека су играчи означени бројевима $1, 2, \ldots, n$, при чему у k-том колу, $k = 1, 2, \ldots, n-1$, играчи x и y, $1 \leqslant x, y \leqslant n-1$, $x \neq y$, играју међусобно

ако је $x + y \equiv k \pmod{n-1}$. Уколико је $x + x \equiv k \pmod{n-1}$, тада играч x игра са играчем n.

Наведеним распоредом играча на турниру, ниједан играч неће играти више од једанпут у истом колу, јер из услова $x + y \equiv x + z \pmod{n-1}$ следи да је $y \equiv z \pmod{n-1}$, односно $y = z$, с обзиром на чињеницу да $1 \leqslant y, z \leqslant n-1$. Осим тога, ни у једном од $n-1$ кола не долази до понављања сусрета, јер из услова $x + y \equiv k \pmod{n-1}$ и $x + y \equiv k' \pmod{n-1}$, следи да је $k = k'$, јер важи $1 \leqslant k, k' \leqslant n-1$.

ПРИМЕР 1.29. Распоред турнира са 6 играча представљен је следећом табелом.

Коло	Сусрети
1	$1-5, 2-4, 3-6$
2	$1-6, 2-5, 3-4$
3	$1-2, 4-6, 3-5$
4	$1-3, 2-6, 4-5$
5	$1-4, 2-3, 5-6$

Глава 2

Комбинаторика

2.1 Увод

Комбинаторика је област математике која се бави питањима распоређивања објеката дефинисаних на коначним или пребројивим скуповима. Ова математичка дисциплина почиње да се развија у XVII веку, упоредо са настанком теорије вероватноће, када су први комбинаторни проблеми били везани за игре на срећу. Комбинаторика се током историје развијала заједно са другим областима математике, прожимајући се са њима. Данас се комбинаторне методе користе у алгебри, теорији бројева, геометрији, топологији, анализи, теорији вероватноће, математичкој статистици, рачунарству, као и у многим другим областима.

Различити проблеми који се проучавају у оквиру комбинаторике могу бити разврстани у три основне групе:

- проблеми *егзистенције* комбинаторних објеката са унапред утврђеним особинама,
- проблеми енумерације, тј. *пребројавања* објеката са задатим својствима,
- проблеми *генерисања*, односно конструкције комбинаторних објеката са утврђеним особинама.

Посебно је значајан део комбинаторике који се бави проблемима пребројавања у циљу решавања различитих проблема, као што је, на пример, проблем одређивања броја различитих телефонских бројева,

одређивање сложености алгоритама или утврђивање вероватноће случајних догађаја. Због тога је веома значајно проналажење ефикасних метода за пребројавање, пре свега, коначних скупова. Приликом решавања проблема пребројавања користе се четири елементарна принципа.

Принцип 1. (**принцип једнакости**) Два коначна непразна скупа A и B имају једнак број елемената, тј. важи да је $|A| = |B|$, ако постоји бијекција $f : A \to B$.

Принцип 2. (**принцип већег броја**) Нека су A и B коначни скупови и $f : A \to B$ функција, таква да за сваки елемент $b \in B$ постоји тачно k елемената $a \in A$ чије су слике при пресликавању f једнаке елементу b, тј. $|\{a \mid a \in A, f(a) = b\}| = k$. Тада је $|A| = k|B|$.

Принцип 3. (**принцип збира**) Ако су A и B коначни дисјунктни скупови, тада је $|A \cup B| = |A| + |B|$.

Овај принцип се може уопштити и на унију призвољног броја дисјунктних коначних скупова $A_1, A_2, \ldots, A_n$, тј. важи

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Принцип 4. (**принцип производа**) Ако су A и B коначни скупови, тада је $|A \times B| = |A| \cdot |B|$, при чему је $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Према наведеном принципу пребројавања, број начина да се изабере један елемент из скупа A и један елемент из скупа B једнак је $|A| \cdot |B|$. Овај принцип се може проширити на производ произвољног броја коначних скупова $A_1, A_2, \ldots, A_n$, тј. важи да је

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

ПРИМЕР 2.1. На полици се налази 5 различитих књига из математике, 3 различите књиге из физике и 2 из хемије. Ако је потребно одабрати једну књигу са полице, колико различитих избора постоји?

Решење. Означимо са M, F и H скуп књига из математике, физике и хемије, респективно. Бирамо књигу из скупа $M \cup F \cup H$. Како су ови скупови међусобно дисјунктни, према принципу збира различитих избора има $|M| + |F| + |H| = 5 + 3 + 2 = 10$. △

ПРИМЕР 2.2. Шифра се састоји од 4 симбола, од којих су прва два слова азбуке, а преостала два су цифре. Колико таквих различитих шифри постоји?

Решење. Избор сваког од слова може се извршити на 30 начина, а сваке од цифара на 10 начина, па је према принципу производа број различитих шифри једнак $30 \cdot 30 \cdot 10 \cdot 10 = 90000$. △

Осим четири наведена основна принципа, приликом пребројавања различитих комбинаторних објеката користи се и **Дирихлеов принцип**. Овај принцип је у литератури на енглеском језику познат као *The Pigeonhole Principle*, јер у својој оригиналној верзији тврди да ако је јато голубова потребно сместити у голубарник, при чему има више голубова него кућица у голубарнику, тада ће се бар у једној кућици наћи бар два голуба. Овај принцип може се исказати на следећи начин.

Теорема 2.1. (**Дирихлеов принцип**) *Ако је $n+1$ или више објеката смештено у n кутија, тада се бар у једној кутији налазе бар два објекта.*

Доказ. Ако свака кутија садржи највише један објекат, тада је укупан број објеката највише n, супротно претпоставци да има најмање $n+1$ објеката. □

ПРИМЕР 2.3. На основу Дирихлеовог принципа важе тврђења:

- у сваком скупу од 8 или више особа, постоје бар две које су рођене истог дана у недељи,
- у сваком скупу од 367 или више особа постоје бар две које славе рођендан истог дана,
- од 6 природних бројева бар два имају исти остатак при дељењу са 5.

ПРИМЕР 2.4. Доказати да постоји број чије цифре припадају скупу $\{0, 1\}$, који нема више од 17 цифара и који је дељив са 17.

Решење. Ако ниједан од 17 бројева $1, 11, 111, \ldots, \underbrace{11\ldots1}_{17}$ није дељив са 17, тада бар два од њих дају исти остатак при дељењу са 17. Разлика та два броја је број записан помоћу цифара 0 и 1, дељив је са 17 и нема више од 17 цифара. △

ПРИМЕР 2.5. Цео лист папира школске свеске обојен је помоћу две боје. Доказати да постоје две тачке тог папира које су исте боје и чије је растојање 3 cm.

Решење. Ако конструишемо на том папиру једнакостранични троугао странице 3 cm, бар два његова темена ће бити исте боје. △

Осим Дирихлеовог принципа, при решавању комбинаторних задатака користи се и његово уопштење.

Теорема 2.2. (**Уопштени Дирихлеов принцип**) *Ако је m објеката смештено у n кутија, при чему је $m > nr$, $r \in \mathbb{N}$, тада се бар у једној кутији налази бар $r+1$ објеката.*

ПРИМЕР 2.6. У једној школи има 1000 ученика. Доказати да у тој школи постоје или 32 ученика из истог одељења или 33 ученика из различитих одељења.

Решење. Ако не постоје 32 ученика из истог одељења, следи да сва одељења имају највише по 31 ученика. Како је $1000 = 31 \cdot 32 + 8$, у школи постоје бар 33 одељења, а тиме и 33 ученика из различитих одељења. △

Два скупа су једнака ако садрже исте елементе, одакле следи да није могуће разликовати скупове у којима је неки елемент наведен једанпут или више пута, на пример скупове $\{a, a, b, c, c, d\}$ и $\{a, b, c, d\}$. У комбинаторици је често потребно посматрати колекције објеката међу којима има и једнаких. Таква колекција објеката назива се **фамилија** или **мултискуп**.

Дефиниција 2.1. *Пресликавање $\phi : X \to \mathbb{N}_0$ назива се **фамилија** елемената скупа X.*

Према претходној дефиницији фамилије, $\phi(x)$ представља број, тј. **вишеструкост** појављивања произвољног елемента $x \in X$ у фамилији. Две фамилије су једнаке ако и само ако имају исте елементе и вишеструкости појављивања истих елемената су једнаке. За неку фамилију каже се да је **подфамилија** дате фамилије ако вишеструкости појављивања сваког њеног елемента нису веће од вишеструкости појављивања тог елемента у полазној фамилији. Број елемената неке фамилије скупа X једнак је збиру вишеструкости свих елемената скупа X.

ПРИМЕР 2.7. Нека је $X = \{a, b, c, d, e\}$. Тада је пресликавање

$$\phi = \begin{pmatrix} a & b & c & d & e \\ 2 & 0 & 3 & 1 & 1 \end{pmatrix}$$

једна фамилија скупа X коју можемо означити са $\{a, a, c, c, c, d, e\}$ или $\{2a, 3c, 1d, 1e\}$. Елементи a, b, c, d, e скупа X се у фамилији појављују,

редом, $2, 0, 3, 1, 1$ пута, одакле следи да ова фамилија има $2 + 0 + 3 + 1 + 1 = 7$ елемената. Фамилије $\{a, c, c, c, d\}$ и $\{c, d, e\}$ су две произвољне подфамилије дате фамилије.

Осим пребројавања комбинаторних објеката са одређеним својствима, често је потребно и генерисати све такве објекте. У циљу ефикасног решавања тог проблема, како би се избегло да се поједини објекти изоставе или понове више пута, потребно је у скупу свих комбинаторних објеката одређеног типа дефинисати поредак којим ће они бити уређени. Основни поредак у комбинаторици заснива се на тзв. лексикографском уређењу које се често користи и у свакодневном животу, нпр. при формирању речника страних речи, телефонских именика и слично.

Дефиниција 2.2. *Нека је $X = \{x_1, x_2, \ldots, x_n\}$ скуп од n елемената потпуно уређен релацијом $\prec$ и нека је $x_1 \prec x_2 \prec \cdots \prec x_n$. Кажемо да су две k-торке $(a_1, a_2, \ldots, a_k)$, $(b_1, b_2, \ldots, b_k) \in X^k$ у релацији $\preceq$ и пишемо $(a_1, a_2, \ldots, a_k) \preceq (b_1, b_2, \ldots, b_k)$, ако и само ако је $a_1 = b_1, a_2 = b_2, \ldots, a_k = b_k$ или је $a_1 = b_1, a_2 = b_2, \ldots, a_s = b_s$ и $a_{s+1} \prec b_{s+1}$, за неко s, $0 \leqslant s \leqslant k - 1$.*

Релација $\preceq$ уведена претходном дефиницијом представља релацију **лексикографског поретка** (**уређења**) на скупу X^k свих k-торки (тј. речи дужине k) формираних од елемената скупа X. Ова релација је релација потпуног поретка на скупу X^k, односно рефлексивна је, антисиметрична и транзитивна и притом су свака два елемента из скупа X^k упоредива у односу на ову релацију. Ова релација је специјалан случај релације лексикографског поретка дефинисане у скупу свих речи произвољне дужине на следећи начин.

Дефиниција 2.3. *Нека је $X = \{x_1, x_2, \ldots, x_n\}$ скуп од n елемената потпуно уређен релацијом $\prec$ тако да је $x_1 \prec x_2 \prec \cdots \prec x_n$, и нека је $\mathbb{X} = \bigcup_{k=1}^{+\infty} X^k$.*

Кажемо да су k-торка $(a_1, a_2, \ldots, a_k)$ и ℓ-торка $(b_1, b_2, \ldots, b_\ell)$ из скупа $\mathbb{X}$ у релацији $\preceq$ и пишемо $(a_1, a_2, \ldots, a_k) \preceq (b_1, b_2, \ldots, b_l)$, ако и само ако је $a_1 = b_1, a_2 = b_2, \ldots, a_k = b_k$, при чему је $k \leqslant \ell$, или је $a_1 = b_1, a_2 = b_2, \ldots, a_s = b_s$ и $a_{s+1} \prec b_{s+1}$, за неко s, $0 \leqslant s < \min\{k, \ell\}$.

Једноставно се проверава да је релација $\preceq$ уведена претходном дефиницијом релација потпуног поретка на скупу $\mathbb{X}$.

2.2 Варијације, пермутације, комбинације

Нека је дат скуп $A_n = \{a_1, a_2, \ldots, a_n\}$.

2.2.1 Варијације (без понављања)

Дефиниција 2.4. ***Варијација*** *k-те класе (без понављања) скупа A_n је свака уређена k-торка различитих елемената скупа A_n.*

Варијација (без понављања) може се дефинисати и на следећи еквивалентан начин.

Дефиниција 2.5. *Варијација k-те класе (без понављања) скупа A_n је свако $1-1$ пресликавање скупа $\{1, 2, \ldots, k\}$ у скуп A_n.*

ПРИМЕР 2.8. Нека је дат скуп $\{a, b, c, d\}$. Све варијације (без понављања) друге класе посматраног скупа су

$$\begin{array}{cccc} ab & ba & ca & da \\ ac & bc & cb & db \\ ad & bd & cd & dc, \end{array}$$

а све варијације (без понављања) треће класе овог скупа су

$$\begin{array}{cccc} abc & bac & cab & dab \\ abd & bad & cad & dac \\ acb & bca & cba & dba \\ acd & bcd & cbd & dbc \\ adb & bda & cda & dca \\ adc & bdc & cdb & dcb. \end{array}$$

При навођењу варијација уређени пар (a, b) означили смо са ab, а уређену тројку (a, b, c) са abc. Аналогно смо поступили при навођењу преосталих уређених парова, односно уређених тројки формираних од елемената скупа $\{a, b, c, d\}$. Осим тога, приликом навођења варијација у претходном примеру водили смо рачуна о лексикографском поретку, при чему је за поредак елемената скупа $\{a, b, c, d\}$ узет одговарајући абецедни редослед ових слова, тј. $a \prec b \prec c \prec d$.

Означимо са V_n^k број варијација (без понављања) k-те класе скупа од n елемената.

Теорема 2.3. *Важи да је*

$$V_n^k = n(n-1)\cdots(n-k+1). \tag{2.1}$$

Доказ. Број варијација k-те класе скупа од n елемената једнак је према дефиницији 2.4 броју уређених k-торки формираних од различитих елемената посматраног скупа. Избор прве координате k-торке може се извршити на n начина, јер се на овој позицији може наћи било који од n елемената полазног скупа. Другу координату k-торке сада можемо попунити на $n-1$ начина, тј. било којим елементом посматраног скупа, осим елементом изабраним за прву координату. Аналогно, закључујемо да је трећу координату могуће попунити на $n-2$ начина, ..., k-ту координату можемо попунити на $n-k+1$ начина. Према принципу производа следи да је укупан број начина да попунимо свих k координата, а тиме и број варијација (без понављања) k-те класе скупа од n елементата дат формулом (2.1). □

Пример 2.9. На основу формуле (2.1) следи да је $V_4^2 = 4 \cdot 3 = 12$ и $V_4^3 = 4 \cdot 3 \cdot 2 = 24$, као што је приказано у примеру 2.8.

Пример 2.10. У радњи постоји n различитих врста разгледница које треба послати пријатељима, којих има k, $n \geqslant k$. На колико начина је могуће послати разгледнице, тачно по једну сваком пријатељу, ако сваком пријатељу треба послати различиту разгледницу?

Решење. Од n врста разгледница потребно је изабрати k различитих врста које ће бити послате пријатељима. Ово се може учинити на $V_n^k = n(n-1)\cdots(n-k+1)$ начина. △

2.2.2 Пермутације (без понављања)

Дефиниција 2.6. ***Пермутација*** *(без понављања) скупа A_n је свака уређена n-торка различитих елемената скупа A_n.*

Пермутација скупа A_n је у ствари варијација (без понављања) n-те класе тог скупа. Према дефиницији 2.5 пермутација скупа A_n је свако $1-1$ пресликавање скупа $\{1, 2, \ldots, n\}$ у скуп A_n. Како ови скупови имају исти број елемената, ово пресликавање је бијекција. Пермутација се може дефинисати и као произвољна бијекција скупа A_n у самог себе.

Број пермутација (без понављања) скупа од n елемената означава се са P_n и једнак је, према формули (2.1),

$$P_n = V_n^n = n(n-1)\cdots 2 \cdot 1 = n!\,.$$

ПРИМЕР 2.11. Све пермутације (без понављања) скупа $\{a, b, c, d\}$ дате у лексикографском поретку су

$$\begin{array}{cccc} abcd & bacd & cabd & dabc \\ abdc & badc & cadb & dacb \\ acbd & bcad & cbad & dbac \\ acdb & bcda & cbda & dbca \\ adbc & bdac & cdab & dcab \\ adcb & bdca & cdba & dcba. \end{array}$$

Њихов укупан број је $P_4 = 4! = 24$.

ПРИМЕР 2.12. Одредити 92. пермутацију у лексикографском поретку скупа $\{a, b, c, d, e\}$.

Решење. Тражена пермутација је $deacb$. Наиме, постоји тачно $4! = 24$ пермутација које почињу сваким од елемената a, b, c, d, e. Како је $92 = 3 \cdot 24 + 20$ тражена пермутација почиње словом d. Пермутација код којих су два почетна елемента фиксирана има $3! = 6$. Како је $20 = 3 \cdot 6 + 2$, водећи рачуна о лексикографском поретку, закључујемо да тражена пермутација почиње са de. Како пермутација са 3 фиксирана почетна елемента има $2! = 2$ и $2 = 1 \cdot 2$, закључујемо да је тражена 92. пермутација посматраног скупа у лексикографском поретку дата са $deacb$. △

ПРИМЕР 2.13. Колико има пермутација скупа $\{1, 2, \ldots, 10\}$ у којима су елементи 3 и 4 суседни?

Решење. Како су бројеви 3 и 4 суседни, њих можемо посматрати као један блок (елемент) који заједно са преосталих 8 елемената скупа $\{1, 2, \ldots, 10\}$ можемо пермутовати на $9!$ начина. Бројеве 3 и 4 можемо међусобно пермутовати на $2!$ начина, па је тражени број пермутација једнак $2 \cdot 9!$. △

ПРИМЕР 2.14. На колико начина се бројеви $1, 2, \ldots, 3n$ могу поређати у низ, тако да сваки број стоји на месту чији редни број при дељењу са 3 даје исти остатак као и сам тај број?

Решење. Бројеве $\{1, 2, \ldots, 3n\}$ можемо поделити у три групе од по n бројева који при дељењу са 3 дају исти остатак, а затим бројеве из сваке од група распоређујемо на неко од n места чији редни број при дељењу са 3 даје исти остатак као сваки број посматране групе. Како се n бројева унутар групе могу распоредити на n места одговарајућих за ту групу на $n!$ начина, према принципу производа бројеве из све три групе можемо распоредити на $(n!)^3$ начина. △

2.2.3 Комбинације (без понављања)

Пре него што дефинишемо комбинације без понављања, дефинисаћемо најпре биномне коефицијенте.

Дефиниција 2.7. *Нека су $n \geqslant k \geqslant 0$ цели бројеви.* ***Биномни коефицијент*** $\binom{n}{k}$ *је број*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Из дефиниције биномних коефицијената следи да је $\binom{n}{k} = \binom{n}{n-k}$, тј. симетрични биномни коефицијенти су међусобно једнаки. О биномним коефицијентима и њиховим особинама биће више речи у одељку 2.3.

Дефиниција 2.8. ***Комбинација*** *(без понављања) k-те класе скупа A_n је сваки његов подскуп који садржи k елемената.*

Према претходној дефиницији, комбинације су, за разлику од варијација и пермутација, неуређени избори елемената, тј. редослед елемената у комбинацији није битан. Ипак, приликом генерисања свих комбинација k-те класе скупа A_n пожељно је водити рачуна о лексикографском поретку, како неке комбинације не би изоставили, а неке навели више пута.

ПРИМЕР 2.15. Нека је дат скуп $A_5 = \{a, b, c, d, e\}$. Све комбинације (без понављања) друге класе су

$$\begin{array}{llll} ab & bc & cd & de, \\ ac & bd & ce & \\ ad & be & & \\ ae & & & \end{array}$$

а све комбинације (без понављања) треће класе су

$$\begin{array}{lll} abc & bcd & cde. \\ abd & bce & \\ abe & bde & \\ acd & & \\ ace & & \\ ade & & \end{array}$$

Означимо са C_n^k број комбинација (без понављања) k-те класе скупа од n елемената.

Теорема 2.4. *Важи да је*

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

Доказ. Ову теорему ћемо доказати на два начина.

Први начин. Варијације k-те класе скупа A_n могу се формирати тако што се најпре образују све комбинације k-те класе скупа A_n, а затим се од сваке добијене комбинације формирају све њене permутације. На тај начин је успостављена веза између permутација, варијација и комбинација, која се може изразити релацијом

$$V_n^k = C_n^k \cdot P_k\,,$$

одакле је

$$C_n^k = \frac{V_n^k}{P_k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \binom{n}{k}\,.$$

Други начин. Означимо са A скуп свих permутација (без понављања) скупа A_n, а са B скуп свих комбинација (без понављања) k-те класе скупа A_n. Тада је $|A| = n!$ и $|B| = C_n^k$. Претпоставимо да су елементи скупова A и B уређени лексикографски. Нека је $f : A \to B$ пресликавање које сваку permутацију скупа A пресликава у ону комбинацију k-те класе скупа B која се добије тако што се узме првих k елемената те permутације. Permутовање првих k елемената permутације, као ни permутовање последњих $n-k$ елемената permутације, не доводи до промене комбинације. На пример, за $n = 4$, $k = 2$ и $A_4 = \{a, b, c, d\}$, свака од permутација $abcd$, $bacd$, $abdc$ и $badc$ скупа A пресликава се у исту комбинацију ab скупа B. Према принципу производа следи да се укупно $k!(n-k)!$ permутација скупа A пресликава у исту комбинацију k-те класе скупа B, одакле, према принципу већег броја, произилази да је $|A| = k!(n-k)!|B|$, тј. $n! = k!(n-k)!C_n^k$, односно

$$C_n^k = \frac{n!}{k!(n-k)!} = \binom{n}{k}\,.$$

□

ПРИМЕР 2.16. Укупан број комбинација (без понављања) друге класе скупа $\{a, b, c, d, e\}$ једнак је $C_5^2 = \binom{5}{2} = 10$, као што је приказано у примеру 2.15.

ПРИМЕР 2.17. У равни је дато $n \geqslant 3$ тачака, тако да никоје три од тих тачака не припадају истој правој. Колико је правих одређено датим тачкама?

Решење. Како сваке две различите тачке одређују једну праву и не постоји тројка колинеарних тачака, укупан број правих одређених са датих n тачака једнак је $C_n^2 = \binom{n}{2}$. △

ПРИМЕР 2.18. На колико начина се од 6 људи може саставити 5 трочланих комисија, тако да никоје две од тих 5 комисија нису истог састава?

Решење. Од 6 људи могуће је саставити $\binom{6}{3} = 20$ трочланих комисија. Од 20 комисија може се изабрати 5 комисија на $\binom{20}{5} = 15504$ начина. △

2.2.4 Варијације са понављањем

Дефиниција 2.9. ***Варијација*** *k-те класе* ***са понављањем*** *скупа A_n је свака уређена k-торка елемената скупа A_n.*

Нека је са $\overline{V}_n^k$ означен број варијација са понављањем k-те класе скупа од n елемената.

Теорема 2.5. *Важи да је $\overline{V}_n^k = n^k$.*

Доказ. Укупан број варијација са понављањем k-те класе скупа од n елемената једнак је броју уређених k-торки образованих од елемената посматраног скупа. Како се избор сваке координате може извршити на n начина, закључујемо да тврђење важи према принципу производа. □

ПРИМЕР 2.19. Варијације са понављањем друге класе скупа $\{a, b, c, d\}$ дате у лексикографском поретку су

$$\begin{array}{cccc} aa & ba & ca & da \\ ab & bb & cb & db \\ ac & bc & cc & dc \\ ad & bd & cd & dd, \end{array}$$

а њихов број је $\overline{V}_4^2 = 4^2 = 16$.

ПРИМЕР 2.20. Коцка за игру чију су стране нумерисане бројевима $1, 2, 3, 4, 5, 6$ се баца четири пута и бележи редослед извучених бројева. Колико има могућих исхода бацања?

Решење. У сваком од четири бацања може се добити било који од бројева $1, 2, \ldots, 6$, одакле произилази да постоји $\overline{V}_6^4 = 6^4$ различитих исхода бацања. △

ПРИМЕР 2.21. У радњи постоји n различитих врста разгледница, које треба послати пријатељима, којих има k.

а) На колико начина је могуће сваком пријатељу послати тачно једну разгледницу?

б) Од сваке врсте разгледница је купљена тачно по једна. На колико начина је могуће послати разгледнице пријатељима, ако пријатељ може добити било који број разгледница (укључујући и 0)?

Решење. а) За сваког од k пријатеља одређујемо једну од n врста разгледница коју ће он добити. Како није захтевано да пријатељи добију разгледнице различите врсте, у питању су варијације са понављањем скупа од n елемената (разгледнице) класе k (пријатељи), па је број могућих начина једнак $\overline{V}_n^k = n^k$.

б) У овом случају, за сваку од n врста разгледница одређујемо неког од k пријатеља који ће добити ту разгледницу. Како пријатељи могу добити произвољан број разгледница, у питању су варијације са понављањем скупа од k елемената (пријатељи) класе n (разгледнице), па је њихов број једнак $\overline{V}_k^n = k^n$. △

2.2.5 Пермутације са понављањем

Дефиниција 2.10. *Свака уређена n-торка чланова једне фамилије од n објеката, при чему су k међу њима међусобно различити, и $n_1, n_2, \ldots, n_k$ $(n_1 + n_2 + \cdots + n_k = n)$ представљају бројеве појављивања у фамилији објеката прве, друге, ..., k-те врсте, респективно, назива се* ***пермутација са понављањем*** *типа $(n_1, n_2, \ldots, n_k)$.*

ПРИМЕР 2.22. Пермутације са понављањем фамилије $\{a, b, b\}$ дате су са

$$aab \quad baa.$$
$$aba$$

Пермутације са понављањем фамилије $\{a, b, b, c, c\}$ дате су са

$$\begin{array}{lll} abbcc & babcc & cabbc \\ abcbc & bacbc & cabcb \\ abccb & baccb & cacbb \\ acbbc & bbacc & cbabc \\ acbcb & bbcac & cbacb \\ accbb & bbcca & cbbac \\ & bcabc & cbbca \\ & bcacb & cbcab \\ & bcbac & cbcba \\ & bcbca & ccabb \\ & bccab & ccbab \\ & bccba & ccbba. \end{array}$$

Означимо са $P^n_{n_1,n_2,\ldots,n_k}$ број пермутација са понављањем описаних у дефиницији 2.10.

Теорема 2.6. *Важи да је*

$$P^n_{n_1,n_2,\ldots,n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}. \tag{2.2}$$

Доказ. Биће изложен доказ теореме на два начина.

Први начин. Посматрајмо фамилију од n објеката

$$\{\underbrace{a_1, a_1, \ldots, a_1}_{n_1}, \underbrace{a_2, a_2, \ldots, a_2}_{n_2}, \ldots, \underbrace{a_k, a_k, \ldots, a_k}_{n_k}\}.$$

Број начина да се од $n = n_1 + n_2 + \cdots + n_k$ позиција изабере n_1 позиција на којима ће се налазити елемент a_1 једнак је $C^{n_1}_n$. Од преосталог броја $n_2 + \cdots + n_k$ позиција бирамо n_2 позиција на којима ће се налазити елемент a_2 на $C^{n_2}_{n_2+\cdots+n_k}$ начина. Настављајући описани начин формирања пермутација са понављањем, у последњем кораку преостаје n_k позиција на којима ће се налазити елемент a_k. Према принципу производа, укупан број избора позиција, а тиме и број пермутација са понављањем траженог типа, једнак је

$$\begin{aligned} & C^{n_1}_n \cdot C^{n_2}_{n_2+\cdots+n_k} \cdots C^{n_k}_{n_{k-1}+n_k} \\ &= \frac{n!}{n_1!(n_2+\cdots+n_k)!} \cdot \frac{(n_2+\cdots+n_k)!}{n_2!(n_3+\cdots+n_k)!} \cdots \frac{(n_{k-1}+n_k)!}{n_{k-1}!\, n_k!} \cdot \frac{n_k!}{n_k!} \\ &= \frac{n!}{n_1! n_2! \cdots n_k!}. \end{aligned}$$

Други начин. Посматрајмо фамилију од n објеката

$$\{\underbrace{a_1, a_1, \ldots, a_1}_{n_1}, \underbrace{a_2, a_2, \ldots, a_2}_{n_2}, \ldots, \underbrace{a_k, a_k, \ldots, a_k}_{n_k}\}$$

и означимо са B скуп свих пермутација са понављањем ове фамилије. Тада је $|B| = P^n_{n_1,n_2,\ldots,n_k}$. Осим тога, придружимо овој фамилији скуп

$$\{a_1^1, a_1^2, \ldots, a_1^{n_1}, a_2^1, a_2^2, \ldots, a_2^{n_2}, \ldots, a_k^1, a_k^2, \ldots, a_k^{n_k}\}$$

и означимо са A скуп свих пермутација овог скупа. Тада је $|A| = n!$. Нека је $f : A \to B$ функција која свакој пермутацији $p \in A$ придружује пермутацију $\widehat{p} \in B$ која се добија од пермутације p брисањем горњих индекса. За сваку пермутацију $\widehat{p} \in B$ постоји тачно $n_1!n_2! \cdots n_k!$ пермутација скупа A које се у њу пресликавају функцијом f. Наиме, пермутовање објеката унутар сваке од k група истих објеката не доводи до промене пермутације са понављањем. Како се n_1 објеката из прве групе могу међусобно пермутовати на $n_1!$ начина, n_2 објеката из друге групе на $n_2!$ начина, ..., n_k објеката из k-те групе могу се међусобно пермутовати на $n_k!$ начина, следи, према принципу производа, да постоји $n_1!n_2! \cdots n_k!$ пермутација скупа A које се пресликавају у исту пермутацију са понављањем скупа B. Одавде, према принципу већег броја произилази да је $|A| = n_1!n_2! \cdots n_k! \cdot |B|$, одакле следи тражени резултат. □

ПРИМЕР 2.23. а) Колико се различитих речи може добити пермутовањем слова речи МАТЕМАТИКА?

б) Колико има описаних речи ако ААА није део речи?

Решење. а) Тражени број речи једнак је броју пермутација са понављањем фамилије од 10 објеката (слова) типа $(3, 2, 2, 1, 1, 1)$, па је њихов број једнак $P^{10}_{3,2,2,1,1,1} = \dfrac{10!}{3!2!2!} = 151200$.

б) У случају да ААА није део речи, тражени број речи добијамо тако што од укупног броја речи одређених у случају а) одузмемо број речи код којих три слова А стоје једно поред другог. У том случају ААА се посматра као један објекат, па је у овом случују реч о пермутацијама са понављањем фамилије од 8 објеката типа $(2, 2, 1, 1, 1, 1)$, којих има $P^8_{2,2,1,1,1,1} = \dfrac{8!}{2!2!} = 10080$. Коначно, број речи са траженом особином у овом случају је 141120. △

2.2.6 Комбинације са понављањем

Дефиниција 2.11. ***Комбинација са понављањем*** *k-те класе скупа A_n је свака фамилија од k (не обавезно различитих) елемената скупа A_n.*

ПРИМЕР 2.24. За скуп $A_4 = \{a, b, c, d\}$ комбинације са понављањем друге класе су

$$\begin{array}{cccc} aa & bb & cc & dd, \\ ab & bc & cd & \\ ac & bd & & \\ ad & & & \end{array}$$

док су комбинације са понављањем треће класе дате са

$$\begin{array}{cccc} aaa & bbb & ccc & ddd. \\ aab & bbc & ccd & \\ aac & bbd & cdd & \\ aad & bcc & & \\ abb & bcd & & \\ abc & bdd & & \\ abd & & & \\ acc & & & \\ acd & & & \\ add & & & \end{array}$$

Означимо са $\overline{C}_n^k$ број комбинација са понављањем k-те класе скупа од n елемената.

Теорема 2.7. *Важи да је*

$$\overline{C}_n^k = \binom{n+k-1}{k}.$$

Доказ. Произвољна комбинација са понављањем k-те класе скупа A_n дата са

$$\phi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \phi(a_1) & \phi(a_2) & \cdots & \phi(a_n) \end{pmatrix},$$

при чему је $\phi(a_1) + \phi(a_2) + \cdots + \phi(a_n) = k$, може да се представи помоћу низа састављеног од k јединица и $n-1$ нула

$$\{\underbrace{1, 1, \ldots, 1}_{\phi(a_1)}, 0, \underbrace{1, 1, \ldots, 1}_{\phi(a_2)}, 0, \ldots, 0, \underbrace{1, 1, \ldots, 1}_{\phi(a_n)}\},$$

при чему се нуле користе да означе „прегради“ које одговарају појединим елементима скупа A_n. На овај начин је успостављено бијективно пресликавање између скупа свих комбинација са понављањем k-те класе скупа A_n и скупа свих низова од $n+k-1$ симбола састављених од $n-1$ нула и k јединица на описани начин. Како је сваки низ симбола одређен положајем јединица у низу (или положајем нула у низу), при чему се k јединица могу разместити на $n+k-1$ места у низу на $\binom{n+k-1}{k}$ начина (односно, $n-1$ нула се могу разместити на $n+k-1$ места у низу на $\binom{n+k-1}{n-1}$ начина), то је према принципу једнакости,

$$\overline{C}_n^k = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}.$$

□

ПРИМЕР 2.25. Колико има шестоцифрених бројева у чијем запису (гледано слева на десно) цифре чине неопадајући низ?

Решење. Бројеви наведеног типа представљају комбинације са понављањем шесте класе скупа $\{1, 2, \ldots, 9\}$, што се једноставно уочава ако захтевамо да при запису комбинација са понављањем водимо рачуна о лексикографском поретку. Због тога тражених бројева има $\binom{9+6-1}{6} = \binom{14}{6} = 3003$. △

2.3 Биномна формула

Биномни коефицијенти представљају важан комбинаторни појам због своје разноврсне примене. Постоји обимна литература посвећена различитим идентитетима са биномним коефицијентима. Према дефиницији 2.7 биномни коефицијент $\binom{n}{k}$ дефинише се са

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}, \quad n \geqslant k \geqslant 0.$$

Како је по дефиницији $0! = 1$, следи да је $\binom{n}{0} = \binom{n}{n} = 1$. Осим тога, симетрични биномни коефицијенти $\binom{n}{k}$ и $\binom{n}{n-k}$ су међусобно једнаки, као што је истакнуто у одељку 2.2.3.

Теорема 2.8. *За свако $n \in \mathbb{N}$ и $1 \leqslant k \leqslant n$ важи*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{2.3}$$

Доказ. Теорему ћемо доказати на два начина, користећи комбинаторни приступ и факторијелну репрезентацију биномних коефицијената.

Први начин. Посматрајмо скуп $A = \{1, 2, \ldots, n\}$. Према теореми 2.4 биномни коефицијент $\binom{n}{k}$ представља број комбинација без понављања k-те класе скупа A, односно, број подскупова са тачно k елемената скупа A. Све подскупове са k елемената скупа A можемо поделити у две групе, тако да првој групи припадају они k-подскупови који не садрже елемент n, а другој они који садрже елемент n. Тада прва група садржи све подскупове са k елемената скупа $\{1, 2, \ldots, n-1\}$, тј. укупно $\binom{n-1}{k}$ подскупова са тачно k елемената скупа A. Друга група садржи подскупове са $(k-1)$ елемената скупа $\{1, 2, \ldots, n-1\}$, одакле произилази да се у другој групи налази $\binom{n-1}{k-1}$ подскупова са k елемената скупа A. Из претходних разматрања закључујемо да важи тврђење теореме.

Другōи начин. Користећи дефиницију биномних коефицијената добијамо

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}. \quad \square\end{aligned}$$

Једнакост (2.3) у литератури је позната и као **Паскалов идентитет**, јер је блиско повезана са тзв. **Паскаловим троуглом**, представљеним испод.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & \vdots & & & & & & \vdots & &
\end{array}$$

У свакој врсти Паскаловог троугла први и последњи члан су једнаки 1, а сваки од осталих бројева једнак је збиру два најближа члана претходне врсте. Математичком индукцијом се уз помоћ једнакости (2.3) једноставно доказује да $(n+1)$-ва врста Паскаловог троугла садржи биномне коефицијенте $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$, $n \in \mathbb{N}_0$.

Веома важна примена биномних коефицијената исказана је у следећој теореми.

Теорема 2.9. (**Биномна теорема**) *За сваки ненеīативан цео број* n *важи једнакост*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \,. \tag{2.4}$$

Доказ. Најпре ће бити изложен доказ математичком индукцијом, а затим комбинаторни доказ.

Први начин. Доказаћемо теорему математичком индукцијом по n. За $n = 0$ обе стране једнакости (2.4) су једнаке 1, па једнакост важи.

Претпоставимо да једнакост (2.4) важи за n и докажимо да важи и за $n+1$. Како је

$$\begin{aligned}
&(x+y)^{n+1} = (x+y)(x+y)^n \\
= \;& (x+y)\sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^k \text{ (индуктивна претпоставка)} \\
= \;& x\sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^k + y\sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^k \\
= \;& \sum_{k=0}^{n} \tbinom{n}{k} x^{n-k+1}y^k + \sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^{k+1} \\
= \;& \sum_{k=0}^{n} \tbinom{n}{k} x^{n-k+1}y^k + \sum_{k=1}^{n+1} \tbinom{n}{k-1} x^{n-k+1}y^k \\
= \;& \tbinom{n}{0} x^{n+1} + \sum_{k=1}^{n} \tbinom{n}{k} x^{n-k+1}y^k + \sum_{k=1}^{n} \tbinom{n}{k-1} x^{n-k+1}y^k + \tbinom{n}{n} y^{n+1} \\
= \;& \tbinom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \left(\tbinom{n}{k} + \tbinom{n}{k-1} \right) x^{n-k+1}y^k + \tbinom{n+1}{n+1} y^{n+1} \\
= \;& \tbinom{n+1}{0} x^{n+1} + \sum_{k=1}^{n} \tbinom{n+1}{k} x^{n-k+1}y^k + \tbinom{n+1}{n+1} y^{n+1} \text{ (према (2.3))} \\
= \;& \sum_{k=0}^{n+1} \tbinom{n+1}{k} x^{n-k+1}y^k,
\end{aligned}$$

једнакост (2.4) важи и за $n+1$, при чему смо искористили да је $\binom{n}{0} = \binom{n+1}{0} = \binom{n}{n} = \binom{n+1}{n+1} = 1$.

Друīи начин. Важи да је

$$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n}.$$

Применом закона дистрибутивности закључујемо да се израз на десној страни последње једнакости може написати као збир од 2^n сабирака

облика производа $c_1c_2\cdots c_n$, при чему $c_1, c_2, \ldots, c_n \in \{x, y\}$. Производе $c_1c_2\cdots c_n$ можемо посматрати и као речи над двочланим скупом $\{x, y\}$ и сваки од ових производа је једнак изразу облика $x^{n-k}y^k$, $0 \leqslant k \leqslant n$, у коме је тачно k од фактора c_i једнако y, а $n-k$ фактора једнако x. Због тога, за свако k, $0 \leqslant k \leqslant n$, постоји тачно $\binom{n}{k}$ сабирака облика $x^{n-k}y^k$, одакле следи тврђење. □

Формула (2.4) зове се **биномна формула**. Коришћењем ове формуле могу се доказати различити идентитети са биномним коефицијентима. У наставку ћемо навести неке од њих.

Последица 2.1. *За ненегативан цео број n важи*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n \tag{2.5}$$

и

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^n\binom{n}{n} = 0. \tag{2.6}$$

Доказ. Ако у биномној формули (2.4) ставимо $x = y = 1$, односно $x = 1, y = -1$, добијамо, респективно, једнакости (2.5) и (2.6). □

Напомена 2.1. *За свако $k = 0, 1, \ldots, n$ произвољан скуп од n елемената има, према теореми 2.4, $\binom{n}{k}$ подскупова са тачно k елемената, одакле следи да је укупан број подскупова скупа од n елемената једнак $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.*

Последица 2.2. *За ненегативан цео број n важи*

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}.$$

Доказ. Ако једнакости (2.5) и (2.6) најпре саберемо, а затим одузмемо, добијамо тражене једнакости. □

Последица 2.3. *За ненегативан цео број n важи*

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}.$$

Доказ. На основу биномне формуле (2.4) важи да је $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. Изједначавањем коефицијената уз x^n у развоју полинома (по x) на левој и десној страни једнакости

$$(1+x)^n(1+x)^n = (1+x)^{2n},$$

добијамо

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} = \binom{2n}{n}.$$

Имајући у виду да су симетрични биномни коефицијенти једнаки, закључујемо да је

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

□

ПРИМЕР 2.26. Одредити коефицијент уз x^5 у развоју израза

$$\left(3\sqrt{x} + \frac{1}{2\sqrt[3]{x}}\right)^{20}.$$

Решење. Приметимо најпре да је дати израз једнак $\left(3x^{\frac{1}{2}} + \frac{1}{2}x^{-\frac{1}{3}}\right)^{20}$, одакле према биномној формули следи да је

$$\begin{aligned}\left(3x^{\frac{1}{2}} + \tfrac{1}{2}x^{-\frac{1}{3}}\right)^{20} &= \sum_{k=0}^{20} \binom{20}{k} \left(3x^{\frac{1}{2}}\right)^{20-k} \left(\tfrac{1}{2}x^{-\frac{1}{3}}\right)^k \\ &= \sum_{k=0}^{20} \binom{20}{k} 3^{20-k}\, 2^{-k}\, x^{\left(\frac{20-k}{2} - \frac{k}{3}\right)}.\end{aligned}$$

Сабирак x^5 у овом изразу се добија за $\frac{20-k}{2} - \frac{k}{3} = 5$, тј. $k = 6$, одакле следи да је одговарајући коефицијент уз x^5 једнак $\binom{20}{6}3^{14}2^{-6}$. △

2.4 Принцип укључења-искључења

Према једном од основних принципа пребројавања, принципу збира, важи да је $|A \cup B| = |A| + |B|$, ако су A и B коначни дисјунктни скупови. У случају да скупови A и B нису дисјунктни, у суми $|A| + |B|$ елементе пресека $A \cap B$ бројимо два пута (једном као елементе скупа A, а други

пут као елементе скупа B), због чега, да бисмо одредили број елемената скупа $A \cup B$, користимо формулу

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{2.7}$$

Слично, у случају три скупа A, B, C, да бисмо одредили број елемената скупа $A \cup B \cup C$ користимо формулу

$$|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|. \tag{2.8}$$

Наиме, у суми $|A| + |B| + |C|$ се елементи који се налазе у тачно два од посматрана три скупа броје два пута, док се елементи који се налазе у пресеку сва три скупа броје три пута. Да бисмо обезбедили да се сваки елемент уније $A \cup B \cup C$ броји тачно једанпут најпре од суме $|A| + |B| + |C|$ одузимамо збир $|A \cap B| + |A \cap C| + |B \cap C|$, чиме се постиже да се елементи који се налазе у пресеку тачно два од посматраних скупова броје тачно једанпут. Међутим, сада се у добијеном изразу $(|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|)$ елементи који се налазе у пресеку сва три скупа уопште не броје (бројали смо их три пута у суми $|A| + |B| + |C|$ и одузели три пута у суми $|A \cap B| + |A \cap C| + |B \cap C|$). Стога, да бисмо сваки елемент скупа $A \cup B \cup C$ бројали тачно једанпут, последњем изразу додајемо број $|A \cap B \cap C|$, одакле следи формула (2.8).

Приликом пребројавања елемената скупа $A \cup B$, односно скупа $A \cup B \cup C$, поједине елементе наизменично укључујемо, односно искључујемо, због чега се наведени принцип пребројавања назива **принцип укључења-искључења**. У случају произвољног броја коначних скупова важи аналогна формула коју наводимо у следећој теореми.

Теорема 2.10. *Нека су $A_1, A_2, \ldots, A_n$ коначни скупови. Тада је*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| = &\sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| \\ &+ \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| \\ &- \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|. \end{aligned} \tag{2.9}$$

Доказ. Доказаћемо теорему на два начина, најпре користећи комбинаторни приступ, а затим математичком индукцијом.

Први начин. Докажимо теорему користећи комбинаторни приступ. „Допринос“ произвољног елемента $x \in A_1 \cup A_2 \cup \cdots \cup A_n$ левој страни

једнакости (2.9) износи 1. Докажимо да је „допринос“ елемента x и десној страни једнакости (2.9) такође 1. Ако тачно k ($1 \leqslant k \leqslant n$) од скупова $A_1, A_2, \ldots, A_n$ садржи елемент x, тада се елемент x у првој суми на десној страни једнакости (2.9) броји $k = \binom{k}{1}$ пута, у другој суми $\binom{k}{2}$ пута, ..., у k-тој суми $\binom{k}{k}$ пута, док се у осталим сумама не броји, одакле следи да је „допринос“ елемента x десној страни једнакости (2.9) једнак

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{k-1}\binom{k}{k}.$$

Како је према (2.6) $\sum_{i=0}^{k}\binom{k}{i}(-1)^i = 0$, тј. $\sum_{i=1}^{k}\binom{k}{i}(-1)^{i-1} = 1$, закључујемо да је „допринос“ елемента x и десној страни једнакости (2.9) једнак 1, одакле следи тврђење.

Други начин. Доказаћемо теорему индукцијом по броју скупова n, $n \geqslant 2$. У случају два скупа, једнакост (2.9) се своди на једнакост (2.7) која важи.

Претпоставимо да је једнакост (2.9) тачна за произвољних n скупова и докажимо да важи у случају уније $n+1$ скупова $A_1, A_2, \ldots, A_{n+1}$.

Како је $|(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}| = |\bigcup_{i=1}^{n}(A_i \cap A_{n+1})|$, на основу индуктивне претпоставке за број елемената уније n скупова $A_1 \cap A_{n+1}, A_2 \cap A_{n+1}, \ldots, A_n \cap A_{n+1}$, важи да је

$$\begin{aligned}
&|(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}| = |\textstyle\bigcup_{i=1}^{n}(A_i \cap A_{n+1})| \\
&= \sum_{i=1}^{n}|A_i \cap A_{n+1}| - \sum_{1\leqslant i<j\leqslant n}|A_i \cap A_j \cap A_{n+1}| \\
&\quad + \sum_{1\leqslant i<j<k\leqslant n}|A_i \cap A_j \cap A_k \cap A_{n+1}| \\
&\quad - \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}|.
\end{aligned} \tag{2.10}$$

Примењујући формулу (2.7) на скупове $A = A_1 \cup A_2 \cup \cdots \cup A_n$ и $B = A_{n+1}$ и користећи једнакости (2.9) и (2.10), добијамо

$$\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| \\
&= |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}| \\
&= \sum_{i=1}^{n+1}|A_i| - \sum_{1\leqslant i<j\leqslant n+1}|A_i \cap A_j| + \sum_{1\leqslant i<j<k\leqslant n+1}|A_i \cap A_j \cap A_k| \\
&\quad - \cdots + (-1)^n|A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}|,
\end{aligned}$$

одакле закључујемо да формула (2.9) важи и у случају уније $n+1$ скупова. □

ПРИМЕР 2.27. На неком турниру учествовало је n такмичара нумерисаних бројевима од 1 до n. На колико начина је након завршетка турнира могуће формирати ранг-листу такмичара, ако се зна да се редослед ниједног такмичара на ранг-листи не поклапа са његовим редним бројем?

Решење. Означимо са A скуп свих могућих распореда n такмичара на ранг листи, а са A_i скуп оних распореда при којима је i-ти такмичар на ранг листи нумерисан бројем i, $1 \leqslant i \leqslant n$. Потребно је одредити број $|A| - |A_1 \cup A_2 \cup \cdots \cup A_n|$.

Имајући у виду да је $|A| = n!$, $|A_i| = (n-1)!$, $1 \leqslant i \leqslant n$, $|A_i \cap A_j| = (n-2)!$, $1 \leqslant i < j \leqslant n$, $\ldots$, $|A_1 \cap A_2 \cap \cdots \cap A_n| = 1 = (n-n)!$, заменом одговарајућих вредности у формули (2.9) добијамо да је тражени број редоследа једнак $n!\left(1 - \dfrac{1}{1!} + \dfrac{1}{2!} - \cdots + (-1)^n \dfrac{1}{n!}\right)$. △

2.5 Партиције и композиције природних бројева

У овом одељку ће бити речи о представљању природних бројева у облику збира других природних бројева. Партиције и композиције представљају изузетно важне комбинаторне појмове који су обимно разматрани у литератури.

Дефиниција 2.12. *Нека је n природан број и $x_1, x_2, \ldots, x_k$ природни бројеви такви да важи*

$$x_1 + x_2 + \cdots + x_k = n. \tag{2.11}$$

Представљање броја n у облику (2.11) назива се k-подела броја n, односно разбијање броја n на k сабирака.

Дефиниција 2.13. ***Партиција*** *природног броја n је свака његова неуређена подела, тј. подела код које је поредак сабирака небитан.* ***Композиција*** *природног броја n је било која уређена подела броја n, тј. подела код које је битан редослед сабирака.*

2.5.1 Партиције природних бројева

Партиција π броја n, $n \in \mathbb{N}$, на k сабирака, $k \geqslant 1$, је према дефиницији 2.13 фамилија $\pi = \{x_1, x_2, \ldots, x_k\}$, таква да $x_i \in \mathbb{N}$, $i = 1, 2, \ldots, k$, при чему је $n = x_1 + x_2 + \cdots + x_k$. Партицију π која садржи α_i сабирака једнаких i, $i = 1, 2, \ldots, n$, означавамо са $\pi = [1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$.

ПРИМЕР 2.28. 1° Партиције броја 4 су $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$, односно $[4^1]$, $[1^1\,3^1]$, $[2^2]$, $[1^2\,2^1]$, $[1^4]$.

2° Партиције броја 5 су $5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$, односно $[5^1]$, $[1^1\,4^1]$, $[2^1\,3^1]$, $[1^2\,3^1]$, $[1^1\,2^2]$, $[1^3\,2^1]$, $[1^5]$.

Укупан број партиција природног броја n означаваћемо са $p(n)$. Првих 10 вредности ове функције приказано је у следећој табели.

n	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42

Постоји тачна формула за $p(n)$, која се може наћи у књизи [30], али је због сложености нећемо наводити. Многи математичари су, да би испитали понашање ове функције када $n \to +\infty$, тражили апроксимативну формулу за $p(n)$. Харди[1] и Раманујан[2] су 1918. године доказали формулу

$$p(n) \approx \frac{\mathrm{e}^{c\sqrt{n}}}{4n\sqrt{3}},$$

где је константа $c = \pi\sqrt{\frac{2}{3}}$. Функција p веома брзо расте са повећањем вредности аргумента n, па је, на пример, $p(50) = 204226$, $p(100) = 190569292$, $p(200) = 3972999029388$.

У следећим теоремама дате су рекурентне формуле чијом се применом може одредити број партиција природног броја n на сабирке једнаке датим природним бројевима.

Теорема 2.11. *Нека су $n_1, n_2, \ldots, n_k$ различити природни бројеви и нека је са $p_1(n_1, n_2, \ldots, n_k; n)$ означен број партиција природног броја n на различите сабирке, код којих је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$. Тада важи једнакост*

$$p_1(n_1, \ldots, n_k; n) = p_1(n_1, \ldots, n_{k-1}; n - n_k) + p_1(n_1, \ldots, n_{k-1}; n),$$

при чему је

$$p_1(n_1, n_2, \ldots, n_k; m) = \begin{cases} 0, & m < 0, \\ 1, & m = 0. \end{cases}$$

[1] Godfrey Harold Hardy (1877–1947), енглески математичар

[2] Srinivasa Ramanujan (1887–1920), индијски математичар

Доказ. Нека је S скуп партиција броја n на различите сабирке, при чему је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$. Нека је $S_1 \subseteq S$ скуп оних партиција броја n код којих постоји сабирак једнак n_k, а $S_2 \subseteq S$ скуп оних партиција броја n које не садрже сабирак једнак n_k. Важи да је $|S| = p_1(n_1, n_2, \ldots, n_k; n)$.

Ако се број n_k садржи као сабирак у датој партицији, онда остатак те партиције представља партицију броја $n - n_k$ на различите сабирке који припадају скупу $\{n_1, n_2, \ldots, n_{k-1}\}$ (како су сабирци различити, број n_k не може да се јави два пута), одакле закључујемо да је $|S_1| = p_1(n_1, n_2, \ldots, n_{k-1}; n - n_k)$.

Ако се број n_k не садржи као сабирак у датој партицији, онда та партиција представља партицију броја n на различите сабирке, али из скупа $\{n_1, n_2, \ldots, n_{k-1}\}$, одакле следи да је $|S_2| = p_1(n_1, n_2, \ldots, n_{k-1}; n)$.

Како је $S = S_1 \cup S_2$ и $S_1 \cap S_2 = \emptyset$, следи да је $|S| = |S_1| + |S_2|$, одакле произилази тражена једнакост. □

Теорема 2.12. *Нека су $n_1, n_2, \ldots, n_k$ различити природни бројеви и нека је са $p_2(n_1, n_2, \ldots, n_k; n)$ означен број партиција природног броја n код којих је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$. Тада важи једнакост*

$$p_2(n_1, \ldots, n_k; n) = p_2(n_1, \ldots, n_k; n - n_k) + p_2(n_1, \ldots, n_{k-1}; n), \tag{2.12}$$

при чему је

$$p_2(n_1, n_2 \ldots, n_k; m) = \begin{cases} 0, & m < 0, \\ 1, & m = 0. \end{cases}$$

Доказ. Нека је S скуп партиција броја n код којих је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$. Нека је $S_1 \subseteq S$ скуп оних партиција броја n код којих постоји сабирак једнак n_k, а $S_2 \subseteq S$ скуп оних партиција броја n које не садрже сабирак једнак n_k. Аналогно доказу претходне теореме, закључујемо да је $|S| = p_2(n_1, n_2, \ldots, n_k; n)$, $|S_1| = p_2(n_1, n_2, \ldots, n_k; n - n_k)$ и $|S_2| = p_2(n_1, n_2, \ldots, n_{k-1}; n)$. Како је $S = S_1 \cup S_2$ и $S_1 \cap S_2 = \emptyset$, следи да је $|S| = |S_1| + |S_2|$, па важи тражена једнакост. □

Применом наведених теорема може се једноставно одредити број партиција природног броја n на сабирке који су једнаки датим природним бројевима.

ПРИМЕР 2.29. Одредити на колико начина можемо број 20 представити у облику збира, ако су дозвољени сабирци $1, 2, 5, 10$, при чему сваки од наведених бројева може бити употребљен произвољан број пута.

Решење. Како сабирци могу да се понављају, потребно је применити теорему 2.12, тј. израчунати број $p_2(1,2,5,10;20)$ применом формуле (2.12). Очигледно је $p_2(1;n) = 1$, за сваки број $n \geqslant 0$. Применом формуле (2.12) добијамо

$$\begin{aligned} p_2(1,2;2k) &= p_2(1;2k) + p_2(1,2;2k-2) \\ &= 1 + p_2(1,2;2k-2) \\ &= 1 + p_2(1;2k-2) + p_2(1,2;2k-4) \\ &= 2 + p_2(1,2;2k-4) = \cdots = \ k + p_2(1,2;0) = k+1, \end{aligned}$$

$$\begin{aligned} p_2(1,2;2k+1) &= p_2(1;2k+1) + p_2(1,2;2k-1) \\ &= 1 + p_2(1,2;2k-1) \\ &= 1 + p_2(1;2k-1) + p_2(1,2;2k-3) \\ &= 2 + p_2(1,2;2k-3) = \cdots = k + p_2(1,2;1) \\ &= k+1, \end{aligned}$$

одакле следи да је

$$\begin{aligned} &p_2(1,2,5;5) = p_2(1,2,5;0) + p_2(1,2;5) = 1+3 = 4, \\ &p_2(1,2,5;10) = p_2(1,2,5;5) + p_2(1,2;10) = 4+6 = 10, \\ &p_2(1,2,5;15) = p_2(1,2,5;10) + p_2(1,2;15) = 10+8 = 18, \\ &p_2(1,2,5;20) = p_2(1,2,5;15) + p_2(1,2;20) = 18+11 = 29, \\ &p_2(1,2,5,10;10) = p_2(1,2,5,10;0) + p_2(1,2,5;10) = 1+10 = 11, \\ &p_2(1,2,5,10;20) = p_2(1,2,5,10;10) + p_2(1,2,5;20) = 11+29 = 40. \end{aligned}$$

Дакле, тражени број је $p_2(1,2,5,10;20) = 40$. △

2.5.2 Композиције природних бројева

Композиција природног броја n је, као што је у уводном делу речено, уређена подела (разбијање) броја n, због чега се понекад назива и уређена партиција броја n.

ПРИМЕР 2.30. Композиције броја 4 су $4 = 3+1 = 1+3 = 2+2 = 2+1+1 = 1+2+1 = 1+1+2 = 1+1+1+1$.

За разлику од партиција, проблем пребројавања композиција датог природног броја n је много једноставнији, о чему говори следећа теорема.

Теорема 2.13. (*а*) *Број композиција природног броја* n *на* k *сабирака,* $1 \leqslant k \leqslant n$, *једнак је* $\binom{n-1}{k-1}$.

(*б*) *Укупан број композиција природног броја* n *једнак је* 2^{n-1}.

Доказ. (а) Нека је A скуп свих композиција на k сабирака, тј. уређених k-подела природног броја n, а B скуп свих низова састављених од n јединица и $k-1$ нула, при чему никоје две нуле у низу нису суседне и први и последњи симбол у низу су јединице. Дефинишимо функцију $f : A \to B$ која свакој уређеној k-подели $x_1 + x_2 + \cdots + x_k$ броја n придружује низ

$$\underbrace{1,1,\ldots,1}_{x_1},0,\underbrace{1,1,\ldots,1}_{x_2},0,\ldots,0,\underbrace{1,1,\ldots,1}_{x_k},$$

чиме је успостављено узајамно једнозначно пресликавање између скупа свих уређених k-подела броја n и скупа свих низова дужине $n+k-1$ састављених од нула и јединица на описани начин. Како две нуле у низу не могу бити суседне и нуле не могу стајати на почетку и крају низа, закључујемо да је потребно разместити $k-1$ нула у $n-1$ међупростора између n јединица, што је могуће урадити на $\binom{n-1}{k-1}$ начина. Дакле, описаних низова састављених од нула и јединица има $\binom{n-1}{k-1}$, одакле, према принципу једнакости, следи да је то и број свих композиција на k сабирака природног броја n.

(б) Означимо са $c_k(n)$ број композиција природног броја n на k сабирака, а са $c(n)$ укупан број композиција природног броја n. Тада, имајући у виду претходно доказани резултат, добијамо

$$c(n) = \sum_{k=1}^{n} c_k(n) = \sum_{k=1}^{n} \binom{n-1}{k-1} = \sum_{k=0}^{n-1} \binom{n-1}{k}.$$

С обзиром да је према (2.5), $\sum\limits_{k=0}^{n-1} \binom{n-1}{k} = 2^{n-1}$, закључујемо да је укупан број композиција природног броја n једнак 2^{n-1}. □

Теорема 2.14. *Број композиција природног броја* n *код којих се сваки сабирак* k, $1 \leqslant k \leqslant n$, *појављује* α_k *пута, при чему је* $1\cdot\alpha_1 + 2\cdot\alpha_2 + \cdots + n\cdot\alpha_n = n$, *једнак је* $\dfrac{(\alpha_1+\alpha_2+\cdots+\alpha_n)!}{\alpha_1!\,\alpha_2!\,\cdots\alpha_n!}$.

Доказ. Објекти које пребројавамо су пермутације са понављањем фамилије од $\alpha_1+\alpha_2+\cdots+\alpha_n$ елемената типа $(\alpha_1,\alpha_2,\ldots,\alpha_n)$, одакле следи да је тражени број композиција једнак $\dfrac{(\alpha_1+\alpha_2+\cdots+\alpha_n)!}{\alpha_1!\,\alpha_2!\,\cdots\alpha_n!}$. □

ПРИМЕР 2.31. Написати све композиције броја 10 помоћу сабирака $1, 2, 2, 5$.

Решење. Имајући у виду теорему 2.14, закључујемо да тражених композиција има $\dfrac{(1+2+1)!}{1!\,2!\,1!} = 12$ и облика су

$$\begin{array}{lll} 1+2+2+5, & 2+1+5+2, & 2+5+2+1, \\ 1+2+5+2, & 2+2+1+5, & 5+1+2+2, \\ 1+5+2+2, & 2+2+5+1, & 5+2+1+2, \\ 2+1+2+5, & 2+5+1+2, & 5+2+2+1. \end{array}$$

△

На крају овог одељка наводимо теорему чијом се применом може одредити број композиција природног броја n на сабирке једнаке датим природним бројевима.

Теорема 2.15. *Нека су $n_1, n_2, \ldots, n_k$ различити природни бројеви и нека је са $c(n_1, n_2, \ldots, n_k; n)$ означен број композиција природног броја n код којих је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$. Тада важи једнакост*

$$c(n_1, n_2, \ldots, n_k; n) = \sum_{j=1}^{k} c(n_1, n_2, \ldots, n_k; n - n_j),$$

при чему је

$$c(n_1, n_2, \ldots, n_k; m) = \begin{cases} 0, & m < 0, \\ 1, & m = 0. \end{cases}$$

Доказ. Означимо са S скуп свих композиција броја n код којих је сваки од сабирака једнак неком од бројева $n_1, n_2, \ldots, n_k$, а са S_j скуп оних композиција из S код којих је први сабирак једнак n_j, $1 \leqslant j \leqslant k$. Скупови $S_1, S_2, \ldots, S_k$ су међусобно дисјунктни, а њихова унија је скуп S, одакле следи да је

$$c(n_1, n_2, \ldots, n_k; n) = |S| = \sum_{j=1}^{k} |S_j| = \sum_{j=1}^{k} c(n_1, n_2, \ldots, n_k; n - n_j). \quad \square$$

ПРИМЕР 2.32. Одредити на колико се начина број 7 може записати као збир сабирака једнаких неком од бројева из скупа $\{1, 2, 3, 4\}$, ако је битан редослед сабирака.

Решење. Потребно је одредити број $c(1,2,3,4;7)$. Означимо овај број краће са $\widetilde{c}(7)$. Према претходној теореми важи да је

$$\widetilde{c}(7) = \widetilde{c}(6) + \widetilde{c}(5) + \widetilde{c}(4) + \widetilde{c}(3).$$

Како је $\widetilde{c}(1) = 1, \widetilde{c}(2) = 2, \widetilde{c}(3) = 4, \widetilde{c}(4) = 8$, следи да је

$$\begin{aligned}
\widetilde{c}(5) &= \widetilde{c}(4) + \widetilde{c}(3) + \widetilde{c}(2) + \widetilde{c}(1) = 8 + 4 + 2 + 1 = 15,\\
\widetilde{c}(6) &= \widetilde{c}(5) + \widetilde{c}(4) + \widetilde{c}(3) + \widetilde{c}(2) = 15 + 8 + 4 + 2 = 29,\\
\widetilde{c}(7) &= \widetilde{c}(6) + \widetilde{c}(5) + \widetilde{c}(4) + \widetilde{c}(3) = 29 + 15 + 8 + 4 = 56.
\end{aligned}$$

Дакле, тражени број је 56. △

Глава 3

Теорија графова

3.1 Увод

Теорија графова је математичка дисциплина чија је примена данас веома значајна у рачунарству, теорији електричних кола, теорији система аутоматског управљања, теорији коначних аутомата, операционим истраживањима, теорији поузданог преноса информација, као и у хемији, економским наукама, социологији, биологији и др. Осим тога, теорија графова се примењује и у другим математичким дисциплинама, нпр. у теорији скупова, топологији, теорији игара и линеарном програмирању. Првим резултатом из теорије графова сматра се Ојлерово решење проблема **кенигсбершких мостова** из 1736. године, о коме ће бити речи касније. Дуго након тога, теорија графова је била скуп неповезаних, углавном помоћних и спорадичних тврђења у тада већ афирмисаним математичким дисциплинама, као што су алгебра, геометрија и анализа. Резултати те врсте су углавном осциловали између „озбиљне“ и рекреативне математике. Тренутком заснивања теорије графова као самосталне математичке дисциплине сматра се објављивање Кенигове[1] монографије 1936. године, када је термин **граф** ушао у општу употребу. Овај термин је први употребио математичар Силвестер[2] у свом раду из 1878. године. Кениг је у својој монографији навео свега 110 до тада објављених радова у којима се термин граф експлицитно појављује. Међу њиховим ауторима били су познати научници попут Кирхофа[3],

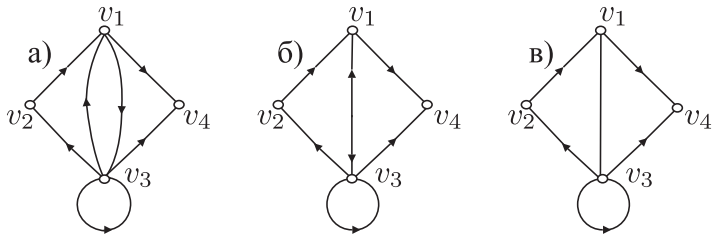
[1] Dénes König (1884–1944), мађарски математичар
[2] James Joseph Sylvester (1814–1897), енглески математичар
[3] Gustav Robert Kirhhoff (1824–1887), немачки физичар

Кејлија[4] и Куратовског[5]. Од тада граф постаје општеприхваћен појам, па су језиком теорије графова постављани и решавани бројни занимљиви проблеми. У 60-тим годинама прошлог века почиње снажан развој истраживања у теорији графова и њеним применама који траје до данас. Необично интензиван развој и велику популарност теорија графова је доживела захваљујући, пре свега, наглом развоју модерних информационих технологија. Осим тога, јасна геометријска представа коју граф садржи и која је блиска интуитивном схватању особина и веза објеката представљених графом, допринела је широком спектру примене графова. С друге стране, графови постају универзално математичко средство којим је могуће описати и моделирати најразличитије, и сасвим апстрактне математичке структуре.

3.2 Графови

Дефиниција 3.1. *Нека је V непразан скуп и $\rho \subseteq V \times V$ бинарна релација скупа V. Уређен пар $G = (V, \rho)$ се назива* ***граф****. Елементи скупа V су* ***чворови*** *графа, а елементи скупа ρ* ***гране*** *графа.*

Граф се може геометријски представити цртежом у равни, при чему чворове графа $v_1, v_2, \ldots, v_n \in V$ представљамо произвољним, међусобно различитим тачкама у равни, а гране графа линијама које повезују одговарајуће чворове. Ако $(v_i, v_j) \in \rho$, тада тачке које одговарају чворовима v_i и v_j спајамо непрекидном глатком линијом оријентисаном на цртежу стрелицом од v_i ка v_j. Ако $(v_i, v_j) \notin \rho$, тада чворови v_i и v_j на цртежу нису директно повезани.



Слика 3.1

Ако $(v_i, v_j) \in \rho$ и $(v_j, v_i) \in \rho$, где су v_i и v_j произвољни чворови графа, тада се на цртежу понекад не повлаче две линије између чворова v_i и

[4] Arthur Cayley (1821–1895), енглески математичар
[5] Kazimierz Kuratowsky (1896–1980), пољски математичар

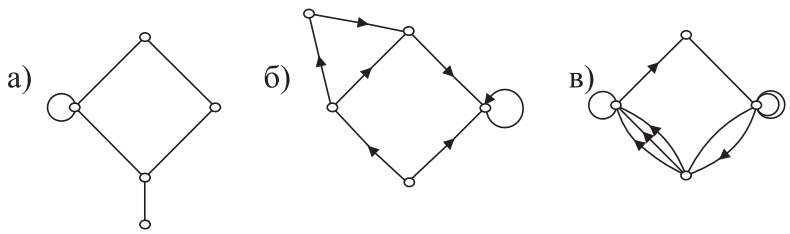
v_j, већ се јединствена линија двострано оријентише или се уопште не оријентише. Грана која повезује чвор са самим собом назива се петља.

ПРИМЕР 3.1. Граф $G = (V, \rho)$, где је $V = \{v_1, v_2, v_3, v_4\}$ и $\rho = \{(v_1, v_3), (v_1, v_4), (v_2, v_1), (v_3, v_1), (v_3, v_2), (v_3, v_3), (v_3, v_4)\}$, представљен је на слици 3.1 на три еквивалентна начина.

Дефиниција 3.2. *Граф $G = (V, \rho)$ је **симетричан** или **неоријентисан** ако и само ако је ρ симетрична релација.*

Код неоријентисаних графова све гране су двострано оријентисане, односно неоријентисане, због чега се при представљању оваквих графова цртежом одговарајуће стрелице изостављају.

Дефиниција 3.3. *Граф $G = (V, \rho)$ је **антисиметричан** или **оријентисан** ако и само ако је ρ антисиметрична релација.*



Слика 3.2

ПРИМЕР 3.2. На слици 3.2 а) и 3.2 б) приказан је један неоријентисан, односно оријентисан граф, респективно. С обзиром на то да петља повезује чвор са самим собом, њена оријентација нема значаја, због чега је уобичајено да се код петље стрелица на цртежу изоставља.

Постоје графови који нису ни оријентисани ни неоријентисани, какав је граф представљен на слици 3.1. Ако при представљању графа не замењујемо сваки пар грана супротне оријентације једном неоријентисаном граном, тада се одговарајући граф назива **дограф**. Такав је, на пример, граф представљен на слици 3.1 а). Оријентисане и неоријентисане графове можемо такође схватити као диграфове. Наиме, оријентисани графови су диграфови код којих не постоји ниједан пар различитих чворова спојених са две гране супротне оријентације, док су неоријентисани графови диграфови код којих не постоји ниједан пар различитих чворова спојених тачно једном оријентисаном граном.

Геометријска представа, односно цртеж графа, сугерише да је могуће дефинисати графове код којих између два чвора постоји више од једне гране исте оријентације (тзв. вишеструке гране). Такви графови се називају **мултиграфови**. Они могу садржати и вишеструке петље. На слици 3.2 в) је приказан један мултиграф. Прецизније, мултиграф се може дефинисати на следећи начин.

Дефиниција 3.4. *Нека је V непразан скуп и E једна фамилија елемената скупа $V \times V$. Уређен пар $G = (V, E)$ назива се **мултиграф**, при чему су елементи скупа V чворови мултиграфа, а елементи фамилије E гране мултиграфа.*

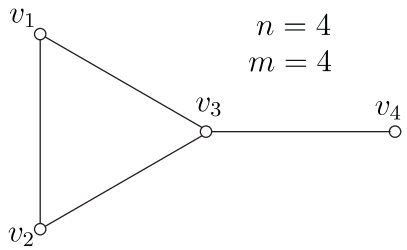
Граф је специјалан случај мултиграфа. Појам оријентисаног, односно неоријентисаног мултиграфа, дефинишу се аналогно одговарајућим појмовима код графова.

Произвољан граф $G = (V, \rho)$ се често означава са $G = (V, E)$, где је E скуп уређених парова елемената скупа V, тј. скуп грана. Дакле, граф је задат ако је познат његов скуп чворова и скуп грана. У случају неоријентисаног графа G користи се иста ознака $G = (V, E)$, при чему је сада E скуп неуређених парова елемената из скупа V, односно скуп неоријентисаних (двострано оријентисаних) грана.

Графови (мултиграфови) могу бити **коначни** или **бесконачни**, зависно од тога да ли је скуп чворова V коначан или бесконачан.

У оквиру ове књиге ћемо, ако другачије не нагласимо, под појмом граф подразумевати коначан, неоријентисан граф без петљи и вишеструких грана. Такви графови се у литератури често срећу под називом **прости графови**.

На слици 3.3 дат је граф $G = (V, E)$, где је $V = \{v_1, v_2, v_3, v_4\}$ и $E = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_3, v_4\}\}$.



Слика 3.3

Број чворова графа G зове се **ред графа** и означава се са n, док се број грана означава са m. Уобичајено је да се грана $\{v, w\}$, где су v и w чворови графа G, означава са vw.

Ако је $e = vw$ грана графа G, тада за грану e кажемо да **спаја** чворове v и w, а за ове чворове кажемо да су **суседни**. Осим тога, кажемо да је грана e **инцидентна** или **суседна** чворовима v и w, као и да су чворови v и w **инцидентни** грани $e = vw$. Скуп свих чворова графа G који су суседни чвору v означава се са $N_G(v)$ (или краће са $N(v)$) и зове се **суседство** или **околина** чвора v. За све гране графа G које су инцидентне истом чвору кажемо да су **суседне гране**. Ако је неки чвор једна од крајњих тачака извесне гране, каже се да се та грана **стиче** у овом чвору. **Степен** чвора v у графу $G = (V, E)$, у ознаци $d_G(v)$ (или краће $d(v)$), је број његових суседа, тј. $d_G(v) = |N_G(v)|$. Степен чвора се може дефинисати и као број грана које се стичу у том чвору. У случају да чвор има петљу, тада је њен допринос степену чвора једнак 2 (по другој конвенцији допринос петље степену чвора је 1).

У случају диграфа, ако грана e спаја чворове v и w и оријентисана је од v ка w, каже се да ова грана **излази** из чвора v, а **улази** у чвор w. Осим тога, каже се и да је чвор v **почетни**, а чвор w **завршни** чвор гране $e = vw$. У диграфу се за сваки чвор дефинише његов **улазни степен**, као број грана које улазе у тај чвор, односно **излазни степен**, као број грана које излазе из тог чвора. Петља се овде сматра и улазном и излазном граном за одговарајући чвор.

Минималан и **максималан степен** графа $G = (V, E)$, у ознаци $\delta(G)$ и $\Delta(G)$, респективно, дефинишу се са

$$\delta(G) = \min_{v \in V} d_G(v), \qquad \Delta(G) = \max_{v \in V} d_G(v).$$

Чвор степена 0 графа G зове се **изоловани чвор**, док се чвор степена 1 зове **висећи чвор** или **лист**.

Збир степена свих чворова графа једнак је двоструком броју грана, јер свака грана доприноси збиру степена чворова два пута - по једанпут за сваки крајњи чвор гране. Дакле, важи следећа теорема.

Теорема 3.1. *У произвољном графу $G = (V, E)$, при чему је $|E| = m$, важи*

$$\sum_{v \in V} d_G(v) = 2m\,. \tag{3.1}$$

Последица 3.1. *У произвољном графу је број чворова непарног степена паран.*

Доказ. Уколико произвољан граф G садржи непаран број чворова непарног степена, тада је збир $\sum_{v \in V} d_G(v)$ непаран број, супротно тврђењу теореме 3.1. □

Последица 3.1 је у литератури позната као теорема о руковању:

У сваком друштву је број особа које су се руковале непаран број пута паран.

Овде особе из друштва представљају чворове графа, при чему између два чвора постоји грана уколико су се одговарајуће особе руковале.

ПРИМЕР 3.3. Доказати да у сваком графу постоје два чвора истог степена.

Решење. Како за степен d произвољног чвора v из графа G са n чворова важи да је $0 \leqslant d \leqslant n-1$, закључујемо да ако су степени свих чворова у графу различити, тада бројеви $0, 1, \ldots, n-1$ представљају степене чворова тог графа. Међутим, ово је немогуће, јер са једне стране постоји изолован чвор (степена 0), а са друге стране стране чвор степена $n-1$ суседан са свим преосталим чворовима у графу. △

3.3 Степени чворова и графички низови

Графу $G = (V, E)$ са скупом чворова $V = \{v_1, v_2, \ldots, v_n\}$ може се придружити низ степена његових чворова $(d_1, d_2, \ldots, d_n)$, при чему је $d_i = d(v_i)$, $i = 1, 2, \ldots, n$, и чворови графа су означени тако да су њихови степени дати у нерастућем или неопадајућем поретку, тј. важи да је $n-1 \geqslant d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n \geqslant 0$ или $0 \leqslant d_1 \leqslant d_2 \leqslant \cdots \leqslant d_n \leqslant n-1$.

Обрнуто не мора да важи, тј. ако је $(d_1, d_2, \ldots, d_n)$ произвољан неопадајући или нерастући низ целих бројева, не мора да постоји граф чији су то степени чворова. За низ целих бројева $(d_1, d_2, \ldots, d_n)$ кажемо да је **графички низ** ако постоји граф $G = (V, E)$ чији је то низ степена чворова. Следеће тврђење, које су независно један од другог доказали Хавел[6] и Хакими[7], омогућава да се одреди који су низови графички.

Теорема 3.2. *Низ целих бројева $(d_1, d_2, \ldots, d_n)$, такав да је $n-1 \geqslant d_1 \geqslant d_2 \geqslant \cdots \geqslant d_n \geqslant 0$, је графички ако и само ако је низ*

$$(d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n)$$

графички.

[6] Vacláv Havel, чешки математичар

[7] Seifollah Louis Hakimi (1932–2005), иранско-амерички математичар

Доказ. Уведимо ознаке

$$D = (d_1, d_2, \ldots, d_n), \quad D' = (d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n).$$

Претпоставимо да је низ D' графички. Тада постоји граф $G' = (V', E')$ са скупом чворова $V' = \{v_2, v_3, \ldots, v_n\}$, такав да је $d_{G'}(v_2) = d_2 - 1$, $d_{G'}(v_3) = d_3 - 1, \ldots, d_{G'}(v_{d_1+1}) = d_{d_1+1} - 1$, $d_{G'}(v_{d_1+2}) = d_{d_1+2}, \ldots, d_{G'}(v_n) = d_n$. Додавањем новог чвора v_1 и нових грана v_1v_2, $v_1v_3, \ldots, v_1v_{d_1+1}$ добија се граф G чији је низ степена чворова управо низ D, одакле произилази да је D графички низ.

Обратно, претпоставимо да је D графички низ. Одатле следи да постоји бар један граф са скупом чворова $V = V(G) = \{v_1, v_2, \ldots, v_n\}$ и низом степена чворова D, тј. граф у коме је $d(v_i) = d_i$, $i = 1, 2, \ldots, n$. Означимо са G онај од тих графова у коме чвор v_1 има највише суседа из скупа $S = \{v_2, v_3, \ldots, v_{d_1+1}\}$, тј. онај граф за који је број $|N_G(v_1) \cap S|$ максималан. Доказаћемо да је $N_G(v_1) = S$.

Претпоставимо да је $N_G(v_1) \neq S$. Тада постоји чвор v_i, $2 \leqslant i \leqslant d_1 + 1$, такав да $v_1v_i \notin E(G)$. Како је $d(v_1) = d_1$, постоји чвор v_j, $d_1 + 2 \leqslant j \leqslant n$, такав да $v_1v_j \in E(G)$. С обзиром на то да је $i < j$ и D је нерастући низ, следи да је $d_i = d_G(v_i) \geqslant d_j = d_G(v_j)$. Како $v_1v_i \notin E(G)$ и $v_1v_j \in E(G)$, закључујемо да постоји чвор v_k, такав да $v_1v_k \in E(G)$ и $v_jv_k \notin E(G)$. Нека је G_1 граф добијен од графа G уклањањем грана v_1v_j и v_iv_k и додавањем нових грана v_1v_i и v_jv_k. Према конструкцији графа G_1 закључујемо да је његов низ степена чворова такође низ D, при чему је $|N_{G_1}(v_1) \cap S| = |N_G(v_1) \cap S| + 1$, што је контрадикција са избором графа G. Дакле, важи да је $N_G(v_1) = S$. Нека је даље G' граф добијен од графа G уклањањем чвора v_1, заједно са свим гранама инцидентним са v_1. Тада је G' граф са низом степена чворова D', одакле следи да је D' графички низ. □

ПРИМЕР 3.4. Утврдити да ли је низ $(5, 5, 4, 4, 3, 2, 2, 1, 1)$ графички.

Решење. Према теореми 3.2 низ $D = (5, 5, 4, 4, 3, 2, 2, 1, 1)$ је графички ако и само ако је низ $D' = (4, 3, 3, 2, 1, 2, 1, 1)$ графички. Како низ D' садржи пет непарних бројева, према последици 3.1 он није графички, па није графички ни низ D. △

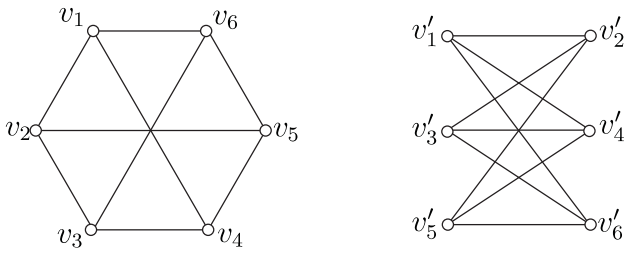
3.4 Изоморфизам графова

Дефиниција 3.5. *Два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ су* ***изоморфна*** *ако постоји бијекција $f : V_1 \to V_2$ која одржава особину суседности*

чворова, тј.

$$(\forall v, w \in V_1) \;\; (vw \in E_1 \Leftrightarrow f(v)f(w) \in E_2)\,.$$

Пресликавање f зове се **изоморфизам**, а чињеницу да су графови G_1 и G_2 изоморфни означавамо са $G_1 \cong G_2$.



G_1 G_2

Слика 3.4

ПРИМЕР 3.5. Графови G_1 и G_2 са слике 3.4 су изоморфни, а одговарајући изоморфизам је пресликавање

$$f = \begin{pmatrix} v_1 & v_2 & \cdots & v_6 \\ v_1' & v_2' & \cdots & v_6' \end{pmatrix}.$$

Релација изоморфности два графа је рефлексивна, симетрична и транзитивна, односно представља релацију еквиваленције у скупу свих графова, па је можемо прогласити за једнакост графова. Према томе, графови су једнаки ако и само ако су изоморфни.

Из дефиниције изоморфности два графа произилази да су изоморфни графови у ствари исти графови, али различито представљени, односно нацртани. Проблем изоморфизма графова је веома тежак и до данас није пронађен одговарајући алгоритам за његово решавање који би био значајно различит од непосредног проверавања.

С обзиром на то да изоморфни графови имају исту структуру, можемо увести још једну важну дефиницију.

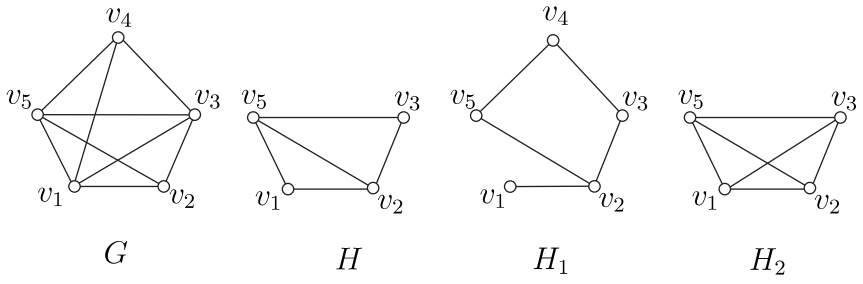
Дефиниција 3.6. *Функција i, дефинисана на скупу графова, се назива* ***инваријанта графова*** *ако за свака два изоморфна графа G_1 и G_2 важи да је $i(G_1) = i(G_2)$.*

Инваријанте графова зависе од структуре графа, а не од начина на који је граф означен. Постоји пуно инваријанти графова, као што су број чворова у графу, број грана у графу, број чворова степена 1, низ степена чворова (сортиран у неопадајући поредак), итд. Оне представљају главни предмет проучавања теорије графова, а могу се, између осталог, користити приликом провере да ли су одговарајући графови изоморфни.

3.5 Подграфови

Дефиниција 3.7. *Нека су $G = (V, E)$ и $G' = (V', E')$ два графа. Граф G' је* ***подграф*** *графа G, у ознаци $G' \subseteq G$, ако и само ако је $V' \subseteq V$ и $E' \subseteq E$. Ако је $V' = V$, за граф G' се каже да је* ***разапињући*** *(****покривајући****)* ***подграф*** *графа G. Кажемо да је граф G'* ***индуковани подграф*** *графа G ако је $V' \subseteq V$ и $E' = E \cap V' \times V'$, тј. граф G' садржи све гране графа G чији су крајњи чворови у V'. У том случају каже се да је граф G' индукован скупом V' и означава се са $G' = G[V']$.*

Према претходној дефиницији, индуковани подграф датог графа G се добија тако што се уочи неки подскуп V' скупа чворова V графа G, а затим се из графа G удаље сви остали чворови, као и гране које су суседне удаљеним чворовима. На тај начин у индукованом подграфу остају само гране које повезују међусобно чворове из V'. Ако је $V' \neq V$, каже се да је G' **прави индуковани подграф** графа G.

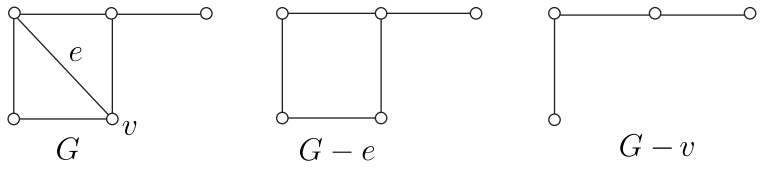


Слика 3.5

Пример 3.6. На слици 3.5 приказан је граф G, његов подграф H, разапињући подграф H_1 и индуковани подграф H_2. Подграф H_2 је индукован скупом чворова $\{v_1, v_2, v_3, v_5\}$.

Ако је e грана графа G, тада је граф $G - e$ подграф графа G добијен из G изостављањем гране e. Аналогно, $G - \{e_1, \ldots, e_k\}$ је подграф графа

G добијен из G изостављањем грана $e_1, \ldots, e_k$. Ако је v чвор графа G, тада је $G - v$ индуковани подграф графа G добијен из G изостављањем чвора v и свих грана графа G које су инцидентне чвору v. Аналогно, граф $G - \{v_1, \ldots, v_k\}$ је индуковани подграф графа G добијен из G изостављањем чворова $v_1, \ldots, v_k$, као и свих грана инцидентних било коме од њих. Ови појмови илустровани су на слици 3.6.



Слика 3.6

3.6 Повезаност графа

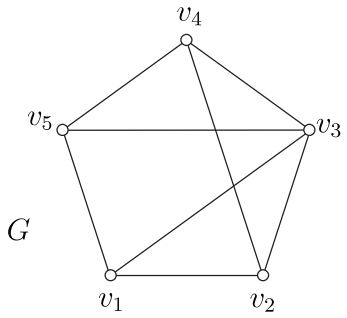
Дефиниција 3.8. *Низ грана $v_0v_1, v_1v_2, \ldots, v_{k-1}v_k$ графа G (или краће $W = v_0v_1v_2 \ldots v_{k-1}v_k$) зове се **шетња** дужине k у графу G. Чвор v_0 је **почетни**, а чвор v_k **завршни** чвор шетње, док су чворови $v_1, \ldots, v_{k-1}$ **унутрашњи** чворови шетње. Шетња са почетним чвором v_0 и завршним чвором v_k зове се $(v_0 - v_k)$-шетња и каже се да **спаја** чворове v_0 и v_k. Шетња $W' = v_iv_{i+1} \ldots v_{j-1}v_j$ $(0 \leqslant i < j \leqslant k)$ представља део шетње W између чворова v_i и v_j и означава се са $W' = W[v_i, v_j]$.*

Шетња дефинисана на претходни начин дозвољава понављање чворова и грана.

Дефиниција 3.9. *Шетња $W = v_0v_1 \ldots v_k$ чије су све гране различите, назива се **стаза** дужине k. Шетња W чији су сви чворови различити назива се **пут** (**отворени пут**) дужине k.*

У графу G, представљеном на слици 3.7, $v_1v_3v_2v_4v_5v_3v_1v_2$ је једна $(v_1 - v_2)$-шетња дужине 7, $v_1v_3v_4v_5v_1v_2$ је једна $(v_1 - v_2)$-стаза дужине 5, док је $v_1v_3v_2v_4v_5$ један $(v_1 - v_5)$-пут дужине 4.

Шетња или стаза $W = v_0v_1v_2 \ldots v_{k-1}v_k$ је **затворена** ако је $v_0 = v_k$. Шетња у којој су сви чворови $v_0, v_1, \ldots, v_k$ међусобно различити, осим почетног и крајњег чвора који се поклапају, зове се **контура** (**затворени пут** или **циклус**).



Слика 3.7

Контура је **парна** ако садржи паран број грана, односно **непарна**, у супротном случају.

У графу G, представљеном на слици 3.7, $v_1v_2v_3v_4v_5v_3v_1$ је једна затворена шетња дужине 6, а $v_1v_2v_3v_4v_5v_1$ је контура дужине 5.

Дефиниција 3.10. *Граф G је повезан ако се свака два његова чвора могу повезати путем. У супротном, граф је неповезан.*

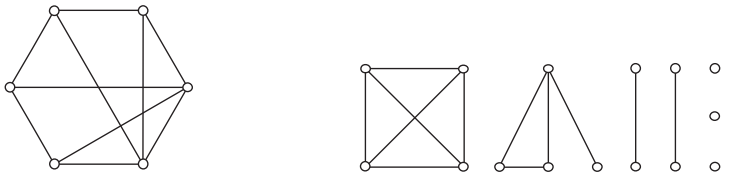
Неповезан граф се састоји од два или више одвојених делова који се називају **компоненте повезаности** (или краће, **компоненте**) графа. Компонента повезаности графа којој припада неки чвор v је подграф образован скупом свих оних чворова који се могу спојити путем са чвором v, укључујући ту и чвор v. Број компоненти повезаности графа G означава се са $\omega(G)$. Из дефиниције повезаности графа следи да је граф повезан ако и само ако има само једну компоненту повезаности.

Ако су $G_1, \ldots, G_k$ $(k \geqslant 2)$ компоненте повезаности графа G, тада је $V(G_i) \cap V(G_j) = \emptyset$, $i, j = 1, \ldots, k$, $i \neq j$, и притом важи да је $V(G) = V(G_1) \cup \cdots \cup V(G_k)$ и $E(G) = E(G_1) \cup \cdots \cup E(G_k)$.

Дефиниција 3.11. *Подграф G_1 графа G је максималан у односу на неку особину, ако он има ту особину, а њу нема ниједан од подграфова графа G у којима се G_1 садржи као прави подграф.*

Уз овакву терминологију, компоненте повезаности графа G су његови максимални повезани подграфови.

ПРИМЕР 3.7. Граф G_1, приказан на слици 3.8, је повезан, док је граф G_2 неповезан и састоји се од седам компоненти повезаности.



Слика 3.8

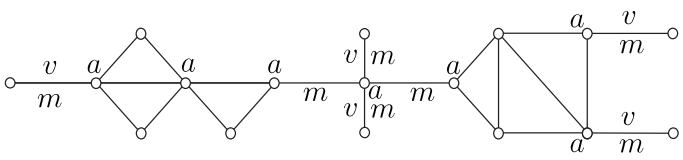
У вези са питањем повезаности графова интересантни су и следећи појмови.

Дефиниција 3.12. ***Артикулациони*** **(*везивни*)** *чвор графа је чвор чијим се удаљавањем из графа повећава број компоненти повезаности графа.*

Мост *графа је грана чијим се удаљавањем из графа повећава број компоненти повезаности графа. Грана која је инцидентна са чвором степена* 1 *назива се* ***висећа грана****.*

Свака висећа грана представља мост графа. Крајеви сваког моста, који није висећа грана, су артикулациони чворови. Ако је мост и висећа грана графа (са више од два чвора), тада је тачно један од његових крајњих чворова артикулациони чвор.

ПРИМЕР 3.8. За граф на слици 3.9 са a, m, v означени су, редом, артикулациони чворови, мостови и висеће гране.



Слика 3.9

Дефиниција 3.13. *Нека је $G = (V, E)$ повезан граф.* ***Растојање*** $d_G(u, v)$ *(или $d(u, v)$) два чвора $u, v \in V$ је дужина најкраћег пута између u и v у графу G.* ***Ексцентрицитет*** $\mathrm{ecc}(u)$ *чвора $u \in V$ је највеће растојање од чвора u до свих осталих чворова у графу, тј.* $\mathrm{ecc}(u) = \max_{v \in V} d_G(u, v)$. ***Дијаметар*** $D(G)$ *графа G је највећи ексцентрицитет, односно* $D(G) = \max_{u \in V} \mathrm{ecc}(u)$*, док је* ***радијус*** $r(G)$ *графа G најмањи ексцентрицитет, тј.* $r(G) = \min_{u \in V} \mathrm{ecc}(u)$.

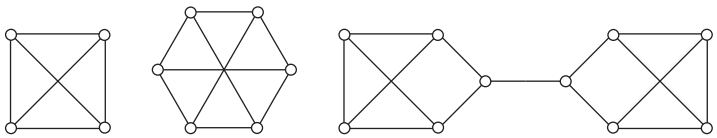
У случају да граф G није повезан, растојање између чворова може се дефинисати за сваки пар чворова из исте компоненте повезаности на начин описан у претходној дефиницији. За чворове u и v из различитих компоненти повезаности графа G, узима се, по конвенцији, да је $d_G(u,v) = \infty$. У том случају су и дијаметар и радијус графа G недефинисани, односно, по конвенцији се узима да су и они једнаки ∞.

3.7 Неке посебне класе графова

Међу бројним графовима поједини су, због својих специфичних особина, добили посебна имена. У овом одељку наводимо неколико таквих врста (класа) графова.

Дефиниција 3.14. *Граф G чији су сви чворови степена r зове се* ***регуларан граф степена*** **r** (*или* **r-*регуларан граф***).

Пример 3.9. Неколико регуларних графова степена 3 представљено је на слици 3.10.



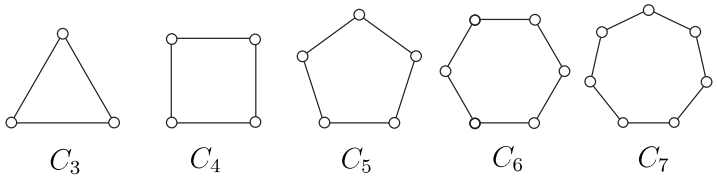
Слика 3.10

Из једнакости (3.1) следи да регуларан граф степена r има $m = \frac{1}{2}nr$ грана, одакле закључујемо да је потребан услов за егзистенцију регуларних графова степена r са n чворова да бар један од бројева n и r буде паран.

Посебно су интересантни регуларни графови степена два.

Дефиниција 3.15. *Повезан регуларан граф степена два зове се* ***контура*** (*или* ***циклус***). *Контура са n чворова означава се са C_n.*

Коначан регуларан граф степена 2 има за компоненте повезаности контуре. Ово не важи за бесконачне графове. Супротан пример је граф чији чворови одговарају целобројним тачакама бројне осе, а суседни су само они чворови чије је међусобно растојање (по оси) једнако 1.



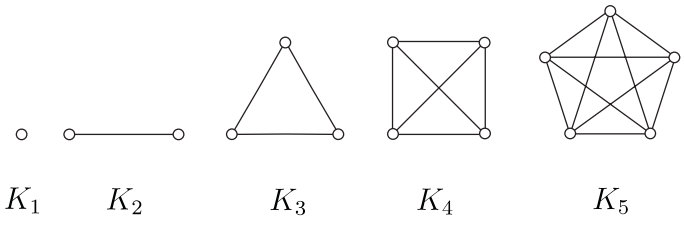
Слика 3.11

ПРИМЕР 3.10. Контуре C_3, C_4, C_5, C_6 и C_7 приказане су на слици 3.11. За неке од контура често се употребљавају и називи из геометрије (троугао, четвороугао, петоугао, . . .).

Дефиниција 3.16. *Граф чија су свака два чвора суседна зове се* ***комплетан*** *или* ***потпун граф****. Комплетан граф са n чворова означава се са K_n.*

Комплетан граф K_n је регуларан граф степена $n-1$ и има $m = \dfrac{n(n-1)}{2} = \binom{n}{2}$ грана.

ПРИМЕР 3.11. На слици 3.12 приказани су комплетни графови K_1, K_2, K_3, K_4 и K_5.



Слика 3.12

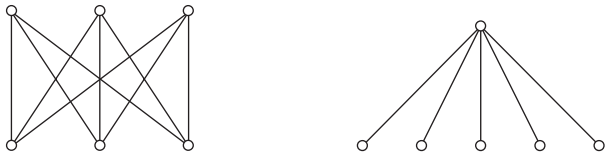
Дефиниција 3.17. ***Празан граф*** *је граф у коме не постоји ниједан пар суседних чворова, тј. састоји се само од изолованих чворова. Празан граф је 0-регуларан граф.*

Дефиниција 3.18. ***Бипартитан граф*** $G = (V, E)$ *је граф чији се скуп чворова V може разбити на два дисјунктна скупа X и Y, тако да свака грана $e \in E$ спаја неки чвор из скупа X са неким чвором из скупа Y. Скупови X и Y називају се* ***партитивни скупови*** *(или* ***класе****).*

Дефиниција 3.19. ***Комплетан бипартитан граф*** (*или* ***бикомплетан граф***) *је бипартитан граф код кога је сваки чвор првог скупа* (*класе*) *суседан са сваким чвором другог скупа* (*класе*). *Ако партитивни скупови садрже* r *и* s *чворова, респективно, тада се комплетан бипартитан граф означава са* $K_{r,s}$.

Бикомплетни графови се називају још и **потпуни бихроматски графови**. Комплетан бипартитан граф $K_{1,n-1}$ зове се **звезда**. Звезда са n чворова означава се и са S_n.

Пример 3.12. На слици 3.13 приказан је комплетан бипартитан граф $K_{3,3}$ и звезда $S_6 = K_{1,5}$.



$K_{3,3}$ $K_{1,5}$

Слика 3.13

Дефиниција 3.20. ***k-партитан граф*** *је граф чији се скуп чворова може разбити на* k *међусобно дисјунктних скупова* (*који се називају класе или партитивни скупови*), *тако да свака грана спаја два чвора која припадају различитим партитивним скуповима.* ***Комплетан k-партитан граф*** (*или* ***k-комплетан граф***) *је* k*-партитан граф, такав да су свака два чвора из различитих партитивних скупова повезана граном, а ниједна грана не повезује чворове из истог партитивног скупа. Ако партитивни скупови садрже редом* $n_1, n_2, \ldots, n_k$ *чворова, тада се комплетан* k*-партитан граф означава са* $K_{n_1,n_2,\ldots,n_k}$.

3.8 Чворна и гранска повезаност

Дефиниција 3.21. *За скуп чворова* $U \subseteq V$ *кажемо да је* ***раздвајајући скуп чворова*** *или* ***чворни сепаратор*** *графа* $G = (V, E)$ *ако граф* $G - U$ *има више од једне компоненте повезаности.*

Сваки граф различит од комплетног графа садржи чворни сепаратор. Наиме, ако је граф неповезан, тада је $U = \emptyset$. Ако је $G \neq K_n$ повезан

граф, тада постоје два несуседна чвора v и w у графу G, одакле следи да је скуп $U = V - \{v, w\}$ раздвајајући скуп чворова у графу G, јер је граф $G - U$ неповезан (састоји се од два изолована чвора v и w).

Дефиниција 3.22. ***Чворна повезаност*** *(или краће* ***повезаност****)* $\kappa(G)$ *графа* G $(G \neq K_n)$ *је минималан број чворова чијим уклањањем из графа настаје неповезан или тривијалан граф (тј. граф* K_1 *који се састоји само од једног изолованог чвора), односно*

$$\kappa(G) = \min |U|,$$

где је U *чворни сепаратор графа* G*.*

Комплетан граф K_n не садржи ниједан раздвајајући скуп чворова, али се удаљавањем $n-1$ чворова своди на тривијалан граф K_1, одакле следи да је $\kappa(K_n) = n-1$. Према дефиницији чворне повезаности графа важи да је $\kappa(G) = 0$ ако и само ако је граф G неповезан граф или је $G \cong K_1$, док је $\kappa(G) = 1$ ако и само ако G је повезан граф са бар једним артикулационим чвором или је $G \cong K_2$.

Дефиниција 3.23. *Граф* G *је* ***чворно*** k***-повезан*** *(или краће* k***-повезан****) ако је* $\kappa(G) \geqslant k$*, тј. ако остаје повезан након уклањања било којих* ℓ *чворова, где је* $\ell < k$*.*

Граф са бар једном граном је 1-повезан ако и само ако је повезан. 2-повезани графови не садрже артикулационе чворове, а њихова карактеризација ће бити дата у наставку.

Менгер[8] је 1927. године доказао да је повезаност графа у вези са бројем дисјунктних путева који спајају различите чворове графа. Да бисмо изложили његов резултат, дефинисаћемо неколико неопходних појмова.

Дефиниција 3.24. *Два пута која повезују чворове* u *и* v *су чворно дисјунктна (тј. дисјунктна у односу на чворове) ако осим чворова* u *и* v *немају других заједничких чворова.*

Дефиниција 3.25. *За скуп* $S \subseteq V$ *каже се да* ***раздваја*** *чворове* u *и* v *графа* $G = (V, E)$ *ако ови чворови припадају различитим компонентама повезаности графа* $G - S$*.*

[8] Karl Menger (1902–1985), аустријско-амерички математичар

Сада ћемо изложити Менгерову теорему, која представља један од фундаменталних резултата теорије графова. Доказ ове теореме, због опширности, неће бити наведен.

Теорема 3.3. (**Менгер**) *Најмањи број чворова који раздваја несуседне чворове u и v једнак је највећем броју дисјунктних $(u-v)$-путева.*

Користећи Менгерову теорему, Витни[9] је 1932. године доказао следеће тврђење, које такође наводимо без доказа.

Теорема 3.4. *Нетривијалан граф је (чворно) k-повезан ако и само ако за свака два различита чвора u и v постоји бар k дисјунктних $(u-v)$-путева у графу G.*

Специјалан случај ове теореме (за $k = 2$) је следећи резултат којим се даје карактеризација 2-повезаних графова.

Последица 3.2. *Граф са n $(n \geqslant 3)$ чворова је 2-повезан ако и само ако свака два његова чвора леже на контури.*

Комплетно уопштење теореме 3.4, које наводимо без доказа, доказао је Дирак[10] 1960. године.

Теорема 3.5. *Ако је G k-повезан граф $(k \geqslant 2)$, тада сваких k чворова графа G леже на контури.*

Претходно уведени појмови дефинишу се и полазећи од грана графа.

Дефиниција 3.26. *За скуп грана $F \subseteq E$ кажемо да је **раздвајајући скуп грана** или **гранични сепаратор** графа $G = (V, E)$ ако граф $G - F$ има више од једне компоненте повезаности.*

Сваки нетривијалан граф (тј. граф различит од K_1) има гранични сепаратор. У случају неповезаног графа важи да је $F = \emptyset$, док је код повезаног нетривијалног графа G скуп свих грана F инцидентних са датим чвором v један гранични сепаратор графа G, јер је $G - F$ неповезан граф са изолованим чвором v.

Дефиниција 3.27. ***Гранична повезаност*** *$\kappa_1(G)$ нетривијалног графа G је минималан број грана чијим уклањањем из графа настаје неповезан или тривијалан граф, односно*

$$\kappa_1(G) = \min |F|,$$

где је F гранични сепаратор графа G.

[9] Hassler Whitney (1907–1989), амерички математичар

[10] Gabriel Andrew Dirac (1925–1984), мађарско-британски математичар

Према дефиницији гранске повезаности графа важи да је $\kappa_1(G) = 0$ ако и само ако је G неповезан или тривијалан граф, док је $\kappa_1(G) = 1$ ако и само ако је G повезан граф који садржи бар један мост.

Дефиниција 3.28. *Граф G је **гранski k-повезан** ако је $\kappa_1(G) \geqslant k$, тј. ако остаје повезан након уклањања било којих ℓ грана, где је $\ell < k$.*

Витни је 1932. године доказао следеће тврђење.

Теорема 3.6. *За сваки граф G важе неједнакости*

$$\kappa(G) \leqslant \kappa_1(G) \leqslant \delta(G), \tag{3.2}$$

где је $\delta(G)$ минималан степен чвора у графу G.

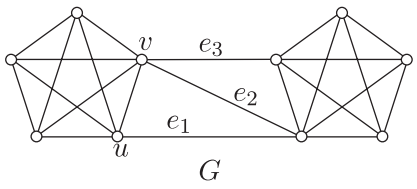
Доказ. Ако је G неповезан или тривијалан граф K_1, тада је $\kappa(G) = \kappa_1(G) = \delta(G)$ и неједнакости (3.2) важе.

Претпоставимо да је G повезан граф са бар два чвора.

Доказ друге неједнакости у (3.2) произилази из чињенице да се удаљавањем $\delta(G)$ грана суседних чвору минималног степена сигурно добија неповезан граф.

Докажимо прву неједнакост у (3.2). Полазећи од произвољног скупа од $\kappa_1(G)$ грана чијим удаљавањем граф постаје неповезан, може се одабрати највише $\kappa_1(G)$ чворова (за сваку удаљену грану по један крајњи чвор) чије удаљавање из графа такође обезбеђује да је резултујући граф неповезан, одакле следи да је $\kappa(G) \leqslant \kappa_1(G)$. □

ПРИМЕР 3.13. За граф G са слике 3.14 важи да је $\kappa(G) = 2$, $\kappa_1(G) = 3$, $\delta(G) = 4$. Одговарајући чворни и гранski сепаратори су $U = \{u, v\}$ и $F = \{e_1, e_2, e_3\}$.



Слика 3.14

3.9 Графови и матрице

Графу G са скупом чворова $V = \{v_1, v_2, ..., v_n\}$ и скупом грана $E = \{e_1, e_2, ..., e_m\}$ могу се придружити различите матрице. Навешћемо неке од њих које се најчешће примењују.

Матрица инциденције чворова и грана графа G је $n \times m$ матрица $R(G) = (r_{ij})$, дефинисана са

$$r_{ij} = \begin{cases} 1, & \text{ако је чвор } v_i \text{ инцидентан са граном } e_j, \\ 0, & \text{у супротном случају.} \end{cases}$$

Број јединица у i-тој врсти ове матрице једнак је броју грана инцидентних са чвором v_i, тј. његовом степену $d(v_i)$, $i = 1, 2, \ldots, n$. С друге стране, у свакој колони се налазе по тачно две јединице, што одговара чињеници да је свака грана инцидентна са два чвора.

Користе се и општије матрице инциденције, чији су елементи, осим 0 и 1, и други бројеви. У случају оријентисаних графова или диграфова користи се матрица инциденције чворова и грана $S(G) = (s_{ij})$ са елементима $-1, 0, 1$, која се дефинише са

$$s_{ij} = \begin{cases} 1, & \text{ако грана } e_j \text{ излази из чвора } v_i, \\ -1, & \text{ако грана } e_j \text{ улази у чвор } v_i, \\ 0, & \text{ако } v_i \text{ и } e_j \text{ нису суседни елементи.} \end{cases}$$

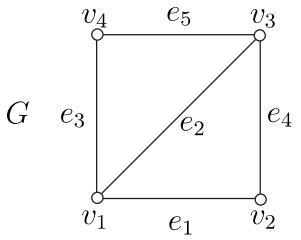
Матрица суседства графа G је $n \times n$ матрица $A(G) = (a_{ij})$, дефинисана са

$$a_{ij} = \begin{cases} 1, & \text{ако су чворови } v_i \text{ и } v_j \text{ суседни,} \\ 0, & \text{у супротном случају.} \end{cases}$$

Матрица суседства A неоријентисаног графа је симетрична матрица, тј. $A = A^T$, при чему је број јединица у i-тој врсти (и i-тој колони) једнак $d(v_i)$. На главној дијагонали (у случају графа без петљи) налазе се нуле. Регуларни графови степена r имају матрицу суседства у чијој се свакој врсти и свакој колони налази тачно r јединица. Матрица суседства комплетних графова има на главној дијагонали елементе једнаке нули, док су сви остали елементи матрице једнаки 1.

За матрицу суседства $A = (a_{ij})$ оријентисаног графа важи

$$a_{ij} = 1 \Rightarrow a_{ji} = 0, \quad i, j = 1, 2, \ldots, n, \; i \neq j.$$



Слика 3.15

За граф G са слике 3.15 матрица инциденције чворова и грана, односно матрица суседства је

$$R(G) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad A(G) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Теорема 3.7. *Нека је $A = (a_{ij})$ матрица суседства произвољног графа G чији су чворови $v_1, v_2, \ldots, v_n$. Елемент $a_{ij}^{(k)}$ из i-те врсте и j-те колоне матрице A^k једнак је броју различитих $(v_i - v_j)$-шетњи дужине k у графу G.*

Доказ. Доказ изводимо математичком индукцијом по k. За $k = 1$ теорема је тачна на основу дефиниције матрице суседства A.

Претпоставимо да теорема важи за $k = s \geqslant 1$.

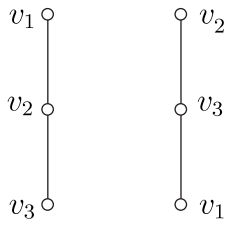
По дефиницији матричног множења, елемент на позицији (i, j) у матрици $A^{s+1} = A \cdot A^s$ једнак је

$$a_{ij}^{(s+1)} = a_{i1}a_{1j}^{(s)} + a_{i2}a_{2j}^{(s)} + \cdots + a_{in}a_{nj}^{(s)}.$$

Нека су $v_{t_1}, v_{t_2}, \ldots, v_{t_\ell}$ чворови до којих се може доћи из чвора v_i шетњом дужине 1. Тада је

$$\begin{aligned} a_{ij}^{(s+1)} &= a_{it_1}a_{t_1j}^{(s)} + a_{it_2}a_{t_2j}^{(s)} + \cdots + a_{it_\ell}a_{t_\ell j}^{(s)} \\ &= a_{t_1j}^{(s)} + a_{t_2j}^{(s)} + \cdots + a_{t_\ell j}^{(s)}. \end{aligned} \tag{3.3}$$

По индуктивној претпоставци $a_{t_pj}^{(s)}$, $p = 1, 2, \ldots, \ell$, представља број $(v_{t_p} - v_j)$-шетњи дужине s, а то је истовремено и број $(v_i - v_j)$-шетњи



Слика 3.16

дужине $s+1$ које пролазе кроз чвор v_{t_p}. Сумирањем оваквих израза за свако t_p добија се број свих $(v_i - v_j)$-шетњи дужине $s+1$, тј. израз (3.3). □

Изоморфни графови могу имати различите матрице суседства. На слици 3.16 су представљена два изоморфна графа G_1 и G_2 (тј. један граф са две различите нумерације) чије су матрице суседства A_1 и A_2 дате са

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

С обзиром на то да су изоморфни графови у ствари исти графови, само различито представљени, и имајући у виду дефиницију матрице суседства, закључујемо да се матрице суседства изоморфних графова могу добити једна из друге одговарајућим пермутовањем врста и колона, при чему је битно да се иста пермутација примењује и на врсте и на колоне. Да бисмо формулисали услов изоморфности графова чије су матрице суседства A_1 и A_2, потребно је увести појам пермутационе матрице.

Дефиниција 3.29. ***Пермутациона матрица*** *је квадратна матрица која у свакој врсти и свакој колони има тачно један елемент једнак* 1*, а сви остали елементи матрице су једнаки* 0*.*

Ако се матрица A помножи (здесна) пермутационом матрицом P, добија се матрица која настаје пермутовањем колона матрице A, док се множењем (слева) матрице A матрицом P^T добија матрица која настаје пермутовањем врста матрице A истом пермутацијом. Како је пермутациона матрица P ортогонална матрица, тј. $P^{-1} = P^T$, следи да ће два графа G_1 и G_2 бити изоморфна ако њихове матрице суседства A_1 и A_2 задовољавају релацију $A_2 = P^{-1}A_1P$, где је P нека пермутациона матрица.

ПРИМЕР 3.14. За матрице суседства A_1 и A_2 графова са слике 3.16 важи релација $A_2 = P^{-1}A_1P$, где је P пермутациона матрица

$$P = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

3.10 Операције са графовима

Над једним или више графова могу се вршити разне операције чији је резултат такође неки граф.

Дефинисаћемо једну унарну и неколико бинарних операција.

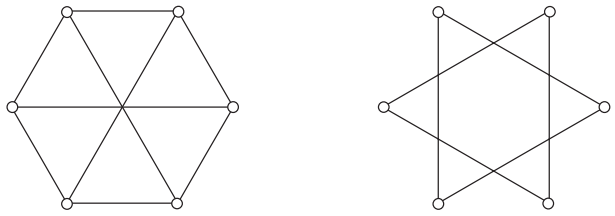
3.10.1 Комплемент графа

Најпре ћемо дефинисати операцију комплементирања графа која је унарна операција.

Дефиниција 3.30. ***Комплемент*** *$\overline{G}$ графа G је граф чији се скуп чворова поклапа са скупом чворова графа G, при чему су два чвора суседна у $\overline{G}$ ако и само ако ти чворови нису суседни у G.*

Из дефиниције следи да је $\overline{(\overline{G})} = G$, тј. комплемент комплемента је полазни граф. Комплемент комплетног графа K_n је празан граф, због чега се он означава са $\overline{K}_n$.

ПРИМЕР 3.15. На слици 3.17 приказан је један пар узајамно комплементарних графова.



Слика 3.17

Матрица суседства $\overline{A}$ графа $\overline{G}$ може се изразити помоћу матрице суседства A графа G. Наиме, према дефиницији комплемента графа,

важи да је $\overline{A} = J - A - I$, где је са J означена матрица чији су сви елементи једнаки 1, а $I = I_n$ је јединична матрица одговарајућег реда.

Теорема 3.8. *Ако је G неповезан граф, тада је његов комплемент $\overline{G}$ повезан, тј. бар један од графова G и $\overline{G}$ је повезан граф.*

Доказ. Потребно је доказати да су у графу $\overline{G}$ произвољна два чвора v и w повезана путем. Како је граф G неповезан, он има бар две компоненте повезаности.

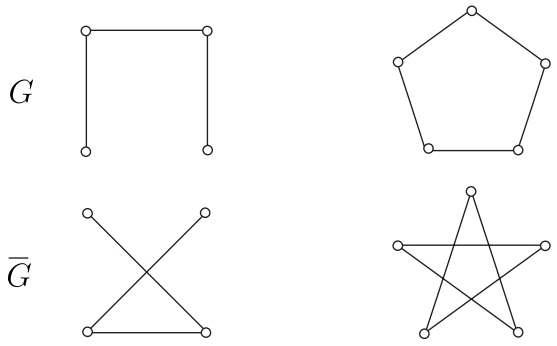
У доказу разликујемо два случаја.

Ако чворови v и w припадају различитим компонентама повезаности графа G, тада су они суседни у графу $\overline{G}$, тј. повезани су путем дужине 1.

Ако чворови v и w припадају истој компоненти повезаности графа G, тада постоји чвор u који не припада тој компоненти повезаности. На основу дефиниције комплемента, чвор u је у графу $\overline{G}$ суседан са чворовима v и w, одакле следи да су чворови v и w повезани путем дужине 2 у графу $\overline{G}$. □

Дефиниција 3.31. *Граф G је **самокомплементаран** ако и само ако је изоморфан свом комплементу $\overline{G}$.*

Граф K_1 је тривијалан пример самокомплементарног графа. Још неки примери самокомплементарних графова дати су на слици 3.18.



Слика 3.18

За самокомплементарне графове важи следећа теорема.

Теорема 3.9. *Ако је G самокомплементаран граф са n чворова, тада је $n \equiv 0 \pmod 4$ или $n \equiv 1 \pmod 4$.*

Доказ. Нека је G граф са n чворова и m грана. Како је $G \cong \overline{G}$, комплемент $\overline{G}$ такође има n чворова и m грана. Обједињавањем скупова грана графова G и $\overline{G}$ добија се комплетан граф, па је $2m = \frac{n(n-1)}{2}$. Одавде је $n(n-1) = 4m$, тј. $4|n(n-1)$. Како су $n-1$ и n узастопни природни бројеви, тачно један од њих је непаран и узајамно прост са бројем 4. Одавде следи да $4|n$ или $4|n-1$, тј. $n \equiv 0 \pmod 4$ или $n \equiv 1 \pmod 4$. □

3.10.2 Унија и потпуни производ графова

Дефинисаћемо две бинарне операције над графовима – унију и потпуни производ графова.

Дефиниција 3.32. *Нека су $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ два графа чији су скупови чворова V_1 и V_2 дисјунктни.* ***Унија*** *$G_1 \cup G_2$ графова G_1 и G_2 је граф $G = (V, E)$, такав да је $V = V_1 \cup V_2$ и $E = E_1 \cup E_2$.*

Према претходној дефиницији следи да је граф унија својих компоненти повезаности.

Дефиниција 3.33. ***Потпуни производ*** *$G_1 \triangledown G_2$ графова G_1 и G_2 је граф који се добија од графа $G_1 \cup G_2$ тако што се сваки чвор из G_1 повеже граном са сваким чвором из G_2.*

Ако са A_1 и A_2 означимо матрице суседства графова G_1 и G_2, редом, тада се, при погодној нумерацији чворова, матрице суседства графова $G_1 \cup G_2$ и $G_1 \triangledown G_2$ могу представити у облику

$$\begin{bmatrix} A_1 & O \\ O & A_2 \end{bmatrix}, \quad \begin{bmatrix} A_1 & J \\ J^T & A_2 \end{bmatrix},$$

где су O и J нула матрица и матрица чији су сви елементи једнаки 1 (одговарајућег реда), респективно.

Имајући у виду дефиницију комплемента графа, као и претходне дефиниције, непосредно се закључује да важи

$$\overline{G_1 \cup G_2} = \overline{G}_1 \triangledown \overline{G}_2, \quad \overline{G_1 \triangledown G_2} = \overline{G}_1 \cup \overline{G}_2.$$

3.11 Стабла

Стабла представљају једну од најједноставнијих, али истовремено и најважнијих класа графова. Стабла су посебно значајна због своје разноврсне примене у електротехници, рачунарству, физици, хемији, итд.

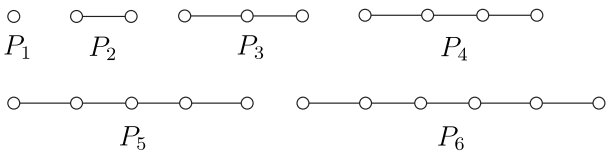
3.11.1 Дефиниција и особине стабала

Дефиниција 3.34. *Повезан граф који не садржи контуре као подграфове назива се* ***стабло*** *или* ***дрво****. Неповезан граф без контура назива се* ***шума****.*

Компоненте повезаности шуме су стабла. Уобичајена ознака за стабло је T. Стабло је **нетривијално** ако има више од једног чвора, у супротном је **тривијално**. У наставку ћемо разматрати само нетривијална стабла и ту чињеницу нећемо посебно истицати.

Дефиниција 3.35. *Стабло у коме ниједан чвор нема степен већи од два назива се* ***пут****. Пут са n чворова означава се са P_n.*

Пример 3.16. На слици 3.19 приказани су путеви са највише шест чворова.



Слика 3.19

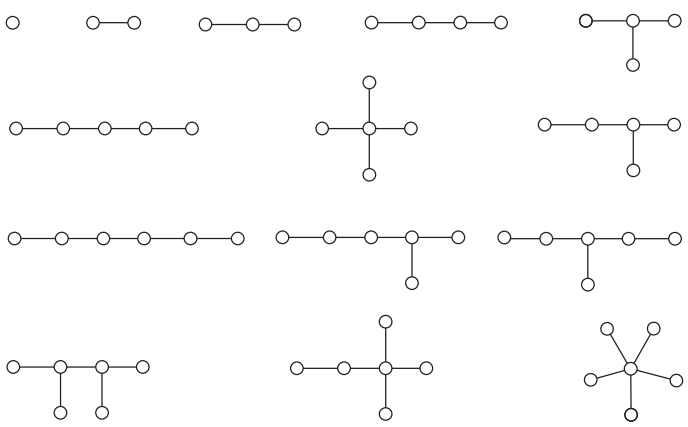
Подсетимо се да се стабло са n чворова које садржи $n-1$ чворова степена 1 назива звезда и означава са $S_n = K_{1,n-1}$.

На слици 3.20 приказана су сва неизоморфна стабла са највише шест чворова. Граф K_1 је једино стабло са једним чвором. То стабло је тривијално стабло. Такође, постоје јединствена стабла са два и три чвора. То су $P_2(\cong S_2)$ и $P_3(\cong S_3)$. Са порастом броја чворова, број различитих стабала нагло расте. Стабла са n чворова добијају се од стабала са $n-1$ чворова додавањем једног чвора и једне гране на све могуће начине, искључујући већ добијена изоморфна стабла.

Најважније особине стабала су изложене у следећим теоремама.

Теорема 3.10. *Свака два чвора стабла повезана су јединственим путем.*

Доказ. Нека су u и v два произвољна чвора стабла T. Како је стабло повезан граф, чворови u и v су повезани путем у стаблу T. Докажимо да је овај пут јединствен. Ако у стаблу T постоје два различита $(u-v)$-пута, P' и P'', тада постоји грана пута P' која не припада путу P''. Нека је



Слика 3.20

$e = w_1w_2$ прва грана пута P' (при кретању путем P' из чвора w_1 у чвор w_2) која не припада путу P'' и нека је w_2' први следећи чвор пута P' који истовремено припада и путу P''. Тада делови путева P' и P'' између чворова w_1 и w_2' образују контуру у стаблу T, што је у супротности са дефиницијом стабла. Дакле, чворови u и v повезани су јединственим путем у стаблу T. □

Теорема 3.11. 1° *Стабло садржи бар два чвора степена* 1.

2° *Ако је* u *чвор степена* 1 *стабла* T, *тада је граф* $T - u$ *такође стабло.*

Доказ. 1° Нека је T стабло и $P = u_1u_2 \dots u_k$, $k \geq 2$, најдужи пут у стаблу T. Доказаћемо да су чворови u_1 и u_k степена 1. Претпоставимо, супротно, да чвор u_1, осим u_2, има бар још једног суседа v. Ако $v \notin V(P)$ тада је $vu_1u_2 \dots u_k$ пут у T дужи од P, што је контрадикција са избором пута P. Ако $v \in V(P)$, тада је $v = u_i$ за неко i, $2 < i \leqslant k$. Међутим, тада је $u_1u_2 \dots u_iu_1$ контура у T, што је контрадикција са чињеницом да је T стабло. Дакле, чвор u_1 је степена 1. Аналогно се доказује да је и чвор u_k степена 1.

2° Докажимо најпре да је граф $T - u$ повезан, односно да за свака два чвора из $T - u$ постоји пут који их спаја. Нека су u_1 и u_2 произвољни чворови графа $T - u$. Како чворови u_1 и u_2 припадају стаблу T, према теореми 3.10 постоји јединствени пут P у T који их повезује. Унутрашњи чворови пута P су степена најмање 2, одакле следи да су различити од чвора u. Дакле, пут P припада графу $T - u$, па закључујемо да је граф $T - u$ повезан. Како стабло T не садржи контуре, ни његов подграф

$T - u$ не садржи контуре, одакле произилази да је $T - u$ повезан граф без контура, тј. стабло. □

Теорема 3.12. *Стабло са n чворова има $n - 1$ грана.*

Доказ. Доказ изводимо индукцијом по броју чворова n.

За $n = 1$ постоји само тривијално стабло K_1 које нема грана. За $n = 2$ постоји јединствено стабло P_2 које садржи тачно једну грану, па тврђење важи.

Претпоставимо да тврђење важи за сва стабла са мање од n чворова и посматрајмо стабло T са n чворова. Према теореми 3.11 стабло T садржи чвор u степена 1, при чему је граф $T - u$ такође стабло са $n - 1$ чворова. За стабло $T - u$ према индуктивној претпоставци важи да је $|E(T - u)| = (n - 1) - 1 = n - 2$. Како је $|E(T)| = |E(T - u)| + 1$, то је $|E(T)| = n - 1$, па тврђење важи и за произвољно стабло са n чворова. □

Теорема 3.13. *Сваки повезан граф садржи стабло као покривајући (разапињући) подграф.*

Доказ. Ако је граф G стабло, доказ је завршен. У супротном, граф G садржи бар једну контуру C. Нека је uv произвољна грана графа G која припада контури C тог графа. Тада у графу G постоје најмање два пута који повезују чворове u и v. Нека су то путеви Q' и $Q'' = uv$. Доказаћемо да је граф $G - uv$, добијен удаљавањем гране uv из графа G, повезан. Нека су w_1 и w_2 произвољни чворови графа $G - uv$. Ови чворови су у графу G повезани путем P. Ако грана uv не припада путу P, тада је P пут у графу $G - uv$ који повезује чворове w_1 и w_2. Ако грана uv припада путу P, тј. $P = w_1 \dots uv \dots w_2$, тада пут $P' + Q' + P''$ повезује чворове w_1 и w_2 у графу $G - uv$, где су $P' = [w_1, u]$ и $P'' = [v, w_2]$ делови пута P. Дакле, ако из графа G удаљимо произвољну грану која припада некој контури тог графа нећемо нарушити повезаност графа. Понављањем овог поступка све док у графу постоји нека контура, на крају се добија повезан граф без контура, тј. стабло. Добијено стабло је покривајући подграф полазног графа. □

Непосредна последица теорема 3.12 и 3.13 је следеће тврђење.

Последица 3.3. *Сваки повезан граф са n чворова садржи најмање $n - 1$ грана. Граф са n чворова и мање од $n - 1$ грана је неповезан.*

Теорема 3.14. *Удаљавањем било које гране из стабла добија се неповезан граф.*

Доказ. Удаљавањем произвољне гране из стабла са n чворова добија се граф са мање од $n-1$ грана који је према последици 3.3 неповезан. □

Теорема 3.15. *Ако се у стабло укључи нова грана између несуседних чворова добија се граф који садржи тачно једну контуру.*

Доказ. Према теореми 3.13, несуседни чворови између којих је укључена нова грана су у стаблу повезани јединственим путем, одакле следи да гране тог пута са новом граном образују контуру. Јединственост добијене контуре произилази из јединствености пута између уочених несуседних чворова. □

ПРИМЕР 3.17. Ако је $(5, 4, 3, 2, 1, 1, \ldots, 1)$ низ степена чворова стабла, одредити колико има јединица у том низу.

Решење. Означимо са n и m број чворова, односно број грана, посматраног стабла. Како је $m = n-1$, то је $2(n-1) = 5+4+3+2+(n-4)\cdot 1$, одакле следи да је $n = 12$, па је тражени број јединица једнак 8. △

ПРИМЕР 3.18. Колико компоненти има шума са 100 чворова и 90 грана?

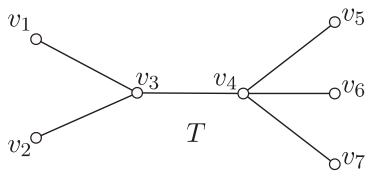
Решење. Нека је T шума са $k = \omega(T)$ компоненти $T_1, T_2, \ldots, T_k$ и означимо са n_i број чворова компоненте T_i, $i = 1, 2, \ldots, k$. Важи да је $n_1 + n_2 + \cdots + n_k = 100$. Како је свака компонента шуме стабло, следи да је $90 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1)$, тј. $90 = 100 - k$, одакле добијамо да је број компоненти шуме једнак 10. △

3.11.2 Коренска стабла

У разним применама су од посебног значаја коренска стабла. Значајна је њихова примена у рачунарским наукама, на пример, у организацији база података, у кодирању и декодирању низова карактера, у теоријском рачунарству за приказивање математичких формула итд. Коренска стабла налазе примену и у ботаници, као и у генеалогији (за приказивање родбинских односа у виду породичних стабала).

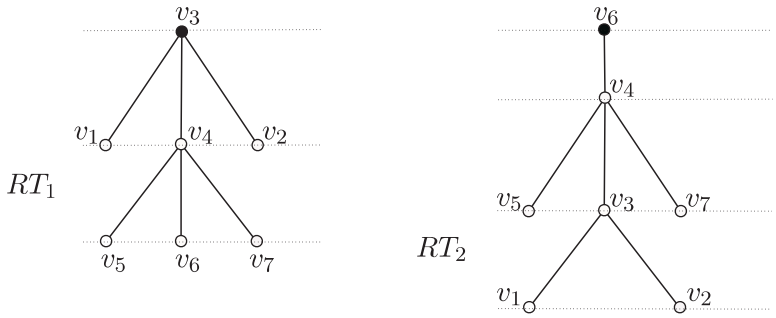
Дефиниција 3.36. *Стабло у коме је један чвор посебно издвојен назива се* ***коренско стабло****, при чему се издвојени чвор назива* ***корен*** *стабла.*

Коренско стабло означавамо као уређен пар $RT = (T, r)$, где је T стабло, а r његов корен.



Слика 3.21

Од једног стабла можемо добити више различитих коренских стабала, бирајући различите чворове за корен стабла. На слици 3.22 представљена су два коренска стабла RT_1 и RT_2 добијена од стабла T са слике 3.21, при чему је у коренском стаблу RT_1 за корен изабран чвор v_3, док је RT_2 коренско стабло чији је корен чвор v_6 (корен је представљен као црни чвор). Према наведеној конвенцији, ова стабла можемо означити и са $RT_1 = (T, v_3)$, односно, $RT_2 = (T, v_6)$.



Слика 3.22

Сваки чвор v коренског стабла $RT = (T, r)$ повезан је јединственим путем са кореном r тог стабла, одакле следи да се чворови коренског стабла могу класификовати у односу на њихово растојање од корена, увођењем појма нивоа чвора.

Дефиниција 3.37. ***Ниво чвора*** *v коренског стабла $RT = (T, r)$ је једнак дужини пута у стаблу T од корена r до чвора v, тј. растојању између чворова r и v и означава се са $n(v)$. Највећи ниво чвора у коренском стаблу назива се* ***висина*** *коренског стабла и означава се са h.*

Пут од корена до сваког чвора коренског стабла је јединствен, па је ниво сваког чвора једнозначно одређен. Ниво корена једнак је 0, а нивои

суседних чворова се разликују за 1. На тај начин се, у односу на корен, може извршити разбијање скупа чворова V коренског стабла на скупове V_i, $0 \leqslant i \leqslant h$, при чему је V_i скуп чворова на растојању i од корена, односно скуп чворова који припадају i-том нивоу. Дакле, скуп чворова V коренског стабла може се представити као $V = V_0 \cup V_1 \cup \cdots \cup V_h$.

ПРИМЕР 3.19. Нивои коренског стабла RT_1 са слике 3.22 приказани су у табели

чвор	v_3	v_1	v_4	v_2	v_5	v_6	v_7
ниво	0	1	1	1	2	2	2

,

а висина овог стабла је $h = 2$.

Нивои чворова коренског стабла RT_2 дати су у табели

чвор	v_6	v_4	v_5	v_3	v_7	v_1	v_2
ниво	0	1	2	2	2	3	3

,

а његова висина је $h = 3$.

При геометријском представљању коренског стабла обично се сви чворови истог нивоа налазе на истој висини, при чему се чворови различитих нивоа представљају одозго надоле, према свом растућем нивоу. Стабла RT_1 и RT_2 са слике 3.22 су геометријски представљена на претходно описани начин.

Коренска стабла налазе примену у генеалогији за формирање породичних стабала, због чега је уобичајено да су у терминологији везаној за коренска стабла користе генеалошки појмови, односно називи одговарајућих родбинских односа.

Дефиниција 3.38. *Нека је $RT = (T, r)$ коренско стабло са скупом чворова V.*

*Ако су чворови $u, v \in V(T)$ суседни и важи да је $n(u) = n(v) - 1$, каже се да је чвор u **родитељ** чвора v, а чвор v је **дете** чвора u.*

*Сваки чвор из $V(T)$ који нема децу назива се **лист** (или **терминални**, односно **завршни** чвор). Сваки чвор из $V(T)$ који није лист зове се **унутрашњи** чвор стабла.*

***Преци** чвора $v \in V(T)$, који није корен, су сви чворови различити од v који припадају путу у стаблу T од корена r до чвора v. **Потомци** чвора $v \in V(T)$, који није лист, су сви чворови из $V(T)$ који имају чвор v као претка.*

***Подстабло** са кореном $v \in V(T)$ коренског стабла RT је подграф стабла RT индукован чвором v и свим његовим потомцима.*

ПРИМЕР 3.20. За коренско стабло RT_1 са слике 3.22 важи:

- чвор v_3 је родитељ чворова v_1, v_2 и v_4, односно чворови v_1, v_2 и v_4 су деца чвора v_3;
- листови стабла RT_1 су чворови v_1, v_2, v_5, v_6, v_7, а његови унутрашњи чворови су v_3 и v_4;
- преци чвора v_6 су чворови v_3 и v_4, а потомци чвора v_3 су чворови $v_1, v_2, v_4, v_5, v_6, v_7$;
- подстабло са кореном v_4 индуковано је чворовима v_4, v_5, v_6, v_7.

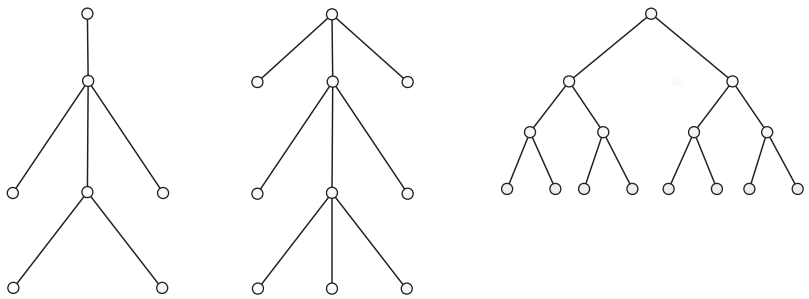
У зависности од тога колико деце може имати сваки чвор, коренска стабла се могу класификовати на следећи начин.

Дефиниција 3.39. *Коренско стабло се назива m-арно стабло ако и само ако сваки његов унутрашњи чвор има највише m деце. За $m = 2$ одговарајуће стабло се назива* ***бинарно*** *стабло.*

Стриктно *m-арно стабло је стабло чији сваки унутрашњи чвор има тачно m деце.*

Потпуно *m-арно стабло је стриктно m-арно стабло код кога сви листови имају исти ниво.*

ПРИМЕР 3.21. На слици 3.23 приказана су три стабла, од којих је прво 3-арно стабло (понекад се назива и тринарно стабло), које није стриктно, друго стабло је стриктно 3-арно стабло, а треће је потпуно бинарно стабло.



Слика 3.23

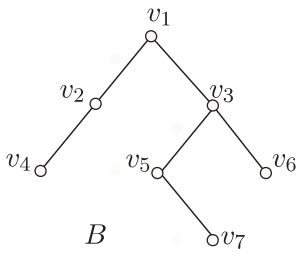
У потпуном бинарном стаблу на нивоу i постоји тачно 2^i чворова, одакле следи да је број чворова потпуног бинарног стабла висине h

једнак

$$n = 1 + 2 + 2^2 + \cdots + 2^h = 2^{h+1} - 1,$$

при чему је број терминалних чворова (листова) једнак $2^h = \dfrac{n+1}{2}$, док унутрашњих чворова има $2^h - 1 = \dfrac{n-1}{2}$.

Код бинарних стабала понекад је потребно да се разликују деца сваког унутрашњег чвора и у складу са тим уводи се појам уређеног стабла у коме су деца сваког унутрашњег чвора дата у одређеном поретку.



Слика 3.24

Дефиниција 3.40. ***Уређено бинарно стабло*** *B је бинарно стабло у коме се за сваки унутрашњи чвор једно његово дете сматра за лево, а друго за десно. У случају да чвор има само једно дете, оно је или лево или десно дете.*

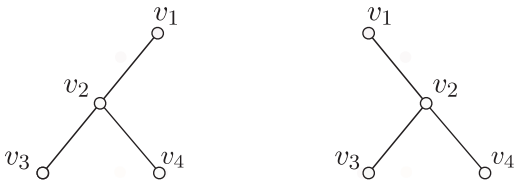
Лево подстабло *унутрашњег чвора v уређеног бинарног стабла B је подстабло стабла B са кореном у левом детету чвора v.*

Десно подстабло *унутрашњег чвора v уређеног бинарног стабла B је подстабло стабла B са кореном у десном детету чвора v.*

ПРИМЕР 3.22. У бинарном стаблу B са слике 3.24 чвор v_5 је лево дете, а чвор v_6 десно дете унутрашњег чвора v_3. Чвор v_5 има само десно дете, а то је чвор v_7. Лево подстабло чвора v_1 је подстабло са кореном v_2 индуковано чворовима v_2 и v_4. Десно подстабло чвора v_1 је подстабло са кореном v_3 индуковано чворовима v_3, v_5, v_6, v_7.

ПРИМЕР 3.23. Одредити колико има уређених бинарних стабала са четири чвора (означена са v_1, v_2, v_3, v_4) код којих је чвор v_1 корен, чвор v_2 његово дете, а чворови v_3 и v_4 су деца чвора v_2.

Решење. Како у овом стаблу чвор v_2 може бити лево или десно дете, постоје два бинарна стабла са траженим особинама, и она су приказана на слици 3.25. △



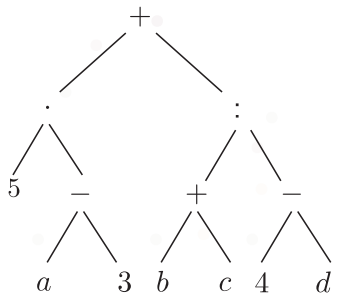
Слика 3.25

Коренским стаблима се представљају различите хијерархијске структуре, а посебно хијерархијске структуре података у рачунарству. При томе нарочито значајну улогу имају бинарна стабла која се, између осталог, могу користити при приказивању алгебарских формула, у организацији скупа уређених података у рачунару, у кодирању података итд. Размотрићемо примену бинарних стабала у представљању алгебарских формула.

Често се у рачунарству једна алгебарска формула представља у облику стриктног уређеног бинарног стабла које се формира на следећи начин. Бинарне операције формуле се приказују као унутрашњи чворови овог стабла, док његовим листовима одговарају променљиве и константе формуле. За сваки унутрашњи чвор важи да његово лево подстабло приказује леву подформулу, а десно подстабло приказује десну подформулу над којима се врши операција додељена овом чвору. Чворови операција мањег приоритета имају мањи ниво, док чворови операција већег приоритета имају већи ниво. На тај начин ће операција најмањег приоритета, тј. она која се последња извршава приликом израчунавања формуле, одговарати корену бинарног стабла. Да би стабло које се додељује алгебарској формули било стриктно, потребно је да она садржи само бинарне операције.

ПРИМЕР 3.24. Алгебарску формулу $5\cdot(a-3)+(b+c) : (4-d)$ представити помоћу стриктног уређеног бинарног стабла.

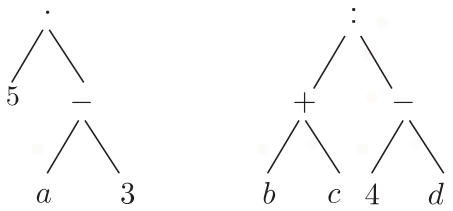
Решење. Овој алгебарској формули одговара уређено бинарно стабло приказано на слици 3.26. Листовима стабла одговарају променљиве и константе алгебарске формуле, тј. симболи $5, a, 3, b, c, 4, d$, док су унутрашњим чворовима додељени симболи операција формуле. Корену



Слика 3.26

стабла одговара операција $+$ која је најнижег приоритета. Лево подстабло корена одговара подформули $5 \cdot (a-3)$, а десно подстабло корена одговара подформули $(b+c) : (4-d)$. △

Једна алгебарска формула се може реконструисати на основу свог бинарног стабла коришћењем неког од алгоритама за обилазак свих чворова бинарног стабла. Постоје три стандардна начина обиласка чворова – **КЛД**, **ЛКД** и **ЛДК**. Слова **К, Л, Д** су скраћенице од речи **корен, лево** и **десно подстабло**, па називи ових обилазака означавају редослед по којима се они врше. На пример, код **КЛД** обиласка прво обилазимо корен стабла, затим цело његово лево подстабло и на крају цело његово десно подстабло, при чему при обиласку сваког подстабла користимо исти **КЛД** принцип (слика 3.27).



Слика 3.27

ПРИМЕР 3.25. Одредити редослед обиласка чворова бинарног стабла приказаног на слици 3.26 при КЛД, ЛКД и ЛДК обиласку овог стабла.

Решење. При **КЛД** обиласку овог стабла, где се прво обилази корен, затим лево подстабло и на крају десно подстабло, редослед обиласка чворова је

$$+ \quad \cdot \quad 5 \quad - \quad a \quad 3 \quad : \quad + \quad b \quad c \quad - \quad 4 \quad d.$$

При **ЛКД** обиласку овог стабла, где се прво обилази лево подстабло, затим корен и на крају десно подстабло, редослед обиласка чворова је

$$5 \cdot a - 3 + b + c : 4 - d.$$

При **ЛДК** обиласку овог стабла, где се прво обилази лево, затим десно подстабло, па корен, редослед обиласка чворова је

$$5\ a\ 3 - \cdot\ b\ c + 4\ d - : +.$$

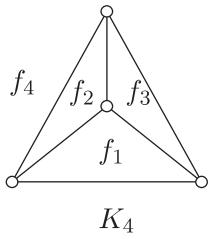
△

3.12 Планарни графови

Дефиниција 3.41. *Граф се може* ***смести у раван*** *ако се може нацртати у равни тако да му се гране не секу, односно ако га је могуће представити у равни тако да заједничка тачка две гране може бити само чвор графа који представља заједничку крајњу тачку тих грана. За граф кажемо да је* ***планаран*** *ако се може сместити у раван.*

Ако је планаран граф смештен у равни, он дели раван на више области, од којих је једна бесконачна, а остале су коначне. Свака коначна област зове се **окце** или **ћелија**.

ПРИМЕР 3.26. Граф K_4, представљен на слици 3.28, је планаран и дели раван на области f_1, f_2, f_3, f_4, при чему је f_4 спољашња област, која је бесконачна (неограничена).



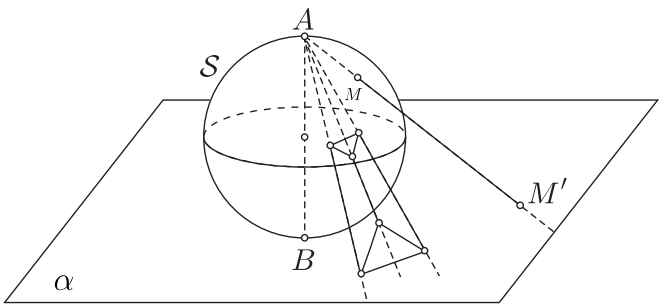
K_4

Слика 3.28

Пример планарног графа је граф придружен мрежи путева, ако не постоје надвожњаци или саобраћајне петље. Постоје и разне техничке примене у којима је потребно да одговарајући граф буде планаран.

Осим смештања графова у равни, може се говорити о смештању графова и на некој другој површи, нпр. сфери. У том случају се чворови графа представљају тачкама на сфери, а гране луковима кривих које припадају сфери и које осим чворова које повезују немају других заједничких тачака.

Граф G који се може сместити у раван, може се сместити и на сферу, и обрнуто. Заиста, претпоставимо да је граф могуће сместити на сферу $\mathcal{S}$. Уочимо произвољну тачку A сфере $\mathcal{S}$ која се не поклапа ни са једним чвором графа G, нити припада некој грани овог графа. Означимо са B дијаметрално супротну тачку тачке A (слика 3.29). Нека је α тангентна раван сфере $\mathcal{S}$ кроз тачку B. **Стереографска пројекција** сфере на раван



Слика 3.29

је пресликавање $\pi_A : \mathcal{S} \setminus \{A\} \to \alpha$ дефинисано са $\pi_A(M) = M'$, где је M' тачка пресека праве MA и равни α. Ово пресликавање је бијекција скупа тачака сфере без тачке A, тј. скупа $\mathcal{S} \setminus \{A\}$, на скуп тачака равни α. Стереографска пројекција π_A графа G који је смештен на сфери $\mathcal{S}$ је планаран граф G' смештен у равни α. Аналогно тврђење важи и у обрнутом смеру, где је одговарајућа бијекција инверзно пресликавање π_A^{-1}, које слика планаран граф смештен у равни α у граф смештен на сфери $\mathcal{S}$. Имајући у виду претходна разматрања, планаран граф се некад дефинише као граф који се може сместити у раван или на сферу.

Међу најважније резултате теорије графова убраја се Ојлерова теорема за планарне графове.

Теорема 3.16. (**Ојлер**) *Повезан планаран граф са n чворова и m грана дели раван на $f = m - n + 2$ области.*

Доказ. Доказ изводимо математичком индукцијом по броју грана.

Минималан број грана повезаног графа са n чворова је $n-1$ и такав граф представља стабло (теорема 3.12 и последица 3.3). Стабло не ограничава ни једну коначну област, па је $f = 1$. Како је $(n-1) - n + 2 = 1$, у овом случају важи Ојлерова формула.

Претпоставимо да тврђење важи за све повезане планарне графове са мање од m грана и посматрајмо повезан планаран граф G са n чворова и m ($m > n-1$) грана који дели раван на f области. Како је $m \geqslant n$, граф G садржи бар једну контуру C. Нека је e произвољна грана која припада контури C. Ова грана је гранична за две области, па њеним уклањањем из графа од две области које она раздваја настаје једна, одакле следи да граф $G - e$ дели раван на $f - 1$ области. Како грана e није мост, јер припада контури, следи да је $G - e$ повезан планаран граф са n чворова, $m - 1$ грана и $f - 1$ области за који према индуктивној претпоставци важи Ојлерова формула, тј. $f - 1 = (m-1) - n + 2$, одакле добијамо да за граф G са m грана важи $f = m - n + 2$. □

Једноставно се доказује да важи следеће уопштење Ојлерове формуле.

Теорема 3.17. *За планаран граф са n чворова, m грана, f области и $\omega(G)$ компоненти повезаности важи једнакост $f = m - n + 1 + \omega(G)$.*

Ојлерова теорема има бројне последице. У наставку ћемо навести неке од њих.

Теорема 3.18. *Ако је G повезан планаран граф са n чворова и m грана у коме најкраћа контура има дужину g, тада је $m \leqslant \dfrac{g(n-2)}{g-2}$.*

Доказ. Нека је f број области које планаран граф G одређује у равни. Свака област $\mathcal{O}_i$, $i = 1, 2, \ldots, f$, ограничена је, по претпоставци, са најмање g грана, тј. важи да је $|\mathcal{O}_i| \geqslant g$. Како свака грана припада двема областима (тј. свака грана се по два пута појављује као граница области, и то за исту област, ако је грана мост, односно за две различите области, у супротном), важи да је

$$2m = \sum_{i=1}^{f} |\mathcal{O}_i| \geqslant g \cdot f,$$

тј.

$$f \leqslant \frac{2m}{g}. \tag{3.4}$$

Са друге стране, како је G планаран граф, према Ојлеровој теореми важи да је $2 = n - m + f$, одакле, имајући у виду (3.4), добијамо

$$2 = n - m + f \leqslant n - m + \frac{2m}{g} = n - \frac{m(g-2)}{g},$$

тј.

$$m \leqslant \frac{g(n-2)}{g-2}.$$

□

Последица 3.4. *У повезаном планарном графу постоји бар један чвор степена мањег од* 6*, тј. за минимални степен чвора* δ *важи да је* $\delta \leqslant 5$*.*

Доказ. Нека је δ минималан степен чвора повезаног планарног графа G. Како је свака област коју граф G одређује у равни ограничена са најмање три гране, добијамо, применом теореме 3.18 (за $g = 3$)

$$n \cdot \delta \leqslant \sum_{v \in V(G)} d(v) = 2m \leqslant 6n - 12,$$

тј.

$$\delta \leqslant 5.$$

□

Дефиниција 3.42. *Планаран граф* G *је* ***максималан*** *ако додавањем ма које нове гране престаје да буде планаран, тј. граф* $G + uv$ *је непланаран за сваки пар несуседних чворова* $u, v \in V(G)$*.*

Све области максималног планарног графа (укључујући и бесконачну) су троуглови, одакле, применом теореме 3.18 (за $g = 3$), закључујемо да важи следеће тврђење.

Последица 3.5. *За сваки планаран граф са* n $(n \geqslant 3)$ *чворова и* m *грана важи да је* $m \leqslant 3n - 6$*.*

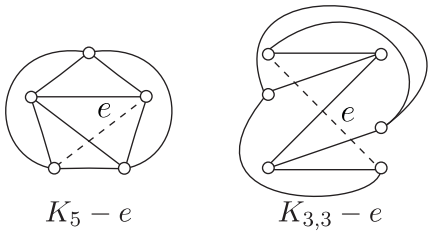
Последица 3.6. *Граф* K_5 *(потпуни пентаграф) није планаран граф.*

Доказ. Претпоставимо да је граф K_5 планаран. Како је $n = 5$ и $m = 10$, применом Ојлерове формуле добијамо да је $f = m - n + 2 = 7$. Како је свака област коју граф K_5 одређује у равни ограничена са најмање три гране, следи да је $2m \geqslant 3f$, тј. $20 \geqslant 21$, што је немогуће. □

Последица 3.7. *Граф* $K_{3,3}$ *(потпуни биграф) није планаран граф.*

Доказ. Претпоставимо да је граф $K_{3,3}$ планаран. Како је $n = 6$ и $m = 9$, применом Ојлерове формуле добијамо да је $f = m - n + 2 = 5$. Свака област коју граф $K_{3,3}$ одређује у равни ограничена је са најмање четири гране, па је $2m \geqslant 4f$, тј. $18 \geqslant 20$, што је немогуће. □

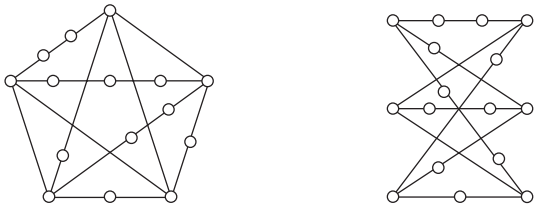
ПРИМЕР 3.27. Графови $K_5 - e$ и $K_{3,3} - e$ (e је произвољна грана ових графова) су планарни, јер се могу представити у равни тако да им се гране не секу (слика 3.30).



Слика 3.30

Сваки подграф планарног графа је планаран, одакле следи, имајући у виду последице 3.6 и 3.7, да граф који садржи неки од графова K_5 или $K_{3,3}$ као подграф није планаран. Очигледно, сваки потпуни граф са више од четири чвора је непланаран.

Дефиниција 3.43. *Потподела гране $e = uv$ графа G врши се уметањем нових чворова $w_1, w_2, \ldots, w_k$, $k \geqslant 0$, степена 2 између чворова u и v, тј. заменом гране $e = uv$ путем $uw_1w_2 \ldots w_kv$. Граф G' добијен потподелом неких грана графа G, назива се* **потподела** *графа G.*



Слика 3.31

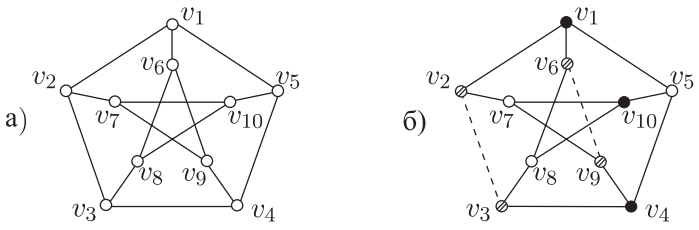
Према дефиницији потподеле и последицама 3.6 и 3.7 следи да граф који садржи потподелу графа K_5 или потподелу графа $K_{3,3}$ (приказане на слици 3.31) није планаран. Међутим, важи и обрнуто тврђење. Овај

значајан резултат, којим су у потпуности окарактерисани планарни графови, доказали су, независно један од другог, Понтрјагин[11] 1929. године и Куратовски 1930. године.

Теорема 3.19. (**Понтрјагин–Куратовски**) *Граф је планаран ако и само ако не садржи као подграф ни граф K_5, ни граф $K_{3,3}$, ни неку њихову потподелу.*

Доказ ове теореме, који се може наћи у [25], је веома сложен, због чега га нећемо наводити.

Пример 3.28. Доказати да Петерсенов[12] граф, приказан на слици 3.32 а), није планаран.



Слика 3.32

Решење. Доказаћемо да Петерсенов граф није планаран на два начина.

Први начин. Уочимо подграф Петерсеновог графа добијен избацивањем грана v_2v_3 и v_6v_9, приказан на слици 3.32 б). Овај подграф представља потподелу потпуног битриграфа $K_{3,3}$, при чему црни чворови v_1, v_4, v_{10} чине једну партицију скупа чворова графа $K_{3,3}$, бели чворови v_5, v_7, v_8 чине другу партицију, а преостали чворови чине потподелу одговарајућих грана. Према теореми 3.19 Петерсенов граф није планаран.

Други начин. Претпоставимо да је Петерсенов граф планаран. Како је $n = 10$ и $m = 15$, применом Ојлерове формуле добијамо да је $f = m - n + 2 = 7$. Свака област коју Петерсенов граф одређује у равни ограничена са најмање пет грана, одакле следи да је $2m \geqslant 5f$, односно $30 \geqslant 35$, што је немогуће. △

[11] Lev Semenovich Pontryagin (1908–1988), руски математичар
[12] Julius Petersen (1839–1910), дански математичар

ПРИМЕР 3.29. Доказати да је потребан услов да граф G и његов комплемент $\overline{G}$ буду планарни дат са $n^2 - 13n + 24 \leqslant 0$, где је n, $n \geqslant 3$, број чворова ових графова.

Решење. Означимо са m и $\overline{m}$ број грана графова G и $\overline{G}$, респективно. Како је $m + \overline{m} = \binom{n}{2}$, следи да је $\max\{m, \overline{m}\} \geqslant \frac{1}{2}\binom{n}{2}$, одакле, на основу последице 3.5, следи да је $\frac{1}{2}\binom{n}{2} \leqslant 3n - 6$, односно $n^2 - 13n + 24 \leqslant 0$. $\triangle$

3.12.1 Примена у геометрији

Сваком полиедру P може се придружити планаран граф $G(P)$ који се добија као његова стереографска пројекција. Наиме, полиедар P се може деформисати тако да се око њега може описати сфера, при чему се не мења број темена, ивица и страна полиедра. Овај поступак се може извести тако да се, након пројектовања темена и ивица полиедра зрацима из центра сфере, на сфери добија граф, који одговара полиедру, чије се гране не секу, тј. граф који је смештен на сфери. Стереографском пројекцијом се добијени граф са сфере пројектује на раван која додирује сферу, при чему је потребно да се центар пројекције не налази на некој грани или у неком чвору графа са сфере. На тај начин се у равни добија планаран граф $G(P)$ чији је број чворова, грана и области једнак броју темена, ивица и страна полиедра P, респективно.

Обрнуто тврђење не важи, тј. за произвољан повезан планаран граф H не мора да постоји полиедар P такав да је $G(P) \cong H$. Наиме, како из сваког темена полиедра излазе бар три ивице, следи да је $\delta(H) \geqslant 3$ један од потребних услова да H буде придружени граф неког полиедра.

Нека је $G = G(P)$ повезан планаран граф који одговара полиедру P. Означимо са F, E и V скуп страна, ивица и темена полиедра P, редом, а са f, m и n број области, грана и чворова графа G, редом. Тада је $|F| = f$, $|E| = m$, $|V| = n$. На основу Ојлерове теореме за планарне графове, важи следеће тврђење.

Теорема 3.20. *За сваки полиедар са n темена, m ивица и f страна важи да је $f - m + n = 2$.*

Ако са f_k означимо број страна полиедра ограничених са k ивица, а са n_k број темена полиедра из којих излази k ивица, $k \geqslant 3$, тада је

$$\sum_{k \geqslant 3} k f_k = \sum_{k \geqslant 3} k n_k = 2m. \tag{3.5}$$

На основу последице 3.4 следи да у сваком полиедру постоји теме из кога излази највише 5 ивица. Слично тврђење важи и за стране полиедра.

Теорема 3.21. *Сваки полиедар садржи страну ограничену многоуглом који има највише* 5 *страница.*

Доказ. Претпоставимо да су све стране полиедра ограничене многоугловима који имају бар 6 страница. Одавде следи да је $f_3 = f_4 = f_5 = 0$. Из (3.5) следи да је

$$2m = \sum_{k\geqslant 6} kf_k \geqslant \sum_{k\geqslant 6} 6f_k = 6\sum_{k\geqslant 6} f_k = 6f,$$

односно

$$f \leqslant \frac{1}{3}m. \tag{3.6}$$

Слично, из

$$2m = \sum_{k\geqslant 3} kn_k \geqslant \sum_{k\geqslant 3} 3n_k = 3\sum_{k\geqslant 3} n_k = 3n,$$

добијамо

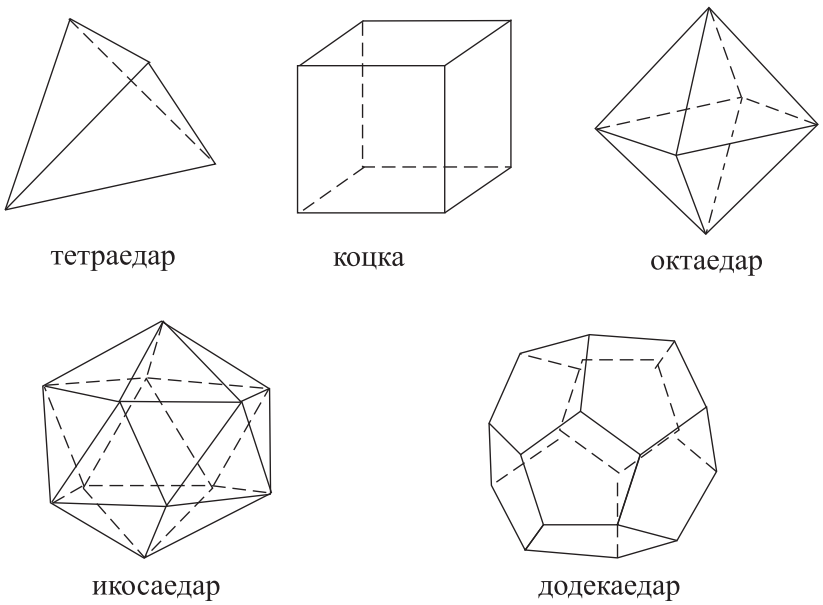
$$n \leqslant \frac{2}{3}m. \tag{3.7}$$

Заменом (3.6) и (3.7) у Ојлеровој формули $f - m + n = 2$, добијамо да је $m = f + n - 2 \leqslant \frac{1}{3}m + \frac{2}{3}m - 2$, тј. $m \leqslant m - 2$, што је немогуће. □

Дефиниција 3.44. ***Правилан полиедар*** *или* ***Платоново тело*** *је полиедар чије су све стране међусобно подударни многоуглови и из чијег сваког темена излази исти број ивица.*

За правилан полиедар важи да је $f = f_s$ и $n = n_t$, за неке $s, t \geqslant 3$. Правилних полиеадра има пет и то је било познато још античким математичарима пре више од 2000 година. То су тетраедар, коцка (хексаедар), октаедар, икосаедар и додекаедар (слика 3.33). Њихове стереографске пројекције приказане су на слици 3.34.

Теорема 3.22. *Постоји тачно пет правилних полиедара.*



Слика 3.33

Доказ. Нека је P правилан полиедар и $G(P)$ њему придружен планаран граф. Тада је $f - m + n = 2$, одакле, користећи једнакости (3.5), добијамо

$$\begin{aligned} -8 &= 4m - 4f - 4n = 2m + 2m - 4f - 4n \\ &= \sum_{k\geqslant 3} kf_k + \sum_{k\geqslant 3} kn_k - 4\sum_{k\geqslant 3} f_k - 4\sum_{k\geqslant 3} n_k \\ &= \sum_{k\geqslant 3}(k-4)f_k + \sum_{k\geqslant 3}(k-4)n_k. \end{aligned}$$

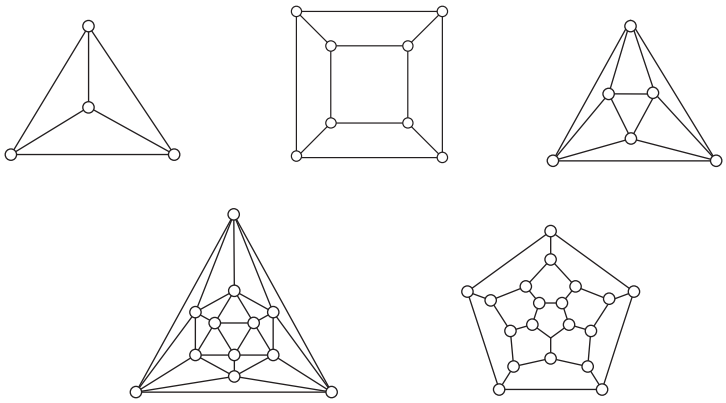
Како је $f = f_s$ и $n = n_t$, за неке $s, t \geqslant 3$, следи да је

$$-8 = (s-4)f_s + (t-4)n_t.$$

На основу последице 3.4 и теореме 3.21 важи $3 \leqslant s,\ t \leqslant 5$. Осим тога, из једнакости (3.5) добијамо да је $sf_s = tn_t = 2m$, односно $sf_s - tn_t = 0$.

Посматрајмо систем линеарних једначина

$$\begin{aligned} (s-4)f_s + (t-4)n_t &= -8 \\ sf_s - tn_t &= \quad 0 \end{aligned}$$



Слика 3.34

по непознатим f_s и n_t, $3 \leqslant s,\ t \leqslant 5$. Овај систем је немогућ за $s = t = 4$, а има решење

$$f_s = \frac{-8t}{t(s-4)+s(t-4)}, \quad n_t = \frac{-8s}{t(s-4)+s(t-4)},$$

ако је $s \neq 4$ или $t \neq 4$.

Добијена решења су позитивна ако је $t(s-4)+s(t-4) < 0$, односно у следећих пет случајева.

1) Ако је $s = t = 3$, тада је $f_3 = n_3 = 4$ и полиедар P је **тетраедар**.

2) Ако је $s = 3$ и $t = 4$, тада је $f_3 = 8$, $n_4 = 6$ и полиедар P је **октаедар**.

3) Ако је $s = 3$ и $t = 5$, тада је $f_3 = 20$, $n_5 = 12$ и полиедар P је **икосаедар**.

4) Ако је $s = 4$ и $t = 3$, тада је $f_4 = 6$, $n_3 = 8$ и полиедар P је **коцка** (**хексаедар**).

5) Ако је $s = 5$ и $t = 3$, тада је $f_5 = 12$, $n_3 = 20$ и полиедар P је **додекаедар**.

Користећи геометријске аргументе, лако се доказује да су ово једини правилни полиедри у сваком појединачном случају. □

3.13 Бојење графова

Дефиниција 3.45. *Граф се **боји** тако што се сваком чвору придружује нека боја, тј. сваки чвор се боји једном бојом. Граф је **правилно обојен** ако*

су свака два суседна чвора обојена различитим бојама. Правилно бојење графа у којем је употребљено k боја зове се ***k-бојење****.*

Дефиниција 3.46. ***Хроматски број*** *$\chi(G)$ графа G једнак је најмањем броју боја потребних да се граф правилно обоји. Ако је $\chi(G) = k$, за граф G кажемо да је* ***k-хроматски****, а ако је $\chi(G) \leqslant k$, кажемо да је граф G* ***k-обојив****.*

Пример 3.30. Важи да је $\chi(K_n) = n$, $\chi(P_n) = 2$ ($n \geqslant 2$), $\chi(C_n) = 2$, ако је n паран број, односно $\chi(C_n) = 3$, у супротном. Ако је G бипартитан граф, тада је G 2-обојив граф, при чему је $\chi(G) = 1$ ако и само ако је $G \cong \overline{K}_n$ (тј. G се састоји само од изолованих чворова), док је сваки непразан бипартитан граф 2-хроматски (или **бихроматски**).

Скуп свих чворова графа обојених истом бојом назива се **хроматска класа**. Произвољна два чвора из исте хроматске класе су несуседна. За њих кажемо да су **независни**. Према дефиницији хроматског броја, следи да је он једнак минималном броју дисјунктних подскупова (хроматских класа) на које се може разбити скуп чворова графа, тако да су чворови сваког подскупа независни.

Следећа два тврђења непосредно следе из дефиниције хроматског броја.

Теорема 3.23. *Ако је H подграф графа G, тада је $\chi(H) \leqslant \chi(G)$.*

Теорема 3.24. *Ако су $G_1, G_2, \ldots, G_s$, $s \geqslant 1$, компоненте повезаности графа G, тада је $\chi(G) = \max\limits_{1 \leqslant i \leqslant s} \chi(G_i)$.*

Ако граф G садржи као подграф комплетан граф са k чворова, тада је $\chi(G) \geqslant k$. Комплетни подграфови са највећим бројем чворова називају се **клике** графа. Ако са $K(G)$ означимо број чворова произвољне клике графа, тада је

$$\chi(G) \geqslant K(G).$$

Наведена доња граница за хроматски број графа може бити доста груба, тј. постоје графови без троуглова (код којих је $\chi(G) = 2$) са произвољно великим хроматским бројем.

Теорема 3.25. *За сваки природан број k постоји k-хроматски граф који не садржи троуглове.*

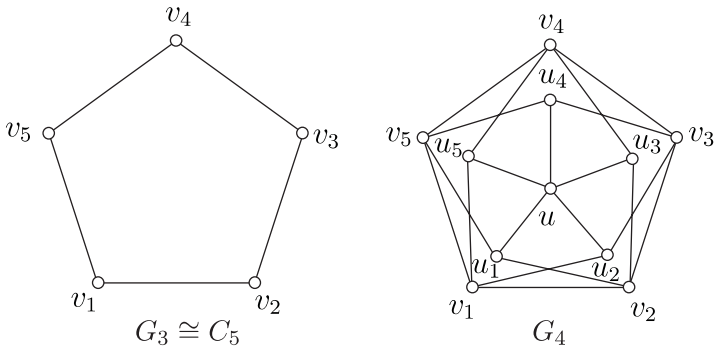
Доказ. Доказ изводимо математичком индукцијом по k. За $k = 1, 2, 3$ тражени графови су редом K_1, K_2, C_5 и за њих тврђење важи.

Нека је G_k k-хроматски граф ($k \geqslant 3$) који не садржи троуглове. Показаћемо да се овај граф може трансформисати у $(k+1)$-хроматски граф G_{k+1} који такође не садржи троуглове. Конструкција коју ћемо навести потиче од Мисиелског[13]. Нека је

$$V(G_k) = \{v_1, v_2, \ldots, v_n\}, \quad V(G_{k+1}) = V(G_k) \cup \{u, u_1, u_2, \ldots, u_n\},$$

где су $u, u_1, u_2, \ldots, u_n$ нови чворови, при чему је чвор u суседан са сваким од чворова u_i, $i = 1, 2, \ldots, n$, док је сваки чвор u_i суседан са свим суседима чвора v_i, $i = 1, 2, \ldots, n$, као и са чвором u. Осим тога, све гране графа G_k су садржане у графу G_{k+1}.

На слици 3.35 је приказан граф G_4, познат као Гречеов[14] граф, добијен описаном конструкцијом од графа $G_3 \cong C_5$ који је 3-хроматски граф без троуглова. Гречеов граф је 4-хроматски и не садржи троуглове.



Слика 3.35

Доказаћемо да је граф G_{k+1}, добијен описаном конструкцијом Мисиелског, $(k+1)$-хроматски граф без троуглова.

Докажимо најпре да је G_{k+1} граф без троуглова. Како никоја два чвора u_i и u_j нису суседна, следи да чвор u не припада ниједном троуглу. По индуктивној претпоставци G_k је граф без троуглова, па према конструкцији графа G_{k+1} закључујемо да само чворови v_i, v_j и u_s (за неке вредности i, j, s) могу да образују троугао у графу G_{k+1}. У том случају, према конструкцији графа G_{k+1}, важи да је $i \neq s, j \neq s$, v_iv_j, v_iv_s,

[13] Jan Mycielski, пољско-амерички математичар, рођен 1932. године
[14] Herbert Grötzsch (1902–1993), немачки математичар

$v_jv_s \in E(G_k)$, одакле произилази да чворови v_i, v_j и v_s образују троугао у графу G_k, што је немогуће.

Докажимо сада да је граф G_{k+1} $(k+1)$-хроматски. Како је $\chi(G_k) = k$, следи да постоји k-бојење графа G_k у коме је чвор v_i обојен бојом $c(v_i)$. Проширимо ово k-бојење графа G_k на $(k+1)$-бојење графа G_{k+1}, тако што чвор u_i обојимо бојом $c(v_i)$, а чвор u бојимо новом $(k+1)$-ом бојом. Добијено бојење је правилно, јер $u_iu_j \notin E(G)$ и $u_iv_i \notin E(G)$, одакле следи да је $\chi(G_{k+1}) \leqslant k+1$.

Докажимо да је $\chi(G_{k+1}) > k$. Довољно је доказати да из егзистенције k-бојења графа G_{k+1} следи егзистенција $(k-1)$-бојења графа G_k, супротно претпоставци да је $\chi(G_k) = k$.

Претпоставимо да постоји правилно k-бојење графа G_{k+1}. Означимо ово бојење са c. Имајући у виду да $uu_i \in E(G_{k+1})$, следи да је $c(u) \neq c(u_i)$, $i = 1, 2, \ldots, n$. Како је $\chi(G_k) = k$, неки од чворова графа G_k обојени су истом бојом као чвор u. Нека је H скуп свих чворова v_i графа G_k, таквих да је $c(v_i) = c(u)$. Уочимо даље бојење c' графа G_k у коме су сви чворови из скупа $V(G_k) \setminus H$ обојени истим бојама као при бојењу c, док сваки чвор $v_i \in H$ добија боју $c'(v_i) = c(u_i)$. На тај начин је добијено бојење c' графа G_k у коме је употребљено $k-1$ боја. Докажимо да је c' правилно бојење графа G_k. Претпоставимо супротно, тј. да у графу G_k постоје суседни чворови v_i и v_j обојени истом бојом при бојењу c', односно да је $c'(v_i) = c'(v_j)$. Очигледно, свака два суседна чвора из $V(G_k) \setminus H$ обојена су различитим бојама, а свака два чвора из H су несуседна. Одавде следи да један од чворова v_i, v_j припада скупу $V(G_k) \setminus H$, док други припада скупу H. Нека је, на пример, $v_i \in H$, $v_j \in V(G_k) \setminus H$. Како је $c'(v_i) = c(u_i)$ и $c'(v_j) = c(v_j)$, закључујемо да је $c(u_i) = c(v_j)$. Према конструкцији графа G_{k+1} следи да су u_i и v_j суседни чворови у графу G_{k+1} који су обојени истом бојом при бојењу c, одакле произилази да бојење c није правилно, супротно претпоставци. Дакле, важи да је $\chi(G_{k+1}) > k$, што заједно са $\chi(G_{k+1}) \leqslant k+1$ имплицира да је $\chi(G_{k+1}) = k+1$. □

Посматрањем степена свих чворова графа, односно максималног степена Δ, може се добити једна горња граница за хроматски број графа.

Теорема 3.26. *За хроматски број $\chi(G)$ повезаног графа G важи*

$$\chi(G) \leqslant \Delta(G) + 1. \tag{3.8}$$

Доказ. Тврђење доказујемо математичком индукцијом по броју чворова n. За $n = 1$ важи да је $G \cong K_1$, па је $\Delta(G) = 0$, $\chi(G) = 1$ и тврђење важи.

Претпоставимо да тврђење важи за све графове са мање од n чворова и посматрајмо граф G са n чворова. Нека је $v \in V(G)$ произвољан чвор графа G и $G' = G - v$. Према индуктивној претпоставци важи да је $\chi(G') \leqslant \Delta(G') + 1 \leqslant \Delta(G) + 1$, одакле следи да постоји $(\Delta(G)+1)$-бојење графа G'. Како је $d_G(v) \leqslant \Delta < \Delta(G) + 1$, постоји бар једна боја којом, при овом бојењу, није обојен ниједан сусед чвора v. Ако чвор v обојимо том бојом, добијамо једно $(\Delta(G)+1)$-бојење графа G, одакле следи да је $\chi(G) \leqslant \Delta(G) + 1$. □

Непосредна последица претходне теореме је да граф чији је хроматски број једнак k обавезно садржи чвор чији је степен једнак најмање $k-1$. Наведена горња граница (3.8) за хроматски број графа може бити доста груба. На пример, за звезду $S_n = K_{1,n-1}$ важи да је $\Delta(S_n) = n-1$, док је $\chi(S_n) = 2$. Међутим, ова горња граница је најбоља могућа, у смислу да за поједине графове важи једнакост у релацији (3.8). За конт̄уру непарне дужине C_{2k+1} је $\Delta(C_{2k+1}) = 2$, а $\chi(C_{2k+1}) = 3$. Осим тога, за комплетан граф K_n је $\Delta(K_n) = n-1$, док је $\chi(K_n) = n$. Брукс[15] је 1941. године доказао да су то једини графови за које важи једнакост у релацији (3.8). Наиме, важи следеће тврђење.

Теорема 3.27. (**Брукс**) *Ако је G п̄овезан ḡраф који није ни непарна конт̄ура ни комп̄летан ḡраф, т̄ада је $\chi(G) \leqslant \Delta(G)$.*

Доказ ове теореме, који се може наћи у [25], изостављамо због сложености.

Ердеш[16] и Ловас[17] су уопштили тврђење теореме 3.25 доказавши следеће тврђење.

Теорема 3.28. *За свака два п̄рӣродна броја k и ℓ, $k \geqslant 2$, $\ell \geqslant 3$, п̄остӣоји k-хромат̄ски ḡраф у коме је дужина најкраће конт̄уре већа од ℓ.*

3.13.1 Бихроматски графови

У општем случају, веза између структуре графа и његовог хроматског броја је компликована. Међутим, у случају бихроматских графова, тј. графова који се могу обојити са две боје, Кениг је доказао да је ова веза једноставна и изражена следећом теоремом.

[15] Rowland Leonard Brooks (1916–1993), енглески математичар
[16] Paul Erdös (1913–1996), мађарски математичар
[17] László Lovász, мађарски математичар, рођен 1948. године

Теорема 3.29. (**Кениг**) *Непразан граф је бихроматски ако и само ако не садржи као подграф ниједну конТуру са непарним бројем чворова.*

Доказ. Претпоставимо најпре да је G бихроматски граф. Ако G садржи као подграф непарну контуру C_{2k+1}, тада је према теореми 3.23 $\chi(G) \geqslant \chi(C_{2k+1}) = 3$, што је супротно претпоставци.

Обратно, претпоставимо да непразан граф G не садржи као подграф ниједну непарну контуру и докажимо да је свака нетривијална компонента (тј. компонента различита од K_1) графа G бихроматски граф. У том случају је према теореми 3.24 и граф G бихроматски.

Нека је H произвољна нетривијална компонента графа G и $v \in V(H)$ произвољан чвор. Нека су скупови $X, Y \subseteq V(H)$ дефинисани са

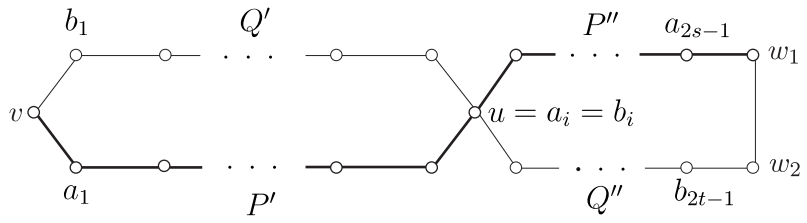
$$X = \{x \in V(H) \mid d(v,x) \text{ је паран број}\},$$

$$Y = \{y \in V(H) \mid d(v,y) \text{ је непаран број}\}.$$

Како је $d(v,v) = 0$, следи да $v \in X$. Осим тога, како је H нетривијална компонента графа G, следи да је и $Y \neq \emptyset$. Скупови X и Y су дисјунктни и важи да је $X \cup Y = V(H)$. Доказаћемо да свака грана из $E(H)$ повезује неки чвор скупа X са неким чвором скупа Y, одакле следи да је граф H бипартитан (са партитивним скуповима X и Y), а тиме и бихроматски граф.

Претпоставимо најпре да постоји грана $w_1w_2 \in E(H)$, при чему w_1, $w_2 \in X$. Обележимо са P и Q, респективно, најкраћи $(v - w_1)$-пут и најкраћи $(v - w_2)$-пут. Према дефиницији скупа X, оба пута су парне дужине. Нека је, на пример, $P = va_1a_2 \ldots a_{2s-1}w_1$ и $Q = vb_1b_2 \ldots b_{2t-1}w_2$, при чему је $s, t \geqslant 1$. Нека је u последњи заједнички чвор путева P и Q, при пролазу по њима из чвора v у чворове w_1 и w_2, респективно (може бити и $u = v$). Претпоставимо да је $u \neq v$. У том случају, чвор u се поклапа са неким чвором a_i, $1 \leqslant i \leqslant 2s-1$, на путу P, односно са неким чвором b_j, $1 \leqslant j \leqslant 2t-1$, на путу Q. Претпоставимо да је $i > j$ и означимо са P', P'', Q', Q'' делове путева P и Q, такве да је $P' = [v, a_i]$, $P'' = [a_i, w_1]$, $Q' = [v, b_j]$, $Q'' = [b_j, w_2]$. Ако са $d(P)$ означимо дужину пута P, како је $i > j$, следи да је $d(P') > d(Q')$, односно $d(P) = d(P') + d(P'') > d(Q') + d(P'')$, одакле произилази да је $Q' + P''$ краћи $(v - w_1)$-пут од пута P, супротно претпоставци. Аналогно се показује да не може бити ни $i < j$, одакле следи да је $i = j$. Дакле, $u = a_i = b_i$ (слика 3.36).

Путеви P и Q су парне дужине, одакле следи да су дужине путева $P'' = [u, w_1]$ и $Q'' = [u, w_2]$ исте парности. Ако је C контура која се састоји од



Слика 3.36

путева P'', Q'' и гране w_1w_2, тада је њена дужина $d(C) = d(P'') + d(Q'') + 1$, што је непаран број. До истог закључка долазимо и када је $u = v$. У том случају контура C се састоји од путева P и Q и гране w_1w_2, па је такође непарне дужине. Дакле, компонента H садржи непарну контуру C, супротно претпоставци.

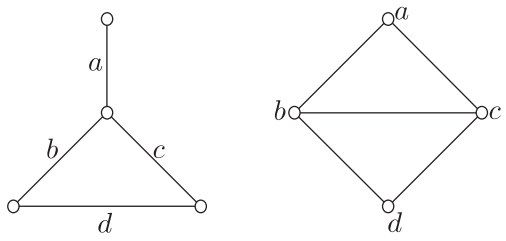
Слично се доказује да су свака два чвора из Y несуседна, одакле следи да компонента H садржи само гране које повезују чворове из скупа X са чворовима из скупа Y, односно H је непразан бипартитан, тј. бихроматски граф. □

3.13.2 Бојење грана графа

Осим бојења чворова графа, у теорији графова се сусрећемо и са бојењем грана графа, као и бојењем и чворова и грана графа. Правилно бојење графа се у овим случајевима дефинише аналогно правилном бојењу чворова графа. Наиме, бојење грана графа је правилно ако су сваке две суседне гране, тј. гране које су инцидентне истом чвору, обојене различитим бојама. При бојењу и чворова и грана графа, реч је о правилном бојењу ако су свака два суседна чвора и сваке две суседне гране графа обојени различитим бојама, при чему крајњи чвор сваке гране мора имати боју која се разликује од боје те гране. Међутим, проблем бојења грана, односно и чворова и грана графа, може се свести на проблем бојења чворова, као што ће бити показано. У том циљу, увешћемо појам графа грана и тоталног графа.

Дефиниција 3.47. ***Граф грана*** *$L(G) = (V_1, E_1)$ графа $G = (V, E)$ је граф чији су чворови у узајамно једнозначној кореспонденцији са гранама графа G, при чему су два чвора из V_1 суседна ако и само ако су њима одговарајуће гране из E суседне.*

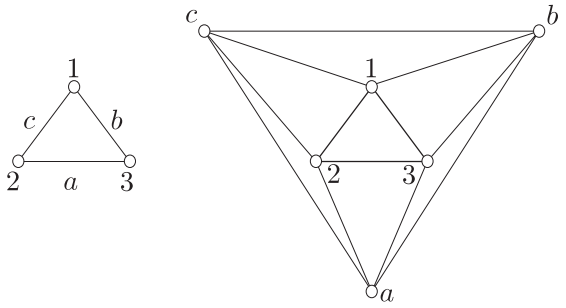
На слици 3.37 је приказан граф G и његов граф грана $L(G)$.



Слика 3.37

Дефиниција 3.48. ***Тоталан граф*** *$T(G) = (V_2, E_2)$ графа $G = (V, E)$ је граф чији су чворови у узајамно једнозначној кореспонденцији са чворовима и гранама скупа $V \cup E$, при чему су два чвора из V_2 суседна ако и само ако су одговарајући елементи из $V \cup E$ суседни (ако су из истог скупа) или инцидентни (ако је један из V, а други из E).*

На слици 3.38 је приказан граф G и његов тотални граф $T(G)$.



Слика 3.38

Проблем правилног бојења грана, односно чворова и грана графа G своди се на правилно бојење чворова његовог графа грана, односно његовог тоталног графа, респективно. Аналогно хроматском броју графа, дефинише се **хроматски индекс графа**, у ознаци $\chi'(G)$, као минималан број боја потребних да се гране графа правилно обоје. У случају бојења и чворова и грана графа дефинише се величина $\chi''(G)$ као минималан број боја потребних за правилно бојење и чворова и грана графа. Имајући у виду везу између правилног бојења грана графа и правилног бојења чворова његовог графа грана, закључујемо да је $\chi'(G) = \chi(L(G))$. Слично, у случају бојења и чворова и грана графа, имајући у виду дефиницију тоталног графа, важи да је $\chi''(G) = \chi(T(G))$.

3.13.3 Проблем четири боје

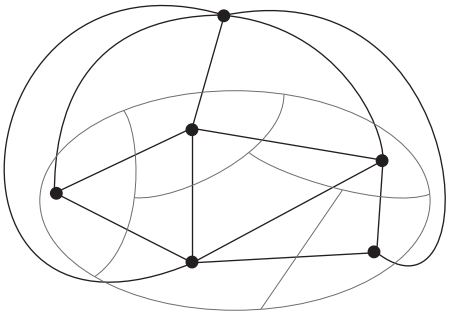
Један од најпознатијих проблема везаних за бојење графова је **проблем четири боје**. Замислимо у равни (или на сфери) географску карту на којој су уцртане државе, при чему се територија сваке државе састоји само од једне регије на карти, а не од више неповезаних подручја. Да бисмо разликовали државе, желимо да их обојимо тако да државе са заједничком границом буду обојене различитим бојама. Проблем се састоји у томе да се одреди минималан број боја потребних да се таква географска карта обоји на описани начин.

Проблем је 1852. године уочио лондонски студент Гатри[18], који је био ангажован на бојењима карти лондонских округа. Сваки округ је, због прегледности, био обојен посебном бојом, при чему су суседни окрузи (под суседним се подразумевају они окрузи са заједничком границом, али не и они који имају једну или више изолованих заједничких тачака) обојени различитим бојама. Гатри је приметио да при тим условима није било довољно мање од четири боје, док је са четири боје било могуће обојити карту на тражени начин. Наметнуло се питање да ли је и за бојење других карти, и то не само стварних, већ свих карти са наведеним особинама које се могу замислити, довољно четири боје. Помоћ је потражио од Де Моргана[19], професора математике на Универзитету у Лондону. Први писани текст о проблему четири боје је писмо које је крајем 1852. године Де Морган послао Хамилтону[20], у коме је објаснио проблем и потражио помоћ. Проблем је постао познат тек након Де Морганове смрти, 1878. године, када га је Кејли изложио на састанку лондонског математичког друштва, а недуго затим објавио први чланак о њему, и то у географском, а не математичком часопису, у коме је изложио тежину проблема и признао да није успео да га реши.

Први озбиљан покушај решавања проблема начинио је Кемпе[21] 1880. године, да би десет година касније, 1890. године, Хивуд[22] открио грешку у овом доказу. Међутим, ни сам Хивуд није успео да реши проблем, већ је доказао да се свака мапа може обојити са пет боја. Од тада је велики број математичара покушавао да реши проблем, да би тек 1976. године

[18] Francis Guthrie (1831–1899), јужноафрички математичар
[19] Augustus De Morgan (1806–1871), британски математичар
[20] William Rowan Hamilton (1805–1865), ирски математичар
[21] Alfred Bray Kempe (1849–1922), британски математичар
[22] Percy John Heawood (1861–1955), британски математичар

то пошло за руком математичарима Апелу[23], Хејкену[24] и Коху[25] и то уз значајну помоћ рачунара и коришћење резултата низа математичара који су објављивани у претходном периоду. До данас није познато да ли је могуће решити овај проблем без употребе рачунара.



Слика 3.39

Проблем четири боје може се превести на језик теорије графова. У том циљу, дефинисаћемо појам **мапе** или **карте**.

Дефиниција 3.49. ***Мапа*** *или* ***карта*** *је повезан планаран граф који нема мостова, односно гранични* 2*-повезан планаран граф.*

Свакој карти може се придружити један планаран граф, тако што се свакој области (регији) на карти придружи по један чвор графа, при чему су чворови који одговарају суседним регијама повезани гранама (слика 3.39). При томе, под суседним регијама подразумевамо оне које имају заједничку граничну линију, али не и оне које се додирују само у једној тачки. На тај начин се проблем бојења регија на карти своди на проблем бојења чворова планарног графа тако да никоја два суседна чвора немају исту боју.

Проблем четири боје преведен на језик теорије графова гласи:

Доказати да је сваки планаран граф 4*-обојив.*

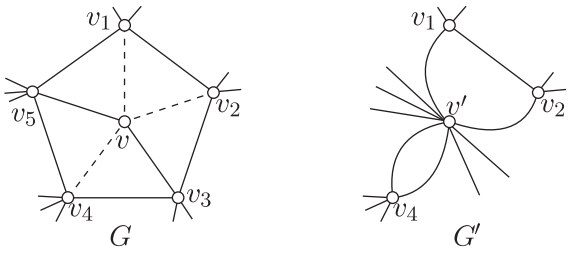
Хивуд је доказао да се свака географска карта може обојити са пет боја, односно доказао је да важи следеће тврђење.

Теорема 3.30. *Сваки планаран граф је* 5*-обојив.*

[23] Kenneth Appel (1932–2013), амерички математичар
[24] Wolfgang Haken, амерички математичар, рођен 1928. године
[25] John Koch, амерички математичар

Доказ. Доказ изводимо математичком индукцијом по броју чворова n. За сваки планаран граф са $n \leqslant 5$ чворова резултат је тривијалан, јер је сваки такав граф 5-обојив.

Претпоставимо да тврђење важи за све планарне графове са мање од n чворова и посматрајмо планаран граф G са n чворова. На основу последице 3.4 планаран граф G садржи бар један чвор степена не већег од 5. Нека је то чвор v.



Слика 3.40

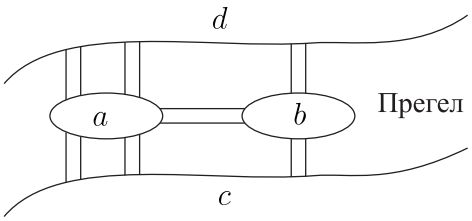
Претпоставимо најпре да је чвор v степена мањег од 5. Удаљимо из графа G чвор v заједно са њему суседним гранама. Добијени граф је на основу идуктивне претпоставке 5-обојив. Вратимо чвор v назад у граф. Како је за бојење чворова суседних чвору v потребно највише 4 боје, следи да чвор v можемо обојити једном од преосталих боја.

Посматрајмо сада случај када је чвор v степена 5. Нека су v_1, v_2, v_3, v_4, v_5 чворови суседни чвору v у графу G. Према последици 3.6 чворови v_1, v_2, v_3, v_4, v_5 не образују потпуни пентаграф K_5 у графу G, одакле следи да постоји бар један пар чворова који није повезан граном. Нека су то, на пример, чворови v_3 и v_5. Уклонимо из графа G гране vv_1, vv_2 и vv_4, а затим удаљимо и гране vv_3 и vv_5, а све гране које долазе до чворова v_3 и v_5 продужимо до новог чвора који ћемо означити са v' (слика 3.40). Тиме смо избацили чворове v_3 и v_5 из графа G. Добијени граф G' је по индуктивној претпоставци 5-обијив. Бојење графа G' одређује и бојење графа G. Наиме, како чворови v_3 и v_5 нису суседни, добијају боју чвора v'. За бојење чворова v_1, v_2 и v_4 потребне су највише три боје, одређене бојењем графа G'. Сада је за бојење чвора v потребна још једна боја, чиме је теорема доказана. □

3.14 Ојлерови и Хамилтонови графови

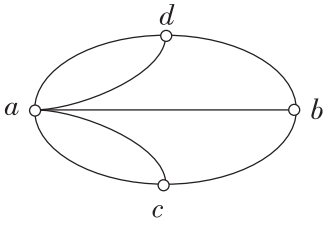
3.14.1 Ојлерови графови

Један од најстаријих познатих проблема који је у вези са графовима је тзв. **проблем кенигсбершких мостова**. Кроз некадашњи пруски град Кенигсберг (данашњи Калињинград) протиче река Прегел, на којој се налазе два острва, повезана међусобно и са обалама реке помоћу седам мостова (слика 3.41).



Слика 3.41

Грађани Кенигсберга су покушавали да одговоре на питање да ли је могуће обићи свих седам мостова, тако да сваки прећу тачно једанпут. Чувени швајцарски математичар Ојлер је 1736. године доказао да то није могуће и формулисао потребне и довољне услове да такав обилазак постоји. Ојлеров резултат се сматра првим резултатом, а тиме и почетком теорије графова. Ојлер је свакој обали и острву придружио по један чвор графа, док су мостови представљали гране између њих. На тај начин добијен је један мултиграф, представљен на слици 3.42.



Слика 3.42

Дефиниција 3.50. ***Ојлерова контура*** *графа (мултиграфа) G је затворена стаза која садржи све гране графа G. Граф (мултиграф) који има Ојлерову контуру назива се* ***Ојлеров граф*** *(Ојлеров мултиграф).*

Ојлеров пут *у графу (мултиграфу) G је стаза која која садржи све гране из G (не мора бити затворена). Граф (мултиграф) који има Ојлеров пут назива се* ***полуојлеров граф*** *(полуојлеров мултиграф).*

У доказу главне теореме о Ојлеровим графовима користићемо следеће тврђење.

Лема 3.1. *Ако је степен сваког чвора графа G већи од 1, тј. $\delta(G) \geqslant 2$, тада граф G садржи контуру.*

Доказ. Нека је $P = v_1 v_2 \dots v_k$ најдужи пут у графу G. Чвор v_1 може бити суседан само са чворовима пута P, тј. $N(v_1) \subseteq V(P)$, јер би у супротном у графу G постојао дужи пут од пута P. Како је $d(v_1) \geqslant 2$, постоји чвор v_i, $3 \leqslant i \leqslant k$, такав да $v_1 v_i \in E(G)$, одакле следи да је $v_1 v_2 \dots v_i v_1$ контура у G. □

Одговор на питање који графови поседују Ојлерову контуру даје следећа теорема.

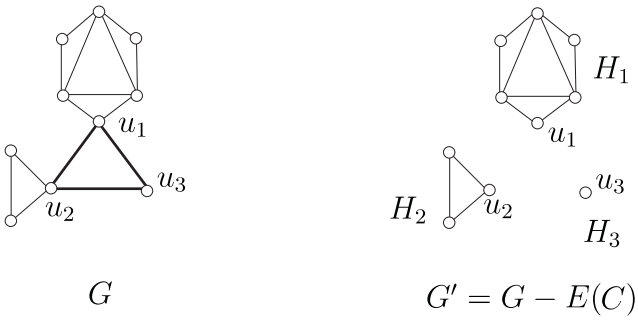
Теорема 3.31. (**Ојлер**) *Повезан мултиграф са бар једном граном је Ојлеров ако и само ако је сваки његов чвор парног степена.*

Доказ. Нека је мултиграф G Ојлеров. Ако се крећемо по Ојлеровој контури мултиграфа G, онда увек када неком граном дођемо у неки чвор, користимо другу грану за напуштање тог чвора. Како морамо проћи кроз све гране Ојлерове контуре и вратити се у почетни чвор, степени свих чворова су парни.

Обратно, претпоставимо да су степени свих чворова повезаног мултиграфа G парни и докажимо да G садржи Ојлерову контуру. Доказ изводимо математичком индукцијом по броју грана m.

Слика 3.43

За повезани мултиграф са две гране, представљен на слици 3.43, тврђење је тачно. Претпоставимо да тврђење важи за мултиграфове са мање од m грана и посматрајмо повезан мултиграф G са m грана чији су сви чворови парног степена. Мултиграф G је повезан, а степени свих његових чворова су парни, одакле следи да је $\delta(G) \geqslant 2$, па на основу леме 3.1 постоји контура C у G. Нека је $G' = G - E(C)$ мултиграф добијен удаљавањем свих грана које припадају контури C из мултиграфа



Слика 3.44

G (слика 3.44). Сви чворови мултиграфа G' су такође парног степена. Наиме, ако $v \in V(C)$, тада је $d_{G'}(v) = d_G(v) - 2$, док за $v \notin V(C)$ важи да је $d_{G'}(v) = d_G(v)$. Мултиграф G' не мора бити повезан. Нека су $H_1, H_2, \ldots, H_t$ компоненте повезаности мултиграфа G', $t \geqslant 1$. Свака од компоненти H_i, $1 \leqslant i \leqslant t$, је повезан граф чији су сви чворови парног степена, па према индуктивној претпоставци садржи Ојлерову контуру (затворену стазу) s_i. Осим тога, како је мултиграф G повезан, свака од затворених стаза $s_1, s_2, \ldots, s_t$ има бар један заједнички чвор са контуром C. Сада се затворена Ојлерова стаза мултиграфа G формира тако што се, почевши од произвољног чвора са контуре C, крећемо по контури, и кад год наиђемо на неки чвор u који се налази на затвореној стази s_i коју нисмо обишли, из њега скренемо и обиђемо целу стазу s_i, вратимо се у чвор u, а затим настављамо обилазак крећући се по контури C, са потребним скретањима за остале стазе s_j. Дакле, тврђење је тачно и за мултиграф са m грана који задовољава услове теореме. □

Последица претходне теореме је следеће тврђење.

Теорема 3.32. *Повезан мултиграф G са бар једном граном је полуојлеров ако и само ако садржи* 0 *или* 2 *чвора непарног степена.*

Доказ. Ако мултиграф поседује Ојлеров пут, тј. затворену Ојлерову стазу или Ојлерову стазу, тада аналогно доказу првог дела претходне теореме, закључујемо да је сваки његов чвор парног степена (у случају затворене Ојлерове стазе), односно садржи два чвора (почетни и крајњи) непарног степена (у случају постојања Ојлерове стазе).

Ако повезан нетривијалан мултиграф G има све чворове парног степена, тада према претходној теореми следи да G садржи затворену Ојлерову стазу, одакле произилази да је G Ојлеров, а тиме и полуојлеров

граф.

Претпоставимо да повезан мултиграф G има два чвора u и v непарног степена. Нека је G' мултиграф добијен од G додавањем новог чвора w и грана uw и vw. Тада су сви чворови повезаног мултиграфа G' парног степена, па он садржи затворену Ојлерову стазу s. Уклањањем чвора w из G' добија се Ојлерова стаза у мултиграфу G која полази из чвора u и завршава се у чвору v. □

Напомена 3.1. *Повезаност мултиграфа представља, осим у тривијалним случајевима, потребан услов за егзистенцију Ојлерове стазе. Наиме, од неповезаних мултиграфова Ојлерову стазу могу евентуално имати само они чије све гране припадају једној компоненти.*

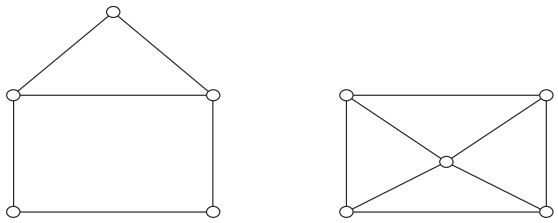
ПРИМЕР 3.31. Обилазак мостова у Кенигсбергу није могућ, јер одговарајући граф, приказан на слици 3.42, садржи 4 чвора непарног степена, па према претходној теореми он није ни полуојлеров, а самим тим ни Ојлеров.

ПРИМЕР 3.32. Ако је у графу G број чворова непарног степена једнак $2k$, $k \geqslant 1$, доказати да тада у графу G постоји k стаза, таквих да свака грана припада једној од тих стаза.

Решење. Нека је G' граф добијен од графа G додавањем чвора v суседног са сваким од $2k$ чворова непарног степена у G. Тада су у графу G' степени свих чворова парни, па према Ојлеровој теореми у графу G' постоји затворена стаза C која садржи све гране графа G'. Како је степен чвора v једнак $2k$, затворена стаза C се састоји од k гранско дисјунктних затворених стаза $C_1, C_2, \ldots, C_k$ са заједничким чвором v. Удаљавањем чвора v из графа G', заједно са свим њему инцидентним гранама, свака од затворених стаза C_i се трансформише у стазу P_i, $1 \leqslant i \leqslant k$, при чему, имајући у виду дефиницију затворене стазе C, свака грана графа G припада једној од тих стаза. △

Ојлерове стазе су значајне за организације које у великим градовима разносе пошту, наплаћују рачуне или врше услуге по домаћинствима, јер ће вршење таквих послова бити изведено најрационалније ако се кроз сваку улицу прође тачно једанпут. Један од најпознатијих проблема ове врсте је **проблем кинеског поштара**. Наиме, поштар ујутру узима писма, обилази улице у свом реону и на крају радног времена се враћа у пошту, што ће бити изведено најрационалније ако кроз сваку улицу прође тачно једанпут. Ово је могуће само ако је одговарајући граф, придружен проблему, Ојлеров, док се у осталим случајевима тражи оптимално решење које ће обезбедити да поштар хода што је мање могуће.

Ојлерове стазе појављују се и у задацима тзв. рекреативне математике. Наиме, ако је потребно да се задата фигура у равни, која се састоји од извесног броја тачака (чворова) и линија које их повезују, нацрта „у једном потезу“, тј. без подизања оловке са папира, тако да се сваком линијом пређе тачно једанпут, док је кроз чворове дозвољено пролазити више пута, то значи да треба нацртати једну Ојлерову стазу у датом графу. На слици 3.45 су представљене две фигуре (које подсећају на отворено и затворено писмо), од којих је прву могуће, а другу немогуће нацртати на описани начин.



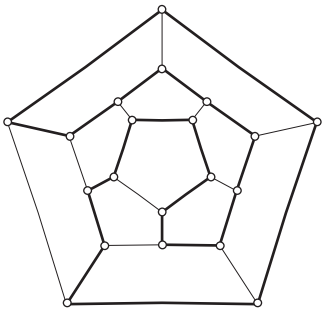
Слика 3.45

3.14.2 Хамилтонови графови

Појам Хамилтонових графова везује се за познатог ирског математичара Хамилтона. Он је је 1857. године представио занимљиву игру на додекаедру, једном од пет правилних полиедара са 20 темена и 12 страна које представљају правилне петоуглове, при чему се у сваком темену сустичу по три стране. Темена додекаедра Хамилтон је обележио именима 20 великих градова тог времена, а циљ игре је био да се обиђу сви градови и врати се у полазни град. При томе, било је дозвољено кретање дуж ивица додекаедра, кроз свако теме (град) дозвољено је проћи тачно једном, а пут почиње и завршава се у истом темену (граду). У циљу боље прегледности, уместо додекаедра ћемо посматрати његову стереографску пројекцију у равни (слика 3.46). Тада се Хамилтонов „пут око света“ своди на контуру која пролази кроз све чворове тако добијеног графа тачно једанпут. На слици је тражена контура која представља решење Хамилтоновог проблема представљена подебљаним линијама. Занимљива је чињеница да је две године пре него што је Хамилтон представио своју игру, британски математичар Киркман[26] поставио проблем да се утврди да ли је могуће у датом графу полиедра пронаћи

[26] Thomas Kirkman (1806–1895), британски математичар

контуру која кроз свако теме пролази тачно једанпут. Дакле, иако је Хамилтонова игра изазвала више интересовања за графове касније називане Хамилтоновим графовима, њих је први проучавао Киркман.



Слика 3.46

Дефиниција 3.51. ***Хамилтонова контура*** *у графу је контура (затворени пут) која садржи све чворове графа, а граф у коме постоји таква контура назива се* ***Хамилтонов граф****.*

Хамилтонов пут *у графу је пут који садржи све чворове графа. Граф који има Хамилтонов пут назива се* ***полухамилтонов граф****.*

Сличним проблемима су се, и пре Хамилтона (и Киркмана), бавили многи математичари. Најпознатији такав проблем је **проблем коњичког скока** (коњ или скакач је шаховска фигура), који се може формулисати на следећи начин.

Да ли је могуће скакачем (коњем) обићи сва поља шаховске табле, тако да се свако поље обиђе тачно једанпут?

Еквивалентна, графовска формулација овог проблема гласи:

Да ли у графу придруженом скакачу постоји Хамилтонов пут?

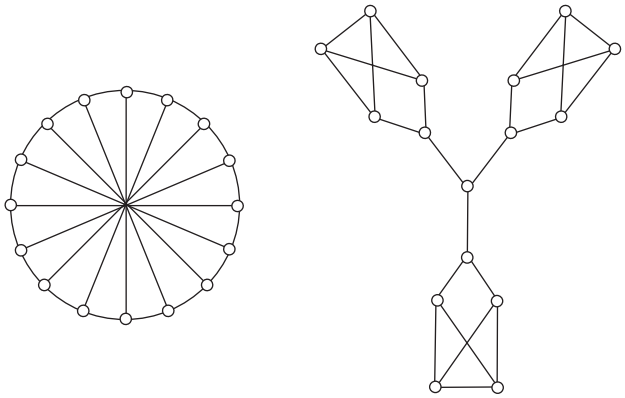
На слици 3.47 је приказано једно решење проблема коњичког скока на класичној шаховској табли димензије 8×8. О овом проблему постоји обимна литература. Испитивана је егзистенција решења на шаховским таблама различитих димензија, као и начин конструкције и број решења. Доказано је да проблем коњичког скока има решење на свим правоугаоним таблама димензије $m \times n$ ($m, n \geqslant 3$), осим табли 3×3, 3×5, 3×6 и 4×4.

Проблем карактеризације Хамилтонових графова је један од најтежих и још увек нерешених проблема теорије графова. За разлику

30	21	50	9	32	19	52	7
49	10	31	20	51	8	33	18
22	29	48	61	42	27	6	53
11	60	41	28	45	62	17	34
40	23	64	47	26	43	54	5
59	12	25	44	63	46	35	16
24	39	2	57	14	37	4	55
1	58	13	38	3	56	15	36

Слика 3.47

од Ојлерових (или полуојлерових) графова, чија егзистенција зависи само од степена чворова, код Хамилтонових (или полухамилтонових) графова то није случај. На слици 3.48 су приказана два графа са по 16 чворова и истим низом степена чворова (оба графа су регуларна, степена 3). Први граф има не само Хамилтонов пут, већ и Хамилтонову контуру, док други граф не поседује Хамилтонов пут.



Слика 3.48

ПРИМЕР 3.33. Нађи пример графа који је:

(1) истовремено Ојлеров и Хамилтонов;

(2) Хамилтонов, али не и Ојлеров;

(3) Ојлеров, али не и Хамилтонов;

(4) није ни Ојлеров ни Хамилтонов.

Решење. (1) Контура C_n је истовремено Ојлеров и Хамилтонов граф.

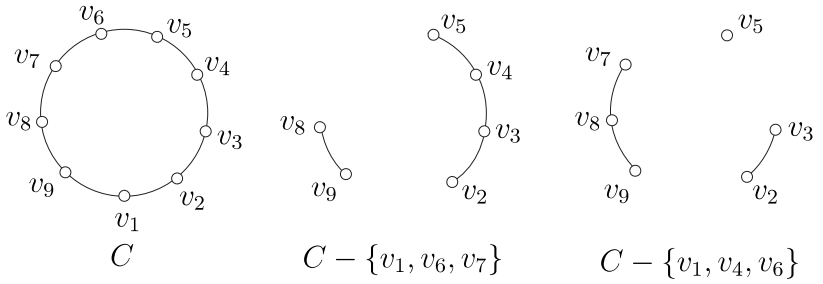
(2) Потпуни граф K_4 није Ојлеров, а јесте Хамилтонов граф.

(3) Потпуни бипартитан граф $K_{2,3}$ јесте Ојлеров, а није Хамилтонов граф.

(4) Звезда $S_4 = K_{1,3}$ није ни Ојлеров ни Хамилтонов граф. △

У литератури је формулисано више потребних и више довољних услова да граф буде Хамилтонов, али међу њима не постоји ниједан који је истовремено и потребан и довољан. У наставку ће бити изложени неки потребни, односно довољни услови да граф буде Хамилтонов.

Теорема 3.33. *Ако је G Хамилтонов граф, тада за сваки прави непразан подскуп $S \subset V(G)$ важи $\omega(G-S) \leq |\ S\ |$, где је са $\omega(G-S)$ означен број компоненти повезаности графа $G-S$.*



Слика 3.49

Доказ. Нека је C Хамилтонова контура графа G. Тада је $V(G) = V(C)$ и за сваки прави непразан подскуп S скупа $V(G)$ испуњено је $\omega(C-S) \leqslant |S|$. Наиме, уклањањем чворова из скупа S, контура C се распада на један или више дисјунктних путева, чији број није већи од броја елемената скупа S, јер уклањањем сваког новог чвора из S добијамо нов пут ако тај чвор није суседан у C са неким претходно избаченим чвором. Једнакост у овој неједнакости важи само у случају када никоја два чвора из S нису суседи у C и тада се контура C распада на тачно $|S|$ дисјунктних путева (слика 3.49).

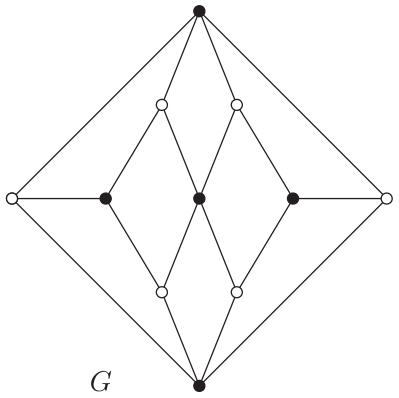
С обзиром на то да је $E(C) \subseteq E(G)$, следи да је $E(C-S) \subseteq E(G-S)$, одакле произилази да је $\omega(G-S) \leqslant \omega(C-S)$, јер се додавањем нових грана не повећава број компоненти графа.

Имајући у виду наведене неједнакости закључујемо да је $\omega(G-S) \leqslant \omega(C-S) \leqslant |S|$, чиме је тврђење доказано. □

Резулатат наведен у теореми 3.33 је често погодан при доказивању да дати граф није Хамилтонов. Наиме, потребно је погодно изабрати подскуп $S \subset V(G)$, такав да је $\omega(G - S) > |S|$.

ПРИМЕР 3.34. Доказати да Хершелов[27] граф, приказан на слици 3.50, није Хамилтонов.

Решење. Означимо посматрани граф са G, а за скуп S изаберимо скуп од 5 црних чворова графа G. Како је $G - S \cong \overline{K}_6$, то је $\omega(G - S) = 6$, па граф G није Хамилтонов. △



Слика 3.50

Услов из теореме 3.33 није и довољан услов за Хамилтонове графове. За Петерсенов граф G, приказан на слици 3.32 а), може се показати да је $\omega(G-S) \leqslant |S|$ за сваки прави непразан подскуп $S \subset V(G)$, а Петерсенов граф није Хамилтонов.

Уколико у теореми 3.33 посматрамо само једночлане скупове S добијамо следећу последицу.

Теорема 3.34. *Сваки Хамилтонов граф је* 2*-повезан.*

Обрнуто тврђење и у овом случају не важи. На пример, посматрајмо граф $K_{2,3}$ који је 2-повезан. Ако за скуп S изаберемо партитивни скуп са 2 чвора овог графа, тада је $K_{2,3}-S \cong \overline{K}_3$, па је $\omega(K_{2,3}-S) = 3 > 2 = |S|$, одакле, према теореми 3.33, следи да граф $K_{2,3}$ није Хамилтонов.

[27] Alexander Stewart Herschel (1836–1907), британски астроном

Довољни услови за Хамилтонове графове су много бројнији од потребних. Најпознатији су Дираков, Ореов[28], као и Бондијев[29] и Хваталов[30].

Теорема 3.35. (**Бонди, Хватал**) *Нека је G граф са n чворова, $n \geqslant 3$, и v и w два несуседна чвора у G, таква да је $d(v) + d(w) \geqslant n$. Тада је граф G Хамилтонов ако и само ако је граф $G + vw$ Хамилтонов.*

Доказ. Ако је граф G Хамилтонов, тада је очигледно и граф $G + vw$ Хамилтонов.

Обратно, претпоставимо да је граф $G + vw$ Хамилтонов, док граф G то није. Тада грана vw припада Хамилтоновој контури графа $G + vw$, а граф G садржи Хамилтонов пут који повезује чвор v са чвором w. Нека су чворови овог пута означени редом са $v = v_1, v_2, \ldots, v_n = w$. Дефинишимо скупове $S, T \subseteq V(G)$ са

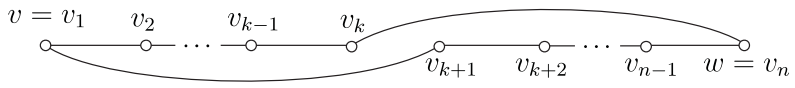
$$S = \{v_k \mid vv_{k+1} \in E(G)\},$$

$$T = \{v_k \mid v_k w \in E(G)\}.$$

Тада $v = v_1 \in S$, $v_{n-1} \in T$ и важи да је $|S| = d(v)$, $|T| = d(w)$. На основу претпоставке теореме закључујемо да важи неједнакост

$$|S| + |T| = d(v) + d(w) \geqslant n. \tag{3.9}$$

Како $w \notin S \cup T$, то је $|S \cup T| < n$, одакле, имајући у виду (3.9), закључујемо да је $S \cap T \neq \emptyset$, тј. постоји чвор $v_k \in S \cap T$. Дакле, постоји чвор v_k, такав да $vv_{k+1} \in E(G)$ и $v_k w \in E(G)$, па граф G садржи Хамилтонову контуру $vv_{k+1}v_{k+2}\ldots v_{n-1}wv_kv_{k-1}\ldots v_2v$ (слика 3.51), што је супротно претпоставци да граф G није Хамилтонов. □



Слика 3.51

Последица претходне теореме је следећа Ореова теорема.

[28] Øystein Ore (1899–1968), норвешки математичар
[29] John Adrian Bondy, британско-канадски математичар, рођен 1944. године
[30] Václav Chvátal, чешко-канадски математичар, рођен 1946. године

Теорема 3.36. (**Оре**) *Ако је G граф са n, $n \geqslant 3$, чворова, такав да за свака два несуседна чвора v и w важи да је $d(v) + d(w) \geqslant n$, тада је G Хамилтонов граф.*

Доказ. Додајући гране између несуседних чворова графа G (докле год у графу G постоје несуседни чворови) и примењујући теорему 3.35, добијамо да је граф G Хамилтонов ако и само ако је комплетан граф K_n Хамилтонов. Како је комплетан граф K_n Хамилтонов за $n \geqslant 3$, тврђење теореме важи. □

Директна последица Ореове теореме је Диракова теорема.

Теорема 3.37. (**Дирак**) *Ако је G граф са n, $n \geqslant 3$, чворова, такав да је $d(v) \geqslant \frac{1}{2}n$ за сваки чвор $v \in V(G)$, тада је G Хамилтонов граф.*

ПРИМЕР 3.35. На двору краља Артура скупило се $2n$ витезова, од којих сваки међу присутнима има највише $n-1$ непријатеља. Доказати да је витезове могуће распоредити око округлог стола тако да ниједан витез не седи поред свог непријатеља.

Решење. Нека је сваки од $2n$ витезова представљен једним чвором графа G, при чему су два чвора суседна у G ако и само ако одговарајући витезови нису непријатељи. Како сваки витез има највише $n-1$ непријатеља међу присутнима, следи да је степен сваког чвора графа G једнак најмање $2n - 1 - (n-1) = n$, одакле, према Дираковој теореми, следи да у графу G постоји Хамилтонова контура која одговара траженом распореду витезова око округлог стола. △

ПРИМЕР 3.36. Нека је G граф са n чворова и $m \geqslant \dfrac{n^2 - 3n + 6}{2}$ грана. Доказати да граф G има Хамилтонову контуру.

Решење. Како је $\dfrac{n(n-1)}{2} - (n-3) = \dfrac{n^2 - 3n + 6}{2}$, граф G се може схватити као делимични граф комплетног графа K_n из кога је удаљено не више од $n-3$ грана. За произвољна два несуседна чвора v_i и v_j овог графа важи да је $d_i + d_j \geqslant 2(n-2) - (n-4) = n$, одакле према теореми Ореа следи да граф G има Хамилтонову контуру. △

На крају наводимо још један важан проблем везан за Хамилтонове графове. То је **проблем трговачког путника** који гласи:

Дат је скуп од n градова које трговачки путник треба да обиђе по једанпут, тако да пут заврши у граду из кога је кренуо. Одредити редослед обиласка градова при коме су трошкови пута минимални.

У графовској формулацији овог проблема користе се **тежински графови**, тј. графови код којих је свакој грани додељена одређена тежина (у случају проблема трговачког путника тежина гране представља трошкове пута између одговарајућих градова). На језику теорије графова проблем трговачког путника гласи:

У задатом тежинском графу одредити Хамилтонову контуру најмање тежине.

Овај проблем је значајан у области операционих истраживања, као и у теоријском рачунарству. Како сам проблем тражења Хамилтонове контуре изискује доста (рачунарског) времена, пронађен је велики број хеуристика које дају „приближно оптимално решење". Доказано је да проблем трговачког путника представља тзв. NP-комплетан проблем, односно сви познати алгоритми за његово решавање имају експоненцијалну сложеност.

3.15 Број унутрашње и спољашње стабилности графа

Дефиниција 3.52. *Нека је $G = (V, E)$ произвољан граф. Подскуп S скупа чворова V зове се **унутрашње стабилан** или **независан** скуп графа G ако су свака два чвора из S несуседна у G, тј. за сваки пар чворова $v, w \in S$ важи $vw \notin E$.*

Према претходној дефиницији следи да подграф $G[S]$ графа G индукован унутрашње стабилним скупом S не садржи ниједну грану, односно састоји се само од изолованих чворова.

Дефиниција 3.53. *Нека је $\mathcal{S}$ скуп свих унутрашње стабилних скупова графа G. **Број унутрашње стабилности** $\alpha(G)$ графа G дефинише се са*

$$\alpha(G) = \max_{S \in \mathcal{S}} |S|.$$

Скупови $S \in \mathcal{S}$ за које је $|S| = \alpha(G)$ називају се максимални унутрашње стабилни или максимални независни скупови графа G.

Максималан унутрашње стабилан скуп графа се може довести у везу са кликом графа. Наиме, ако је S максималан унутрашње стабилан скуп чворова графа G, тада су свака два чвора из S несуседна у графу G,

односно суседна у његовом комплементу $\overline{G}$, одакле, због максималности скупа S, следи да чворови из S формирају клику (потпуни подграф са максималним бројем чворова) у $\overline{G}$, па важи једнакост

$$\alpha(G) = K(\overline{G}).$$

Број унутрашње стабилности $\alpha(G)$ графа G се може довести у везу и са његовим хроматским бројем $\chi(G)$. Како су при правилном бојењу графа сви чворови исте боје међусобно несуседни, они образују унутрашње стабилан скуп графа, одакле следи да број чворова исте боје није већи од $\alpha(G)$. Претпоставимо да граф G има n чворова и означимо са n_i број чворова обојених i-том бојом, $i = 1, 2, \ldots, \chi(G)$. Тада је $n_i \leqslant \alpha(G)$ за свако i, а како је $\sum_{i=1}^{\gamma(G)} n_i = n$, то је

$$\alpha(G)\chi(G) \geqslant n,$$

тј.

$$\alpha(G) \geqslant \frac{n}{\chi(G)}. \tag{3.10}$$

Према Бруксовој процени хроматског броја (неједнакост (3.8)) важи да је $\chi(G) \leqslant \Delta(G) + 1$, где је са $\Delta(G)$ означен максималан степен графа G. Комбинујући овај резултат и неједнакост (3.10), закључујемо да важи следеће тврђење.

Теорема 3.38. *За број унутрашње стабилности $\alpha(G)$ графа G важи неједнакост*

$$\alpha(G) \geqslant \frac{n}{\Delta(G) + 1}.$$

Појам унутрашње стабилних скупова графа се може довести у везу са неким занимљивим шаховским проблемима. У том циљу, показаћемо најпре како се свакој шаховској фигури може придружити одговарајући граф. Сваком пољу шаховске табле придружује се по један чвор графа, при чему су два произвољна чвора v и w овог графа спојена граном ако и само ако одговарајућа фигура може у једном потезу да пређе са поља v на поље w и обрнуто.

Положај више фигура исте врсте на шаховкој табли, при коме се оне међусобно не нападају, одговара у графу придруженом тој фигури једном унутрашње стабилном скупу. Максималан број фигура исте врсте које

се могу поставити на шаховску таблу тако да се међусобно не нападају представља број унутрашње стабилности придруженог графа.

За шаховску фигуру даму (краљицу) на табли димензије 8×8 број унутрашње стабилности придруженог графа једнак је 8, док је за произвољну таблу димензије $n \times n$ тај број једнак n, за $n \geqslant 4$, односно $1, 1, 2$ за $n = 1, 2, 3$, респективно. За топа, односно ловца, важи да је $\alpha(G) = n$, односно $\alpha(G) = 2n - 2$, на табли димензије $n \times n$.

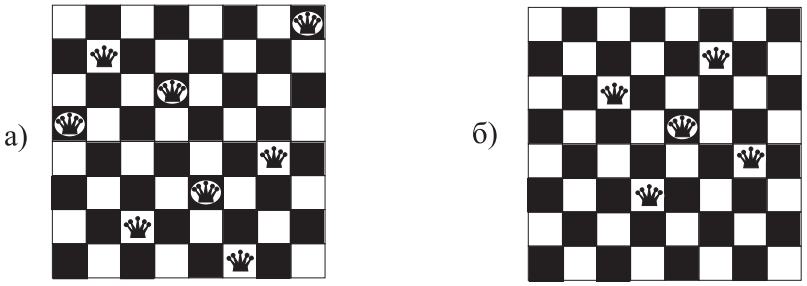
У шаховској литератури познат је **проблем осам дама** објављен 1848. године, који гласи:

На колико се начина 8 *дама може поставити на шаховску таблу димензије* 8×8*, тако да се међусобно не нападају?*

У графовској интерпретацији овај проблем гласи:

Колико има максималних унутрашње стабилних скупова у графу придруженом шаховској фигури дами?

Проблем осам дама решио је Наук[31] 1850. године. Постоји укупно 92 решења, а једно од решења је приказано на слици 3.52 а).



Слика 3.52

Проблем размештања дама није решен у општем случају, када се уместо табле димензије 8×8 посматра произвољна табла димензије $n \times n$.

Појам унутрашње стабилних скупова графа има, осим за решавање шаховских проблема, и друге различите примене. Поменућемо везу овог појма и једног проблема из теорије кодова који исправљају грешке.

Посматрајмо скуп уређених n-торки облика $X = (x_1, x_2, \ldots, x_n)$, при чему $x_i \in \{1, 2, \ldots, b\}$. Оваквих уређених n-торки има b^n. Две n-торке су међусобне једнаке ако и само ако су им све одговарајуће

[31] Franz Nauck

координате једнаке. Каже се да су n-торке $X = (x_1, x_2, \ldots, x_n)$ и $Y = (y_1, y_2, \ldots, y_n)$ на растојању d ако имају тачно d различитих координата (овакво растојање n-торки назива се Хемингово[32] растојање).

Код кодовског растојања $d = 2\ell + 1$ има особину да ако се приликом преношења произвољне n-торке кода кроз систем везе погрешно пренесе не више од ℓ координата n-торке, у пријемном уређају се одговарајућа n-торка може реконструисати.

Један од важних проблема у теорији кодова који исправљају грешке је следећи:

Колико у датом скупу n-торки постоји n-торки чија међусобна растојања нису мања од d, тј. колико n-торки садржи највећи код кодовског растојања d?

Овај проблем се може формулисати као проблем теорије графова на следећи начин. Означимо са $G_{nb\ell}$ граф чији чворови одговарају описаним n-торкама, при чему су два чвора суседна ако и само ако је растојање одговарајућих n-торки мање од $d = 2\ell + 1$. Број чворова овог графа једнак је b^n. Како постоји $\binom{n}{k}(b-1)^k$ n-торки које су на растојању k, $1 \leqslant k \leqslant n$, од сваке n-торке, следи да је сваки чвор графа суседан са $\sum_{k=1}^{2\ell} \binom{n}{k}(b-1)^k$ других чворова. Дакле, $G_{nb\ell}$ је регуларан граф.

Графовска интерпретација постављеног проблем гласи:

Одредити број унутрашње стабилности графа $G_{nb\ell}$.

Проучавање особина графа $G_{nb\ell}$ је значајно не само за наведени, већ и за друге проблеме теорије кодова који исправљају грешке.

Осим унутрашње стабилних скупова дефинишу се и спољашње стабилни скупови графа.

Дефиниција 3.54. *Подскуп T скупа чворова V графа $G = (V, E)$ назива се спољашње стабилан скуп графа G, ако из сваког чвора који не припада скупу T води бар једна грана у неки од чворова из T.*

Дефиниција 3.55. *Нека је $\mathcal{T}$ скуп свих спољашње стабилних скупова графа G. **Број спољашње стабилности** $\beta(G)$ графа G дефинише се са*

$$\beta(G) = \min_{T \in \mathcal{T}} |T|.$$

Скупови $T \in \mathcal{T}$ за које је $|T| = \beta(G)$ називају се минимални спољашње стабилни скупови графа G.

[32] Richard Hamming (1915–1998), амерички математичар

Појам спољашње стабилности графа се, слично појму унутрашње стабилности графа, доводи у везу са шаховским проблемом познатим као **проблем пет дама** који гласи:

Колико је најмање дама потребно поставити на шаховску таблу да би сва поља била нападнута, ако дама напада и поље на коме се налази?

За решење постављеног проблема потребно је најмање пет дама. Показано је да има укупно 4860 решења, а једно од њих је приказано на слици 3.52 б). Решења проблема пет дама представљају минималне спољашње стабилне скупове у графу придруженом шаховској фигури дами.

ПРИМЕР 3.37. Нека чворови $v_1, v_2, \ldots, v_k$, чији су степени $d_1, d_2, \ldots, d_k$, респективно, образују спољашње стабилан скуп у графу са n чворова. Доказати да важи неједнакост

$$k + \sum_{i=1}^{k} d_i \geqslant n.$$

Решење. Нека је $T = \{v_1, v_2, \ldots, v_k\}$ спољашње стабилан скуп у графу $G = (V, E)$ са n чворова. По дефиницији спољашње стабилног скупа, из сваког чвора скупа $V \setminus T$ води бар једна грана у неки од чворова из T. Како је $|V \setminus T| = n - k$, ових грана има бар $n - k$, одакле следи тражена неједнакост. △

Дефиниција 3.56. *Подскуп скупа чворова V графа $G = (V, E)$ који је истовремено и унутрашње и спољашње стабилан скуп графа G назива се* ***језгро графа***.

Појам језгра графа има примену у теорији игара. Посматрајмо једну игру на графу коју играју два играча тако што наизменично бирају чворове графа. Најпре се одреди један произвољан чвор графа, затим први играч бира неки од чворова до кога се може стићи граном из почетног чвора, док други играч бира неки од чворова до кога води грана из чвора који је изабрао први играч, итд. Игру губи онај играч који не може више да изабере ниједан чвор.

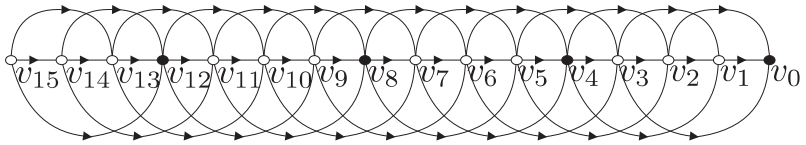
Следеће тврђење указује на везу између стратегије играња описаних игара и појма језгра графа.

Теорема 3.39. *Играч који изабере чвор из језгра графа не може (при правилној игри) да изгуби.*

Доказ. Претпоставимо да у игри учествују два играча, A и B, при чему игру почиње играч A. Ако играч A изабере чвор из језгра графа,

тада играч B мора да изабере чвор ван језгра, јер је језгро унутрашње стабилан скуп графа. Како је језгро и спољашње стабилан скуп, то из сваког чвора ван језгра води бар једна грана у неки од чворова из језгра, па играч A поново бира чвор из језгра и ситуација се понавља, одакле следи да играч A не може да изгуби игру. □

Сваки граф не мора да има језгро и језгро не мора бити јединствено.



Слика 3.53

ПРИМЕР 3.38. У кутији се налази 15 куглица. Играчи A и B узимају наизменично по једну, две или три куглице. Игру губи онај играч који не може да узме више ниједну куглицу када дође на ред. Ко побеђује при правилној игри?

Решење. Игра се може интерпретирати као игра на графу са слике 3.53. Чворови графа су означени са v_i, $i = 0, 1, 2, \ldots, 15$, тако да чвор v_i одговара стању игре „у кутији се налази i куглица“. Играч који изабере чвор из језгра графа (језгро се састоји од црних чворова) добија игру.△

Индекс појмова

Литература

[1] M. Aigner, *Combinatorial Theory*, Springer–Verlag, Berlin, 1979.

[2] J. A. Anderson, *Дискретна математика са комбинаториком*, Рачунарски факултет, Београд, 2005.

[3] G. E. Andrews, *The Theory of Partitions*, Adison–Wesley, London, 1976.

[4] K. Appel, W. Haken, J. Koch, *Every planar map is four-colorable*, Illinois J. Math. 21 (1977), 429–567.

[5] H. A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, Cambridge, 1994.

[6] V. K. Balakrishnan, *Combinatorics*, Shaum's Outline Series, 1995.

[7] V. K. Balakrishnan, *Graph Theory*, Shaum's Outline Series, 1997.

[8] L. W. Beineke, R. J. Wilson, *Selected Topics in Graph Theory*, Academic Press, London, 1978.

[9] N. L. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1974.

[10] B. Bollobás, *Modern Graph Theory*, Springer–Verlag, New York 1998.

[11] J. A. Bondy, V. Chvatal, *A method in graph theory*, Discrete Math. 15 (1976), 111–136.

[12] R. L. Brooks, *On coloring the nodes of a network*, Proc. Cambridge Philos. Soc. 37 (1955), 194–197.

[13] D. M. Burton, *Elementary Number Theory*, McGraw Hill Book Company, New York, 2002.

[14] Д. Вељан, *Комбинаторика са теоријом графова*, Школска књига, Загреб, 1989.

[15] C. D. Godsil, *Algebraic Combinatorics*, Chapman & Hall, New York–London, 1993.

[16] R. L. Graham, M. Grötschel, L. Lovász (editors), *Handbook of Combinatorics*, Volume 1&2, North–Holland, 1995.

[17] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, Adison–Wesley Publishing Company 1994.

[18] Р. Дацић, *Елементарна комбинаторика*, Математички институт, Београд, 1977.

[19] R. Diestel, *Graduate Text in Mathematics*, Springer, 1997.

[20] A. Dujella, *Увод у теорију бројева* (скрипта), ПМФ, Математички одјел, Свеучилиште у Загребу, 2003.

[21] И. Матић, *Увод у теорију бројева* (скрипта), Свеучилиште Josipa Jurja Strossmayera у Осијеку, Одјел за математику, Осијек, 2015.

[22] J. Matoušek, J. Nešetřil, *Invitation to Discrete Mathematics*, Oxford, Clarendon Press, 1988.

[23] В. Мићић, З. Каделбург, *Увод у теорију бројева*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 15, Београд, 2001.

[24] П. Младеновић, *Комбинаторика*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 22, Београд, 2001.

[25] В. Петровић, *Теорија графова*, Универзитет у Новом Саду, Нови Сад, 1998.

[26] М. Петровић, *Дискретна математика*, материјал припремљен за студенте, Природно-математички факултет, Крагујевац.

[27] H. E. Rose, *A Course in Number Theory*, Oxford University Press, Oxford, 1995.

[28] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison–Wesley Publishing Company, 1993.

[29] K. H. Rosen, *Discrete Mathematics and its Applications*, Mc-Graw Hill, New York, 2003.

[30] М. Станић, Н. Икодиновић, *Теорија бројева, Збирка задатака*, Завод за уџбенике и наставна средства, Београд, 2004.

[31] Д. Стевановић, М. Милошевић, В. Балтић, *Дискретна математика, Збирка решених задатака*, Друштво математичара Србије, Београд, 2004.

[32] Д. Стевановић, С. Симић, В. Балтић, М. Ћирић, *Дискретна математика, Основе комбинаторике и теорије графова*, Друштво математичара Србије, Београд, 2008.

[33] I. Tomescu, *Problems in Combinatorics and Graph Theory*, John Wiley & Sons, New York, 1985.

[34] Р. Тошић, В. Вукославчевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.

[35] M. Hall, *Combinatorial Theory*, Blaisdel, Waltham, 1976.

[36] G. H. Hardy, E. M. Wright, *An introduction to the Theory of Numbers*, Oxford, Clarendon Press, 1960.

[37] Д. Цветковић, *Комбинаторна теорија матрица*, Научна књига, Београд, 1987.

[38] Д. Цветковић, *Теорија графова и њене примене*, Научна књига, Београд, 1990.

[39] Д. Цветковић, С. Симић, *Дискретна математика, Математика за компјутерске науке*, Просвета, Ниш, 1996.

[40] Д. Цветковић, С. Симић, *Одабрана поглавља из дискретне математике*, Академска мисао, Београд, 2012.

[41] Д. Цветковић, С. Симић , *Комбинаторика и графови*, Рачунарски факултет и СЕТ, Београд, 2006.