

TARTU ÜLIKOOL  
ARVUTITEADUSE INSTITUUT

---

Reimo Palm

**DISKREETSE  
MATEMAATIKA  
ELEMENDID**

Tartu 2009

Kaane kujundanud Aita Linnas

Käesoleva raamatu väljaandmist on toetanud Eesti Infotehnoloogia Sihtasutus projekti „Tiigriülikool“ raames.

## SISUKORD

Eessõna . . . . .	3
I. Matemaatiline induktsioon . . . . .	4
II. Kombinatorika põhimõisteid . . . . .	12
III. Binoomkordajad . . . . .	23
IV. Rekurrentsed võrrandid . . . . .	32
V. Graafid . . . . .	47
VI. Puud . . . . .	63
VII. Suunatud graafid . . . . .	77
VIII. Relatsioonid . . . . .	87
IX. Tehted relatsioonidega . . . . .	96
X. Boole'i maatriksid . . . . .	110
XI. Jaguvus . . . . .	117
XII. Suurim ühistegur . . . . .	127
XIII. Kongruentsid . . . . .	136
XIV. Kongruentside lahendamine . . . . .	145
Aineregister . . . . .	156

*Õpiku digiversioonis on parandatud trükiversioonis avastatud vead.*

© Reimo Palm, 2003

ISBN 9985-4-0354-1

Tartu Ülikooli Kirjastuse trükikoda  
Tiigi 78, 50410 Tartu  
Tellimus nr 512

## EESSÕNA

Matemaatilisi struktuure võib tinglikult jaotada kaheks klassiks: pidevad ja diskreetsed. Pidevateks nimetatakse neid struktuure, mis tuginevad reaalarvu mõistele ning mille puhul on esmajoones uurimise all mitmesugused pidevuse ja piirväärtusega seotud küsimused. Diskreetsete struktuuride aluse aga moodustab naturaalarvu mõiste. Matemaatika haru, mis uurib diskreetsed struktuure, nimetatakse diskreetses matemaatikaks. Väga sageli on need struktuurid lõplikud, seepärast nimetatakse diskreetses matemaatikas teinekord ka lõplikuks matemaatikaks.

Käesolev õpik annab lugejale ettekujutuse selle valdkonna põhilistest mõistetest. Õpiku esimene peatükk käsitleb diskreetses matemaatikas tihti kasutatavat tõestusmeetodit, matemaatilist induktsiooni, edasise materjali aga võib koondada neljaks teemaks. Peatükid 2–4 on pühendatud kombinatoorikale, mille eesmärk on loendada lõplikust hulgast vastavalt etteantud reeglitele elementide valimise võimalusi või nende paigutamise võimalusi mingil kindlaksmääratud viisil. Peatükid 5–7 käsitlevad graafiteooriat, mille iseärasuseks on graafilise lähenemisviisi uuritavatele objektidele. Vaadeldav objekt esitatakse nn graafina, tippude kogumina, kusjuures mõnede tippude vahele on joonistatud servad. Graafi abil saab näiteks kujutada teatava terviku osade vahel valitsevaid seoseid. Peatükid 8–10 tegelevad binaarsete relatsioonidega lõplikul hulgal, seejuures vaadeldakse lisaks põhimõistetele ja -omadustele ka relatsioonide esitusviise Boole'i matricsite abil. Relatsiooni mõistet võib vajaduse korral pidada graafi mõiste üldistuseks. Peatükid 11–14 kujutavad endast sissejuhatust arvuteooriasse, mis uurib naturaalarvude (st positiivsete täisarvude 1, 2, 3, ...) omadusi.

Üks peatükk vastab ligikaudu ühele õppenädalale. Iga peatüki lõpus on toodud komplekt ülesanded, mille lahendamine aitab paremini mõista vastava peatüki materjali.

Autor soovib tänada Mati Tombakut mitmete kasulike soovitude eest, Härmel Nestrat, Ahti Pederit ja Sven Lauri, kes olid abiks ülesannete valimisel, ning Ülo Kaasikut, kes käsikirja läbi vaadates tegi palju häid täiendus- ja parandusettepanekuid.

# I. MATEMAATILINE INDUKTSIOON

**1. Matemaatilise induktsiooni printsiip.** Matemaatikas tuleb tihti teha tegemist väidetega, mis sõltuvad mingist arvulisest parameetrist. Vaatleme näiteks väidet „arv  $4^n + 8$  jagub 12-ga iga naturaalarvu  $n$  korral“. Andes parameetrile  $n$  mitmesuguseid väärtusi, saame konkreetseid väited. Näiteks kui võtta  $n = 1$ , saame väite „arv  $4^1 + 8$  jagub 12-ga“; valides  $n = 2$ , saame „arv  $4^2 + 8$  jagub 12-ga“, juhul  $n = 3$  saame „arv  $4^3 + 8$  jagub 12-ga“ jne. Sisuliselt on vaadeldavas väites haaratud lõpmata palju osaväiteid, igatüüpi neist saame kätte, kui omistame parameetrile sobiva väärtuse.

Parameetrit sisaldavat väidet nimetame *üldväiteks*, parameetrile väärtuse andmisel saadud väidet aga *üksikväiteks*. Üldväite puudutab korraga paljusid, tavaliselt isegi lõpmata paljusid objekte, üksikväite seevastu piirdub üheainsa objektiga. Üldväite parameetreid võib loomulikult olla ka rohkem kui üks ja need parameetrid ei pea tingimata olema naturaalarvud, vaid võivad olla ükskõik millist tüüpi objektid: reaalarvud, geomeetrilised kujundid, esemete erinevad paigutusvõimalused või midagi muud. Näiteks üldväitel „suvaliste reaalarvude  $x$  ja  $y$  korral kehtib võrdus  $(x + y)^2 = x^2 + 2xy + y^2$ “ on kaks reaalarvulist parameetrit, valides  $x = 2,5$  ja  $y = 3,5$ , saame sellest üksikväite „kehtib võrdus  $(2,5 + 3,5)^2 = 2,5^2 + 2 \cdot 2,5 \cdot 3,5 + 3,5^2$ “. Edaspidises piirdume siiski üldväidetega, mille parameetriks on naturaalarv.

Üksikväite kehtivuses veenduda on enamasti üsnagi lihtne. Näiteks üksikväite „arv  $4^3 + 8$  jagub 12-ga“ kontrollimiseks piisab, kui avaldise väärtus välja arvutada ja kindlaks teha, kas saadud arv jagub 12-ga või mitte. Ent kuidas kontrollida vastava üldväite „arv  $4^n + 8$  jagub 12-ga iga naturaalarvu  $n$  korral“ kehtivust? Selleks ei piisa ainult mõne  $n$  väärtuse läbivaatamisest, sest keegi ei garanteeri, et ülejäänud väärtuste seas ei leidu mõnda sellist, mille puhul väide osutub vääraks. Me peame seega järjestikku läbi kontrollima kõik parameetri  $n$  väärtused, mida on lõpmata palju. Parameetrit sisaldavate väidete tõestamiseks kasutatakse sageli matemaatilise induktsiooni meetodit, mida väljendab järgmine *matemaatilise induktsiooni printsiip*.

**Matemaatilise induktsiooni printsiip.** *Olgu  $A(n)$  üldväide, mille parameetri  $n$  võimalikud väärtused on naturaalarvud. Kui*

- 1. väide  $A(1)$  kehtib,*
- 2. iga naturaalarvu  $k$  puhul sellest, et väide  $A(k)$  kehtib, järeldub, et väide  $A(k + 1)$  kehtib,*

*siis väide  $A(n)$  kehtib mistahes naturaalarvu  $n$  korral.*

Väite tõestamiseks matemaatilise induktsiooni printsiibi abil tuleb seega teha kahte asja: esiteks, kontrollida, et väide kehtib parameetri väärtusel  $n = 1$ , ning teiseks, tõestada, et väite kehtivusest juhul  $n = k$  järeldeb tema kehtivus juhul  $n = k + 1$ . Kui need kaks tingimust on täidetud, siis  $A(n)$  kehtib kõigi  $n$  väärtuste korral. Tõepoolest,  $A(1)$  kehtib printsiibi esimese tingimuse põhjal. Teisest tingimusest saame juhul  $n = 1$ , et kuna  $A(1)$  kehtib, siis ka  $A(2)$  kehtib, edasi saame teisest tingimusest juhul  $n = 2$ , et kuna  $A(2)$  kehtib, siis ka  $A(3)$  kehtib jne. Nii kandub väite kehtivuse tõestus teise tingimuse põhjal samm-sammult üha edasi ja jõuab seega arvu  $n$  ükskõik millise etteantud väärtuseni. See aga tähendabki, et üldväide  $A(n)$  kehtib iga  $n$  korral.

Mõnikord sõltub üldväide mitmest parameetrist. Kui valime neist ühe, mille puhul kontrollime induktsiooniprintsiibi tingimusi, siis räägime induktsioonist selle parameetri järgi.

Tingimust 1 matemaatilise induktsiooni printsiibi formuleeringus nimetatakse *induktsiooni baasiks* ehk lühemalt *baasiks*, tingimust 2 aga *induktsiooni sammuks* ehk *sammuks*. Induktsiooni sammu juures kasutatavat eeldust, et väide  $A(n)$  kehtib juhul  $n = k$ , nimetatakse *induktsiooni eelduseks*.

Matemaatilise induktsiooni printsiip on üks naturaalarvude aritmeetika aksioomidest, seepärast teda ei tõestata.

**2. Induktsiooni kasutamine.** Vaatleme nüüd mõnda näidet induktsiooniprintsiibi rakendamise kohta.

*Näide 1.* Tõestada, et arv  $4^n + 8$  jagub 12-ga iga naturaalarvu  $n$  korral.

*Induktsiooni baas.* Kontrollime, et väide kehtib, kui  $n = 1$ . Sel juhul omandab väide kuju „arv  $4^1 + 8$  jagub 12-ga“. See väide kehtib, sest jagatav arv ongi 12 ise.

*Induktsiooni samm.* Eeldame, et väide kehtib juhul, kui  $n = k$ , st eeldame, et arv  $4^k + 8$  jagub 12-ga. Tõestame, et väide kehtib siis ka juhul  $n = k + 1$ . Meil on seega vaja tõestada, et arv  $4^{k+1} + 8$  jagub 12-ga. Seda arvu teisendades saame

$$4^{k+1} + 8 = 4 \cdot 4^k + 8 = 3 \cdot 4^k + 4^k + 8.$$

Liige  $3 \cdot 4^k$  jagub 12-ga, sest ta jagub nii 3-ga kui ka 4-ga. Samuti arv  $4^k + 8$  jagub 12-ga, sest seda me eeldasime induktsiooni sammu alguses. Järelikult jagub terve avaldis 12-ga. Seega oleme saanud, et väite kehtivusest juhul  $n = k$  järeldeb väite kehtivus juhul  $n = k + 1$ .

Matemaatilise induktsiooni printsiibi põhjal võime nüüd öelda, et vaadeldav väide kehtib iga naturaalarvu korral.

Näide 2. Tõestada võrdus

$$1 \cdot 2 + 2 \cdot 3 + \dots + n \cdot (n + 1) = \frac{n(n + 1)(n + 2)}{3}.$$

*Baas.* Kui  $n = 1$ , siis muutub vaadeldav üldväide üksikväiteks  $1 \cdot 2 = 1(1 + 1)(1 + 2)/3$ , mis on samaväärne võrdusega  $2 = 2$ . Järelikult kehtib üldväide juhul  $n = 1$ .

*Samm.* Eeldame, et väide kehtib juhul  $n = k$ , st

$$1 \cdot 2 + 2 \cdot 3 + \dots + k \cdot (k + 1) = \frac{k(k + 1)(k + 2)}{3}.$$

Tõestame, et siis kehtib väide ka juhul  $n = k + 1$ . Asetades üldväites parameetri  $n$  kohale arvu  $k + 1$ , tuleb seega tõestada võrdus

$$1 \cdot 2 + 2 \cdot 3 + \dots + (k + 1) \cdot (k + 2) = \frac{(k + 1)(k + 2)(k + 3)}{3}.$$

Võtame ette tõestatava võrduse vasaku poole. Esimese  $k$  liikme summa võime siin induksiooni eelduse põhjal asendada avaldisega  $k(k + 1)(k + 2)/3$ , misjärel vasak pool omandab kuju

$$\frac{k(k + 1)(k + 2)}{3} + (k + 1) \cdot (k + 2).$$

Nüüd võtame korrutise  $(k + 1)(k + 2)$  sulgude ette ja saame

$$(k + 1)(k + 2) \left( \frac{k}{3} + 1 \right) = \frac{(k + 1)(k + 2)(k + 3)}{3}.$$

Teisenduste tulemusena saime tõestatava võrduse parema poole. See-  
ga oleme tõestanud võrduse juhul  $n = k + 1$ .

Induksiooni baas ja induksiooni samm kehtivad, järelikult kehtib võrdus iga  $n$  korral.

Mõnikord algavad parameetri lubatavad väärtused mitte ühest, vaid mingist muust arvust. Vastavalt tuleb siis tõestamisel induksiooni baasiks valida parameetri vähim lubatav väärtus.

Näide 3. Tõestada, et iga  $n > 1$  korral kehtib võrratus

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{n}} > \sqrt{n}.$$

*Baas.* Induksiooni baasiks on siin  $n = 2$ , sel juhul omandab võrratus kuju  $1/\sqrt{1} + 1/\sqrt{2} > \sqrt{2}$ . Korrutades selle võrratuse pooli positiivse arvuga  $\sqrt{2}$ , näeme, et ta on samaväärne võrratusega  $\sqrt{2} + 1 > 2$  ehk  $\sqrt{2} > 1$ . Viimane võrratus ilmselt kehtib.

*Samm.* Eeldame, et võrratus kehtib juhul  $n = k$ , ja näitame, et ta kehtib siis ka juhul  $n = k + 1$ . Et induksiooni eelduse põhjal

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} > \sqrt{k},$$

siis

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}.$$

Paremat poolt teisendades saame nüüd

$$\sqrt{k} + \frac{1}{\sqrt{k+1}} = \frac{\sqrt{k(k+1)} + 1}{\sqrt{k+1}} > \frac{\sqrt{k^2} + 1}{\sqrt{k+1}} = \frac{k+1}{\sqrt{k+1}} = \sqrt{k+1}.$$

Niisiis, kokkuvõttes

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \dots + \frac{1}{\sqrt{k+1}} > \sqrt{k+1}.$$

Järelikult kehtib võrratus ka  $n = k + 1$  korral.

*Näide 4.* Tasandile on joonestatud  $n$  sirget, mis jagavad tasandi piirkondadeks. Tõestada, et kõik piirkonnad saab värvida kahe värviga nii, et ühise rajajoonega eraldatud piirkonnad on erinevat värvi.

*Baas.* Kui  $n = 1$ , siis on meil üks sirge, mis jagab tasandi kaheks pooltasandiks. Värvime ühe pooltasandi ühte, teise pooltasandi teist värvi.

*Samm.* Eeldame, et väide kehtib  $k$  sirge korral: piirkonnad, milleks  $k$  sirget jagavad tasandi, võib värvida ülesandes nõutud viisil. Joonestame tasandile veel ühe sirge, nüüd on sirgete arv  $k + 1$ . Ühel pool uut sirget jätame kõigi piirkondade värvid samaks, teisel pool aga muudame kõigi piirkondade värvid vastupidiseks. Kui kahe piirkonna ühine rajajoon asub lisatud sirgel, siis on nende piirkondade värvid erinevad äsjase värvivahetuse tõttu. Kui kahe piirkonna ühine rajajoon ei asunud uuel sirgel, siis on piirkondade värvid erinevad vastavalt induktsiooni eeldusele.

On oluline, et matemaatilise induktsiooni printsiibi rakendamisel kontrollitakse *mõlema* tingimuse täidetust, sest vastasel korral ei saa me olla kindlad, et väite tõesus kandub juhult  $n = 1$  sammhaaval üle igale järgnevale väitele.

*Näide 5.* Vaatleme avaldist  $n^2 + n + 41$ . Juhul  $n = 1$  on selle väärtuseks 43, mis on algarv. Juhul  $n = 2$  on avaldise väärtuseks 47, samuti algarv. Juhul  $n = 3$  saame 53, juhul  $n = 4$  saame 61, juhul  $n = 5$  saame 71, kõik need arvud on algarvud. Kas me võime siit teha järelduse, et avaldise  $n^2 + n + 41$  väärtus on alati algarv, ükskõik millise väärtuse me parameetrile  $n$  ka ei annaks?

Eelnevate katsetustega oleme küll leidnud, et väide „iga naturaalarvu  $n$  korral on arv  $n^2 + n + 41$  algarv“ kehtib parameetri  $n$  mõnel üksikul väärtusel, kuid me pole esitanud ühtegi argumenti, miks väite kehtivus kandub edasi parameetri kõigile järgnevatele väärtustele, ka

neile, mida me kontrollinud pole. Oleme tõestanud induktsiooni baasi (tingimus 1), kuid induktsiooni samm (tingimus 2) puudub. Seega ei saa kindlalt väita, et vaadeldav üldväide kehtib iga  $n$  korral. Üldväide osutubki vääramaks näiteks juhtudel  $n = 40$  ja  $n = 41$ , mil avaldise  $n^2 + n + 41$  väärtusteks on kordardvud  $1681 = 41^2$  ja  $1763 = 41 \cdot 43$ .

*Näide 6.* Püüame tõestada, et arv  $5^{2n} + 7^{n+1}$  jagub 6-ga iga naturaalarvu  $n$  korral.

Eeldame, et  $n = k$  korral väide kehtib, st  $5^{2k} + 7^{k+1}$  jagub 6-ga. Olgu  $n = k + 1$ . Siis

$$5^{2(k+1)} + 7^{k+2} = 5^2 5^{2k} + 7 \cdot 7^{k+1} = 24 \cdot 5^{2k} + 6 \cdot 7^{k+1} + 5^{2k} + 7^{k+1}.$$

Viimase avaldise kaks esimest liiget jaguvad mõlemad 6-ga, kahe viimase liikme summa aga jagub 6-ga induktsiooni eelduse põhjal.

Ometi vaadeldav väide ei kehti, näiteks juhul  $n = 1$  saame arvu  $5^2 + 7^{1+1} = 74$ , mis ei jagu 6-ga. Eelnevas tõestasime küll induktsiooni sammu (tingimus 2), aga jätsime kontrollimata baasi (tingimus 1). Kui väide ei kehti baasjuhul, siis puudub toetuspunkt väite kehtivuse laiendamiseks parameetri järgnevatele väärtustele.

**3. Tugev induktsiooniprintsiip.** Esitatud induktsiooniprintsiipi nimetatakse mõnikord ka *nõrgaks*, vastandina *tugevale induktsiooniprintsiibile*, mille võib sõnastada järgmiselt.

**Tugev induktsiooniprintsiip.** *Olgu  $A(n)$  üldväide, mille parameetri  $n$  võimalikud väärtused on naturaalarvud. Kui*

1. *väide  $A(1)$  kehtib,*
2. *iga naturaalarvu  $k$  puhul sellest, et väide  $A(m)$  kehtib kõigi naturaalarvude  $m < k$  korral, järeldub, et väide  $A(k)$  kehtib,*

*siis väide  $A(n)$  kehtib mistahes naturaalarvu  $n$  korral.*

Võrreldes eelmise kujuga eeldatakse siin induktsiooni sammu puhul väite kehtivust mitte parameetri eelmisel, vaid kõigil eelnevatel väärtustel. Kaks induktsiooniprintsiipi on tegelikult samaväärsed, kuid mõnes olukorras võib viimast kuju olla parem kasutada.

*Näide 7.* Arvujadas  $(a_n)$  on  $a_0 = 1$  ja iga järgmine liige on kõigi eelmiste liikmete summa. Tõestada, et  $a_n = 2^{n-1}$  iga naturaalarvu  $n$  korral.

*Baas.* Kui  $n = 1$ , siis on meil väide  $a_1 = 2^0$ . See väide kehtib, sest  $a_1 = a_0 = 1$ .

*Samm.* Eeldame, et väide kehtib parameetri kõigi väärtuste korral, mis on väiksemad kui  $k$ , ja tõestame, et siis kehtib väide ka parameetri väärtusel  $k$ . Tõepoolest, kui  $a_1 = 2^0$ ,  $a_2 = 2^1$ , ...,  $a_{k-1} = 2^{k-2}$ , siis



geomeetrilise jada liikmete summa valemit kasutades saame

$$\begin{aligned} a_k &= a_0 + a_1 + a_2 + \dots + a_{k-1} = \\ &= 1 + (1 + 2 + \dots + 2^{k-2}) = 1 + 2^{k-1} - 1 = 2^{k-1}. \end{aligned}$$

Järelikult kehtib väide juhul  $n = k$ .

Seega on täidetud tugeva induktsiooniprintsiibi tingimused 1 ja 2 ning vaadeldav väide kehtib iga  $n = 1, 2, \dots$  korral.

*Näide 8.* Šokolaaditahvlit mõõtmetega  $a \times b$  ruutu murtakse mööda jooni tükkeks senikaua, kuni enam murdmisi teha ei saa. Tõestada, et murdmiste arv on alati  $ab - 1$ .

Tõestame väite induktsiooniga tahvli tükide arvu  $n = ab$  järgi.

*Baas.* Kui  $n = 1$ , siis koosneb tahvel ühestainsast ruudust, murdmiste arv on 0 ning väide kehtib.

*Samm.* Eeldame, et väide kehtib iga šokolaaditahvli korral, mis koosneb vähem kui  $k$  ruudust. Tõestame, et siis kehtib väide ka sellise tahvli puhul, millel on  $k$  ruutu. Murrame sellise tahvli kaheks tükiks, suurusega  $c$  ja  $d$  ruutu. Siis  $c < k$  ja  $d < k$  ning  $c + d = k$ . Induktsiooni eelduse põhjal kulub esimese tahvli ühiktükideks jagamiseks  $c - 1$ , teise tahvli puhul aga  $d - 1$  murdmist. Koos esimese kaheksjagamisega on murdmiste arv  $c - 1 + d - 1 + 1 = c + d - 1 = k - 1$ .

## Ülesanded

Tõestada järgmised üldväited.

1.  $5 \cdot 2^{3n+1} + 3^{3n+2}$  jagub 19-ga iga mittenegatiivse täisarvu  $n$  korral.
2.  $11^{n+1} + 12^{2n-1}$  jagub 133-ga iga naturaalarvu  $n$  korral.
3. kui  $n > 1$ , siis arv  $2^{2^n} + 1$  lõpeb 7-ga.

Tõestada võrdused.

4.  $1 + 3 + 5 + \dots + (2n - 1) = n^2$
5.  $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$
6.  $1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2$
7.  $\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \dots + \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}$
8.  $\left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{3^2}\right) \dots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$
9.  $1^2 - 2^2 + 3^2 - \dots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$

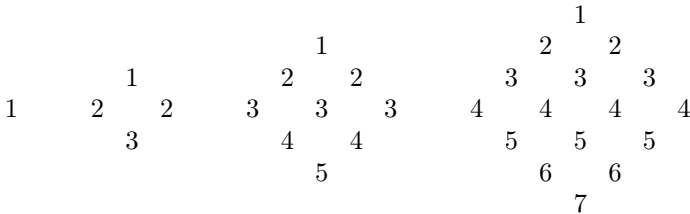
10.  $1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n! = (n + 1)! - 1$
11.  $1 + 2x + 3x^2 + \dots + nx^{n-1} = \frac{1 - (n + 1)x^n + nx^{n+1}}{(1 - x)^2}$
12.  $(x^2 - x + 1)(x^4 - x^2 + 1)(x^8 - x^4 + 1) \dots (x^{2^{n+1}} - x^{2^n} + 1) = \frac{x^{2^{n+2}} + x^{2^{n+1}} + 1}{x^2 + x + 1}$

Tõestada võrratused.

13.  $\frac{1}{2} \cdot \frac{3}{4} \cdot \dots \cdot \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$
14.  $1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$
15.  $\frac{n}{2} < 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^n - 1} < n$
16. Tõestada, et kui  $n$  positiivse reaalarvu  $x_1, x_2, \dots, x_n$  korral  $x_1 + x_2 + \dots + x_n \leq 1/2$ , siis  $(1 - x_1)(1 - x_2) \dots (1 - x_n) \geq 1/2$ .
17. Tõestada induktsiooniga, et kumera  $n$ -nurga sisenurkade summa  $S_n$  avaldub valemiga  $S_n = (n - 2) \cdot 180^\circ$ .
18. Tõestada, et tasandi lõikamisel  $n$  sirgega tekib kõige rohkem  $(n^2 + n)/2 + 1$  piirkonda.
19. Läbi ühe punkti pannakse  $n$  tasandit nii, et ükski kolm neist ei lõiku mööda sama sirget. Tõestada, et need tasandid jaotavad ruumi  $n^2 - n + 2$  osaks.
20. Loeme, et kogum tasandeid on üldasendis siis, kui igal kahel tasandil leidub ühine lõikesirge ja igal kolmel tasandil leidub ühine lõikepunkt, kusjuures need lõikesirged ja lõikepunktid on kõik erinevad. Tõestada, et  $n$  üldasendis tasandit jaotavad ruumi  $(n^3 + 5n + 6)/6$  osaks.
21. Seifi pannakse üks kuldmünt ja seif suletakse. Seejärel paigutatakse ta natuke suuremasse seifi koos veel ühe kuldmündiga. Saadud seif paigutatakse omakorda kolmandasse, veel suuremasse seifi ja lisatakse kõrvale 4 kuldmünti. Protsessi jätkatakse analoogiliselt: igal sammul lisatakse koos järjekordse seifiga niipalju kuldmünti, kui suur on paigutatava seifi järjekorranumbri ruut. Tõestada, et  $n$ -nda seifi väärtus (temas leiduvate kuldmüntide arv) avaldub valemiga  $(n + 1)(2n^2 - 5n + 6)/6$ .
22. Ringmaanteel, mille pikkus on 100 km, seisab  $n$  autot. Neil on ühtekokku nii palju bensiini, et katta 101 km. Tõestada, et leidub üks auto, mis, alustades oma bensiiniga ja kogudes teel bensiini

ülejäänud autodelt, võib läbida täisringi. (Bensiini tohib võtta ainult siis, kui autod on kõrvuti; autot lükata ei tohi.)

23. Naturaalarvudest koostatakse rombide küljepikkusega 1, 2, 3, ... allnäidatud viisil. Leida  $n$ -nda rombi arvude summa ja tõestada saadud valemi õigsus induktsiooniga.



24. Linnas elab  $n$  vanaeite, kusjuures  $n \geq 4$ . Kõigil neil on telefon. Ühel päeval samal ajal saab igaüks neist teada mingi uudise. Tõestada, et on võimalik organiseerida telefonikõned niiviisi, et pärast  $2n - 4$  kõnet teab iga vanaeit iga ülejäänud uudist.

25. Malelual mõõtmetega  $2^n \times 2^n$  ruutu värvitakse üks valibalt valitud ruut punaseks. Tõestada, et maleluala saab katta kolmeruuduliste L-kujuliste tükkidega nii, et nähtavale jääb ainult punane ruut.



Leida viga järgmises kahes „tõestuses“.

26. Kõik linnud on ühte värvi.

*Baas.* Kui  $n = 1$ , siis on meil tegemist üheainsa linnuga ja väide kehtib.

*Samm.* Eeldame, et väide kehtib  $k$  linnu korral. Vaatleme  $k + 1$  lindu  $L_1, \dots, L_{k+1}$ . Jättes esialgu viimase linnu välja, saame induktsiooni eelduse põhjal, et linnud  $L_1, \dots, L_k$  on ühte värvi. Jättes välja esimese linnu, näeme, et ka linnud  $L_2, \dots, L_{k+1}$  on ühte värvi. Siit järeldub, et lind  $L_{k+1}$  on sama värvi nagu linnud  $L_1, \dots, L_k$ , seega on kõik  $k + 1$  lindu ühte värvi.

27. Kõik naturaalarvud on võrdsed. Märgime tähisega  $\max(x, y)$  arvude  $x$  ja  $y$  seast suurimat. Tõestame väite induktsiooniga arvu  $\max(x, y)$  väärtuse järgi.

*Baas.* Kui  $\max(x, y) = 1$ , siis peab olema  $x = y = 1$ , sest tegemist on naturaalarvudega.

*Samm.* Eeldame, et väide kehtib arvude puhul, mille maksimum on  $k$ . Olgu nüüd arvud  $x$  ja  $y$  sellised, et  $\max(x, y) = k + 1$ . Viimane võrdus on samaväärne võrdusega  $\max(x - 1, y - 1) = k$ . Induktsiooni eelduse põhjal  $x - 1 = y - 1$ , millest  $x = y$ .

## II. KOMBINATOORIKA PÕHIMÕISTEID

**1. Permutatsioonid.** Kombinatoorika uurib probleeme, mis on seotud teatava, enamasti lõpliku hulga elementide valimise ja paigutamise etteantud tingimuste järgi. Eesmärgiks on tavaliselt leida nõuetele vastavate valimis- või paigutamisevõimaluste koguarv, ja kui vaja, siis ka need võimalused ise.

On olemas hulk standardseid kombinatoorikaülesandeid, mis esinevad praktikas kõige sagedamini. Neid ülesandeid eristatakse esiteks selle järgi, kas valitavate elementide järjekord on oluline (permutatsioonid) või ei ole oluline (kombinatsioonid), ning teiseks selle järgi, kas hulga iga element võib valikus esineda ainult üks kord või võivad elemendid ka korduda. Esialgu piirdume juhuga, mil valitavate elementide hulgas kordumisi olla ei tohi.

Olgu antud mingi  $n$ -elemendiline hulk. Selle hulga kõikidest elementidest moodustatud järjestatud hulki nimetatakse *permutatsioonideks* ning nende arvu (ehk hulga järjestamisvõimaluste arvu) tähistatakse sümboliga  $P(n)$ .

Alustades  $n$ -elemendilise hulga järjestamist, on meil  $n$  võimalust valida elementi, mida paigutada esimesele kohale. Pärast esimese koha täitmist võime teisele kohale valida elemendi  $n - 1$  allesjäänu seast. Kahte esimest kohta saab järelikult täita  $n(n - 1)$  viisil, sest igale esimese koha elemendile saab teise koha elementi juurde lisada  $n - 1$  viisil. Niiviisi jätkates näeme, et kõigi  $n$  koha täitmiseks on võimalusi

$$P(n) = n(n - 1)(n - 2) \cdot \dots \cdot 2 \cdot 1.$$

See ongi  $n$ -elemendilise hulga erinevate ümberjärjestuste arv. Naturaalarvude korrutist 1-st kuni  $n$ -ni nimetatakse arvu  $n$  *faktoriaaliks* ja tähistatakse sümboliga  $n!$ . Lisaks defineeritakse  $0! = 1$ . Seega kehtib permutatsioonide arvu puhul

$$P(n) = n!.$$

*Näide 1.* Vaatleme 4-elementilist hulka  $\{\textcircled{1}, \textcircled{2}, \textcircled{3}, \textcircled{4}\}$ . Sellel hulgal on  $P(4) = 4! = 24$  permutatsiooni, sõnedena kirjutatult on need

①②③④	②①③④	③①②④	④①②③
①②④③	②①④③	③①④②	④①③②
①③②④	②③①④	③②①④	④②①③
①③④②	②③④①	③②④①	④②③①
①④②③	②④①③	③④①②	④③①②
①④③②	②④③①	③④②①	④③②①

Esimeses veerus asuvad järjestused, kus esimesele kohale on valitud element  $\textcircled{1}$ , teises veerus järjestused, kus esimesel kohal on  $\textcircled{2}$  jne.

Näide 2. Mitmel viisil saab pulmasündmuse jäädvustav fotograaf paigutada ühte ritta pruudi ja peigmehe ning kummagi vanemad (kokku 6 inimest) selliselt, et a) pruut ja peigmees seisavad kõrvuti; b) pruut ja peigmees seisavad eraldi?

Kui pruut ja peigmees peavad seisma kõrvuti, siis me võime neid tinglikult käsitleda kui ühte inimest. Viiest inimesest saab moodustada  $P(5) = 5! = 120$  erinevat rivi. Iga niisugune rivi annab kaks paigutusvõimalust sõltuvalt sellest, kas pruut seisab peigmehe vasakul või paremal käel. Üldse on paigutusvõimalusi seega  $2 \cdot 120 = 240$ .

Kui pruut ja peigmees peavad seisma eraldi, siis eemaldame kõigist võimalikest järjestustest need, kus pruut ja peigmees on kõrvuti. Et kuuest inimesest saab moodustada  $P(6) = 6! = 720$  erinevat rida ning 240 juhul seisavad pruut ja peigmees kõrvuti, siis eraldi seisavad nad  $720 - 240 = 480$  reas.

Sageli on eesmärgiks loendada mitte niivõrd hulga enda järjestamisvõimalusi, kui võrd tema mingi kindla suurusega järjestatud alamhulki. Antud  $n$ -elemendilise hulga  $m$ -elemendilisi järjestatud alamhulki nimetatakse *permutatsioonideks* (mõnikord ka *variatsioonideks*)  $n$  elemendist  $m$ -kaupa ning nende arvu märgitakse tähisega  $P(n, m)$ . Valemi arvu  $P(n, m)$  leidmiseks saab tuletada samasuguse arutlusega nagu ennegi: asudes valima  $n$ -elemendilisest hulgast  $m$ -elemendilist järjestatud osahulka, võime esimesele kohale valida elemendi  $n$  viisil, pärast seda teisele kohale elemendi  $n - 1$  viisil jne kuni viimasele,  $m$ -ndale kohale elemendi  $n - m + 1$  viisil. Seetõttu

$$P(n, m) = n(n - 1) \dots (n - m + 1).$$

Paremal esinevat  $m$  tegurist koosnevat korrutist nimetatakse arvu  $n$  *kahanevaks  $m$ -faktoriaaliks* ja märgitakse tähisega  $(n)_m$ . Korrutades ja jagades saadud avaldist suurusega  $(n - m)!$ , võime viimase arvu esitada ka järgmisel kujul, mis on kasulik avaldiste teisendamisel:

$$P(n, m) = (n)_m = \frac{n!}{(n - m)!}.$$

Kui  $m = n$ , siis on tegemist terve hulga järjestusvõimaluste arvu leidmisega ning ülesanne taandub varem vaadeldud juhule. Viimane valem annab siis  $P(n, n) = n!$ . Valides aga  $m = 0$ , saame  $P(n, 0) = 1$ .

Näide 3. Sõudevõistluse finaalis osales 6 sportlast. Kolme esimese nimed avaldatakse lehes. Mitu erinevat järjestust võib lehes ilmuda?

Järjestuste arv on sama suur, kui mitmel viisil saab 6 sportlase hulgast valida 3, kusjuures valitud sportlaste omavaheline järjekord on oluline. Valemi järgi on erinevate järjestuste arv

$$P(6, 3) = 6 \cdot 5 \cdot 4 = 120.$$

**2. Kombinatsioonid.** Antud  $n$ -elemendilise hulga  $m$ -elemendilisi alamhulki nimetatakse *kombinatsioonideks*  $n$  elemendist  $m$ -kaupa. Erinevalt permutatsioonidest pole kombinatsioonide puhul elementide järjekord oluline ning neid eristatakse üksteisest ainult koosseisu järgi. Kombinatsioonide arvu  $n$  elemendist  $m$ -kaupa tähistame sümbooliga  $C(n, m)$ .

Arvu  $C(n, m)$  leidmiseks vaatleme  $n$ -elemendilise hulga  $m$ -elemendilisi alamhulki. Iga sellist alamhulka võib teatavasti järjestada  $m!$  viisil, seega vastab igale kombinatsioonile  $m!$  permutatsiooni ning iga permutatsiooni võib saada mingist kombinatsioonist. Järelikult on permutatsioonide arv  $n$  elemendist  $m$ -kaupa parajasti  $m!$  korda suurem kui vastav kombinatsioonide arv ning

$$C(n, m) = \frac{P(n, m)}{m!} = \frac{n!}{m!(n-m)!}.$$

Viimane murd kujutab endast nn *binoomkordaja* avaldist, seepärast tähistatakse kombinatsioonide arvu  $n$  elemendist  $m$ -kaupa mõnikord ka binoomkordaja  $\binom{n}{m}$  abil. Muu hulgas näiteks  $\binom{n}{n} = \binom{n}{0} = 1$ , st antud  $n$ -elemendilisest hulgast saab tervet hulka ja tühja hulka valida ainult ühel viisil.

*Näide 4.* Kuuelemendilisest hulgast  $\{①, ②, ③, ④, ⑤, ⑥\}$  saab moodustada kolmeelemendilisi kombinatsioone kokku

$$C(6, 3) = \frac{6!}{3!3!} = 20$$

tükki ning need kombinatsioonid on

$$\begin{array}{cccc} \{①, ②, ③\} & \{①, ③, ⑤\} & \{②, ③, ④\} & \{②, ⑤, ⑥\} \\ \{①, ②, ④\} & \{①, ③, ⑥\} & \{②, ③, ⑤\} & \{③, ④, ⑤\} \\ \{①, ②, ⑤\} & \{①, ④, ⑤\} & \{②, ③, ⑥\} & \{③, ④, ⑥\} \\ \{①, ②, ⑥\} & \{①, ④, ⑥\} & \{②, ④, ⑤\} & \{③, ⑤, ⑥\} \\ \{①, ③, ④\} & \{①, ⑤, ⑥\} & \{②, ④, ⑥\} & \{④, ⑤, ⑥\} \end{array}$$

Igaühte neist alamhulkadest saab järjestada  $P(3) = 3! = 6$  viisil, seega annavad need kombinatsioonid ühtekokku  $20 \cdot 6 = 120$  erinevat permutatsiooni, nagu leidsime ka näites 3.

*Näide 5.* Mitu võimalust on valida 16-liikmelisele klubile juhatus, mis koosneb esimehest ja tema kolmest asetäitjast?

Kõigepealt valime klubi liikmete hulgast 4, kes kuuluvad juhatusse, selleks on  $C(16, 4)$  võimalust. Pärast seda on  $C(4, 1)$  võimalust valida juhatusse liikmete hulgast esimees, ülejäänud kolmest saavad siis asetäitjad. Seega on esimehe ja asetäitjate valimiseks võimalusi

$$C(16, 4)C(4, 1) = 1820 \cdot 4 = 7280.$$

**3. Kordumistega valikud.** Pöördume nüüd selliste olukordade juurde, kus valitud elementide hulgas võib olla korduvaid, teiste sõnadena, valitava komplekti moodustamisel võib iga elementi võtta mitu korda. Seda võime mõista nii, et hulga igast elemendist on olemas mitu eksemplari, nii et ühe elemendi eemaldamine ei takista sedasama elementi valimast ka järgmisel sammul. Siingi tehakse vahet permutatsioonide ja kombinatsioonide vahel vastavalt sellele, kas elementide omavaheline järjekord on oluline või mitte.

Olgu antud  $n$ -elemendiline hulk, mille igast elemendist on olemas piiramata varu. Kõiki  $m$ -elemendilisi järjestatud komplekte, kus üks ja sama element võib esineda ka rohkem kui üks kord, nimetatakse *kordumistega permutatsioonideks*. Erinevate kordumistega permutatsioonide arvu  $n$  elemendist  $m$ -kaupa tähistame sümboliga  $W(n, m)$ .

Lihtne on veenduda, et

$$W(n, m) = n^m.$$

Tõepoolest, asudes moodustama mingit  $m$ -elemendilist komplekti, saame esimese koha täita  $n$  viisil, teise koha täitmiseks on meil samuti valida  $n$  elemendi vahel, sest võime kasutada ikka kõiki  $n$  elementi, ning samamoodi ka iga ülejäänud koha puhul. Erinevaid elemendikomplekte saame seega moodustada  $n \cdot n \cdot \dots \cdot n = n^m$  tükki.

*Näide 6.* Trükikojas on 8 kasti, igaühes ühte liiki tähed. Mitu kolmetähelist sõna saab nendest moodustada?

Et sõnas võivad tähed korduda ja tähtede omavaheline järjekord on oluline, siis on tegemist kordumistega permutatsioonide moodustamisega. Nõutav sõnade arv on seega

$$W(8, 3) = 8^3 = 512.$$

*Näide 7.* Jõuluvanal on  $k$  erinevat kingitust, igaühte üks eksemplar. Kingitused tuleb ära jagada  $l$  lapse vahel, seejuures võib mõnele lapsele anda mitu kingitust, mõnele aga mitte ühtegi. Mitu võimalust on jõuluvanal kingituste jagamiseks?

Kujutleme, et jõuluvana võtab kingitusi kotist välja alati kindlas järjekorras, näiteks väiksemast suuremani. Esimese kingituse võib ta anda ühele lapsele  $l$  lapse hulgast, teise kingituse samuti ühele  $l$  lapse hulgast jne. Kokku peab jõuluvana tegema  $k$  taolist valikut. Erinevaid võimalusi kingitusi jagada on seega  $W(l, k) = l^k$ .

Kordumistega permutatsioonide teise juhu saame siis, kui iga elementi on lubatud kasutada ainult piiratud koguses. Vaatleme jällegi  $n$ -elemendilist hulka, kuid eeldame nüüd, et esimest elementi on  $m_1$  eksemplari, teist elementi  $m_2$  eksemplari jne kuni  $n$ -ndat elementi

$m_n$  eksemplari. Lihtsuse mõttes piirdume siinkohal ainult selliste järjestatud hulkade vaatlemisega, kuhu on haaratud kõigi olemasolevate elementide kõik eksemplarid, st vaatleme ainult komplekte, mis koosnevad  $m = m_1 + m_2 + \dots + m_n$  liikmest. Olgu  $K(m_1, m_2, \dots, m_n)$  niisuguste järjestatud kompleksite arv.

Igast sellisest komplektist võime saada  $m$  erineva elemendi permutatsiooni, kui muudame iga elemendi kõik eksemplarid üksteisest eristatavaks, näiteks varustame nad järjekorranumbriga. Omistades numbreid erinevas järjekorras, saame erinevad permutatsioonid. Esimese elemendi numbreid võib isekeskis ümber paigutada  $m_1!$  viisil, iga sellise ümberpaigutuse korral võib teise elemendi numbreid ümber paigutada  $m_2!$  viisil jne. Ühest komplektist saame seega üldse  $m_1!m_2! \dots m_n!$  erinevat permutatsiooni. Et kokku on  $m$  erinevast elemendist võimalik moodustada  $m!$  permutatsiooni, siis

$$K(m_1, m_2, \dots, m_n) = \frac{m!}{m_1!m_2! \dots m_n!}.$$

Leitud valem ühtib järgmises peatükis vaadeldava *multinoomkordaja*

$$\binom{m}{m_1, m_2, \dots, m_n}$$

avaldisega, seda kasutatakse piiratud eksemplaride arvuga permutatsioonide arvu märkimiseks tihti tähise  $K(m_1, m_2, \dots, m_n)$  asemel.

*Näide 8.* Anagramm on sõna, mis saadakse etteantud sõnast tähtede järjekorra muutmise teel. Mitu anagrammi saab moodustada sõnast RODODENDRON?

Meie käsutuses on kaks eksemplari tähte R, kolm eksemplari tähte O, kolm eksemplari tähte D, üks eksemplar tähte E ja kaks eksemplari tähte N. Üldse on sõnas 11 tähte. Nende tähtede erinevaid ümberjärjestusi ehk anagramme on seega

$$K(2, 3, 3, 1, 2) = \frac{11!}{2!3!3!1!2!} = 277\,200.$$

*Näide 9.* Vaatleme uuesti näite 7 olukorda ja eeldame, et  $k$  kingitusest tuleb  $k_1$  tükki anda esimesele lapsele,  $k_2$  tükki teisele lapsele jne kuni  $k_l$  tükki viimasele lapsele. Mitu võimalust on nüüd kingituste jagamiseks?

Oletame jällegi, et jõuluvana võtab kingitusi kotist välja suure järjekorras ja seejuures paneb igale kingitusele külge varem valmistatud sildi lapse nimega, kellele see kingitus anda tuleb. Niiviisi tekib rida, kus  $k_1$  korda esineb esimese lapse nimi,  $k_2$  korda teise lapse nimi jne. Iga selline siltide rida määrab ühe võimaluse kingituste jagamiseks, erinevaid võimalusi on seega  $K(k_1, k_2, \dots, k_l)$ .



Kuid me võime ka kujutleda, et jõuluvana võtab kingitusi kotist juhuslikus järjekorras ja paneb nad kõik lauale ritta. Seejärel võtab esimene laps reast  $k_1$  esimest kingitust, teine laps  $k_2$  järgmist jne. Üldse saab  $k$  kingitust järjestada  $k!$  viisil. Seejuures saab esimene laps sama kingitusekogumi alati siis, kui esimesed  $k_1$  kingitust mingil viisil ümber paigutada, mida saab teha  $k_1!$  viisil. Teise lapse kingitusi võib ümber paigutada  $k_2!$  viisil jne. Seega on kingituste jagamiseks

$$\frac{k!}{k_1!k_2! \dots k_l!}$$

võimalust, mis ühtib eelmise tulemusega.

Kui hulga iga element on saadaval piiramatul hulgal eksemplarides, kuid valitud elementide omavaheline järjestus oluline ei ole, siis räägitakse *kordumistega kombinatsioonidest*. Kordumistega kombinatsioonideks  $n$  elemendist  $m$ -kaupa nimetatakse antud  $n$ -elemendilise hulga  $m$ -elemendilisi alamhulki, kusjuures iga alamhulk võib sisaldada korduvaid elemente. Mõnda elementi mitmes eksemplaris sisaldavat hulka nimetatakse vahel ka multihulgaks

Kordumistega kombinatsioonide arvu  $F(n, m)$  võib avaldada harilike, kordumisteta kombinatsioonide arvu kaudu. Olgu meil tarvis valida  $n$ -elemendilisest hulgast  $m$  elementi, mille seas võib olla võrdseid. Eeldame, et antud hulga elemendid on nummerdatud 1-st  $n$ -ni. Seega tuleb meil valida teatav arv esimesi elemente, teatav arv teisi elemente jne, kokku  $m$  tükki. Paigutame kõik valitud esimesed elemendid ühte ritta ja lisame rea lõppu eraldaja – mingi elemendi, mis erineb kõigist vaadeldava hulga elementidest. Selle järele paigutame kõik teised elemendid ja lisame veel ühe eraldaja. Rida lõpeb  $n$ -ndate elementide järjendiga. Eraldaja lisame ikkagi ka sel juhul, kui mingit liiki elemente üldse ei valita. Tulemusena asub reas  $n - 1$  eraldajat ja ühtekokku  $m$  elementi (joonisel on  $n = 4$  ja  $m = 10$ ):

$$\underline{①} \underline{①} \underline{①} \text{ * } \underline{②} \underline{②} \underline{②} \underline{②} \text{ * * } \underline{④} \underline{④} \underline{④}$$

Elementide valikuviisi määravad üheselt eraldajate asukohad. Kordumistega kombinatsioone on seega sama palju, kui palju on võimalusi valida  $n + m - 1$  kohast välja need  $n - 1$ , kuhu eraldajad panna. Neid võimalusi on ilmselt  $C(n + m - 1, n - 1)$ , järelikult

$$F(n, m) = C(n + m - 1, n - 1).$$

*Näide 10.* Kolmeelemendilisest hulgast  $\{①, ②, ③\}$  saab moodustada  $F(3, 3) = C(5, 2) = 10$  kordumistega kombinatsiooni ja nimelt

$$\begin{array}{ccccc} \{①, ①, ①\} & \{①, ①, ②\} & \{①, ①, ③\} & \{①, ②, ②\} & \{①, ②, ③\} \\ \{①, ③, ③\} & \{②, ②, ②\} & \{②, ②, ③\} & \{②, ③, ③\} & \{③, ③, ③\} \end{array}$$

*Näide 11.* Mitmel viisil saab valida 10 kooki einelauas pakutavate nelja liiki kookide hulgast nii, et igast liigist valitakse vähemalt üks?

Võtame kõigepealt igast liigist ühe koogi ja valime neile lisaks nelja liigi seast veel 6 kooki. Selliseks valikuks on võimalusi

$$F(4, 6) = C(9, 3) = 84.$$

Üldiselt, kui  $n$  liiki elementide hulgast tuleb valida  $m$  elementi, kusjuures iga liiki elementi valitakse vähemalt üks, siis on niisuguseks valikuks ühtekokku võimalusi

$$F(n, m - n) = C(m - 1, n - 1).$$

*Näide 12.* Mitu võimalust on paigutada 4 punast ja 6 sinist palli viide erinevat värvi kasti?

Paigutame kõigepealt 4 punast palli viide kasti. Valime viiest kastist 4, võttes iga kasti täpselt nii mitu korda, kui mitu punast palli sinna paneme. Niisuguseks valikuks on võimalusi

$$F(5, 4) = C(8, 4) = 70.$$

Samamoodi on kuue sinise palli viide kasti paigutamiseks võimalusi

$$F(5, 6) = C(10, 4) = 210.$$

Iga punaste pallide valikut võib kombineerida iga siniste pallide valikuga, järelikult on nii punaste kui ka siniste pallide paigutamiseks  $70 \cdot 210 = 14700$  võimalust.

Otse valemi asemel võime aga kasutada ka meetodit, mille abil see tuletati. Paigutame 4 punast palli ritta ja lisame neile  $5 - 1 = 4$  musta kuubikut. Pallid rea algusest kuni esimese kuubikuni paneme esimesse kasti, esimese ja teise kuubiku vahel asuvad pallid teise kasti jne. Erinevaid võimalusi punaseid palle kastidesse jagada on nii palju, kui mitmel viisil saab kaheksa koha hulgast valida 4, kuhu panna mustad kuubikud, ehk  $C(8, 4) = 70$ . Siniste pallide puhul tuleb kuubikute jaoks valida kümnest kohast 4, selleks on võimalusi  $C(10, 4) = 210$ .

*Näide 13.* Olgu  $n$  naturaalarv. Leida, mitu lahendit on võrrandil

$$x_1 + x_2 + \dots + x_k = n,$$

kui  $x_1, x_2, \dots, x_k$  väärtused on mittenegatiivsed täisarvud.

Eelmise näite mõistes tuleb siin paigutada  $n$  ühte värvi palli  $k$  kasti. Võimaluste arv ehk võrrandi lahendite arv on järelikult  $F(k, n)$ .

**4. Korrutamis- ja liitmisreegel.** Suurt hulka kõige mitmekehisemaid kombinatoorikaülesandeid, nende hulgas ka selliseid, mille puhul ei saa otseselt rakendada eespool tuletatud valemeid, võib lahendada järgmise kahe reegli abil, mida võib pidada kombinatoorika põhireegliteks.

**Korrutamisreegel.** Eeldame, et mingi tegevus koosneb kahest alamtegevusest. Kui esimest alamtegevust saab teha  $m$  viisil ja pärast esimese alamtegevuse täitmist saab teist alamtegevust teha  $n$  viisil, siis kogu tegevuse sooritamiseks on  $mn$  erinevat võimalust.

**Liitmisreegel.** Kui ühte tegevust saab teha  $m$  viisil ja teist tegevust  $n$  viisil, kusjuures neid tegevusi ei saa teha korraga, siis kas esimese või teise tegevuse sooritamiseks on  $m + n$  erinevat võimalust.

Korrutamisreegli puhul on oluline, et teist alamtegevust saab teha  $n$  viisil alati, sõltumata sellest, milline viis valiti esimese alamtegevuse jaoks. Kui tegevus tähendab näiteks elementide valimist, siis ei tohi teise sammu valikuvõimaluste arv sõltuda sellest, milline valik tehti esimesel sammul (küll aga võivad sellest sõltuda valikuvõimalused ise). Korrutamisreegel vastab loendamisülesannetes tihti esinevatele arutluskäikudele, kus otsitava paigutus- või valikuvõimaluste arvu leidmiseks kombineeritakse ühe tegevuse kõiki teostamisviise teise tegevuse kõigi teostamisviisidega.

Liitmisreegel väidab sisuliselt seda, et kui uuritavad valikud on jagatud kahte klassi, siis valikuvõimaluste koguarvu saame, kui liidame mõlema klassi võimaluste arvud. Seejuures tuleb jälgida, et klassidel poleks ühisosa, sest muidu loeksime mõnda võimalust kaks korda.

Nii korrutamise- kui ka liitmisreeglit saab lihtsasti üldistada rohkem kui kahe (alam)tegevuse juhule.

Mõlemat reeglit oleme eelnevas mitmel pool kasutanud. Näiteks permutatsioonide arvu ja kordumistega permutatsioonide arvu leidsime puhtalt korrutamisreegli abil, liitmisreeglit kasutasime näite 2 teises osas. Toome kummagi reegli rakendamise kohta veel ühe näite.

*Näide 14.* Antsul on 5 laevamudelit ja 6 lennukimudelit. Näituse jaoks valib ta nendest välja 3 ühte liiki mudelit ja 4 teist liiki mudelit. Mitu erinevat näitusekomplekti saab Ants moodustada?

Kui Ants valib kolm laevamudelit ja neli lennukimudelit, siis kolme laevamudeli valimiseks viie hulgast on  $C(5, 3) = 10$  võimalust ning nelja lennukimudeli valimiseks kuue hulgast  $C(6, 4) = 15$  võimalust. Korrutamisreegli põhjal saab laevu ja lennukeid nii valida ühtekokku  $10 \cdot 15 = 150$  viisil.

Teiseks, kui Ants valib neli laevamudelit ja kolm lennukimudelit, siis on laevade valimiseks  $C(5, 4) = 5$  võimalust ja lennukite valimiseks  $C(6, 3) = 20$  võimalust. Korrutamisreegli põhjal saab sel juhul laevu ja lennukeid valida  $5 \cdot 20 = 100$  viisil.

Et kolme laevaga mudelikomplekti ja nelja laevaga komplekti ei saa valida korraga, siis neist emma-kumma valikuks on võimalusi liitmisreegli põhjal  $150 + 100 = 250$ .

## Ülesanded

1. Läti autonumbrid koosnevad kahest tähest ja sellele järgnevast ühe- kuni neljakohalisest arvust, näiteks CZ-2357 ja BH-34. Mitmele autole numbreid jätkub, kui tähti A-st Z-ni on kokku 26?
2. Klassis on kaks rida pinke, kummaski reas kuus pinki. Kaheistkümnest õpilasest soovib neli istuda aknapoolses reas, kolm uksepoolses reas ja viiel on ükskõik, kus istuda. Mitmel viisil saab õpilased vastavalt nende soovile istuma paigutada?
3. Ühikatoas elab kolm üliõpilast. Neil on kokku 4 tassi, 5 alustassi ja 6 teelusikat (kõik omavahel erinevad). Mitmel viisil saavad nad katta kohvilaua (igäühele tass, alustass ja lusikas)?
4. Röövel nägi, et neljakohalise PIN-koodi kaks numbrit olid 4 ja 8. PIN-koodi kõik numbrid on erinevad. Mitu koodi vastab niisugustele tingimustele?
5. Hulgast  $A$ , mis sisaldab  $n$  elementi, valitakse kaks alamhulka  $X$  ja  $Y$ . Mitmel viisil saab neid alamhulki valida, et kehtiks a)  $X \neq Y$ ; b)  $X \subseteq Y$ ?
6. Mitmel viisil saab sirge laua äärde paigutada 5 poissi ja 5 tüdrukut nii, et poleks kahte kõrvuti istuvat poissi ega kahte kõrvuti istuvat tüdrukut?
7. Ümmarguse laua ääres on 10 kohta. Mitmel viisil saab sinna istuma paigutada 5 meest ja 5 naist nii, et mehed ja naised istuksid vaheldumisi? Paigutused, mis saadakse üksteisest laua pööramisega, lugeda samaks.
8. Ruudukujulise laua ümber istub neli meest ja neli naist, mehed ja naised vaheldumisi, ruudu igal küljel kaks inimest. Mitmel viisil võib inimesi niiviisi laua äärde istuma paigutada? Paigutused, mis saadakse üksteisest laua pööramisega, lugeda samaks.
9. Palindroomiks nimetame naturaalarvu, mis jääb samaks, kui teda lugeda vasakult paremale või paremalt vasakule. Näiteks 121, 1, 2002 ja 4 on kõik palindroomid. Kui palju leidub palindroome, mis on väiksemad kui 1000000?
10. Härra Detsimaal soovib oma lapsele õpetada ühe- kuni neljakohaliste arvude lugemist. Selleks valmistab ta kaardid ning kirjutab igäühele ühe arvu. Kirjutamisel kasutab ta harilikku taskuarvutite kirjaviisi: kui kaarti pöörata 180 kraadi võrra, siis numbrid 0, 1, 2, 5, 8 ei muutu, number 6 läheb numbriks 9 ja vastupidi. Vähemalt mitu kaarti peab härra Detsimaal valmistama, et ta saaks oma lapsele näidata kõiki ühe- kuni neljakohalisi arve?

11. Jõuluvanal on  $n$  liiki kingitusi. Lasteaias korraldatakse jõulupidu. Igale lapsele võib jõuluvana anda igast liigist ülimalt ühe kingituse, seejuures tuleb arvestada järgmisi tingimusi.
- Ükski laps ei tohi jääda ilma kingituseta ning ei tohi ka saada sama komplekti kingitusi nagu keegi teine.
  - Iga kahe lapse korral peab leiduma kingitus, mille mõlemad saavad.
- Maksimaalselt mitu last võib jõulupeost osa võtta?
12. Puhas eesti tähestik (ilma võõrsõnades esinevate tähtedeta) on järgmine: A, B, D, E, G, H, I, J, K, L, M, N, O, P, R, S, T, U, V, Ö, Ä, Õ, Ü. Oletame, et kolmetähelises sõnas esineb kindlasti vähemalt üks täishäälik ja vähemalt üks kaashäälik. Mitu niisugust kolmetähelist „sõna“ saab selles tähestikus moodustada?
13. Mitmel viisil saab sõnas MATEMAATIKA tähti ümber paigutada nii, et kaks A-tähte poleks kuskil kõrvuti?
14. Mitmel viisil saab sõnas KOMBINATOORIKA tähti ümber paigutada nii, et kaks ühesugust tähte poleks kuskil kõrvuti?
15. Haljastuskeskusel on haljastustöödeks kasutada kuut liiki puid. Tänavaaärde tahetakse istutada kuuest puust koosnev rida, milles on 1 ühte liiki, 2 teist liiki ja 3 kolmandat liiki puud. Sama liiki puude omavaheline järjekord oluline ei ole. Mitu võimalust on niisugust puude rida moodustada?
16. Kuus tennisehuvilist korraldas paarismänguturniiri. Igas mängus moodustasid neli inimest kaks paari, kes mängisid omavahel, ülejäänud kaks olid selle mängu kohtunikud. Iga paar pidas iga võimaliku vastaspaariga täpselt ühe mängu. Mitu mängu toimus turniiri käigus?
17. Praktikumist võtab osa 12 üliõpilast. Laboratoorse töö jaoks tuleb neist moodustada 4 rühma, igaühes 3 tudengit. Rühmi eristatakse ainult koosseisu poolest, rühmade omavaheline järjestus oluline ei ole. Mitu võimalust on rühmi moodustada?
18. Kapis on kümmet liiki raamatuid, igaühte kaks eksemplari. Mitmel viisil võib need jagada nelja inimese vahel nii, et keegi ei saaks ühest ja samast raamatust mõlemat eksemplari?
19. Numbritest 0 ja 1 koostatakse kõikvõimalikud  $n$ -kohalised arvud, mis sisaldavad  $k$  ühte ( $k < n$ ). Mitmel viisil saab nende hulgast valida kaks arvu, milles nullid asuvad kõik erinevatel kohtadel?
20. Mitmel viisil saab numbritest 0 ja 1 koostada  $n$ -kohalise järjendi,

milles leidub  $k$ -kohaline ( $k < n$ ) ainult ühtedest koosnev osajär-jend, kuid ei leidu ( $k + 1$ )-kohalist?

21. Rahukõnelustest riikide  $A$  ja  $B$  vahel võtab osa 6 riigi  $A$  esinda-jat, 7 riigi  $B$  esindajat ja 8 neutraalset vaatlejat. Mitmel viisil saab nende inimeste hulgast moodustada 7-liikmelise täidesaatva komitee, milles riikide  $A$  ja  $B$  esindajaid on ühepalju?
22. Õukonna 16 ministrist on 9 kuninga ja 7 kardinali pooldajad. Mitmel viisil saab ministrite hulgast valida 12-liikmelise sõja-nõukogu, kus ühegi poole esindajaid pole rohkem kui 8?
23. Ehitusfirma püstitas tänava äärde 12 uut maja, kummalegi poole tänavat 6 maja. Osa maju otsustati värvida roheliseks, ülejäänud aga oranžiks. Mitu võimalust on maju värvida, et kummalgi pool tänavat oleks rohelisi maju võrdne arv?
24. Tasand võrrandiga  $x + y + z = 20$  läbib teiste seas ka selliseid punkte, mille kõik koordinaadid on positiivsed täisarvud. Kui palju niisuguseid punkte see tasand läbib?
25. Mitmel viisil saab kolme värviga värvida 6 ühesugust palli, kui on nõutav, et iga värv peab esinema vähemalt üks kord?
26. Mitmel erineval viisil on võimalik valida kolme sinise, nelja valge ja viie punase palli seast 4 palli?
27. Mitmel erineval viisil on võimalik valida viie punase, viie sinise ja viie kollase palli hulgast 10 palli, kui iga värvi palle peab valikus olema vähemalt kaks tükki.
28. Kontrolltöös on 5 ülesannet, igaühe eest võib saada 0 kuni 10 punkti. Mitmel viisil võivad kontrolltöö punktid jaguneda, kui kogusumma on 25? Punktide järjekord on oluline, näiteks jaotus 3-4-5-6-7 erineb jaotusest 7-6-5-4-3.
29. Marpallivõistkond on kuueliikmeline ning koosneb kolmest mees- ja naismängija paarist. Rahvuskoondise liikmeks kandideerib 7 meest ja 7 naist, seejuures riigi 7 provintsist igaühest üks mees ja üks naine. Kogemustest on teada, et kahte sama provintsi män-gijat ühte paari paigutada ei tasu. Mitu võimalust on peatreeneril sellistel tingimustel koondvõistkonda moodustada?
30. Nurgapeasel lillemüüjal on hommikusest kauplemisest järele jää-nud veel 4 tulpi, 5 nartsissi ja 6 maikellukest. Ostjate ligimeeli-tamiseks moodustab ta neist kolm kimpu, igaühes 5 lille. Mitmel viisil saab kimpe koostada, kui ühte liiki lilled lugeda samaväär-seteks ja kimpude järjekorda ei arvestata?

### III. BINOOMKORDAJAD

**1. Binoomkordajate omadusi.** Nagu eespool nimetatud, on binoomkordaja arv, mille väärtuse suvaliste mittenegatiivsete täisarvude  $n$  ja  $m$  korral võib esitada järgmisel kujul (loetakse „ $n$  üle  $m$ -i“):

$$\binom{n}{m} = \frac{(n)_m}{m!} = \frac{n!}{m!(n-m)!}.$$

Arve  $n$  ja  $m$  nimetatakse indeksiteks. Binoomkordaja väljendab kombinatsioonide arvu  $n$  elemendist  $m$ -kaupa ehk teiste sõnadega, võimaluste arvu valida  $n$ -elemendilisest hulgast välja mingi  $m$ -elemendiline alamhulk. Et binoomkordajad esinevad kombinatoorikas väga sageli, on kasulik tunda nende olulisemaid omadusi.

Paljude omaduste tõestamiseks ja tuletamiseks võib kasutada ülaltoodud valemit, kuid sageli saab seda teha ka puhtalt kombinatoorse arutelu teel: binoomkordaja kombinatoorse interpretatsiooni kaudu taandame tõestatava seose väiteks teatavate valikuvõimaluste arvu kohta, misjärel saab rakendada korrutamise- või liitmisreeglit või mingit muud eelmises peatükis vaadeldud võtet.

**Omadus 1.** *Kui  $n$  ja  $m$  on mittenegatiivsed täisarvud, siis*

$$\binom{n}{m} = \binom{n}{n-m}.$$

**Tõestus.** Vaadeldav võrdus järeldub otseselt binoomkordaja viimati toodud esitusest, sest seal esineva avaldise väärtus ei muutu, kui asendada arv  $m$  arvuga  $n - m$ .  $\square$

Seda omadust nimetatakse ka binoomkordajate sümmeetrlisuseks alumise indeksi suhtes. Järgmine omadus võimaldab avaldada binoomkordajat ühe võrra väiksema ülemise indeksiga binoomkordajate kaudu.

**Omadus 2.** *Kui  $n$  ja  $m$  on positiivsed täisarvud, siis*

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}.$$

**Tõestus.** Valemi järgi

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-1-m)!} + \frac{(n-1)!}{(m-1)!(n-m)!} = \\ &= \frac{(n-1)!(n-m) + (n-1)!m}{m!(n-m)!} = \frac{(n-1)!(n-m+m)}{m!(n-m)!} = \binom{n}{m}, \end{aligned}$$

millega oleme parema poole teiseks vasakuks pooleks.  $\square$

Kumbagi võrdust saab tõestada ka kombinatoorselt. Näiteks omadus 1 väidab, et  $n$ -elemendilisel hulgal on  $m$ -elemendilisi alamhulki

sama palju kui  $(n - m)$ -elemendilisi. Tõepoolest, et iga  $m$ -elemendilise alamhulga täiend on  $(n - m)$ -elemendiline hulk ja vastupidi, on need kaks alamhulkade klassi omavahel üksüheses vastavuses.

Omaduse 2 põhjendamiseks märgistame ühe elemendi antud  $n$ -elemendilises hulgas ning jaotame selle hulga kõik  $m$ -elemendilised alamhulgad kahte liiki: need, mis sisaldavad märgitud elementi, ja need, mis seda ei sisalda. Esimest liiki alamhulki on ilmselt  $\binom{n-1}{m-1}$ , sest märgitud elemendile tuleb lisada veel  $m - 1$  elementi ülejäänud  $n - 1$  seast. Teise liiki aga kuulub  $\binom{n-1}{m}$  alamhulka, sest sel juhul tuleb hulga kõik  $m$  elementi valida ülejäänute seast. Liitmisreegli abil saamegi nüüd vajaliku tulemuse.

Näide 1. Tõestada võrdus

$$\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \dots + \binom{n+m}{m} = \binom{n+m+1}{m}.$$

Kirjutame esimese liikme asemele temaga võrdse arvu  $\binom{n+1}{0}$ . Kui nüüd liita sellele summa teine liige, siis saame omaduse 2 põhjal

$$\binom{n+1}{0} + \binom{n+1}{1} = \binom{n+2}{1},$$

liites tulemusele kolmanda liikme, saame

$$\binom{n+2}{1} + \binom{n+2}{2} = \binom{n+3}{2}$$

jne. Pärast viimast liitmist jääb järele üksainus binoomkordaja

$$\binom{n+m+1}{m},$$

millega võrdus ongi tõestatud.

Binoomkordajaid võib esitada kolmnurkse tabelina, mida nimetatakse *Pascali kolmnurgaks* prantsuse matemaatiku ja filosoofi Blaise Pascali (1623–1662) järgi, kes koostas põhjaliku uurimuse binoomkordajate omaduste kohta. Pascali kolmnurga iga rida koosneb kõigist sama ülemise indeksiga binoomkordajatest:

$$\begin{array}{cccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & & \binom{1}{0} & \binom{1}{1} & & & \\
 & & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & & \\
 & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & & \\
 & \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & & & \\
 \binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & & & \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
 \end{array}$$



Asendades binoomkordajad nende väärtustega, võime selle tabeli kirja panna ka kujul

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & 1 & & 1 \\
 & & & 1 & 2 & & 1 \\
 & & 1 & 3 & 3 & & 1 \\
 & 1 & 4 & 6 & 4 & & 1 \\
 1 & 5 & 10 & 10 & 5 & & 1 \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots
 \end{array}$$

Omaduse 2 põhjal võrdub Pascali kolmnurgas iga arv kahe tema kohal asuva arvu summaga. Selle seaduspärasuse järgi võib tabelit lihtsasti, ainult liitmistehetega jätkata kuitahes kaugele ja arvutada välja kuitahes suure ülemise indeksiga binoomkordajaid. Omaduse 1 tõttu on Pascali kolmnurk sümmeetriline vertikaaltelje suhtes, samuti on lihtne näha, et iga rea esimene ja viimane element on alati võrdsed ühega, teine ja eelviimane element aga vastava rea binoomkordajate ülemise indeksiga.

**2. Binoomvalem.** Üldiselt tuntuks võib lugeda valemid

$$\begin{aligned}
 (x + y)^2 &= x^2 + 2xy + y^2 \\
 (x + y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3
 \end{aligned}$$

Analoogsed seosed teiste astendajate jaoks annab järgmine teoreem.

**Teoreem 1.** *Kui  $n$  on mittenegatiivne täisarv, siis*

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

Seda võrdust nimetatakse *binoomvalemiks* ning formuleeritud teoreemi ka *binoomteoreemiks*. Sõna „binoom“ tähendab kahest liikmest koosnevat avaldist, praegusel juhul siis kaksliiget  $x + y$ . Binoomkordajad on seega lihtsalt binoomvalemi liikmete kordajad, millest on tulnud ka nende nimetus.

**Tõestus.** Kirjutame vasaku poole kujul

$$(x + y)^n = (x + y)(x + y) \dots (x + y)$$

ja avame sulud. Iga liikme saamiseks tuleb teatud arvust teguritest valida  $y$  ja ülejäänutest  $x$ . Seejuures alati, kui  $i$  tegurist võtta  $y$  ja ülejäänud  $n - i$  tegurist  $x$ , moodustub liige  $x^{n-i}y^i$ . Et neid  $i$  tegurit, kust võetakse  $y$ , saab antud  $n$  teguri hulgast välja valida  $\binom{n}{i}$  viisil, siis liige  $x^{n-i}y^i$  esineb tekkivas summas ka sama palju kordi.  $\square$

Tuginedes tõestatud teoreemile ja kasutades Pascali kolmnurka, võime seega kirjutada

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

$$(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

Ka kõrgema astmega valemeid saab lihtsasti tuletada. Kahe arvu vahe astmete valemid on samuti binoomvalemi erijuhud, kui seal võtta  $y$  asemel  $-y$ .

**Näide 2.** Kui suur on astme  $\left(2x + \frac{1}{x^2}\right)^{12}$  arendises vabaliige? Arendise  $i$ -s liige on binoomvalemi järgi

$$\binom{12}{i}(2x)^{12-i}(x^{-2})^i = \binom{12}{i}2^{12-i}x^{12-3i}.$$

Vabaliikme puhul peab seega olema  $12 - 3i = 0$  ehk  $i = 4$ . Niisiis, otsitav liige on

$$\binom{12}{4}2^8 = 126\,720.$$

Mitmed seosed binoomkordajate vahel tulenevad binoomvalemist otseste järeldustena.

**Järeldus 1.** *Kehtib võrdus*

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

**Tõestus.** Võtame binoomvalemis  $x = y = 1$ . □

**Järeldus 2.** *Kehtib võrdus*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^n \binom{n}{n} = \begin{cases} 0, & \text{kui } n \geq 1, \\ 1, & \text{kui } n = 0. \end{cases}$$

**Tõestus.** Võtame binoomvalemis  $x = 1$  ja  $y = -1$ . Paremalt saame siis vahelduvate märkidega binoomkordajate summa, liidetava märgi määrab tegur  $(-1)^i$ . Vasakul saame avaldise  $0^n$ , mille väärtus on 0 juhul  $n \geq 1$  ja 1 juhul  $n = 0$ . □

Mõlemat võrdust on võimalik jällegi tõestada ka kombinatoorse tähenduse abil. Näiteks järeldus 1 tuleneb asjaolust, et  $n$ -elemendilisel hulgal on parajasti  $2^n$  alamhulka, binoomkordajate summa võrduse vasakul poolel aga loebki üles kõigi 0-elementiliste, 1-elementiliste jne alamhulkade arvud. Järelduse 2 saame sellest, et juhul  $n \geq 1$  on  $n$ -elemendilisel hulgal paarisarvu elemente sisaldavaid alamhulki sama palju kui paaritut arvu elemente sisaldavaid. Tõepoolest, fikseerime mingi elemendi. Kõigist alamhulkadest, mis sisaldavad seda elementi, jätame ta välja, kõigisse neisse aga, mis teda ei sisalda, lisame juurde. Niisugune operatsioon teisendab paarisarvu elementidega

alamhulgad paaritu arvu elementidega alamhulkadeks ja vastupidi, seega on need kaks alamhulkade klassi üksiheses vastavuses.

Vaatleme veel mõnda näidet, kuidas binoomvalemi abil kindlaks teha binoomkordajate vahelisi seoseid.

*Näide 3.* Tõestada võrdus

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

Võrdleme seose

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

mõlemal poolel liikme  $x^n$  kordajaid. Paremalt on see kordaja vastavalt binoomvalemile  $\binom{2n}{n}$ . Vasakul saab pärast kummaski tegurist sulgude avamist liige  $x^n$  tekkida mitmel viisil: kas võetakse esimesest tegurist  $x^n$  ja teisest 1 või esimesest tegurist  $x^{n-1}$  ja teisest  $x$  jne. Liikme  $x^{n-i}$  kordaja esimeses tegurist on binoomvalemi järgi  $\binom{n}{i}$ , teises tegurist on vastava liikme  $x^i$  kordaja  $\binom{n}{n-i}$ . Et liikme  $x^n$  kordaja võrduse mõlemal poolel on sama, siis

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

Vastavalt binoomkordajate omadusele 1 on igas liidetavas teine tegur võrdne esimesega, seega on nõutav võrdus tõestatud.

Binoomvalemis esinevad avaldised on kõik kas hulkliikmed või nende astmed, seetõttu võib avaldiste uurimisel rakendada kõiki hulkliikmete puhul lubatud teisendusi.

*Näide 4.* Tõestada võrdus

$$\binom{n}{1} + 2\binom{n}{2} + \dots + n\binom{n}{n} = n \cdot 2^{n-1}.$$

Binoomvalemi põhjal

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \dots + \binom{n}{n}x^n.$$

Diferentseerides seda seost, saame

$$n(1+x)^{n-1} = \binom{n}{1} + 2\binom{n}{2}x + \dots + n\binom{n}{n}x^{n-1}.$$

Võttes siin nüüd  $x = 1$ , jõuamegi otsitava võrduseni.

Lõpuks toome veel ühe näite binoomvalemi rakendamisest niisuguste väidete tõestamisel, mis otseselt binoomkordajaid ei puuduta.

*Näide 5.* Piirväärtuste teoorias vaadeldakse jada  $(a_n)$  üldliikmega  $a_n = \left(1 + \frac{1}{n}\right)^n$ . Tõestada, et iga  $n$  korral kehtib võrratus  $a_n < 3$ .

Binoomvalemist

$$a_n = \sum_{i=0}^n \binom{n}{i} \frac{1}{n^i} = \sum_{i=0}^n \frac{n!}{i!(n-i)!n^i}.$$

Summamärgi all  $n! \leq (n-i)!n^i$ , sest kui korrutises  $n! = 1 \cdot 2 \cdot \dots \cdot n$  asendame  $i$  viimasest tegurist igäihe arvuga  $n$ , saame võrratuse parema poole. Seega

$$a_n \leq \sum_{i=0}^n \frac{1}{i!}.$$

Edasi, asendades juhul  $i \geq 1$  arvus  $i! = 1 \cdot 2 \cdot \dots \cdot i$  kõik tegurid peale esimese teguritega 2, näeme, et kehtib võrratus  $i! \geq 2^{i-1}$ . Järelikult

$$a_n \leq 1 + \sum_{i=1}^n \frac{1}{2^{i-1}} = 1 + \frac{1 - \frac{1}{2^n}}{1 - \frac{1}{2}} = 1 + 2 - \frac{1}{2^{n-1}} < 3.$$

Et  $\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n = e$ , siis oleme ühtlasi ka tõestanud, et  $e \leq 3$ .

**3. Multinoomvalem.** Binoomvalemiga analoogiline seos kehtib ka juhul, kui astendatakse mitte kaks-, vaid üldisemalt hulkliiget. Vastavat võrdust nimetatakse *multinoomvalemiks* ja selle liikmete kordajad on multinoomkordajad

$$\binom{n}{m_1, m_2, \dots, m_k} = \frac{n!}{m_1! m_2! \dots m_k!}.$$

Multinoomvalem ise on järgmine.

**Teoreem 2.** *Kui  $n$  on mittenegatiivne täisarv, siis*

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\substack{i_1 + \dots + i_k = n \\ 0 \leq i_1, \dots, i_k \leq n}} \binom{n}{i_1, i_2, \dots, i_k} x_1^{i_1} x_2^{i_2} \dots x_k^{i_k}.$$

**Tõestus.** Sarnaselt binoomvalemi tõestusega vaatleme korrutatist

$$(x_1 + \dots + x_k)^n = (x_1 + \dots + x_k)(x_1 + \dots + x_k) \dots (x_1 + \dots + x_k).$$

Sulgude avamisel saame liikme  $x_1^{i_1} x_2^{i_2} \dots x_k^{i_k}$  alati siis, kui  $i_1$  sulust valime  $x_1$ ,  $i_2$  sulust  $x_2$  jne kuni  $i_k$  sulust  $x_k$ . Ülesanne on sisuliselt sama nagu leida võimaluste arv moodustada  $n$ -tähelist sõna, mis sisaldab  $i_1$  eksemplari esimest tähte,  $i_2$  eksemplari teist tähte jne. Nagu eelmises peatükis nägime, avaldub selliste võimaluste arv multinoomkordajana, mis ongi järelikult liikme  $x_1^{i_1} x_2^{i_2} \dots x_k^{i_k}$  kordajaks.  $\square$

Multinoomvalemis toimub summeerimine üle arvu  $n$  kõigi lahutuste  $k$  mittenegatiivse liidetava summaks ehk teiste sõnadega, üle kõigi võrrandi  $x_1 + \dots + x_k = n$  lahendite. Eelmise peatüki näites 13

leidsime nende lahendite arvuks kordumistega kombinatsioonide arvu  $F(k, n)$ . See arv näitab ka, mitu erinevat liiget multinoomvalemil paremal poolel üldse tekib. Näiteks kolmeliikme astme  $(a + b + c)^4$  lahtikirjutamisel tekib  $F(3, 4) = 15$  liiget.

Näide 6. Leida avaldise  $(x^2 + x + 1)^8$  arendises liikme  $x^5$  kordaja. Multinoomvalemil põhjal

$$\begin{aligned} (x^2 + x + 1)^8 &= \sum_{i_1+i_2+i_3=8} \binom{8}{i_1, i_2, i_3} (x^2)^{i_1} x^{i_2} 1^{i_3} \\ &= \sum_{i_1+i_2+i_3=8} \frac{8!}{i_1! i_2! i_3!} x^{2i_1+i_2}. \end{aligned}$$

Liikme  $x^5$  saame indeksite  $i_1, i_2, i_3$  nende väärtuste puhul, mille korral  $2i_1 + i_2 = 5$ . Selleks, et viimane võrdus kehtiks, peab olema  $i_1 = 0$  ja  $i_2 = 5$  või  $i_1 = 1$  ja  $i_2 = 3$  või  $i_1 = 2$  ja  $i_2 = 1$ . Kõigil kolmel juhul peab arvu  $i_3$  väärtus olema selline, et indeksid annaksid summaks kokku 8. Liikme  $x^5$  kordaja on seega

$$\frac{8!}{0!5!3!} + \frac{8!}{1!3!4!} + \frac{8!}{2!1!5!} = 504.$$

Erijuhul  $k = 2$  saame multinoomvalemist binoomvalemil ning multinoomkordaja taandub binoomkordajaks. Ka siis, kui  $k > 2$ , võib multinoomkordaja avaldada binoomkordajate kaudu seosega

$$\binom{n}{m_1, m_2, \dots, m_k} = \binom{n}{m_1} \binom{n-m_1}{m_2} \dots \binom{n-m_1-\dots-m_{k-1}}{m_k},$$

sest kirjutades võrduse parema poole vastavalt binoomkordajate valemile lahti, saame korrutise

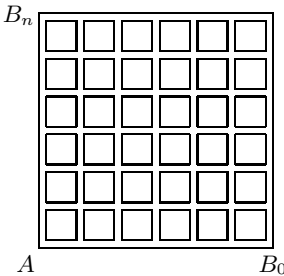
$$\frac{n!}{m_1!(n-m_1)!} \cdot \frac{(n-m_1)!}{m_2!(n-m_1-m_2)!} \cdot \dots \cdot \frac{(n-m_1-\dots-m_{k-1})!}{m_k!(n-m_1-\dots-m_k)!},$$

millest pärast taandamisi jääbki järele võrduse vasakul poolel asuva multinoomkordaja avaldis.

## Ülesanded

1. Millise  $k$  väärtuse korral on binoomkordaja  $\binom{n}{k}$  kõige suurem, kui  $n$  on fikseeritud?
2. Malelaua vasakul alumisel ruudul a1 asub kuningas, millel lubatakse ühe käiguga liikuda ainult kas sammu paremale või sammu üles. Mitu võimalikku teekonda saab kuningas valida, et jõuda laua paremale ülemisele ruudule h8? Mitu erinevat teekonda on siis, kui malelaua mõõtmed on  $k \times l$ ?

3. Tasast maastikku katab korrapärane teedevõrk mõõtmetega  $n \times n$  ruutu. Punktist  $A$  väljub täpselt keskööl  $2^n$  inimest. Pooled neist lähevad punkti  $B_0$  suunas ja pooled punkti  $B_n$  suunas. Ühe lõigu läbimiseks kulub üks tund. Teeristini jõudes jaguneb kumbki rühm kaheks: pooled lähevad  $B_0$  suunas ja pooled  $B_n$  suunas. Samasugune jagunemine toimub igal teeristil. Kus asuvad need inimesed  $n$  tunni pärast ja mitu inimest on siis igal teeristil?



Tõestada võrdused.

4.  $\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$       8.  $\sum_{i=0}^k \binom{n}{i} \binom{m}{k-i} = \binom{n+m}{k}$   
 5.  $\sum_{i \geq 0} \binom{n}{2i+1} = 2^{n-1}$       9.  $\sum_{i=1}^n (-1)^i i \binom{n}{i} = 0$ , kui  $n > 1$   
 6.  $\sum_{i=0}^m \binom{n-i}{m-i} = \binom{n+1}{m}$       10.  $\sum_{i=0}^n \frac{1}{i+1} \binom{n}{i} = \frac{2^{n+1} - 1}{n+1}$   
 7.  $\sum_{i=0}^n \binom{n+i}{n} = \binom{2n+1}{n+1}$       11.  $\sum_{i=0}^n (2i+1) \binom{n}{i} = 2^n(n+1)$

12. Olgu  $m \geq n$ . Tõestada, et

$$\sum_{i=0}^n \frac{\binom{n}{i}}{\binom{m}{i}} = \frac{m+1}{m-n+1}.$$

13. Kasutades avaldise  $(1+x)^n$  ja tema tuletise arendist, tõestada võrdus

$$\sum_{i=1}^n i \binom{n}{i}^2 = \frac{n}{2} \binom{2n}{n}.$$

14. Kasutades samasust  $(1+x)^n(1-x)^n = (1-x^2)^n$ , tõestada võrdus

$$\sum_{i=0}^m (-1)^i \binom{n}{i} \binom{n}{m-i} = \begin{cases} (-1)^k \binom{n}{k}, & \text{kui } m = 2k, \\ 0, & \text{kui } m = 2k+1. \end{cases}$$

15. Tõestada valemid (siin on  $r$  mingi naturaalarv)

$$\sum_{i=0}^n i(i-1)\dots(i-r+1) \binom{n}{i} = n(n-1)\dots(n-r+1) \cdot 2^{n-r}$$

ning

$$\sum_{i=0}^n (-1)^i i(i-1) \dots (i-r+1) \binom{n}{i} = 0.$$

16. Eelmise ülesande tulemust kasutades leida summad

$$\sum_{i=0}^n i^2 \binom{n}{i} \quad \text{ja} \quad \sum_{i=0}^n i^3 \binom{n}{i}.$$

17. Vaatleme teekondi, mis algavad koordinaattasandi punktis  $(0, 0)$ , kulgevad ühikpikkusega lõikudena mööda täisarvuliste koordinaatidega punkte ainult paremale ja üles ning lõpevad punktis  $(n+m+1, k)$ . Kõik sellised teekonnad võib jaotada klassidesse selle järgi, milline on nende  $y$ -koordinaat sellal, kui nad siirduvad sirgelt  $x = n$  sirgele  $x = n+1$ . Kasutades niisugust geomeetrilist tõlgendust, tõestada võrdus

$$\sum_{i=0}^k \binom{n+i}{n} \binom{m+k-i}{m} = \binom{n+m+k+1}{n+m+1}.$$

18. Tõestada võrratus  $\binom{2n+m}{n} \binom{2n-m}{n} \leq \binom{2n}{n}^2$ .

19. Leida summa  $\sum_{i_1=1}^m \sum_{i_2=1}^{i_1} \dots \sum_{i_{n-1}=1}^{i_{n-2}} \sum_{i_n=1}^{i_{n-1}} 1$ .

20. Tõestada Vandermonde'i valem

$$(x+y)_n = \sum_{i=0}^n \binom{n}{i} (x)_i (y)_{n-i},$$

kus kirjutus  $(a)_k$  tähistab arvu  $a$  kahanevat  $k$ -faktoriaali.

21. Olgu  $k$  fikseeritud naturaalarv. Tõestada, et iga mittenegatiivse täisarvu  $n$  korral leidub selline üheselt määratud arvujärjend  $0 \leq a_1 < a_2 < \dots < a_k$ , et

$$n = \binom{a_1}{1} + \binom{a_2}{2} + \dots + \binom{a_k}{k}.$$

22. Tõestada võrdus  $(x+y+z)^n = \sum_{i=0}^n \sum_{j=0}^{n-i} \binom{n}{i} \binom{n-i}{j} x^i y^j z^{n-i-j}$ .

23. Tõestada, et multinoomkordajate puhul kehtib seos

$$\binom{n}{m_1, \dots, m_k} = \sum_{i=1}^k \binom{n-1}{m_1, \dots, m_{i-1}, m_i-1, m_{i+1}, \dots, m_k}.$$

## IV. REKURRENTSED VÕRRANDID

**1. Fibonacci arvud.** Sageli kasutatakse kombinatoorikas võtet, kus antud loendamisülesanne taandatakse ühele või mitmele analoogilisele, kuid lihtsamale ülesandele. Selleks näidatakse viis, kuidas lihtsamate ülesannete lahendite järgi leida keerukama ülesande lahendit. Alustades siis ülesannetest, mille lahendamine raskusi ei valmista, leitakse järk-järgult üha keerukamate ülesannete lahendeid, kuni lõpuks jõutakse lähteülesandeni. Kui ülesanne sõltub naturaalarvulisest parameetrist, siis tähendab taandamine tavaliselt seda, et ülesande lahend avaldatakse parameetri väiksematele väärtustele vastavate ülesannete lahendite kaudu. Seejuures osutuvad ülesanded, mille puhul parameetri väärtus on kõige väiksem, tihti peale triviaalseks, nii et peamine küsimus seisneb selles, kuidas lahendit parameetri väiksematelt väärtustelt suurematele edasi kanda.

Itaalia matemaatik Leonardo Fibonacci (u 1175 – u 1250), keda peetakse keskaja üheks silmapaistvaimaks matemaatikuks, vaatles oma 1202. aastal avaldatud teoses „Liber abaci“ järgmist ülesannet. Talunikul on üks paar vastsündinud jäneseid, isane ja emane. Ühe kuu pärast sünnist alates muutuvad jäneseid paaritumisvõimeliseks ning kaks kuud pärast sünni annab emane jänes ühe paari järglasi. Eeldame, et ükski jänes ei sure ning et emane jänes annab uue paari, isase ja emase, igal kuul, alates kahe kuu vanuseks saamisest. Mitu paari jäneseid on talunikul  $n$ -ndal kuul?

Kui  $n$  on väike, siis võime tulemuse leida otse loendades. Esimesel kuul on talunikul üks jänestepaar, teisel kuul samuti üks, kolmandal kaks (sest siis hakkab esimene paar järglasi andma), neljandal kolm (esimene paar annab järgmised järglased), viiendal viis (esimene järglastepaar annab juba ise järglasi) jne.

Olgu  $F_n$  paaride arv  $n$ -ndal kuul. Siis järgmisel kuul on talunikul olemas kõik need jäneseid, kes tal olid  $n$ -ndal kuul, uusi paare lisandub aga parajasti niipalju, kuipalju oli paare eelmisel,  $(n - 1)$ -l kuul, sest need on järgmisel kuul kõik vähemalt kaks kuud vanad ja annavad igaüks ühe uue paari järglasi. Niisiis kehtib võrdus

$$F_{n+1} = F_n + F_{n-1}.$$

Lisaks teame, et  $F_1 = 1$ ,  $F_2 = 1$ ,  $F_3 = 2$ ,  $F_4 = 3$ ,  $F_5 = 5$ . Kasulik on defineerida veel  $F_0 = 0$ , siis jääb leitud seos kehtima ka  $n = 1$  korral. Nüüd saame jänestepaaride arvu ükskõik millisel kuul järk-järgult lihtsasti välja arvutada:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \dots$$



Arve  $F_0, F_1, F_2, \dots$ , kus  $F_0 = 0$  ja  $F_1 = 1$  ning iga naturaalarvu  $n$  korral  $F_{n+1} = F_n + F_{n-1}$ , nimetatakse *Fibonacci arvudeks*.

Vaatleme veel ühte loendamisülesannet. Kui palju saab tähtedest A ja B koostada niisuguseid  $n$ -tähelisi sõnu, kus kaks tähte A ei esine kuskil kõrvuti?

Olgu  $G_n$  selliste  $n$ -täheliste sõnade arv. Leiame valemi, mille järgi saab arvutada  $(n + 1)$ -täheliste sõnade arvu  $G_{n+1}$ . Selleks jaotame kõik  $(n + 1)$ -tähelised sõnad viimase tähe järgi kahte klassi. Kui sõna lõpeb tähega B, siis võib sellele eelneeda suvaline  $n$ -täheline sõna, kus ei esine kõrvuti kahte A-tähte. Kui aga sõna lõpeb tähega A, siis peab eelviimane täht olema B, sest muidu oleksid kaks A-tähte kõrvuti, ent  $n - 1$  esimest tähte võivad jällegi moodustada suvalise  $(n - 1)$ -tähelise sõna, kus pole kõrvuti kahte A-tähte. Liitmisreegli põhjal seega

$$G_{n+1} = G_n + G_{n-1}.$$

Tulemuseks on sama võrrand nagu Fibonacci arvude puhul. Kuid ükski see veel ei tähenda, et  $G_n = F_n$ , sest kumbki arvujada võib lähtuda erinevatest algväärtustest. Näemegi, et  $G_1 = 2$ , sest tingimusi rahuldavaid ühetähelisi sõnu on kaks: A ja B, samuti  $G_2 = 3$ , sest sobivad kahetähelised sõnad on AB, BA ja BB. Kuid et  $G_1 = F_3$  ja  $G_2 = F_4$ , siis on jada  $G_n$  liikmed võrreldes jadaga  $F_n$  nihutatud kahe koha võrra. Järelikult

$$G_n = F_{n+2}.$$

See võrdus kehtib  $n = 1$  ja  $n = 2$  korral ning et jada edasised liikmed arvutatakse kummalgi juhul sama valemi järgi, kehtib võrdus ka siis, kui  $n = 3$ ,  $n = 4$  jne.

Jada, mille iga liige arvutatakse teatava kindla valemi abil sama jada eelnevate liikmete põhjal, nimetatakse *rekurrentseks jadaks* ning jada liikmeid siduvat seost *rekurrentseks seoseks*. Selleks, et rekurrentne jada oleks üheselt määratud, peame lisaks valemile teadma jada esimeste liikmete väärtusi, *algväärtusi*, mille järgi arvutada jada järgmisi liikmeid.

Jada liikmete arvutamine sama jada eelnevate liikmete järgi meenutab induktsioonisammu ja matemaatilist induktsiooni kasutataksegi rekurrentsete jadade omaduste tõestamiseks väga sageli.

*Näide 1.* Tõestada, et Fibonacci arvude vahel kehtib seos

$$F_0 + F_1 + F_2 + \dots + F_n = F_{n+2} - 1.$$

Tõestame selle väite matemaatilise induktsiooniga.

*Baas.* Kui  $n = 0$ , siis omandab tõestamisele kuuluv võrdus kuju  $F_0 = F_2 - 1$  ehk  $0 = 1 - 1$ .

*Samm.* Eeldame, et võrdus kehtib juhul  $n = k$ , st

$$F_0 + F_1 + \dots + F_k = F_{k+2} - 1.$$

Liites mõlemale poolele  $F_{k+1}$ , saame

$$F_0 + F_1 + \dots + F_k + F_{k+1} = F_{k+2} - 1 + F_{k+1}$$

ehk

$$F_0 + F_1 + \dots + F_k + F_{k+1} = F_{k+3} - 1.$$

Järelikult kehtib võrdus ka juhul  $n = k + 1$ .

*Näide 2.* Tõestada, et  $F_{3n}$  on paarisarv.

*Baas.* Kui  $n = 0$ , siis väide kehtib, sest  $F_0 = 0$  on paarisarv.

*Samm.* Eeldame, et  $F_{3k}$  on mingi  $k$  korral paarisarv ning vaatleme arvu  $F_{3(k+1)} = F_{3k+3}$ . Rakendades korduvalt Fibonacci arvude rekurrentset seost, saame

$$F_{3k+3} = F_{3k+2} + F_{3k+1} = F_{3k+1} + F_{3k} + F_{3k+1} = 2F_{3k+1} + F_{3k}.$$

Tulemuse esimene liidetav on ilmselt paarisarv, samuti on induktsiooni eelduse põhjal paarisarv ka teine liidetav.

*Näide 3.* Tõestada, et

$$F_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots,$$

kus summale lisatakse liikmeid niikaua, kuni binoomkordajate ülemine indeks saab alumisest väiksemaks.

Vaatleme tähtedest A ja B koostatud sõnu pikkusega  $n - 1$ , kus kaks tähte A ei esine kõrvuti. Jaotame need sõnad klassidesse, lugedes  $i$ -ndasse klassi sõnad, mis sisaldavad  $i$  korda tähte A ja  $n - 1 - i$  korda tähte B. Kõik  $i$ -nda klassi sõnad võime koostada järgmiselt. Paigutame ühte ritta kõik sõnas esinevad tähed B. Tähtede vahele, samuti rea ette ja taha jääb nüüd  $n - i$  vaba kohta. Valime nendest  $i$  ja paigutame sinna tähed A. Järelikult kuulub  $i$ -ndasse klassi  $\binom{n-i}{i}$  sõna, sest nii mitmel viisil saab  $n - i$  kohast välja valida  $i$  kohta tähtede A jaoks. Kõigi klasside peale kokku on sõnu

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots$$

Teiselt poolt aga teame eelnevast, et sobivate sõnade arv on  $F_{n+1}$ .

**2. Rekurrentse seose koostamine.** Vaatleme nüüd rekurrentsete seoste kasutamist mõne loendamisülesande lahendamisel.

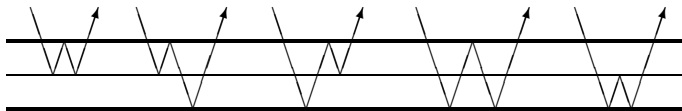
*Näide 4.* Kui palju leidub sõnu pikkusega  $n$ , mis koosnevad tähtedest A, B, C ja D ning mis sisaldavad paaritu arvu tähti A?

Olgu  $A_n$  selliste sõnade arv. Viimase tähe järgi jagunevad kõik sõnad nelja klassi. Kui kustutame sõnades, mis lõpevad tähega A või B, viimase tähe, saame kahe klassi peale kõik sõnad pikkusega  $n - 1$ : need, mis sisaldavad tähte A paarisarv kordi, tekivad A-ga lõppevatest sõnadest, need aga, mis sisaldavad tähte A paaritu arv kordi, B-ga lõppevatest sõnadest. Seega kuulub neisse kahte klassi kokku  $4^{n-1}$  sõna. Sõnu, mis lõpevad tähega C või D, on kumbagi  $A_{n-1}$ , sest pärast viimase tähe kustutamist jäävad mõlemas klassis järele paaritud arvu A-tähti sisaldavad sõnad pikkusega  $n - 1$ . Järelikult kehtib seos

$$A_n = 2A_{n-1} + 4^{n-1}.$$

Selle seose abil saab välja arvutada otsitava sõnade arvu ükskõik millise sõnapikkuse  $n$  korral, lähtudes algväärtusest  $A_1 = 1$ . Edaspidi vaatleme ka meetodeid vastava üldvalemi leidmiseks. Käesoleval juhul osutub selleks  $A_n = (4^n - 2^n)/2$ , sest see avaldis rahuldab nii rekurrentset seost kui ka tingimust  $A_1 = 1$ .

*Näide 5.* Kahekihilisse klaasplaati siseneb ülevalt valguskiir, peegeldub plaatide välisäärtelt ja kihtide eralduspinnalt ning väljub. Mõnel erineval viisil saab kiir plaati läbida, sooritades seejuures täpselt  $n$  peegeldumist? (Joonisel on näidatud kõik võimalused juhul  $n = 3$ .)



Olgu  $A_n$  peegeldumiste arv. Kui viimane peegeldumine toimus välisäärelt, siis jõudis kiir  $n - 1$  peegeldumisega sisenemispunktist välisäärele, seda teed võis ta läbida  $A_{n-1}$  viisil. Kui viimane peegeldumine toimus kihtide eralduspinnalt, siis pidi eelviimane peegeldumine toimuma välisäärelt, sel juhul jõudis kiir  $n - 2$  peegeldumisega sisenemispunktist välisäärele ja ta võis läbida  $A_{n-2}$  erinevat teed. Järelikult

$$A_n = A_{n-1} + A_{n-2}$$

ehk arvud  $A_n$  rahuldavad sama rekurrentset seost nagu Fibonacci arvud. Otsese kontrollimisega võib veenduda, et jada esimesed väärtused  $A_0 = 1$  ja  $A_1 = 2$  langevad kokku Fibonacci jada elementidega  $F_2$  ja  $F_3$ . Seega

$$A_n = F_{n+2}.$$

Rekurrentse seose koostamisel tuleb jälgida, et väiksemamõõtmeline ülesanne oleks esialgselt täpselt analoogiline, teisendades ta vajaduse korral sobivale kujule.

*Näide 6.* Kuus inimest saabub külla ja igauks riputab esikus nagise oma mütsi. Kui hiljem kõik valmistuvad lahkuma, kustub esikus tuli ja igauks võtab pimeduses nagist ühe mütsi. Mitmel viisil võivad külalised mütse võtta, et keegi ei saaks enda oma?

Vaatleme üldjuhtu, kus mütse võtab  $n$  inimest ja olgu  $D_n$  vastav võimaluste arv. Nummerdame inimesed ja mütsid arvudega 1 kuni  $n$  nii, et iga inimese number ja tema mütsi number on samad.

Inimene  $n$  võib mütsi valida  $n-1$  viisil, sest enda oma võtta ei tohi. Oletame et ta valib mütsi number  $i$ . Kui nüüd inimene  $i$  valib mütsi  $n$ , siis on inimesed  $n$  ja  $i$  omavahel mütsid vahetanud ning ülejäänud  $n-2$  inimest saavad mütse võtta  $D_{n-2}$  viisil. Kui aga inimene  $i$  ei vali mütsi  $n$ , siis loeme, nagu kuuluks inimesele  $i$  müts  $n$  ning jätame kõrvale inimese  $n$  koos mütsiga  $i$ . Ülejäänud  $n-1$  inimest peavad siis jagama omavahel ülejäänud  $n-1$  mütsi nii, et keegi ei saaks enda oma. Selleks on  $D_{n-1}$  võimalust.

Nii siis, kui inimene  $n$  valib mütsi  $i$ , siis võivad ülejäänud inimesed endale mütse võtta  $D_{n-1} + D_{n-2}$  viisil. Et aga inimene  $n$  võib mütsi valida  $n-1$  viisil, siis saame seose

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

Algväärtused on  $D_1 = 0$  (ühe inimese puhul pole segiajamine võimalik) ja  $D_2 = 1$  (kahe inimese puhul on ainuke võimalus mütsid vahetada). Nüüd võime arvutada:  $D_3 = 2 \cdot (1+0) = 2$ ,  $D_4 = 3 \cdot (2+1) = 9$ ,  $D_5 = 4 \cdot (9+2) = 44$  ja  $D_6 = 5 \cdot (44+9) = 265$ .

Saadud arve nimetatakse *subfaktoriaalideks* ning neil on kombinaatorikas üsna suur tähtsus lõpliku hulga selliste teisenduste loendamisel, mis jätavad kindla arvu elemente paigale. Sama rekurrentset seost rahuldavad ka faktoriaalid  $n!$ , ainult algtingimused on teised.

**3. Lineaarne rekurrentne võrrand.** Rekurrentne seos võimaldab küll järk-järgult leida jada liikmeid, ent kui meid huvitab jadas ainult ühe liikme väärtus, siis on mõttekam otsida valemit, mille järgi saab selle otse välja arvutada ilma eelnevaid liikmeid leidmata. Kui pole olemas üldist meetodit, kuidas leida lahendivalemit suvalise rekurrentse seose korral, saab seda siiski teha mitmel erijuhul.

Kõige sagedamini esineb rakendustes *lineaarne konstantsete kordajatega rekurrentne võrrand*. Selle üldkuju on

$$A_{n+k} = b_1 A_{n+k-1} + b_2 A_{n+k-2} + \dots + b_k A_n,$$

kus  $b_1, b_2, \dots, b_k$  on teatavad arvilised kordajad ja  $b_k \neq 0$ . Siin avaldub jada järjekordne liige  $k$  eelmise liikme kaudu, arvu  $k$  nimetatakse ka rekurrentse võrrandi *järguks*. Rekurrentse võrrandi *lahendiks* nimetatakse iga jada  $(A_n)$  (mõnikord ka jada üldliikme  $A_n$  avaldist),

mis seda võrrandit rahuldab. Selleks, et jada  $(A_n)$  oleks üheselt määratud, tuleb ette anda tema  $k$  esimese liikme väärtused ehk *algtingimused*, nõudes, et  $A_0 = m_0, A_1 = m_1, \dots, A_{k-1} = m_{k-1}$ , kus  $m_0, m_1, \dots, m_{k-1}$  on arvud. Kui on teada võrrand ja algtingimused, siis saab leida jada ükskõik millise järgneva liikme.

Lihtsuse mõttes vaatleme esialgu teist järku rekurrentset võrrandit

$$A_{n+2} = b_1 A_{n+1} + b_2 A_n,$$

kusjuures algtingimused on  $A_0 = m_0$  ja  $A_1 = m_1$ .

Otsime võrrandi lahendit kujul  $A_n = q^n$ . Asetades selle võrrandisse, saame

$$q^{n+2} = b_1 q^{n+1} + b_2 q^n,$$

ehk tuues kõik liikmed vasakule ja võttes ühise kordaja sulgude ette,

$$q^n (q^2 - b_1 q - b_2) = 0.$$

Näeme, et jada  $A_n = q^n$  sobib rekurrentse võrrandi lahendiks sel juhul, kui arv  $q$  rahuldab *karakteristlikku võrrandit*

$$q^2 - b_1 q - b_2 = 0.$$

Siin võib esineda kaks juhtu: kas karakteristlikul võrrandil on kaks erinevat lahendit (mis võivad olla ka kompleksed) või langevad lahendid kokku. Karakteristliku võrrandi ükski lahend ei saa olla null, sest lahendite korrutis peab võrduma vabaliikmega, aga  $-b_2 \neq 0$ .

Olgu karakteristlikul võrrandil kaks erinevat lahendit  $q_1$  ja  $q_2$ . Näitame, et siis avaldub rekurrentse võrrandi iga lahend kujul

$$A_n = c_1 q_1^n + c_2 q_2^n,$$

kui valida sobivalt kordajad  $c_1$  ja  $c_2$ . Seda avaldist nimetatakse rekurrentse võrrandi *üldlahendiks*, selles kordajate  $c_1$  ja  $c_2$  fikseerimisel saadud avaldist aga *erilahendiks*.

Tõepoolest, esitatud üldlahend rahuldab rekurrentset võrrandit. Kõigepealt rahuldavad seda võrrandit jadad  $A_n = q_1^n$  ja  $A_n = q_2^n$ , sest arvud  $q_1$  ja  $q_2$  on karakteristliku võrrandi lahendid, mistõttu

$$q_1^{n+2} = b_1 q_1^{n+1} + b_2 q_1^n$$

$$q_2^{n+2} = b_1 q_2^{n+1} + b_2 q_2^n.$$

Korrutame esimest võrdust arvuga  $c_1$ , teist arvuga  $c_2$  ning liidame tulemused. Saame

$$(c_1 q_1^{n+2} + c_2 q_2^{n+2}) = b_1 (c_1 q_1^{n+1} + c_2 q_2^{n+1}) + b_2 (c_1 q_1^n + c_2 q_2^n).$$

Järelikult on ka jada üldliikmega  $A_n = c_1 q_1^n + c_2 q_2^n$  võrrandi lahend. Samuti võib üldlahendi avaldisest kordajatele  $c_1$  ja  $c_2$  sobivate väärtuste andmisega saada võrrandi ükskõik millise erilahendi: et võrrandi

iga erilahend on määratud algtingimustega  $A_0 = m_0$ ,  $A_1 = m_1$ , siis valides üldlahendi avaldises  $n = 0$  ja  $n = 1$ , peavad kordajad  $c_1$  ja  $c_2$  rahuldama võrrandisüsteemi

$$\begin{aligned}c_1 + c_2 &= m_0 \\c_1q_1 + c_2q_2 &= m_1.\end{aligned}$$

See süsteem on aga üheselt lahenduv, sest tema determinant  $q_2 - q_1$  erineb eelduse järgi nullist.

Kui karakteristikliku võrrandi lahendid  $q_1$  ja  $q_2$  langevad kokku, siis rekurrentse võrrandi üldlahend on

$$A_n = c_1q_1^n + c_2nq_1^n.$$

Tõepoolest, rekurrentset võrrandit rahuldavad jaded  $A_n = q_1^n$  ja  $A_n = nq_1^n$ , sest arv  $q_1$  on karakteristikliku võrrandi lahend, mistõttu

$$\begin{aligned}q_1^{n+2} &= b_1q_1^{n+1} + b_2q_1^n \\(n+2)q_1^{n+2} &= b_1(n+1)q_1^{n+1} + b_2nq_1^n.\end{aligned}$$

Teise võrduse puhul arvestame, et Viète'i valemitel põhjal  $q_1 + q_2 = b_1$ , mis  $q_1 = q_2$  tõttu omandab kuju  $2q_1 = b_1$ . Korrutame esimest võrdust arvuga  $c_1$ , teist arvuga  $c_2$  ning liidame tulemused. Täpselt samuti nagu eelmisel juhul saame siit, et jada üldliikmega  $A_n = c_1q_1^n + c_2nq_1^n$  on rekurrentse võrrandi lahend. Samuti võib üldlahendi avaldisest kordajatele  $c_1$  ja  $c_2$  sobivate väärtuste andmisega saada võrrandi ükskõik millise lahendi: juhul  $n = 0$  ja  $n = 1$  saame kordajate väärtuste määramiseks võrrandisüsteemi

$$\begin{aligned}c_1 &= m_0 \\c_1q_1 + c_2q_1 &= m_1.\end{aligned}$$

See süsteem on lahenduv, sest tema determinant  $q_1$  ei võrdu nulliga.

Saadud tulemused võtame kokku teoreemiks.

**Teoreem 1.** a) Kui rekurrentse võrrandi  $A_{n+2} = b_1A_{n+1} + b_2A_n$  karakteristiklikul võrrandil  $q^2 - b_1q - b_2 = 0$  on kaks erinevat lahendit  $q_1$  ja  $q_2$ , siis rekurrentse võrrandi üldlahend on

$$A_n = c_1q_1^n + c_2q_2^n,$$

kus  $c_1$  ja  $c_2$  on suvalised konstandid. Erilahendi, mis rahuldab algtingimusi  $A_0 = m_0$ ,  $A_1 = m_1$  saame siis, kui leiame kordajate  $c_1$  ja  $c_2$  väärtused võrrandisüsteemist  $c_1 + c_2 = m_0$ ,  $c_1q_1 + c_2q_2 = m_1$ .

b) Kui karakteristiklikul võrrandil on üks kahekordne lahend  $q_1$ , siis rekurrentse võrrandi üldlahend on

$$A_n = c_1q_1^n + c_2nq_1^n,$$

kus  $c_1$  ja  $c_2$  on suvalised konstandid. Erilahendi, mis rahuldab algtingimusi  $A_0 = m_0$ ,  $A_1 = m_1$  saame siis, kui leiame kordajate  $c_1$  ja  $c_2$  väärtused võrrandisüsteemist  $c_1 = m_0$ ,  $c_1q_1 + c_2q_1 = m_1$ .

Läbiviidud analüüsi põhjal saame rekurrentse võrrandi lahendamiseks järgmise meetodi. Moodustame karakteristliku võrrandi, leiame selle lahendid ning kirjutame välja üldlahendi avaldise. Kordajate määramiseks koostame algtingimusi kasutades võrrandisüsteemi ja lahendame selle. Lõpptulemuseks saame jada, mis rahuldab nii rekurrentset võrrandit kui ka algtingimusi.

*Näide 7.* Lahendada rekurrentne võrrand  $A_{n+2} = 5A_{n+1} - 6A_n$  algtingimustel  $A_0 = 1$  ja  $A_1 = 4$ .

Karakteristlik võrrand on

$$q^2 - 5q + 6 = 0,$$

mille lahenditeks saame  $q_1 = 3$  ja  $q_2 = 2$ . Et need lahendid on erinevad, siis avaldub rekurrentse võrrandi üldlahend kujul

$$A_n = c_1 3^n + c_2 2^n.$$

Kordajate  $c_1$  ja  $c_2$  määramiseks kasutame algtingimusi. Võttes  $n = 0$  ja  $n = 1$ , saame võrrandisüsteemi

$$c_1 + c_2 = 1$$

$$3c_1 + 2c_2 = 4,$$

mille lahendiks on  $c_1 = 2$ ,  $c_2 = -1$ . Rekurrentse võrrandi erilahend, mis rahuldab ka algtingimusi, on

$$A_n = 2 \cdot 3^n - 2^n.$$

*Näide 8.* Leida arvutusvalem Fibonacci arvude jaoks.

Meil tuleb lahendada rekurrentne võrrand  $A_{n+2} = A_{n+1} + A_n$  algtingimustel  $A_0 = 0$ ,  $A_1 = 1$ . Karakteristliku võrrandi  $q^2 - q - 1 = 0$  lahendid on  $q_1 = (1 + \sqrt{5})/2$  ja  $q_2 = (1 - \sqrt{5})/2$ . Rekurrentse võrrandi üldlahend on seega

$$A_n = c_1 \left( \frac{1 + \sqrt{5}}{2} \right)^n + c_2 \left( \frac{1 - \sqrt{5}}{2} \right)^n.$$

Määrame kordajad  $c_1$  ja  $c_2$ . Juhtudel  $n = 0$  ja  $n = 1$  peavad kehtima tingimused

$$c_1 + c_2 = 0 \quad \text{ja} \quad \left( \frac{1 + \sqrt{5}}{2} \right) c_1 + \left( \frac{1 - \sqrt{5}}{2} \right) c_2 = 1,$$

millest  $c_1 = 1/\sqrt{5}$  ja  $c_2 = -1/\sqrt{5}$ . Fibonacci arvude üldavaldis tuleb järelikult kujul

$$F_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n.$$

Seda võrdust nimetatakse *Binet' valemiks*. Irratsionaalsustele vaatamata on parema poole väärtus iga  $n$  korral täisarv.

Võib tähele panna, et avaldise teises liikmes on astendatava absoluutväärtus väiksem kui 1, st  $\left| \frac{1 - \sqrt{5}}{2} \right| < 1$ , mistõttu  $n$  kasvades läheneb see liige nullile. Seega piisavalt suure  $n$  korral võib Fibonacci arve leida ligikaudsest valemist

$$F_n \approx \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n.$$

Kui ümardada siit saadud väärtus lähimaks täisarvuks, siis langeb tulemus Fibonacci arvu tegeliku väärtusega ühte iga  $n$  korral.

*Näide 9.* Lahendada rekurrentne võrrand  $A_{n+2} = 4A_{n+1} - 4A_n$  algtingimustel  $A_0 = 3$ ,  $A_1 = 2$ .

Karakteristliku võrrandi  $q^2 - 4q + 4 = 0$  ainuke lahend on  $q = 2$ . Järelikult tuleb rekurrentse võrrandi üldlahend kujul

$$A_n = c_1 2^n + c_2 n 2^n.$$

Kordajad  $c_1$  ja  $c_2$  saame määrata tingimustest  $c_1 = 3$  ja  $2c_1 + 2c_2 = 2$ , kust  $c_2 = -2$ . Rekurrentse võrrandi erilahend on

$$A_n = 3 \cdot 2^n - 2n 2^n = (3 - 2n) 2^n.$$

*Näide 10.* Lahendada rekurrentne võrrand  $A_{n+2} = 2A_{n+1} - 2A_n$  algtingimustel  $A_0 = 1$ ,  $A_1 = -1$ .

Karakteristliku võrrandi  $q^2 - 2q + 2 = 0$  lahendid on  $q_1 = 1 + i$  ja  $q_2 = 1 - i$  ning võrrandi üldlahend

$$A_n = c_1 (1 + i)^n + c_2 (1 - i)^n.$$

Kordajate väärtuste määramiseks valime  $n = 0$  ja  $n = 1$  ning koostame võrrandisüsteemi  $c_1 + c_2 = 1$ ,  $(1 + i)c_1 + (1 - i)c_2 = -1$ , mida lahendades saame  $c_1 = 1/2 + i$ ,  $c_2 = 1/2 - i$ . Rekurrentse võrrandi erilahend on seega

$$A_n = \left( \frac{1}{2} + i \right) (1 + i)^n + \left( \frac{1}{2} - i \right) (1 - i)^n.$$

Saadud valem annab iga  $n$  korral täisarvu, vaatamata sellele, et arvutusi tehakse kompleksarvudega. Üldiselt pole teada, kas seda tüüpi juhtudel saab valemi avaldada ka kujul, mis kompleksarve ei sisalda.

Kõrgemat kui teist järku lineaarseid rekurrentseid võrrandeid saab lahendada sama skeemi järgi. Koostame karakteristliku võrrandi ning leiame selle lahendid. Olgu karakteristliku võrrandi lahenditeks  $q_1, q_2, \dots, q_s$  vastavalt kordsustega  $k_1, k_2, \dots, k_s$ , kusjuures loomulikult kõigi kordsuste summa võrdub võrrandi järguga:  $k_1 + k_2 + \dots + k_s = k$ .



Siis avaldub rekurrentse võrrandi üldlahend kujul

$$A_n = (c_{1,0} + c_{1,1}n + \dots + c_{1,k_1-1}n^{k_1-1})q_1^n + \\ + (c_{2,0} + c_{2,1}n + \dots + c_{2,k_2-1}n^{k_2-1})q_2^n + \dots \\ \dots + (c_{s,0} + c_{s,1}n + \dots + c_{s,k_s-1}n^{k_s-1})q_s^n.$$

Kordajate väärtused määratakse algtingimuste abil: juhtudel  $n = 0$ ,  $n = 1, \dots, n = k - 1$  peab valem andma väärtused  $m_0, m_1, \dots, m_{k-1}$ .

*Näide 11.* Lahendada viiendat järku lineaarne rekurrentne võrrand  $A_{n+5} = A_{n+4} + 5A_{n+3} - A_{n+2} - 8A_{n+1} - 4A_n$  algtingimustel  $A_0 = 5$ ,  $A_1 = 2$ ,  $A_2 = 8$ ,  $A_3 = -8$ ,  $A_4 = -2$ .

Koostame karakteristliku võrrandi

$$q^5 - q^4 - 5q^3 + q^2 + 8q + 4 = 0$$

ja teisendame ta kujule

$$(q + 1)^3(q - 2)^2 = 0.$$

Siit näeme, et võrrandil on kolmekordne lahend  $q_1 = -1$  ja kahekordne lahend  $q_2 = 2$ . Rekurrentse võrrandi üldlahend on järelikult

$$A_n = (c_1 + c_2n + c_3n^2)(-1)^n + (c_4 + c_5n)2^n.$$

Tundmatute kordajate  $c_1$  kuni  $c_5$  väärtused määrame algtingimuste abil. Valides üldlahendis  $n = 0, 1, 2, 3, 4$ , saame võrrandisüsteemi

$$\begin{aligned} c_1 &+ c_4 &= 5 \\ -c_1 - c_2 - c_3 + 2c_4 + 2c_5 &= 2 \\ c_1 + 2c_2 + 4c_3 + 4c_4 + 8c_5 &= 8 \\ -c_1 - 3c_2 - 9c_3 + 8c_4 + 24c_5 &= -8 \\ c_1 + 4c_2 + 16c_3 + 16c_4 + 64c_5 &= -2 \end{aligned}$$

Lahendades selle (näiteks Gaussi meetodiga), leiame  $c_1 = 2$ ,  $c_2 = -1$ ,  $c_3 = 1$ ,  $c_4 = 3$ ,  $c_5 = -1$ . Niisiis, rekurrentse võrrandi erilahend on

$$A_n = (2 - n + n^2)(-1)^n + (3 - n)2^n.$$

**4. Lineaarne mittehomoogeenne rekurrentne võrrand.** Üsna tihti esineb praktikas ka selliseid lineaarseid rekurrentseid võrrandeid, kus otsitava jada järjekordne liige sõltub lisaks eelmistele liikmetele veel ka liikme indeksist. Sellise *lineaarse mittehomoogeenne rekurrentse võrrandi* üldkujul on

$$A_{n+k} = b_1A_{n+k-1} + b_2A_{n+k-2} + \dots + b_kA_n + f(n),$$

kus  $f$  on teatav funktsioon. Eelnevas vaadeldud võrrandit, mille puhul  $f(n) = 0$ , nimetatakse tarbe korral ka *homoogenseks*.

Lineaarse mittehomoogeenne rekurrentse võrrandi lahendamine põhineb järgmisel võttel. Moodustame mittehomoogeennele võrrandile

vastava homogeense võrrandi, jättes võrrandist ära liikme  $f(n)$ , ja leiame selle üldlahendi  $A_n^{(c)}$ . Seejärel leiame ühe, ükskõik millise lahendi  $A_n^{(p)}$ , mis rahuldab mittehomoogeenset võrrandit. Antud mittehomoogeense võrrandi üldlahend on siis

$$A_n = A_n^{(c)} + A_n^{(p)}.$$

Tõepoolest, see avaldis rahuldab võrrandit, nagu nähtub samasuste

$$A_{n+k}^{(c)} = b_1 A_{n+k-1}^{(c)} + b_2 A_{n+k-2}^{(c)} + \dots + b_k A_n^{(c)}$$

ja

$$A_{n+k}^{(p)} = b_1 A_{n+k-1}^{(p)} + b_2 A_{n+k-2}^{(p)} + \dots + b_k A_n^{(p)} + f(n)$$

liitmisel. Samuti on võimalik liikme  $A_n^{(c)}$  avaldises esinevate kordajate  $c_1, c_2, \dots, c_k$  väärtuste fikseerimise teel saada kätte võrrandi kõik lahendid, sest algtingimuste järgi välja kirjutatud võrrandisüsteem erineb homogeense võrrandi juhul saadavast süsteemist ainult vabaliikmete poolest.

Seega taandub mittehomoogeense võrrandi lahendamine ühe erilahendi leidmisele. Üldisi reegleid, kuidas erilahendit leida, ei ole, ent mitmel juhul võib selles kasutada määramata kordajate meetodit. Sageli on funktsioon  $f$  polünoom, sellisel juhul võib ka erilahendit otsida polünoomi kujul. Kui  $f$  on polünoomi ja eksponentfunktsiooni korrutis, siis leidub võrrandil ka erilahend samasugusel kujul.

*Näide 12.* Lahendada lineaarne mittehomoogeenne rekurrentne võrrand  $A_{n+2} = 5A_{n+1} - 6A_n + 4n$  algtingimustel  $A_0 = 1, A_1 = 2$ .

Homogeense võrrandi

$$A_{n+2} = 5A_{n+1} - 6A_n$$

üldlahend on näite 7 põhjal

$$A_n = c_1 3^n + c_2 2^n.$$

Ülesandes antud mittehomoogeense võrrandi lahendit otsime kujul  $A_n = an + b$ . Asetades selle võrrandisse, saame

$$a(n+2) + b = 5a(n+1) + 5b - 6an - 6b + 4n,$$

ehk

$$(2a - 4)n - 3a + 2b = 0.$$

Et  $A_n$  on võrrandi lahend, peab viimane võrdus kehtima iga  $n$  korral. See on võimalik ainult juhul, kui  $2a - 4 = 0$  ja  $-3a + 2b = 0$ , kust  $a = 2$  ja  $b = 3$ . Mittehomoogeense võrrandi erilahendiks sobib järelikult jada üldliikmega  $A_n = 2n + 3$  ning võrrandi üldlahend avaldub kujul

$$A_n = c_1 3^n + c_2 2^n + 2n + 3.$$

Kordajate  $c_1$  ja  $c_2$  määramiseks kasutame algtingimusi. Valides  $n = 0$  ja  $n = 1$ , koostame võrrandisüsteemi

$$\begin{aligned}c_1 + c_2 + 3 &= 1 \\3c_1 + 2c_2 + 5 &= 2\end{aligned}$$

millest leiame  $c_1 = 1$ ,  $c_2 = -3$ . Võrrandi lahend on

$$A_n = 3^n - 3 \cdot 2^n + 2n + 3.$$

*Näide 13.* Leida võrrandi  $A_{n+2} = 3A_{n+1} + 4A_n + (3n + 1)2^n$  üldlahend.

Vastava homogeense võrrandi  $A_{n+2} = 3A_{n+1} + 4A_n$  karakteristiklik võrrand on  $q^2 - 3q - 4 = 0$ , selle lahenditeks leiame  $q_1 = 4$ ,  $q_2 = -1$ . Homogeense võrrandi üldlahend on niisiis

$$A_n = c_1 4^n + c_2 (-1)^n.$$

Mittehomogeense võrrandi erilahendit otsime kujul  $A_n = (an + b)2^n$ . Kui see avaldis võrrandisse asetada, tekib seos

$$(an + 2a + b)2^{n+2} = 3(an + a + b)2^{n+1} + 4(an + b)2^n + (3n + 1)2^n$$

ehk pärast liikmete kokkuvõtmist ja teguri  $2^n$  sulgude taha viimist

$$((-6a - 3)n + 2a - 6b - 1)2^n = 0.$$

See võrdus peab kehtima iga  $n$  korral, seega saame  $-6a - 3 = 0$ ,  $2a - 6b - 1 = 0$ , millest  $a = -1/2$  ja  $b = -1/3$ . Mittehomogeense võrrandi üldlahend on

$$A_n = c_1 4^n + c_2 (-1)^n - \left(\frac{n}{2} + \frac{1}{3}\right)2^n.$$

*Näide 14.* Lahendada näite 4 võrrand  $A_n = 2A_{n-1} + 4^{n-1}$  algtingimusel  $A_1 = 1$ .

Homogeense võrrandi karakteristiklik võrrand on  $q = 2$  ning üldlahend  $A_n = c \cdot 2^n$ . Mittehomogeense võrrandi üldlahendit otsime kujul  $A_n = a \cdot 4^n$ . Asetades selle võrrandisse, saame  $a \cdot 4^n = 2a \cdot 4^{n-1} + 4^{n-1}$  ehk  $4a = 2a + 1$ , kust  $a = 1/2$ . Mittehomogeense võrrandi erilahend on järelikult  $A_n = \frac{1}{2} \cdot 4^n$  ning üldlahend  $A_n = c \cdot 2^n + \frac{1}{2} \cdot 4^n$ . Kordaja  $c$  määrame algtingimusest. Võttes üldlahendi avaldises  $n = 1$ , saame võrrandi  $2c + 2 = 1$ , millest  $c = -1/2$ . Mittehomogeense võrrandi erilahend on seega

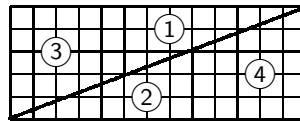
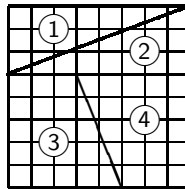
$$A_n = -\frac{1}{2} \cdot 2^n + \frac{1}{2} \cdot 4^n,$$

nagu ka näites 4 nimetatud.

## Ülesanded

Tõestada võrdused Fibonacci arvude vahel.

1.  $F_1 + F_3 + \dots + F_{2n-1} = F_{2n}$
2.  $F_0 - F_1 + F_2 - \dots - F_{2n-1} + F_{2n} = F_{2n-1} - 1$
3.  $F_0F_1 + F_1F_2 + \dots + F_{2n-1}F_{2n} = F_{2n}^2$
4.  $F_0^2 + F_1^2 + F_2^2 + \dots + F_n^2 = F_nF_{n+1}$
5.  $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$
10.  $\sum_{i=0}^n \binom{n}{i} F_i = F_{2n}$
6.  $F_{m+n} = F_mF_{n+1} + F_{m-1}F_n$
7.  $F_{2n} = F_{n+1}^2 - F_{n-1}^2$
11.  $\sum_{i=0}^n \binom{n}{i} 2^i F_i = F_{3n}$
8.  $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$
9.  $\sum_{i=0}^n iF_i = nF_{n+2} - F_{n+3} + 2$
12.  $\sum_{i=0}^n (-1)^i \binom{n}{i} F_{2n-i} = 0$
13. Tõestada *Catalani võrdus*  $F_n^2 - F_{n+r}F_{n-r} = (-1)^{n-r}F_r^2$ , kus  $r$  on naturaalarv. Juhul  $r = 1$  saame siit võrduse ülesandest 5.
14. Tõestada *d'Ocagne'i võrdus*  $F_mF_{n+1} - F_nF_{m+1} = (-1)^nF_{m-n}$ , kui  $m \geq n$ .
15. Tõestada võrdus  $F_aF_b - F_cF_d = (-1)^r(F_{a-r}F_{b-r} - F_{c-r}F_{d-r})$ , kui  $a + b = c + d$  ja  $r$  pole suurem ühestki arvust  $a, b, c$  ja  $d$ . Selle võrduse erijuhud on nii *Catalani võrdus* kui ka *d'Ocagne'i võrdus*.
16. Tõestada, et kui jada  $(G_n)$  rahuldab seost  $G_{n+1} = G_n + G_{n-1}$ , siis tema puhul kehtivad võrdused  $G_{n+m} = F_mG_{n+1} + F_{m-1}G_n$  ning  $G_{n-m} = (-1)^m(F_{m+1}G_n - F_mG_{n+1})$ .
17. Maagiline geomeetria on valdkond, milles püütakse mitmesuguste kujundite tükkideks lõikamise ja seejärel tükide kokkupanemise teel näidata, et mateeria jäävuse seadus on ilmselt väär. Kõrvalolev joonis näitab tõestab, et  $64 = 65$ . Milles on viga? Millisel eespool toodud võrdusel „maagia“ põhineb? Pannes tähele, et kujundite küljepikkused on Fibonacci arvud, leida viis niisuguse konstruktsiooni üldistamiseks.



18. Tõestada, et  $F_{5n}$  jagub 5-ga.
19. Tõestada, et kui  $m$  jagub  $n$ -ga, siis  $F_m$  jagub  $F_n$ -ga.
20. Lucas' arvudeks nimetatakse jada  $(L_n)$ , kus  $L_0 = 2$ ,  $L_1 = 1$  ja iga naturaalarvu  $n$  korral  $L_{n+1} = L_n + L_{n-1}$ . Tõestada, et  $L_n = F_{n+1} + F_{n-1}$ .
21. Tõestada, et Lucas' arvude ja Fibonacci arvude vahel kehtib seos  $F_m L_n = F_{m+n} + (-1)^n F_{m-n}$ . Võttes siin  $m = n$ , saame võrduse  $F_{2n} = F_n L_n$ .
22. Tõesta, et ainukesed naturaalarvud, mis kuuluvad nii Fibonacci kui Lucas' arvude jadasse, on 1, 2 ja 3.
23. Leida arvutusvalem Lucas' arvude jaoks.
24. Arvujada  $(a_n)$  defineeritakse järgmiselt:  $a_0 = -1$  ning iga  $n \geq 0$  korral  $a_{n+1} = (a_0 - 2)(a_1 - 2) \dots (a_n - 2) - 2$ . Tõestada, et see jada rahuldab rekurrentset seost

$$a_{n+1} = a_n^2 - 6.$$

25. Arvujada  $(a_n)$  defineeritakse järgmiselt:  $a_0 = \sqrt{2}$  ning iga  $n \geq 0$  korral  $a_{n+1} = \sqrt{2 + a_n}$ . a) Tõestada, et jada  $(a_n)$  on rangelt kasvav, st  $a_n < a_{n+1}$  iga  $n \geq 0$  korral. b) Tõestada, et jada  $(a_n)$  on ülalt tõkestatud, st leidub selline arv  $M$ , et  $a_n < M$  iga  $n \geq 0$  korral. c) Kahest eelmisest punktist järeldub, et on olemas piirväärtus  $\lim_{n \rightarrow \infty} a_n$ . Leida see piirväärtus.

Lahendada rekurrentsed võrrandid.

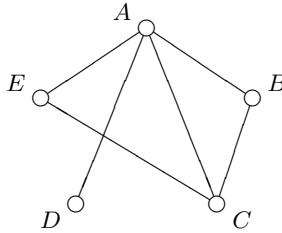
26.  $A_{n+2} = A_{n+1} + 2A_n$ , algtingimused  $A_0 = 2$ ,  $A_1 = 1$
27.  $A_{n+2} = 7A_{n+1} - 12A_n$ , algtingimused  $A_0 = 7$ ,  $A_1 = 25$
28.  $A_{n+2} = 4A_{n+1} - 4A_n$ , algtingimused  $A_0 = 1$ ,  $A_1 = 4$
29.  $A_{n+3} = 2A_{n+2} + A_{n+1} - 2A_n$ , algtingimused  $A_0 = 1$ ,  $A_1 = 2$ ,  $A_2 = 5$
30.  $A_{n+3} = 7A_{n+1} + 6A_n$ , algtingimused  $A_0 = 2$ ,  $A_1 = 3$ ,  $A_2 = 7$
31.  $A_{n+1} = 3A_n + 2n$ , algtingimus  $A_0 = 0$
32.  $A_{n+2} = -4A_{n+1} - 3A_n + 5(-2)^n$ , algtingimused  $A_0 = -2$ ,  $A_1 = 3$
33.  $A_{n+2} = 6A_{n+1} - 9A_n - 3^n$ , algtingimused  $A_0 = 1$ ,  $A_1 = 3$
34.  $A_{n+2} = 6A_{n+1} + 7A_n + 8((-1)^n + 7^n)$ , algtingimused  $A_0 = 5$ ,  $A_1 = 11$
35. Lahendada rekurrentne võrrand  $A_{n+2} = \sqrt{\frac{A_n}{A_{n+1}}}$  algtingimustel  $A_0 = 8$ ,  $A_1 = 1/\sqrt{8}$ .

36. Arvujada  $(a_n)$  defineeritakse järgmiselt:  $a_0 = 1$  ning iga  $n \geq 0$  korral  $a_{n+1} = a_0 + a_1 + \dots + a_n + n3^n$ . Leida  $a_n$  avaldis.
37. Mitmel viisil saab doominokividega katta laua mõõtmetega  $2 \times n$ ?
38. Mitmel erineval viisil saab üles minna  $n$ -astmelisest trepist, kui iga sammuga võib võtta ühe või kaks astet?
39. Ümmarguse laua ääres istub  $n$  inimest. Mitmel viisil saab nende hulgast valida rühma nii, et sinna ei kuulu kahte kõrvuti istuvat inimest?
40. Hamster kogub koopasse talvevarusid, mida ta kõigest hoolimata kunagi ei puutu. Igal aastal hangib ta juurde kaks korda nii palju seemneid, kui palju tal oli eelmisel aastal, ning viskab ära üle-eelmisest aastast pärinevad seemned, mis on läinud hallitama. Esimesel aastal õnnestus tal koguda üksainus seeme, varem oli ta sunnitud ilma läbi ajama. Mitmest seemnest koosneb hamstri talvevaru kümnendal aastal?
41. Talikuurordi omanik tegi kokkuvõtet lõppenud hooajast. Selgus huvipakkuv seos: kui käesoleva aasta külastajate arvu kahekordsest lahutada eelmise aasta külastajate arv, on tulemus sama kui üle-eelmise aasta külastajate arvu kahekordsest lahutada tollele aastale eelneva aasta külastajate arv. Eeldades, et see seos kehtib kõigil aastatel, leida, mitu inimest külastab kuurorti  $n$ -ndal aastal, kui esimesel aastal pärast avamist viibis seal 1000 inimest.
42. Watu riigi autonumbrites tohib kasutada ainult tähti W, A, T ja U. Seejuures peavad kõik tähed W esinema enne kõiki tähti A. Näiteks WATA on lubatud numbrimärk, kuid WATW ei ole. Watu riigis on ühtekokku miljon autot. Vähemalt kui palju tähti peab autonumber sisaldama, et neile kõigile numbreid jätkuks?
43. Olümpiasüsteemis läbiviidaval tenniseturniiril osaleb  $2^n$  mängijat. Igas ringis jagatakse mängijad paaridesse ning paaride võitjad pääsevad järgmisse ringi. Turniir lõpeb siis, kui on selgunud üks võitja. Arvestades, et hilisemates ringides kohtuvad omavahel paremad ja ühtlasi võimetelt võrdsemad tennisistid, on kehtestatud järgmised reeglid. Iga esimese ringi kohtumine kestab ühe seti, võitja läheb edasi teise ringi. Iga teise ringi kohtumine kestab ülimalt 3 setti, võitja on see, kes võidab neist vähemalt kaks (parem kolmest). Iga kolmanda ringi kohtumine kestab ülimalt 5 setti, võitja on see, kes võidab neist vähemalt kolm (parem viiest). Üldiselt, iga  $k$ -nda ringi kohtumine mängitakse stiilis parem  $2k - 1$  setist. Leida maksimaalne settide arv, mida sellise turniiri käigus mängitakse.

## V. GRAAFID

**1. Graafi mõiste.** Nii nagu joonised, skeemid ja diagrammid aitavad piltlikustada mitmesuguseid seoseid ja omandada käsilolevast situatsioonist paremat ülevaadet, nii on osutunud ka matemaatikas otstarbekaks kasutada objektide vaheliste sõltuvuste kirjeldamiseks graafilisi kujutisi. Süstemaatiliseks teooriaks arendatuna aitab selline lähenemine mõnelgi juhul muuta arutlusi näitlikumaks ja lihtsamaks ning tõsta uuritavaid seaduspärasusi paremini esile.

Vaatleme järgmist olukorda. Koosviibimisest võtab osa viis inimest  $A, B, C, D$  ja  $E$ . Neist  $A$  on tuttav kõigi kohalviibijatega, lisaks on omavahel tuttavad veel  $B$  ja  $C$  ning  $C$  ja  $E$ . Eeldame, et kõik tutvused on vastastikused: kui üks inimene tunneb teist, siis ka teine tunneb esimest. Niisugust olukorda võib kirjeldada pildiga, kus inimesi tähistavad punktid ja vastastikust tutvuseost jooned punktide vahel:



Sellist pilti nimetatakse *graafiks*. Graaf koosneb *tippudest* ja neid ühendavatest *servadest*. Pole tähtis, millise kujuga serv joonisel on, oluliseks osutub ainult see, milliseid tippe ta omavahel seob.

Graafi täpne definitsioon on järgmine.

**Definitsioon 1.** *Graaf on paar  $G = (V, E)$ , kus  $V$  on mittetühi hulk ning  $E$  hulk, mille elementideks on hulga  $V$  kaheelemendilised alamhulgad.*

Hulga  $V$  elemente nimetatakse graafi *tippudeks*, hulga  $E$  elemente aga *servadeks*. Ülaltoodud graafi puhul näiteks on

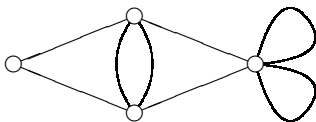
$$V = \{A, B, C, D, E\}$$

ja

$$E = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{C, E\}\}.$$

Et toodud definitsioonis loetakse servadeks ainult tippude hulga kaheelemendilisi alamhulki, siis ei tohi graafis esineda *silmuseid*, st servi mis ühendavad mingit tippu iseendaga, ega *kordseid servi*, olukordi, kus mingit kahte tippu ühendab rohkem kui üks serv. Siiski tuleb vahel ka neid arvestada, sellisel juhul räägitakse graafi asemel

*multigraafist.* Üks silmuste ja kordse servaga multigraaf on kujutatud järgmisel joonisel:

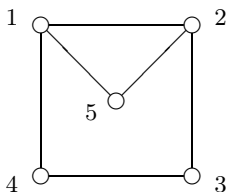


Rakenduslikes ülesannetes vaadeldakse sageli graafe, mille igale servale on vastavusse seatud üks reaalarv, *kaal*. Vastavat graafi nimetatakse siis *kaalutud graafiks*.

Graafidel on väga palju rakendusi, neid saab kasutada igal pool, kus on vaja kirjeldada, mis millega seotud on. Näiteks võivad tipud tähistada linnu ja servad linnadevahelisi teid, raudteid, elektriliine vms. Graafi tipud võivad olla elektriskeemi elemendid ning servad elemente ühendavad viigud, graafide abil saab esitada molekulides valitsevaid keemilisi sidemeid, ühendusi neuronite vahel, inimeste sugulusseoseid. Graafide abil saab kujutada ka abstraktsemaid objekte, näiteks võivad tipud olla mingi suure projekti etapid ning servad tööd, mis viivad ühest etapist teise. Samuti võivad tipud tähistada kõikvõimalikke seise mingis mängus (näiteks males), servad aga ühe-kaigulisi üleminekuid ühest seisust teise. Ükskõik, kui keeruline graaf on ja millist situatsiooni ta kirjeldab, ikka kehtivad selles kõik graafide üldised omadused, mis igal konkreetsel juhul võivad uuritava olukorra kohta anda väärtuslikku informatsiooni.

Kui graafi tipp  $v$  kuulub servale  $e$ , siis öeldakse, et tipp  $v$  ja serv  $e$  on *intsidentsed*. Iga serv on seega intsidentne täpselt kahe tipuga, serva *otstipuga*. Serva tippude  $u$  ja  $v$  vahel tähistatakse  $\{u, v\}$  asemel ka lühemalt tähisega  $uv$ . Graafi tippu  $u$  ja  $v$  nimetatakse *naabertippudeks*, kui nad on servaga ühendatud. Servi  $d$  ja  $e$  nimetatakse *naaberservadeks*, kui neil on ühine otstipp.

Olgu  $G = (V, E)$  graaf tippude hulgaga  $V = \{v_1, v_2, \dots, v_n\}$ . Graafi  $G$  *naabrusmaatriks* on  $n \times n$ -maatriks  $A = (a_{ij})$ , kus  $a_{ij} = 1$ , kui tippude  $v_i$  ja  $v_j$  vahel on graafis serv, ning  $a_{ij} = 0$ , kui nende tippude vahel serv puudub. Joonisel on esitatud üks nummerdatud tippudega graaf koos oma naabrusmaatriksiga:

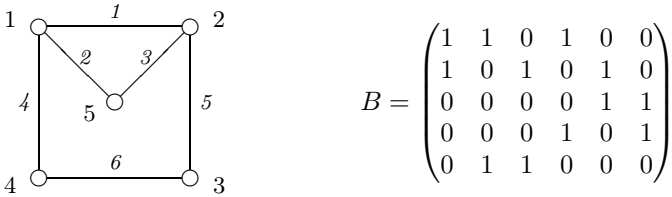


$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$



Naabusmaatriks on ilmselt sümmeetriline peadiagonaali suhtes, sest kui leidub serv tipust  $v_i$  tippu  $v_j$ , siis leidub ka serv tipust  $v_j$  tippu  $v_i$ . Samuti on naabusmaatriksi peadiagonaali elemendid alati võrdsed nulliga, sest graafis ei tohi olla silmuseid.

Mõnikord kasutatakse graafi esitamiseks ka *intsidentsusmaatriksit*. Kui  $G = (V, E)$  on graaf tippude hulgaga  $V = \{v_1, v_2, \dots, v_n\}$  ja servade hulgaga  $E = \{e_1, e_2, \dots, e_m\}$ , siis selle graafi intsidentsusmaatriks on  $n \times m$ -maatriks  $B = (b_{ij})$ , kus  $b_{ij} = 1$  parajasti siis, kui tipp  $v_i$  on intsidentne servaga  $e_j$ , see tähendab, on serva otstipp. Eelmisel joonisel kujutatud graafi intsidentsusmaatriksi leidmiseks numbridame lisaks tippudele ka graafi servad:



Intsidentsusmaatriksi igas veerus asub täpselt kaks ühte, need paiknevad ridades, mis vastavad serva otstippudele.

Kui  $n$ -tipulises graafis on olemas serv iga kahe tipupaari vahel, siis nimetatakse graafi *täisgraafiks* ja märgitakse tähisega  $K_n$ . Analooiliselt, kui  $n$ -tipulises graafis pole serva ühegi tipupaari vahel, siis sellist graafi nimetatakse *nullgraafiks* ja tähistatakse sümboliga  $O_n$ . Joonisel vasakul on kujutatud graaf  $K_5$  ja paremal  $O_5$ :

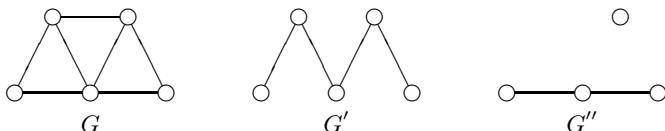


Graafi  $G$  *täiendgraafiks* ehk *täiendiks*  $\overline{G}$  nimetatakse graafi, millel on sama tippude hulk nagu graafil  $G$ , aga servaga on ühendatud parajasti need tipud, mille vahel graafis  $G$  serv puudub. Üks täiendgraafide paar on  $K_n$  ja  $O_n$ , kuid lihtne on ette kujutada ka selliseid paare, kus kummagi graafi servade hulk ei ole tühi. Graafidel  $G$  ja  $\overline{G}$  pole ühiseid servi ja kokku moodustavad nad täisgraafi. Graafi  $\overline{G}$  täiend on lähtegraaf  $G$ .

Sageli tuleb graafidega teha mitmesuguseid teisendusi. Levinumad neist on serva või tipu kustutamine ja lisamine. Graafist serva kustutamisel katkeb otseühendus kahe tipu vahel, serva lisamisel aga muutuvad kaks seni ühenduseta tippu seotuks. Tulemuseks saadud graafi

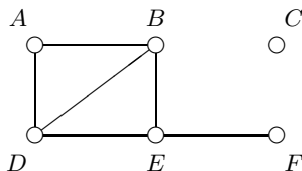
servade hulgas  $E'$  on algsega võrreldes seega vastavalt üks element vähem või rohkem. Tipu kustutamisel eemaldatakse graafist ühtlasi kõik selle tipuga intsidentsed servad, tipu lisamisel lisatakse graafile tavaliselt ka teatud hulk servi uue tipu ja vanade tippude vahele.

Graafi  $G' = (V', E')$ , mis on saadud graafist  $G = (V, E)$  teatava hulga tippude ja servade kustutamisel, nimetatakse graafi  $G$  *alamgraafiks*. Kui  $G'$  on graafi  $G$  alamgraaf, siis kehtivad sisalduvused  $V' \subseteq V$  ja  $E' \subseteq E$ . Üks graafi  $G$  alamgraafidest on loomulikult  $G$  ise. Kustutades graafist kõik servad, näeme, et iga  $n$ -tipulise graafi alamgraaf on ka nullgraaf  $O_n$ . Paar näidet on toodud veel järgmisel joonisel, kus  $G'$  ja  $G''$  on mõlemad graafi  $G$  alamgraafid.



**2. Tipu aste.** Graafe iseloomustavatest näitajatest üks tähtsaimaid on tipuga intsidentsete (tipust väljuvate) servade arv. Graafi tipuga  $v$  intsidentsete servade arvu nimetatakse tipu  $v$  *astmeks* ehk *valentsiks* ja tähistatakse sümboliga  $d(v)$ .

Tippu, mille aste on 0, nimetatakse *isoleeritud tipuks*, temast ei vii serva ühessegi teise tippu. Tippu astmega 1 nimetatakse *rippuvaks tipuks*. Maksimalne aste, mis mingi  $n$ -tipulise graafi tipul üldse olla saab, on  $n - 1$ , sellisest tipust peab siirduma serv graafi igasse teise tippu. Graafis



on  $d(A) = 2$ ,  $d(B) = d(D) = d(E) = 3$ ,  $d(C) = 0$  ja  $d(F) = 1$ . Tipp  $C$  on isoleeritud, tipp  $F$  on rippuv tipp.

**Teoreem 1.** *Igas graafis on kõigi tippude astmete summa võrdne servade arvu kahekordsega.*

**Tõestus.** Tippude astmete summa leidmisel loeme iga tipu juures kokku kõik servad. Seejuures võtame iga serva arvesse kaks korda: üks kord ühe, teine kord teise otstipu servade hulgas. Seega on tippude astmete summa parajasti kaks korda suurem kui servade arv.  $\square$

**Järeldus 1.** *Igas graafis on paaritu astmega tippe paarisarv.*

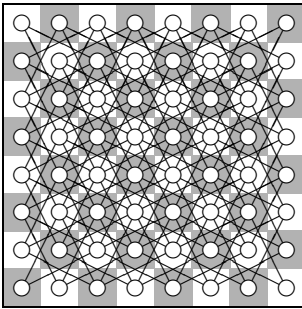
**Tõestus.** Selleks, et kõigi tippude astmete summa tuleks paarisarv, peab summas esinema paarisarv paaritult liidetavat.  $\square$

Näide 1. Kas on võimalik värvida 15-tipulise täisgraafi mõned servad roheliseks ja ülejäänud kollaseks nii, et igast tipust väljub rohelisi servi sama palju kui kollaseid?

Oletame, et servad saab niiviisi värvida. Siis oleks meil 15-tipuline graaf, mille igast tipust väljub 7 rohelist ja 7 kollast serva. Kustutame sellest graafist kõik kollased servad. Järele jääb 15-tipuline graaf, mille igast tipust väljub 7 rohelist serva. Kuid sellises graafis on paaritu arv paaritu astmega tippu, mis pole võimalik.

Näide 2. Mitmel viisil saab malelauale paigutada kaks valget ratsut nii, et nad teineteist kaitseksid?

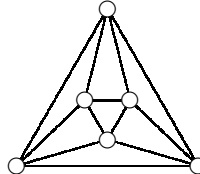
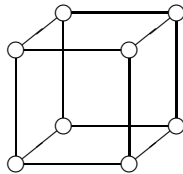
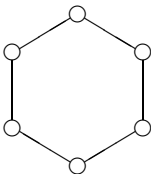
Vaatleme graafi, mille tippudeks on malelaua ruudud, ning servaga on ühendatud need ruudud, mis asuvad teineteisest ratsukäigu kaugusel (joonisel vasakul). Igale kahe ratsu paigutusvõimalusele vastab graafis üks serv, seega peame leidma selle graafi servade arvu.



2	3	4	4	4	4	3	2
3	4	6	6	6	6	4	3
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
3	4	6	6	6	6	4	3
2	3	4	4	4	4	3	2

Leiame kõigi tippude astmed (joonisel paremal). Liites need kokku, saame tulemuseks  $4 \cdot 2 + 8 \cdot 3 + 20 \cdot 4 + 16 \cdot 6 + 16 \cdot 8 = 336$  ehk graafil on  $336 : 2 = 168$  serva. Järelikult saab kahte ratsut nõutaval viisil malelauale paigutada 168 erineval viisil.

Graafi, mille kõigi tippude astmed on võrdsed, nimetatakse *regulaarseks*. Täpsemini, kui regulaarse graafi tippude ühine aste on  $r$ , siis nimetatakse graafi *regulaarseks astmega  $r$* . Näiteks kõik järgmised graafid on regulaarsed vastavalt astmega 2, 3 ja 4:



Regulaarsed on samuti täisgraaf  $K_n$  ja nullgraaf  $O_n$ , neist esimene astmega  $n - 1$  ja teine astmega 0. Kui graaf  $G$  on regulaarne, siis

ka tema täiendgraaf  $\overline{G}$  on regulaarne. Vastavalt teoreemile 1 sisaldab  $n$ -tipuline regulaarne graaf astmega  $r$  ühtekokku  $nr/2$  serva.

**3. Ahelad ja tsüklid.** Ahel graafis  $G$  on selline tippude järjend  $v_0, v_1, \dots, v_k$ , kus iga kaks järjestikust tippu on servaga ühendatud. Tippe  $v_0$  ja  $v_k$  nimetatakse ahela *otstippudeks*, ahela ülejäänud tipud  $v_1, \dots, v_{k-1}$  on *sisetipud*. Tippudest  $v_0, v_1, \dots, v_k$  koosnev ahelat (ehk ahelat tipust  $v_0$  tippu  $v_k$ ) märgime tähisega  $v_0v_1 \dots v_k$ . Seega ahel kulgeb ühest otstipust teise, läbides oma teel üksteise järel kõik sisetipud. Ahela servade arvu nimetatakse *ahela pikkuseks*, näiteks ahela  $v_0v_1 \dots v_k$  pikkus on  $k$ .

Täiesti lubatav on, et ahel külastab mõnda tippu mitu korda, pöördues selleks mingisse juba läbitud tippu tagasi. Kui aga kõik ahela tipud on erinevad, siis nimetatakse ahelat *lihtahelaks*. Nagu nähtub järgmisest teoreemist, võib ahela kahe tipu vahel alati asendada lihtahelaga, st kui on leitud ahel ühest tipust teise, siis võib alati eeldada, et ta ei sisalda korduvaid tippe.

**Teoreem 2.** Kui graafis  $G$  leidub ahel tipust  $u$  tippu  $v$ , siis leidub graafis  $G$  ka lihtahel tipust  $u$  tippu  $v$ .

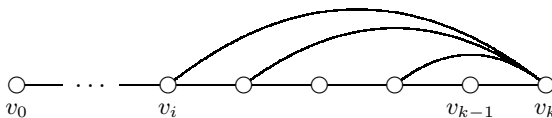
Tõestus. Olgu meil teada ahel tipust  $u$  tippu  $v$ . Kui see ahel läbib mingit tippu  $w$  kaks korda, siis on ahelal kuju  $u \dots w \dots w \dots v$ . Siis aga võime ringkäigu tipust  $w$  tippu  $w$  ahelast välja jätta: jõudes esimest korda tippu  $w$ , liigume edasi samamoodi nagu pärast teist korda samasse tippu jõudmist. Sellega saame lühema ahela tipust  $u$  tippu  $v$ . Niisugust lühendamist jätkame senikaua, kuni korduvaid tippe enam pole. Tulemuseks on lihtahel tippude  $u$  ja  $v$  vahel.  $\square$

Loomulikult võib kahe tipu vahel leiduda graafis ka rohkem kui üks lihtahel. Tippude  $u$  ja  $v$  vahelise lühima lihtahela pikkust nimetatakse tippude  $u$  ja  $v$  *kauguseks*.

Ahelat, mis lõpeb samas tipus, kus algab, nimetatakse *tsükliks*. Tsükli servade arv on *tsükli pikkus*. Tsüklit, mis ei läbi ühtegi tippu ega serva kaks korda, nimetatakse *lihttsükliks*.

**Teoreem 3.** Kui graafi iga tipu aste on vähemalt  $l \geq 2$ , siis leidub graafis lihtahel pikkusega  $l$  ja lihttsükkel pikkusega vähemalt  $l + 1$ .

Tõestus. Olgu  $v_0v_1 \dots v_k$  pikim lihtahel graafis  $G$ . Siis peavad tipu  $v_k$  kõik naabrid asuma selsamal ahelal (joonis), sest muidu saaksime lihtahelat  $v_0v_1 \dots v_k$  lõpust ühe serva võrra pikendada. Et tipu  $v_k$  aste on vähemalt  $l$ , siis leidub tipul  $v_k$  tippude  $v_0, \dots, v_{k-1}$  hulgas



$l$  naabrit. See on võimalik ainult siis, kui  $k \geq l$  ehk vaadeldava lihtahela pikkus on vähemalt  $l$ .

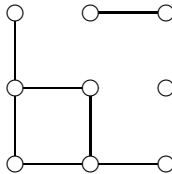
Olgu nüüd  $v_i$  tipu  $v_k$  naabrite seas see, mis asub tipule  $v_0$  kõige lähemal. Siis  $v_i \dots v_k v_i$  on lihtsükkel pikkusega vähemalt  $l + 1$ , sest ta sisaldab tippu  $v_k$  ja kõiki tipu  $v_k$  naabreid.  $\square$

**Järeldus 2.** Igas graafis, milles on servi vähemalt sama palju kui tippe, leidub tsükkel.

**Tõestus.** Vaatleme graafi  $G$ , kus on servi vähemalt sama palju kui tippe. Kustutame graafist kõik isoleeritud tipud ja kõik rippuvad tipud. Järele jääb graaf, millel on vähemalt kolm tippu, sest pärast iga isoleeritud või rippuva tipu kustutamist jääb servade arv ikka vähemalt sama suureks kui tippude arv, mistõttu graaf ei saa tippude arvult kahaneda väiksemaks kolmetipulisest ja kolmeservalisest graafist  $K_3$ . Nüüd on aga graafi iga tipu aste vähemalt 2 ning teoreemi põhjal leidub seal lihtsükkel pikkusega vähemalt 3.  $\square$

**4. Sidusus.** Graafi, milles iga kahe tipu korral leidub neid tippe ühendav ahel, nimetatakse *sidusaks*. Sidusas graafis saab igast tipust mööda servi liikuda igasse teise tippu. Näiteks täisgraaf  $K_n$  on sidus iga  $n$  korral, kuid vähemalt kahetipuline nullgraaf  $O_n$  ei ole. Ühtsuse mõttes loetakse ka, et ühetipuline graaf on samuti sidus.

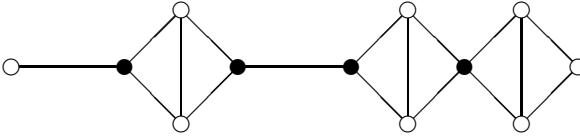
Kui graaf ei ole sidus, siis jaguneb ta eraldiseisvateks osadeks, millest igaüks omaette on sidus graaf. Neid osi nimetatakse *sidusateks komponentideks*. Iga sidusa komponendi piires võib pääseda ühest tipust teise, kuid erinevatesse komponentidesse kuuluvaid tippe ei ühenda ükski serv ega ahel. Joonisel on näidatud graaf, mis koosneb kolmest sidusast komponendist, suurusega 1, 2 ja 6 tippu:



Sidus graaf on parajasti see, millel on täpselt üks sidus komponent. Graafi sidusat komponenti võib iseloomustada ka kui sellist sidusat alamgraafi, mis ei sisaldu üheski teises sidusas alamgraafis – iga alamgraaf, mis teda sisaldab ja temast erineb, on mittesidus.

Kustutades sidusast graafist ühe serva, võib graaf kaotada sidususe ja laguneda kaheks sidusaks komponendiks. Üldiselt, graafi serva nimetatakse *sillaks*, kui tema eemaldamisel graafi sidusate komponentide arv kasvab. Samamoodi võib sidusate komponentide arv kasvada mõne tipu eemaldamisel (koos tipuga eemaldame loomulikult

ka kõik temaga intsidentsed servad), sellist tippu nimetatakse *eraldavaks tipuks*. Joonisel kujutatud graafil näiteks on kaks silda ning neli eraldavat tippu, viimased on värvitud mustaks:



Silla otstipp, kui ta juhtumisi pole rippuv tipp, on ühtlasi ka eraldav. Rippuva tipu eemaldamisel graafi sidusate komponentide arv ei muutu. Peale selle võib graafis esineda veel niisuguseid eraldavaid tippe, mis ei ole ühegi silla otstipuks.

**Tooreem 4.** *Graafi serv on sild parajasti siis, kui ta ei kuulu ühessegi tsükklisse.*

**Tõestus.** *Tarvilikkus.* Eeldame, et graafi serv  $uv$  on sild. Selle serva eemaldamisel jäävad tipud  $u$  ja  $v$  erinevatesse sidusatesse komponentidesse. Kui serv  $uv$  kuuluks mingisse tsükklisse, siis aga jääksid tipud  $u$  ja  $v$  pärast serva eemaldamist samasse sidusasse komponenti, sest tipust  $u$  saaks liikuda tippu  $v$  mööda tsükli allesjäänud osa.

*Püsavus.* Eeldame, et serv  $uv$  ei kuulu ühessegi tsükklisse. Siis peab iga ahel tipust  $u$  tippu  $v$  läbima seda serva, sest muidu moodustaks see ahel koos servaga  $uv$  tsükli. Järelikult, kui serv  $uv$  eemaldada, siis ühendus tippude  $u$  ja  $v$  vahel katkeb.  $\square$

Selgitame veel, kui palju servi peab graafil olema, et ta oleks sidus.

**Tooreem 5.** *Kui  $n$ -tipulisel graafil on  $m$  serva ja  $k$  sidusat komponenti, siis kehtivad võrratused*

$$n - k \leq m \leq \frac{(n - k)(n - k + 1)}{2}.$$

**Tõestus.** Vasakpoolse võrratuse tõestame induktsiooniga graafi servade arvu  $m$  järgi.

*Baas.* Kui  $m = 0$ , siis on meil tegemist  $n$ -tipulise nullgraafiga  $O_n$ . Sellel graafil on  $n$  sidusat komponenti ja tõestatav võrratus omandab kuju  $n - n \leq 0$ .

*Samm.* Eeldame nüüd, et võrratus kehtib kõigi graafide korral, millel on  $m = s$  serva, ning vaatleme graafi, mille servade arv on  $m = s + 1$ . Kustutame graafist ühe serva. Kui serv oli sild, siis jaguneb üks sidus komponent kaheks ning tulemuseks saame graafi, millel on  $n$  tippu,  $s$  serva ja  $k + 1$  komponenti. Induktsiooni eelduse põhjal  $n - (k + 1) \leq s$ , millest  $n - k \leq s + 1$ . Kui kustutud serv polnud sild, siis jääb komponentide arv samaks ning saadaval graafil on  $n$  tippu,  $s$

serva ja  $k$  komponenti. Induktsiooni eelduse põhjal saame  $n - k \leq s$ , kust samuti järeldub vajalik võrratus  $n - k \leq s + 1$ .

Parempoolse võrratuse tõestamiseks uurime, mitu serva saab maksimaalselt olla  $k$  komponendiga  $n$ -tipulisel graafil. Ilmselt peavad kõik komponendid olema täisgraafid. Kui kustutame kõige väiksema tipu arvuga komponendist ühe tipu ja lisame kõige suurema tippude arvuga komponendile ühe tipu juurde, ühendades ta servade abil selle komponendi kõigi ülejäänud tippudega, siis graafi servade arv kindlasti ei kahane. Korrates seda operatsiooni niikaua kui võimalik, näeme, et suurim servade arv realiseerub siis, kui graafi  $k - 1$  komponenti on ühetipulised ja üks komponent  $(n - k + 1)$ -tipuline täisgraaf. Niisugusel graafil on parajasti  $(n - k)(n - k + 1)/2$  serva.  $\square$

**Järeldus 3.** *Kui  $n$ -tipulisel graafil on vähem kui  $n - 1$  serva, siis see graaf on mittesidus.*

**Tõestus.** Eeldusel  $m < n - 1$  saame teoreemist  $n - k < n - 1$  ehk  $k > 1$ . Järelikult on graafil rohkem kui üks sidus komponent.  $\square$

**Järeldus 4.** *Kui  $n$ -tipulisel graafil on rohkem kui  $(n - 1)(n - 2)/2$  serva, siis see graaf on sidus.*

**Tõestus.** Kui servade arv  $m$  rahuldab seost  $m > (n - 1)(n - 2)/2$ , siis saame teoreemi põhjal võrratuse

$$\frac{(n - 1)(n - 2)}{2} < \frac{(n - k)(n - k + 1)}{2},$$

mis pärast sulgude avamist ja liikmete koondamist omandab kuju

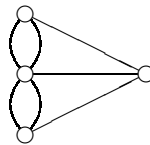
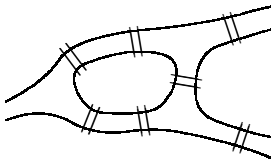
$$k^2 - (2n + 1)k + 4n - 2 > 0$$

ehk

$$(k - 2)(k - 2n + 1) > 0.$$

Ruutparabooli omaduste põhjal  $k < 2$  või  $k > 2n - 1$ . Teine võrratus ei sobi, sest sidusate komponentide arv ei saa ületada graafi tippude arvu, esimene aga ütleb, et graafi sidusate komponentide arv on 1.  $\square$

**5. Euleri ja Hamiltoni graafid.** Graafiteooria alguseks loetakse aastat 1736, mil šveitsi matemaatik Leonhard Euler (1707 – 1783) pööras tähelepanu järgmisele ülesandele. Ida-Preisimaa suurim linn ja halduskeskus Königsberg asus Pregeli jõe ääres. Jõeharude kaldaid ning jõe keskel asuvat Kneiphofi saart ühendas omavahel seitse silda (joonisel vasakul). Pärastlõunaseid jalutuskäike armastavaid haritud



linnaelanikke hakkas huvitama küsimus: kas on võimalik kodust alustades teha ringkäik läbi linna, ületada iga sild täpselt üks kord ja jõuda lõpuks koju tagasi?

Moodustame graafi, mille tippudeks on jõeharude kaldad ning servadeks sillad (joonisel paremal). Küsimus taandub siis sellele, kas saadud (multi)graafis leidub tsükkel, mis läbib kõiki servi täpselt üks kord. Esimene tulemus graafiteoorias ongi Euleri tõestatud teoreem, millest järeldub, et niisugust tsükli ja seega ka otsitavat ringkäiku üle Pregeli sildade pole olemas.

Tsükli, mis läbib graafi kõik servad täpselt üks kord, nimetatakse *Euleri tsükliks*, ning graafi, kus leidub Euleri tsükkel, vastavalt *Euleri graafiks*. Praktikas tuleb Euleri tsükliga tegemist näiteks mitmesuguste jaotusvõrkude optimeerimisel, muu hulgas posti laialikandmisel, kui soovime efektiivsuse huvides läbida iga tänavat ainult ühe korra. Samuti esineb Euleri tsükliga seostuvaid probleeme skeemide joonistamisel plotteriga, kus püütakse võimalikult vältida sule paberilt tõstmist joonistamise ajal.

Tõestame nüüd Euleri teoreemi aastast 1736, mis annab täpse tingimuse, millal graafis leidub Euleri tsükkel.

**Teoreem 6.** *Sidusas graafis leidub Euleri tsükkel parajasti siis, kui graafi iga tipu aste on paarisarv.*

**Tõestus.** *Tarvilikkus.* Eeldame, et graafis leidub Euleri tsükkel. Iga kord, kui see tsükkel läbib teatavat tippu  $v$ , kasutab ta ära kaks sealte lähtuvat serva. Et tsükkel saaks ära kasutada kõik servad tipu  $v$  juures ja pärast seda pöörduda ikkagi algtipu tagasi, peab tipu  $v$  aste olema paarisarv.

*Piisavus.* Eeldame, et graaf on sidus ja iga tipu aste on paarisarv. Valime vabalt ühe tipu  $u$  ja hakkame liikuma mööda servi, läbides iga serva ainult üks kord. See teekond saab lõppeda ainult siis, kui oleme jõudnud tagasi tippu  $u$ , sest igast muust tipust on võimalik pärast sisenemist ka väljuda. Kui oleme sellega läbinud kõik servad, siis on Euleri tsükkel leitud. Vastasel korral leidub tsükli tipp  $v$ , mille juures on mõni serv läbimata (muidu oleks see tsükkel iseseisev sidus komponent). Tipust  $v$  hakkame liikuma mööda varem läbimata servi. Et eelnev tsükkel kasutas iga tipu juures ära paarisarvu servi, on ka nüüd iga tipu juures läbimata servi paarisarv. Sarnaselt eelnevaga jõuame lõpuks tagasi tippu  $v$ . Nüüd võime algset tsükli pikendada, lisades talle juurde viimati leitud tsükli tipust  $v$  tippu  $v$ . Sellist võtet korrates saame lõpuks tsükli, mis läbib graafi kõiki servi.  $\square$

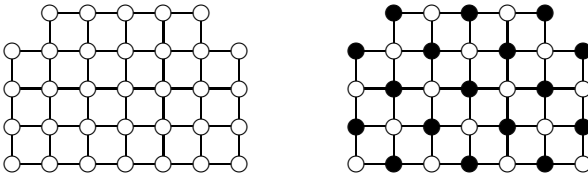


Königsbergi sildadele vastavas graafis ei kehti tingimus, et iga tipu aste on paarisarv, ning seetõttu ei leidu seal ka Euleri tsüklit. Muu hulgas jäeldub tõestatud teoreemist näiteks veel, et täisgraaf  $K_n$  on Euleri graaf parajasti siis, kui tippude arv  $n$  on paaritu, sest ainult sel juhul on graafis iga tipu aste paarisarv. Seega saab graafe  $K_3$ ,  $K_5$ ,  $K_7$ , ... joonistada ühe joonega, kuid graafe  $K_4$ ,  $K_6$ ,  $K_8$ , ... mitte.

Lisaks Euleri tsüklile, mis läbib graafi iga serva täpselt üks kord, vaadeldakse ka tsükleid, mis läbib täpselt üks kord graafi iga tippu. Niisuguse omadusega tsüklit nimetatakse iiri matemaatiku ja füüsiku William Rowan Hamiltoni (1805 – 1865) järgi *Hamiltoni tsükliks* ning vastavat graafi *Hamiltoni graafiks*. Aastal 1859 esitas Hamilton ülesande, mille põhiosaks oli puust valmistatud korrapärase 12-tahukas ning mööda selle tippe tuli sooritada ümbermaailmareis, külastades iga linna täpselt üks kord ja jõudes lõpuks tagasi alguspunkti.

Erinevalt Euleri tsüklitest on Hamiltoni tsüklitega seotud omadused märgatavalt keerulisemad. Hamiltoni tsükli leidumise või mitteleidumise kontrolliks pole olemas ühtegi lihtsat tingimust, isegi arvu-tiga lahendades pole teada oluliselt efektiivsemat algoritmi kui kõigi erinevate tipujärjestuste läbivaatamine. Sageli tuleb Hamiltoni tsükli puudumises veendumiseks kasutada mitmesuguseid erivõtteid.

*Näide 3.* Tõestada, et joonisel vasakul kujutatud graafis ei leidu Hamiltoni tsüklit.



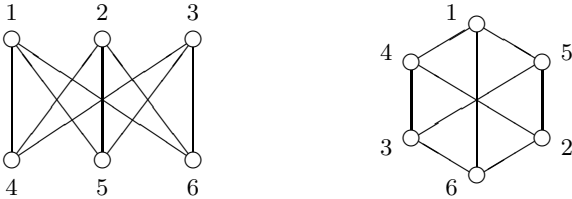
Värvime graafi tipud mustaks ja valgeks, nagu joonisel paremal. Värvitud graafil on omadus, et mustast tipust saab mööda serva liikuda ainult valgesse tippu ja valgest tipust ainult musta. Oletame, et graafis leidub Hamiltoni tsükel. Lähtudes mustast tipust, peab tsükli esimene, kolmas, viies ja üldse iga paaritu numbriga tipp olema must, iga paarisnumbriga tipp aga valge, sest tipu värv vaheldub iga sammul. Et graafil on 33 tippu, siis on viimane tipp enne algusesse tagasipöördumist must. See aga tähendab, et tsüklil peaksid kaks musta tippu, esimene ja viimane, olema servaga ühendatud.

**6. Graafide isomorfism.** Ühte ja sama graafi võib üles joonistada mitmel viisil, varieerides tippude paigutust ja servade kuju. Vaatamata erinevale väljanägemisele, on niisugustel graafidel ikka samad

omadused, mistõttu nende vahel pole mõtet vahet teha. Et graafide puhul on oluline ainult see, milliseid tippe ühendab serv ja milliseid mitte, siis loeme ühesuguseks neid graafe, mille tippude ja servade vahel saab korraldada üksühese vastavuse.

Graafe  $G = (V, E)$  ja  $G' = (V', E')$  nimetatakse *isomorfsseteks*, kui leidub niisugune bijektsioon  $\varphi: V \rightarrow V'$ , et graafis  $G$  on serv tippude  $u$  ja  $v$  vahel parajasti juhul, mil graafis  $G'$  on serv tippude  $\varphi(u)$  ja  $\varphi(v)$  vahel.

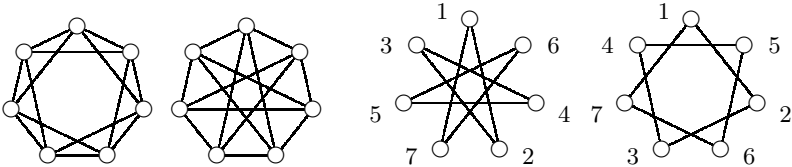
Teisiti öeldes tähendab isomorfsus seda, et mõlemas graafis võib tipud nummerdada nii, et samade numbritega tipud on kas mõlemas graafis servaga ühendatud või mõlemas ühendamata. Näiteks kummaski joonisel kujutatud graafis on serv tippude 1 ja 4 vahel, tippude 1 ja 5 vahel jne. Igale servale esimeses graafis vastab teises graafis serv samade numbritega tippude vahel ja vastupidi. Järelikult on need graafid isomorfsed.



Isomorfsed graafe me üksteisest ei erista. Kui näiteks nõutakse leida kõik teatava omadusega graafid, siis mõeldakse selle all, et need graafid peavad olema mitteisomorfsed. Teiste sõnadega, graafe loendatakse isomorfsismi täpsusega.

Otse definitsioonist järeldub, et kahe isomorfsse graafi täiendgraafid on samuti isomorfsed. Seda omadust kasutatakse mõnikord isomorfsuse kindlakstegemiseks, kui täiendgraafide servade arv on väiksem graafide endi servade arvust.

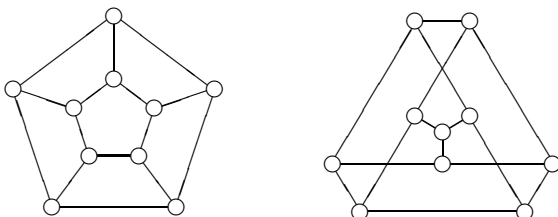
Näide 4. Tõestada, et kaks graafi joonisel vasakul on isomorfsed.



Leiame nende graafide täiendgraafid (joonisel paremal). Et viimased koosnevad ainsast tsüklist ja sisaldavad ühepalju tippe, siis on nad isomorfsed. Seega on isomorfsed ka esialgsed graafid.

Arusaadavalt on isomorfsetel graafidel ühepalju tippe ja ühepalju servi. Suurust, mis on ühesugune kõigi isomorfsete graafide puhul, nimetatakse *invariandiks*. Lihtsamad invariandid lisaks tippude ja servade arvule on veel näiteks tipu maksimaalne aste, pikima lihttsükli pikkus, erinevate lihtahelate arv kahe tipu vahel jne. Kui kahe graafi puhul on mingi invariandi väärtused erinevad, siis ei saa need graafid olla isomorfsed.

Näide 5. Tõestada, et joonisel kujutatud graafid ei ole isomorfsed.



Mõlemal graafil on 10 tippu ja 15 serva. Kuid vasakpoolses graafis on lühima tsükli pikkus 4, parempoolses aga 5. Et lühima tsükli pikkused on erinevad, siis pole need graafid isomorfsed.

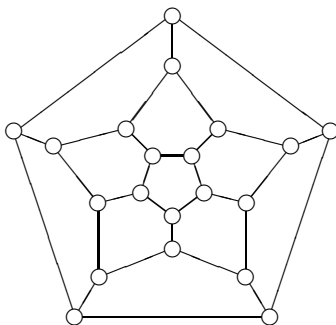
Invariandi väärtuste võrdsusest üldiselt ei järeldu, et graafid on isomorfsed. Iseäranis ei tarvitse see, et kahel graafil on ühesugune tippude arv ning ühe graafi tippude astmed võrduvad teise graafi tippude astmetega, tähendada isomorfsust. Eelmise näite graafid ei ole isomorfsed, vaatamata sellele, et kõik tippude astmed on võrdsed.

## Ülesanded

- Joonistada kõik 2-tipulised, 3-tipulised ja 4-tipulised graafid.
- Kui palju leidub 5 tipu ja 7 servaga graafe?
- Joonistada graaf või tõestada, et sellist ei leidu, kui graafi tippude astmed on: a) 1, 2, 2, 3, 3, 3; b) 1, 1, 2, 2, 3, 4, 4; c) 1, 3, 3, 4, 5, 6, 6; d) 0, 1, 2, 3, 4, 5, 6, 7; e) 1, 1, 1, 1, 1, 2, 2, 2, 3.
- Tõestada, et igas vähemalt kaheliikmelises seltskonnas leidub kaks inimest, kellel on koosviibijate hulgas sama arv tuttavaid.
- Linnapea ja tema naine korraldasid peo ning kutsusid sinna  $n$  tuttavat koos abikaasadega, kokku  $2n$  inimest. Pärast tervituste vahetamist küsis linnapea igaühe, kaasa arvatud oma naise käest, mitmel inimesel ta kätt surus, ja sai  $2n + 1$  erinevat vastust. Abikaasad loomulikult teineteisel kätt ei surunud. a) Tõestada, et isik, kes surus kätt kõige rohkem, polnud linnapea naine. b) Mitmel inimesel surus kätt linnapea?

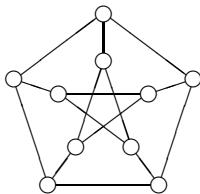
6. Tõestada, et graaf tippude astmetega  $d_1, d_2, \dots, d_n$ , kus  $d_1 \geq 1$  ja  $n \geq 2$ , on olemas parajasti siis, kui on olemas graaf tippude astmetega  $d_2 - 1, d_3 - 1, \dots, d_{d_1+1} - 1, d_{d_1+2}, d_{d_1+3}, \dots, d_n$ . Seda omadust korduvalt rakendades saab kindlaks teha, kas etteantud arvujärjend sobib graafi tipuastmete järjendiks.
7. Kas leidub graaf, millel on servi  $k$  korda rohkem kui tippe?
8. Tõestada, et majas, millel on ainult üks välisuku, leidub ruum, kus on paaritu arv uksti.
9. Maagaasi sisseveoks ja tarbijatele edasisuunamiseks otsustas gaasifirma ehitada 9 jaotusjaama. Selleks, et kindlustada ennast torujuhtmete võimalike tõrgete vastu, seadis firma juhtmete ehitamisel tingimuseks, et igal jaamal peab olema täpselt 5 teise taseme (st kahelüülist) ühendust ülejäänud jaamadega. Kas sellist nõuet on võimalik täita?
10. Graafi, mille tippudeks on kõikvõimalikud kahendarvud pikkusega  $n$  ja servaga on ühendatud need tipud, millele vastavad arvud erinevad parajasti ühe koha poolest, nimetatakse  *$n$ -mõõtmeliseks kuubiks*. Leida  $n$ -mõõtmelise kuubi tippude arv ja servade arv.
11. Mitmel viisil saab malelauale asetada kaks valget lippu nii, et nad teineteist kaitseksid?
12. Antud  $n$ -tipulises graafis leidub igal kahel tipul ühine naaber. Tõestada, et graafil on vähemalt  $3(n - 1)/2$  serva ning näidata, et seda hinnangut ei saa parandada.
13. Joonistada kõik 5-, 6- ja 7-tipulised regulaarsed graafid.
14. Tõestada, et kui  $n$  on paarisarv ja  $n \geq 4$ , siis leidub  $n$ -tipuline regulaarne graaf astmega 3.
15. Antud on graaf  $G$  ja täisarv  $d$ , mis on vähemalt sama suur kui  $G$  tippude maksimaalne aste. Tõestada, et leidub selline regulaarne graaf astmega  $d$ , et temast teatud arvu tippe kustutades jääb järele graaf  $G$ .
16. Tõestada, et kui graafis  $G$  leidub kaks erinevat tsükli, mis läbivad serva  $e$ , siis leidub graafis  $G$  tsükkel, mis serva  $e$  ei läbi.
17. Tõestada, et kui graaf  $G$  on regulaarne astmega 3, siis leidub selles paarisarvulise pikkusega lihttsükkel.
18. Kuuetipulise täisgraafi  $K_6$  iga serv värvitakse kas siniseks või punaseks. Tõestada, et värvitud graafis leidub kolmnurk, mis koosneb täielikult sinistest või täielikult punastest servadest.
19. Viietipulise täisgraafi  $K_5$  iga serv värvitakse kas punaseks või siniseks. Tõestada, et värvitud graafis leidub ühte värvi tsükkel.

20. Tõestada või lükata ümber järgmine väide: graafis, mille kõigi tippude astmed on paarisarvud, ei leidu ühtegi silda.
21. Tõestada, et graaf ise või tema täiendgraaf on alati sidus.
22. Tõestada, et sidusas graafis leidub vähemalt üks tipp, mis ei ole eraldav.
23. Tõestada, et graafidel  $G$  ja  $\overline{G}$  pole ühiseid eraldavaid tippe.
24. Tõestada, et kui graafis on täpselt kaks paaritu astmega tippu, siis leidub ahel, mis algab ühest neist tippudest, läbib kõik graafi servad täpselt üks kord ja lõpeb teises tipus.
25. Olgu  $G$  sidus graaf, millel on  $m > 0$  paaritu astmega tippu. Tõestada, et graafis  $G$  leidub  $m/2$  sellist lihtahelat, et graafi iga serv kuulub täpselt ühele lihtahelale.
26. Näituseruum jaguneb hulgaks koridorideks, mis lõikuvad üksteisega paljudes erinevates kombinatsioonides. Ruumil on üksainus sissepääs. Koridoride seintele on välja pandud pildid mõlemat kätt. Külastaja võib mööda koridori liikudes vaadata kas ainult ühel seinal asuvaid pilte või vaadata läbi mõlema seina pildid. Kas saab olla kindel, et külastaja võib siseneda näituseruumi, teha ringkäigu ja väljuda nii, et ta näeb iga pilti üksainus kord?
27. Vaatleme doominokive, mille kummagi poole silmade arv on mit-tenegatiivne täisarv 0-st  $n$ -ni. Kaks kivi võib panna teineteise kõrvale, kui neil on vähemalt ühel pool võrdne arv silmi. Millise  $n$  väärtuse korral saab neist kividest koostada kinnise ringi?
28. Tõestada, et suvalise sidusa graafi  $G$  võib saada teatavast Euleri graafist ühe tipu kustutamise teel.
29. Joonistada kõik 7-servalised Hamiltoni graafid.
30. Mitu erinevat Hamiltoni tsüklit sisaldab  $n$ -tipuline täisgraaf?
31. Joonisel on kujutatud graaf, mis on saadud korrapärase 12-tahuka projekteerimisel tasandile. Graafi tipud vastavad 12-tahuka tippudele ja servad tahuka servadele. Üks tahk projekteerub seejuures tervet joonist ümbritsevaks lõp-matuks tasandiosaks. Leida sellises graafis Hamiltoni tsüklid. See on Hamiltoni 1859. aastal esita-tud ülesande tasandiline variant.



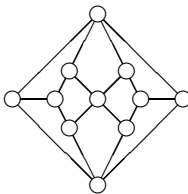
Kas järgmistes graafides leidub Hamiltoni tsükkel?

32.



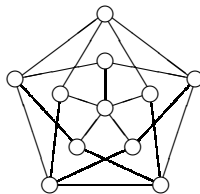
*Peterseni graaf*

33.



*Herscheli graaf*

34.



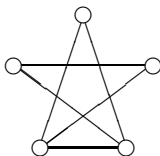
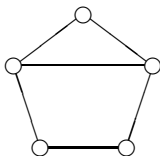
*Grötzsch'i graaf*

35. Vaatleme ratsu liikumist malelual mõõtmetega  $n \times n$ . Loeme graafi tippudeks malelaua ruudud ja ühendame kaks tippu servaga, kui ratsu saab ühe käiguga minna ühelt ruudult teisele. Tõestada, et kui  $n$  on paaritu, siis see graaf pole Hamiltoni graaf.

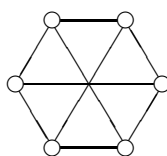
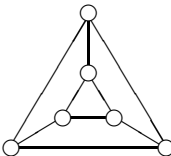
36. Väike hiir katvab süüa kuubikujulist juustu. Selleks jagab ta mõttes juustu  $3 \times 3 \times 3$  võrdseks kuubikuks, alustab nurkmisest kuubikust ning soovib lõpetada keskel. Pärast iga kuubiku söömist liigub hiir naaberkuubikusse. Kas hiirel õnnestub see plaan?

Teha kindlaks, kas järgmised graafid on isomorfsed.

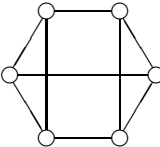
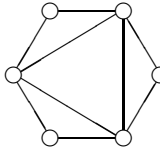
37.



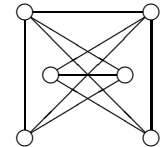
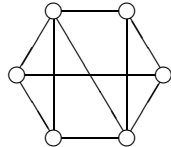
39.



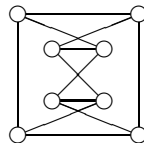
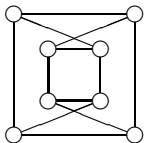
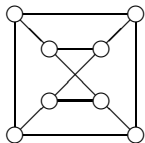
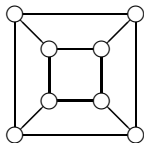
38.



40.



41. Millised järgnevate graafide hulgast on omavahel isomorfsed?



42. Vaatleme graafe, mis on isomorfsed oma täiendiga. a) Millist tingimust peab rahuldama sellise graafi tippude arv? b) Leida kõik 4- ja 5-tipulised graafid, mis on isomorfsed oma täiendgraafiga.

43. Rahuldagu graafi tippude arv  $n$  eelmises ülesandes leitud tingimust. Leida  $n$ -tipuline graaf, mis on isomorfne oma täiendiga.

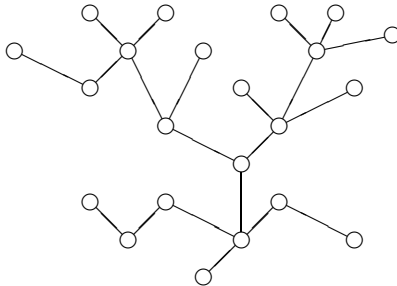
## VI. PUUD

**1. Puu mõiste.** Võtame nüüd vaatluse alla graafide olulise eriliigi, puud. Kõigi graafiklasside hulgas on just puude kasutusvaldkonnad ühed mitmekesisemad ja laiemad, eriti palju rakendusi leiavad nad arvutiteaduses.

**Definitsioon 1.** Graafi  $G = (V, E)$  nimetatakse puuks, kui ta on sidus ja ei sisalda tsükleid.

Puu definitsioon ühendab endas kahte vastandlikku omadust. Et graaf oleks sidus, ei tohi ta sisaldada liiga vähe servi, sest sidusale graafile serva lisamisel jääb graaf sidusaks, kuid serva kustutamisel võib ta sidususe kaotada. Tsüklite puudumine aga tähendab, et graafis, vastupidi, ei tohi olla servi liiga palju, sest tsükliteta graafist serva kustutades saame ikka tsükliteta graafi, kuid serva lisamisel kahe tipu vahele võib tekkida tsüklitel.

Kõige lihtsam puu on ühetipuline graaf, millel pole ainsatki serva. See graaf ei sisalda tsükleid ja on kokkuleppe kohaselt sidus. Lihtsuselt järgmine puu on kahetipuline ahel. Üks mõnevõrra keerukam puu on kujutatud järgmisel joonisel:

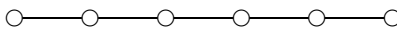


Puu servi nimetatakse ka *oksadeks* ja rippuvaid tippe *lehtedeks*.

**Teoreem 1.** Vähemalt kahetipulisel puul on vähemalt kaks lehte.

**Tõestus.** Valime graafis suvalise tipu ning hakkame liikuma mööda tippe, viibimata üheski neist rohkem kui üks kord. Selline teekond saab lõppeda ainult tipus astmega 1, sest kui niisugust tippu ette ei tuleks, siis jõuaksime varem või hiljem tagasi mõnda juba läbitud tippu, millega oleksime graafis leidnud tsükli. Järelikult leidub graafis vähemalt üks leht  $u$ . Lähtume nüüd tipust  $u$  ja kordame sama protsessi. Nii jõuame mingisse teise tippu  $v$ , mille aste on 1.  $\square$

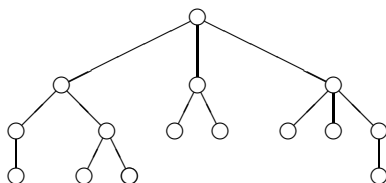
Leidub kuitahes suure tippude arvuga puud, millel ongi ainult kaks lehte, sellised on  $n$ -tipulised ahelad



Graafi, mille iga sidus komponent on puu, nimetatakse *metsaks*. Suvaline graaf, mis ei sisalda tsükleid, on mets. Sidus mets on puu. Et aga graafi iga sidus komponent on omaette graaf, siis võime piirduda komponentide uurimisega, käsitledes neid üheskoos ainult siis, kui olukord nõuab.

Rakendustes esineb sageli ka *juurega puud*, kus tippude hulgast on välja eraldatud üks tipp, *juur*. Kõik juurega puu tipud võib jagada klassidesse selle järgi, kui kaugel nad juurest asuvad: juure loeme kuuluvaks klassi null, esimesse klassi kuuluvad juure naabertipud, teise tipud, mille kaugus juurest on 2 jne. Puu iga serv ühendab kahte naaberklassidesse kuuluvat tippu. Serva seda otstippu, mis asub juurele lähemal, nimetatakse *ülemtipuks*, teist otstippu aga *alamtipuks*. Juure kõik naabrid on juure alamtipud, lehtedel alamtippe pole. Suurimat kaugust juure ja mingi lehe vahel ehk pikima juurest lähtuva lihtahela pikkust nimetatakse juurega puu *kõrguseks* või ka *sügavuseks*.

Juurega puud sobivad hästi algoritmides läbivaadatavate variantide organiseerimiseks, samuti mitmesuguste hierarhiate kirjeldamiseks. Alluvussuhteid silmas pidades kujutataksegi juurega puud tihthele looduslikuga võrreldes ümberpööratult, juur üleval:



**2. Puude põhiomadused.** Kõigepealt näitame, et puu servade arv sõltub ainult tippude arvust, mitte aga sellest, kuidas on tipud üksteisega ühendatud.

**Teoreem 2.** *Igal  $n$ -tipulisel puul on  $n - 1$  serva.*

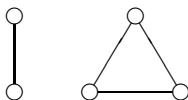
**Tõestus.** Selle tulemuse saame otse eelmise peatüki järeldustest 2 ja 3. Siiski esitame ka iseseisva tõestuse induktsiooniga graafi tippude arvu  $n$  järgi.

**Baas.** Kui  $n = 1$ , siis on meil tegemist ühetipulise graafiga, millel pole ühtegi serva. Seega kehtib väide sel juhul.

**Samm.** Eeldame, et väide kehtib kõigi  $k$ -tipuliste puude korral. Olgu  $G$  puu, millel on  $k + 1$  tippu. Teoreemi 1 põhjal leidub puul  $G$  vähemalt kaks lehte. Kustutame ühe lehe koos servaga. Tulemuseks saadud  $k$ -tipuline graaf on ikka puu, sest lehe kustutamisel sidusus säilib, samuti ei saa tekkida ühtegi tsüklit. Induktsiooni eelduse põhjal on sellel graafil  $k - 1$  serva. Järelikult graafil  $G$  on  $k$  serva.  $\square$

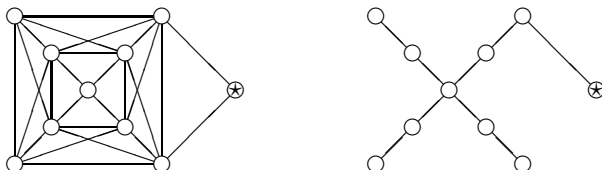


Vastupidine väide ei kehti: kui  $n$ -tipulisel graafil on  $n - 1$  serva, siis graaf ei tarvitse olla puu. Näiteks järgmisel graafil on küll 5 tippu ja 4 serva, kuid graaf pole puu, sest ta pole ei sidus ega tsükliteta:



Teoreemi tõestuses kasutatud võte näitab muuhulgas ka seda, et iga puud saab konstrueerida graafile ükshaaval servi lisades. Lähtume ühetipulisest graafist, igal sammul loome uue tipu ja ühendame ta servaga juba olemasoleva graafi mingi tipu külge. Tekkinud graaf on puu: ta on sidus, sest igast tipust on võimalik liikuda kõige esimesse tippu, ning ei sisalda tsükleid, sest suvalise serva eemaldamisel eraldub serva otstipu külge kinnituv alamgraaf ülejäänud graafist. Vastupidi, iga  $n$ -tipulise puu saab konstrueerida sellisel viisil, sest kui on võimalik konstrueerida puud, mis on saadud antud puust ühe lehe kustutamisel, siis on võimalik konstrueerida ka puud ennast.

*Näide 1.* Joonisel vasakul on esitatud küla elektriliinide plaan. Iga kahe ühendatud punkti vahel on kahesuunaline kaablilõik, tärniga on tähistatud alajaam. Mitu ühendust võib maksimaalselt katkeda, ilma et ükski punkt jääks elektrita?



Et ükski punkt ei jääks elektrita, peab graaf pärast servade eemaldamist jääma sidusaks. Kui saadud graaf sisaldaks tsükleid, siis võiksime kustutada ühe serva tsüklist, millega graafi sidusus ei kao. Seega peab pärast servade kustutamist alles jääma puu. Et antud graafil on 26 serva, 10-tipuline puu aga sisaldab 9 serva, siis võib kustutada 17 serva. Joonisel paremal ongi näidatud üks sobiv puu.

Maksimaalset servade arvu, mida võib graafist eemaldada, ilma et graaf kaotaks sidusust, nimetatakse graafi *tsükloomaatiliseks arvuks*. Kui sidusas graafis on  $n$  tippu ja  $m$  serva, siis tema tsükloomaatiline arv on  $m - n + 1$  ehk antud graafi servade arvu ja sama tippude arvuga puu servade arvu vahe.

Järgnevalt esitame mõningad tingimused, mille järgi saab kindlaks teha, kas graaf on puu või mitte. Need kujutavad endast erinevaid,

kuid üksteisega samaväärseid võimalusi puu defineerimiseks. Nimelt võib puud mõista kui servade arvu mõttes vähimat sidusat graafi või kui servade arvu mõttes suurimat tsükliteta graafi.

**Teoreem 3.** *Graafi  $G$  puhul on järgmised väited samaväärsed:*

1.  $G$  on puu;
2.  $G$  on sidus, kuid ükskõik millise serva kustutamisel muutub mittesidusaks;
3.  $G$  ei sisalda tsükleid, kuid ükskõik millise serva lisamisel tekib tsükkel.

**Tõestus.** Et näidata mitme väite samaväärsust, tõestame järeldumiste ahela  $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$ .

$1 \Rightarrow 2$ . Eeldame, et graaf  $G$  on puu. Siis on ta kindlasti sidus. Kui oletada, et mingi serva  $uv$  kustutamisel jääb graaf sidusaks, siis see serv ei ole sild ning eelmise peatüki teoreemi 4 põhjal kuulub ta mingisse tsükklisse. See on aga võimatu, sest puu ei sisalda tsükleid.

$2 \Rightarrow 3$ . Eeldame, et  $G$  on sidus, kuid suvalise serva kustutamisel kaotab sidususe. Graaf  $G$  ei saa sisaldada tsükleid, sest tsükklisse kuuluva serva eemaldamisel jääks graaf sidusaks. Edasi, et graaf  $G$  on sidus, siis leidub iga kahe tipu  $u$  ja  $v$  korral neid ühendav ahel. Tippude  $u$  ja  $v$  vahele serva lisamisel tekib siis tsükkel, mis koosneb ahelast ja sellest servast.

$3 \Rightarrow 1$ . Eeldame, et  $G$  ei sisalda tsükleid, kuid suvalise serva lisamisel tekib tsükkel. Siis peab graaf  $G$  olema sidus. Tõepoolest, kui leiduks kaks tippu  $u$  ja  $v$ , mis kuuluvad erinevatesse sidusatesse komponentidesse, siis ei tekiks nende ühendamisel juurde ühtegi tsüklit, sest serv  $uv$  oleks saadava graafi sild. Et graaf  $G$  ei sisalda tsükleid ja on sidus, siis ta on puu.  $\square$

**Järeldus 1.** *Graafi  $G$  puhul, millel on  $n$  tippu ja  $m$  serva, on järgmised väited samaväärsed:*

1.  $G$  on puu;
2.  $G$  on sidus ja  $m \leq n - 1$ ;
3.  $G$  ei sisalda tsükleid ja  $m \geq n - 1$ .

**Tõestus.** Kui  $G$  on puu, siis ta on sidus, ei sisalda tsükleid ja teoreemi 2 põhjal  $m = n - 1$ . Seega järeldub väitest 1 nii väide 2 kui ka väide 3.

Vastupidi, kui graaf  $G$  on sidus ja  $m \leq n - 1$ , siis peab graaf suvalise serva kustutamisel kaotama sidususe, sest eelmise peatüki järelduse 3 tõttu ei saa ükski vähem kui  $n - 1$  tipuga graaf olla sidus. Seega kehtib eelmise teoreemi tingimus 2, millest järeldub, et  $G$  on puu.

Kui graaf  $G$  ei sisalda tsükleid ja  $m \geq n - 1$ , siis leidub suvalise serva lisamisega saadud graafis tsükkel: eelmise peatüki järelduse 2 põhjal sisaldab iga graaf, millel on vähemalt sama palju servi kui tippe, vähemalt ühte tsükli. Nüüd on täidetud eelmise teoreemi tingimus 3, millest saame, et  $G$  on puu.  $\square$

Viimane järeldus võimaldab puude kindlakstegemiseks kasutada tippude ja servade arvu graafis. Anname veel ühe tingimuse, mis kirjeldab puud neis sisalduvate lihtahelate kaudu.

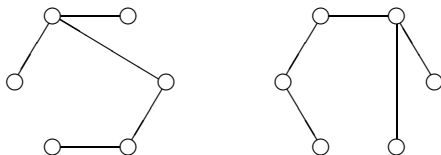
**Teoreem 4.** *Graaf  $G$  on puu parajasti siis, kui tema iga kahte erinevat tippu ühendab täpselt üks lihtahel.*

**Tõestus.** *Tarvilikkus.* Et  $G$  on puu, siis ta on sidus ja iga kahe tipu vahel leidub lihtahel. Kui mingeid tippe  $u$  ja  $v$  ühendaks kaks erinevat lihtahelat, siis saaksime konstrueerida tsükli: lähtume kahe lihtahela võimaliku ühise algusosa viimasest tipust  $w$  ja liigume mööda esimest lihtahelat, kuni jõuame tipuni, mis paikneb taas teisel lihtahelal, seejärel liigume mööda teist lihtahelat tippu  $w$  tagasi.

*Piisavus.* Et iga kahte tippu ühendab ahel, siis on graaf sidus. Kui graafis leiduks tsükkel, siis ühendaks tsükli kahte naabertippu  $u$  ja  $v$  kaks lihtahelat: serv  $uv$  ja tsükli ülejäänud osa tipust  $u$  tippu  $v$  (millest saab eraldada lihtahela).  $\square$

**3. Puude loendamine.** Püüame vastata küsimusele: kui palju leidub erinevaid  $n$ -tipulisi puud?

Kõigepealt peame kokku leppima, milliseid puud üldse lugeda erinevaks. Näiteks puud



on isomorfsed ja neid võib omavahel samastada. Ent kui joonised kujutavad näiteks linnadevaheliste teede kaarte, siis tuleb puud pidada erinevaks: on oluline, kas mingit kahte linna ühendab tee või mitte. Teisel juhul võime puu tipud varustada nimede või üldisemalt mingite märgenditega, seejuures tuleb kahe puu võrdlemisel arvestada ka tippude märgendeid. Eristame seega kahte juhtu:

1. puu tipud on märgendatud, kahte puud loeme samaks, kui mõlemas on servad sama märgendiga tippude vahel;
2. puu tipud on märgendamata, kahte puud loeme samaks, kui võimalik kummagi puu tipud märgendada nii, et mõlemas on servad sama märgendiga tippude vahel.

Enamasti valitakse märgenditeks naturaalarvud ning vastavalt nimetatakse *märgendatud puuks* sellist  $n$ -tipulist puud, mille igale tipule on omistatud märgendiks erinev arv hulgast  $\{1, 2, \dots, n\}$ .

Vaatlemegi kõigepealt märgendatud puid. Igale sellisele puule seame vastavusse ühe  $(n - 2)$ -liikmelise arvujärjendi  $(x_1, x_2, \dots, x_{n-2})$ , mida nimetatakse *Prüferi koodiks*. Prüferi kood identifitseerib puu üheselt, lisaks on see kood väga kompaktne ning tema abil esitatud puu võtab näiteks arvuti mälus vähe ruumi. Prüferi koodi võib kasutada ka siis, kui mingil põhjusel on vaja genereerida juhuslikult üks  $n$ -tipuline puu.

Olgu  $G$  puu, mille tipud on märgendatud arvudega  $1, 2, \dots, n$ . Selle puu Prüferi kood konstrueeritakse järgmiselt. Leiame puust vähima märgendiga lehe ja kirjutame välja vastava serva otstippude märgendid: lehe oma üles ja naabertipu oma alla. Seejärel kustutame selle lehe koos servaga. Järelejäänud puu lehtede hulgast valime jälle vähima märgendiga lehe ja kirjutame serva otstippude märgendid eelmiste kõrvale, seejuures ikka lehe märgendi üles ja naabri oma selle alla. Niisugust operatsiooni kordame senikaua, kuni kõik servad on kustutatud. Tulemuseks saame tabeli

$$\begin{array}{cccccc} y_1 & y_2 & \dots & y_{n-2} & y_{n-1} & \\ x_1 & x_2 & \dots & x_{n-2} & x_{n-1} & \end{array}$$

kus ülemises reas on igal sammul leitud vähima märgendiga lehtede ja alumises reas nende naabertippude märgendid ning iga veerg vastab ühele servale. Elemendi  $x_{n-1}$  väärtus on alati  $n$ , sest suurima märgendiga tipp jääb alati viimaseks. Prüferi koodi moodustavad tabeli teise rea esimesed  $n - 2$  arvu:

$$(x_1, x_2, \dots, x_{n-2}).$$

Igaüks neist arvudest võib olla  $1, 2, \dots, n$ .

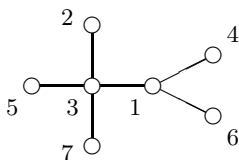
Sellega oleme näidanud, et igale märgendatud puule vastab Prüferi kood. Näitame, et Prüferi koodi järgi saab puu ka üheselt taastada.

Olgu antud järjend  $(x_1, x_2, \dots, x_{n-2})$ , kus iga arv  $x_i$  võib olla  $1, 2, \dots, n$ . Kirjutame järjendi lõppu arvu  $x_{n-1} = n$  ja hakkame koostama ülemist rida  $y_1, y_2, \dots, y_{n-1}$ . Arvu  $y_1$  väärtus peab olema vähim arv, mis ei esine alumises reas, sest esimesel sammul eemaldati vähima märgendiga leht. Arvu  $y_2$  väärtus peab olema vähim märgend, mis oli puu lehtedel pärast esimese lehe eemaldamist. See ei saa olla  $y_1$ , sest niisuguse märgendiga lehte puus enam ei ole, ega ükski arvudest  $x_2, \dots, x_{n-1}$ , sest nende arvudega märgendatud tipud esinevad kas käesoleval või mõnel järgmisel sammul lehtede naabritena. Järelikult on  $y_2$  vähim arv, mis erineb arvudest  $y_1, x_2, \dots, x_{n-1}$ . Analoogiliselt

on  $y_3$  vähim arv, mis erineb arvudest  $y_1, y_2, x_3, \dots, x_{n-1}$  jne. Igal sammul valime ülemise rea järjekordset kohta täitma vähima arvu, mis ei esine ülemises reas vasakul ega alumises reas all ja paremal. Niisugune arv leidub alati, sest igal kohal on keelatud ülimalt  $n - 1$  arvu, valikuid saab aga teha  $n$  arvu  $1, 2, \dots, n$  hulgest.

Pärast ülemise rea täitmist oleme leidnud graafi servade loendi. Tõestame, et saadud graaf on puu. Tabeli ülemises reas saavad esineda ainult arvud  $1$  kuni  $n - 1$ . Valikuviisi tõttu ei saa ükski neist korduda, seega peab ülemine rida koosnema arvudest  $1, 2, \dots, n - 1$  mingis järjekorras. Suvalisest tipust märgendiga  $i$  saame mööda teatavat serva  $\overset{i}{j}$  liikuda tippu  $j$ , edasi mööda serva  $\overset{j}{k}$  tippu  $k$  jne. Seejuures esineb märgend  $j$  ülemises reas kindlasti märgendist  $i$  paremal, mistõttu teekond jõuab varem või hiljem viimasesse veergu ja seega tippu  $n$ . Et graafi igast tipust saab moodustada ahela tippu  $n$ , siis on graaf sidus. Peale selle sisaldab ta  $n - 1$  serva ning on järelduse  $1$  põhjal puu.

Näide 2. Leida järgmise puu Prüferi kood:



Vähima märgendiga leht on  $2$  ja tema naaber on  $3$ . Koodi koostamist alustame seega veeruga  $\frac{2}{3}$ . Kustutame tipu märgendiga  $2$ . Järelejäänud puus on vähima märgendiga tipp  $4$ , tema naaber on  $1$ . Lisame veeru  $\frac{4}{1}$  ja kustutame tipu  $4$ . Jätkame seni, kuni kõik servad on ammendatud. Niiviisi saame tabeli

2	4	5	6	1	3
3	1	3	1	3	7

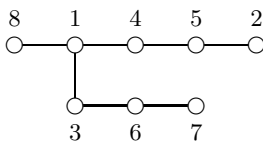
Prüferi kood on viimane rida ilma viimase elemendita:  $(3, 1, 3, 1, 3)$ .

Näide 3. Joonistada puu, mille Prüferi kood on  $(5, 4, 1, 6, 3, 1)$ .

Koodi pikkus on  $n - 2 = 6$ , seega lisame lõppu arvu  $n = 8$ . Seejärel täidame ülemise rea. Esimene element on vähim arv, mis ei esine alumises reas, ehk  $2$ . Teine element on vähim arv, mis ei esine ülemises reas vasakul ega alumises reas all ja paremal. See arv on  $5$ . Täites sama põhimõtte järgi kõik ülemise rea vabad kohad, saame tabeli

2	5	4	7	6	3	1
5	4	1	6	3	1	8

Iga veerg vastab siin puu ühele servale. Kui servad on teada, siis saame ka puu välja joonistada:



Eelnevas nägime, et märgendatud puud ja Prüferi koodid on üks-üheses vastavuses. Et Prüferi kood koosneb  $n-2$  arvust ning koodi iga arv võib sõltumata teistest omandada  $n$  erinevat väärtust, siis võime sõnastada järgmise nn *Cayley teoreemi*, mille esmakordselt tõestas inglise matemaatik Arthur Cayley (1821 – 1895).

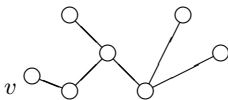
**Teoreem 5.** *Erinevate  $n$ -tipuliste märgendatud puude arv on  $n^{n-2}$ .*

Teiseks uurime juhtu, kus puu tipud ei ole märgendatud. Täpset valemit siin küll teada ei ole, kuid on võimalik anda puude arvu ülemine ja alumine tõke. Kasutame sama võtet nagu märgendatud puude korral, seades igale puule vastavusse teatava koodi.

Olgu  $G$  puu. Valime mingi tipu  $v$  ja loeme selle juureks. Lähtudes sellest, teeme ringkäigu ümber puu, kuni jõuame tippu  $v$  tagasi. Kogu aeg liigume nii, et puu serv jääb liikumissuunaga võrreldes vasakule. (Võib ette kujutada, et servad tähistavad maanteid ning me läbime järjest kõik teed nii ühes kui teises suunas.) Kui teeme sammu tipust  $v$  eemale (nii, et kaugus tipust  $v$  suureneb), siis lisame koodi arvu 1; kui aga liigume tipu  $v$  poole, siis arvu 0. Ringkäigu lõppedes oleme saanud teatava numbrist 0 ja 1 koosneva järjendi, mida nimetame puu *binaarkoodiks*. Koodi pikkus võrdub puu servade arvu kahekordsega,  $n$ -tipulise puu binaarkoodis on seega  $2(n-1)$  kahendkohta.

Binaarkoodi põhjal saab puu üheselt taastada. Alustame graafist, mis koosneb ainult juurest  $v$ . Seejärel vaatame koodi elementhaaval läbi, vajaduse korral graafile tippe lisades. Nimelt, kui koodis esineb mingil kohal arv 1, siis loome uue tipu, ühendame ta graafis eelneva tipuga ning liigume järjega lisatud tippu, arvu 0 puhul aga liigume tipust, kus parajasti asume, naabertippu, mis jääb juure  $v$  poole. Niimoodi tekkinud graaf on puu, sest ta on konstrueeritud servade ükshaaval lisamise meetodil, mida vaatlesime pärast teoreemi 2.

*Näide 4.* Leida järgmise puu binaarkood:



Valides juureks  $v$  vasakpoolse tipu, saame koodi 111101001000.

Vastupidiselt Prüferi koodile ei ole binaarkood üheselt määratud: ühele puule võib vastata mitu koodi, sest juureks võib valida erinevaid tippe, kuid igale koodile vastab kindlasti üks puu.

**Teoreem 6.** *Erinevate  $n$ -tipuliste puude arv  $T_n$  rahuldab võrratust*

$$\frac{n^{n-2}}{n!} < T_n < 2^{2(n-1)}.$$

**Tõestus.** Kui  $n$ -tipulise puu tippudele omistada kõikvõimalikel viisidel märgendeid, siis võib see puu anda ülimalt  $n!$  märgendatud puud – mõnikord, näiteks ahela puhul, ka vähem. Niimoodi võib saada iga märgendatud puu. Et  $n$ -tipuliste märgendatud puude arv on  $n^{n-2}$ , siis peab kehima võrratus  $T_n n! > n^{n-2}$ . Teiselt poolt on  $n$ -tipulisi puid vähem kui vastavaid binaarkoode. Kahendarve pikkusega  $2(n-1)$  on aga  $2^{2(n-1)}$ , seega  $T_n < 2^{2(n-1)}$ .  $\square$

Järgmises tabelis on antud  $n$ -tipuliste puude arv  $T_n$  parameetri mõne väiksema väärtuse korral:

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$T_n$	1	1	1	2	3	6	11	23	47	106	235	551	1301	3159	7741	19320

**4. Graafi aluspuud.** Sidusa graafi  $G$  *aluspuuks* nimetatakse sellist alamgraafi, mis on puu ja sisaldab kõiki graafi  $G$  tippe. Näiteks joonisel kujutatud graafi  $G$  üks aluspuu on graaf  $G'$ :



Lihtne on näha, et aluspuu leidub igal sidusal graafil. Kustutame antud graafist servi niikaua, kui see on võimalik, ilma et graaf kaotaks sidusust. Kui ühtegi serva enam eemaldada ei saa, siis ongi järele jäänud aluspuu. Tõepoolest, allesjäänud graaf sisaldab lähtegraafi kõiki tippe, ta on sidus, kuid ükskõik millise serva eemaldamisel sidusus kaob. Teoreemi 3 põhjal on selline graaf puu.

Aluspuu on seega vähima servade arvuga alamgraaf, mis ühendab graafi kõiki tippe.

Igal puul on ainult üks aluspuu, tema ise. Kõige rohkem aluspuid on täisgraafil. Nagu nähtub Cayley teoreemist, on  $n$ -tipulisel täisgraafil ühtekokku  $n^{n-2}$  erinevat aluspuud.

Praktikas esinevad aluspuud näiteks järgmist tüüpi ülesannetes. Antud on  $n$  asulat, mis tuleb ühendada teedevõrguga nii, et igast asulast pääseks igasse teise, kusjuures ehituse kogumaksumus peab olema nii väike kui võimalik. Sama ülesanne kerkib ka siis, kui on

vaja ühendada võrgukaabliga  $n$  arvutit, luua ühendus  $n$  mikrokiibi vahele vms. Selleks, et arvutada ehituse hinda ja võrrelda erinevaid variante, olgu meil iga kahe asula puhul, mille vahele tee rajamine üldse kõne alla võib tulla, teada selle tee ehitamise kulu.

Odavam ühendusteede graaf peab olema puu: ta peab olema sidus ja ei tohi sisaldada tsükleid: kui graafis esineks tsükel, siis võiksime sealt ühe serva välja jätta, millega ühendusvõrgu koguhind väheneks.

Matemaatilises püstituses on ülesanne seega järgmine. Antud on graaf  $G$ , mille igale servale on omistatud kaal – teatav, tavaliselt positiivne reaalarv. Leida graafi  $G$  vähima kaaluga aluspuu. Siin mõistame aluspuu kaalu all tema kõigi servade kaalude summat.

Üks võimalus seda ülesannet lahendada on vaadata läbi graafi  $G$  kõik aluspuud ja valida nende hulgast välja see, mille kaal on kõige väiksem. Kuid niisugune meetod võib tippude vähegi suurema arvu juures muutuda äärmiselt töömahukaks. Näiteks täisgraafi  $K_n$  puhul peaksime läbi kontrollima  $n^{n-2}$  erinevat varianti, mis käiks kiirematele arvutitele üle jõu juba mõneteistkümnne tipu juures. Siiski on vähima kaaluga aluspuu leidmiseks olemas oluliselt efektiivsem viis, mille esmakordselt pakkus välja ameerika matemaatik Martin Kruskal (1925) ja mida tema järgi nimetatakse *Kruskali algoritmiks*.

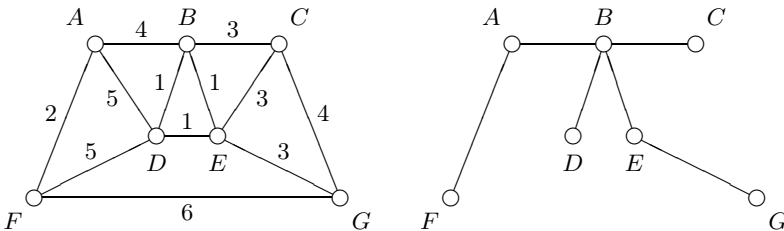
**Kruskali algoritm.** Olgu  $G$  kaalutud  $n$ -tipuline graaf.

- Valime graafist  $G$  vähima kaaluga serva  $e_1$ .
- Iga  $i = 2, 3, \dots, n - 1$  korral valime graafist  $G$  sellise vähima kaaluga serva  $e_i$ , mis erineb servadest  $e_1, e_2, \dots, e_{i-1}$  ja ei moodusta koos nendega tsükli.

Algoritmi tulemuseks on servadest  $e_1, e_2, \dots, e_{n-1}$  moodustuv graaf.

Kruskali algoritm kuulub nn *ahnete algoritmide* klassi. Nende algoritmide iseloomulik tunnus on see, et igal sammul täiendatakse konstruktsiooni just niisuguse objektiga, mille valimine näib just sel hetkel kõige soodsam, pööramata tähelepanu võimalusele, et hilisematel sammudel tuleb seetõttu teha võib-olla ebasoodsaid valikuid.

*Näide 5.* Leida joonisel vasakul kujutatud graafi vähima kaaluga aluspuu, kus numbrid servade juures tähistavad servade kaalu.





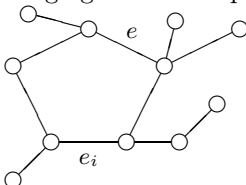
Vastavalt Kruskali algoritmile valime servaks  $e_1$  graafi vähima kaaluga serva, olgu  $e_1 = BD$ . Ülejäänud servade hulgast valime jälle vähima kaaluga serva, olgu see  $e_2 = BE$ . Servaks  $e_3$  ei saa valida graafi serva  $DE$ , sest siis tekiks tsükkel, seepärast võtame  $e_3 = AF$ . Edasi saame  $e_4 = BC$ ,  $e_5 = EG$ ,  $e_6 = AB$ . Nüüd on vähima kaaluga aluspuu servad leitud. Aluspuu kaal on  $1 + 1 + 2 + 3 + 3 + 4 = 14$  ning puu ise on näidatud joonisel paremal.

Siit nähtub ka, et algoritmi tulemus ei tarvitse olla ühene, vähima kaalu võib anda mitu aluspuud. Esimesel sammul oleksime võinud võtta  $e_1 = DE$ , siis oleksime saanud aluspuu, mis sisaldab serva  $DE$ , näiteks  $e_2 = BD$ ,  $e_3 = AF$ ,  $e_4 = CE$ ,  $e_5 = EG$ ,  $e_6 = AB$ . Selle aluspuu kaal on samuti 14.

Tõestame nüüd, et Kruskali algoritm on korrektne.

**Teoreem 7.** *Kui  $G$  on sidus graaf, siis leiab Kruskali algoritm graafi  $G$  vähima kaaluga aluspuu.*

Tõestus. Kui graafil  $G$  on  $n$  tippu, siis Kruskali algoritmiga saadud graaf  $H$  ei sisalda tsükleid ning tal on  $n - 1$  serva ja ülimalt  $n$  tippu. Järelduse 1 põhjal on graaf  $H$  puu. Siis aga kuuluvad sinna graafi  $G$  kõik  $n$  tippu ning  $H$  on seega graafi  $G$  aluspuu.

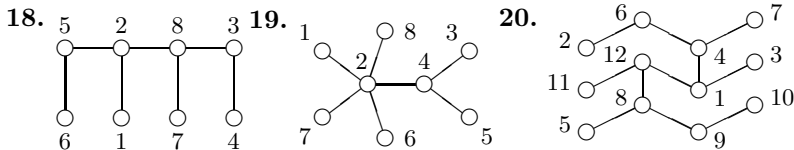


Tõestame, et  $H$  kaal on kõigi aluspuude seas vähim. Olgu  $H_1$  graafi  $G$  suvaline aluspuu ja  $e_i$  puu  $H$  konstrueerimisel esimene serv, mis ei kuulu puusse  $H_1$ . Kui lisame serva  $e_i$  puule  $H_1$ , siis tekib seal tsükkel, mis sisaldab serva  $e_i$  (joonis). Et puu  $H$  tsükleid ei sisalda, siis leidub sellel tsükli serv  $e$ , mis ei kuulu puusse  $H$ . Serva  $e$  kaal peab olema vähemalt sama suur kui serva  $e_i$  kaal, sest muidu oleks Kruskali algoritm valinud puud  $H$  konstrueerides serva  $e_i$  asemel serva  $e$ . Serv  $e$  ei saanud olla välistatud ka tsükli tekkimise tõttu, sest kõik selle hetkeni puusse  $H$  valitud servad ja serv  $e$  sisalduvad puus  $H_1$ . Kustutame nüüd puust  $H_1$  serva  $e$  ja lisame serva  $e_i$ . Saadud graaf  $H_2$  on samuti puu, sest ta on sidus ja koosneb  $n - 1$  servast, lisaks ei ületa tema kaal puu  $H_1$  kaalu. Puudel  $H_2$  ja  $H$  on rohkem ühiseid servi kui puudel  $H_1$  ja  $H$ . Niiviisi servi asendades teiseid puu  $H_1$  järkjärgult puuks  $H$ , puu kaal saab seejuures ainult väheneda. Järelikult ei saa puu  $H_1$  kaal olla väiksem puu  $H$  kaalust.  $\square$

## Ülesanded

1. Joonistada kõik 6-tipulised puud ja kõik 7-tipulised puud.
2. Joonistada kõik 5-tipulised juurega puud kõrgusega 1, 2, 3 ja 4.
3. Tõestada, et igal puul on vähemalt nii palju lehti, kui suur on tema tippude maksimaalne aste.
4. Millega võrdub  $n$ -tipulise puu kõigi tippude astmete summa?
5. Puu tippude astmed on 1, 1,  $\dots$ , 1, 2, 3, 4, 5, 6, 7. Mitu lehte on sellel puul?
6. Kui palju saab 12-tipulises puus leiduda tippe astmega 3?
7. Tõestada, et kümnetipulises puus, mille kõik astmed on paaritud, leidub vähemalt kuus lehte.
8. Tõestada, et lahtise ahelaga küllastunud süsivesinik sisaldab  $n$  süsiniku aatomi korral alati  $2n + 2$  vesiniku aatomit.
9. Olgu  $G$  ja  $G'$  mingid  $n$ -tipulised puud ning tähistagu  $a_i$  ja  $b_i$  astmega  $i$  tippude arvu vastavalt puus  $G$  ja  $G'$ . Tõestada, et
$$\sum_{i \geq 1} i(a_i - b_i) = 0.$$
10. Tõestada, et kui vähemalt kolmetipulise puu ühegi tipu aste pole 2, siis puus leidub tipp, millest väljub vähemalt kaks lehte.
11. Tõestada, et kui  $d_1, d_2, \dots, d_n$  on naturaalarvud, mille summa on  $2n - 2$ , siis leidub puu, mille tippude astmed on need arvud.
12. Juurega puu sisaldab  $n$  tippu, kusjuures igal sisetipul (st tipul, mis pole leht) on parajasti  $k$  alamtippu. Leida puu sisetippude arv  $s$  ja lehtede arv  $l$ .
13. Kui kustutada puust tipp  $v$  koos temast lähtuvate servadega, siis tekib hulk sidusaid komponente, millest igaüks on samuti puu. Nimetame neid tipu  $v$  *harudeks*. Tõestada, et puus leidub alati tipp, mille ükski haru ei sisalda rohkem kui pooli puu tippe.
14. Tõestada, et puu maksimaalse pikkusega lihtahelad läbivad kõik ühte ja sama tippu.
15. Mitu värvi tuleb minimaalselt kasutada, et värvida puu tipud nii, et naabertipud oleksid erinevat värvi?
16. Olgu  $G$  suvaline  $n$ -tipuline puu. Tõestada, et iga graaf  $H$ , mille kõigi tippude astmed on vähemalt  $n - 1$ , sisaldab alamgraafi, mis on isomorfne puuga  $G$ .
17. Kirjeldada puude ja tsüklite abil kõik sidusad graafid, mille tippude ja servade arv on võrdsed.

Leida järgmiste puude Prüferi koodid.



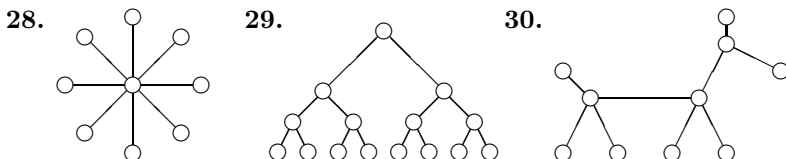
Joonistada Prüferi koodile vastav puu.

21. (1, 1, 1, 1, 1, 1) 23. (2, 3, 2, 3, 2, 3, 2) 25. (6, 2, 7, 3, 1, 5, 9, 8, 4)

22. (1, 2, 3, 4, 5, 6) 24. (4, 3, 4, 5, 4, 7, 7) 26. (2, 9, 2, 1, 5, 6, 2, 5, 1)

27. Tõestada, et märgendatud puu tipu  $v$  märgend esineb puu Prüferi koodis täpselt  $d(v) - 1$  korda.

Leida järgmiste puude binaarkoodid.



Kontrollida, kas järgmised binaarkoodid esitavad puud ning jaataval juhul joonistada vastavad puud.

31. 1100011100

33. 1110011010100100

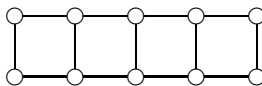
32. 11101001101000

34. 1111100100011011010000

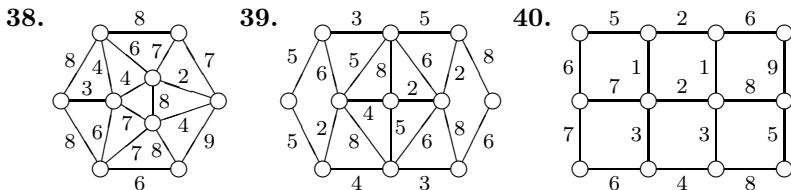
35. Leida tingimus, millal antud kahendarv  $b_1b_2 \dots b_{2n-2}$  sobib mingi  $n$ -tipulise puu binaarkoodiks.

36. Puu ühes tipus istus sipelgas. Olles teinud jalutuskäigu mööda puu servi, selgus, et iga serva läbis sipelgas täpselt kaks korda. Tõestada, et teekonna lõpus jõudis sipelgas tagasi samasse tippu, kust alustas.

37. Koostada rekurrentne võrrand  $2n$ -tipulise redeli (joonisel) aluspuude arvu leidmiseks ja lahendada see võrrand.

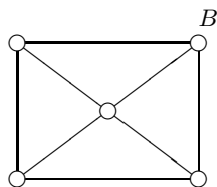


Leida järgmiste graafide vähima kaaluga aluspuud.



41. Tõestada, et graafi serv  $e$  on sild parajasti siis, kui ta kuulub graafi igasse aluspuusse.
42. Tõestada, et graafi vähima kaaluga aluspuu võib leida ka järgmiselt: igal sammul kustutada graafist suurima kaaluga serv, mis pole sild; kui enam servi eemaldada ei saa, siis järelejäanud graaf ongi otsitav.
43. Riigi  $n$  linna vahele rajatakse telefonivõrk järgmisel viisil. Algukses ehitatakse kõige odavam liin pealinnast mingisse teise linna, seejärel kõige odavam liin, mis ühendab emba-kumba linna mõne kolmanda linnaga jne, igal sammul ehitatakse kõige odavam liin, mis viib mingist juba ühendatud linnast uude linna. Tõestada, et valminud telefonivõrgu maksumus on võimalikest väikseim.
44. Riigi  $n$  linna vahele tuleb rajada telefonivõrk. Riigis on kaks parteid, optimistid ja pessimistid. Optimistid lähtuvad strateegiast, mille järgi ehitatakse uus liin alati nende kahe linna vahele, mille ühendamine on kõige odavam, tingimusel, et see ei tekita tsiklit. Pessimistid kasutavad strateegiat, mille puhul välistatakse esmalt kõige kallim liin, seejärel kalliduselt järgmine jne ning kahe linna vahele ehitatakse liin alles siis, kui selle välistamine muudaks linnadevahelise ühenduse võimatuks. Valitsuses vahetuvad optimistid ja pessimistid määramata ajavahemike tagant. Tõestada, et valminud telefonivõrgu maksumus on võimalikest väikseim.
45. Tõestada, et kui graafil on mitu vähima kaaluga aluspuud, siis saab need kõik konstrueerida Kruskali algoritmiga seal sobivalt servi valides.

46. *Shannoni mängu* mängitakse graafil  $G$ , kus on tähistatud kaks tippu  $A$  ja  $B$ . Kaks mängijat, „positiivne“ mängija  $P$  ja „negatiivne“ mängija  $N$ , sooritavad kordamööda käike, ühe käiguga võib  $P$  omistada graafi vabale servale märgi  $+$  ning  $N$  märgi  $-$ . Olemasolevaid märke muuta ei tohi. Mängija  $P$



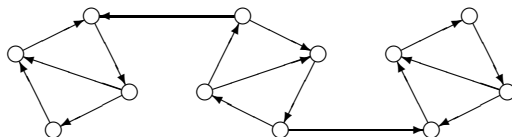
- eesmärk on tähistada märkidega  $+$  mingi ahel tipust  $A$  tippu  $B$ , mängija  $N$  püüab seda takistada. Tõestada, et kui graafil  $G$  leidub kaks aluspuud, millel pole ühiseid servi, siis leidub mängijal  $P$  võitev strateegia, sõltumata sellest, kumb alustab. Näiteks leidub mängijal  $P$  võitev strateegia joonisel kujutatud graafi puhul.
47. Tõestada, et kui Shannoni mängus leidub mängijal  $P$  võitev strateegia graafi  $G$  puhul ja  $G$  on graafi  $H$  alamgraaf, siis leidub mängijal  $P$  võitev strateegia ka graafi  $H$  puhul.

## VII. SUUNATUD GRAAFID

**1. Suunatud graafi mõiste.** Paljudel juhtudel ei piisa rakendustes olukorra kirjeldamisest niisuguse graafiga, mis näitab ainult seda, kas mingid kaks tippu on omavahel ühendatud. Sageli tuleb arvestada ka servade suundi ja teha vahet serva algus- ning lõpptipu vahel. Seepärast tuuakse sisse suunatud graafi mõiste.

**Definitsioon 1.** *Suunatud graaf on paar  $G = (V, E)$ , kus  $V$  on mittetühi hulk ning  $E$  hulk, mis koosneb hulga  $V$  järjestatud paaridest.*

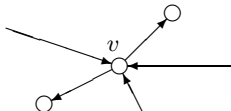
Seega loetakse siin servadeks mitte tippude hulga  $V$  kaheelemendilisi alamhulki, vaid järjestatud paare, nii et paar  $(u, v)$  erineb paarist  $(v, u)$ . Suunatud graafi servi nimetatakse traditsiooniliselt *kaarteks*. Kaare  $(u, v)$  märkimiseks kasutame ikka tähist  $uv$ , kuid erinevalt eelnevast ei tähenda kirjutised  $uv$  ja  $vu$  nüüd enam ühte ja sedasama. Kaare  $uv$  tippu  $u$  nimetatakse kaare *algtipuks*, tippu  $v$  aga *lõpptipuks*. Joonisel tähistab kaart tavaliselt nool algtipust lõpptippu:



Suunatud graafi servad võivad näiteks kujutada ühesuunalisi teid ristmike vahel. Paneme tähele, et graafis võivad korruga esineda kaared  $uv$  ja  $vu$ , niisugust kahekordset kaart võib käsitleda kui kahesuunalist teed. Ka harilikku graafi võib vajaduse korral vaadelda suunatud graafina, kus kõik servad on kahesuunalised.

Kui asendame suunatud graafis kõik kaared suunata servadega (st jätame kaartel suuna ära), siis saame graafi, mida nimetatakse antud suunatud graafi *alusgraafiks*. Võimalik on ka vastupidine operatsioon: määrame graafi kõigile servadele suunad, millega mittesuunatud graaf muutub suunatuks.

Suunatud graafi tippudel tuleb eristada kahte tüüpi astmeid. Tipu *sisendastmeks* nimetatakse sellesse tippu sisenevate kaarte arvu ning *väljundastmeks* sealt väljuvate kaarte arvu. Tipu  $v$  sisendastme tähiseks on  $d_+(v)$ , väljundastme tähiseks aga  $d_-(v)$ . Näiteks joonisel



on tipu  $v$  puhul  $d_+(v) = 3$  ning  $d_-(v) = 2$ . Tipuastmete summat puudutav teoreem kehtib järgmisel kujul ka suunatud graafide puhul.

**Teoreem 1.** *Igas suunatud graafis on tippude sisendastmete summa võrdne tippude väljundastmete summaga ehk*

$$\sum_{v \in V} d_+(v) = \sum_{v \in V} d_-(v).$$

**Tõestus.** Tippude väljundastmete summa võrdub graafi kaarte arvuga, sest selles võetakse arvesse kõik tippudest väljuvad kaared. Samuti võrdub kõigi sisendastmete summa graafi kaarte arvuga.  $\square$

**Teoreem 2.** *Kui suunatud graafis on iga tipu sisend- ja väljundastmete summa sama, siis*

$$\sum_{v \in V} d_+^2(v) = \sum_{v \in V} d_-^2(v).$$

**Tõestus.** Eeldame, et iga tipu sisend- ja väljundastmete summa on  $d$ . Et

$$d_+^2(v) - d_-^2(v) = (d_+(v) + d_-(v))(d_+(v) - d_-(v)) = d \cdot d_+(v) - d \cdot d_-(v),$$

siis eelmise teoreemi põhjal

$$\sum_{v \in V} d_+^2(v) - \sum_{v \in V} d_-^2(v) = d \sum_{v \in V} d_+(v) - d \sum_{v \in V} d_-(v) = 0.$$

Seega on tõestatava võrduse vasak ja parem pool võrdsed.  $\square$

Tippude järjendit  $v_0, v_1, \dots, v_k$ , kus iga kaks järjestikust tippu  $v_i$  ja  $v_{i+1}$  on ühendatud kaarega  $v_i v_{i+1}$ , nimetatakse *suunatud ahelaks*. Kui ükski tipp ei kordu, siis on tegemist *suunatud lihtahelaga*. Kummalgi juhul võib ahel lõppeda samas tipus, kus algab, vastavalt räägitakse siis *suunatud tsüklis* või *suunatud lihttsüklis*. Paneme tähele, et suunatud ahelas või tsüklis peavad kõik kaared olema orienteeritud ühtepidi. Analoogiliselt saab suunatud graafide juhule üle kanda ka teisi mõisteid, näiteks vaadelda Euleri või Hamiltoni tsüklit. Suunatud graafe nimetatakse *isomorfseteks*, kui nende tippude hulkade vahel leidub üksühene vastavus  $\varphi$ , mis arvestab nii tippude ühendatust kui ühenduse suunda: esimeses graafis leidub kaar tipust  $u$  tippu  $v$  parajasti siis, kui teises graafis leidub kaar tipust  $\varphi(u)$  tippu  $\varphi(v)$ .

Kui graafi mingist tipust kaared ainult väljuvad, siis nimetatakse sellist tippu graafi *sisendiks*. Tippu, kuhu kaared ainult sisenevad, nimetatakse vastavalt graafi *väljundiks*. Arusaadavalt võib ühel graafil olla mitu sisendit ja/või väljundit.

**Teoreem 3.** *Kui suunatud graafis pole suunatud tsükleid, siis leidub graafil vähemalt üks sisend ja vähemalt üks väljund.*

**Tõestus.** Valime graafis ühe tipu  $v$ . Kui see pole graafi väljund, siis liigume mööda väljuvat kaart naabertippu. Kui ka see ei ole graafi väljund, siis liigume mööda väljuvat kaart järgmise naabertippu jne,

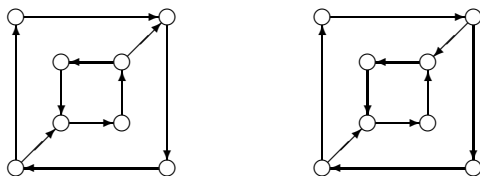
igal sammul valime seejuures sihtpunktiks sellise naabertipu, kus me varem pole viibinud. Niisugune teekond saab lõppeda kahel põhjusel: kas jõuame tippu, kust ükski kaar ei välju, või tippu, kust kõik kaared viivad juba külastatud tippudesse. Teine juht pole võimalik, sest siis leiduks graafis tsükel.

Seega peab graafis leiduma väljund. Sisendi leidmiseks kordame sama arutust, liikudes mööda kaari vastupidises suunas.  $\square$

**2. Tugev ja nõrk sidusus.** Seoses servadele suuna andmisega saab rääkida kahest sidususe mõistest sõltuvalt sellest, kas me ühest tipust liigume teise suundi arvestades või neid arvestamata. Suunatud graafi nimetatakse *tugevalt sidusaks*, kui iga kahe tipu  $u$  ja  $v$  korral leidub suunatud ahel tipust  $u$  tippu  $v$ . Suunatud graafi nimetatakse *nõrgalt sidusaks*, kui tema alusgraaf on sidus.

Piltlikult öeldes tähendab tugev sidusus seda, et graafi igast tipust on võimalik liikuda mööda nooli igasse teise tippu, nõrk sidusus on aga samaväärne hariliku sidususega: kustutame kaartelt nooled ja vaatame, kas järelejäänud graaf on sidus.

Järgmisel joonisel on vasakpoolne graaf tugevalt sidus, sest igast tipust pääseb mööda kaari igasse teise tippu. Parempoolne graaf on küll nõrgalt sidus, aga mitte tugevalt, sest keskmisest neljast tipust pole võimalik liikuda ühessegi välimisest neljast tipust:

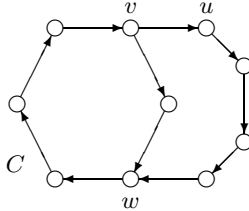


Iga tugevalt sidus graaf on ka nõrgalt sidus, sest kui graafi ühest tipust saab liikuda teise mööda suunatud ahelat, siis on need tipud ahelaga ühendatud ka juhul, kui kaarte suunda määravad nooled kustutada. Vastupidine aga ei kehti: nagu jooniselt näha, leidub nõrgalt sidusaid graafe, mis pole tugevalt sidusad. Lisaks tähendab graafi tugev sidusus seda, et graafil (kui ta pole ühetipuline) ei leidu ühtegi sisendit ega ühtegi väljundit: iga tipu juures peab leiduma vähemalt üks sisenev ja vähemalt üks väljuv kaar, muidu poleks võimalik kas teistest tippudest sinna jõuda või sealt mujale liikuda. Sisendeid ja väljundeid sisaldav graaf saab olla ainult nõrgalt sidus. Vastupidine jällegi ei kehti: kui nõrgalt sidusas graafis pole sisendeid ega väljundeid, siis ei tähenda see veel, et graaf oleks tugevalt sidus, selles veendumiseks sobib samuti eelmise joonise parempoolne graaf.

Tugeva ja nõrga sidususe vahekorda iseloomustab veel järgmine omadus.

**Teoreem 4.** *Kui sidusas graafis ei leidu ühtegi silda, siis saab tema servadele määrata suunad nii, et tekkinud graaf on tugevalt sidus.*

**Tõestus.** Et graafis pole sildu, siis leidub seal vähemalt üks tsükel  $C$ . Orienteerime tsükli kõik servad ühtepidi, nii on võimalik liikuda sellel igast tippust igasse teise. Kui tsükel  $C$  ei haara graafi kõiki tip-



pe, siis leidub serv, mis ühendab tsükli mingit tippu  $v$  välise tipuga  $u$ . Serv  $uv$  ei ole sild, järelikult leidub peale tema veel mingi ahel tipust  $u$  tippu  $v$ . Olgu  $w$  sellel ahelal tipu  $u$  poolt lugedes esimene tipp, mis kuulub tsükklisse  $C$ . Määrame servale  $uv$  suuna tipust  $v$  välja ning ahela  $u \dots w$  servadele suuna tipu  $u$  poolt tipu  $w$  poole. Omavahel kaartega ühendatud tippude hulgas pääseb nüüd ikka igast tipust igasse teise. Nii viisi jätkates seome kaartega kõik graafi tipud, kasutamata jäänud servadele võib omistada ükskõik millise suuna.  $\square$

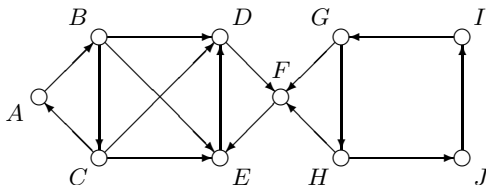
Teiselt poolt on ilmne, et tugevalt sidusas graafis pole ühtegi silda, sest sillaks oleva kaare lõpptipust pole võimalik pääseda algtippu.

Tugeva sidususe mõttes jaguneb graaf sidusateks komponentideks nii nagu hariliku sidususe puhulgi. Sidus komponent tugeva sidususe mõttes on selline tugevalt sidus alamgraaf, mis ei sisaldu üheski teises tugevalt sidusas alamgraafis. Ükski tipp ei saa kuuluda korraga mitmesse komponenti ning komponendid üheskoos katavad graafi kõik tipud. Graaf on tugevalt sidus parajasti siis, kui tal on täpselt üks tugevalt sidus komponent.

Ehkki joonisel pole need komponendid nii lihtsasti eraldatavad kui sidusad komponendid harilikus mõttes, võib neid leida järgmise meetodiga. Valime graafis mingi tipu  $u$  ja määrame kõik tipud  $v$ , mille korral leidub suunatud ahel tipust  $u$  tippu  $v$  ja tipust  $v$  tippu  $u$ . Niisugune tippude hulk koos tipuga  $u$  moodustabki tugevalt sidusa komponendi: iga kahe tippu vahel leidub suunatud ahel ühest tipust teise – kui mitte otse, siis kindlasti läbi tipu  $u$ , samuti ei saa sinna ühtegi tippu lisada, sest vastasel korral oleks see tipp pidanud olema kahepidises seoses tipuga  $u$ . Kustutame nüüd kõik need tipud graafist ning allesjäänud graafi puhul kordame sama protseduuri.



Näide 1. Leida järgmise graafi tugevalt sidusad komponendid:



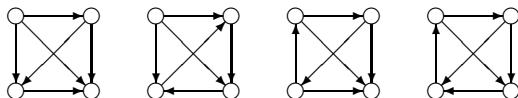
Vaatleme tippu  $A$ . Tipust  $A$  saab liikuda tippu  $B$  ja tipust  $B$  tipu  $A$ . Teine samasuguse omadusega tipp on  $C$  ning see on ka kõik. Järelikult moodustavad tipud  $A, B, C$  ühe tugevalt sidusa komponendi. Jätame need tipud koos intsidentsete kaartega graafist välja ja vaatleme ülejäänud tippe.

Tipust  $D$  saab liikuda tippudesse  $F$  ja  $E$  ning kummastki saab tulla tagasi tippu  $D$ . Et rohkem niisuguseid tippe ei ole, moodustavad tipud  $D, E, F$  teise tugevalt sidusa komponendi. Kustutades need tipud graafist, jääb järele tsükkel  $GHJI$ , mis on kolmas komponent.

Kokkuvõttes on graafil tugeva sidususe mõttes kolm komponenti:  $\{A, B, C\}$ ,  $\{D, E, F\}$  ja  $\{G, H, I, J\}$ . Lihtne on näha, et esimese komponendi igast tipust saab liikuda teise komponendi igasse tippu, kuid mitte vastupidi. Samamoodi ei saa teise komponendi tippudest liikuda kolmanda komponendi tippudesse.

**3. Turniirid.** Kui omistame täisgraafi igale servale suuna, siis saame suunatud graafi, mida nimetatakse *turniiriks*. Niisugune nimi tuleneb analoogiast võrkpalli- vms turniiriga, kus iga osavõtja peab iga teisega ühe mängu. Eeldades, et mängud ei saa lõppeda viigiga, seame osavõtjatele vastavusse graafi tipud ning tõmbame kaare suunaga võitjast kaotajani. Üheringilise turniiri lõpptulemust kirjeldab siis graaf, kus iga kahe tipu vahel on kaar.

Näiteks leidub erinevaid (mitteisomorfseid) neljatipulisi turniire üldse neli tükki – kui nelja meeskonna omavahelistes mängudes ei esine viike, siis võib tekkida ainult neli üksteisest põhimõtteliselt erinevat turniiritabelit:



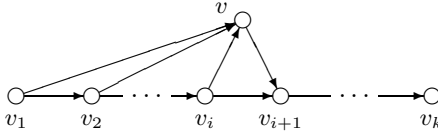
**Teoreem 5.** Igas turniiris leidub suunatud lihtahel, mis läbib turniiri kõiki tippe.

**Tõestus.** Tõestame väite induktsiooniga tippude arvu  $n$  järgi.

**Baas.** Kui  $n = 2$ , siis väide kehtib.

*Samm.* Eeldame, et väide kehtib kõigi  $k$ -tipuliste turniiride korral, ning vaatleme turniiri, mis sisaldab  $k + 1$  tippu. Kustutame ajutiselt graafist ühe tipu  $v$ . Ülejäänud  $k$  tippu moodustavad „alamturniiri“, kus vastavalt induktsiooni eeldusele leidub kõiki tippe läbiv suunatud lihtahel  $v_1 v_2 \dots v_k$ . Paneme nüüd tipu  $v$  tagasi.

Kui tipust  $v$  viib kaar tippu  $v_1$ , siis saame ahelat pikendada algusest: lihtahel  $vv_1 v_2 \dots v_k$  läbib graafi kõiki tippe. Kui tippu  $v$  siseneb kaar esimesest  $i$  tipust  $v_1, \dots, v_i$ , kus  $i = 1, 2, \dots, k - 1$ , ja



esimene väljuv kaar viib tippu  $v_{i+1}$ , siis saame tipu  $v$  lisada ahelasse  $v_i$  ja  $v_{i+1}$  vahele:  $v_1 \dots v_i v v_{i+1} \dots v_k$ . Kui tipust  $v$  ühtegi kaart ei välju, siis saame tipu  $v$  lisada ahela lõppu:  $v_1 v_2 \dots v_k v$ . Kõigil juhtudel oleme leidnud suunatud lihtahela, mis läbib graafi kõiki tippe.  $\square$

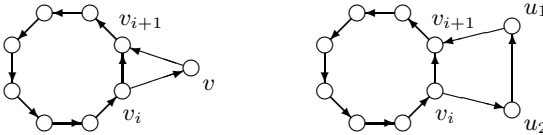
Siit järeldub, et näiteks võrkpalliturniiril saab kõik võistkonnad järjestada nii, et igaüks neist on võitnud järgnevat.

**Teoreem 6.** *Kui turniir on tugevalt sidus, siis leidub seal suunatud lihtsükkel, mis läbib kõiki tippe.*

Seega, igas tugevalt sidusas turniiris leidub Hamiltoni tsükkel.

*Tõestus.* Et tugevalt sidusal graafil pole sisendeid ega väljundeid, siis järeldub teoreemist 3, et vaadeldavas turniiris leidub mingi suunatud lihtsükkel  $C$ . Näitame, et tsükli saab järk-järgult pikendada, kuni ta haarab graafi kõik tipud.

Kui tsükklisse  $C$  mittekuuluvate tippude seas leidub selline tipp  $v$ , et kaared tipu  $v$  ja tsükli tippude vahel pole kõik samasuunalised, siis olgu  $v_i$  piki tsükli liikudes viimane tipp, pärast mida tippu  $v$  sisenevad kaared asenduvad tipust  $v$  väljuvate kaartega. Sellelt kohalt saame tsükli pikendada, asendades kaare  $v_i v_{i+1}$  ahelaga  $v_i v v_{i+1}$ .



Kui niisugust tippu  $v$  ei leidu, siis jagunevad kõik tsükklisse  $C$  mittekuuluvad tipud kahte klassi: need, millest viib kaar igasse tsükli tippu, ja need, millesse siseneb kaar igast tsükli tipust. Kumbki klass ei saa olla tühi. Siis peab esimeses klassis leiduma tipp  $u_1$  ja teises tipp  $u_2$  nii, et nendevaheline kaar on suunaga  $u_2 u_1$ , sest kui kõik kaared viiksid ainult esimesest klassist teise, siis ei saaks teisest klassist

liikuda väljapoole. Valides tsüklis  $C$  kaks järjestikust tippu  $v_i$  ja  $v_{i+1}$ , saame nüüd kaare  $v_i v_{i+1}$  asendada ahelaga  $v_i u_2 u_1 v_{i+1}$ .  $\square$

**4. Lühima tee leidmine.** Graafi tugevalt sidusate komponentide määramisel pidime leidma, kas ühest tipust viib teise suunatud ahel. Lihtsate graafide puhul pole see ülesanne raske, kuid võib vähegi suuremate graafide puhul muutuda üsnagi tülikaks.

Taalised ülesanded esinevad rakendustes väga sageli, kusjuures eesmärgiks pole mitte ainult teha kindlaks ahela olemasolu, vaid leida kõikide ahelate hulgast teatavas mõttes optimaalne. Näiteks kui suunatud graaf esitab teedevõrku ning teada on iga tee pikkus või selle läbimiseks kuluv aeg, siis huvitab meid kindlasti lühim või kiireim tee ühest punktist teise. Kui graaf kujutab sidekanalite võrku, kus iga kanal ei tarvitse olla absoluutselt usaldusväärne, siis võib ülesandeks seada suurima usaldusväärsusega tee leidmise kahe võrgusõlme vahel. Või siis kirjeldab graaf aine molekulide vahelisi keemilisi sidemeid ning leida tuleb ahel, mis vahendab kahe antud molekuli vahel kõige nõrgemat sidet.

Üldkujulise ülesande võib sõnastada järgmiselt. Antud on suunatud graaf  $G$ , mille igale kaarele on omistatud mittenegatiivse reaalarvuga väljendatud kaal. Kaare kaalu nimetame kaare kaalutud pikkuseks, ahela kaalutud pikkus on tema kaarte kaalutud pikkuste summa. Leida kahe fikseeritud tipu vahel vähima kaalutud pikkusega suunatud ahel. Niisuguse ülesande lahendamiseks esitasid 1962. aastal meetodi ameerika matemaatikud Stephen Warshall ja Robert Floyd, autorite järgi kannab see nime *Floyd-Warshalli algoritm*.

**Floyd-Warshalli algoritm.** Olgu  $G$  kaalutud suunatud  $n$ -tipuline graaf, mille tipud on nummerdatud naturaalarvudega  $1, 2, \dots, n$ . Algoritm kasutab kahte  $n \times n$ -maatriksit  $A$  ja  $B$ .

- Omistada maatriksi  $A$  iga elemendi  $a_{ij}$  väärtuseks kaare  $ij$  kaal; kui seda kaart graafis pole, siis omistada väärtuseks  $\infty$ . Maatriksi  $B$  iga elemendi  $b_{ij}$  väärtuseks omistada arv  $j$ .
- Iga  $k = 1, 2, \dots, n$  korral, iga  $i = 1, 2, \dots, n$  korral, iga  $j = 1, 2, \dots, n$  korral: kui  $a_{ik} + a_{kj} < a_{ij}$ , siis asendada  $a_{ij}$  väärtus arvuga  $a_{ik} + a_{kj}$  ja  $b_{ij}$  väärtus arvuga  $b_{ik}$ .

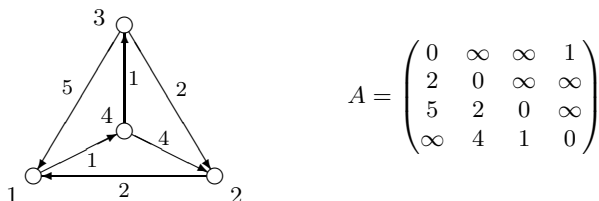
Tulemuseks on maatriksid  $A$  ja  $B$ .

Maatriksi  $A$  elemendi  $a_{ij}$  väärtus tähistab tipust  $i$  tippu  $j$  siirduva lühima ahela kaalutud pikkust, maatriksi  $B$  elemendi  $b_{ij}$  väärtus aga selle ahela esimest vahetippu. Algoritm leiab seega lahendi korraga kõigi tipupaaride jaoks.

Vaatleme, kuidas toimub lühima ahela leidmine tipust  $i$  tippu  $j$ . Töö alguses loeb algoritm parimaks ahelaks otsetee: kaare tipust  $i$  tippu  $j$ . Iga  $k = 1, 2, \dots, n$  korral kontrollitakse, kas seni leitud lühima ahela saab asendada veel lühemaga, kui teha põige läbi tipu  $k$ , st liikuda mööda kõige lühemat selle hetkeni leitud ahelat tipust  $i$  tippu  $k$  ja seejärel tipust  $k$  tippu  $j$ . Kui jah, siis jäetakse meelde sellise ahela pikkus ja esimene vahetipp.

Kahe tipu vahelisel lühimal ahelal ei saa ükski tipp esineda rohkem kui üks kord. Kui kontrollimisjärg jõuab suurima numbriga tipuni, mida lühim ahel läbib, siis leitakse see lühim ahel ka üles, sest tema osad tipust  $i$  suurima numbriga tipuni ja suurima numbriga tipust tipuni  $j$  on leitud juba eelmistel sammudel.

*Näide 2.* Leida Floyd-Warshalli algoritmiga tippudevahelised lühimad teed joonisel vasakul kujutatud graafis:



Maatriksi  $A$  elementide väärtused algoritmi töö alguses on näidatud joonisel paremal. Pärast iga sammu saame järgmised maatriksid:

$$\begin{pmatrix} 0 & \infty & \infty & 1 \\ 2 & 0 & \infty & 3 \\ 5 & 2 & 0 & 6 \\ \infty & 4 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & \infty & \infty & 1 \\ 2 & 0 & \infty & 3 \\ 4 & 2 & 0 & 5 \\ 6 & 4 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & \infty & \infty & 1 \\ 2 & 0 & \infty & 3 \\ 4 & 2 & 0 & 5 \\ 5 & 3 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 4 & 2 & 1 \\ 2 & 0 & 4 & 3 \\ 4 & 2 & 0 & 5 \\ 5 & 3 & 1 & 0 \end{pmatrix}$$

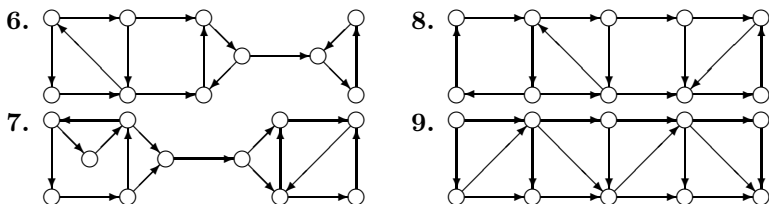
Viimase maatriksi element, mis asub reas  $i$  ja veerus  $j$ , näitabki lühima tee pikkust tipust  $i$  tippu  $j$ .

## Ülesanded

1. Graafi tippudeks on kahendarvud  $000, 001, \dots, 111$ , kaared viivad parajasti tipust  $b_1b_2b_3$  tippu  $b_2b_3b_4$ . Leida selles graafis suunatud tsüklil, mis läbib kõik tipud täpselt üks kord. Paigutada ringjoonele neli numbrit 0 ja neli numbrit 1 nii, et tekkiv ringjärjend sisaldab kõiki kahendarve  $000, 001, \dots, 111$ .
2. Paigutada ringjoonele kaheksa numbrit 0 ja kaheksa numbrit 1 nii, et tekkiv ringjärjend sisaldab kõiki neljakohalisi kahendarve  $0000, 0001, \dots, 1111$ .

3. Suunatud graafi  $G$  tippudeks loeme kõik kahendarvud pikkusega  $n$ , kusjuures igast arvust  $b_1 b_2 \dots b_n$  viib kaar erineva arvuni  $b_2 b_3 \dots b_n b_{n+1}$ . Tõestada, et graafis  $G$  leidub: a) suunatud ahel, mis läbib kõik servad täpselt üks kord; b) suunatud tsükkel, mis läbib kõik tipud täpselt üks kord.
4. Tõestada, et sidusas suunatud graafis leidub Euleri tsükkel parajasti siis, kui iga tipu  $v$  korral  $d_+(v) = d_-(v)$ .
5. Suunatud graafis  $G$  leidub kaks tippu  $a$  ja  $b$ , mis rahuldavad tingimust  $d_+(a) - d_-(a) = d_-(b) - d_+(b) = k$ , iga ülejäänud tipu  $v$  korral aga  $d_+(v) = d_-(v)$ . Tõestada, et graafis  $G$  leidub  $k$  paarikaupa ühiste kaarteta suunatud lihtahelat, mis kõik viivad tipust  $a$  tipu  $b$ .

Leida järgmiste graafide tugevalt sidusad komponendid.



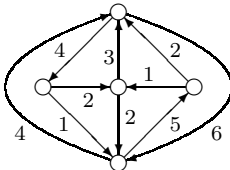
10. Rahvusvahelise konverentsi eel vaatas tõlkekeskus üle oma ressursid ja leidis, et konverentsil kasutamiseks on tal olemas järgmised tõlgid: eesti-läti, islandi-eesti, islandi-rootsi, leedu-rootsi, läti-islandi, läti-leedu, norra-läti, norra-poola, poola-eesti, poola-vene, rootsi-läti, soome-norra, soome-taani, taani-vene, vene-soome (iga tõlk tõlgib ainult võõrkeelest emakeelde, tõlgi emakeel on nimetatud teisena). Kas tõlkekeskus saab teha tõlkeid igast keelest igasse teise keelde? Kui ei saa, siis milline on vähim tõlkide arv, mis tuleb juurde muretseda, et iga kahe keele vahel tõlkimine võimalik oleks, ja milliste keelte vahel need tõlgid peavad tõlkima?
11. Kuidas võib muutuda suunatud graafi tugevalt sidusate komponentide arv, kui graafile lisada juurde üks kaar?
12. Kas tugevalt sidusas graafis võib leiduda eraldavaid tippe?
13. Tõestada, et suvalise graafi servad võib orienteerida nii, et ühegi tipu sisendaste ja väljundaste ei erine rohkem kui ühe võrra.
14. Teatavas riigis on  $n$  linna ( $n \geq 5$ ). Iga kahte linna ühendab tee. Väljaspool linnu teed ei lõiku (kasutatakse viadukte). Tõestada, et teedel saab kehtestada ühesuunalise liikluse nii, et igast linnast

võib pääseda igasse teise linna, sõites kas mööda neid kahte linna ühendavat teed või läbi mingi kolmanda linna.

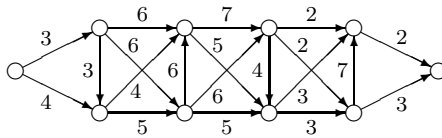
15. Olgu  $G$  turniir ja  $v$  tema suurima väljundastmega tipp. Tõestada, et tipust  $v$  viib turniiri  $G$  igasse teise tippu ahel, mille pikkus pole suurem kui 2.
16. Tõestada, et kui turniir  $G$  ei ole tugevalt sidus, siis leidub üks kaar, mille suuna vahetamisel  $G$  muutub tugevalt sidusaks.
17. Olgu  $G$  tugevalt sidus  $n$ -tipuline turniir, kusjuures  $n \geq 4$ . Valime suvalise täisarvu  $k$  nii, et  $3 \leq k \leq n - 1$ . Tõestada, et turniiri  $G$  iga tipp kuulub teatavasse suunatud tsükklisse, mille pikkus on  $k$ .

Leida tippudevahelised lühimad teed järgmistes graafides (kaks esimest on suunatud, kaks viimast aga suunamata graafid).

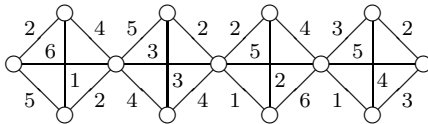
18.



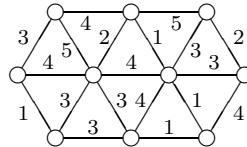
19.



20.



21.



22. Floyd-Warshalli algoritmi juures eeldasime, et iga kaare kaal on mittenegatiivne. Kui mõne kaare kaal on negatiivne, siis võib juhtuda, et vähima kaaluga ahelat ühest tipust teise ei leidu. Tuua näide sellise olukorra kohta.
23. Graafi iga kaare  $e$  kohta on teada kaare läbimise tõenäosus  $p(e)$ , kusjuures  $0 \leq p(e) \leq 1$ . Ahela läbimise tõenäosus võrdub tema kaarte tõenäosuste korrutisega. Koostada algoritm kõige usaldusväärsema (kõige suurema läbimistõenäosusega) ahela leidmiseks tipust  $u$  tippu  $v$ .
24. Teatava toote valmistamiseks tuleb sooritada kümme erinevat tööoperatsiooni  $A_1, A_2, \dots, A_{10}$ , igaüks võtab aega 10 minutit. Operatsioonid  $A_1, A_3$  ja  $A_5$  ei nõua eeltöid. Töö  $A_2$  tegemiseks peavad olema tehtud tööd  $A_8$  ja  $A_6$ , töö  $A_4$  eeldab töid  $A_5$  ja  $A_1$ , töö  $A_6$  eeldab töid  $A_7$  ja  $A_4$ , töö  $A_7$  eeldab tööd  $A_3$ , töö  $A_8$  eeldab töid  $A_4$  ja  $A_7$ , töö  $A_9$  eeldab töid  $A_2$  ja  $A_6$  ning töö  $A_{10}$  eeldab tööd  $A_9$ . Kui kiiresti on võimalik toode valmis teha?

## VIII. RELATSIOONID

**1. Relatsiooni mõiste.** Igapäevases elus on tihti vaja analüüsida olukordi, kus mingid objektid on üksteisega teataval viisil seotud. Sageli puutume kokku sugulusseosega või tutvusseosega: kas kaks inimest on omavahel sugulased või tuttavad. Teineteisega võib seostada näiteks raamatu ja autori, koera ja omaniku, poldi ja temale sobiva mutri või kaks riiki, mis on teineteise naabrid. Ei ole oluline, kas omavahel seotud objektid kuuluvad samasse klassi või erinevatesse klassidesse. Sarnaseid näiteid on lihtne tuua teisigi.

Mitmesuguseid seoseid esineb laialt ka matemaatikas. Näiteks võime lugeda kahte hulka  $A$  ja  $B$  seotuks, kui üks on teise alamhulk. Suvalised kaks reaalarvu  $x$  ja  $y$  võivad olla sama märgiga või kindlas suurusvahekorras, nende vahel võib kehtida võrdus  $x^2 + y^2 = 1$  jne. Niisuguste olukordade kirjeldamiseks ja nendes esinevate seaduspärasuste kindlakstegemiseks tuleb seose mõistele anda matemaatilisel tähendusel põhinev definitsioon.

Mittetühjade hulkade  $X$  ja  $Y$  otsekorrutis  $X \times Y$  on kõigi niisuguste paaride  $(x, y)$  hulk, kus  $x \in X$  ja  $y \in Y$ . Teiste sõnadega,

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Näiteks hulkade  $X = \{a, b\}$  ja  $Y = \{1, 2, 3\}$  otsekorrutis  $X \times Y$  koosneb järgmisest kuuest paarist:

$$(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3).$$

Kui  $X$  ja  $Y$  on lõplikud hulgad, siis on  $X \times Y$  elementide arv korrutamise reegli põhjal võrdne  $X$  ja  $Y$  elementide arvude korrutisega:

$$|X \times Y| = |X| \cdot |Y|.$$

**Definitsioon 1.** Hulga  $X \times Y$  iga alamhulka  $\mathcal{R}$  nimetatakse *relatsiooniks* ehk *seoseks* hulkade  $X$  ja  $Y$  vahel.

Seega valime kõigist otsekorrutisse  $X \times Y$  kuuluvatest elemendipaaridest  $(x, y)$  välja need, mille komponendid on omavahel seotud, selliste paaride hulk moodustabki relatsiooni  $\mathcal{R}$ . Kui hulk  $\mathcal{R}$  sisaldab teatavat paari  $(x, y)$ , siis öeldakse, et elemendid  $x$  ja  $y$  on relatsioonis  $\mathcal{R}$  (ehk kuuluvad relatsiooni  $\mathcal{R}$  ehk relatsioon  $\mathcal{R}$  kehtib elementide  $x$  ja  $y$  korral). Kirjutise  $(x, y) \in \mathcal{R}$  asemel kirjutatakse ka  $x\mathcal{R}y$ .

Siin vaadeldavaid relatsioone nimetatakse ka *kahekohalisteks* ehk *binaarseteks*, sest nad kehtivad kahe objekti vahel. Harvemini esineb relatsioone, mis seovad suuremat arvu objekte, sel juhul räägitakse siis vastavalt kolmekohalistest, neljakohalistest jne relatsioonidest.

Ülaltoodud definitsioon ei sea mingeid kitsendusi sellele, milline alamhulk  $\mathcal{R}$  olla võib. Erijuhul, kui  $\mathcal{R}$  on tühi hulk, st ei sisalda ühtegi

paari, on tegemist *tühirelatsiooniga*  $\emptyset$ . Teise äärmusena võib hulk  $\mathcal{R}$  hulgaga  $X \times Y$  kokku langeda, niisugune relatsioon on *täisrelatsioon*. Viimast märgitakse mõnikord ka sümboliga  $\mathcal{U}$ .

Kui hulgad  $X$  ja  $Y$  relatsiooni definitsioonis ühtivad, siis räägitakse *relatsioonist hulgal*  $X$ . Üks selline on näiteks ka *samasusrelatsioon* ehk *võrdus*  $\mathcal{I}$ , kuhu kuuluvad parajasti kõik need paarid, mille komponendid on võrdsed. Seega

$$\mathcal{I} = \{(x, x) : x \in X\}.$$

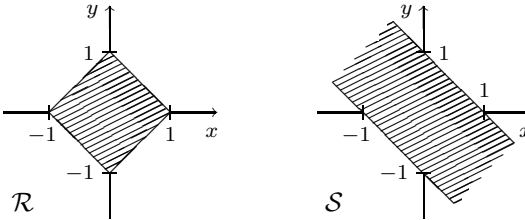
Toome nüüd relatsiooni mõiste selgituseks mõned näited.

*Näide 1.* Olgu  $X = \{a, b, c, d, e, f, g, h\}$  ja  $Y = \{1, 2, 3, 4, 5, 6, 7, 8\}$ . Kaks elementi  $x \in X$  ja  $y \in Y$  loeme seotuks parajasti siis, kui nad koos määravad tavalisel malelual musta värvi välja. Niiviisi saame relatsiooni  $\mathcal{R} \subseteq X \times Y$ , mis koosneb 32 paarist

$$(a, 1), (a, 3), (a, 5), (a, 7), (b, 2), \dots, (h, 8)$$

See relatsioon on 64-elementilise hulga  $X \times Y$  alamhulk.

*Näide 2.* Olgu  $X = Y = \mathbb{R}$ , st vaatleme relatsioone reaalarvude hulgal. Loeme, et reaalarvud  $x$  ja  $y$  on relatsioonis  $\mathcal{R}$  parajasti siis, kui kehtib võrratus  $|x| + |y| \leq 1$ , ning relatsioonis  $\mathcal{S}$  parajasti siis, kui kehtib võrratus  $|x + y| \leq 1$ . Kumbki relatsioon on alamhulk otsekorrutises  $\mathbb{R} \times \mathbb{R}$ , nii et neid võib kujutada tasandi punktihulkadena:



Niisugune geomeetriline interpretatsioon on kasulik siis, kui reaalarvude hulgal määratud relatsioonidega tuleb teostada tehteid.

*Näide 3.* Olgu  $X = Y = \mathbb{N}$ . Kõik aritmeetikast tuntud seosed  $<$ ,  $\leq$ ,  $>$ ,  $\geq$ ,  $=$ ,  $\neq$  on relatsioonid eelneva definitsiooni mõttes: näiteks järjestuses  $<$  tähendab naturaalarvupaaride hulka  $\{(x, y) : x < y\}$ , kus igas paaris on esimene komponent väiksem kui teine. Samuti näeme siin juhtu, mil kahe elemendi vahelist relatsiooni on kombeks panna kirja kujul  $x\mathcal{R}y$ , mitte kujul  $(x, y) \in \mathcal{R}$ .

*Näide 4.* Olgu  $X$  mingi programmi  $P$  moodulite hulk ja  $(x, y) \in \mathcal{R}$  parajasti siis, kui moodul  $x$  kutsus programmis  $P$  välja mooduli  $y$ .



Näide 5. Olgu  $X$  kõigi inimeste hulk. Siis võime defineerida relatsioone  $\mathcal{R} = \{(x, y) : x \text{ on } y\text{-i isa}\}$  ja  $\mathcal{S} = \{(x, y) : x \text{ on } y\text{-i ema}\}$ . Niiviisi saab relatsiooni mõiste abil kirjeldada ka inimestevahelisi sugulussidemeid.

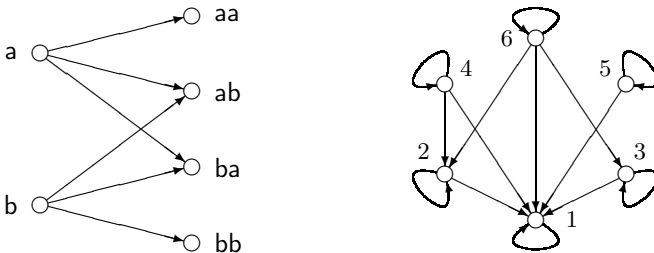
**2. Relatsioonide esitusviisid.** Relatsiooni määramiseks on mitu võimalust. Milline neist on kõige sobivam, sõltub konkreetsest eesmärgist. Eeldame siinkohal, et hulgad, mille vahel relatsioon defineeritakse, on lõplikud.

Kui relatsioon kehtib väheste elementide vahel, siis võib teda lihtsalt ette anda paaride loendina. Vaatleme näiteks neljaelemendilisel hulgal  $X = \{1, 2, 3, 4\}$  määratud relatsiooni  $\mathcal{R}$ , mis kehtib kahe arvu  $x$  ja  $y$  vahel parajasti siis, kui nende arvude sõnalisel kujul ei leidu ühist tähte („sõltumatud arvud“). Lihtne on üle kontrollida kõik arvupaarid ning tulemuseks saame

$$\mathcal{R} = \{(1, 4), (2, 4), (4, 1), (4, 2)\}.$$

Teise võimalusena võib relatsiooni esitada suunatud graafi abil. Kujutame hulga  $X$  elemente ja hulga  $Y$  elemente punktidenäidena joonisel ning tõmbame kaare elementidest  $x \in X$  elementini  $y \in Y$  parajasti siis, kui paar  $(x, y)$  kuulub vaadeldavasse relatsiooni. Niimoodi saame graafi, milles kõik kaared viivad ainult hulgast  $X$  hulka  $Y$  ning kus pole ühtegi kaart kummagi hulga sees.

Näiteks olgu  $X$  tähtede hulk  $\{a, b\}$  ning  $Y$  kõigi kahetäheliste sõnade hulk, mida saab neist tähtedest koostada, st  $Y = \{aa, ab, ba, bb\}$ . Loeme, et täht  $x$  ja sõna  $y$  on relatsioonis  $\mathcal{R}$ , kui täht  $x$  esineb sõnas  $y$ . Seda relatsiooni esitab vasakul kujutatud graaf:



Kui hulgad  $X$  ja  $Y$  langevad kokku, siis võime relatsiooni esitada suunatud graafiga, mille tippude hulk on  $X$  ning milles on tõmmatud kaar tipust  $x$  tippu  $y$  kõikide relatsiooni kuuluvate paaride  $(x, y)$  korral. Et relatsioon võib sisaldada paare, mille komponendid on võrdsed, siis võib saadud graaf, erinevalt eelnevas vaadeldud suunatud graafidest, sisaldada ka silmuseid. Graaf, mis kujutab samasusrelatsiooni, koosnebki ainult silmustest. Ülemisel joonisel paremal antud

graaf kujutab näiteks jaguvusrelatsiooni hulgal  $X = \{1, 2, 3, 4, 5, 6\}$ , st tipust  $x$  viib kaar tippu  $y$  parajasti siis, kui arv  $x$  jagub arvuga  $y$ .

Suunatud graafide ja relatsioonide vahel on täielik analoogia: igale suunatud graafile, kus võib esineda silmuseid, vastab relatsioon ja igale relatsioonile graaf. Sisuliselt on siin tegemist ühe ja sama objekti kirjeldamisega erinevate vahendite abil. Matemaatiliste mudelite konstrueerimisel ja analüüsimisel kasutatakse valdavalt relatsioone; kui aga oluline on seoste näitlikustamine, siis eelistatakse graafe.

Relatsiooni hulkade  $X = \{x_1, x_2, \dots, x_m\}$  ja  $Y = \{y_1, y_2, \dots, y_n\}$  vahel saab ette anda ka maatriksiga, mille mõõtmed on  $m \times n$ , kusjuures reas  $i$  ja veerus  $j$  asub väärtus 1, kui elemendipaar  $(x_i, y_j)$  kuulub relatsiooni, ning väärtus 0 vastasel korral. Juhul  $X = Y$  saame ruutmaatriksi. Kui  $\mathcal{R}$  on näiteks viimati vaadeldud jaguvusrelatsioon, siis tema maatriks on

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Relatsioonil võib olla mitu maatriksesitust, sest hulkade  $X$  ja  $Y$  elemente võib järjestada mitmel viisil. Seega ei tarvitse kaks erinevat maatriksit kujutada erinevaid relatsioone, segaduste vältimiseks tuleks alati selgelt kindlaks määrata vastavus hulga elementide ja maatriksi ridade või veergude vahel. Maatrikskuju sobib oma kompaktsuse ja ülevaatlikkuse tõttu hästi relatsiooni esitamiseks arvutis.

**3. Ekvivalentsi- ja järjestusrelatsioon.** Praktikasse esinevad sageli teatavate kindlate omadustega relatsioonid. Hulgal  $X$  määratud relatsiooni  $\mathcal{R}$  nimetatakse

- *refleksiivseks*, kui iga  $x \in X$  korral  $(x, x) \in \mathcal{R}$ ;
- *antirefleksiivseks*, kui iga  $x \in X$  korral  $(x, x) \notin \mathcal{R}$ ;
- *sümmeetriliseks*, kui  $(x, y) \in \mathcal{R}$  korral alati  $(y, x) \in \mathcal{R}$ ;
- *antisümmeetriliseks*, kui  $(x, y) \in \mathcal{R}$  ja  $(y, x) \in \mathcal{R}$  korral alati  $x = y$ ;
- *transitiivseks*, kui  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{R}$  korral alati  $(x, z) \in \mathcal{R}$ .

Refleksiivne relatsioon sisaldab endas kõiki paare, mille komponendid on võrdsed. Sellise omadusega on näiteks samasusrelatsioon  $\mathcal{I}$ . Lihtne on näha, et iga muu refleksiivne relatsioon  $\mathcal{R}$  sisaldab endas relatsiooni  $\mathcal{I}$ , st  $\mathcal{I} \subseteq \mathcal{R}$ . Vastupidi, antirefleksiivne relatsioon ei tohi sisaldada ühtegi võrdsete komponentidega paari, st  $\mathcal{I} \cap \mathcal{R} = \emptyset$ .

Relatsioon on sümmeetriline, kui ta koos paariga  $(x, y)$  sisaldab ka vastupidist paari  $(y, x)$ . Sümmeetriline on näiteks relatsioon

$$\mathcal{R} = \{(1, 2), (2, 1), (3, 3), (3, 5), (5, 3)\}.$$

Eelnevas vaadeldud relatsioonidest on sümmeetrilised veel reaalarvude hulgal määratud relatsioonid  $|x| + |y| = 1$  ja  $|x + y| = 1$  ning relatsioonid  $=$  ja  $\neq$ .

Antisümmeetriline relatsioon ei tohi sisaldada korraga paare  $(x, y)$  ja  $(y, x)$ , välja arvatud juhul, kui paari komponendid on võrdsed. See tähendab, et kui  $x \neq y$ , siis võib relatsiooni kuuluda kas paar  $(x, y)$  või  $(y, x)$ , aga mitte mõlemad. Antisümmeetriline on näiteks isaks olemist väljendav relatsioon: kahest erinevast inimesest  $x$  ja  $y$  saab ainult üks olla teise isa, võib ka juhtuda, et pole kumbki. Relatsioon võib olla korraga sümmeetriline ja antisümmeetriline, niisugused on parajasti samasusrelatsioon  $\mathcal{I}$  ja kõik selle alamhulgad.

Transitiivne on ükskõik millisel hulgal määratud jaguvusrelatsioon (näiteks kui 12 jagub 6-ga ja 6 jagub 3-ga, siis 12 jagub 3-ga) ning samuti näiteks relatsioon

$$\mathcal{R} = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 4)\}.$$

Kui võtame kaks paari  $(x, y)$  ja  $(y, z)$  nii, et esimese paari teine ja teise paari esimene komponent ühtivad, siis leidub relatsioonis kindlasti ka paar  $(x, z)$ , mis on moodustatud paaride ülejäänud komponentidest.

Relatsiooni, mis on refleksiivne, sümmeetriline ja transitiivne, nimetatakse *ekvivalentsiks*. Ekvivalents on üks levinumaid relatsioonematematikas, tema mitmekesiseid avaldumisvorme illustreerivad järgmised näited.

*Näide 6.* Suvalisel hulgal  $X$  määratud samasusrelatsioon  $\mathcal{I}$  on ekvivalents. Et samasusrelatsiooni kuuluvad ainult võrdsete komponentidega paarid, rahuldab see relatsioon triviaalselt nii refleksiivsuse, sümmeetrilisuse kui ka transitiivsuse tingimust. Siia kuulub ka kahe arvu võrdusseos  $=$ .

*Näide 7.* Valime hulgaks  $X$  täisarvude hulga  $\mathbb{Z}$  ning fikseerime positiivse täisarvu  $m$ . Määrame relatsiooni  $\mathcal{R}$ , mis kehtib kahe täisarvu  $a$  ja  $b$  puhul parajasti siis, kui need arvud annavad arvuga  $m$  jagades sama jäägi. Selline relatsioon on ekvivalents.

*Näide 8.* Olgu  $X$  kõigi lausearvutusvalemite hulk. Loeme, et kaks valemit on relatsioonis  $\mathcal{R}$  parajasti siis, kui nad on samaväärsed. Niisugune relatsioon on samuti ekvivalents: ta on refleksiivne, sest iga lausearvutusvalem  $F$  on samaväärne iseendaga, samuti sümmeetriline, sest kui valem  $F$  on samaväärne valemiga  $G$ , siis on ka valem  $G$

samaväärne valemiga  $F$ , ta on ka transitiivne, sest kui valem  $F$  on samaväärne valemiga  $G$  ja valem  $G$  valemiga  $H$ , siis on valem  $F$  samaväärne valemiga  $H$ .

*Näide 9.* Olgu  $X$  suunatud graafi  $G$  tippude hulk ning kaks tippu  $u$  ja  $v$  relatsioonis  $\mathcal{R}$  parajasti siis, kui tipust  $u$  viib suunatud ahel tippu  $v$  ning tipust  $v$  viib suunatud ahel tippu  $u$ . Kui teha loomulik kokkulepe, et iga tipp on relatsioonis iseendaga, siis on  $\mathcal{R}$  ekvivalents.

*Näide 10.* Olgu  $X$  ja  $Y$  mingid hulgad ning  $f : X \rightarrow Y$  funktsioon hulgast  $X$  hulka  $Y$ . Defineerime relatsiooni  $\mathcal{R}$  hulgal  $X$  nii, et loeme kahe elemendi  $a \in X$  ja  $b \in X$  puhul  $(a, b) \in \mathcal{R}$  parajasti siis, kui  $f(a) = f(b)$ . Lihtsalt võib veenduda, et  $\mathcal{R}$  on ekvivalents. Kui näiteks  $X$  on kõigi inimeste hulk,  $Y$  mittenegatiivsete täisarvude hulk ning funktsioon  $f$  seab igale inimesele vastavusse tema vanuse, siis seab relatsioon  $\mathcal{R}$  parajasti neid inimestepaare, kelle vanused on võrdsed.

Intuiitiivselt võib ekvivalentsi mõista kui teatavat nõrgemat liiki võrdust, st loeme kahte elementi, mille vahel kehtib ekvivalents, teineteisest teatavas mõttes eristamatuks.

Hulgateoorias tõestatakse, et hulgal  $X$  määratud ekvivalents jagab selle hulga klassideks, seejuures on klassid omavahel lõikumatud ja üheskoos katavad nad kogu hulga  $X$ . Ühte klassi kuuluvad elemendid on kõik omavahel ekvivalentsed. Näites 7 vaadeldud ekvivalentsi puhul koosneb iga klass arvudest, mis annavad jagamisel  $m$ -ga ühesuguse jäägi, näite 9 puhul kujutab iga ekvivalentsiklass parajasti graafi tugevalt sidusat komponenti. Samasusrelatsiooni ehk võrduse puhul on kõik ekvivalentsiklassid üheelemendilised.

Relatsiooni, mis on refleksiivne, antisümmeetriline ja transitiivne, nimetatakse *mitterangeks järjestuseks*, relatsiooni, mis on antirefleksiivne ja transitiivne, aga *rangeks järjestuseks*.

Järjestusrelatsioonide tuntuimad näited on ükskõik millisel arvu hulgal määratud mitterange võrratus  $\leq$  ja range võrratus  $<$ . Võrratus  $\leq$  on refleksiivne, sest iga arvu  $a$  korral  $a \leq a$ , antisümmeetriline, sest võrratustest  $a \leq b$  ja  $b \leq a$  järeljub  $a = b$ , ning transitiivne, sest kui  $a \leq b$  ja  $b \leq c$ , siis  $a \leq c$ . Samuti on võrratus  $<$  antirefleksiivne, sest ühegi arvu  $a$  korral ei saa kehtida  $a < a$ , ning transitiivne.

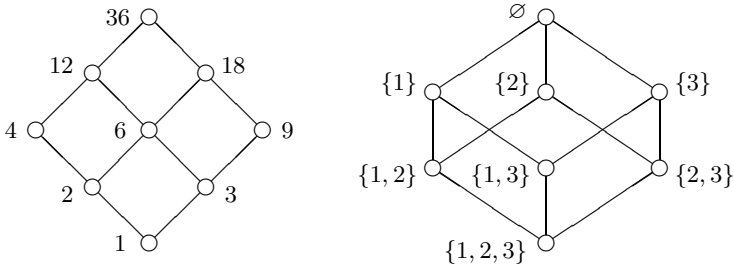
Järjestusrelatsioonid on ka teatava hulga  $A$  kõigi alamhulkade hulgal  $\mathcal{P}(A)$  määratud mitterange sisalduvus  $\subseteq$  ja range sisalduvus  $\subset$ .

Kui  $X$  on naturaalarvude hulk, siis osutub relatsioon  $\mathcal{R}$ , mis kehtib kahe arvu  $x$  ja  $y$  vahel parajasti siis, kui arv  $x$  jagub  $y$ -ga, samuti järjestuseks. Kõigi sõnade hulgal saab määrata leksikograafilise järjestuse, mida kasutatakse näiteks nimestike või sõnaraamatutes sõnaraar-

tiklite sorteerimiseks. Kõik need järjestused rahuldavad definitsiooni tingimusi. Muuhulgas rahuldab mitterange järjestuse tingimusi ka samasusrelatsioon  $\mathcal{I}$ .

Mitterange järjestusrelatsiooni kujutamiseks kasutatakse sageli nn *Hasse diagrammi*, mis saadakse relatsiooni graafist järgmiste lihtsususte teel. Kõigepealt eemaldatakse graafist kõik silmused: mitterange järjestusrelatsioon on refleksiivne ja seetõttu tuleks niikuinii iga tipu juurde silmus lisada. Teiseks eemaldatakse kõik kaared, mille olemasolu järeldub transitiivsusest. See tähendab, kui graafis on kaar tipust  $x$  tippu  $y$  ja kaar tipust  $y$  tippu  $z$ , siis kaart tipust  $x$  tippu  $z$  enam ei joonistata. Lõpuks korraldatakse graafi tipud nii, et kõik kaared on suunatud ülevalt alla, ja jäetakse ära nooled.

Valime näiteks hulga  $X$  arvu 36 kõigi jagajate hulga, seega  $X = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$  ja vaatleme sellel jaguvusrelatsiooni, mis, nagu teame, on mitterange järjestus. Selle relatsiooni Hasse diagramm on kujutatud järgmisel joonisel vasakul. Kuigi näiteks arvude 36 ja 6 vahel kaart ei ole, järeldub jooniselt siiski, et paar  $(36, 6)$  kuulub vaadeldavasse relatsiooni, sest sinna kuuluvad paarid  $(36, 12)$  ja  $(12, 6)$ . Samuti kuuluvad relatsiooni kõik võrdsete liikmetega paarid, ehkki vastavad silmused on diagrammilt ära jäetud. Teise näitena on joonisel paremal esitatud kolmeelemendilise hulga  $A = \{1, 2, 3\}$  kõigi alamhulkade hulgal  $\mathcal{P}(A)$  määratud mitterange sisalduvusrelatsioon. Selle Hasse diagrammi lugemisel kehtivad samasugused reeglid.



## Ülesanded

1. Tõestada, et kolme hulga  $X$ ,  $Y$  ja  $Z$  korral kehtivad võrdused:
  - a)  $X \times (Y \cap Z) = (X \times Y) \cap (X \times Z)$ ;
  - b)  $X \times (Y \cup Z) = (X \times Y) \cup (X \times Z)$ ;
  - c)  $X \times (Y \setminus Z) = (X \times Y) \setminus (X \times Z)$ .
2. Selgitada, kui palju leidub  $n$ -elemendilisel hulgal: a) üldse relatsioone; b) refleksiivseid relatsioone; c) sümmeetrilisi relatsioone;

d) refleksiivseid ja sümmeetrilisi relatsioone; e) sümmeetrilisi ja antisümmeetrilisi relatsioone.

3. Esitada koordinaatteljestikus reaalarvude hulgal  $\mathbb{R}$  määratud relatsioon  $\mathcal{R} = \{(x, y) : -x^2 + 1 \geq y \text{ ja } y > x + 1\}$ .

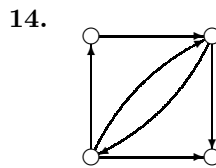
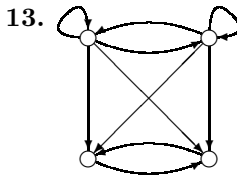
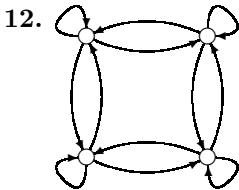
4. Olgu  $X$  hulk, mis koosneb järgmistest Vana-Kreeka jumalatest: Eurybia, Gaia, Kronos, Nereis, Pontos, Rhea, Zeus, Uranos. Sellel hulgal on defineeritud relatsioon  $\mathcal{R}$ , mille puhul  $(x, y) \in \mathcal{R}$  parajasti siis, kui  $y$  on  $x$ -i järglane. Kõrval on toodud relatsiooni maatriks, kus  $i$ -nda rea ja  $j$ -nda veeru element on 1, kui nimekirja  $i$ -nda liikme järeltulija on nimekirja  $j$ -s liige. Joonistada sellele relatsioonile vastav sugupuugraaf.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Leida, millised omadused (refleksiivus, antirefleksiivus, sümmeetrilisus, antisümmeetrilisus, transitiivsus) on järgmistel hulgal  $X$  määratud relatsioonidel.

5.  $X = \mathbb{Z}$ ,  $\mathcal{R} = \{(m, n) : m + n \text{ on paarisarv}\}$ .
6.  $X = \mathbb{Z}$ ,  $\mathcal{R} = \{(m, n) : m^2 = n^3\}$ .
7.  $X = \mathbb{R}$ ,  $\mathcal{R} = \{(x, y) : x - y < 10\}$ .
8.  $X = \mathbb{R}$ ,  $\mathcal{R} = \{(x, y) : |x| \leq |y|\}$ .
9.  $X = \mathcal{P}(A)$ ,  $\mathcal{R} = \{(U, V) : U \setminus V = \emptyset\}$ .
10.  $X$  on kõigi inimeste hulk,  $\mathcal{R} = \{(x, y) : x \text{ on } y\text{-i isa}\}$ .
11. Millised omadused on tühi relatsioonil  $\emptyset$  ja täisrelatsioonil  $\mathcal{U}$ ?

Millised omadused on järgmiste graafidega antud relatsioonidel?



15. Leida relatsioon hulgal  $X = \{1, 2, 3, 4\}$ , mis
- a) on refleksiivne ja pole sümmeetriline ega antisümmeetriline;
  - b) on refleksiivne ja pole transitiivne;
  - c) on refleksiivne ja sümmeetriline, kuid pole transitiivne;
  - d) on antirefleksiivne, sümmeetriline ja transitiivne;
  - e) on antirefleksiivne, antisümmeetriline ja transitiivne.

16. Milline iseloomulik omadus on relatsiooni graafil, kui relatsioon on a) refleksiivne, b) antirefleksiivne, c) sümmeetriline, d) antisümmeetriline, e) transitiivne?

Relatsiooni  $\mathcal{R} \subseteq X \times X$  nimetatakse nõrgalt transitiivseks, kui  $(x, y) \in \mathcal{R}$ ,  $(y, z) \in \mathcal{R}$  ja  $(z, w) \in \mathcal{R}$  korral alati ka  $(x, w) \in \mathcal{R}$ .

17. Kas iga transitiivne relatsioon on ka nõrgalt transitiivne?  
18. Kas iga refleksiivne nõrgalt transitiivne relatsioon on transitiivne?

Kas järgmised hulgal  $X$  määratud relatsioonid on ekvivalentsid?

19.  $X = \mathbb{Z}$ ,  $\mathcal{R} = \{(m, n) : |m| = -n\}$ .  
20.  $X = \mathbb{R}$ ,  $\mathcal{R} = \{(x, y) : x|y| = y|x|\}$ .  
21.  $X = \mathbb{R}$ , arvud  $x$  ja  $y$  on relatsioonis  $\mathcal{R}$  parajasti siis, kui nad annavad lähimaks täisarvuks ümardades võrdsed arvud.  
22.  $X = \mathbb{R} \times \mathbb{R}$ , paarid  $(a, b)$  ja  $(c, d)$  on relatsioonis  $\mathcal{R}$  parajasti siis, kui  $a - d = c - b$ .  
23.  $X$  on tasandi sirgete hulk,  $\mathcal{R} = \{(s, t) : \text{sirged } s \text{ ja } t \text{ on risti}\}$ .  
24. Teha kindlaks, kas järgmised kõigi inimeste hulgal määratud relatsioonid on ekvivalentsid: a) „vähemalt niisama vana kui“; b) „sugulane“; c) „samast soost“; d) „sama riigi kodanik“; e) „sõber“.  
25. Leida kõik ekvivalentsirelatsioonid hulgal  $X = \{1, 2, 3, 4\}$ .  
26. Tõestada, et relatsioon  $\mathcal{R}$  on ekvivalents parajasti siis, kui ta on refleksiivne ja rahuldab tingimust:  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{R}$  korral alati  $(z, x) \in \mathcal{R}$ .  
27. Leida viga järgmises „tõestuses“. Iga sümmeetriline ja transitiivne relatsioon  $\mathcal{R} \subseteq X \times X$  on ka refleksiivne ning kujutab seega ekvivalentsi. Olgu  $x \in X$ . Relatsiooni  $\mathcal{R}$  sümmeetrilisus tähendab, et alati, kui  $(x, y) \in \mathcal{R}$ , on ka  $(y, x) \in \mathcal{R}$ . Rakendades seoste  $(x, y) \in \mathcal{R}$  ja  $(y, x) \in \mathcal{R}$  transitiivsust, saame  $(x, x) \in \mathcal{R}$ . Et see arutelu kehtib suvalise elemendi  $x \in X$  korral, siis sisaldab relatsioon  $\mathcal{R}$  kõiki paare  $(x, x)$  ja on refleksiivne.  
28. Leida kõik mitteranged ja ranged järjestusrelatsioonid, mis on määratud hulgal  $X = \{a, b, c\}$ .

Koostada järgmiste hulgal  $X$  antud järjestusrelatsioonide Hasse diagrammid.

29.  $X = \{-5, -4, \dots, 4, 5\}$ ,  $\mathcal{R} = \{(m, n) : |m| < |n|\}$ .  
30.  $X$  on kahest tähest A ja B koostatud kolmetäheliste sõnade hulk,  $\mathcal{R}$  tähestikulise järjestuse relatsioon.

## IX. TEHTED RELATSIOONIDEGA

**1. Põhitehted.** Et relatsioonid on hulgad, siis saab nendega sooritada samasuguseid tehteid nagu üldse hulkadega.

Olgu  $\mathcal{R}$  ja  $\mathcal{S}$  kaks relatsiooni hulkade  $X$  ja  $Y$  vahel. Relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  ühend on relatsioon  $\mathcal{R} \cup \mathcal{S}$ , mis koosneb nii relatsiooni  $\mathcal{R}$  kui ka relatsiooni  $\mathcal{S}$  kuuluvatest paaridest:

$$\mathcal{R} \cup \mathcal{S} = \{(x, y) : (x, y) \in \mathcal{R} \text{ või } (x, y) \in \mathcal{S}\}.$$

Relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  ühisosa on relatsioon  $\mathcal{R} \cap \mathcal{S}$ , mis koosneb relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  ühistest paaridest:

$$\mathcal{R} \cap \mathcal{S} = \{(x, y) : (x, y) \in \mathcal{R} \text{ ja } (x, y) \in \mathcal{S}\}.$$

Relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  vahe on relatsioon  $\mathcal{R} \setminus \mathcal{S}$ , mis koosneb sellistest relatsiooni  $\mathcal{R}$  kuuluvatest paaridest, mis samal ajal ei kuulu relatsiooni  $\mathcal{S}$ :

$$\mathcal{R} \setminus \mathcal{S} = \{(x, y) : (x, y) \in \mathcal{R} \text{ ja } (x, y) \notin \mathcal{S}\}.$$

Kui  $\mathcal{R}$  on relatsioon hulkade  $X$  ja  $Y$  vahel, siis saame leida tema täiendi  $\mathcal{R}'$ , mis koosneb kõigist neist otsekorrutisse  $X \times Y$  kuuluvatest paaridest, mis ei kuulu vaadeldavasse relatsiooni  $\mathcal{R}$ :

$$\mathcal{R}' = \{(x, y) : (x, y) \notin \mathcal{R}\}.$$

Teiste sõnadega,  $\mathcal{R}' = \mathcal{U} \setminus \mathcal{R}$ , kus  $\mathcal{U}$  tähistab täisrelatsiooni.

Olgu näiteks hulgal  $X = \mathbb{R}$  antud kaks relatsiooni

$$\mathcal{R} = \{(x, y) : x < y\} \quad \text{ja} \quad \mathcal{S} = \{(x, y) : x = y\}.$$

Siis

$$\begin{aligned} \mathcal{R} \cup \mathcal{S} &= \{(x, y) : x \leq y\}, & \mathcal{R} \cap \mathcal{S} &= \emptyset, \\ \mathcal{R} \setminus \mathcal{S} &= \mathcal{R}, & \mathcal{R}' &= \{(x, y) : x \geq y\}. \end{aligned}$$

Kõigi nimetatud tehete tulemusena saame uuesti relatsiooni hulkade  $X$  ja  $Y$  vahel. Samuti kanduvad neile tehetele üle kõik omadused, mis on üldse hulkadega sooritatavatel tehetel.

Lisaks vaadeldakse veel relatsiooni  $\mathcal{R}$  pöördrelatsiooni  $\mathcal{R}^{-1}$ , mis saadakse relatsioonist  $\mathcal{R}$ , muutes kõigis sinna kuuluvates elemendi-paarides komponentide järjekorra vastupidiseks:

$$\mathcal{R}^{-1} = \{(y, x) : (x, y) \in \mathcal{R}\}.$$

Kui  $\mathcal{R}$  on relatsioon hulkade  $X$  ja  $Y$  vahel, siis  $\mathcal{R}^{-1}$  on relatsioon hulkade  $Y$  ja  $X$  vahel. Näiteks juhul, kui  $\mathcal{R} = \{(a, 3), (b, 4)\}$ , on  $\mathcal{R}^{-1} = \{(3, a), (4, b)\}$ .

Kui relatsiooni  $\mathcal{R}$  kõigis paarides muuta kaks korda komponentide järjekorda, siis saame jälle sama relatsiooni. Seega kehtib võrdus



$(\mathcal{R}^{-1})^{-1} = \mathcal{R}$ . Samuti võib kergesti veenduda, et relatsioon  $\mathcal{R}$  on sümmeetriline parajasti siis, kui  $\mathcal{R}^{-1} = \mathcal{R}$ .

**2. Kompositsioon.** Olgu  $\mathcal{R} \subseteq X \times Y$  ja  $\mathcal{S} \subseteq Y \times Z$  kaks relatsiooni. Relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  *kompositsiooniks* nimetatakse relatsiooni  $\mathcal{R} \circ \mathcal{S} \subseteq X \times Z$ , mis on määratud avaldisega

$$\mathcal{R} \circ \mathcal{S} = \{(x, z): \text{leidub } y \in Y \text{ nii, et } (x, y) \in \mathcal{R} \text{ ja } (y, z) \in \mathcal{S}\}.$$

Vaatleme näiteks kõigi inimeste hulgal määratud relatsioone  $\mathcal{R}$  ja  $\mathcal{S}$ , kusjuures  $(x, y) \in \mathcal{R}$ , kui  $x$  on  $y$ -i isa, ning  $(x, y) \in \mathcal{S}$ , kui  $x$  on  $y$ -i ema. Kompositsioon  $\mathcal{R} \circ \mathcal{S}$  tähendab seega selliste paaride  $(x, z)$  hulka, mille korral leidub element  $y$  nii, et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S}$ , teiste sõnadega, leidub inimene, kellele  $x$  on isa ja kes ise on  $z$ -i ema, st  $x$  on  $z$ -i emapoolne vanaisa.

Teise näitena olgu täisarvude hulgal  $\mathbb{Z}$  antud relatsioonid

$$\mathcal{R} = \{(x, x+1): x \in \mathbb{Z}\} \quad \text{ja} \quad \mathcal{S} = \{(x, 2x): x \in \mathbb{Z}\}.$$

Arvupaar  $(x, z)$  kuulub relatsiooni  $\mathcal{R} \circ \mathcal{S}$  parajasti siis, kui leidub selline arv  $y$ , et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S}$ . Viimased tingimused tähendavad võrdusi  $y = x + 1$  ja  $z = 2y$ , millest  $z = 2x + 2$ . Niisiis sisaldab relatsioon  $\mathcal{R} \circ \mathcal{S}$  ainult arvupaare kujul  $(x, 2x+2)$ . Näeme ka, et sellesse relatsiooni kuuluvad kõik niisugused arvupaarid, järelikult  $\mathcal{R} \circ \mathcal{S} = \{(x, 2x+2): x \in \mathbb{Z}\}$ . Samamoodi võib leida kompositsiooni  $\mathcal{S} \circ \mathcal{R} = \{(x, 2x+1): x \in \mathbb{Z}\}$ .

Kompositsiooni abil saab väljendada mitmesuguseid tingimusi.

*Näide 1.* Teatavas kontoris võib iga töötaja asuda ühes või mitmes ruumis ning tal võib olla teatav hulk võtmeid, mis ruume avavad. Olgu *Töötajad* kontori kõigi töötajate hulk, *Ruumid* ruumide hulk ja *Võtmed* võtmete hulk. Antud on relatsioonid

$$\begin{aligned} asub &\subseteq \text{Töötajad} \times \text{Ruumid}, \\ valdab &\subseteq \text{Töötajad} \times \text{Võtmed}, \\ avab &\subseteq \text{Võtmed} \times \text{Ruumid}. \end{aligned}$$

Ülesandeks on a) avaldada kujul  $(x, y) \in \mathcal{R}$  väide: töötaja  $x$  pääseb ruumi  $y$ ; b) leida tingimus, mis peab olema täidetud, et iga töötaja pääseks ruumi, kus ta asub.

a) Selleks, et töötaja  $x$  pääseks ruumi  $y$ , peab tal olema võti, mis seda ruumi avab. Teiste sõnadega, hulgas *Võtmed* peab leiduma selline element  $z$ , et  $(x, z) \in \text{valdab}$  ja  $(z, y) \in \text{avab}$ . Vastavalt kompositsiooni definitsioonile võib nõutava väite kirja panna kujul

$$(x, y) \in \text{valdab} \circ \text{avab}.$$

b) Et töötaja  $x$  pääseks ruumi  $y$ , kus ta asub, peab eelmine seos  $(x, y) \in \text{valdab} \circ \text{avab}$  kehtima iga elemendipaari  $(x, y) \in \text{asub}$  korral. Otsitav tingimus on järelikult

$$\text{asub} \subseteq \text{valdab} \circ \text{avab}.$$

Teeme nüüd kindlaks mõned kompositsiooni omadused ja tema seosed teiste tehetega.

**Teoreem 1.** *Suvaliste relatsioonide  $\mathcal{R} \subseteq X \times Y$ ,  $\mathcal{S} \subseteq Y \times Z$  ja  $\mathcal{T} \subseteq Z \times W$  korral*

$$(\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T} = \mathcal{R} \circ (\mathcal{S} \circ \mathcal{T}).$$

See tähendab, relatsioonide kompositsioon on assotsiatiivne.

**Tõestus.** Kahe hulga võrduse tõestamiseks näitame, et sisalduvused  $(x, w) \in (\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T}$  ja  $(x, w) \in \mathcal{R} \circ (\mathcal{S} \circ \mathcal{T})$  on teineteisega samaväärsed.

Tõepoolest, sisaldumus  $(x, w) \in (\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T}$  on kompositsiooni definitsiooni põhjal samaväärne tingimusega

$$\text{leidub } z \in Z, \text{ et } (x, z) \in \mathcal{R} \circ \mathcal{S} \text{ ja } (z, w) \in \mathcal{T},$$

viimane aga samal põhjusel tingimusega

$$\text{leiduvad } z \in Z \text{ ning } y \in Y, \text{ et } (x, y) \in \mathcal{R}, (y, z) \in \mathcal{S} \text{ ja } (z, w) \in \mathcal{T}.$$

Siin võime kombineerida kaks viimast elemendipaari kompositsiooni definitsiooni abil ja kirjutada tingimuse kujul

$$\text{leidub } y \in Y, \text{ et } (x, y) \in \mathcal{R} \text{ ja } (y, w) \in \mathcal{S} \circ \mathcal{T},$$

see aga tähendabki, et  $(x, w) \in \mathcal{R} \circ (\mathcal{S} \circ \mathcal{T})$ . Et kõik teisendusammud säilitavad samaväärsuse, siis on vaadeldavad kaks sisalduvust tõesti teineteisega samaväärsed.  $\square$

**Teoreem 2.** *Kui  $\mathcal{I}_X$  on samasusrelatsioon hulgal  $X$  ja  $\mathcal{I}_Y$  samasusrelatsioon hulgal  $Y$ , siis suvalise relatsiooni  $\mathcal{R} \subseteq X \times Y$  korral*

$$\mathcal{R} \circ \mathcal{I}_Y = \mathcal{I}_X \circ \mathcal{R} = \mathcal{R}.$$

Teiste sõnadega, samasusrelatsioon on kompositsiooni suhtes ühik-element.

**Tõestus.** Tõestame võrduse  $\mathcal{R} \circ \mathcal{I}_Y = \mathcal{R}$ . Kõigepealt on sisaldumus  $(x, y) \in \mathcal{R} \circ \mathcal{I}_Y$  samaväärne tingimusega

$$\text{leidub } z \in Y, \text{ et } (x, z) \in \mathcal{R} \text{ ja } (z, y) \in \mathcal{I}_Y.$$

Et samasusrelatsioon koosneb paaridest, mille komponendid on võrdsed, siis on saadud tingimus samaväärne tingimusega  $(x, y) \in \mathcal{R}$ .

Võrdus  $\mathcal{I}_X \circ \mathcal{R} = \mathcal{R}$  tõestatakse analoogiliselt.  $\square$

Kes on vastavate algebraliste mõistetega tuttav, see võib tähele panna kahest tõestatud omadusest järelduvat asjaolu, et kõigi ühel

ja samal hulgal  $X$  määratud relatsioonide hulk moodustab monoidi, ühe matemaatikas laialt kasutatava algebralise struktuuri. Tehteks on siin relatsioonide kompositsiooni leidmine ja ühikelemendiks samasusrelatsioon. Kuid see monoid ei osutu rühmaks ning samuti ei ole ta üldiselt kommutatiivne.

*Näide 2.* Näidata, et relatsiooni  $\mathcal{R} \subseteq X \times Y$  korral ei tarvitse kehtida võrdus  $\mathcal{R} \circ \mathcal{R}^{-1} = \mathcal{I}$ .

Valime  $X = Y = \{1, 2\}$  ning vaatleme konkreetset relatsiooni  $\mathcal{R} = \{(1, 2)\}$ . Siis  $\mathcal{R} \circ \mathcal{R}^{-1} = \{(1, 1)\}$ , kuid  $\mathcal{I} = \{(1, 1), (2, 2)\}$ . Veel lihtsam võimalus on valida relatsiooniks  $\mathcal{R}$  tühi relatsioon  $\emptyset$ . Siis saame võrduse vasakul poolel tühi relatsiooni, mis ilmselt ei võrdu samasusrelatsiooniga  $\mathcal{I}$ .

*Näide 3.* Näidata, et hulgal  $X$  määratud relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  korral ei tarvitse kehtida võrdus  $\mathcal{R} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{R}$ .

Valime põhihulgaks hulga  $X = \{1, 2\}$  ning vaatleme relatsioone  $\mathcal{R} = \{(1, 1)\}$  ja  $\mathcal{S} = \{(1, 2)\}$ . Siis  $\mathcal{R} \circ \mathcal{S} = \{(1, 2)\}$ , kuid  $\mathcal{S} \circ \mathcal{R} = \emptyset$ . Seega üldiselt kaks relatsiooni ei kommuteeru.

Edasi võtame vaatluse alla omadused, mis puudutavad kompositsiooni seost teiste tehetega.

**Teoreem 3.** *Suvaliste relatsioonide  $\mathcal{R} \subseteq X \times Y$  ja  $\mathcal{S} \subseteq Y \times Z$  korral*

$$(\mathcal{R} \circ \mathcal{S})^{-1} = \mathcal{S}^{-1} \circ \mathcal{R}^{-1}.$$

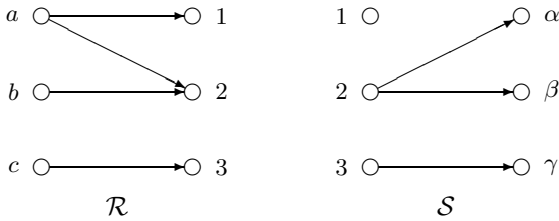
*Tõestus.* Analoogiliselt eelnevate tõestustega saame samaväärsete tingimuste ahela:

$$\begin{aligned} (z, x) \in (\mathcal{R} \circ \mathcal{S})^{-1} &\Leftrightarrow (x, z) \in (\mathcal{R} \circ \mathcal{S}) \Leftrightarrow \\ &\Leftrightarrow \text{leidub } y, \text{ et } (x, y) \in \mathcal{R} \text{ ja } (y, z) \in \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow \text{leidub } y, \text{ et } (y, x) \in \mathcal{R}^{-1} \text{ ja } (z, y) \in \mathcal{S}^{-1} \Leftrightarrow \\ &\Leftrightarrow (z, x) \in \mathcal{S}^{-1} \circ \mathcal{R}^{-1} \end{aligned}$$

Kui alustada selle samaväärsuste ahela lugemist algusest, siis saame tõestuse, et  $(\mathcal{R} \circ \mathcal{S})^{-1} \subseteq \mathcal{S}^{-1} \circ \mathcal{R}^{-1}$ . Liikudes aga ahelas lõpust algusesse, saame teistpidi sisalduvuse  $\mathcal{S}^{-1} \circ \mathcal{R}^{-1} \subseteq (\mathcal{R} \circ \mathcal{S})^{-1}$ . Mõlematpidi sisaldumisest aga järeldubki hulkade võrdsus.  $\square$

*Näide 4.* Kontrollime viimase võrduse kehtivust ühel konkreetset juhul, kasutades kompositsiooni ja pöördrelatsiooni leidmiseks graafe. Olgu  $X = \{a, b, c\}$ ,  $Y = \{1, 2, 3\}$  ning  $Z = \{\alpha, \beta, \gamma\}$ . Seejuures olgu hulkade  $X$  ja  $Y$  vahel antud relatsioon  $\mathcal{R} = \{(a, 1), (a, 2), (b, 2), (c, 3)\}$  ning hulkade  $Y$  ja  $Z$  vahel relatsioon  $\mathcal{S} = \{(2, \alpha), (2, \beta), (3, \gamma)\}$ .

Mõlemat relatsiooni võib kujutada järgmiste graafidega:



Kompositsioon  $\mathcal{R} \circ \mathcal{S}$ , mis on relatsioon hulkade  $X$  ja  $Z$  vahel, sisaldab paari  $(x, z)$  parajasti siis, kui vasakpoolses graafis viib kaar tipust  $x$  mingisse tippu  $y$  ja parempoolses graafis kaar tipust  $y$  tippu  $z$ . Näiteks pääseb vasakpoolses graafis tipust  $a$  tippu 2 ning parempoolses graafis tipust 2 tippu  $\alpha$ , seega kuulub kompositsiooni paar  $(a, \alpha)$ . Niiviisi kõiki võimalusi läbi vaadates leiame

$$\mathcal{R} \circ \mathcal{S} = \{(a, \alpha), (a, \beta), (b, \alpha), (b, \beta), (c, \gamma)\}.$$

Kompositsiooni pöördrelatsioon on relatsioon hulkade  $Z$  ja  $X$  vahel ja koosneb samadest paaridest, ainult vastupidises järjekorras:

$$(\mathcal{R} \circ \mathcal{S})^{-1} = \{(\alpha, a), (\beta, a), (\alpha, b), (\beta, b), (\gamma, c)\}.$$

Kui muuta relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  graafides noolte suunad vastupidiseks, saame relatsioonide  $\mathcal{R}^{-1}$  ja  $\mathcal{S}^{-1}$  graafid, millelt võime samasugusel viisil välja lugeda pöördrelatsioonide kompositsiooni. Et  $\mathcal{S}^{-1} = \{(\alpha, 2), (\beta, 2), (\gamma, 3)\}$  ja  $\mathcal{R}^{-1} = \{(1, a), (2, a), (2, b), (3, c)\}$ , siis

$$\mathcal{S}^{-1} \circ \mathcal{R}^{-1} = \{(\alpha, a), (\alpha, b), (\beta, a), (\beta, b), (\gamma, c)\}.$$

Näeme, et antud kahe relatsiooni puhul võrdus  $(\mathcal{R} \circ \mathcal{S})^{-1} = \mathcal{S}^{-1} \circ \mathcal{R}^{-1}$  kehtib. Soovitav on jälgida eelnevas tõestuses esitatud arutluskäiku juhul, kui relatsioonideks  $\mathcal{R}$  ja  $\mathcal{S}$  on käesolevas näites vaadeldavad.

**Teoreem 4.** *Suvaliste relatsioonide  $\mathcal{R} \subseteq X \times Y$ ,  $\mathcal{S} \subseteq Y \times Z$  ja  $\mathcal{T} \subseteq Y \times Z$  korral*

$$\mathcal{R} \circ (\mathcal{S} \cup \mathcal{T}) = (\mathcal{R} \circ \mathcal{S}) \cup (\mathcal{R} \circ \mathcal{T}).$$

Seega, kompositsioon on distributiivne ühendi suhtes.

**Tõestus.** Tõestame, et võrduse vasak pool sisaldub paremas ja vastupidi, parem pool sisaldub vasakus.

Kui  $(x, z) \in \mathcal{R} \circ (\mathcal{S} \cup \mathcal{T})$ , siis leidub  $y \in Y$  nii, et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S} \cup \mathcal{T}$ . Kui viimasest seoses  $(y, z) \in \mathcal{S}$ , siis  $(x, z) \in \mathcal{R} \circ \mathcal{S}$ ; kui aga  $(y, z) \in \mathcal{T}$ , siis  $(x, z) \in \mathcal{R} \circ \mathcal{T}$ . Igal juhul  $(x, z) \in (\mathcal{R} \circ \mathcal{S}) \cup (\mathcal{R} \circ \mathcal{T})$ .

Vastupidi, kui  $(x, z) \in (\mathcal{R} \circ \mathcal{S}) \cup (\mathcal{R} \circ \mathcal{T})$ , siis kas  $(x, z) \in \mathcal{R} \circ \mathcal{S}$  või  $(x, z) \in \mathcal{R} \circ \mathcal{T}$ . Esimesel juhul leidub element  $y$  nii, et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S}$ , viimasest saame  $(y, z) \in \mathcal{S} \cup \mathcal{T}$ . Teisel juhul leidub element  $y$  nii, et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{T}$ , mis samuti annab  $(y, z) \in \mathcal{S} \cup \mathcal{T}$ . Et kummalgi juhul kehtib lisaks  $(x, y) \in \mathcal{R}$ , siis  $(x, z) \in \mathcal{R} \circ (\mathcal{S} \cup \mathcal{T})$ .  $\square$

Kompositsiooni ja ühisosa vahel distributiivsus ei kehti, kuid saab väita järgmist.

**Teoreem 5.** *Suvaliste relatsioonide  $\mathcal{R} \subseteq X \times Y$ ,  $\mathcal{S} \subseteq Y \times Z$  ja  $\mathcal{T} \subseteq Y \times Z$  korral*

$$\mathcal{R} \circ (\mathcal{S} \cap \mathcal{T}) \subseteq (\mathcal{R} \circ \mathcal{S}) \cap (\mathcal{R} \circ \mathcal{T}).$$

**Tõestus.** Kui  $(x, z) \in \mathcal{R} \circ (\mathcal{S} \cap \mathcal{T})$ , siis leidub  $y \in Y$  nii, et  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S} \cap \mathcal{T}$ . Viimasest seosest saame  $(y, z) \in \mathcal{S}$  ja  $(y, z) \in \mathcal{T}$ . Tingimused  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{S}$  annavad nüüd  $(x, z) \in \mathcal{R} \circ \mathcal{S}$ , tingimused  $(x, y) \in \mathcal{R}$  ja  $(y, z) \in \mathcal{T}$  aga  $(x, z) \in \mathcal{R} \circ \mathcal{T}$ . Järelikult  $(x, z) \in (\mathcal{R} \circ \mathcal{S}) \cap (\mathcal{R} \circ \mathcal{T})$ .  $\square$

**Näide 5.** Näidata, et tõestatud teoreemis ei või alamhulgamärgi asemele kirjutada võrdusmärki.

Selleks piisab tuua näide relatsioonidest  $\mathcal{R}$ ,  $\mathcal{S}$  ja  $\mathcal{T}$ , mille puhul vasak ja parem pool on erinevad. Valime hulkadeks  $X$ ,  $Y$  ja  $Z$  eelmise näite hulgad. Olgu  $\mathcal{R} = \{(a, 1), (a, 2)\}$ ,  $\mathcal{S} = \{(1, \alpha)\}$  ja  $\mathcal{T} = \{(2, \alpha)\}$ . Nüüd on  $\mathcal{S} \cap \mathcal{T} = \emptyset$ , mistõttu ka  $\mathcal{R} \circ (\mathcal{S} \cap \mathcal{T}) = \emptyset$ . Samal ajal  $\mathcal{R} \circ \mathcal{S} = \{(a, \alpha)\}$  ja  $\mathcal{R} \circ \mathcal{T} = \{(a, \alpha)\}$  ning  $(\mathcal{R} \circ \mathcal{S}) \cap (\mathcal{R} \circ \mathcal{T}) = \{(a, \alpha)\}$ . Järelikult on selliste relatsioonide korral teoreemi sisalduvuse vasakul poolel tühi relatsioon, paremal aga mittetühi relatsioon.

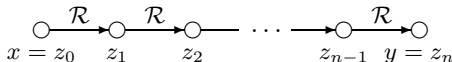
**3. Relatsiooni aste.** Olgu  $\mathcal{R}$  relatsioon hulgal  $X$ , st  $\mathcal{R} \subseteq X \times X$ . Relatsiooni  $\mathcal{R}$  *aste* defineeritakse järgmiselt:  $\mathcal{R}^0 = \mathcal{I}$  ja iga naturaalarvu  $n$  korral  $\mathcal{R}^n = \mathcal{R}^{n-1} \circ \mathcal{R}$ . Relatsiooni aste on niisiis korduv kompositsioon iseendaga. Assotsiatiivsuse tõttu kehtib ka  $\mathcal{R}^n = \mathcal{R} \circ \mathcal{R}^{n-1}$ .

Näiteks täisarvude hulgal määratud relatsiooni

$$\mathcal{R} = \{(x, x+1) : x \in \mathbb{Z}\}$$

korral on  $\mathcal{R}^2 = \{(x, x+2) : x \in \mathbb{Z}\}$ ,  $\mathcal{R}^3 = \{(x, x+3) : x \in \mathbb{Z}\}$  ja üldiselt,  $\mathcal{R}^n = \{(x, x+n) : x \in \mathbb{Z}\}$ . Kui  $\mathcal{R}$  tähendab „saks olemise“ relatsiooni, siis  $\mathcal{R}^2$  on relatsioon „isa isa“ (isapoolne vanaisa),  $\mathcal{R}^3$  on relatsioon „isapoolse vanaisa isa“ jne.

**Teoreem 6.** *Paar  $(x, y)$  kuulub astmesse  $\mathcal{R}^n$ , kus  $n \geq 1$ , parajasti siis, kui hulgas  $X$  leiduvad elemendid  $z_0, \dots, z_n$  nii, et  $z_0 = x$ ,  $z_n = y$  ja iga  $i = 0, \dots, n-1$  korral  $(z_i, z_{i+1}) \in \mathcal{R}$ .*



**Tõestus.** Tõestame selle väite induktsiooniga astenda ja  $n$  järgi.

**Baas.** Kui  $n = 1$ , siis  $z_0 = x$  ja  $z_1 = y$  ning väide on ilmne.

**Samm.** Eeldame, et väide kehtib juhul  $n = k$ , ning vaatleme juhtu, kus  $n = k + 1$ .

Kui  $(x, y) \in \mathcal{R}^{k+1}$ , siis astme mõiste kohaselt  $(x, y) \in \mathcal{R}^k \circ \mathcal{R}$ . Järelikult leidub hulgas  $X$  element  $z$ , mille korral  $(x, z) \in \mathcal{R}^k$  ja  $(z, y) \in \mathcal{R}$ . Neist seostest esimesele rakendame induktsiooni eeldust: leiduvad elemendid  $z_0, \dots, z_k$  nii, et  $z_0 = x$ ,  $z_k = z$  ja  $(z_i, z_{i+1}) \in \mathcal{R}$  iga  $i = 0, \dots, k-1$  korral. Võttes nüüd  $z_{k+1} = y$ , saamegi sobiva järjendi  $z_0, \dots, z_{k+1}$ .

Vastupidi, kui leiduvad elemendid  $z_0, \dots, z_{k+1}$ , millel on nõutavad omadused, st  $z_0 = x$ ,  $z_{k+1} = y$  ja  $(z_i, z_{i+1}) \in \mathcal{R}$  iga  $i = 0, \dots, k$  korral, siis osajärjendile  $z_0, \dots, z_k$  induktsiooni eeldust rakendades saame  $(x, z_k) \in \mathcal{R}^k$ , mis koos seosega  $(z_k, z_{k+1}) \in \mathcal{R}$  annabki, et  $(x, y) \in \mathcal{R}^{k+1}$ .  $\square$

**4. Sulundid.** Oleme vaadelnud relatsioonide mitmesuguseid omadusi: refleksiivsus, sümmeetrilisus, transitiivsus jne. Kui antud relatsioonil  $\mathcal{R} \subseteq X \times X$  mingi omadus puudub, siis pakub huvi küsimus, kui palju ja milliseid paare tuleb talle lisada, et see omadus tekiks. Vähimat teatava omadusega relatsiooni, mis relatsiooni  $\mathcal{R}$  sisaldab, nimetatakse relatsiooni  $\mathcal{R}$  *sulundiks* selle omaduse suhtes. Sulundit mõistetakse vähimana hulkade sisalduvuse mõttes: iga teine relatsioon, millel on vaadeldav omadus ja mis sisaldab relatsiooni  $\mathcal{R}$ , sisaldab ühtlasi ka relatsiooni  $\mathcal{R}$  sulundit.

Praktikas olulisimaid on *transitiivne sulund*, vähim transitiivne relatsioon, mis sisaldab antud relatsiooni, ning *refleksiivne transitiivne sulund* ehk vähim antud relatsiooni sisaldav relatsioon, mis on nii refleksiivne kui ka transitiivne. Neile kahele sulundiliigile pööramegi järgnevas tähelepanu. Relatsiooni  $\mathcal{R}$  transitiivset sulundit märgitakse tähisega  $\mathcal{R}^+$ , refleksiivset transitiivset sulundit aga tähisega  $\mathcal{R}^*$ . Definiitsioonist järeldub otse, et relatsioon on transitiivne parajasti siis, kui ta ühtib oma transitiivse sulundiga.

*Näide 6.* Leida hulgal  $X = \{1, 2, 3\}$  määratud relatsiooni  $\mathcal{R} = \{(1, 2), (2, 3), (3, 2)\}$  transitiivne sulund ja refleksiivne transitiivne sulund.

Vaadeldav relatsioon ei ole transitiivne, sest ta sisaldab küll paare  $(1, 2)$  ja  $(2, 3)$ , aga mitte paari  $(1, 3)$ , nagu nõuab transitiivsuse tingimus. Seetõttu peab transitiivne sulund sisaldama seda paari. Lisame selle relatsioonile, millega saame relatsiooni

$$\mathcal{R}_1 = \{(1, 2), (1, 3), (2, 3), (3, 2)\}.$$

See relatsioon pole ikka transitiivne, sest sinna kuuluvad paarid  $(2, 3)$  ja  $(3, 2)$ , aga mitte paar  $(2, 2)$  ega paar  $(3, 3)$ . Lisame need paarid:

$$\mathcal{R}_2 = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}.$$

Tulemuseks on transitiivne relatsioon, järelikult  $\mathcal{R}^+ = \mathcal{R}_2$ .

Et lisaks transitiivsusele kindlustada refleksiivsust, peame lisama viimasele relatsioonile kõik paarid kujul  $(x, x)$ . Seega

$$\mathcal{R}^* = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}.$$

Definitsiooni asemel võib transitiivse sulundi leidmiseks kasutada ka järgmist teoreemi.

**Teoreem 7.** *Relatsiooni  $\mathcal{R} \subseteq X \times X$  transitiivne sulund  $\mathcal{R}^+$  avaldub valemiga*

$$\mathcal{R}^+ = \bigcup_{i=1}^{\infty} \mathcal{R}^i.$$

**Tõestus.** Tõestame, et valemi parem pool kujutab vähimat transitiivset relatsiooni, mis sisaldab relatsiooni  $\mathcal{R}$ .

Kõigepealt, relatsioon  $\cup_{i=1}^{\infty} \mathcal{R}^i$  on transitiivne. Tõepoolest, kui ta sisaldab paare  $(x, y)$  ja  $(y, z)$ , siis peab mingite  $k \geq 1$  ja  $l \geq 1$  korral olema  $(x, y) \in \mathcal{R}^k$  ja  $(y, z) \in \mathcal{R}^l$ . Kompositsiooni definitsiooni põhjal  $(x, z) \in \mathcal{R}^k \circ \mathcal{R}^l = \mathcal{R}^{k+l}$  ning järelikult  $(x, z) \in \cup_{i=1}^{\infty} \mathcal{R}^i$ .

Olgu nüüd  $\mathcal{S}$  mingi transitiivne relatsioon, mis sisaldab relatsiooni  $\mathcal{R}$ . Valime suvalise paari  $(x, y) \in \cup_{i=1}^{\infty} \mathcal{R}^i$ . Sel juhul  $(x, y) \in \mathcal{R}^k$  mingi  $k \geq 1$  korral ning teoreemi 6 põhjal leiduvad elemendid  $z_0, \dots, z_k$  nii, et  $z_0 = x$ ,  $z_k = y$  ja iga  $i = 0, \dots, k-1$  korral  $(z_i, z_{i+1}) \in \mathcal{R}$ . Ent siis ka  $(z_i, z_{i+1}) \in \mathcal{S}$  ning relatsiooni  $\mathcal{S}$  transitiivsuse tõttu  $(x, y) \in \mathcal{S}$ . Järelikult kehtib  $\cup_{i=1}^{\infty} \mathcal{R}^i \subseteq \mathcal{S}$ .

Et vaadeldav relatsioon  $\cup_{i=1}^{\infty} \mathcal{R}^i$  sisaldab ka relatsiooni  $\mathcal{R}$ , siis rahuldab ta kõiki transitiivse sulundi tingimusi ja peab seega võrduma relatsiooniga  $\mathcal{R}^+$ .  $\square$

**Järeldus 1.** *Relatsiooni  $\mathcal{R} \subseteq X \times X$  refleksiivne transitiivne sulund  $\mathcal{R}^*$  avaldub valemiga*

$$\mathcal{R}^* = \bigcup_{i=0}^{\infty} \mathcal{R}^i.$$

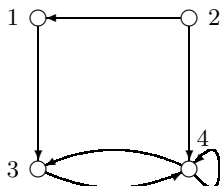
**Tõestus.** Et transitiivne sulund oleks ka refleksiivne, peame sinna lisama kõik võrdsete komponentidega paarid. See on aga sama kui leida relatsiooni ühend relatsiooniga  $\mathcal{I} = \mathcal{R}^0$ .  $\square$

Relatsiooni transitiivne sulund on seega relatsiooni kõigi astmete ühend. Selle omaduse põhjal võime transitiivsele sulundile anda järgmise interpretatsiooni. Olgu relatsioon  $\mathcal{R}$  esitatud suunatud graafiga  $G$ , kus tipust  $x$  viib kaar tippu  $y$  parajasti siis, kui  $(x, y) \in \mathcal{R}$ . Siis näitab relatsioon  $\mathcal{R}^2$  mingi kahe tipu  $x$  ja  $y$  vahel seda, et esimesest tipust on võimalik liikuda teise täpselt kahe sammuga: leidub selline vahepealne tipp  $z$ , et tipust  $x$  viib serv tippu  $z$  ja tipust  $z$  tippu  $y$ . Kui kaks tippu on relatsioonis  $\mathcal{R}^3$ , siis on esimesest võimalik minna

teise täpselt kolme sammuga jne. Seega on transitiivse sulundi  $\mathcal{R}^+$  niisugune relatsioon, mis kehtib suvalise kahe tipu vahel parajasti siis, kui ühest tipust on üldse võimalik minna teise tippu, ükskõik mitu sammu selleks ka ei kuluks. Refleksiivse transitiivse sulundi  $\mathcal{R}^*$  puhul loetakse veel iga tipp automaatselt seotuks iseendaga.

Näide 7. Leida hulgal  $X = \{1, 2, 3, 4\}$  määratud relatsiooni  $\mathcal{R} = \{(1, 3), (2, 1), (2, 4), (3, 4), (4, 3), (4, 4)\}$  transitiivne sulund.

Joonistame relatsiooni  $\mathcal{R}$  graafi:



Iga tipu puhul teeme kindlaks, millistesse tippudesse on sealt võimalik mööda kaari liikuda, tulemuseks saame transitiivse sulundi

$$\mathcal{R}^+ = \{(1, 3), (1, 4), (2, 1), (2, 3), (2, 4), (3, 3), (3, 4), (4, 3), (4, 4)\}.$$

Näide 8. Kõigi inimeste hulgal on määratud relatsioonid

$$vanem = \{(x, y) : x \text{ on } y\text{-i vanem}\}$$

$$abikaasa = \{(x, y) : x \text{ ja } y \text{ on abikaasad}\}$$

Kahte inimest loeme lähisugulasteks, kui üks on teise vanem või kui nad on omavahel abielus. Sugulasteks üldse loeme inimesi, keda ühendab lähisugulussidemete ahel. Kuidas avaldub antud relatsioonide kaudu sugulusrelatsioon?

Kui  $x$  ja  $y$  on lähisugulased, siis kehtib kas  $(x, y) \in vanem$  või  $(y, x) \in vanem$  või  $(x, y) \in abikaasa$ . Teise seose võime kirjutada pöördrelatsiooni abil kujul  $(x, y) \in vanem^{-1}$ . Lähisuguluse relatsiooni moodustavad need kolm varianti üheskoos:

$$lähisugulane = vanem \cup vanem^{-1} \cup abikaasa.$$

Kahe sugulase puhul võib ahel ühest teiseni olla pikkusega 1, pikkusega 2 jne, järelikult on relatsioon, mis väljendab sugulust inimeste vahel, relatsiooni  $lähisugulane$  transitiivne sulund

$$sugulane = (vanem \cup vanem^{-1} \cup abikaasa)^+.$$

Sageli tuleb transitiivset sulundit arvutada lõplikul hulgal määratud relatsioonidest. Sel juhul võib teoreemis 7 lõpmatu ühendi asendada lõplikuga, leides ainult nii palju relatsioonide astmeid, kui suur on hulga elementide arv.



**Teoreem 8.** Kui  $X$  on  $n$ -elemendiline hulk, siis avalduvad sellel hulgal määratud relatsiooni  $\mathcal{R}$  transitiivne sulund  $\mathcal{R}^+$  ja refleksiivne transitiivne sulund  $\mathcal{R}^*$  vastavalt valemitega

$$\mathcal{R}^+ = \bigcup_{i=1}^n \mathcal{R}^i \quad \text{ja} \quad \mathcal{R}^* = \bigcup_{i=0}^{n-1} \mathcal{R}^i.$$

**Tõestus.** Vaatleme kõigepealt refleksiivset transitiivset sulundit. Olgu  $(x, y) \in \mathcal{R}^*$ . Et  $\mathcal{R}^* = \bigcup_{i=0}^{\infty} \mathcal{R}^i$ , siis mingi  $k$  korral  $(x, y) \in \mathcal{R}^k$ . Kui nüüd  $k \geq n$ , siis leidub teoreemi 6 põhjal  $k+1$  elemendist koosnev järjend  $z_0, \dots, z_k$  nii, et  $z_0 = x$ ,  $z_k = y$  ja iga  $i = 0, \dots, k-1$  korral  $(z_i, z_{i+1}) \in \mathcal{R}$ . Et järjendis on elemente rohkem kui hulgas  $X$ , peavad kaks neist olema võrdsed. Olgu  $s$  ja  $t$  võrdsete elementide indeksid. Jätame välja lõigu  $z_{s+1}, \dots, z_t$ , millega saame lühema järjendi, kus kaks järjestikust elementi on ikka relatsioonis  $\mathcal{R}$ . Niisugust operatsiooni korrates jõuame varem või hiljem järjendini, mille elementide arv ei ületa hulga  $X$  elementide arvu  $n$ . Maksimaalse pikkuse puhul on tegemist sellise järjendiga  $z_0, \dots, z_{n-1}$ , et  $z_0 = x$ ,  $z_{n-1} = y$  ja iga  $i = 0, \dots, n-2$  korral  $(z_i, z_{i+1}) \in \mathcal{R}$ . Vastavalt teoreemile 6 siis  $(x, y) \in \mathcal{R}^{n-1}$ . Kui lõppjärjendi pikkus osutub väiksemaks, siis kuulub paar  $(x, y)$  relatsiooni  $\mathcal{R}$  madalamasse astmesse. Erijuhul, kui lõppjärjendi pikkus on 1, siis  $x = y$  ja  $(x, y) \in \mathcal{I}$ .

Eelnevaga oleme tõestanud, et  $\mathcal{R}^* \subseteq \bigcup_{i=0}^{n-1} \mathcal{R}^i$ . Vastupidine sisalduvus on ilmne ega sõltu hulga  $X$  elementide arvust. Niisiis, refleksiivse transitiivse sulundi puhul valem kehtib.

Olgu nüüd  $(x, y) \in \mathcal{R}^+$ . Et  $\mathcal{R}^+ = \bigcup_{i=1}^{\infty} \mathcal{R}^i$ , siis  $(x, y) \in \mathcal{R}^k$  mingi  $k \geq 1$  korral. Võrduse  $\mathcal{R}^k = \mathcal{R} \circ \mathcal{R}^{k-1}$  tõttu leidub element  $z \in X$  nii, et  $(x, z) \in \mathcal{R}$  ja  $(z, y) \in \mathcal{R}^{k-1}$ . Viimasest seosest järeldub analoogiliselt tõestuse eelmise osaga, et  $(z, y) \in \bigcup_{i=0}^{n-1} \mathcal{R}^i$ . Kasutades teoreemis 4 tõestatud seost kompositsiooni ja ühendi vahel, saame  $(x, y) \in \mathcal{R} \circ (\bigcup_{i=0}^{n-1} \mathcal{R}^i) = \bigcup_{i=1}^n \mathcal{R}^i$ . Seega  $\mathcal{R}^+ \subseteq \bigcup_{i=1}^n \mathcal{R}^i$ . Vastupidine sisalduvus on jällegi ilmne.  $\square$

**5. Projektsioon ja lõige.** Lõpuks nimetame veel kahte tehet, mille tulemuseks ei ole relatsioon kahe hulga vahel, vaid nendest ühe alamhulk.

Relatsiooni  $\mathcal{R} \subseteq X \times Y$  projektsiooniks esimesele komponendile nimetatakse hulka  $\pi_1 \mathcal{R} = \{x : (x, y) \in \mathcal{R}\}$  ning projektsiooniks teisele komponendile hulka  $\pi_2 \mathcal{R} = \{y : (x, y) \in \mathcal{R}\}$ . Relatsiooni  $\mathcal{R}$  lõige vasakult alamhulgaga  $X' \subseteq X$  on

$$X' | \mathcal{R} = \{y : (x, y) \in \mathcal{R} \text{ ja } x \in X'\}$$

ning lõige paremalt alamhulgaga  $Y' \subseteq Y$

$$\mathcal{R} \upharpoonright Y' = \{x: (x, y) \in \mathcal{R} \text{ ja } y \in Y'\}.$$

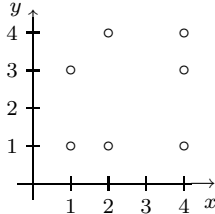
Relatsiooni projektsioon esimesele komponendile on relatsiooni lõige vasakult hulgaga  $X$ , projektsioon teisele komponendile aga lõige paremalt hulgaga  $Y$ .

Lõplike hulkade  $X$  ja  $Y$  puhul võime relatsiooni kujutada graafikul, seades hulga  $X$  elementidele vastavusse  $x$ -telje järjestikused naturaalarvulised punktid ja hulga  $Y$  elementidele analoogiliselt punktid  $y$ -teljel. Kui paar  $(x, y)$  kuulub relatsiooni, siis märgime koordinaattasandil vastava punkti. Relatsiooni projektsioon esimesele koordinaadile tähendab siis tasandipunktide projektsiooni  $x$ -teljele, projektsioon teisele koordinaadile aga punktide projektsiooni  $y$ -teljele.

Vaatleme näiteks hulgal  $X = \{1, 2, 3, 4\}$  määratud relatsiooni

$$\mathcal{R} = \{(1, 1), (1, 3), (2, 1), (2, 4), (4, 1), (4, 3), (4, 4)\}.$$

Märgime koordinaattasandil nende koordinaatidega punktid:



Seejärel projekteerime kogu võrestiku  $x$ -teljele. Relatsiooni  $\mathcal{R}$  projektsiooniks esimesele komponendile on  $\pi_1(\mathcal{R}) = \{1, 2, 4\}$ . Projektsiooniks teisele komponendile saame analoogiliselt  $\pi_2(\mathcal{R}) = \{1, 3, 4\}$ .

Relatsiooni lõiget saab leida samamoodi, ainult pärast teljele projekteerimist tuleb veel leida tulemuse ühisosa hulgaga  $X'$  või  $Y'$ .

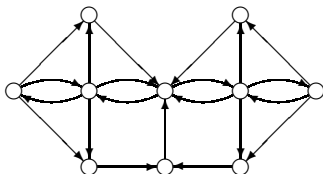
## Ülesanded

1. Reaal arvude hulgal on antud relatsioonid  $\mathcal{R} = \{(x, y): y > 2x\}$ ,  $\mathcal{S} = \{(x, y): x + 3y > 7\}$  ja  $\mathcal{T} = \{(x, y): x < 4y\}$ . Teha joonised, mis kujutavad relatsioone  $(\mathcal{R} \cup \mathcal{S}) \cap \mathcal{T}$  ja  $(\mathcal{R} \cup \mathcal{S})' \cap \mathcal{T}$ .
2. Relatsioon hulkade  $X = \{0, \pm 1, \pm 2, \dots, \pm 4\}$  ja  $\mathbb{N}$  vahel on määratud funktsiooniga  $f(x) = x^2 + 1$ . Leida pöördrelatsioon.
3. Olgu  $X = \{1, 2, 3\}$  ja  $Y = \{4, 5, 6\}$ . Hulkade  $X$  ja  $Y$  vahel olgu määratud relatsioon  $\mathcal{R} = \{(1, 4), (1, 5), (2, 5), (3, 6)\}$  ning hulgal  $Y$  relatsioon  $\mathcal{S} = \{(4, 5), (4, 6), (5, 4), (6, 6)\}$ . Leida relatsioonid  $\mathcal{R} \circ \mathcal{S}$ ,  $\mathcal{R} \circ \mathcal{S}^{-1}$  ja  $\mathcal{S} \circ \mathcal{S}$ .

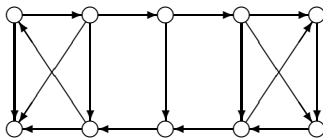
4. Leida reaalarvudel antud relatsioonide  $\mathcal{R} = \{(x, y) : y > 2x + 1\}$  ja  $\mathcal{S} = \{(x, y) : y > 3x + 2\}$  puhul relatsioonid  $\mathcal{R} \circ \mathcal{S}$  ja  $\mathcal{R}^{-1} \circ \mathcal{S}$ .

Järgmistel joonistel on kujutatud teatavate relatsioonide graafid. Leida nende relatsioonide vähim aste, mis osutub täisrelatsiooniks.

5.



6.



Leida järgmiste relatsioonide transitiivsed sulundid, kui relatsioonid on määratud hulgal, mis koosneb esimestest naturaalarvudest.

7.  $\mathcal{R} = \{(1, 3), (1, 4), (2, 5), (3, 4), (4, 2), (5, 2)\}$   
 8.  $\mathcal{R} = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)\}$   
 9.  $\mathcal{R} = \{(1, 2), (2, 5), (3, 4), (3, 5), (4, 1), (4, 5), (5, 2)\}$

10. Vaatleme kõigi inimeste hulgal  $X$  relatsiooni

$$\text{laps} = \{(x, y) : y \text{ on } x\text{-i laps}\}.$$

Väljendada relatsiooni *laps* ning vastavate tehete kaudu relatsioonid

- a)  $\text{vanem} = \{(x, y) : y \text{ on } x\text{-i vanem}\};$   
 b)  $\text{lapselaps} = \{(x, y) : y \text{ on } x\text{-i lapselaps}\};$   
 c)  $\text{vanavanem} = \{(x, y) : y \text{ on } x\text{-i vanavanem}\};$   
 d)  $\text{esivanem} = \{(x, y) : y \text{ on } x\text{-i esivanem}\};$   
 e)  $\text{õdevend} = \{(x, y) : y \text{ on } x\text{-i õde või vend}\};$   
 f)  $\text{sugulane} = \{(x, y) : y \text{ on } x\text{-i sugulane}\}.$

11. Teatava ettevõtte kõigi töötajate hulgal on määratud relatsioonid

$$\text{allub} = \{(x, y) : x \text{ allub } y\text{-le}\},$$

$$\text{austab} = \{(x, y) : x \text{ austab } y\text{-t}\}.$$

Väljendada järgmised väited kujul  $(x, y) \in \mathcal{R}$ :

- a)  $x$  ja  $y$  alluvad samale inimesele;  
 b)  $x$  ja  $y$  alluvad samale inimesele, keda aga kumbki ei austa;  
 c)  $x$ -i ja  $y$ -i ülemused austavad teineteist;  
 d)  $x$ -i mingi alluv ja  $y$ -i mingi alluv austavad teineteist;  
 e)  $x$  austab nii  $y$ -t kui ka kõiki tema alluvaid;  
 f)  $x$  ja  $y$  pole vastastikku teineteise alluvad.

12. Vaatleme suunatud graafi  $G$  tippude hulgal määratud relatsiooni

$$kaar = \{(u, v): \text{tipust } u \text{ viib kaar tippu } v\}.$$

Väljendada relatsiooni  $kaar$ , tehete ja relatsioonide vahelise võrduse abil väited

- $G$  naabusmaatriks on sümmeetriline;
  - $G$  on tugevalt sidus;
  - $G$  on nõrgalt sidus;
  - $G$  ei sisalda silmuseid;
  - $G$  ei sisalda suunatud tsükleid.
13. Vaatleme naturaalarvude hulgal  $\mathbb{N}$  määratud relatsioone  $>$ ,  $<$ ,  $\geq$ ,  $\leq$ ,  $=$  ja  $\neq$ . Millised neist on teiste kaudu avaldatavad? Milline on minimaalne arv relatsioone, mille kaudu saab kõik need relatsioonid avaldada?
14. Olgu  $X$  teatava hulga  $A$  kõigi mittetühjade alamhulkade hulk, st  $X = \mathcal{P}(A) \setminus \{\emptyset\}$ . Vaatleme sellel hulgal määratud relatsioone  $\mathcal{R} = \{(U, V): U \subseteq V\}$  ja  $\mathcal{S} = \{(U, V): U \cap V \neq \emptyset\}$ . Tõestada, et  $\mathcal{S} = \mathcal{R}^{-1} \circ \mathcal{R}$ .
15. Tõestada, et mistahes kahe relatsiooni  $\mathcal{R}$  ja  $\mathcal{S}$  korral kehtivad võrdused  $(\mathcal{R}_1 \cup \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cup \mathcal{R}_2^{-1}$  ja  $(\mathcal{R}_1 \cap \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cap \mathcal{R}_2^{-1}$ .
16. Leida võimalikult väikesel hulgal määratud relatsioonid  $\mathcal{R}$  ja  $\mathcal{S}$ , et ei kehtiks võrdus  $(\mathcal{R} \circ \mathcal{S})' = \mathcal{R}' \circ \mathcal{S}'$ .
17. Millisel sammul tekib tõrge, kui püüame teoreemis 5 tõestada kuuluvust vastupidises suunas?
18. Näidata, et teoreemi 5 seoses ei tarvitse võrdus kehtida isegi juhul, kui kõik relatsioonid on määratud ühel ja samal hulgal.
19. Tõestada, et kehtivad seosed  $(\mathcal{R} \cup \mathcal{S}) \circ \mathcal{T} = (\mathcal{R} \circ \mathcal{T}) \cup (\mathcal{S} \circ \mathcal{T})$  ja  $(\mathcal{R} \cap \mathcal{S}) \circ \mathcal{T} \subseteq (\mathcal{R} \circ \mathcal{T}) \cap (\mathcal{S} \circ \mathcal{T})$ .
20. Relatsioon  $\mathcal{R}$  on määratud  $n$ -elemendilisel hulgal. Tõestada, et kui  $\mathcal{R}^n \neq \emptyset$ , siis iga naturaalarvu  $k$  korral  $\mathcal{R}^k \neq \emptyset$ .
21. Hulgal  $X = \{a, b, c, d\}$  on antud relatsioon
- $$\mathcal{R} = \{(a, d), (b, b), (d, a), (d, c)\}.$$
- Leida vähim relatsioon, mis sisaldab relatsiooni  $\mathcal{R}$  ja on: a) refleksiivne ja sümmeetriline; b) sümmeetriline ja transitiivne; c) refleksiivne, sümmeetriline ja transitiivne.
22. Tõestada, et transitiivne sulund ja refleksiivne transitiivne sulund on omavahel seotud võrdusega  $\mathcal{R}^+ = \mathcal{R} \circ \mathcal{R}^*$ .

23. Tõestada või lükata ümber väide: mistahes relatsiooni  $\mathcal{R}$  korral  $(\mathcal{R}^{-1})^+ = (\mathcal{R}^+)^{-1}$ .
24. Tõestada või lükata ümber väide: mistahes relatsiooni  $\mathcal{R}$  korral  $(\mathcal{R}')^+ = (\mathcal{R}^+)'$ .
25. Leida näide  $n$ -elemendilisel hulgal määratud relatsioonist  $\mathcal{R}$ , mille korral  $\mathcal{R}^+ \neq \cup_{i=1}^{n-1} \mathcal{R}^i$ . Millise omadusega peab relatsioon  $\mathcal{R}$  olema, et kehtiks võrdus  $\mathcal{R}^+ = \cup_{i=1}^{n-1} \mathcal{R}^i$ ?
26. Tõestada, et  $n$ -elemendilisel hulgal määratud relatsiooni  $\mathcal{R}$  refleksiivne transitiivne sulund avaldub valemiga  $\mathcal{R}^* = (\mathcal{R} \cup \mathcal{I})^{n-1}$ .
27. Tõestada, et relatsiooni  $\mathcal{R} \subseteq X \times Y$  sümmeetriline sulund avaldub kujul  $\mathcal{R} \cup \mathcal{R}^{-1}$ .
28. Olgu  $\mathcal{R}$  ja  $\mathcal{S}$  sümmeetrilised relatsioonid. Millised relatsioonidest  $\mathcal{R} \cup \mathcal{S}$ ,  $\mathcal{R} \cap \mathcal{S}$ ,  $\mathcal{R}'$ ,  $\mathcal{R}^{-1}$ ,  $\mathcal{R} \circ \mathcal{S}$ ,  $\mathcal{R}^+$  on siis samuti sümmeetrilised?
29. Olgu  $\mathcal{R}$  ja  $\mathcal{S}$  antisümmeetrilised relatsioonid. Millised relatsioonidest  $\mathcal{R} \cup \mathcal{S}$ ,  $\mathcal{R} \cap \mathcal{S}$ ,  $\mathcal{R}'$ ,  $\mathcal{R}^{-1}$ ,  $\mathcal{R} \circ \mathcal{S}$ ,  $\mathcal{R}^+$  on siis samuti antisümmeetrilised?
30. Olgu  $\mathcal{R}$  ja  $\mathcal{S}$  transitiivsed relatsioonid. Millised relatsioonidest  $\mathcal{R} \cup \mathcal{S}$ ,  $\mathcal{R} \cap \mathcal{S}$ ,  $\mathcal{R}'$ ,  $\mathcal{R}^{-1}$ ,  $\mathcal{R} \circ \mathcal{S}$ ,  $\mathcal{R}^+$  on siis samuti transitiivsed?
31. Olgu  $\mathcal{R}$  mingi relatsioon. Tõestada, et  $\mathcal{R}$  on
- refleksiivne parajasti siis, kui  $\mathcal{I} \subseteq \mathcal{R}$ ;
  - antirefleksiivne parajasti siis, kui  $\mathcal{I} \subseteq \mathcal{R}'$ ;
  - sümmeetriline parajasti siis, kui  $\mathcal{R}^{-1} = \mathcal{R}$ ;
  - antisümmeetriline parajasti siis, kui  $\mathcal{R}^{-1} \cap \mathcal{R} \subseteq \mathcal{I}$ ;
  - transitiivne parajasti siis, kui  $\mathcal{R}^2 \subseteq \mathcal{R}$ .
32. Tõestada, et kui relatsioon  $\mathcal{R}$  on refleksiivne, siis  $\mathcal{R} \subseteq \mathcal{R}^2$ .
33. Tõestada, et relatsioon  $\mathcal{R}$  on sümmeetriline parajasti siis, kui  $\mathcal{R}' \cup \mathcal{R}^{-1} = \mathcal{U}$ .
34. Olgu  $\mathcal{R}$  mingi relatsioon. Teha kindlaks, kas kehtivad järgmised väited: a) kui  $\mathcal{R}$  on sümmeetriline, siis ka  $\mathcal{R}^2$  on sümmeetriline; b) kui  $\mathcal{R}^2$  on sümmeetriline, siis ka  $\mathcal{R}$  on sümmeetriline.
35. Olgu  $\mathcal{R} \subseteq X \times Y$ . Tõestada, et relatsioonid  $\mathcal{R} \circ \mathcal{R}^{-1}$  ja  $\mathcal{R}^{-1} \circ \mathcal{R}$  on sümmeetrilised. Millisel tingimusel on kumbki neist refleksiivne?
36. Olgu  $\mathcal{R}$  ja  $\mathcal{S}$  hulgal  $X$  määratud sümmeetrilised relatsioonid. Tõestada, et relatsioon  $\mathcal{R} \circ \mathcal{S}$  on sümmeetriline parajasti siis, kui kehtib võrdus  $\mathcal{R} \circ \mathcal{S} = \mathcal{S} \circ \mathcal{R}$ .

## X. BOOLE'I MAATRIKSID

**1. Boole'i maatriksi mõiste.** Käsitledes arve 1 ja 0 tõeväärtustena (kus 1 tähistab tõest ja 0 väära tõeväärtust), võib nende arvudega sooritada lausearvutuse tehteid, näiteks leida eitust, konjunktsiooni ja disjunktsiooni. Samal viisil saab viimased tehted üle kanda maatriksitele, mille iga element on kas 1 või 0. Maatriksit, mille kõik elemendid kuuluvad hulka  $\{0, 1\}$ , nimetatakse *Boole'i maatriksiks*.

Kui  $A = (a_{ij})$  on Boole'i maatriks mõõtmetega  $m \times n$ , siis tema eitus on Boole'i maatriks  $C = (c_{ij})$ , kus iga  $i$  ja  $j$  korral  $c_{ij} = \neg a_{ij}$ . Maatriksi  $A$  eitust tähistakse kujul  $\neg A$ .

Kahe samade mõõtmetega Boole'i maatriksi  $A = (a_{ij})$  ja  $B = (b_{ij})$  korral võib defineerida nende *konjunktsiooni*, milleks on maatriks  $C = (c_{ij})$  elementidega  $c_{ij} = a_{ij} \& b_{ij}$ , ning maatriksite  $A$  ja  $B$  *disjunktsiooni*, mille puhul tulemusmaatriksi  $C = (c_{ij})$  elemendid arvutatakse valemist  $c_{ij} = a_{ij} \vee b_{ij}$ . Kahe maatriksi  $A$  ja  $B$  konjunktsiooni ja disjunktsiooni märgitakse vastavalt tähisega  $A \& B$  ja  $A \vee B$ . Kõigi kolme tehte puhul saame antud ühest või kahest  $(m \times n)$ -maatriksist uuesti  $(m \times n)$ -maatriksi.

Need kolm tehet langevad täpselt kokku oma lausearvutuse analoogidega juhul, kui piirduda maatriksitega, millel on üksainus rida ja üksainus veerg.

*Näide 1.* Vaatleme Boole'i maatrikseid

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Nende maatriksite konjunktsiooni leidmiseks arvutame konjunktsiooni maatriksi  $A$  elemendi ja maatriksi  $B$  samas kohas asuva elemendi vahel. Maatriksite disjunktsioon arvutatakse analoogiliselt, leides maatriksite samas reas ja samas veerus asuvate elementide disjunktsiooni. Seega

$$A \& B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{ja} \quad A \vee B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Maatriksi eituse leidmisel tuleb kõigi elementide väärtused muuta vastupidiseks, näiteks

$$\neg A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Peale lausearvutuse tehete võib vaadelda veel ka maatriksite *Boole'i korrutist*. Kui  $A$  ja  $B$  on Boole'i maatriksid, seejuures  $A$  mõõtmetega  $m \times n$  ning  $B$  mõõtmetega  $n \times l$ , siis nende maatriksite Boole'i korrutis on maatriks  $C = (c_{ik})$  mõõtmetega  $m \times l$ , kusjuures

$$c_{ik} = \bigvee_{j=1}^n a_{ij} \& b_{jk}.$$

Boole'i korrutis sarnaneb maatriksite harilikku korrutisega, ainult arvude korrutamist tõlgendatakse siin tõeväärtuste konjunktsioonina ja arvude liitmist disjunktsioonina. Seda, et maatriks  $C$  on maatriksite  $A$  ja  $B$  Boole'i korrutis, märgitakse kujul  $C = AB$ .

**Näide 2.** Korrutades eelmises näites vaadeldud maatriksid  $A$  ja  $B$ , saame tulemuseks maatriksi

$$AB = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Näiteks esimese rea esimene saadakse siin maatriksi  $A$  esimesest reast ja maatriksi  $B$  esimesest veerust teheteaga  $1 \& 0 \vee 1 \& 0 \vee 0 \& 1$ , mis annab tulemuse 0.

Lõpuks on Boole'i maatriksitega võimalik teostada veel mõningaid tehteid, mida saab teostada maatriksitega üldse, näiteks Boole'i maatriksi  $A = (a_{ij})$  transponeeritud maatriks on maatriks  $A^T = (a_{ji})$ .

**2. Tehted relatsioonidega Boole'i maatriksite abil.** Relatsiooni maatriksesituses vastab kahe lõpliku hulga vahel määratud relatsioonile  $\mathcal{R}$  Boole'i maatriks  $R$ . Järgnevas tõestame, et vastavus relatsioonide ja maatriksite vahel on üksühene ka tehete mõttes: igale tehetele relatsioonidega vastab tehe maatriksitega.

**Teoreem 1.** *Lõplike hulkade vahel määratud relatsioonide korral kehtivad järgmised väited.*

- Kui  $R$  on relatsiooni  $\mathcal{R} \subseteq X \times Y$  Boole'i maatriks, siis relatsioonide  $\mathcal{R}'$  ja  $\mathcal{R}^{-1}$  Boole'i maatriksid on vastavalt  $\neg R$  ja  $R^T$ .*
- Kui  $R$  ja  $S$  on relatsioonide  $\mathcal{R} \subseteq X \times Y$  ja  $\mathcal{S} \subseteq X \times Y$  Boole'i maatriksid, siis relatsioonide  $\mathcal{R} \cup \mathcal{S}$  ja  $\mathcal{R} \cap \mathcal{S}$  Boole'i maatriksid on vastavalt  $R \vee S$  ja  $R \& S$ .*
- Kui  $R$  ja  $S$  on relatsioonide  $\mathcal{R} \subseteq X \times Y$  ja  $\mathcal{S} \subseteq Y \times Z$  Boole'i maatriksid, siis relatsiooni  $\mathcal{R} \circ \mathcal{S}$  Boole'i maatriks on  $RS$ .*

**Tõestus.** Nende väidete tõestused on võrdlemisi sirgjoonelised. Tõestame näiteks väite b) relatsioonide ühendi kohta.

Olgu  $X = \{x_1, x_2, \dots, x_m\}$  ja  $Y = \{y_1, y_2, \dots, y_n\}$ . Meil on vaja näidata, et kui  $R = (r_{ij})$ ,  $S = (s_{ij})$  ja  $T = (t_{ij})$  on vastavalt relatsioonide  $\mathcal{R}$ ,  $\mathcal{S}$  ja  $\mathcal{T} = \mathcal{R} \cup \mathcal{S}$  Boole'i maatriksid, siis kehtib võrdus  $T = R \vee S$ . Tõepoolest, sammukaupa lahti kirjutades saame

$$\begin{aligned} t_{ij} = 1 &\Leftrightarrow (x_i, y_j) \in \mathcal{T} \Leftrightarrow (x_i, y_j) \in \mathcal{R} \cup \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow (x_i, y_j) \in \mathcal{R} \text{ või } (x_i, y_j) \in \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow r_{ij} = 1 \text{ või } s_{ij} = 1 \Leftrightarrow r_{ij} \vee s_{ij} = 1. \end{aligned}$$

Seega  $t_{ij} = 1$  parajasti siis, kui  $r_{ij} \vee s_{ij} = 1$ , ehk  $T = R \vee S$ .

Tõestame veel väite c). Olgu  $X = \{x_1, \dots, x_m\}$ ,  $Y = \{y_1, \dots, y_n\}$  ja  $Z = \{z_1, \dots, z_l\}$ . Sarnaselt eelneva juhuga on vaja näidata, et kui  $R = (r_{ij})$ ,  $S = (s_{jk})$  ja  $T = (t_{ik})$  on vastavalt relatsioonide  $\mathcal{R}$ ,  $\mathcal{S}$  ja  $\mathcal{T} = \mathcal{R} \circ \mathcal{S}$  Boole'i maatriksid, siis kehtib võrdus  $T = RS$ . Tõepoolest, iga  $i$  ja  $j$  korral

$$\begin{aligned} t_{ik} = 1 &\Leftrightarrow (x_i, z_k) \in \mathcal{T} \Leftrightarrow (x_i, z_k) \in \mathcal{R} \circ \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow \text{leidub } y_j \text{ nii, et } (x_i, y_j) \in \mathcal{R} \text{ ja } (y_j, z_k) \in \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow (x_i, y_1) \in \mathcal{R} \text{ ja } (y_1, z_k) \in \mathcal{S} \text{ või } (x_i, y_2) \in \mathcal{R} \text{ ja } (y_2, z_k) \in \mathcal{S} \\ &\quad \text{või } \dots \text{ või } (x_i, y_n) \in \mathcal{R} \text{ ja } (y_n, z_k) \in \mathcal{S} \Leftrightarrow \\ &\Leftrightarrow (r_{i1} = 1 \text{ ja } s_{1k} = 1) \text{ või } (r_{i2} = 1 \text{ ja } s_{2k} = 1) \text{ või } \dots \\ &\quad \dots \text{ või } (r_{in} = 1 \text{ ja } s_{nk} = 1) \Leftrightarrow \\ &\Leftrightarrow r_{i1} \& s_{1k} \vee r_{i2} \& s_{2k} \vee \dots \vee r_{in} \& s_{nk} = 1 \Leftrightarrow \bigvee_{j=1}^n r_{ij} \& s_{jk} = 1. \end{aligned}$$

Boole'i maatriksite korrutise definitsiooni järgi annab samaväärsuste ahela esimene ja viimane liige nüüd  $T = RS$ .

Ülejäänud väited tõestatakse analoogiliselt.  $\square$

**Järeldus 1.** Kui  $R$  on relatsiooni  $\mathcal{R} \subseteq X \times X$  Boole'i maatriks, siis relatsiooni  $\mathcal{R}^n$  Boole'i maatriks on  $R^n$ , kus  $n$  on suvaline mitte-negatiivne täisarv.

**Tõestus.** Et  $\mathcal{R}^n = \mathcal{R} \circ \mathcal{R} \circ \dots \circ \mathcal{R}$ , siis selle relatsiooni maatriks on teoreemi väite c) põhjal  $R \cdot R \cdot \dots \cdot R = R^n$ .  $\square$

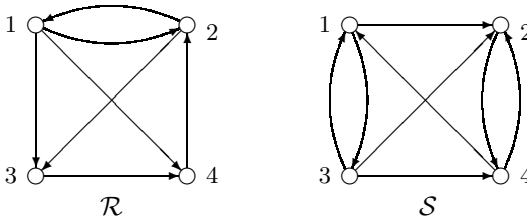
See teoreem annab lihtsa meetodi relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  kompositsiooni arvutamiseks: tuleb leida relatsioonide maatriksid ja korrutada need omavahel. Peale selle, eelmise peatüki teoreemi 8 põhjal kehtib  $n$ -elemendilisel hulgal määratud relatsiooni  $\mathcal{R}$  korral võrdus

$$\mathcal{R}^+ = \mathcal{R} \cup \mathcal{R}^2 \cup \dots \cup \mathcal{R}^n,$$

mille järgi saab kergesti arvutada relatsiooni transitiivset sulundit. Niisugust võtet võib kasutada transitiivse sulundi leidmisel arvutiga, sest arvutis esitamiseks sobib relatsioonide maatrikskuju hästi.



Näide 3. Hulgale  $X = \{1, 2, 3, 4\}$  on järgmisel joonisel kujutatud graafidega antud relatsioonid  $\mathcal{R}$  ja  $\mathcal{S}$ . Leida  $\mathcal{R} \circ \mathcal{S}$ .



Relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  maatriksid on vastavalt

$$R = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{ja} \quad S = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Korrutame need maatriksid:

$$RS = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Tulemuseks saadud maatriks esitab relatsiooni  $\mathcal{R} \circ \mathcal{S}$ . Vajaduse korral võime siit välja kirjutada ka kompositsiooni paaride loetelu  $(1, 1)$ ,  $(1, 2)$ ,  $(1, 4)$ ,  $(2, 1)$ ,  $(2, 2)$ ,  $(2, 3)$ ,  $(2, 4)$ ,  $(3, 1)$ ,  $(3, 2)$ ,  $(4, 4)$  või joonistada vastava graafi.

Näide 4. Arvutada hulgal  $X = \{1, 2, 3\}$  määratud relatsiooni  $\mathcal{R} = \{(1, 3), (2, 1), (2, 2), (3, 2)\}$  transitiivne sulund.

Et hulk, millel relatsioon on antud, koosneb kolmest elemendist, siis eelmise peatüki teoreemi 8 kohaselt  $\mathcal{R}^+ = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3$ . Leiame relatsioonide  $\mathcal{R}$ ,  $\mathcal{R}^2$  ja  $\mathcal{R}^3$  maatriksid:

$$R = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad R^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad R^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Järelikult relatsiooni  $\mathcal{R}^+$  maatriks on

$$R \vee R^2 \vee R^3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Seega on relatsiooni  $\mathcal{R}$  transitiivne sulund täisrelatsioon  $\mathcal{U}$ .

**3. Transitiivse sulundi leidmise algoritm.** Eelnevas vaadeldud meetod relatsiooni transitiivse sulundi leidmiseks on küll lihtne, kuid ta pole kõige efektiivsem. Selleks, et arvutada  $n$ -elemendilisel hulgal määratud relatsiooni  $\mathcal{R}$  transitiivset sulundit, tuleb teostada  $n - 1$  maatriksite korrutamist, millega leiame relatsiooni maatriksile  $R$  lisaks maatriksid  $R^2, \dots, R^n$ , ning kõigi nendega omakorda  $n - 1$  maatriksite disjunktsiooni. Elementaarseid loogikatehteid kulub kahe  $(n \times n)$ -maatriksi korrutamiseks ühtekokku  $n^2(2n - 1)$  ning kahe maatriksi disjunktsiooni arvutamiseks  $n^2$ , seega kulub transitiivse sulundi leidmiseks  $n^2(2n - 1)(n - 1) + n^2(n - 1) = 2n^3(n - 1)$  tehet (keerukusteooria terminites on selle algoritmi tööaeg  $O(n^4)$ ).

Parema algoritmi saame aga suunatud graafide peatükis vaadeldud Floyd-Warshalli algoritmi modifitseerides, kui jätame seal servade pikkused arvestamata ja uurime ainult seda, kas graafi ühest tipust pääseb mööda ahelat teise tippu või mitte. Sellise kujuga algoritmi esitaski kõigepealt Warshall, seetõttu nimetatakse transitiivse sulundi leidmise algoritmi Warshalli algoritmiks.

**Warshalli algoritm.** Olgu relatsioon  $\mathcal{R}$  määratud  $n$ -elemendilisel hulgal Boole'i maatriksiga  $R$ . Peale selle kasutab algoritm töö käigus veel ühte Boole'i maatriksit  $A$  mõõtmega  $n \times n$ .

- Omistada maatriksi  $A$  iga elemendi  $a_{ij}$  väärtuseks maatriksi  $R$  elemendi  $r_{ij}$  väärtus.
- Iga  $k = 1, 2, \dots, n$  korral, iga  $i = 1, 2, \dots, n$  korral, iga  $j = 1, 2, \dots, n$  korral: asendada  $a_{ij}$  väärtus arvuga  $a_{ik} \& a_{kj} \vee a_{ij}$ .

Tulemuseks on maatriks  $A$ .

Relatsiooni  $\mathcal{R}$  transitiivse sulundi  $\mathcal{R}^+$  maatriks ongi maatriks  $A$ . Tõepoolest, kui  $X = \{x_1, x_2, \dots, x_n\}$ , siis välimise tsükli (tsükliindeksiga  $k$ ) igan sammul lisatakse maatriksiga  $A$  esitatud relatsioonile need paarid  $(x_i, x_j)$ , mille korral viib elemendist  $x_i$  elemendini  $x_j$  järjend, kus iga kaks järjestikust elementi on relatsioonis  $\mathcal{R}$  ja ühegi vahepealse elemendi indeks pole suurem kui  $k$ . Selline järjend saab leiduda ainult kahel juhul: kas on juba elemendipaari  $(x_i, x_j)$  puhul leitud järjend, mille vahepealsete elementide indeksid pole suuremad kui  $k - 1$ , või on leitud kaks sama omadusega järjendit elemendipaaride  $(x_i, x_k)$  ja  $(x_k, x_j)$  vahel. Esimesel juhul on tsükli mõnel varasemast sammust  $a_{ij} = 1$ , teisel juhul aga  $a_{ik} = 1$  ja  $a_{kj} = 1$ . Pärast viimast sammu, kui  $k = n$ , on vahepealsete elementidena lubatud kõik elemendid, st arvesse võetud parajasti kõik paarid  $(x_i, x_j)$ , mille komponente üldse mingi järjend ühendab. Teiste sõnadega, on konstrueeritud relatsiooni transitiivne sulund.

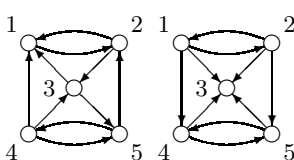
Warshalli algoritmis täidetakse tsüklite sisu  $n^3$  korda ning iga kord tehakse kaks loogilist tehet. Seega kulutab Warshalli algoritm transitiivse sulundi leidmiseks  $2n^3$  tehet (keerukusteooria terminites on algoritmi keerukus  $O(n^3)$ ). Arvu  $n$  suure väärtuse korral on töökulu tunduvalt väiksem kui eelmise meetodi puhul.

## Ülesanded

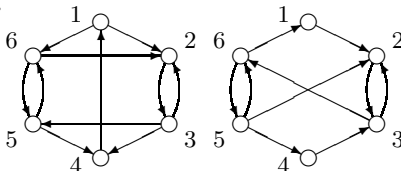
1. Olgu antud relatsioonide  $\mathcal{R}$  ja  $\mathcal{S}$  Boole'i maatriksid. Milline on nende relatsioonide vahe Boole'i maatriks?

Leida järgmiste graafidega määratud relatsioonide kompositsioon.

2.



3.



4. Tõestada, et Boole'i maatriksite korrutamine on distributiivne disjunktsiooni suhtes, st  $A(B \vee C) = (AB) \vee (AC)$ .
5. Tuua näide, millest selgub, et Boole'i maatriksite korrutamine pole distributiivne konjunktsiooni suhtes, st üldiselt ei kehti võrdus  $A(B \& C) = (AB) \& (AC)$ .
6. Hulgal  $X = \{1, 2, \dots, n\}$  on määratud relatsioon

$$\mathcal{R} = \{(x, y) : |x - y| \leq 1\}.$$

Leida relatsiooni  $\mathcal{R}^k$  maatriks, kus  $k = 1, 2, \dots$

7. Milline iseloomulik omadus on relatsiooni maatriksil, kui relatsioon on: a) refleksiivne; b) antirefleksiivne; c) sümmeetriline; d) antisümmeetriline; e) transitiivne?
8. Kasutades asjaolu, et relatsioon  $\mathcal{R}$  on transitiivne parajasti siis, kui  $\mathcal{R}^2 \subseteq \mathcal{R}$ , formuleerida tingimus maatrikskujul antud relatsiooni transitiivsuse kontrollimiseks.
9. Eelmises ülesandes leitud tingimuse abil kontrollida, kas maatriksitega

$$R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

määratud relatsioonid on transitiivsed.

Rakendada Warshalli algoritmi järgmiste maatriksitega määratud relatsioonide transitiivse sulundi arvutamiseks.

10. 
$$R = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

11. 
$$R = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

12. Kuidas tuleks Warshalli algoritmi täiendada, et tema abil saaks arvutada relatsiooni  $\mathcal{R}$  refleksiivset transitiivset sulundit?

13. Meiliviruse levib ühepäevaste tsüklite kaupa. Iga päev kell 23.59 saadab ta ennast edasi kõikidele meiliprogrammi aadressiraamatus leiduvatele aadressidele ning jääb siis ootama järgmist päeva. Vaatleme viiruse levikut kümneliikmelises tutvuskonnas. Järgneva tabeli  $i$ -nda rea  $j$ -ndas veerus on arv 1, kui inimese  $i$  aadressiraamatus on kirjas inimese  $j$  aadress.

	1	2	3	4	5	6	7	8	9	10
1	0	1	0	1	0	0	0	1	0	0
2	1	0	0	0	1	0	0	0	0	0
3	0	0	0	1	0	1	1	0	0	0
4	1	0	1	0	0	0	1	1	0	0
5	1	0	0	0	0	0	0	1	0	0
6	0	0	1	0	0	0	1	0	0	0
7	0	0	0	1	0	0	0	0	0	1
8	0	0	0	1	1	0	0	0	0	0
9	0	0	0	0	0	1	0	0	0	0
10	0	0	1	0	0	0	1	0	1	0

Mitme päevaga on kõigi kümne inimese arvutid nakatunud, kui esimese päeva alguses satub viirus ühte arvutisse neist kümnest? Leida inimesed, kelle arvuti nakatumisel haarab viirus kõige kiiremini kõik arvutid enda valdusse ja kelle puhul kõige aeglasemalt. Milline on minimaalne ja maksimaalne selleks kuluv päevade arv?

14. Muusikapala võib sisaldada järgmist tüüpi osi: *allegro*, *moderato*, *andante* ja *vivo*. Mitmekülgsuse huvides on kehtestatud järgmised kompositsioonipõhimõtted: 1) *andante*-osa ei või vahetult järgneda *moderato*-osale ega *moderato*-osa *andante*-osale, 2) *allegro*-osale ei või vahetult järgneda *vivo*.

- Mitu 4-osalist muusikapala saab neil tingimustel koostada?
- Lisame nüüd tingimuse, et muusikapala peab sisaldama vähemalt kahte tüüpi osa. Mitu võimalust siis on?
- Muusikapalas peab kindlasti olema vähemalt üks *allegro*-osa. Mitu võimalust on nüüd muusikapala koostada?

## XI. JAGUVUS

**1. Arvude jaguvus.** Olgu  $a$  ja  $b$  täisarvud. Ütleme, et arv  $a$  jagab arvu  $b$  ehk arv  $b$  jagub arvuga  $a$ , kui leidub täisarv  $m$  nii, et  $b = am$ . Kui  $a \neq 0$ , siis tähendab jaguvus seda, et jagatis  $b/a$  on täisarv. Kui arv  $a$  jagab arvu  $b$ , siis nimetatakse arvu  $a$  arvu  $b$  teguriks ehk jagajaks ja arvu  $b$  arvu  $a$  kordseks. Asjaolu, et arv  $a$  jagab arvu  $b$ , tähistatakse  $a \mid b$  või ka  $b : a$ . Näiteks  $3 \mid 111$ ,  $7 \mid -91$ ,  $-7 \mid -91$ . Vastupidist asjaolu, et arv  $a$  ei jaga arvu  $b$ , tähistatakse  $a \nmid b$ .

Igal täisarvul  $a$  on kindlasti vähemalt järgmised tegurid:  $a$ ,  $-a$ ,  $1$ ,  $-1$ . Peale selle järeldub jaguvuse definitsioonist, et iga täisarvu  $a$  korral  $a \mid 0$  ning  $0 \mid a$  ainult siis, kui  $a = 0$ . Samuti  $1 \mid a$  iga täisarvu  $a$  korral ning  $a \mid 1$  ainult siis, kui  $a = 1$  või  $a = -1$ .

Kui mingil hulgal, näiteks täisarvude hulgal on defineeritud jaguvus, siis võime sellel hulgal vaadelda jaguvusrelatsiooni

$$\mathcal{R} = \{(a, b) : a \mid b\}.$$

**Teoreem 1.** Täisarvude hulgal  $\mathbb{Z}$  määratud jaguvusrelatsioonil on järgmised omadused.

- Jaguvus on refleksiivne: iga täisarvu  $a$  korral  $a \mid a$ .
- Kui  $a \mid b$  ja  $b \mid a$ , siis  $a = b$  või  $a = -b$ .
- Jaguvus on transitiivne: kui  $a \mid b$  ja  $b \mid c$ , siis  $a \mid c$ .

Tõestus. Omadus a) kehtib ilmselt. Vaatleme omadust b). Kui  $a \mid b$ , siis leidub täisarv  $m$  nii, et  $b = am$ . Samuti, kui  $b \mid a$ , siis leidub täisarv  $n$  nii, et  $a = bn$ . Asetades viimase võrduse eelmisse, saame  $b = bnm$ . Kui nüüd  $b$  erineb nullist, siis võime selle võrduse pooli taandada ning saame  $nm = 1$ . Viimane võrdus saab kehtida ainult siis, kui  $n = 1$ ,  $m = 1$ , millisel juhul  $a = b$ , või siis, kui  $n = -1$ ,  $m = -1$  ja seega  $a = -b$ . Kui aga  $b$  võrdub nulliga, siis järeldub seosest  $a = bn$ , et ka  $a$  võrdub nulliga ning ka sel juhul  $a = b$ .

Tõestame lõpuks omaduse c). Kui  $a \mid b$  ja  $b \mid c$ , siis leiduvad täisarvud  $m$  ja  $n$  nii, et  $b = am$  ja  $c = bn$ . Neist võrdustest saame  $c = amn$ . Et  $mn$  on täisarv, siis jaguvuse definitsiooni kohaselt  $a \mid c$ .  $\square$

**Järeldus 1.** Naturaalarvude hulgal  $\mathbb{N}$  määratud jaguvusrelatsioon on mitterange järjestusrelatsioon.

Tõestus. Naturaalarvude puhul ei saa teoreemi omaduses b) realiseeruda juht  $a = -b$ , järelikult on naturaalarvudel määratud jaguvusrelatsioon antisümmeetriline.  $\square$

Vaatleme nüüd jaguvuse seost aritmeetiliste tehetega. Järgmises teoreemis loetletud väiteid pole raske põhjendada vahetult jaguvuse definitsiooni abil.

**Teoreem 2.** Jaguvusrelatsioonil on järgmised omadused.

- a) Kui  $a \mid b$ , siis  $\pm a \mid \pm b$ .
- b) Kui  $a \mid b$  ja  $a \mid c$ , siis  $a \mid bs + ct$  suvaliste  $s, t \in \mathbb{Z}$  korral.
- c) Seosed  $a \mid b$  ning  $ac \mid bc$  on samaväärsed suvalise  $c \in \mathbb{Z}$ ,  $c \neq 0$  korral.

**Tõestus.** Tõestame näiteks osa b). Kui  $a \mid b$  ja  $a \mid c$ , siis leiduvad täisarvud  $m$  ja  $n$  nii, et  $am = b$  ja  $an = c$ . Korrutades esimest võrdust arvuga  $s$  ja teist arvuga  $t$  ning liites tulemused, saame  $a(ms + nt) = bs + ct$ , mis tähendabki, et  $a \mid bs + ct$ . Teoreemi ülejäänud osad tõestatakse analoogiliselt.  $\square$

Teoreemi osast a) jäeldub, et jaguvuse käsitlemisel võime piirduda ainult mittenegatiivsete täisarvudega. Osast b) saame juhul  $s = 1$ ,  $t = 1$ , et kui arv  $a$  jagab arve  $b$  ja  $c$ , siis jagab ta ka nende summat. Valides aga  $s = 1$ ,  $t = -1$ , saame, et  $a$  jagab arvude  $b$  ja  $c$  vahet.

Olgu  $a > 0$ . Kui arv  $b$  ei jagu arvuga  $a$ , siis võime neid arve jagada jäägiga. Jäägiga jagamine tähendab arvu  $b$  esitamist kujul

$$b = aq + r,$$

kus  $0 \leq r < a$ . Siin nimetatakse arvu  $b$  jagatavaks, arvu  $a$  jagajaks, arvu  $q$  jagatiseks ja arvu  $r$  jäägiks. Näiteks kui  $b = 17$  ja  $a = 7$ , siis esitusest  $17 = 7 \cdot 2 + 3$  saame  $q = 2$  ja  $r = 3$ . Kui  $r = 0$ , siis arv  $a$  jagab arvu  $b$  ehk  $a \mid b$ .

Jäägiga jagamine on alati võimalik (ka juhul, kui jagatav  $b$  on negatiivne). Tõepoolest, arvu  $a$  kordsete

$$\dots, -a, 0, a, 2a, 3a, \dots$$

seast võime leida parajasti ühe sellise kordse  $qa$ , et arv  $b$  asub arvude  $qa$  ja  $(q+1)a$  vahel (esimene kaasa arvatud, teine välja arvatud). Arv  $q$  sobibki siis arvude  $b$  ja  $a$  jagatiseks ning jääk  $r = b - aq$  rahuldab tingimusi  $0 \leq r < a$ .

Tuleb tähele panna, et sõltumata sellest, kas arv  $b$  on positiivne või mitte, peab jääk asuma alati arvude  $0$  ja  $a - 1$  vahel, st ta ei tohi olla negatiivne. Näiteks arvude  $b = -17$  ja  $a = 7$  jagamisel saame  $-17 = (-3) \cdot 7 + 4$  ehk  $q = -3$  ning  $r = 4$ .

**2. Algarvud.** Järgnevas tegeleme ainult naturaalarvudega. Iga naturaalarv  $a$  jagub kindlasti arvudega  $1$  ja  $a$ . Ühest suuremat naturaalarvu  $p$ , mis jagub ainult arvudega  $1$  ja  $p$ , nimetatakse *algarvuks*. Näiteks  $2, 3, 5, 7$  ja  $11$  on algarvud, kuid  $4, 6, 8, 9$  ja  $10$  mitte. Ühest suuremat naturaalarvu, millel leidub teisigi tegureid peale ühe ja iseenda, nimetatakse *kordarvuks*. Kokkuleppeliselt ei loeta arvu  $1$  ei algarvuks ega kordarvuks.

Algarvud on huvi pakkunud juba antiikajast alates. Algarvude jada on väga korrapäratu ja nende puhul on mingeidki seaduspärasusi kindlaks teha väga raske. Mitmed probleemid, millest osa pärineb enam kui 2000 aasta tagant, on siiani lahendamata, mõned on lahenduse leidnud alles viimase sajandi jooksul.

Üks olulisi küsimusi on järgmine: kuidas efektiivselt kontrollida, kas etteantud arv on algarv? Kui on antud arv  $n$ , siis võime vastavalt definitsioonile läbi vaadata kõik arvud 1-st  $n$ -ni ja lugeda kokku, mitmega neist arv  $n$  jagub. Kui arvul ei leidu rohkem tegureid kui 1 ja  $n$ , siis ta on algarv. Selline meetod muutub aga ebapraktiliseks niipea, kui arvu kümnendkohtade arv saab suuremaks paarikümnest. Näiteks 30-kohalise arvu puhul tuleb sooritada suurusjärgus  $10^{30}$  jagamistehet, mis on ilmselt liiga palju.

Mõnevõrra aitab töömahtu vähendada tähelepanek, et piisab läbi vaadata ainult need arvud, mis jäävad arvude 1 ja  $\sqrt{n}$  vahele. Tõepoolest, kui  $n = ab$ , siis ei saa tegurid  $a$  ja  $b$  olla korraga arvust  $\sqrt{n}$  suuremad, sest sel juhul oleks nende korrutis arvust  $n$  suurem. Seega kui  $n$  on kordarv, siis leidub tal tegur, mis ei ületa arvu  $\sqrt{n}$ . Järelikult piisab 30-kohalise arvu puhul läbi kontrollida suurusjärgus  $10^{15}$  arvu, mis oleks kiire arvuti puhul mõeldav, aga suurendades arvu pikkust näiteks kaks korda, kasvab arvutuste maht kiiremagi arvuti puhul üle kättesaamatu määra.

Kiiremaid meetodeid on loodud alles viimase paarikümne aasta jooksul, kui huvi algarvude vastu kasvas seoses nende rakendamisega mitmesugustes krüptosüsteemides. On olemas hulk teste, mis suudavad mõistliku aja jooksul anda vastuse, kas arv on algarv, kuid see vastus on tõenäosuslik: jääb võimalus (kuigi väike), et vastus on vale. Vea tõenäosuse saab siiski arvutusaja pikendamisega teha nii väikeseks kui vaja. Alles 2002. aasta augustis õnnestus rühmal matemaatikutel leida efektiivne meetod, millega saab arvu  $n$  „algarvulisust“ tuvastada absoluutselt täpselt, kuid ka siin on probleemiks see, et meetodi tegelik efektiivsus ilmneb alles suurte arvude juures.

Uurime nüüd lähemalt algarve naturaalarvude jadas. Järgmine teoreem pärineb kreeka matemaatiku Eukleidese (u 325 – u 265 e.m.a) peateoselt „Elemendid“.

**Teoreem 3.** *Leidub lõpmata palju algarve.*

Tõestus. Oletame, et algarve on ainult lõplik hulk. Sel juhul on võimalik nad kõik kirja panna järjendina  $p_1, p_2, \dots, p_k$ . Vaatleme arvu  $n = p_1 p_2 \dots p_k + 1$ . Arv  $n$  peab olema kordarv, sest ta on suurem kõigist algarvudest  $p_1, p_2, \dots, p_k$ , ning ei jagu ühegi nimetatud algarvuga, sest ta annab igaiühega neist jagades jäägiks 1. Siis aga leidub

arvul  $n$  algarvuline tegur, mis erineb antud algarvudest. See on aga vastuolus tingimusega, et järjendis  $p_1, p_2, \dots, p_k$  on üles loetud kõik algarvud. Järelikult ei saa algarve olla lõplik hulk.

Seda teoreemi saab tõestada ka otse, vastuväitelist tõestust kasutamata. Näitame, et iga positiivse arvu  $n$  jaoks leidub temast suurem algarv. Olgu  $p$  arvu  $n! + 1$  vähim tegur. Siis on  $p$  algarv ning lisaks  $p > n$ , sest arvu  $n$  mitte ületavate arvudega jagades annab arv  $n! + 1$  alati jäägiks 1. Seega on  $p$  vajaliku omadusega algarv.  $\square$

On olemas lihtne meetod, mille abil saab leida kõik etteantud arvust  $n$  väiksemad algarvud. Selle autor on kreeka matemaatik Eratosthenes (276 – 194 e.m.a) ja meetod kannab piltlikku nime *Eratosthenese sõel*. Kirjutame välja arvud 1-st  $n$ -ni:

$$1, 2, 3, 4, \dots, n.$$

Kriipsutame maha arvu 1, mis ei ole algarv. Edasi võtame arvu 2 ja kriipsutame maha kõik tema kordsed: 4, 6, 8 jne. Pärast seda on esimene allesjäänud arv 3. Kriipsutame maha kõik arvu 3 kordsed: 6, 9, 12 jne. Järgmine allesjäänud arv on 5, kriipsutame maha kõik arvu 5 kordsed jne. Kui oleme niiviisi kõik kordsed eemaldanud, jäävad järele parajasti kõik algarvud.

Näiteks esimese 100 naturaalarvu hulgas on järgmised algarvud:

$$\begin{array}{cccccccc}
 \times & 2 & 3 & \times & 5 & \times & 7 & \times & \times & \times \\
 11 & \times & 13 & \times & \times & \times & 17 & \times & 19 & \times \\
 \times & \times & 23 & \times & \times & \times & \times & \times & 29 & \times \\
 31 & \times & \times & \times & \times & \times & 37 & \times & \times & \times \\
 41 & \times & 43 & \times & \times & \times & 47 & \times & \times & \times \\
 \times & \times & 53 & \times & \times & \times & \times & \times & 59 & \times \\
 61 & \times & \times & \times & \times & \times & 67 & \times & \times & \times \\
 71 & \times & 73 & \times & \times & \times & \times & \times & 79 & \times \\
 \times & \times & 83 & \times & \times & \times & \times & \times & 89 & \times \\
 \times & \times & \times & \times & \times & \times & 97 & \times & \times & \times
 \end{array}$$

Koostades Eratosthenese sõela abil arvu  $n$  mitteületavate algarvude tabelit, võib iga järjekordse arvu  $p$  kordsete mahatõmbamisest alustada arvust  $p^2$ , sest arvu  $p$  kõik väiksemad kordsed on juba eelmistel sammudel arvesse võetud. Siit järeldub ka, et kui järjekordne läbikriipsutamata arv on suurem kui  $\sqrt{n}$ , siis on kõik algarvud leitud ja tabeli töötlemise võib lõpetada. Näiteks piisab ülaltoodud tabeli koostamiseks vaadelda ainult arvude 2, 3, 5 ja 7 kordseid.

Algarvud paiknevad naturaalarvude reas väga ebahühtlaselt. Leidub algarve, mis asuvad teineteisele väga lähedal, samas leidub pikki lõike, kus pole ühtegi algarvu. Kui kaks algarvu erinevad teineteisest kahe võrra, siis nimetatakse neid *kaksikalgarvudeks* või lühemalt



*kaksikuteks*. Näiteks 11 ja 13 on kaksikud, samuti 101 ja 103 jne. Arvuteoreetikud oletavad, et nagu algarve, nii on ka kaksikalgarve lõpmata palju, kuid seda väidet pole tänini õnnestunud tõestada.

Teise äärmuse annab algarvude jaotumise kohta järgmine teoreem.

**Teoreem 4.** *Naturaalarvude jadas leidub kuitahes pikki lõike, mis koosnevad ainult kordarvudest.*

Tõestus. Vaatleme järjestikuseid naturaalarve

$$n! + 2, n! + 3, n! + 4, \dots, n! + n.$$

Esimene neist jagub 2-ga, teine 3-ga, kolmas 4-ga jne kuni viimane jagub  $n$ -ga. Kokku on meil  $n-1$  järjestikust arvu, millest igaüks jagub mingi arvuga ja pole seetõttu algarv. Arvu  $n$  võime valida kuitahes suure ja konstrueerida seega kuitahes pika kordarvujärjendi.  $\square$

Näiteks 100 järjestikust kordarvu on  $101!+2, 101!+3, 101!+4, \dots, 101!+101$ . Loomulikult võib järjestikustest kordarvudest koosnevaid sama pikki lõike ette tulla varemgi, kui teoreemi tõestus näitab.

Järgnev ribadiagramm kujutab algarvude jaotumist esimese 1000 naturaalarvu seas:



Oluline on veel küsimus sellest, kui palju leidub algarve esimese  $n$  naturaalarvu seas. Selle probleemi uurimiseks on kasutusele võetud *algarvufunktsioon*  $\pi(n)$ , mille väärtus argumenti  $n$  korral näitab, mitu arvu naturaalarvude  $1, 2, \dots, n$  seas on algarvud. Näiteks  $\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(4) = 2, \pi(5) = 3, \pi(6) = 3$  jne. Lihtsat valemit funktsiooni  $\pi(n)$  väärtuste arvutamiseks pole teada (leidub küll mitmeid valemeid, kuid praktilisteks arvutusteks need ei sobi), kuid on olemas ligikaudne valem, mille avastas 18. sajandi lõpus saksa matemaatik Gauss algarvude tabeli empiirilise analüüsi teel ja mille kehtivuse tõestasid prantsuse matemaatikud Hadamard ja de la Vallée Poussin aastal 1896. Vastav väide kannab *algarvuteoreemi* nime.

**Teoreem 5.** *Kehtib asümptootiline ekvivalents*

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

Viimane seos tähendab, et funktsioonide  $\pi(n)$  ja  $n/\ln n$  suhe läheneb arvu  $n$  kasvades väärtusele 1 ehk

$$\lim_{n \rightarrow \infty} \frac{\pi(n) \ln n}{n} = 1.$$

Teoreemi tõestus on raske, mida näitab juba seegi, et tõestada õnnestus see teoreem alles rohkem kui 100 aastat pärast esialgse oletuse püstitamist. Meie seda tõestust täpsemalt ei vaatle, piirdume teoreemi kasutusvõimaluste demonstreerimisega.

*Näide 1.* Hinnata algarvuteoreemi abil, kui palju leidub algarve esimese miljoni ja esimese miljardi naturaalarvu seas.

Esimese miljoni naturaalarvu hulgas on ligikaudu

$$\frac{10^6}{\ln 10^6} \approx 72\,382$$

algarvu, esimese miljardi naturaalarvu seas aga on algarve ligikaudu

$$\frac{10^9}{\ln 10^9} \approx 48\,254\,942.$$

Täpsed väärtused on  $\pi(10^6) = 78\,498$  ja  $\pi(10^9) = 50\,847\,534$ .

*Näide 2.* Hinnata, kui suur on 200-kohaliste naturaalarvude hulgas algarvude osakaal.

Selliste algarvude arvu saame, kui eemaldame arvude  $1, \dots, 10^{200}$  hulgas esinevatest algarvudest kõik algarvud, mis pole suuremad kui  $10^{199}$ . Seega on 200-kohalisi algarve umbes

$$\frac{10^{200}}{\ln 10^{200}} - \frac{10^{199}}{\ln 10^{199}} \approx 1,95 \cdot 10^{197}.$$

Et 200-kohalisi arve on üldse  $10^{200} - 10^{199} = 9 \cdot 10^{199}$ , siis on algarvude osakaal nende hulgas

$$\frac{1,95 \cdot 10^{197}}{9 \cdot 10^{199}} \approx \frac{1}{460}.$$

Seega on 200-kohaliste arvude seas keskmiselt üks arv 460-st algarv.

Tuleb veelkord rõhutada, et kõik need arvutused on üksnes ligikaudsed, sest nad ei kasuta mitte algarvufunktsiooni ennast, vaid tema ligikaudset lähendit.

**3. Aritmeetika põhiteoreem.** Iga ühest suurema naturaalarvu saab lahutada algarvude korrutiseks: algarvu tõlgendame ühetegurlise korrutisena, kui aga arv ei ole algarv, siis ta esitub kahe väiksema arvu korrutisena. Kui tegurid ei ole algarvud, siis nad esituvad omakorda väiksemate arvude korrutisena. Niisugust lahutamist võime jätkata senikaua, kuni enam ühtegi kordarvu tegurite hulgas pole.

Järgmine teoreem näitab, et algarvulisteks teguriteks ehk *algteguriteks* lahutus on alati ühene (arvestamata tegurite järjekorra võimalikku vahetamist). Seda teoreemi nimetatakse ka *aritmeetika põhiteoreemiks* või *jaguvusteooria põhiteoreemiks*.

**Teoreem 6.** Iga ühest suurema naturaalarvu saab parajasti ühel viisil esitada algarvude korrutisena (arvestamata tegurite järjekorda).

Tõestus. Oletame, et teoreemi väide ei kehti, vaid et leidub mingi ühest suurem naturaalarv, mida saab vähemalt kahel viisil lahutada algarvude korrutiseks. Olgu  $n$  vähim selline naturaalarv, millel leidub kaks lahutust:

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_s.$$

Võime eeldada, et  $p_1$  on vähim kõigi siin esinevate algtegurite hulgas, sest vastasel korral võime üleskirjutust ümber korraldada: vahetada lahutused omavahel või muuta tegurite järjekorda. Samuti võime eeldada, et  $p_1$  ei lange kokku ühegi arvuga  $q_1, q_2, \dots, q_s$ , sest muidu saaksime taandada ühise teguri  $p_1$  mõlemal poolel, siis aga tekiks veel väiksem arv, millel on kaks lahutust.

Jagame kõik teise lahutuse tegurid arvuga  $p_1$  ja leiame jäägid:

$$\begin{aligned} q_1 &= p_1 a_1 + r_1 & (1 \leq r_1 < p_1), \\ q_2 &= p_1 a_2 + r_2 & (1 \leq r_2 < p_1), \\ &\dots & \dots \\ q_s &= p_1 a_s + r_s & (1 \leq r_s < p_1). \end{aligned}$$

Ükski jääk  $r_1, r_2, \dots, r_s$  ei saa olla 0, sest ükski arv  $q_1, q_2, \dots, q_s$  kui algarv ei jagu arvuga  $p_1$ .

Moodustame arvu

$$n' = r_1 r_2 \dots r_s.$$

See arv on väiksem kui arv  $n$ , sest kõik jäägid  $r_1, r_2, \dots, r_s$  on väiksemad kui väikseim algarv, mis arvu  $n$  lahutustes üldse leidis. Näitame, et arvul  $n'$  leidub samuti kaks erinevat lahutust algtegurite korrutiseks. Tõepoolest, ühe lahutuse saame ülaltoodust: lahutame jäägid  $r_1, r_2, \dots, r_s$  algteguriteks ja moodustame kõigi tekkinud algtegurite korrutise. Teise lahutuse aga annab võrdus

$$n' = (q_1 - p_1 a_1)(q_2 - p_1 a_2) \dots (q_s - p_1 a_s),$$

mille oleme saanud eelmisest võrdusest jääkide  $r_1, r_2, \dots, r_s$  asendamisel. Viimase võrduse parem pool jagub  $p_1$ -ga, sest sulgude avamisel tekivad liikmed jaguvad kõik arvuga  $p_1$ . Eraldame seega paremast poolest teguri  $p_1$  ja lahutame ülejäänud osa algtegurite korrutiseks.

Need lahutused on erinevad, sest esimeses on kõik algtegurid väiksemad kui  $p_1$  (sest juba kõik jäägid  $r_1, r_2, \dots, r_s$  olid väiksemad kui  $p_1$ ), teises lahutuses aga esineb algtegur  $p_1$ . Oleme leidnud arvust  $n$  väiksema arvu, millel on kaks lahutust. Ent  $n$  oli valitud niisuguste arvude hulgas vähimana ning temast väiksemat enam olla ei saa. Vastuolu tuli oletusest, et leidub mingi arv, millel on kaks lahutust. See oletus ei saa järelikult õige olla.  $\square$

Tõestatud teoreemist järeldub, et iga ühest suurema naturaalarvu  $n$  saab üheselt esitada nn *kanoonilisel kujul*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

kus  $p_1, p_2, \dots, p_k$  on parajasti kõik algarvud, millega  $n$  jagub, ja  $\alpha_1, \alpha_2, \dots, \alpha_k$  on naturaalarvud, mida nimetatakse *kordsusteks*.

Näiteks arvu 600 kanooniline kuju on

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

Kanoonilise kuju põhjal on võimalik kirjeldada arve, millega antud arv jagub.

**Teoreem 7.** *Kui arvu  $n$  kanooniline kuju on*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

*siis selleks, et arv  $m$  oleks arvu  $n$  tegur, on tarvilik ja piisav, et*

$$m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

*kus iga  $i = 1, 2, \dots, k$  korral  $0 \leq \beta_i \leq \alpha_i$ .*

**Tõestus.** *Tarvilikkus.* Olgu  $m \mid n$ . Valime algarvu  $p$ , mille puhul  $p \mid m$ . Siis ka  $p \mid n$ . Aritmeetika põhiteoreemist saame, et  $p$  peab olema üks algarvudest  $p_1, p_2, \dots, p_k$ . Seega võib tegur  $m$  sisaldada ainult neid algtegureid, mis esinevad ka arvus  $n$  ehk teguril  $m$  peab olema teoreemi sõnastuses esitatud kuju.

Jääb veel näidata, et ühegi algteguri kordsus arvus  $m$  ei ületa sama teguri kordsust arvus  $n$ . Olgu  $n = m \cdot q$ . Siis saame võrduse

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} q.$$

Kui mõne  $i$  korral oleks  $\beta_i > \alpha_i$ , siis jagame viimase võrduse pooled läbi arvuga  $p_i^{\alpha_i}$ , millega saaksime arvu  $n/p_i^{\alpha_i}$  jaoks kaks algteguriteks lahtust, millest üks sisaldab tegurit  $p_i$ , teine aga ei sisalda:

$$\frac{n}{p_i^{\alpha_i}} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i - \alpha_i} \dots p_k^{\beta_k} q.$$

See tulemus annaks vastuolu aritmeetika põhiteoreemiga.

*Piisavus.* Jagades arvu  $n$  arvuga  $m$ , saame arvu

$$q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}.$$

See arv on täisarv, sest kõikide algtegurite astendajad on mittenegatiivsed. Seega  $n = m \cdot q$ , mis tähendab, et  $n$  jagub  $m$ -ga.  $\square$

**Näide 3.** Kirjutada välja arvu 60 kõik tegurid.

Vaatleme arvu 60 kanoonilist kuju

$$60 = 2^2 \cdot 3 \cdot 5.$$

Arvu tegurid on

$$\begin{array}{lll} 2^0 3^0 5^0 = 1 & 2^1 3^0 5^0 = 2 & 2^2 3^0 5^0 = 4 \\ 2^0 3^0 5^1 = 5 & 2^1 3^0 5^1 = 10 & 2^2 3^0 5^1 = 20 \\ 2^0 3^1 5^0 = 3 & 2^1 3^1 5^0 = 6 & 2^2 3^1 5^0 = 12 \\ 2^0 3^1 5^1 = 15 & 2^1 3^1 5^1 = 30 & 2^2 3^1 5^1 = 60 \end{array}$$

Kokku on arvu 60 seega 12 tegurit.

Kanoonilise kuju põhjal saab leida ka arvu

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

tegurite arvu ilma kõiki neid tegureid välja kirjutamata. Leides mingit tegurit, tuleb määrata algarvude  $p_1, p_2, \dots, p_k$  astendajad. Esimese astendaja valimiseks on  $\alpha_1 + 1$  võimalust (astendaja väärtus võib tegurisi olla  $0, 1, \dots, \alpha_1$ ), teise astendaja valimiseks  $\alpha_2 + 1$  võimalust jne. Kui oleme kõigi algtegurite astendajad fikseerinud, oleme leidnud ühe teguri. Üldse on erinevate tegurite arv järelikult

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

Näiteks arvu  $60 = 2^2 \cdot 3 \cdot 5$  puhul on  $\alpha_1 = 2, \alpha_2 = 1, \alpha_3 = 1$  ning tegurite arvuks saame  $(2 + 1)(1 + 1)(1 + 1) = 12$ .

## Ülesanded

1. Tõestada, et kui arv  $11a + 3b$  jagub 17-ga, siis ka arv  $5a + 6b$  jagub 17-ga.
2. Tõestada, et kui  $a - b \mid ac + bd$ , siis ka  $a - b \mid ad + bc$ .
3. Tõestada, et iga naturaalarvu  $n$  korral  $n^3 + 5n$  jagub 6-ga.
4. Tõestada, et iga naturaalarvu  $n$  korral  $n^5 - n$  jagub 30-ga.
5. Tõestada, et kolme järjestikuse täisarvu kuupide summa jagub 9-ga.
6. Tõestada, et kui  $n$  on positiivne paarisarv, siis  $5^n - 1$  jagub 24-ga.
7. Tõestada, et iga naturaalarvu  $n$  korral  $5^{2n} + 24n - 1$  jagub 48-ga.
8. Leida kõik naturaalarvud  $a$ , mille korral  $a - 3 \mid a^2 - 3$ .
9. Tõestada, et suvalise täisarvu  $a$  korral  $a - 1 \mid a^n - 1$ , kus  $n$  on naturaalarv.
10. Leida kõik sellised naturaalarvud  $n$ , et suvalise täisarvu  $a$  korral  $a + 1 \mid a^n + 1$ .
11. Leida kõik sellised naturaalarvud  $n$ , et suvalise täisarvu  $a$  korral  $a + 1 \mid a^n - 1$ .

12. Jagada arv  $b$  (jäägiga) arvuga  $a$ , kui: a)  $b = 175$ ,  $a = 13$ ; b)  $b = -320$ ,  $a = 17$ ; c)  $b = -17$ ,  $a = 30$ .
13. Tõestada, et kui  $a$  on naturaalarv ja  $b$  täisarv, siis leiduvad üheselt määratud arvud  $q$  ja  $r$  nii, et  $b = aq + r$  ja  $-a/2 < r \leq a/2$ .
14. Lahutada teguriteks arvud 1147 ja 1716, proovides läbi kõik algarvud kuni arvuni  $\sqrt{1147}$  (vastavalt arvuni  $\sqrt{1716}$ ).
15. Leida Eratosthenese sõela abil kõik algarvud 350 ja 400 vahel.
16. Millise jäägi võib anda algarv jagamisel 6-ga?
17. Millise jäägi võib anda algarv jagamisel 30-ga?
18. Olgu  $p$  ja  $q$  kaks algarvu, kusjuures  $p, q \geq 5$ . Tõestada, et  $p^2 - q^2$  jagub 24-ga.
19. Tõestada, et kui  $a$  ja  $n$  on naturaalarvud, kusjuures  $n \geq 2$ , siis saab arv  $a^n - 1$  olla algarv ainult juhul  $a = 2$ .
20. Tõestada, et kui arv  $2^n - 1$  on algarv, siis peab  $n$  olema algarv.
21. Tõestada, et kui arv  $2^n + 1$  on algarv, siis peab astendaja  $n$  avalduma kujul  $n = 2^k$ .
22. Tõestada, et naturaalarvul  $4k + 3$  on olemas vähemalt üks algtegur, millel on sama kuju.
23. Tõestada, et kujuga  $4k + 3$  arvude hulgas on lõpmata palju algarve.
24. Olgu  $(p_n)$  algarvude jada, st  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$  jne. Tõestada või lükata ümber väide: iga  $n$  korral on arv  $p_1 p_2 \dots p_n + 1$  algarv.
25. Tõestada, et kui  $p$  on algarv siis  $p \mid \binom{p}{k}$  iga täisarvu  $k$  korral, mis rahuldab võrratusi  $0 < k < p - 1$ .
26. Olgu  $a$ ,  $b$  ja  $c$  positiivsed täisarvud, mille korral  $c \mid ab$ . Tõestada, et kui  $\frac{ab}{c}$  on algarv, siis  $a \mid c$  või  $b \mid c$ .
27. Leida arvu 61 507 446 000 lahutus algteguriteks.
28. Arvu *tegurdamispuu* on puu, mille juur on antud arv ning mille igal kordarvule  $n$  vastaval tipul on kaks alluvat  $n_1$  ja  $n_2$  nii, et  $n_1 n_2 = n$ , kus  $n_1, n_2 > 1$ . Joonistada kõik tegurdamispuid, mis vastavad: a) arvule 308, b) arvule 968.
29. Mitu tegurit on arvul 54 217 671 253 200?
30. Leida arv, mille kõigi tegurite korrutis on  $2^{36} 3^{60}$ .
31. Tõestada, et arvul  $n$  saab olla ülimalt  $\log_2 n$  algtegurit.

## XII. SUURIM ÜHISTEGUR

**1. Suurima ühisteguri mõiste.** Naturaalarvude  $a$  ja  $b$  ühisteguriks nimetatakse iga naturaalarvu, millega jagub nii  $a$  kui ka  $b$ . Näiteks on kahel arvul alati olemas ühistegur 1. Arvude  $a$  ja  $b$  ühistegurite hulgast kõige suuremat nimetatakse nende arvude suurimaks ühisteguriks ja märgitakse tähisega  $S\ddot{U}T(a, b)$  (mõnikord kasutatakse ka tähiseid  $(a, b)$  või  $\gcd(a, b)$ ). Analoogilisel viisil defineeritakse mitme arvu  $a_1, a_2, \dots, a_n$  ühistegur ja suurim ühistegur  $S\ddot{U}T(a_1, a_2, \dots, a_n)$ .

Näiteks arvude 12 ja 18 kõik ühistegurid on 1, 2, 3, 6, järelikult  $S\ddot{U}T(12, 18) = 6$ . Mõnikord on kasulik lugeda veel, et  $S\ddot{U}T(a, 0) = a$  iga  $a \geq 0$  korral.

Arve, mille suurim ühistegur on 1, nimetatakse ühistegurita arvudeks. Ühistegurita on näiteks arvud 9 ja 10. Arv 1 on ühistegurita iga teise arvuga, st  $S\ddot{U}T(a, 1) = 1$ . Kui jagame kaks arvu nende suurima ühisteguriga, siis jäävad järele ühistegurita arvud. Teiste sõnadega, kui  $S\ddot{U}T(a, b) = d$ , siis  $S\ddot{U}T\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .

Kahe arvu  $a$  ja  $b$  suurimat ühistegurit saab välja kirjutada nende arvude kanooniliste kujude järgi. Olgu  $p_1, p_2, \dots, p_k$  kõik erinevad algtegurid, mis esinevad arvude  $a$  ja  $b$  kanoonilistes kujudes, ning

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

kus algtegurite astendajad on kõik mittenegatiivsed:  $\alpha_i \geq 0$  ja  $\beta_i \geq 0$ . Nende arvude suvaline ühistegur  $d$  avaldub siis samasugusel kujul

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}.$$

Selleks, et  $d$  üldse oleks arvude  $a$  ja  $b$  ühistegur, peab iga algteguri  $p_i$  astendaja  $\gamma_i$  rahuldama võrratusi  $\gamma_i \leq \alpha_i$  ja  $\gamma_i \leq \beta_i$ , mis üheskoos on samaväärsed tingimusega  $\gamma_i \leq \min(\alpha_i, \beta_i)$ . Teiselt poolt, et  $d$  oleks suurim, peab seal iga algteguri  $p_i$  astendaja  $\gamma_i$  olema maksimaalne võimalik. Kokkuvõttes seega

$$S\ddot{U}T(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}.$$

Ühtlasi oleme selle arutlusega tõestanud suurima ühisteguri järgmise omaduse.

**Teoreem 1.** Arvude  $a$  ja  $b$  suurim ühistegur jagub nende arvude iga ühisteguriga.

Sageli võetakse see omadus aluseks suurima ühisteguri defineerimisel, lugedes arvude  $a$  ja  $b$  suurimaks ühisteguriks vaadeldavate arvude sellist ühistegurit, mis jagub nende iga ühisteguriga. Niisuguse

lähene misviisi eeliseks on see, et siis võime piirduda ainult ühe arvuhulgal määratud relatsiooniga, jaguvusrelatsiooniga, tarvitsemata tähelepanu pöörata arvude järjestusele.

Teeme nüüd kindlaks veel mõned suurima ühisteguri omadused.

**Teoreem 2.** Iga naturaalarvu  $n$  korral

$$\text{SÜT}(na, nb) = n \text{SÜT}(a, b).$$

Tõestus. Olgu  $d$  arvude  $a$  ja  $b$  suurim ühistegur. Tõestatava võrduse parema poole väärtus on siis  $nd$ . Et  $d \mid a$  ja  $d \mid b$ , siis järelikult  $nd \mid na$  ja  $nd \mid nb$ . Seega on  $nd$  arvude  $na$  ja  $nb$  ühistegur.

Näitame nüüd, et  $nd$  on nende arvude suurim ühistegur. Arvude  $na$  ja  $nb$  suurim ühistegur peab olema arvu  $nd$  mingi kordne, st  $\text{SÜT}(na, nb) = knd$ , kus  $k \geq 1$ . Arvestades, et  $d$  on arvude  $a$  ja  $b$  suurim ühistegur, võime kirjutada  $a = da'$  ja  $b = db'$ , kus  $\text{SÜT}(a', b') = 1$ . Siis  $na = nda'$  ja  $nb = دنب'$ . Seostest  $knd \mid na$  ning  $knd \mid nb$  järeldub seetõttu  $k \mid a'$  ja  $k \mid b'$  ehk arv  $k$  on arvude  $a'$  ja  $b'$  ühistegur. Et nende arvude ainuke ühistegur on 1, siis  $k = 1$ . See tähendab, et arvude  $na$  ja  $nb$  suurim ühistegur on  $nd$ .  $\square$

**Järeldus 1.** Kui  $c$  on arvude  $a$  ja  $b$  ühistegur, siis

$$\text{SÜT}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{SÜT}(a, b)}{c}.$$

Tõestus. Teoreemi põhjal

$$\text{SÜT}(a, b) = c \text{SÜT}\left(\frac{a}{c}, \frac{b}{c}\right).$$

Jagades võrduse pooli arvuga  $c$ , saamegi vajaliku tulemuse.  $\square$

**Teoreem 3.** Kui  $\text{SÜT}(a, b) = 1$ , siis iga naturaalarvu  $c$  korral  $\text{SÜT}(ac, b) = \text{SÜT}(c, b)$ .

Tõestus. Olgu  $d$  arvude  $ac$  ja  $b$  mingi ühistegur, see tähendab,  $d \mid ac$  ja  $d \mid b$ . Et  $b \mid bc$ , siis ka  $d \mid bc$ . Järelikult on  $d$  arvude  $ac$  ja  $bc$  ühistegur ning teoreemi 1 põhjal  $d \mid \text{SÜT}(ac, bc)$ . Teoreemist 2 saame, et  $\text{SÜT}(ac, bc) = c \text{SÜT}(a, b) = c$ , mistõttu  $d \mid c$ . Seega on arv  $d$  arvude  $b$  ja  $c$  ühistegur, järelikult  $d \mid \text{SÜT}(b, c)$ .

Vastupidi, olgu  $d$  arvude  $b$  ja  $c$  mingi ühistegur. Siis  $d \mid b$  ja  $d \mid c$ . Et  $c \mid ac$ , siis ka  $d \mid ac$ . Järelikult on  $d$  arvude  $ac$  ja  $b$  ühistegur, mistõttu  $d \mid \text{SÜT}(ac, b)$ .

Niisiis, arvude  $ac$  ja  $b$  iga ühistegur on ka arvude  $b$  ja  $c$  ühistegur ning vastupidi, st nende arvupaaride ühistegurite hulgad on samad. Seepärast on samad ka nende hulkade suurimad elemendid.  $\square$

**Järeldus 2.** Kui  $\text{SÜT}(a, c) = 1$  ja  $\text{SÜT}(b, c) = 1$ , siis kehtib võrdus  $\text{SÜT}(ab, c) = 1$ .



**Tõestus.** Kui  $\text{SÜT}(b, c) = 1$ , siis saame tõestatud teoreemi põhjal  $\text{SÜT}(ab, c) = \text{SÜT}(a, c) = 1$ .  $\square$

**Järeldus 3.** Kui  $a \mid bc$  ning  $\text{SÜT}(a, b) = 1$ , siis  $a \mid c$ .

**Tõestus.** Rakendame teoreemi, arvestades, et tingimus  $a \mid bc$  on samaväärne võrdusega  $\text{SÜT}(bc, a) = a$  ning tingimus  $a \mid c$  võrdusega  $\text{SÜT}(c, a) = a$ .  $\square$

**Järeldus 4.** Kui  $a \mid c$  ja  $b \mid c$  ning  $\text{SÜT}(a, b) = 1$ , siis  $ab \mid c$ .

**Tõestus.** Kirjutame eelduse  $a \mid c$  kujul  $a \mid \frac{c}{b} \cdot b$ . Et  $\text{SÜT}(a, b) = 1$ , siis eelmise järelduse põhjal  $a \mid \frac{c}{b}$ . See aga tähendabki, et  $ab \mid c$ .  $\square$

**Näide 1.** Leida arvude 560 ja 315 suurim ühistegur.

Vastavalt suurima ühisteguri omadustele

$$\text{SÜT}(560, 315) = 5 \text{SÜT}(112, 63).$$

Et arv 63 ei jagu 2-ga, siis võime arvust 112 eraldada kõik tegurid 2:

$$\text{SÜT}(112, 63) = \text{SÜT}(2^4 \cdot 7, 63) = \text{SÜT}(7, 63) = 7.$$

Järelikult

$$\text{SÜT}(560, 315) = 5 \cdot 7 = 35.$$

Mitme arvu suurima ühisteguri leidmiseks võib leida mitu korda järjest kahe arvu suurimat ühistegurit.

**Teoreem 4.** Arvude  $a_1, a_2, \dots, a_n$  suurim ühistegur avaldub kujul

$$\text{SÜT}(a_1, a_2, \dots, a_n) = \text{SÜT}(\dots \text{SÜT}(\text{SÜT}(a_1, a_2), a_3), \dots, a_n).$$

**Tõestus.** Tõestame väite induktsiooniga.

**Baas.** Kui  $n = 2$ , siis on väitel kuju  $\text{SÜT}(a_1, a_2) = \text{SÜT}(a_1, a_2)$ .

**Samm.** Eeldame, et väide kehtib  $n = k$  korral, ning vaatleme juhtu  $n = k + 1$ . Induktsiooni eeldust kasutades saame tõestatavale võrdusele anda kuju

$$\text{SÜT}(a_1, a_2, \dots, a_k, a_{k+1}) = \text{SÜT}(\text{SÜT}(a_1, a_2, \dots, a_k), a_{k+1}).$$

Suvalise arvu  $d$  puhul on tingimused  $d \mid a_1, d \mid a_2, \dots, d \mid a_{k+1}$  samaväärsed tingimustega  $d \mid \text{SÜT}(a_1, a_2, \dots, a_k)$  ja  $d \mid a_{k+1}$ , seetõttu on vasaku poole arvudel  $a_1, a_2, \dots, a_{k+1}$  ja parema poole arvudel  $\text{SÜT}(a_1, a_2, \dots, a_k), a_{k+1}$  samad ühistegurite hulgad ning järelikult langevad kokku ka kummagi poole arvude suurimad ühistegurid.  $\square$

**Näide 2.** Leida arvude 24, 84, 30 ja 75 suurim ühistegur.

Järjest arvutades leiame

$$\text{SÜT}(24, 84) = 12, \quad \text{SÜT}(12, 30) = 6, \quad \text{SÜT}(6, 75) = 3.$$

Järelikult

$$\text{SÜT}(24, 84, 30, 75) = 3.$$

**2. Suurima ühisteguri arvutamine.** Arvude suurimat ühistegurit saab küll leida nende kanoonilise kuju järgi, kuid selline tee ei ole alati kõige otstarbekam – arve algteguriteks lahutada on eriti suurte arvude puhul üsna keeruline. Järgmine algoritm, mis pärineb Eukleideselt ja on tuntud *Eukleidesese algoritmi* nime all, võimaldab suurimat ühistegurit arvutada märgatavalt efektiivsemalt. Formuleerime selle algoritmi järgmisel kujul.

**Eukleidesese algoritm.** Olgu  $a$  ja  $b$  mittenegatiivsed täisarvud.

- Kui  $b = 0$ , siis lõpetada töö.
- Leida muutuja  $a$  jagamisel muutujaga  $b$  tekkiv jääk  $r$ . Omistada muutujale  $a$  muutuja  $b$  väärtus ning muutujale  $b$  väärtus  $r$ . Minna tagasi esimese punkti juurde.

Tulemuseks on muutuja  $a$  väärtus.

*Näide 3.* Leida arvude 560 ja 315 suurim ühistegur Eukleidesese algoritmi abil.

Algoritmi rakendades saame

$$\begin{aligned} \text{SÜT}(560, 315) &= \text{SÜT}(315, 245) = \text{SÜT}(245, 70) = \\ &= \text{SÜT}(70, 35) = \text{SÜT}(35, 0) = 35. \end{aligned}$$

Eukleidesese algoritm lõpetab alati töö, sest iga sammuga asendatakse töödeldav arvupaar  $(a, b)$  paariga  $(b, r)$ , kus  $r$  on  $a$  jagamisel  $b$ -ga tekkiv jääk ning seetõttu  $r < b$ . Arvupaari teine komponent väheneb igal sammul ja varem või hiljem saab ta nulliks.

Algoritmi korrektsus põhineb järgmisel teoreemil.

**Teoreem 5.** *Kui  $r$  on jääk, mis tekib arvu  $a$  jagamisel arvuga  $b$ , siis  $\text{SÜT}(a, b) = \text{SÜT}(b, r)$ .*

*Tõestus.* Eelduse põhjal kehtib võrdus  $a = bq + r$ . Kui  $d$  on arvude  $a$  ja  $b$  mingi ühistegur, siis ka arv  $r = a - bq$  jagub arvuga  $d$ , st viimane on arvude  $b$  ja  $r$  ühistegur. Vastupidi, kui  $d$  on arvude  $b$  ja  $r$  ühistegur, siis jagub ka arv  $a = bq + r$  arvuga  $d$ , mis on seega arvude  $a$  ja  $b$  ühistegur. Järelikult ühtib arvude  $a$  ja  $b$  ühistegurite hulk arvude  $b$  ja  $r$  ühistegurite hulgaga ning nende hulcade suurimad elemendid on samad.  $\square$

Teoreemist järeldub, et Eukleidesese algoritmi igal sammul jääb arvude suurim ühistegur samaks. Kui lõpuks on teine arv kahanenud nulliks, siis on suurim ühistegurit juba lihtne leida, see võrdub esimese arvuga. Kahe arvu suurim ühistegur on seega Eukleidesese algoritmis saadav viimane nullist erinev jääk.

Suurima ühisteguri leidmiseks on Eukleidesese algoritm väga efektiivne selles mõttes, et vajaminev sammude arv sõltub sisendarvude kohtade arvust (st nende pikkusest), mitte aga nende väärtusest.

**Teoreem 6.** *Arvude  $a$  ja  $b$  (kus  $a > b$ ) suurima ühisteguri leidmiseks kutsutab Eukleidese algoritmi ülimalt  $1 + \log_2 a + \log_2 b$  sammu.*

**Tõestus.** Eukleidese algoritmi ühe sammuga asendatakse arvud  $(a, b)$  arvudega  $(b, r)$ , kus  $r$  on arvude  $a$  ja  $b$  jagamisel tekkinud jääk. Seega kehtib võrdus  $a = bq + r$ . Et  $b > r$  ja eelduse  $a > b$  tõttu  $q \geq 1$ , siis  $a > r + r = 2r$ . Järelikult  $ab > 2rb$  ehk  $rb < ab/2$ , mis tähendab, et vaadeldava kahe arvu korrutis kahaneb Eukleidese algoritmi iga sammuga vähemalt kaks korda. Pärast  $k$  sammu on korrutise väärtus seega ülimalt  $ab/2^k$ . Kui pärast  $k$  sammu on mõlemad arvud veel positiivsed, siis kehtib võrratus  $ab/2^k \geq 1$  ehk  $ab \geq 2^k$ , kust saame, et  $k$  peab rahuldama tingimust

$$k \leq \log_2(ab) = \log_2 a + \log_2 b.$$

Seega hiljemalt  $1 + \log_2 a + \log_2 b$  sammu pärast on üks arvudest kindlasti muutunud nulliks.  $\square$

Näiteks kahe 1024-bitise arvu (umbes 300 kümnendkohta) suurima ühisteguri leidmiseks ei kulu rohkem kui

$$1 + \log_2 2^{1024} + \log_2 2^{1024} = 1 + 1024 + 1024 = 2049$$

sammu.

Eukleidese algoritmi rakendusvaldkonnad ulatuvad kaugemalegi kui kahe arvu suurima ühisteguri leidmine.

Rakendades Eukleidese algoritmi naturaalarvudele  $a$  ja  $b$ , saame vahetulemused avaldada kujul

$$\begin{aligned} a &= bq_1 + r_1 & (0 < r_1 < b), \\ b &= r_1q_2 + r_2 & (0 < r_2 < r_1), \\ r_1 &= r_2q_3 + r_3 & (0 < r_3 < r_2), \\ &\dots & \dots \\ r_{k-2} &= r_{k-1}q_k + r_k & (0 < r_k < r_{k-1}), \\ r_{k-1} &= r_kq_{k+1}, \end{aligned}$$

mis vastab algoritmi töökäigule

$$\text{SÜT}(a, b) = \text{SÜT}(b, r_1) = \text{SÜT}(r_1, r_2) = \dots = \text{SÜT}(r_k, 0) = r_k.$$

Avaldame  $k$ -ndast seosest arvu  $r_k$ :

$$r_k = r_{k-2} - r_{k-1}q_k,$$

see sisaldab jääke  $r_{k-1}$  ja  $r_{k-2}$ . Nüüd avaldame samal viisil  $k$ -ndale eelnevast seosest arvu  $r_{k-1}$  ning asendame selle viimasesse võrdusesse. Saame  $r_k = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k$  ehk

$$r_k = -r_{k-3}q_k + r_{k-2}(1 + q_{k-1}q_k).$$

See avaldis sisaldab jääke  $r_{k-2}$  ja  $r_{k-3}$ . Samamoodi jätkates asendame üksteise järel kõik jäägid, kuni lõpuks jõuame võrduseni

$$r_k = as + bt,$$

kus  $s$  ja  $t$  on teatavad täisarvud. Et  $r_k$  on arvude  $a$  ja  $b$  suurim ühistegur, siis oleme saanud järgmise teoreemi.

**Teoreem 7.** *Naturaalarvude  $a$  ja  $b$  suurima ühisteguri võib avaldada kujul*

$$\text{SÜT}(a, b) = as + bt,$$

kus  $s$  ja  $t$  on teatavad täisarvud.

Näide 4. Leida teoreemis 7 nimetatud esitus juhul, kui vaadeldavad arvud on  $a = 92$  ja  $b = 17$ .

Eukleidese algoritmiga saame

$$92 = 17 \cdot 5 + 7$$

$$17 = 7 \cdot 2 + 3$$

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3$$

Eelviimasest reast saame nüüd järk-järgult asendada

$$1 = 7 - 3 \cdot 2$$

$$1 = 7 - (17 - 7 \cdot 2) \cdot 2 = 17 \cdot (-2) + 7 \cdot 5$$

$$1 = 17 \cdot (-2) + (92 - 17 \cdot 5) \cdot 5 = 92 \cdot 5 + 17 \cdot (-27)$$

Seega sobib nõutavaks esituseks näiteks  $1 = 92 \cdot 5 + 17 \cdot (-27)$ .

Vaadeldud võttega saab lahendada ka näiteks *lineaarseid diofantilisi võrrandeid*, st võrrandeid kujul

$$ax + by = c,$$

kus  $a$ ,  $b$  ja  $c$  on etteantud täisarvud ning  $x$  ja  $y$  otsitavad, mis peavad samuti olema täisarvud.

**3. Vähim ühiskordne.** Naturaalarvude  $a$  ja  $b$  *ühiskordseks* nimetatakse iga naturaalarvu, mis jagub nii  $a$ -ga kui  $b$ -ga. Vähimat selliste arvude hulgast nimetatakse arvude  $a$  ja  $b$  *vähimaks ühiskordseks* ja tähistatakse  $\text{VÜK}(a, b)$  (vahel ka  $[a, b]$  või  $\text{lcm}(a, b)$ ). Sarnaselt ühisteguritega vaadeldakse ühiskordset ja vähimat ühiskordset ka suurema hulga arvude juhul.

Näiteks  $\text{VÜK}(12, 18) = 36$ , sest 36 on kõige väiksem naturaalarv, mis jagub nii 12-ga kui ka 18-ga.

Samuti nagu suurimat ühistegurit saab leida arvude kanooniliste kujude abil, võime analoogilise valemi tuletada ka vähima ühiskordse jaoks. Olgu  $a$  ja  $b$  kaks naturaalarvu ning  $p_1, p_2, \dots, p_k$  kõik erinevad algarvud, mis esinevad arvude  $a$  ja  $b$  algteguritena. Lähtume jälle nende arvude esitustest

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

kus algtegurite astendajad on kõik mittenegatiivsed. Arvude  $a$  ja  $b$  vähim ühiskordne peab sisaldama iga algtegurit  $p_i$  minimaalses astmes, mis pole väiksem selle teguri astmest arvus  $a$  ega astmest arvus  $b$ . Järelikult peab  $p_i$  astendajaks olema  $\max(\alpha_i, \beta_i)$ . Seetõttu

$$\text{VÜK}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}.$$

Vähim ühiskordne ja suurim ühistegur on teineteisega seotud: teades neist ühte, saab teise lihtsasti arvutada.

**Teoreem 8.** *Kehtib võrdus*  $\text{SÜT}(a, b) \text{VÜK}(a, b) = ab$ .

*Tõestus.* Kasutame eespool saadud kanoonilisi kujusid  $\text{SÜT}(a, b)$  ja  $\text{VÜK}(a, b)$  jaoks. Kui need avaldised omavahel korrutada, siis saame algteguri  $p_1$  astendajaks

$$\min(\alpha_1, \beta_1) + \max(\alpha_1, \beta_1),$$

kus  $\alpha_1$  on selle algteguri astendaja arvus  $a$  ja  $\beta_1$  astendaja arvus  $b$ . Sõltumata sellest, kumb neist astendajatest on suurem, võrdub viimane summa ikka avaldisega  $\alpha_1 + \beta_1$ . See on aga algteguri  $p_1$  astendaja korrutises  $ab$ . Korrates sama arutluskäiku kõigi arvudes  $a$  ja  $b$  esinevate algtegurite kohta, saame, et tõestatava võrduse kummalgi pool on kõigi algtegurite astendajad võrdsed.  $\square$

**Järeldus 5.** *Kui*  $\text{SÜT}(a, b) = 1$ , *siis*  $\text{VÜK}(a, b) = ab$ .

Kehtib ka järgmine omadus, mis võimaldab vähima ühiskordse defineerimisel piirduda jaguvusrelatsiooniga täisarvude hulgal.

**Järeldus 6.** *Arvude*  $a$  *ja*  $b$  *vähim ühiskordne on nende arvude iga ühiskordse tegur.*

*Tõestus.* Olgu  $k$  arvude  $a$  ja  $b$  mingi ühiskordne. Siis teoreemist 2

$$ab \text{SÜT}\left(\frac{k}{a}, \frac{k}{b}\right) = \text{SÜT}(kb, ka) = k \text{SÜT}(b, a).$$

Järelikult

$$ab \text{SÜT}\left(\frac{k}{a}, \frac{k}{b}\right) \text{VÜK}(a, b) = k \text{SÜT}(a, b) \text{VÜK}(a, b) = kab.$$

Seega

$$\text{SÜT}\left(\frac{k}{a}, \frac{k}{b}\right) \text{VÜK}(a, b) = k$$

ehk  $\text{VÜK}(a, b)$  on  $k$  tegur.  $\square$

Teoreem 8 võimaldab taandada vähima ühiskordse omaduste uurimise suurima ühisteguri omaduste uurimisele. Mitmed suurima ühisteguri omadused kanduvad vahetult üle ka vähimale ühiskordsele.

**Teoreem 9.** *Iga naturaalarvu*  $n$  *korral*

$$\text{VÜK}(na, nb) = n \text{VÜK}(a, b).$$

Tõestus. Teoreemi 2 põhjal

$$\text{SÜT}(na, nb) = n \text{SÜT}(a, b),$$

eelmise teoreemi põhjal aga

$$\text{SÜT}(na, nb) \text{VÜK}(na, nb) = n^2 ab$$

ja

$$n \text{SÜT}(a, b) \cdot n \text{VÜK}(a, b) = n^2 ab.$$

Järelikult

$$\text{SÜT}(na, nb) \text{VÜK}(na, nb) = n \text{SÜT}(a, b) \cdot n \text{VÜK}(a, b),$$

millest võrdseid tegureid taandades saamegi nõutud tulemuse.  $\square$

**Järeldus 7.** Kui  $c$  on arvude  $a$  ja  $b$  ühistegur, siis

$$\text{VÜK}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{VÜK}(a, b)}{c}.$$

Tõestus. Kirjutame teoreemi põhjal välja võrduse

$$\text{VÜK}(a, b) = c \text{VÜK}\left(\frac{a}{c}, \frac{b}{c}\right)$$

ning jagame selle mõlemat poolt arvuga  $c$ .  $\square$

Vähima ühiskordse seos suurima ühisteguriga võimaldab ka vähima ühiskordse arvutamiseks kasutada Eukleidese algoritmi.

## Ülesanded

Leida arvude suurim ühistegur.

1. 221 ja 391                      3. 15283 ja 11160                      5. 120, 750 ja 1200  
2. 481 ja 1755                      4. 123123 ja 555555                      6. 588, 2058 ja 2849

Taandada murrud.

7.  $\frac{555}{2627}$                       8.  $\frac{9968}{7832}$                       9.  $\frac{3381821}{17759}$                       10.  $\frac{48539591}{6186818}$
11. Tõestada, et murd  $\frac{21n+4}{14n+3}$  on taandumatu iga naturaalarvu  $n$  korral.
12. Tõestada, et kui arvude  $a$  ja  $b$  suurim ühistegur on  $d$ , siis ka arvude  $15a+8b$  ja  $13a+7b$  suurim ühistegur on  $d$ .
13. Tõestada, et kaks järjestikust Fibonacci arvu on ühistegurita.
14. Tõestada, et iga kahe ühistegurita arvu  $m$  ja  $n > 1$  korral leidub arv  $k$  nii, et jääk arvu  $mk$  jagamisel  $n$ -ga on 1.
15. Tõestada, et kui  $a \mid bc$ , siis  $a \mid \text{SÜT}(a, b)c$ .

16. Tuua näide kolmest täisarvust  $a$ ,  $b$  ja  $c$  ( $a < b$ ,  $a < c$ ), mille korral  $a \mid bc$ , aga  $a \nmid b$  ega  $a \nmid c$ .

17. Tõestada, et kui  $a \mid c$  ja  $b \mid c$ , siis  $ab \mid \text{SÜT}(a, b)c$ .

18. Tõestada, et naturaalarvude  $a$ ,  $b$  ja  $c$  korral kehtivad võrdused

a)  $\text{SÜT}(a, \text{VÜK}(b, c)) = \text{VÜK}(\text{SÜT}(a, b), \text{SÜT}(a, c));$

b)  $\text{VÜK}(a, \text{SÜT}(b, c)) = \text{SÜT}(\text{VÜK}(a, b), \text{VÜK}(a, c)).$

Teiste sõnadega, suurim ühistegur ja vähim ühiskordne on vastastikku teineteise suhtes distributiivsed.

19. Tõestada, et naturaalarvude  $a$  ja  $b$  korral kehtivad võrdused

a)  $\text{SÜT}(a, \text{VÜK}(a, b)) = a;$

b)  $\text{VÜK}(a, \text{SÜT}(a, b)) = a.$

See tähendab, suurima ühisteguri ja vähima ühiskordse vahel kehtib neelduvus.

20. Tõestada, et kui arvud  $a$  ja  $b$  on arvu  $n$  tegurid, siis

$$\text{SÜT}(a, b) \text{VÜK}\left(\frac{n}{a}, \frac{n}{b}\right) = \text{VÜK}(a, b) \text{SÜT}\left(\frac{n}{a}, \frac{n}{b}\right) = n.$$

21. Tõestada, et  $\text{SÜT}(a^m - 1, a^n - 1) = a^{\text{SÜT}(m, n)} - 1$ .

22. Tõestada, et suvaliste naturaalarvude  $a$ ,  $b$ ,  $c$ ,  $d$  korral kehtib  $\text{SÜT}(a, b) \text{SÜT}(c, d) \mid \text{SÜT}(ac, bd)$ . Leida arvud  $a$ ,  $b$ ,  $c$ ,  $d$ , mille korral  $\text{SÜT}(a, b) \text{SÜT}(c, d) \neq \text{SÜT}(ac, bd)$ .

23. Arvujada  $(a_n)$  defineeritakse järgmiselt:  $a_0 = 2$  ning iga  $n \geq 0$  korral  $a_{n+1} = 1 + a_0 a_1 \dots a_n$ . Tõestada, et selle jada elemendid on paarikaupa ühistegurita.

24. Tõestada, et kui  $\text{SÜT}(a, b) = 1$ , siis  $\text{SÜT}(a + b, a - b)$  on kas 1 või 2.

25. Leida arvude  $a = 60$  ja  $b = 35$  suurim ühistegur  $d$  ning määrata  $x$  ja  $y$  nii, et  $ax + by = d$ .

26. Tõestada, et diofantilisel võrrandil  $ax + by = c$  leidub lahend parajasti siis, kui  $\text{SÜT}(a, b) \mid c$ .

27. Kilpla küla otsustas kasutusele võtta oma raha. Laekus kolm ideepakkumist: 53- ja 45-kroonine, 34- ja 51-kroonine ning 49- ja 56-kroonine. Millise pakkumise peab külavolikogu vastu võtma, et oleks võimalik tehinguid sooritada ühe krooni täpsusega? Kuidas peavad ostja ja müüja raha sel juhul vahetama, et maksta ühte krooni? Leida võimalused, mille puhul kasutatakse minimaalne arv rahatähti.

28. Lahendada diofantiline võrrand  $36x + 15y + 114z = 3072$ .

### XIII. KONGRUENTSID

**1. Kongruentsi mõiste ja omadused.** Olgu  $m$  mingi fikseeritud naturaalarv, mida edaspidi nimetame *mooduliks*. Täisarve  $a$  ja  $b$  nimetatakse *kongruentseteks* mooduli  $m$  järgi, kui nad annavad  $m$ -ga jagades sama jäägi. Kui arvud  $a$  ja  $b$  on kongruentsed mooduli  $m$  järgi, siis seda märgitakse nn *kongruentsina*

$$a \equiv b \pmod{m}$$

(ja mittekongruentsust vastavalt tähisega  $a \not\equiv b \pmod{m}$ ).

Kui kaks arvu on kongruentsed, siis nende vahe ilmselt jagub mooduliga  $m$ . Tõepoolest, kui näiteks  $a = q_1m + r$  ja  $b = q_2m + r$ , siis  $a - b = (q_1 - q_2)m$ . Kui kahe arvu  $a$  ja  $b$  vahe jagub  $m$ -ga, siis peavad nende arvude jagamisel  $m$ -ga tekkima võrdsed jäägid. Seega on kaks arvu mooduli  $m$  järgi kongruentsed parajasti siis, kui nende vahe jagub mooduliga  $m$ .

**Teoreem 1.** *Kongruentsus mooduli  $m$  järgi on ekvivalents täisarvude hulgal.*

**Tõestus.** Lihtne on kindlaks teha, et kongruentsus on refleksiivne (see tähendab, iga täisarvu  $a$  korral  $a \equiv a \pmod{m}$ ), sümmeetriline (st kui  $a \equiv b \pmod{m}$ , siis  $b \equiv a \pmod{m}$ ), ning transitiivne (st kui  $a \equiv b \pmod{m}$  ja  $b \equiv c \pmod{m}$ , siis  $a \equiv c \pmod{m}$ ).  $\square$

**Teoreem 2.** *Kui  $a \equiv b \pmod{m}$  ja  $d \mid m$ , siis  $a \equiv b \pmod{d}$ .*

**Tõestus.** Kui  $m \mid a - b$  ja  $d \mid m$ , siis ka  $d \mid a - b$ .  $\square$

Teiste sõnadega, kui kaks arvu on kongruentsed mingi mooduli järgi, siis on nad kongruentsed ka selle mooduli iga teguri järgi.

**Teoreem 3.** *Kui kehtivad  $a \equiv b \pmod{m_1}$ ,  $a \equiv b \pmod{m_2}$ , ...,  $a \equiv b \pmod{m_n}$ , siis  $a \equiv b \pmod{VÜK(m_1m_2 \dots m_n)}$ .*

**Tõestus.** Et  $m_1 \mid a - b$ ,  $m_2 \mid a - b$ , ...,  $m_n \mid a - b$ , siis on  $a - b$  arvude  $m_1, m_2, \dots, m_n$  ühiskordne. Et vähim ühiskordne on iga ühiskordne tegur, siis  $VÜK(m_1, m_2, \dots, m_n) \mid a - b$ .  $\square$

Järgnevalt esitame mõned kongruentside omadused, mis puudutavad aritmeetilisi tehteid.

**Teoreem 4.** *Kui  $a \equiv b \pmod{m}$  ning  $c \equiv d \pmod{m}$ , siis ka  $a + c \equiv b + d \pmod{m}$  ja  $ac \equiv bd \pmod{m}$ .*

**Tõestus.** Vahe  $(a + c) - (b + d) = (a - b) + (c - d)$  jagub arvuga  $m$ , sest vastavalt eeldusele jagub arvuga  $m$  viimase summa kumbki liidetav. Järelikult  $a + c \equiv b + d \pmod{m}$ .

Et  $ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$ , siis vahe  $ac - bd$  jagub  $m$ -ga, sest nii  $a - b$  kui ka  $c - d$  jaguvad  $m$ -ga. Seega kehtib ka  $ac \equiv bd \pmod{m}$ .  $\square$



**Järeldus 1.** Kui  $a \equiv b \pmod{m}$  ning  $c \equiv d \pmod{m}$ , siis ka  $a - c \equiv b - d \pmod{m}$ .

Tõestus. Kui teoreemis 4 valime  $a = b = -1$ , siis saame kongruentsi  $-c \equiv -d \pmod{m}$ . Liidame selle tulemuse kongruentsiga  $a \equiv b \pmod{m}$ , mis annabki  $a - c \equiv b - d \pmod{m}$ .  $\square$

Teoreem 4 ja järeldus 1 näitavad, et kongruentse võib pooliti liita, lahutada ja korrutada.

**Järeldus 2.** Kui  $a \equiv b \pmod{m}$ , siis suvaliste täisarvude  $u$  ja  $v$  korral  $a + um \equiv b + vm \pmod{m}$ .

Tõestus. Teoreemis 4 valime  $c = um$  ja  $d = vm$ .  $\square$

**Järeldus 3.** Kui  $a \equiv b \pmod{m}$ , siis suvalise täisarvu  $k$  korral  $ak \equiv bk \pmod{m}$ .

Tõestus. Teoreemis 4 tarvitseb valida  $c = d = k$ .  $\square$

Viimased kaks järeldust ütlevad, et kongruentsi kummalegi poolele võib liita või temast lahutada suvaline arv korda moodulit ning et kongruentsi pooli võib korrutada ühe ja sama arvuga. Neid järeldusi kasutatakse sageli siis, kui on vaja kongruentsi lahendada, st leida sellist arvu, mis etteantud kongruentsi rahuldab.

**Järeldus 4.** Kui  $a \equiv b \pmod{m}$ , siis iga naturaalarvu  $n$  korral  $a^n \equiv b^n \pmod{m}$ .

Tõestus. Korrutame omavahel pooliti  $n$  ühesugust kongruentsi  $a \equiv b \pmod{m}$ ,  $\dots$ ,  $a \equiv b \pmod{m}$ .  $\square$

Kongruentside pooliti jagamise kohta võib ütelda järgmist.

**Teoreem 5.** Kui  $ak \equiv bk \pmod{m}$  ning  $\text{SÜT}(k, m) = 1$ , siis  $a \equiv b \pmod{m}$ .

Tõestus. Kui arvud  $ak$  ja  $bk$  on kongruentsed mooduli  $m$  järgi, siis  $m \mid ak - bk$  ehk  $m \mid (a - b)k$ . Et siin  $\text{SÜT}(k, m) = 1$ , siis eelmise peatüki järelduse 3 põhjal  $m \mid a - b$ . Seega on arvud  $a$  ja  $b$  kongruentsed.  $\square$

Niiisi, kongruentsi pooli võib jagada mingi ühe ja sama arvuga siis, kui see arv on mooduliga ühistegurita. Näiteks võime kongruentsi  $48 \equiv 6 \pmod{7}$  pooli taandada 6-ga ja saada tulemuseks kongruentsi  $8 \equiv 1 \pmod{7}$ . Kui aga arvul ja moodulil leidub ühest suurem ühistegur, siis selle arvuga kongruentsi taandada üldiselt ei või. Näiteks püüdes kongruentsi  $30 \equiv 12 \pmod{9}$  pooli jagada 6-ga, saaksime mittekehtiva kongruentsi  $5 \equiv 2 \pmod{9}$ .

**Teoreem 6.** Kongruents  $a \equiv b \pmod{m}$  kehtib parajasti siis, kui suvalise naturaalarvu  $k$  korral  $ak \equiv bk \pmod{mk}$ .

Tõestus. Kongruents  $a \equiv b \pmod{m}$  kehtib parajasti siis, kui  $a - b$  jagub  $m$ -ga. See aga on samaväärne seosega  $mk \mid ak - bk$ , mis tähendab, et  $ak \equiv bk \pmod{mk}$ .  $\square$

Viimasest omadusest järeldub muuhulgas, et kui kongruentsi vasakul ja paremal poolel ning moodulil on ühine tegur, siis võib kõiki kolme selle ühise teguriga taandada. Näiteks eespool vaadeldud kongruentsis  $30 \equiv 12 \pmod{9}$  võime jagada vasaku poole, parema poole ja mooduli ühisteguriga 3. Sellega tekib kongruents  $10 \equiv 4 \pmod{3}$ , mis kehtib. Tulemuse poole võime nüüd taandada arvuga 2, sest sellel arvul ja moodulil puudub ühistegur (teoreem 5), nii saame veel ühe kehtiva kongruentsi  $5 \equiv 2 \pmod{3}$ .

**2. Kongruentside kasutamine.** Kongruentsi mõiste abil saab lahendada ülesandeid, kus tuleb arvutada mingi avaldise jääk jagamisel naturaalarvuga. Tehete teostamisel võime igal sammul asendada vahetulemustes saadavad arvud moodulist väiksemate arvudega.

*Näide 1.* Leida jääk, mis tekib arvu  $1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$  jagamisel 7-ga.

Olgu lühiduse mõttes  $a = 1395^4 \cdot 675^3 + 12 \cdot 17 \cdot 22$ . Esmalt asendame kõik moodulist 7 suuremad tegurid ja astendatavad moodulist 7 väiksemate arvudega. Et  $1395 \equiv 2 \pmod{7}$ ,  $675 \equiv 3 \pmod{7}$ ,  $12 \equiv 5 \pmod{7}$ ,  $17 \equiv 3 \pmod{7}$  ja  $22 \equiv 1 \pmod{7}$ , siis

$$a \equiv 2^4 \cdot 3^3 + 5 \cdot 3 \cdot 1 \pmod{7}.$$

Edasi lihtsustame astmed ja korrutised. Et  $2^4 = 16 \equiv 2 \pmod{7}$ ,  $3^3 = 27 \equiv 6 \pmod{7}$  ning  $5 \cdot 3 \cdot 1 = 15 \equiv 1 \pmod{7}$ , siis

$$a \equiv 2 \cdot 6 + 1 \pmod{7}.$$

Lõpuks  $2 \cdot 6 + 1 = 13 \equiv 6 \pmod{7}$  ja seega

$$a \equiv 6 \pmod{7}.$$

*Näide 2.* Leida jääk, mis tekib arvu  $53 \cdot 47 \cdot 51 \cdot 43$  jagamisel 56-ga.

Et  $53 \cdot 47 = 2491 \equiv 27 \pmod{56}$  ja  $51 \cdot 43 = 2193 \equiv 9 \pmod{56}$ , siis

$$53 \cdot 47 \cdot 51 \cdot 43 \equiv 27 \cdot 9 \pmod{56}.$$

Edasi, seoste  $27 \cdot 9 = 243 \equiv 19 \pmod{56}$  tõttu

$$53 \cdot 47 \cdot 51 \cdot 43 \equiv 19 \pmod{56}.$$

Teine, arvutuslikult võib-olla lihtsam võimalus selle ülesande lahendamiseks on kasutada negatiivseid jääke. Et tegurid on moodulist ainult natuke väiksemad, siis võime võtta  $53 \equiv -3 \pmod{56}$ ,  $47 \equiv -9 \pmod{56}$ ,  $51 \equiv -5 \pmod{56}$ ,  $43 \equiv -13 \pmod{56}$ . Seega

$$53 \cdot 47 \cdot 51 \cdot 43 \equiv (-3)(-9)(-5)(-13) \pmod{56}.$$

Edasi saame  $(-3)(-9)(-5)(-13) = 1755 \equiv 19 \pmod{56}$  ehk

$$53 \cdot 47 \cdot 51 \cdot 43 \equiv 19 \pmod{56}.$$

Krüptograafias ja üldse arvuteooria mitmesugustes rakendusvaldkondades tuleb tihti peale arvutada jääke, mis tekivad astme  $a^n$  jagamisel arvuga  $m$ . Seejuures võib astendaja  $n$  olla väga suur, näiteks 100-kohaline arv. Niisugusel juhul ei tule kõne alla arvutada järjestikku korrutades  $a^n$  ja seejärel leida jääk jagamisel  $m$ -ga, sest korrutamisi kulub liiga palju (100-kohalise astendaja puhul suurusjärgus  $10^{100}$ ) ning teiseks võib arv  $a^n$  olla liiga pikk, et teda üldse välja kirjutada või arvuti mälus hoida (100-kohalise astendaja puhul suurusjärgus  $a^{100}$  kohta). Seetõttu kasutatakse suurte astmete puhul tekkiva jäägi arvutamiseks *ruututõstmismeetodit*.

*Näide 3.* Olgu vaja leida arvu  $45^{69}$  jagamisel arvuga 89 tekkiv jääk. Selleks arvutame järk-järgult

$$\begin{aligned} 45 &\equiv 45 \pmod{89}, \\ 45^2 &\equiv 67 \pmod{89}, \\ 45^4 &= (45^2)^2 \equiv 39 \pmod{89}, \\ 45^8 &= (45^4)^2 \equiv 8 \pmod{89}, \\ 45^{16} &= (45^8)^2 \equiv 64 \pmod{89}, \\ 45^{32} &= (45^{16})^2 \equiv 2 \pmod{89}, \\ 45^{64} &= (45^{32})^2 \equiv 4 \pmod{89}. \end{aligned}$$

Edasi valime välja need astendajad, mille summa on 69. Arvestades, et  $69 = 64 + 4 + 1$ , saame

$$45^{69} = 45^{64} \cdot 45^4 \cdot 45^1 \equiv 4 \cdot 39 \cdot 45 \equiv 7020 \equiv 78 \pmod{89}.$$

Selle, millised astmed on vaja korrutada, määrab astendaja kahendesitus. Näiteks arvul 69 on kahendsüsteemis kuju 1000101, seega tuleb omavahel korrutada astmed, mis vastavad kuuendale kahendkohale (astendaja  $2^6$ ), teisele kahendkohale (astendaja  $2^2$ ) ja nullindale kahendkohale (astendaja  $2^0$ ).

Ruututõstmismeetodi algoritmi võib kirja panna järgmiselt. Olgu antud täisarv  $a$  ning naturaalarvud  $n$  ja  $m$ .

- Omistada muutujale  $b$  väärtus 1.
- Korrata, kus  $n > 0$ :
  - kui  $n$  on paaritu arv, siis omistada muutujale  $b$  jääk, mis tekib arvu  $ba$  jagamisel  $m$ -ga;
  - omistada muutujale  $n$  arv  $\lfloor n/2 \rfloor$ ;
  - omistada muutujale  $a$  jääk arvu  $a^2$  jagamisel  $m$ -ga.

Tulemuseks on muutuja  $b$  väärtus.

Paneme tähele, et siin säilitatakse ruututõstmise tulemust ühesainsas muutujas  $a$  ja korrutatakse teda vastusele  $b$  juurde siis, kui vastav järk kahendesituses on 1. Et kõik ruututõstmised ja korrutamised sooritatakse mooduli  $m$  järgi, siis jääb vahetulemuste pikkus tõkestatuks.

Muuhulgas saab seda meetodit rakendada ka näiteks statistikas, kui on vaja tõsta maatrikseid suurde astmesse.

Vaatleme veel ühte kongruentside rakendust. Kui soovime teha kindlaks, kas mingi arv jagub 3-ga või 9-ga, siis piisab kontrollida, kas arvu ristsumma jagub vastavalt 3-ga või 9-ga. Analoogilisi tunnuseid saab tuletada ka teiste arvudega jagumise kontrolliks.

*Näide 4.* Tuletada jaguvustunnus jagumiseks 11-ga.

Olgu uuritav arv  $n = \overline{a_k a_{k-1} \dots a_1 a_0}$  avaldatud kümnenndkohtade kaudu kujul

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0.$$

Kui soovime leida, selle arvu jagamisel 11-ga tekkivat jääki, siis vaatleme toodud lahutuses esinevaid kümne astmeid. Paneme tähele, et

$$\begin{aligned} 10^0 &\equiv 1 \pmod{11}, \\ 10^1 &\equiv -1 \pmod{11}, \\ 10^2 &\equiv 1 \pmod{11}, \\ 10^3 &\equiv -1 \pmod{11}. \end{aligned}$$

Kehtib üldine seaduspära: iga  $i \geq 0$  korral  $10^i \equiv (-1)^i \pmod{11}$ . Tõepoolest, et  $10 \equiv -1 \pmod{11}$ , siis tõstes mõlemad pooled astmesse  $i$ , saame  $10^i \equiv (-1)^i \pmod{11}$ .

Niiis

$$n \equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + \dots - a_1 + a_0 \pmod{11}.$$

Tulemuse parem pool on vahelduvate märkidega summa arvu  $n$  kümnenndkohtadest, lõpust lugedes on paariskohtadel märk  $+$ , paaritutel kohtadel aga  $-$ . Järelikult annab arv  $n = \overline{a_k a_{k-1} \dots a_1 a_0}$  jagamisel 11-ga sama jäägi nagu avaldis

$$(a_0 + a_2 + \dots) - (a_1 + a_3 + \dots).$$

Näiteks arv 34425730438 jagub 11-ga, sest 11-ga jagub avaldis

$$(8 + 4 + 3 + 5 + 4 + 3) - (3 + 0 + 7 + 2 + 4) = 27 - 16 = 11.$$

Üldiselt, arv  $n = \overline{a_k a_{k-1} \dots a_1 a_0}$  jagub arvuga  $m$  parajasti siis, kui arvuga  $m$  jagub arv

$$a_k r_k + a_{k-1} r_{k-1} + \dots + a_1 r_1 + a_0,$$

kus  $r_i$  on jääk, mis tekib arvu  $10^i$  jagamisel  $m$ -ga.

**3. Fermat' väike teoreem.** Üks kõige laialdasemalt kasutatavaid teoreeme arvuteoorias on järgmine teoreem, mille tõestas prantsuse matemaatik Pierre de Fermat (1601 – 1665) ja mida tema järgi nimetatakse *Fermat' väikeseks teoreemiks*.

**Teoreem 7.** *Kui  $p$  on algarv, siis iga täisarvu  $a$  korral, mis ei jagu  $p$ -ga, kehtib kongruents  $a^{p-1} \equiv 1 \pmod{p}$ .*

Tõestus. Vaatleme arve

$$1, 2, \dots, p-1$$

ning korrutame neid kõiki arvuga  $a$ . Saame arvud

$$a, 2a, \dots, (p-1)a.$$

Näitame, et kui viimaseid arve jagada  $p$ -ga, siis tekivad parajasti jäägid  $1, 2, \dots, p-1$  mingis järjekorras.

Tõepoolest, ükski tekkivatest jääkidest ei saa võrduda nulliga, sest ei arv  $a$  ega ka ükski kordaja  $1, 2, \dots, p-1$  ei jagu  $p$ -ga. Samuti ei saa kaks jääki olla võrdsed, sest kui arvud  $ia$  ja  $ja$ , kus  $i < j$ , annaksid  $p$ -ga jagades sama jäägi, siis peaks nende vahe  $(j-i)a$  jaguma  $p$ -ga. Seda aga ei saa olla, sest  $a$  ei jagu  $p$ -ga ning ka kordaja  $j-i$  kui  $p$ -st väiksem positiivne arv ei jagu  $p$ -ga. Siit järeldub, et arvud  $a, 2a, \dots, (p-1)a$  peavad  $p$ -ga jagamisel andma jäägid  $1, 2, \dots, p-1$ . Siis aga

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

ehk

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Taandades kongruentsi pooli arvuga  $(p-1)!$ , mis on mooduliga  $p$  ühistegurita, saame

$$a^{p-1} \equiv 1 \pmod{p}. \quad \square$$

Tihti peale pannakse Fermat' teoreem kirja ka mõnevõrra teistsuguses variandis, mille formuleerime järgmise järeldusena.

**Järeldus 5.** *Kui  $p$  on algarv, siis iga täisarvu  $a$  korral kehtib kongruents  $a^p \equiv a \pmod{p}$ .*

Tõestus. Kui  $a$  ei jagu  $p$ -ga, siis saame Fermat' teoreemi põhjal  $a^{p-1} \equiv 1 \pmod{p}$ . Korrutades mõlemat poolt  $a$ -ga, jõuamegi vajaliku tulemuseni.

Kui aga  $a$  jagub  $p$ -ga, siis  $a^p \equiv 0 \pmod{p}$  ja  $a \equiv 0 \pmod{p}$  ning väide kehtib ka sel juhul.  $\square$

Näide 5. Leida jääk, mis tekib arvu  $3^{4565}$  jagamisel 13-ga.

Fermat' teoreemi põhjal  $3^{12} \equiv 1 \pmod{13}$ . Jagame astendaja 4565 arvuga 12 ja leiame jäägi:  $4565 = 380 \cdot 12 + 5$ . Nüüd

$$3^{4565} = (3^{12})^{380} 3^5 \equiv 1^{380} 3^5 \equiv 243 \equiv 32 \equiv 6 \pmod{13}.$$

## Ülesanded

Leida jääk arvu  $a$  jagamisel arvuga  $b$ .

- $a = (35 + 55)^7$ ,  $b = 9$
  - $a = 52^{54}54^{52}$ ,  $b = 53$
  - $a = 1^3 + 2^3 + \dots + 15^3$ ,  $b = 14$
  - $a = 10^{1024} - 1$ ,  $b = 11$
  - $a = (15^{10})!$ ,  $b = 16$
  - $a = 99!$ ,  $b = 101$
7. Tõestada, et kongruentsi pooltel on mooduliga sama suurim ühis-tegur, st kui  $a \equiv b \pmod{m}$ , siis  $\text{SÜT}(a, m) = \text{SÜT}(b, m)$ .
8. Tõestada, et kui kongruentsi  $a \equiv b \pmod{m}$  üks pool ja moodul jaguvad mingi arvuga, siis jagub ka teine pool selle arvuga.
9. Tõestada, et kui  $\text{SÜT}(a, m) = 1$ , siis leidub selline täisarv  $b$ , et  $ab \equiv 1 \pmod{m}$ .
10. Tõestada, et kui kehtivad kongruentsid  $ac \equiv bd \pmod{m}$  ning  $c \equiv d \pmod{m}$ , kusjuures  $\text{SÜT}(c, m) = 1$ , siis kehtib ka kongruents  $a \equiv b \pmod{m}$ .
11. Olgu  $p$  algarv. Tõestada, et kui kehtib kongruents
- $$a^2 \equiv b^2 \pmod{p},$$
- siis
- $$a \equiv b \pmod{p} \quad \text{või} \quad a \equiv -b \pmod{p}.$$
12. Tõestada, et kui  $p$  on algarv, siis kehtib suvaliste täisarvude  $a$  ja  $b$  korral kongruents
- $$(a + b)^p \equiv a^p + b^p \pmod{p}.$$
13. Tõestada, et kui  $p$  on algarv, siis kongruentsist  $a \equiv b \pmod{p^n}$  järgeldub kongruents  $a^p \equiv b^p \pmod{p^{n+1}}$ .
14. Tõestada, et naturaalarv  $n$  on algarv parajasti siis, kui iga  $k = 0, 1, \dots, n - 1$  korral
- $$\binom{n-1}{k} \equiv (-1)^k \pmod{n}.$$
15. Kangelane valdab eeskujulikult nelja mõõgalööki, millega saab lohel maha raiuda vastavalt 1, 15, 48 või 67 pead, kuid seejuures kasvab mahalöödud peade asemele kohe vastavalt 349, 0, 57 või 16 uut pead. Kui viimase hoobiga saavad kõik lohe pead maha löödud, siis enam uusi päid juurde ei kasva – viimaseks löögiks peab aga jääma täpselt niipalju päid, kuipalju ühe löögiga maha raiuda saab. Kas kangelane suudab lohest jagu saada, kui lohel on: a) 2004 pead; b) 2005 pead?
16. Kaks mängijat koostavad  $2k$ -numbrilist arvu, kirjutades kordamööda arvu lõppu ühe numbriga 1-st 5-ni. Alustaja vastasmängija

eesmärk on saada pärast viimase numbri kirjutamist 9-ga jaguv arv, alustaja eesmärk on seda takistada. Kummal mängijal leidub võitev strateegia, kui a)  $k = 10$ ; b)  $k = 15$ ?

17. Tõestada, et kui  $3^n \equiv -1 \pmod{10}$ , siis ka  $3^{n+4} \equiv -1 \pmod{10}$ .
18. Leida jääkide hulk, mille annavad arvud  $3^n$  jagamisel 30-ga.
19. Tuletada jaguvustunnus jagumiseks 7-ga, 13-ga ja 99-ga.
20. Tõestada, et igal algarvul leidub kordne, mis koosneb ainult numbritest 0 ja 3.
21. Tõestada, et iga algarvu  $p > 5$  korral leidub selline  $p$ -ga jaguv arv, mis koosneb ainult ühtedest.
22. 2004-kohaline arvu esimene number on 6. Suvaline kahest kõrvutiastuvast numbrist moodustatud arv jagub kas 17-ga või 23-ga. Milline on arvu viimane number?
23. Tõestada, et iga paaritu arvu ruut annab 16-ga jagades jäägiks kas 1 või 9.
24. Tõestada, et naturaalarvu kujul  $4k + 3$  ei saa esitada kahe täisarvu ruutude summana.
25. Tõestada, et kui  $n \equiv 7 \pmod{8}$ , siis arvu  $n$  ei saa avaldada kolme täisarvu ruutude summana.
26. Ruumi teatavat punktide hulka laiendatakse sammhaaval selliselt, et hulga mingit punkti peegeldatakse mingi teise punkti suhtes ja lisatakse saadud punkt hulgale juurde. Kas hulgale, mis koosneb seitsmest ühikkuubi tipust, saab pärast mingit arvu peegeldamisi lisada juurde ka ühikkuubi kaheksanda tipu?
27. Kaardipakis on  $2^n$  kaarti. Kaardipakki segatakse järgmisel viisil. Kui enne järjekordset segamist on kaardid pakis järjekorras

$$a_1, a_2, a_3, a_4, \dots, a_{2^n-1}, a_{2^n},$$

siis pärast segamist on kaardid pakis järjekorras

$$a_{2^{n-1}+1}, a_1, a_{2^{n-1}+2}, a_2, \dots, a_{2^n}, a_{2^{n-1}}.$$

Leida vähim segamiste arv, mille järel kaardipakis taastub esialgne järjekord.

28. Ringikujulise laua ümber istub  $n$  last. Õpetaja valib ühe lapse ja annab talle kompveki. Seejärel jätab ta päripäeva liikudes ühe lapse vahele ning annab kompveki järgmisele, siis jätab vahele kaks last, annab järgmisele kompveki, jätab vahele kolm last jne. Leida kõik arvu  $n$  väärtused, mille korral iga laps saab lõpuks vähemalt ühe kompveki.

Leida jääk arvu  $a$  jagamisel arvuga  $b$ .

29.  $a = 6^{52}$ ,  $b = 11$

32.  $a = 2^{10^6}$ ,  $b = 17$

30.  $a = 15^{83}$ ,  $b = 13$

33.  $a = 2^{22}3^{33}4^{44}$ ,  $b = 11$

31.  $a = 6^{100003}$ ,  $b = 101$

34.  $a = 20^{20} + 21^{21} + 22^{22}$ ,  $b = 19$

35. Tõestada, et  $2^{70} + 3^{70}$  jagub 13-ga.

36. Tõestada, et  $2^{2^5} + 1$  jagub 641-ga.

37. Tõestada, et  $2^{37 \cdot 73} - 1 \equiv 1 \pmod{37 \cdot 73}$ .

38. Leida jääk, mis tekib arvu

$$(98^{62}126^{95} + 158^{151}95^{92})^{122}$$

jagamisel 31-ga.

39. Tõestada, et  $n^7 - n$  jagub kahega, kolmega ja seitsmega iga naturaalarvu  $n$  korral.

40. Tõestada, et kolmest järjestikusest arvust  $a^5 - 1$ ,  $a^5$ ,  $a^5 + 1$  üks jagub kindlasti 11-ga ( $a$  on täisarv).

41. Tõestada, et kui  $S\ddot{U}T(a, 17) = S\ddot{U}T(b, 17) = 1$ , siis arv

$$a^{50}b^{33} - a^{18}b^{17}$$

jagub 17-ga.

42. Tõestada Fermat' teoreemi põhjal, et  $a^{561} - a$  jagub kordarvuga 561 iga täisarvu  $a$  korral. Selleks tõestada, et  $a^{561} - a$  jagub arvudega 3, 11 ja 17.

43. Selgitada, milline jääk tekib siis, kui arv  $2^{p-2}$  jagada  $p$ -ga, kus  $p > 2$  on algarv.

44. Näidata, et Fermat' teoreem kujul  $a^p \equiv a \pmod{p}$  ei jää kehtima, kui seal loobuda eeldusest, et  $p$  on algarv.

45. Tähestikust, milles on  $a$  tähte, koostatakse kõikvõimalikud sõnad pikkusega  $p$ , kus  $p$  on algarv. Seejärel jaotatakse sõnad klassidesse: ühte klassi paigutatakse need sõnad, mis on üksteisest saadavad tähtede tsüklilise nihke teel. Näiteks satuvad samasse klassi sõnad  $aabca$  ja  $bcaaa$ . Leida, millised klassid tekivad ja mitu sõna kuulub igasse klassi. Tulemuse abil tõestada Fermat' väike teoreem.

46. Tõestada Fermat' väike teoreem induktsiooniga naturaalarvu  $a$  järgi, kasutades binoomvalemit.



## XIV. KONGRUENTSIDE LAHENDAMINE

**1. Linearkongruentsid.** Sarnaselt algebras esinevate võrranditega

$$f(x) = 0$$

tuleb tihtipeale lahendada ka kongruentse kujul

$$f(x) \equiv 0 \pmod{m},$$

kus  $f$  on mingi täisarvude hulgal määratud ja täisarvuliste väärtustega funktsioon ning  $m$  fikseeritud moodul. Ülesandeks on leida tundmatu  $x$  kõik sellised väärtused, mis seda seost rahuldavad. Järgnevas vaatlemegi niisuguste kongruentside lahendamist, piirdudes seejuures kõige lihtsama juhuga, mil  $f$  on lineaarfunktsioon, st  $f(x) = ax - b$  ning tegemist nn *linearkongruentsiga*

$$ax \equiv b \pmod{m}.$$

Linearkongruentsil ei saa kunagi olla ainult ühte lahendit. Lihtne on näha, et kui kongruentsi rahuldab arv  $c$ , siis teda rahuldavad ka arvud  $c + m, c + 2m, \dots$ . Liites lahendile (või lahutades sellest) suvaline arv korda moodulit, saame jälle lahendi, sest kui  $c$  on kongruentsi lahend, siis mistahes täisarvu  $k$  korral

$$a(c + km) = ac + akm \equiv b \pmod{m}.$$

Seepärast räägitakse niisuguse kongruentsi lahenditest enamasti alati mooduli  $m$  järgi. Samuti järeldub siit, et kui kongruentsil üldse leidub lahend, siis leidub tal ka lahend arvude  $0, 1, \dots, m - 1$  seas.

*Näide 1.* Kongruentsi

$$3x \equiv 1 \pmod{5}$$

üks lahend on kergesti leitav:  $x = 2$ . Kuid et lahendid on määratud mooduli täpsuseni, siis rahuldavad seda kongruentsi ka arvud  $x = 7, x = 12, x = 17, \dots$  ning samuti veel ka arvud  $x = -3, x = -8, x = -13, \dots$  Kõik need lahendid võib kokku võtta avaldisega

$$x \equiv 2 \pmod{5}.$$

Kongruentside lahendeid esitatakse väga sageli just viimasel kujul.

Järgnevas vaatleme linearkongruentside lahenduvuse küsimust. Et lahendiks peab olema täisarv, siis on kongruents kindlasti lahenduv sel juhul, kui  $a \mid b$ . Kuid erinevalt lineaarvõrrandist võib linearkongruentsil leiduda täisarvulisi lahendeid ka siis, kui viimane seos ei kehti. Rääkides edaspidi lahendi ühesusest teatava mooduli järgi, mõistame seda nii, et kongruentsil leidub täpselt üks lahend moodulist väiksemate mittenegatiivsete täisarvude hulgas.

**Teoreem 1.** a) Kui  $S\ddot{U}T(a, m) \mid b$ , siis leidub lineaarkongruentsil  $ax \equiv b \pmod{m}$  parajasti üks lahend mooduli  $m : S\ddot{U}T(a, m)$  järgi.

b) Kui tingimus  $S\ddot{U}T(a, m) \mid b$  pole täidetud, siis kongruentsil  $ax \equiv b \pmod{m}$  lahendit ei leidu.

Tõestus. a) Olgu  $d = S\ddot{U}T(a, m)$ ,  $a = a'd$ ,  $b = b'd$  ja  $m = m'd$ . Jagades kongruentsi

$$ax \equiv b \pmod{m}$$

mõlemat poolt ja moodulit suurima ühisteguriga  $d$ , saame

$$a'x \equiv b' \pmod{m'}.$$

Need kongruentsid on samaväärsed, sest kui mingi arv rahuldab ühte kongruentsi, siis see arv rahuldab ka teist ja vastupidi.

Näitame, et viimasel kongruentsil on parajasti üks lahend mooduli  $m'$  järgi. Võtame vaatlusele  $m'$  arvu

$$a' \cdot 0, a' \cdot 1, \dots, a' \cdot (m' - 1).$$

Mooduliga  $m'$  jagades annavad need arvud kõik erinevad jäägid. Tõepoolest, kui näiteks arvud  $a'i$  ja  $a'j$ , kus  $i < j$ , annaksid sama jäägi, siis nende vahe  $a'(j - i)$  jaguks  $m'$ -ga. See on aga võimatu, sest  $S\ddot{U}T(a', m') = 1$  ja tegur  $j - i$  on väiksem kui  $m'$ . Et kõik jäägid osutusid erinevaks, siis on nad lihtsalt arvud  $0, 1, \dots, m' - 1$  mingis järjekorras. Sealhulgas peab mingi jääk langema kokku jäägiga, mis tekib  $b'$  jagamisel  $m'$ -ga. Vastava liikme  $a'k$  tegur  $k$  sobibki kongruentsi lahendiks. Lisaks on see lahend ainus mooduli  $m' = m : S\ddot{U}T(a, m)$  järgi, sest nagu nägime, ei saa vaadeldavate arvude puhul tekkida korduvaid jääke.

b) Oletame väitevastaselt, et kongruentsil leidub lahend  $c$ . Olgu  $d = S\ddot{U}T(a, m)$ . Et  $d \mid a$ , siis  $d \mid ac$  ehk  $ac \equiv 0 \pmod{d}$ . Teiselt poolt  $d \mid m$  ja  $m \mid ac - b$ , millest  $d \mid ac - b$  ehk  $ac \equiv b \pmod{d}$ . Järelikult  $b \equiv 0 \pmod{d}$  ehk  $d \mid b$ . Seega oleme saanud  $S\ddot{U}T(a, m) \mid b$ .  $\square$

Erijuhul, kui tundmatu  $x$  kordaja ja moodul on ühistegurita, saame teoreemist järgmise järelduse.

**Järeldus 1.** Kui  $S\ddot{U}T(a, m) = 1$ , siis leidub lineaarkongruentsil  $ax \equiv b \pmod{m}$  parajasti üks lahend mooduli  $m$  järgi.

Viimase teoreemi ja järelduse abil saab lihtsasti kindlaks teha kongruentsi lahenduvust või lahendumatust. Näiteks kongruents

$$6x \equiv 9 \pmod{15}$$

on lahenduv, sest arvude 6 ja 15 suurim ühistegur 3 jagab kongruentsi paremat poolt. Selle kongruentsi lahendiks on  $x \equiv 4 \pmod{5}$ . Seevastu aga kongruents

$$6x \equiv 8 \pmod{15}$$

pole lahenduv, sest arvude 6 ja 15 suurim ühistegur 3 ei ole kongruentsi parema poole 8 teguriks.

Kui arvude  $a$  ja  $m$  suurim ühistegur on 1, siis osutub kongruents lahenduvaks, sõltumata paremast poolest. Selline juht esineb näiteks kongruentsi

$$10x \equiv 6 \pmod{21}$$

puhul, mille lahend on  $x \equiv 9 \pmod{21}$ .

Oleme leidnud tingimuse, mis aitab kindlaks teha, kas kongruentsil leidub lahend, aga kuidas seda lahendit tegelikult leida?

Ühe, kuigi mitte kõige efektiivsema võimaluse näitab teoreemi tõestuses kasutatud võte vaadata järjest läbi arvud kujul  $ai$ , kus  $i = 0, 1, \dots, m - 1$ , kuni leitakse selline, mis annab mooduliga jagades sobiva jäägi. Selline täieliku läbivaatamise meetod tuleb kõne alla siiski ehk ainult väiksemate moodulite korral.

Efektiivsem võte on mooduli kordse liitmise meetod: liidame kongruentsi paremale poolele või lahutame sellest mooduli kordseid seni, kuni tekib olukord, kus kongruentsi pooli saab jagada mingi ühe ja sama arvuga. Seejärel kordame sama operatsiooni, kuni jälle saab kongruentsi pooli mingi arvuga jagada jne. Niiviisi väheneb järk-järgult  $x$ -i kordaja kongruentsi vasakul poolel. Kui ta saab lõpuks võrdseks ühega, ongi kongruents lahendatud.

*Näide 2.* Lahendada lineaarkongruents

$$15x \equiv 18 \pmod{24}.$$

Kongruents on lahenduv, sest 18 jagub arvuga  $\text{SÜT}(15, 24) = 3$ . Jagades kongruentsi pooli ja moodulit 3-ga, saame kongruentsi

$$5x \equiv 6 \pmod{8}.$$

Liidame paremale poolele või lahutame sellest mooduli kordseid seni, kuni saame 5-ga jaguva arvu:

$$5x \equiv 6 + 3 \cdot 8 = 30 \pmod{8}.$$

Jagame pooli 5-ga, mis on mooduliga ühistegurita, ning lahend on

$$x \equiv 6 \pmod{8}.$$

Kui meid huvitavad lahendid mooduli 24 järgi, siis on neid kolm:  $x \equiv 6 \pmod{24}$ ,  $x \equiv 14 \pmod{24}$  ja  $x \equiv 22 \pmod{24}$ .

*Näide 3.* Lahendada lineaarkongruents

$$24x \equiv 1 \pmod{29}.$$

Kongruents on lahenduv, sest  $\text{SÜT}(24, 29) = 1$ . Liidame kongruentsi paremale poolele mooduli:

$$24x \equiv 30 \pmod{29}.$$

Nüüd võime kongruentsi pooli jagada 6-ga, sest arv 6 on mooduliga ühistegurita. Saame

$$4x \equiv 5 \pmod{29}.$$

Lahutame paremast poolest mooduli:

$$4x \equiv -24 \pmod{29}.$$

Jagame kongruentsi pooli 4-ga, mis on mooduliga ühistegurita:

$$x \equiv -6 \pmod{29}.$$

Liites paremale poolele mooduli, võime selle lahendi esitada kujul

$$x \equiv 23 \pmod{29}.$$

**2. Linearkongruentside süsteemid.** Teinekord esineb rakedustes olukordi, kus arv  $x$  peab rahuldama mitte ühte, vaid korraga mitut kongruentsi

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ a_nx &\equiv b_n \pmod{m_n} \end{aligned}$$

ehk teiste sõnadega,  $x$  peab rahuldama kongruentside süsteemi ehk kongruentsisüsteemi. Kui leidub arv  $x$ , mis rahuldab kõiki neid kongruentse, siis peab iga üksik kongruents olema lahenduv. Lahendades vajaduse korral kõik kongruentsid eraldi, võime seega alati eeldada, et süsteem on antud kujul

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ x &\equiv c_n \pmod{m_n} \end{aligned}$$

Selle kuju võtamegi analüüsi aluseks.

Näiteks kongruentsisüsteemis

$$\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 3x &\equiv 2 \pmod{5} \end{aligned}$$

on esimese kongruentsi lahend  $x \equiv 2 \pmod{3}$  ning teise kongruentsi lahend  $x \equiv 4 \pmod{5}$ , mistõttu sellele süsteemile võib anda kuju

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

Niisuguste kongruentsisüsteemide lahendamisega tegelesid palju Vana-Hiina matemaatikud, nendelt pärineb järgmine teoreem, mis avaldati esmakordselt aastal 1247 ja mida on kombeks nimetada *hiina jäägiteoreemiks*.

**Teoreem 2.** *Kui moodulid  $m_1, m_2, \dots, m_n$  on paarikaupa ühistegurita, siis leidub kongruentsisüsteemil*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\dots \dots \dots \\ x &\equiv c_n \pmod{m_n} \end{aligned}$$

*parajasti üks lahend mooduli  $M = m_1 m_2 \dots m_n$  järgi.*

Tõestus. Vaatleme  $n$  arvu  $M_1, M_2, \dots, M_n$ , mis on määratud avaldisega

$$M_i = \frac{M}{m_i} \quad (1 \leq i \leq n).$$

Nende kaudu saame leida arvud  $M'_1, M'_2, \dots, M'_n$  nii, et

$$M_i M'_i \equiv 1 \pmod{m_i} \quad (1 \leq i \leq n).$$

Tõepoolest, et  $SÜT(M_i, m_i) = 1$ , siis on see kongruents  $M'_i$  suhtes lahenduv ja tal leidub parajasti üks lahend mooduli  $m_i$  järgi.

Vaadeldava süsteemi lahendiks sobib arv

$$x = M_1 M'_1 c_1 + M_2 M'_2 c_2 + \dots + M_n M'_n c_n,$$

sest asetades selle  $i$ -ndasse kongruentsi, saame

$$M_1 M'_1 c_1 + M_2 M'_2 c_2 + \dots + M_n M'_n c_n \equiv M_i M'_i c_i \equiv c_i \pmod{m_i}.$$

Tõepoolest, arvu  $x$  avaldises jaguvad kõik liikmed peale  $i$ -nda arvuga  $m_i$ , lisaks on arvude  $M'_i$  valiku tõttu  $M_i M'_i \equiv 1 \pmod{m_i}$ .

Näitame, et lahend on ainus mooduli  $M = m_1 m_2 \dots m_n$  järgi. Kui süsteemi kõiki kongruentse rahuldaks peale arvu  $x$  veel arv  $x'$ , siis annavad  $x$  ja  $x'$  moodulitega  $m_1, m_2, \dots, m_n$  jagades sama jäägi. Seega jagub vahe  $x - x'$  kõigi moodulitega ning järelikult ka nende vähima ühiskordsega. Et moodulid on eelduse kohaselt ühistegurita, siis võrdub nende vähim ühiskordne parajasti korrutisega  $m_1 m_2 \dots m_n$ . Seega jagub vahe  $x - x'$  arvuga  $M$  ehk  $x \equiv x' \pmod{M}$ .  $\square$

Teoreemi tõestus annab ka meetodi kongruentsisüsteemi lahendamiseks. Selleks tuleb moodustada arvud  $M_1, M_2, \dots, M_n$ , abikongruentse lahendades leida arvud  $M'_1, M'_2, \dots, M'_n$  ning kirjutada valemi põhjal välja süsteemi lahend.

*Näide 4.* Lahendada kongruentsisüsteem

$$\begin{aligned} 3x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{6} \\ 5x &\equiv 1 \pmod{7} \end{aligned}$$

Kõigepealt viime süsteemi kujule, kus iga tundmatu kordaja on 1. Kongruentsi  $3x \equiv 2 \pmod{5}$  lahendiks saame näiteks mooduli liitmise meetodiga  $x \equiv 4 \pmod{5}$  ning kongruentsi  $5x \equiv 1 \pmod{7}$

lahendiks  $x \equiv 3 \pmod{7}$ . Seega on süsteem viidud kujule

$$\begin{aligned}x &\equiv 4 \pmod{5} \\x &\equiv 3 \pmod{6} \\x &\equiv 3 \pmod{7}\end{aligned}$$

Et moodulid on paarikaupa ühistegurita, siis võime kasutada tuletatud lahendivalemit. Moodustame arvud

$$M = 5 \cdot 6 \cdot 7 = 210,$$

$$M_1 = \frac{M}{5} = 42, \quad M_2 = \frac{M}{6} = 35, \quad M_3 = \frac{M}{7} = 30.$$

Arvud  $M'_1, M'_2, M'_3$  määrame tingimustest

$$\begin{aligned}42M'_1 &\equiv 1 \pmod{5} && \text{ehk} && 2M'_1 &\equiv 1 \pmod{5}, \\35M'_2 &\equiv 1 \pmod{6} && \text{ehk} && -M'_2 &\equiv 1 \pmod{6}, \\30M'_3 &\equiv 1 \pmod{7} && \text{ehk} && 2M'_3 &\equiv 1 \pmod{7}.\end{aligned}$$

Viimastest kongruentsidest leiame  $M'_1 = 3, M'_2 = 5, M'_3 = 4$ . Lahendivalemi järgi siis

$$x \equiv 42 \cdot 3 \cdot 4 + 35 \cdot 5 \cdot 3 + 30 \cdot 4 \cdot 3 = 1389 \equiv 129 \pmod{210}.$$

Järelikult võib süsteemi lahendi esitada kujul

$$x \equiv 129 \pmod{210}.$$

Teine meetod on lahendada kongruentse järk-järgult, asendades igal sammul eelmiste kongruentside lahendi uude kongruentsi. Süsteemi

$$\begin{aligned}x &\equiv c_1 \pmod{m_1} \\x &\equiv c_2 \pmod{m_2} \\&\dots \dots \dots \\x &\equiv c_n \pmod{m_n}\end{aligned}$$

lahendamiseks võtame kõigepealt ette esimese kongruentsi. Selle lahendid avalduvad kõik kujul

$$x = c_1 + m_1 t_1,$$

kus  $t_1$  on suvaline täisarv. Selleks, et  $x$  rahuldaks ka teist kongruentsi, määrame  $t_1$  väärtuse, asetades saadud avaldise teise kongruentsi, millega viimane omandab kuju  $c_1 + m_1 t_1 \equiv c_2 \pmod{m_2}$  ehk  $m_1 t_1 \equiv c_2 - c_1 \pmod{m_2}$ . Tekkinud kongruentsi lahendame  $t_1$  suhtes, olgu lahendiks  $t_1 \equiv d_1 \pmod{m_2}$ , st lahendid avalduvad üldkujul

$$t_1 = d_1 + m_2 t_2,$$

kus  $t_2$  on suvaline täisarv. Järelikult

$$x = c_1 + m_1(d_1 + m_2 t_2) = c_1 + m_1 d_1 + m_1 m_2 t_2.$$

Leitud arv rahuldab süsteemist kahte esimest kongruentsi. Teiste sõnadega, kahest esimesest kongruentsist koosneva alamsüsteemi lahend on  $x \equiv c_1 + m_1 d_2 \pmod{m_1 m_2}$ . Edasi asendame lahendi avaldise kolmandasse kongruentsi jne. Pärast viimase kongruentsi arvesevõtmist oleme leidnud lahendi, mis rahuldab süsteemi kõiki kongruentse.

*Näide 5.* Lahendame uuesti eelmises näites vaadeldud lineaarkongruentsisüsteemi

$$\begin{aligned}x &\equiv 4 \pmod{5} \\x &\equiv 3 \pmod{6} \\x &\equiv 3 \pmod{7}\end{aligned}$$

Esimese kongruentsi lahendid avalduvad kõik kujul

$$x = 4 + 5t_1,$$

kus  $t_1$  on suvaline täisarv. Asendame saadud üldavaldise süsteemi teise kongruentsi. Sellega tekib kongruents  $4 + 5t_1 \equiv 3 \pmod{6}$  ehk  $5t_1 \equiv -1 \pmod{6}$ . Liites paremale poolele üks kord mooduli, saame  $5t_1 \equiv 5 \pmod{6}$ , millest  $t_1 \equiv 1 \pmod{6}$ . Seega  $t_1 = 1 + 6t_2$ , kus  $t_2$  on suvaline täisarv. Asendades tulemuse eelmisena saadud üldavaldisesse, näeme, et nii esimest kui ka teist kongruentsi rahuldavad arvud

$$x = 4 + 5(1 + 6t_2) = 9 + 30t_2.$$

Lõpuks asendame selle avaldise kolmandasse kongruentsi, millega tekib kongruents  $9 + 30t_2 \equiv 3 \pmod{7}$ , ehk pärast esimese liikme paremale viimist ja seejärel vasakult  $28t_2$  lahutamist kongruents  $2t_2 \equiv -6 \pmod{7}$ . Siit  $t_2 \equiv -3 \pmod{7}$  ehk  $t_2 = -3 + 7t_3$ , kus  $t_3$  on suvaline täisarv. Asendades tulemuse eelmisse üldavaldises, saame, et kõiki kolme kongruentsi rahuldavad arvud

$$x = 9 + 30(-3 + 7t_3) = -81 + 210t_3,$$

ehk kongruentsina kirjutades

$$x \equiv -81 \equiv 129 \pmod{210}.$$

Järjestikuse asendamise meetodi puhul pole tegelikult tähtis, et igas kongruentsis oleks vasaku poole kordaja 1. Samuti saab seda meetodit, erinevalt otse hiina jäägiteoreemil põhinevast meetodist, kasutada ka nende süsteemide lahendamisel, mille puhul ei ole kõik moodulid paarikaupa ühistegurita.

Kui kongruentsisüsteemi moodulid ei ole paarikaupa ühistegurita, siis ei tarvitse süsteemil enam lahendit leiduda. Analoogiliselt üksiku lineaarkongruentsiga võib formuleerida tarviliku ja piisava tingimuse, millal süsteem on lahenduv ja millal mitte.

**Teoreem 3.** a) Kui  $c_i \equiv c_j \pmod{\text{SÜT}(m_i, m_j)}$  iga  $i$  ja  $j$  korral, siis leidub kongruentsisüsteemil

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\dots \dots \dots \\ x &\equiv c_n \pmod{m_n} \end{aligned}$$

parajasti üks lahend mooduli  $M = \text{VÜK}(m_1, m_2, \dots, m_n)$  järgi.

b) Kui mingite  $i$  ja  $j$  korral seos  $c_i \equiv c_j \pmod{\text{SÜT}(m_i, m_j)}$  ei kehti, siis süsteemil lahendit ei leidu.

Tõestus. a) Moodustame arvud  $M_1, M_2, \dots, M_n$  avaldistega

$$M_i = \frac{m_1 m_2 \dots m_n}{m_i} \quad (1 \leq i \leq n).$$

Rakendades korduvalt üle-eelmise peatüki teoreemi 7, leiame sellised arvud  $M'_1, M'_2, \dots, M'_n$ , et oleks

$$\text{SÜT}(M_1, M_2, \dots, M_n) = M_1 M'_1 + M_2 M'_2 + \dots + M_n M'_n.$$

Vaatleme arvu

$$x = \frac{M_1 M'_1 c_1 + M_2 M'_2 c_2 + \dots + M_n M'_n c_n}{\text{SÜT}(M_1, M_2, \dots, M_n)}.$$

See arv on täisarv, sest arvud  $M_1, M_2, \dots, M_n$  jaguvad oma suurima ühisteguriga. Tõestame, et  $x$  sobib süsteemi lahendiks. Konkreetseuse mõttes leiame arvu  $x$  jäägi jagamisel mooduliga  $m_1$ . Kui viimase avaldise lugejas liita ning lahutada arvud  $M_2 M'_2 c_1, \dots, M_n M'_n c_1$ , siis võime esitada lugeja kujul

$$\begin{aligned} &M_1 M'_1 c_1 + M_2 M'_2 c_1 + \dots + M_n M'_n c_1 + \\ &+ M_2 M'_2 c_2 - M_2 M'_2 c_1 + \dots + M_n M'_n c_n - M_n M'_n c_1 = \\ &= \text{SÜT}(M_1, M_2, \dots, M_n) c_1 + M_2 M'_2 (c_2 - c_1) + \dots + M_n M'_n (c_n - c_1). \end{aligned}$$

Seega

$$x = c_1 + \frac{M_2 M'_2 (c_2 - c_1) + \dots + M_n M'_n (c_n - c_1)}{\text{SÜT}(M_1, M_2, \dots, M_n)}.$$

Eelduse põhjal on iga  $i = 2, \dots, n$  korral  $\text{SÜT}(m_i, m_1) \mid (c_i - c_1)$ , järelikult  $c_i - c_1 = k_i \text{SÜT}(m_i, m_1)$ , kus  $k_i$  on teatav täisarv. Et lisaks

$$M_i = m_1 \frac{M_1}{m_i},$$

siis iga  $i = 2, \dots, n$  korral

$$\frac{M_i M'_i (c_i - c_1)}{\text{SÜT}(M_1, M_2, \dots, M_n)} = \frac{m_1 \frac{M_1}{m_i} M'_i k_i \text{SÜT}(m_i, m_1)}{\text{SÜT}(M_1, M_2, \dots, M_n)}.$$



Viimane avaldis aga võrdub avaldisega

$$\frac{m_1 M'_i k_i \text{SÜT}\left(\frac{M_1}{m_i} m_i, \frac{M_1}{m_i} m_1\right)}{\text{SÜT}(M_1, M_2, \dots, M_n)} = \frac{m_1 M'_i k_i \text{SÜT}(M_1, M_i)}{\text{SÜT}(M_1, M_2, \dots, M_n)}.$$

Suurim ühistegur lugejas on nimetajas esineva suurima ühisteguri kordne, seega jagub kogu avaldis  $m_1$ -ga. Kokkuvõttes näeme seega, et  $x$  avaldub kujul

$$x = c_1 + m_1 t$$

mingi täisarvu  $t$  korral ning järelikult

$$x \equiv c_1 \pmod{m_1}.$$

Seega on süsteemi esimene kongruents rahuldatud. Täieliku sümmeetria tõttu saame, et  $x$  rahuldab ka ülejäänud kongruentse ehk on süsteemi lahend.

Kui  $x$  ja  $x'$  on vaadeldava kongruentsisüsteemi kaks lahendit, siis jagub  $x - x'$  kõigi moodulitega  $m_1, m_2, \dots, m_n$  ning järelikult ka arvuga  $M = \text{VÜK}(m_1, m_2, \dots, m_n)$ . Seega on süsteemi lahend ühene mooduli  $M$  järgi.

b) Kui  $x$  on süsteemi lahend, siis peab ta rahuldama ka iga alam-süsteemi

$$\begin{aligned} x &\equiv c_i \pmod{m_i} \\ x &\equiv c_j \pmod{m_j} \end{aligned}$$

Et  $\text{SÜT}(m_i, m_j) \mid m_i$  ja  $m_i \mid x - c_i$ , siis  $\text{SÜT}(m_i, m_j) \mid x - c_i$ . Analoogiliselt  $\text{SÜT}(m_i, m_j) \mid x - c_j$ . Kahest viimasest seosest saame  $\text{SÜT}(m_i, m_j) \mid (x - c_i) - (x - c_j)$  ehk  $\text{SÜT}(m_i, m_j) \mid c_i - c_j$ . See aga tähendab, et  $c_i \equiv c_j \pmod{\text{SÜT}(m_i, m_j)}$ .  $\square$

Niisiis leidub igal lahenduval kongruentsisüsteemil ühene lahend üksikute moodulite vähima ühiskordse järgi. Kui moodulid on paarikaupa ühistegurita, siis võrdub vähim ühiskordne parajasti nende moodulite korrutisega. Sellisel juhul taandub tõestatud teoreem hiina jäägteoreemiks.

Formuleeritud teoreemi abil saab ilma kongruentsisüsteemi lahendamata kindlaks teha, kas tal lahend leidub.

*Näide 6.* Vaatleme lineaarkongruentside süsteemi

$$\begin{aligned} x &\equiv 2 \pmod{4} \\ x &\equiv 3 \pmod{6} \end{aligned}$$

Siin on  $\text{SÜT}(4, 6) = 2$ , kuid paremad pooled 2 ja 3 ei ole omavahel kongruentsed mooduli 2 järgi. Seega puudub sellel süsteemil lahend. Vaadeldava lihtsa näite korral saab selles ka otse veenduda: süsteemi esimest kongruentsi rahuldavad ainult paarisarvud, teist aga ainult paaritud arvud.

## Ülesanded

Lahendada lineaarkongruentsid.

1.  $5x \equiv 4 \pmod{7}$
2.  $7x \equiv 2 \pmod{13}$
3.  $2(3x + 1) \equiv 8 \pmod{37}$
4.  $42x \equiv 11 \pmod{67}$
5.  $60x \equiv 42 \pmod{198}$
6.  $1215x \equiv 560 \pmod{2755}$

7. Lahendada kongruentsisüsteem

$$\begin{aligned}4(3x - 5) - 2(y - x) &\equiv 2 \\ 2(5x - y) - 3y &\equiv 5\end{aligned}$$

mooduli 23 järgi ja mooduli 31 järgi.

Lahendada järgmised lineaarkongruentside süsteemid.

8.  $x \equiv 3 \pmod{5}$   
 $x \equiv 2 \pmod{6}$   
 $x \equiv 4 \pmod{7}$
  9.  $3x \equiv 1 \pmod{14}$   
 $2x \equiv 5 \pmod{13}$   
 $x \equiv 8 \pmod{15}$
  10.  $5x \equiv 1 \pmod{8}$   
 $3x \equiv 5 \pmod{10}$   
 $4x \equiv 4 \pmod{12}$
  11.  $5x \equiv 14 \pmod{21}$   
 $7x \equiv 1 \pmod{18}$   
 $3x \equiv 6 \pmod{15}$
  12.  $x \equiv 1 \pmod{6}$   
 $3x \equiv 4 \pmod{10}$   
 $2x \equiv -1 \pmod{15}$
  13.  $x - a \equiv 0 \pmod{3}$   
 $3x + b \equiv 0 \pmod{5}$   
 $2x + c \equiv 0 \pmod{7}$
14. Kaks hammasratast, millest ühel on 21 ja teisel 52 hammast, hambuvad teineteisega.

- a) Mitu pööret peab suurem hammasrattas tegema, et alguses kohakuti olnud hammas ja hambavahe satuksid taas kokku?
- b) Nummerdame esimese hammasratta hambad 0-st 20-ni ja teise hammasratta vahed 0-st 51-ni, kummalgi pöörlemis-suunas. Alguses on kohakuti hammas 0 ja vahe 0. Mitu pööret peavad mõlemad rattad tegema, et kohakuti oleksid väiksema ratta hammas 17 ja suurema ratta vahe 11?
- c) Kas hambumisel võib esineda suvaline hamba ja hambavahe kombinatsioon?
- d) Teises süsteemis on suuremal hammasrattal 54 hammast, väiksemal ikka 21. Millised hamba ja hambavahe kombinatsioonid võivad esineda, kui alguses hambusid mõlemal rattal arvud 0?
- e) Väiksema ratta üks hammas on paindunud ja kulutab vahet teisel rattal iseäranis tugevasti. Milline ülekanne (52:21 või 54:21) on kasulikum suurema hammasratta hammaste ühtlase kulumise seisukohalt?

15. Järves on ujumissillast alates paigutatud 3 paralleelset poide rida, mis tähistavad ujumisradu. Punased poid paiknevad 5 m vahedega, rohelised 7 m vahedega ja valged 9 m vahedega. Allveeujuja hüppas vette ujumissillalt ning tõusis pinnale 2 m pärast punast poid, 3 m pärast rohelist ja 3 m enne valget poid. Mitu meetrit ta vee all läbis?
16. Geotermiliselt aktiivses kuumaveeallikate piirkonnas asub kolm suurt geisrit – Heitur, Djúpur ja Forugur. Neist Heitur purskab perioodiga 6 päeva, Djúpur perioodiga 7 päeva ning Forugur perioodiga 11 päeva. Kui geisreid uurima saadetud ekspeditsioon kohale jõudis, siis tuli Djúpuri purset oodata üks päev, Foruguri purset kaks ja Heituri purset viis päeva. Millal peab ekspeditsioon tagasi tulema, et näha kõigi kolme geisri purset samal päeval?
17. Kui sa lähed trepist üles, võttes korraga 2 astet, siis jääb viimaseks sammuks 1 aste üle. Võttes 3 astet korraga, jääb viimaseks sammuks 2 astet. Kui ühe sammuga võtta 4 või 5 astet, siis jääb viimaseks sammuks vastavalt 3 või 4 astet. Kui pingutatud tugevasti ja võtad ühe sammuga 6 astet, siis jääb viimaseks sammuks 5 astet. Alles siis, kui suudad võtta 7 astet korraga, jõuad viimase sammuga ülemisele trepiplatvormile. Mitu astet on trepil?
18. Kui teatud arvust ühikkuubikutest koostada kuubid küljepikkusega 3, siis jääb kasutamata 2 kuubikut. Kui nendest kuubikutest koostada kuubid küljepikkusega 4, siis jääb kasutamata 3 kuubikut. Kui aga kuubikutest koostada kuubid küljepikkusega 5, siis jääb kasutamata 1 kuubik. Leida kuubikute arv.
19. Linnaliinibusse haldavas firmas ei õnnestunud ametiühingu vastuseisu tõttu paika panna ühe bussi liikumise graafikut. Nimelt, kui buss kulutaks ühe ringi läbimiseks 20 minutit, siis lõpetaks bussijuht vahetuse 5 minutit ettenähtud tööajast hiljem. Sama lugu on ka siis, kui buss kulutaks ringi läbimiseks 25 minutit. Ent kui ringi läbimiseks kuluks 30 minutit, siis lõpetaks juht vahetuse 5 minutit ettenähtust varem, mis aga ei meeldinud juhtkonnale. Milline on vahetuse ettenähtud kestus?
20. Planeedil Xantur valitsevate eripäraste tingimuste tõttu kasutavad sealsed elanikud järgmist ajaarvamissüsteemi. On olemas kolme liiki nädalaid: *kajen*, mille kestus on 5 päeva, *seskajen*, mille kestus on 6 päeva, ja *tekajen* kestusega 7 päeva. Iga aasta alguses teatavad preestrid, kas saabuv aasta on *kajen*-, *seskajen*- või *tekajen*-tüüpi, vastavalt sellele, millistest nädalatest ta koosneb. Üldiselt võib aasta koosneda ainult ühte liiki nädalatest, kuid sel-

leks, et astronoomiline pikkus täis saaks, võib aasta lõppu lisada ühe teist liiki nädala. Sel põhjusel ongi *kajen*-tüüpi aasta lõpus üks *tekajen*-nädal, *tekajen*-tüüpi aasta lõpus *seskajen*-nädal ja *seskajen*-tüüpi aasta lõpus *kajen*-nädal. Mitu päeva kestab planeedi Xanturi aasta?

- 21.** Üks Hiina keiser kasutas oma vaenlaste kõrvaldamiseks järgmist meetodit. Korraldati pidusöök, kus külalised istusid koos keisriga ümmarguse laua taga. Teener tõi hõbepeekri, milles olid kullast kirsid. Keiser võttis ühe kirsi ja ulatas peekri parempoolsele naabrile, naaber võttis samuti ühe kirsi, ulatas peekri parempoolsele naabrile ja nii edasi. Kellele jäi viimane kirss, see hukati. Seejärel korjati kirsid kokku ja pandi peekrisse tagasi. Kui vaja, siis korrati seda protseduuri: keiser võttis esimese kirsi ja andis peekri parempoolsele naabrile, kes võttis omakorda kirsi, andis peekri oma naabrile jne. Kord oli pidusöögil kutsutud 7 külalist. Mitu kullast kirssi peab teener peekrisse panema, kui keiser soovib lasta hukata kaks külalist, kes istuvad tema mõlemal käel? Leida kõik võimalused, mis on väiksemad kui 100.

- 22.** Tõestada, et kui  $SÜT(m, n) = 1$ , siis leiduvad arvud  $e_1$  ja  $e_2$ , mis rahuldavad süsteemi

$$\begin{array}{l} e_1 \equiv 1 \pmod{m} \\ e_1 \equiv 0 \pmod{n} \end{array} \quad \text{ja} \quad \begin{array}{l} e_2 \equiv 0 \pmod{m} \\ e_2 \equiv 1 \pmod{n} \end{array}$$

Avaldada süsteemi

$$\begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array}$$

lahend arvude  $e_1$  ja  $e_2$  kaudu.

- 23.** Avaldada kongruentsisüsteemi

$$\begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{array}$$

lahend kongruentsi  $m_1x \equiv c_2 - c_1 \pmod{m_2}$  lahendi kaudu.

- 24.** Tõestada, et kui moodulid  $m_1, m_2, \dots, m_n$  on paarikaupa ühis-tegurita, siis on süsteem

$$\begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots \dots \dots \\ x \equiv c_n \pmod{m_n} \end{array}$$

samaväärne kongruentsiga

$$(M_1 + \dots + M_n)x \equiv M_1c_1 + \dots + M_nc_n \pmod{m_1m_2\dots m_n},$$

kus iga  $i = 1, 2, \dots, n$  korral  $M_i = m_1m_2\dots m_n/m_i$ .

## AINEREGISTER

- ahel, 52
- ahela otstipp, 52
- ahela pikkus, 52
- ahela sisetipp, 52
- ahne algoritm, 72
- alamgraaf, 50
- alamtipp, 64
- algarv, 118
- algarvufunktsioon, 121
- algarvuteoreem, 121
- algtegur, 122
- algtingimused, 37
- algtipp, 77
- algväärtused, 33
- alusgraaf, 77
- aluspuu, 71
- antirefleksivne relatsioon, 90
- antisümmeetriline relatsioon, 90
- aritmeetika põhiteoreem, 122
  
- baas, 5
- binaarkood, 70
- binaarne relatsioon, 87
- Binet' valem, 39
- binoomkordaja, 14, 23
- binoomteoreem, 25
- binoomvalem, 25
- Boole'i korrutis, 111
- Boole'i maatriks, 110
- Boole'i maatriksi eitus, 110
- Boole'i maatriksite disjunktsioon, 110
- Boole'i maatriksite konjunktsioon, 110
  
- Cassini võrdus, 44
- Catalani võrdus, 44
- Cayley teoreem, 70
  
- d'Ocagne'i võrdus, 44
  
- ekvivalents, 91
- eraldav tipp, 54
  
- Eratosthenese sõel, 120
- erilahend, 37
- Eukleidese algoritm, 130
- Euleri graaf, 56
- Euleri tsükkel, 56, 78
  
- faktoriaal, 12
- Fermat' väike teoreem, 141
- Fibonacci arvud, 33
- Floyd-Warshalli algoritm, 83
  
- graaf, 47
- graafi serv, 47
- graafi sisend, 78
- graafi tipp, 47
- graafi täiend, 49
- graafi väljund, 78
- graafide isomorfsus, 58, 78
- Grötzschi graaf, 62
  
- Hamiltoni graaf, 57
- Hamiltoni tsükkel, 57, 78
- haru, 74
- Hasse diagramm, 93
- Herscheli graaf, 62
- hiina jäägiteoreem, 148
- hulkade otsekorrutis, 87
  
- induktsiooni baas, 5
- induktsiooni eeldus, 5
- induktsiooni samm, 5
- induktsiooniprintsiip, 4
- intsidentsus, 48
- intsidentsusmaatriks, 49
- invariant, 59
- isoleeritud tipp, 50
- isomorfsed graafid, 58, 78
  
- jagaja, 117
- jaguvus, 117
- jaguvusteooria põhiteoreem, 122
- jaguvustunnused, 140
- juur, 64

juurega puu, 64  
 järjestusrelatsioon, 92  
 jäägiga jagamine, 118

kaal, 48  
 kaalutud graaf, 48  
 kaar, 77  
 kaare algtip, 77  
 kaare lõpptipp, 77  
 kahanev faktoriaal, 13  
 kahekohaline relatsioon, 87  
 kaksikalgarvud, 120  
 kaksikud, 121  
 kanooniline kuju, 124  
 karakteristlik võrand, 37  
 kaugus, 52  
 kombinatsioonid, 14  
 kompositsioon, 97  
 kongruents, 136  
 kongruentsed arvud, 136  
 kongruentsisüsteem, 148  
 kordarv, 118  
 kordne, 117  
 kordne serv, 47  
 kordumistega kombinatsioonid, 17  
 kordumistega permutatsioonid, 15  
 korrutamiseegel, 19  
 Kruskali algoritm, 72

leht, 63  
 lihtahel, 52  
 lihttsükkel, 52  
 liitmisreegel, 19  
 lineaarkongruents, 145  
 lineaarne diofantiline võrand, 132  
 lineaarne konstantsete kordajatega  
 rekurrentne võrand, 36  
 lineaarne mittehomoogeenne rekur-  
 rentne võrand, 41  
 Lucas' arvud, 45  
 lõige, 105  
 lõpptipp, 77

matemaatilise induktsiooni print-  
 siip, 4

mets, 64  
 mitterange järjestus, 92  
 moodul, 136  
 mooduli liitmise meetod, 147  
 multigraaf, 48  
 multinoomkordaja, 16, 28  
 multinoomvalem, 28  
 märgendatud puu, 68

*n*-mõõtmeline kuup, 60  
 naaberservad, 48  
 naabertipud, 48  
 naabusmaatriks, 48  
 nullgraaf, 49  
 nõrgalt sidus graaf, 79  
 nõrgalt transitiivne relatsioon, 95

oks, 63  
 otsekorrutis, 87  
 otstipp, 48, 52

Pascali kolmnurk, 24  
 permutatsioonid, 12, 13  
 Peterseni graaf, 62  
 projektsioon, 105  
 Prüferi kood, 68  
 puu, 63  
 puu kõrgus, 64  
 puu sügavus, 64  
 pöördrelatsioon, 96

range järjestus, 92  
 redel, 75  
 refleksiivne relatsioon, 90  
 refleksiivne transitiivne sulund, 102  
 regulaarne graaf, 51  
 regulaarse graafi aste, 51  
 rekurrentne jada, 33  
 rekurrentne seos, 33  
 rekurrentne võrand, 36  
 rekurrentse võrandi erilahend, 37  
 rekurrentse võrandi järk, 36  
 rekurrentse võrandi lahend, 36  
 rekurrentse võrandi üldlahend, 37  
 relatsioon, 87

relatsioon hulgal, 88  
 relatsiooni aste, 101  
 relatsiooni esitamine graafiga, 89  
 relatsiooni esitamine maatriksiga, 90  
 relatsiooni lõige, 105  
 relatsiooni projektsioon, 105  
 relatsiooni pöördrelatsioon, 96  
 relatsiooni täiend, 96  
 relatsioonide kompositsioon, 97  
 relatsioonide vahe, 96  
 relatsioonide ühend, 96  
 relatsioonide ühisosa, 96  
 rippuv tipp, 50  
 ruututõstmismeetod, 139

samasusrelatsioon, 88  
 samm, 5  
 seos, 87  
 serv, 47  
 Shannoni mäng, 75  
 sidus graaf, 53  
 sidus komponent, 53  
 sild, 53  
 silmus, 47  
 sisend, 78  
 sisendaste, 77  
 sisetipp, 52  
 subfaktoriaalid, 36  
 sulund, 102  
 suunatud ahel, 78  
 suunatud graaf, 77  
 suunatud lihtahel, 78  
 suunatud lihttsükkel, 78  
 suunatud tsükkel, 78  
 suurim ühistegur, 127  
 sümmeetriline relatsioon, 90

tegur, 117  
 tegurdamispuu, 126  
 tipp, 47  
 tipu aste, 50  
 tipu haru, 74  
 tipu sisendaste, 77  
 tipu väljundaste, 77  
 transitiivne relatsioon, 90  
 transitiivne sulund, 102  
 tsükkel, 52  
 tsükli pikkus, 52  
 tsüklomaatilise arv, 65  
 tugev induktsiooniprintsiip, 8  
 tugevalt sidus graaf, 79  
 turniir, 81  
 täiendgraaf, 49  
 täisgraaf, 49  
 täisrelatsioon, 88  
 tühirelatsioon, 88

valents, 50  
 variatsioonid, 13  
 võrdus, 88  
 vähim ühiskordne, 132  
 väljund, 78  
 väljundaste, 77

Warshalli algoritm, 114

ühiskordne, 132  
 ühistegur, 127  
 ühistegurita arvud, 127  
 üksikväide, 4  
 üldlahend, 37  
 üldväide, 4  
 ülemtipp, 64