Ристо Малчески
Вера Малческа

МАТЕМАТИКА 1
АЛГЕБАРСКИ СТРУКТУРИ
(трето непроменето издание)

Скопје, 2020

Рецензенти:
Проф. д-р Костадин Тренчевски, Природно-математички факултет, Скопје
Проф. д-р Билјана Крстеска, Природно-математички факултет, Скопје

Компјутерска обработка: Ристо Малчески и Самоил Малчески

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

510/511
512.1/.6

МАЛЧЕСКИ, Ристо
Математика 1 : алгебарски структури / Ристо Малчески, Вера Малческа. - Скопје : Армаганка, 2020. - 260 стр. ; 25 см

Библиографија: стр. 255-256. - Регистар

ISBN 978-608-4904-66-3
1. Малческа, Вера [автор]
а) Алгебарски структури - Дискретна математика
COBISS.MK-ID 112059914

СОДРЖИНА

III ГЛАВА
АКСИОМИ. ТЕОРЕМИ. МЕТОДИ ЗА ДОКАЖУВАЊЕ

IV ГЛАВА
МНОЖЕСТВА И ПРЕСЛИКУВАЊА

V ГЛАВА
БИНАРНИ РЕЛАЦИИ

VI ГЛАВА
ГРУПИ, ПРСТЕНИ И ПОЛИЊА

ПРЕДГОВОР КОН ВТОРОТО ИЗДАНИЕ

> Ниедно истражување на човекот не може да се нарече вистинска наука, ако истото не е поткрепено со математички доказ.
>
> Проблематична е веродостојноста на тврдењата во науките, каде што нема примена на ниту една математичка дисциплина, т.е. кои не се поврзани со математиката.
>
> Леонардо да Винчи

Оваа книга е наменета за предметот *Дискретна математика*, кој студентите на факултетите за информатика во Република Македонија најчесто го слушаат во прва година. Во неа се разработени дел од содржините од Дискретната математика или како што уште популарно е наречена Математика за комјутерски науки. Книгава е поделена на шест глави и тоа:

- Елементи од математичка логика,
- Елементарна теорија на броеви,
- Аксиоми. Теореми. Методи на докажување
- Множества и пресликувања,
- Релации и
- Групи. Прстени. Полиња.

Всушност, во овој курс се поместени дел од содржините кои на повеќето Универзитети се изучуваат во предметите Дискретна математика I и II.

Во првата глава се разработени основните елементи од математичката логика, при што посебно внимание е посветено на нормалните форми, Карноовите мапи и дијаграмите на дигиталните кола. Притоа, во функција на дијаграмите на дигиталните кола се разгледувани Шеферовата црта и Пирсоновата стрелка, како и комплетноста на исказната логика.

Втората глава е посветена на елементарната теорија на броеви и во истата покрај прашањата за деливост се разработени конгруенциите, системите на остатоци и мултипликативните функции. Притоа посебно внимание е посветено на Ојлеровата функција и тврдењата поврзани со истата, а заради комплетност на изложувањата на ова ниво одделно се разработени линеарната Диофантова и конгруентна равенка и Кинеската теорема за остатоци, а преку примери се прикажани елементарните методи за решавање на нелинеарните Дифантови равенки.

Во третата глава, нестандардно за информатичкото образование во потесното опкружување, се разработени математичките тврдења, аксиомите, теоремите, правилата за изведување заклучоци и методите за докажување на математички тврдења. Основна причина за оваа определба е што секоја компјутерска

програма без логички грешки е еквивалентна на логички доказ на кое било математичко тврдење. Токму затоа, од посебно значење е студентите по информатика покрај алгоритамското мислење, да ги совладаат и методите на логичкото мислење и заклучување.

Во четвртата глава која носи наслов Множества и пресликувања, покрај основните поими од теоријата на множества се разработени и основните комбинаторни принципи и конфигурации. Исто така, во оваа глава се разгледани и Буловите алгебри, како и пребројливите и непребројливите множества.

Во петтата глава се разработени бинарните релации, видовите бинарни релации, како и нивните затворања. На крајот од оваа глава, на елементарно ниво, одделно разработени релациите за еквиваленција и подредување.

Шестата глава е посветена на теоријата на групи. Се разбира, како и во претходните глави и овде разработените содржи се на елементарно ниво, меѓутоа заради специфичните барања на информатичкото образование во овој дел посебно внимание е посветено на конечните групи, хомоморфизмите, изоморфизмите, директните производи, цикличните и конечните Абелови групи, структурате на групата S_n, пермутационите групи, нормалните подгрупи, прстените, интегралните домени и полињата.

Изложувањата на лемите, теоремите и последиците се пропратени со бројни забелешки, коментари, цртежи и поголем број решени примери. Имено, усвојувањето на која било математичка дисциплина не е можно без решавање на голем број задачи, па затоа во сите делови на книгата теориските разгледувања се пропратени со 249 решени примери, како и 418 задачи за самостојна работа, голем дел од кои содржат и повеќе подзадачи што значи вистинскиот број на решени примери и задачи за самостојна работа е значително поголем.

На крајот од книгата е дадена користената литература, со што се надеваме ќе се олесни нејзиното користење, но и на читателот ќе му овозможи да консултира дополнителна сродна литература, која пред сè е пишувана со ист или сличен методски пристап. Исто така е даден и индекс на поими, чија намена е да го олесни користењето на самата книга.

Се надеваме дека книгава ќе им биде од корист како на студентите, за кои пред сè истата е наменета, така и на поширок круг читатели, кои секојдневно се среќаваат со материјата која е предмет на разработка на оваа книга.

Пријатна должност и особено задоволство ни е да им се заблагодариме на рецензентите проф. д-р Костадин Тренчевски и проф. д-р Билјана Крстеска, кои со своите сугестии придонесоа да се подобри изложувањето на презентираниот материјал.

И покрај вложениот напор, свесни сме за можните подобрувања во изложувањето на разработуваниот материјал и за пропустите кои ги содржи оваа книга. Затоа сме однапред благодарни на секоја добронамерна сугестија и критика, која ќе овозможи подобрување на книгава.

Ноември, 2015 Авторите

I ГЛАВА
ЕЛЕМЕНТИ ОД МАТЕМАТИЧКА ЛОГИКА

1. ИСКАЗИ

1.1. Често пати се среќаваме со реченици од видот: "Реката Вардар минува низ Скопје." Со неа е искажано тврдење што е вистинито. Со реченицата пак "Реката Вардар минува низ Прилеп" е искажано едно тврдење што не е вистинито.

Претходните реченици се декларативни и за секоја од нив има смисла да се постави прашањето дали е вистинито или невистинито тоа што е искажано со нив. Ваквите реченици имаат посебна важност во математиката и воопшто во животот. Така ја имаме следната дефиниција.

1.2. Дефиниција. Декларативната, осмислена реченица, којашто е или вистинита или невистинита ја нарекуваме *исказ.*

1.3. Пример. Следните реченици се искази:

а) Три плус пет е еднакво на девет.

б) 8 е парен број.

в) Скопје е главен град на Р. Македонија.

г) $5+3<8$.

Притоа од овие искази вистините се исказите под б) и в). ♦

1.4. Пример. Следните реченици не се искази:

а) Зелената боја е најпривлечна.

б) $3x+2=8$.

Имено, во случајот под а) за едни зелената боја е најпривлечна, но за други тоа не е точно. Во случајот под б) за $x=0$ се добива $3\cdot 0+2=8$ што е невистинито, а за $x=2$ се добива $3\cdot 2+2=8$ што е вистинито. ♦

1.5. Претходниот пример покажува дека не секоја декларативна реченица е исказ.

Исказите најчесто ги означуваме со малите букви од латиницата: $p,q,r,\ldots$ истите ќе ги нарекуваме исказни променливи. Притоа, наместо p е ознака за исказ ќе велиме p е исказ.

Даден исказ p може да биде или вистинит или невистинит. Зборовите "вистинит" (точен) или "невистинит" (неточен) ги нарекуваме вистинитосни вредности и тие се означуваат со симболите T (те) и $\perp$ (не те), соодветно. Понатаму, наместо реченицата: "Исказот p е вистинит" ќе пишуваме

$$\tau(p)=\mathsf{T}$$

и ќе читаме тау од p е те, а кога исказот p е невистинит ќе пишуваме

$$\tau(p) = \bot$$

и ќе читаме тау од p е не те.

1.6. Дефиниција. Декларативните реченици формирани од два дадени искази со помош на сврзниците "и", "или", "ако...,тогаш", "ако и само ако" и негацијата "не" ги нарекуваме *сложени искази*.

Исказот, што не содржи ниту еден од наведените сврзници или негацијата не, го нарекуваме *прост* или *елементарен исказ*.

1.7. Пример. Исказите

а) Пет е непарен број,

б) Шест е поголем од четири

се елементарни искази, а исказите

в) Ако врне дожд, тогаш улицата е мокра.

г) Ако четириаголникот има еднакви страни, тогаш тој е ромб или квадрат.

се сложени искази. ♦

1.8. Коментар. Сложениот исказ може да биде или вистинит или невистинит и неговата вистинитостна вредност зависи од вистинитосните вредности на исказите од кои е составен и сврзникот кој притоа е употребен.

2. КОНЈУНКЦИЈА. ДИСЈУНКЦИЈА. НЕГАЦИЈА

2.1. Дефиниција. Нека p и q се искази. Составната реченица "p и q" ја нарекуваме *конјункција* на исказите p и q. Конјункцијата "p и q" на исказите p и q е исказ, вистинит кога обата искази p и q се вистинити, а невистинит кога барем едниот од нив е невистинит.

Конјункцијата на исказите p и q ја означуваме со $p \wedge q$.

2.2 Пример. а) Исказ p: Реката Драгор минува низ Битола.

Исказ q: Планината Галичица лежи меѓу Охридското и Преспанското езеро.

Нивната конјункција, т.е. исказот $p \wedge q$:

"Реката Драгор минува низ Битола и планината Галичица
лежи меѓу Охридското и Преспанското езеро."

е вистинит исказ, бидејќи обата исказа p и q се вистинити.

б) Искази: $p: 4 \mid 16$ и $q: 6 < 5$. Конјункцијата $p \wedge q: 4 \mid 16$ и $6 < 5$ е невистинит исказ бидејќи не е вистинит исказот q, т.е. $\tau(6 < 5) = \bot$. ♦

2.3. Зависноста на вистинитосната вредност на конјункцијата $p \wedge q$ од вистинитосните вредности на p и q прегледно може да се даде со следнава вистинитосна таблица.

p	q	$p \wedge q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

Да забележиме дека во првиот ред наместо $\tau(p)$, $\tau(q)$ и $\tau(p \wedge q)$ за пократко пишуваме p, q и $p \wedge q$.

2.4. Дефиниција. Нека p и q се искази. Разделната реченица "p или q" ја нарекуваме *дисјункција* на исказите p и q. Дисјункцијата "p или q" на исказите p и q е исказ, вистинит кога барем едниот од исказите p и q е вистинит, а невистинит кога обата се невистинити.

Дисјункцијата на исказите p и q ја означуваме со $p \vee q$.

2.5. Пример. а) За исказите p: Велес е град во Р. Македонија и q: Европската Унија има унитарно уредување, дисјункцијата $p \vee q$:

"Велес и град во Р. Македонија или Европската
Унија има унитарно уредување"

е вистинит исказ, бидејќи исказот p е вистинит, т.е. $\tau(p) = \top$.

б) Дисјункцијата

$$(256 : 5 = 51) \vee (6 \cdot 3 = 13)$$

е невистинита, бидејќи и двата искази од кои е формирана се невистинити. ♦

2.6. Таблицата на вистинитост за дисјункцијата $p \vee q$ на исказите p и q е следнава:

p	q	$p \vee q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

2.7. Дефиниција. Нека p е исказ. Реченицата "Не p" е исказ кој го нарекуваме *негација* на исказот p и го означуваме со $\neg p$. Негацијата $\neg p$ е вистинит исказ кога исказот p е невистинит, а невистинит кога исказот p е вистинит.

Таблицата на вистинитост на негацијата $\neg p$ е:

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

2.8. Пример. а) За исказот p: 6 е парен број, кој е вистинит негацијата $\neg p$ е: "Не е точно дека бројот 6 е парен број" и тоа е невистинит исказ.

б) За исказот q: Реката Брегалница минува низ Штип, кој е вистинит негацијата $\neg q$ е: "Реката Брегалница не минува низ Штип" и тоа е невистинит исказ. ♦

2.9. Коментар. Исказите "2 е прост број или 2 е парен број" и "или 2 е прост број или 2 е парен број" се различни и имаат различни вистинитосни вредности. Исказот "или p или q" го нарекуваме *исклучна дисјункција* на исказите p и q во ознака $p \underline{\vee} q$. Исклучната дисјункција е вистинита само во случај кога едниот од исказите p и q е вистинит, а другиот е невистинит. Така исказот "или 2 е прост број или 2 е парен број" е невистинит исказ, а исказот "2 е прост број или 2 е парен број" е вистинит исказ.

2.10. Пример. Да го разгледаме исказот: "Илија ќе ја плати ратата за колата или во спротивно ќе ја изгуби својата кола и ќе мора да оди пешки."

Во случајот станува збор за сложен исказ кој со помош на простите искази:

p: Илија ќе ја плати ратата за колата

q: Илија ќе ја задржи својата кола, и

r: Илија ќе оди пешки

може да се запише во видот: $p \vee (\neg q \wedge r)$. Притоа, таблицата на вистинитост ни овозможува да знаеме точно во кои случаи исказот $p \vee (\neg q \wedge r)$. е вистинит. Јасно, притоа мораме да сме сигурни дека сме ги разгледале сите случаи. Имаме

p	q	r	$\neg q$	$\neg q \wedge r$	$p \vee (\neg q \wedge r)$.
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$

3. УСЛОВНИ ИСКАЗИ

3.1. Дефиниција. Нека p и q се искази. Условната реченица "Ако p тогаш q" ја нарекуваме *импликација* на исказите p и q. Импликацијата "Ако p тогаш q" на исказите p и q е исказ, невистинит кога p е вистинит и q е невистинит, а вистинит во сите други случаи.

Импликацијата на исказите p и q ја означуваме со $p \Rightarrow q$. Во импликацијата $p \Rightarrow q$ исказот p го нарекуваме претпоставка, а исказот q заклучок.

3.2. Пример. За исказите p и q:

p: Четириаголникот $ABCD$ е правоаголник

q: Дијагоналите на четириаголникот $ABCD$ се еднакви

импликацијата $p \Rightarrow q$ е: Ако четириаголникот $ABCD$ е правоаголник, тогаш неговите дијагонали се еднакви. ♦

3.3. Таблицата на вистинитост на импликацијата $p \Rightarrow q$ на исказите p и q е:

p	q	$p \Rightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

Во математиката со импликацијата се поврзани три нови искази. Имено, ако е дадена импликацијата $p \Rightarrow q$, тогаш можеме да ги формираме исказите:

$$q \Rightarrow p,\ \neg p \Rightarrow \neg q \text{ и } \neg q \Rightarrow \neg p$$

кои соодветно ги нарекуваме конверзија од $p \Rightarrow q$, инверзија од $p \Rightarrow q$ и контрапозиција од $p \Rightarrow q$. На читателот му препуштаме да ги состави таблиците на вистинитоста за овие искази.

3.4. Дефиниција. Нека p и q се искази. Сложениот исказ

$$(p \Rightarrow q) \wedge (q \Rightarrow p)$$

го нарекуваме *еквиваленција* на исказите p и q и го означуваме $p \Leftrightarrow q$.

3.5. Ако еквиваленцијата $p \Leftrightarrow q$ ја запишеме со помош на условни реченици, тогаш истата го има видот:

Ако p, тогаш q и ако q, тогаш p.

кој говорно можеме да го искажеме со зборовите: p ако и само ако q. Ќе ја определиме таблицата на вистинитост на еквиваленцијата $p \Leftrightarrow q$. Имаме:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \Rightarrow q \wedge q \Rightarrow p$
T	T	T	T	T
T	$\perp$	$\perp$	T	$\perp$
$\perp$	T	T	$\perp$	$\perp$
$\perp$	$\perp$	T	T	T

Според тоа, исказот $p \Leftrightarrow q$ е вистинит единствено кога p и q имаат иста вистинитосна вредност.

3.6. Пример. а) Исказот: "$2^3 = 8$ ако и само ако $2^3 = 2 \cdot 2 \cdot 2$" е вистинит исказ бидејќи $\tau(2^3 = 8) = \mathsf{T}$ и $\tau(2^3 = 2 \cdot 2 \cdot 2) = \mathsf{T}$.

б) Исказот: "$(-3)(-4) = -12$ ако и само ако $3 \cdot 4 = 12$" е невистинит, бидејќи $\tau((-3)(-4) = -12) = \perp$,а $\tau(3 \cdot 4 = 12) = \mathsf{T}$. ♦

4. ИСКАЗНИ ФОРМУЛИ. ТАФТОЛОГИИ

4.1. Дефиниција. *i)* Константите T и $\perp$ и исказните букви се исказни формули.

ii) Ако A и B се исказни формули, тогаш и симболите $\neg A$, $(A \wedge \mathrm{B})$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$ и $(A \underline{\vee} B)$ се исказни формули.

iii) Исказните формули може да се формираат само со помош на конечен број примени на правилата *i)* и *ii)*

4.2. Забелешка. За симболите $\wedge, \vee, \Rightarrow, \Leftrightarrow$ и $\neg$ е прифатено логичките операции да се извршуваат по следниот редослед: прво $\neg$, потоа $\wedge$, па $\vee$, па $\Rightarrow$ и на крајот $\Leftrightarrow$. Последното овозможува исказните формули да ги запишуваме со помалку загради.

4.3. Пример. Исказот: "Ако $4 \neq 2$, тогаш $5 = 4+1$ и $5 \neq 4+1$" со исказна формула може да се запише на следниот начин:

$$p \Rightarrow q \wedge \neg q$$

каде што $p : 4 \neq 2$ и $q : 5 = 4+1$. ♦

4.4. Пример. Да ги разгледаме исказите

p: Денес врнеше дожд, и

q: Денес врнеше снег.

Од овие искази ќе ги формираме исказите:

$\neg(p \vee q)$: Не е точно дека денес врнеше дожд или снег.

$\neg p \wedge \neg q$: Денес не врнеше дожд и денес не врнеше снег.

За последните искази ќе ги формираме таблиците на вистинитост. Имаме

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q):$	$\neg p \wedge \neg q:$
T	T	$\bot$	$\bot$	T	$\bot$	$\bot$
T	$\bot$	$\bot$	T	T	$\bot$	$\bot$
$\bot$	T	T	$\bot$	T	$\bot$	$\bot$
$\bot$	$\bot$	T	T	$\bot$	T	T

Забележуваме дека во сите четири случаи вистинитосната вредност на исказот $\neg(p \vee q):$ е иста со вистинитосната вредност на исказот $\neg p \wedge \neg q:$. Последното значи дека сложениот исказ

$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

е вистинит за секоја вредност на исказите p и q. ♦

4.5. Пример. Да го разгледаме исказот

$p:$ Улицата е мокра

и од истиот да го формираме исказот:

$p \wedge \neg p:$ Улицата е мокра и улицата не е мокра.

За последниот исказ таблицата на вистинитост е:

p	$\neg p$	$p \wedge \neg p$
T	$\bot$	$\bot$
$\bot$	T	$\bot$

Последното значи дека исказот $p \wedge \neg p$ е невистинит за секоја вредност на вистинитост на исказот p. ♦

4.6. Пример. Дадена е исказната формула

$$p \Rightarrow (q \wedge \neg q) \tag{1}$$

каде што p и q се искази, чии вистинитосни вредности не ги знаеме. Да ја одредиме вистинитосната вредност на оваа исказна формула за сите можни комбинации на вистинитосните вредности од исказните букви p и q. Таблицата на вистинитост на исказната формула (1) е:

p	q	$\neg q$	$q \wedge \neg q$	$p \Rightarrow (q \wedge \neg q)$
T	T	$\bot$	$\bot$	$\bot$
T	$\bot$	T	$\bot$	$\bot$
$\bot$	T	$\bot$	$\bot$	T
$\bot$	$\bot$	T	$\bot$	T

како што можеме да видиме, за некои вредности на вистинитост на p и q исказната формула (1) е вистинита, но за некои таа не е вистинита. ♦

4.7. Последните три примери се причина за класификација на исказните формули. Така ја имаме следнава дефиниција.

Дефиниција. Исказната формула која секогаш е вистинита ја нарекуваме *тафтологија*, исказната формула која што секогаш е невистинита ја нарекуваме *контрадикција*, а исказната формула која е за едни вредности на исказните променливи вистинита, а за други невистинита ја нарекуваме *неутрална исказна формула*.

Од сите видови формули, тавтологиите имаат посебно значење. Секоја тавтологија е некој *логички закон* или *закон на мислењето*. Во следната теорема, чиј доказ го препуштаме на читателот за вежби, се дадени логичките закони кои најчесто се среќаваат во практиката.

4.8. Теорема. *i)* $p \vee \neg p$, закон за исклучување на третото

ii) $\neg(p \wedge \neg p)$, закон за непротивречност

iii) $\neg\neg p \Rightarrow p$, закон за двојна негација

iv) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$, закон за транзитивност на импликација

v) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$, закон за контрапозиција

vi) $(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$, закон за транзитивност на еквиваленција

vii) $p \vee p \Leftrightarrow p$, закон за идемпотентност на дисјункцијата

viii) $p \wedge p \Leftrightarrow p$, закон за идемпотентност на конјункција

ix) $p \vee q \Leftrightarrow q \vee p$, закон за комутативност на дисјункција

x) $p \wedge q \Leftrightarrow q \wedge p$, закон за комутативност на конјункција

xi) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$, закон за асоцијативност на дисјункцијата

xii) $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$, закон за асоцијативност на конјункција

xiii) $p \vee (p \wedge q) \Leftrightarrow p$, закон за апсорпција на дисјункцијата кон конјунцијата

xiv) $p \wedge (p \vee q) \Leftrightarrow p$, закон за апсорпција на конјункцијата кон дисјункцијата

xv) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$, закон за дистрибутивност на дисјункцијата кон конјункцијата

xvi) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$, закон за дистрибутивност на конјункцијата кон дисјункцијата

xvii) $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$, Де Морганов закон

xviii) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$, Де Морганов закон

5. КОМПЛЕТНОСТ ВО ИСКАЗНАТА ЛОГИКА

5.1. Една од важните примени на таблиците на вистинитост, покрај примена во логиката, е проектирањето на дигиталните кола. Пред да преминеме на нивното изучување, ќе го разгледаме прашањето на минималниот број на логички сврзници кој е доволен за изразување на кој било исказ составен со помош на до сега дефинираните логички сврзници. Одговорот на ова прашање го дава следната теорема, чиј доказ го оставаме на читателот за вежба.

5.2. Теорема. а) $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$

б) $(p \underline{\vee} q) \Leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$. ♦

5.3. Коментар. Знаеме дека исказот $p \Leftrightarrow q$ може да се изрази како $(p \Rightarrow q) \wedge (q \Rightarrow p)$, па затоа сврзникот $\Leftrightarrow$ е погоден за користење, но не е неопходен. Понатаму, според теоремата 5.2. а) сврзникот $\Rightarrow$ не е потребен ако ги имаме сврзниците $\neg$ и $\vee$.

Исто така, според теоремата 4.8. *xviii)* исказот $p \wedge q$ е еквивалентен на исказот $\neg(\neg p \vee \neg q)$, а според теорема 4.8. *xvii)* исказот $p \vee q$ е еквивалентен со исказот $\neg(\neg p \wedge \neg q)$. Конечно од теорема 5.2. б) следува дека свзниците $\neg$ и $\vee$ или сврзниците $\neg$ и $\wedge$ ни се доволни за изразување на било кој исказ, при што и во едниот и во другиот случај ни се потребни и двата сврзници.

Од претходно изнесеното следува дека минималниот број сврзници доволен за изразување на кој било исказ составен со помош на до сега дефинираните сврзници е два, и тоа $\neg$ и $\vee$ или $\neg$ и $\wedge$.

5.4. Шеферова црта и Пирсова стрелка. Ќе разгледаме два сврзници кои имаат својство само со еден од нив да може да се запише кој било исказ. Тоа е сврзникот $\uparrow$ кој го нарекуваме Шеферова црта и сврзникот $\downarrow$ кој го нарекуваме Пирсова стрелка. На овие сврзници им соодветствуваат следните таблици на вистинитост:

p	q	$p \uparrow q$
T	T	$\bot$
T	$\bot$	T
$\bot$	T	T
$\bot$	$\bot$	T

p	q	$p \downarrow q$
T	T	$\bot$
T	$\bot$	$\bot$
$\bot$	T	$\bot$
$\bot$	$\bot$	T

5.5. За да докажеме дека сврзникот $\uparrow$ може да замени било кој сврзник доволно е да докажеме дека сврзниците $\neg$ и $\vee$ или $\neg$ и $\wedge$ може да се изразат со користење само на сврзникот $\uparrow$. За таа цел ќе ја докажеме следнава теорема.

Теорема. а) Исказот $p \uparrow p$ е еквивалентен на исказот $\neg p$.

б) Исказот $(p \uparrow p) \uparrow (q \uparrow q)$ е еквивалентен со исказот $p \vee q$.

в) Исказот $(p \uparrow q) \uparrow (p \uparrow q)$ е еквивалентен со исказот $p \wedge q$.

Доказ. а) Имаме

p	$\neg p$	$p \uparrow p$	$(p \uparrow p) \Leftrightarrow \neg p$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\top$

б) Имаме:

p	q	$p \vee q$	$p \uparrow p$	$q \uparrow q$	$(p \uparrow p) \uparrow (q \uparrow q)$	$(p \vee q) \Leftrightarrow ((p \uparrow p) \uparrow (q \uparrow q))$
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\top$

в) Имаме

p	q	$p \wedge q$	$p \uparrow q$	$(p \uparrow q) \uparrow (p \uparrow q)$	$(p \wedge q) \Leftrightarrow ((p \uparrow q) \uparrow (p \uparrow q))$
$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$

5.6. За да докажеме дека сврзникот $\downarrow$ може да го замени кој било сврзник доволно е да докажеме дека сврзниците $\neg$ и $\wedge$ или $\neg$ и $\vee$ можат да се изразат со користење само на сврзникот $\downarrow$. За таа цел ќе ја докажеме следнава теорема.

Теорема. а) Исказот $p \downarrow p$ е еквивалентен на исказот $\neg p$.

б) $(p \downarrow p) \downarrow (q \downarrow q)$ е еквивалентен на исказот $p \wedge q$.

в) $(p \downarrow q) \downarrow (p \downarrow q)$ е еквивалентен на исказот $p \vee q$.

Доказ. Доволно е да составиме таблица на вистинитост. Деталите ги оставаме на читателот за вежба. ♦

5.7. Коментар. На крајот од овој дел да забележиме дека исказот $p \uparrow q$ е еквивалентен на исказот $\neg(p \wedge q)$, а исказот $p \downarrow q$ е еквивалентен на исказот $\neg(p \vee q)$. Затоа во следните разгледувања сврзникот $\uparrow$ ќе го нарекуваме *ни*, а сврникот $\downarrow$ ќе го нарекуваме *нили*.

6. НОРМАЛНИ ФОРМИ

6.1. Пример. Нека е дадена следнава таблица на вистинитост:

случај	p	q	
1	$\top$	$\top$	$\top$
2	$\top$	$\bot$	$\top$
3	$\bot$	$\top$	$\top$
4	$\bot$	$\bot$	$\top$

Знаеме дека $p \wedge q$ е точен во првиот случај и неточен во сите останати случаи. Исто така, исказот $p \wedge \neg q$ е точен само во вториот случај, исказот $\neg p \wedge q$ само во третиот случај, а исказот $\neg p \wedge \neg q$ само во четвртиот случај. Ако за секој случај кој сакаме да биде точен земеме исказ кој е точен само во тој случај и овие искази меѓусебно ги поврземе со сврзникот $\vee$, ќе добиеме исказ кој е точен само во саканите случаи. Така, за дадената таблица на вистинитост го добиваме исказот

$$(p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q) . \blacklozenge$$

6.2. Пример. Во следната таблица за променливите p, q и r во последната колона се дадени соодветните искази кои се точни само во редот во кој се наоѓаат

Случај	p	q	r	
1	$\top$	$\top$	$\top$	$p \wedge q \wedge r$
2	$\top$	$\top$	$\bot$	$p \wedge q \wedge \neg r$
3	$\top$	$\bot$	$\top$	$p \wedge \neg q \wedge r$
4	$\top$	$\bot$	$\bot$	$p \wedge \neg q \wedge \neg r$
5	$\bot$	$\top$	$\top$	$\neg p \wedge q \wedge r$
6	$\bot$	$\top$	$\bot$	$\neg p \wedge q \wedge \neg r$
7	$\bot$	$\bot$	$\top$	$\neg p \wedge \neg q \wedge r$
8	$\bot$	$\bot$	$\bot$	$\neg p \wedge \neg q \wedge \neg r$

Ако сакаме да имаме исказ кој е точен само во определени случаи, ќе ги земеме изразите кои соодвествуваат на случаите кои се точни и ќе ги поврземе со сврзникот $\vee$. Така, исказот кој соодвествува на таблицата на вистинитост

Случај	p	q	r	
1	$\top$	$\top$	$\top$	$\top$
2	$\top$	$\top$	$\bot$	$\top$
3	$\top$	$\bot$	$\top$	$\bot$
4	$\top$	$\bot$	$\bot$	$\bot$
5	$\bot$	$\top$	$\top$	$\top$
6	$\bot$	$\top$	$\bot$	$\bot$
7	$\bot$	$\bot$	$\top$	$\bot$
8	$\bot$	$\bot$	$\bot$	$\top$

гласи

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) . \blacklozenge \qquad (1)$$

6.3. Исказот даден во видот (1) го нарекуваме дисјунктивна нормална форма, а исказите $p \wedge q \wedge r; p \wedge q \wedge \neg r; \neg p \wedge q \wedge r$ и $\neg p \wedge \neg q \wedge \neg r$ ги нарекуваме конјункти. Поточно ја имаме следнава дефиниција.

Дефиниција. Нека се дадени простите искази $p_1, p_2, ..., p_n$. Исказите од видот $x_1 \wedge x_2 \wedge ... \wedge x_n$, каде $x_i = p_i$ или $\neg p_i$ ги нарекуваме *конјункти*. Исказот од видот $m_1 \vee m_2 \vee ... \vee m_n$, каде $m_i, i = 1, 2, ..., n$ се конјункти го нарекуваме *дисјунктивна нормална форма*.

6.4. Пример. Во следнава таблица за променливите p, q и r во последната колона се дадени соодветните искази кои се неточни само во редот во кој се наоѓаат и точни во сите останати случаи

Случај	p	q	r	
1	$\top$	$\top$	$\top$	$\neg p \vee \neg q \vee \neg r$
2	$\top$	$\top$	$\bot$	$\neg p \vee \neg q \vee r$
3	$\top$	$\bot$	$\top$	$\neg p \vee q \vee \neg r$
4	$\top$	$\bot$	$\bot$	$\neg p \vee q \vee r$
5	$\bot$	$\top$	$\top$	$p \vee \neg q \vee \neg r$
6	$\bot$	$\top$	$\bot$	$p \vee \neg q \vee r$
7	$\bot$	$\bot$	$\top$	$p \vee q \vee \neg r$
8	$\bot$	$\bot$	$\bot$	$p \vee q \vee r$

Ако сакаме да најдеме исказ на кој му соодвествува дадена таблица на вистинитост, за секој од случаевите во кој таблицата има неточна вредност, ќе го земеме соодветниот исказ и добиените искази меѓусебно ќе ги поврземе со сврникот $\wedge$. Така на таблицата на вистинитост

Случај	p	q	r	
1	$\top$	$\top$	$\top$	$\top$
2	$\top$	$\top$	$\bot$	$\top$
3	$\top$	$\bot$	$\top$	$\bot$
4	$\top$	$\bot$	$\bot$	$\bot$
5	$\bot$	$\top$	$\top$	$\top$
6	$\bot$	$\top$	$\bot$	$\bot$
7	$\bot$	$\bot$	$\top$	$\bot$
8	$\bot$	$\bot$	$\bot$	$\top$

и соодвествува исказот

$$(\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r)\,. \blacklozenge \qquad (2)$$

6.5. Исказот даден во видот (2) го нарекуваме конјунктивна нормална форма, а исказите $\neg p \vee q \vee \neg r; \neg p \vee q \vee r; p \vee \neg q \vee r$ и $p \vee q \vee \neg r$ ги нарекуваме дисјункти. Поточно ја имаме следнава дефиниција.

Дефиниција. Нека се дадени простите искази $p_1, p_2, ..., p_n$. Исказите од видот $x_1 \vee x_2 \vee ... \vee x_n$, каде $x_i = p_i$ или $\neg p_i$ ги нарекуваме *дисјункти*. Исказот од видот $m_1 \wedge m_2 \wedge ... \wedge m_n$, каде $m_i, i = 1, 2, ..., n$ се дисјункти го нарекуваме *конјунктивна нормална форма*.

7. КАРНООВИ МАПИ

7.1. Иако кој било исказ може да се изрази како дисјунктивна нормална форма, сепак тоа најчесто не е и наједноставен облик. Во овој дел ќе ги разгледаме Карноовите мапи, кои ни овозможуваат да ги поедноставиме исказите дадени во дисјунктивна нормална форма.

7.2. За простите искази $p_1, p_2, ..., p_n$ постојат 2^n различни конјункти (тврдење кое ќе го докажеме во следните разгледувања). На пример, за исказите p и q постојат конјунктите $p \wedge q$, $p \wedge \neg q$, $\neg p \wedge q$ и $\neg p \wedge \neg q$. *Карноова мапа* е табелата во која секое поле преставува еден конјункт. На пример, за исказите p и q Карноовата мапа има вид даден на цртеж 1, каде внатрешните полиња претставуваат конјункти дадени на цртеж 2.

	q	$\neg q$
p		
$\neg p$		

Цртеж 1

	q	$\neg q$
p	$p \wedge q$	$p \wedge \neg q$
$\neg p$	$\neg p \wedge q$	$\neg p \wedge \neg q$

Цртеж 2

Даден исказ во дисјунктна нормална форма со помош на Карноова мапа го преставуваме така, што симболот x го ставаме во полето кое соодветствува на конјункцијата во исказот. На пример, на исказот $(p \wedge q) \vee (\neg p \wedge \neg q)$ му соодветствува Карноовата мапа дадена на цртеж 3.

	q	$\neg q$
p	×	
$\neg p$		×

Цртеж 3

	q	$\neg q$
p	×	×
$\neg p$		

Цртеж 4

Ако Карноовата мапа има два соседни симболи x, во иста редица или иста колона, тогаш изразот може да се поедностави со редукција на два конјунктни на еден и така да се добие израз кој содржи еден исказ помалку (т.е. или p не се јавува во изразот или не се јавува q). На пример, изразот

$$(p \wedge q) \vee (p \wedge \neg q)$$

на кој му соодвествува Карноовата мапа дадена на цртеж 4 е еквивалентен на искажзот p, бидејќи

$$(p \wedge q) \vee (p \wedge \neg q) \equiv p \wedge (q \vee \neg q) \equiv p \wedge \mathsf{T} \equiv p .$$

7.3. Пример. Карноовата мапа за исказите p, q и r има вид даден на цртежот 5, во кој внатрешните полиња ги преставуваат конјунктите прикажани на цртеж 6.

	q	q	$\neg q$	$\neg q$
p				
$\neg p$				
	r	$\neg r$	$\neg r$	r

Цртеж 5

	q	q	$\neg q$	$\neg q$
p	$p \wedge q \wedge r$	$p \wedge q \wedge \neg r$	$p \wedge \neg q \wedge \neg r$	$p \wedge \neg q \wedge r$
$\neg p$	$\neg p \wedge q \wedge r$	$\neg p \wedge q \wedge \neg r$	$\neg p \wedge \neg q \wedge \neg r$	$\neg p \wedge \neg q \wedge r$
	r	$\neg r$	$\neg r$	r

Цртеж 6

Според тоа, на исказот

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r)$$

му соодвествува Карноовата мапа дадена на цртеж 7.

	q	q	$\neg q$	$\neg q$
p		×		×
$\neg p$		×		
	r	$\neg r$	$\neg r$	r

Цртеж 7

И во овој случај, бидејќи две полиња со знакот x се соседни, двата соодветни конјункти можат да се редуцираат во еден, кој нема да содржи еден од исказите p, q или r. Во случајот

$$(p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \equiv (p \vee \neg p) \wedge (q \wedge \neg r) \equiv \mathsf{T} \wedge (q \wedge \neg r) = q \wedge \neg r$$

па изразот го добива видот

$$(q \wedge \neg r) \vee (p \wedge \neg q \wedge r)\,. \blacklozenge$$

7.4. Пример. Да го разгледаме изразот

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r) \qquad (1)$$

чија Карноова мапа е дадена на цртежот 8.

	q	q	$\neg q$	$\neg q$
p		×	×	
$\neg p$		×	×	
	r	$\neg r$	$\neg r$	r

Цртеж 8

Во првата редица имаме два соседни симболи x, а истото и во втората, па затоа овие два по два конјункти можат да се редуцираат на по еден, соодветно. Имаме:

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) = (q \wedge \neg q) \vee (p \wedge \neg r) = \mathsf{T} \wedge (p \wedge \neg r) = p \wedge \neg r\,,$$

$$(\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r) = (q \wedge \neg q) \vee (\neg p \wedge \neg r) = \mathsf{T} \wedge (\neg p \wedge \neg r) = \neg p \wedge \neg r\,.$$

Според тоа (1) го добива видот

$$(p \wedge \neg r) \vee (\neg p \wedge \neg r)\,. \qquad (2)$$

Понатаму за изразот (2) ја формираме Карноовата мапа која е дадена на цртеж 9.

	r	$\neg r$
p		×
$\neg p$		×

Цртеж 9

Во втората колона имаме два соседни симболи x па затоа овие два конјункти можат да се редуцираат во еден. Имаме,

$$(p \wedge \neg r) \vee (\neg p \wedge \neg r) = (p \vee \neg p) \wedge \neg r = \mathsf{T} \wedge \neg r = \neg r\,.$$

Конечно, изразот (1) се редуцира во изразот $\neg r$. ♦

7.5. Коментар. Во досегашните разгледувања соседството на означените полиња, по редица или колона во Карноовата мапа, само ни покажуваат кај кои конјункти може да се изврши упростување. Меѓутоа, самото упростување се базира на теоремата 4.8. *xvi)* на законот за дистрибутивност на конјункцијата кон дисјункцијата.

7.6. Пример. Да го разгледаме изразот:

$$\begin{aligned}&(p\wedge q\wedge r\wedge s)\vee(p\wedge q\wedge\neg r\wedge s)\vee(p\wedge q\wedge r\wedge\neg s)\vee\\&(p\wedge q\wedge\neg r\wedge\neg s)\vee(\neg p\wedge q\wedge r\wedge\neg s)\vee(\neg p\wedge q\wedge\neg r\wedge\neg s)\vee\\&(\neg p\wedge q\wedge r\wedge s)\vee(\neg p\wedge q\wedge\neg r\wedge s)\vee(p\wedge\neg q\wedge\neg r\wedge s)\vee\\&(p\wedge\neg q\wedge r\wedge s)\vee(p\wedge\neg q\wedge r\wedge\neg s)\end{aligned}\qquad(3)$$

за кој Карноовата мапа е дадена на цртеж 10.

	q	q	$\neg q$	$\neg q$	
p	×	×	×	×	s
p	×	×		×	$\neg s$
$\neg p$	×	×			$\neg s$
$\neg p$	×	×			s
	r	$\neg r$	$\neg r$	r	

Цртеж 10

Истата се формира по следниов принцип: на пример за конјунктот

$$p\wedge\neg q\wedge\neg r\wedge\neg s$$

крвчето се наоѓа во вкупниот пресек на првите две редици (од p), последните две колони (од $\neg q$), третата и втората колона (од $\neg r$) и првата и четвртата редица (од s), што заедно дава пресек на првата редица и третата колона.

Аналогно, како во претходните примери, земајќи ги предвид конјунктите соодветни на соседните полиња во Карноовата мапа ќе извршиме упростување. Така, земајќи ги предвид соседните полиња по редици имаме:

$$(p\wedge q\wedge r\wedge s)\vee(p\wedge q\wedge\neg r\wedge s)\equiv(r\vee\neg r)\wedge(p\wedge q\wedge s)\equiv p\wedge q\wedge s$$

$$(p\wedge q\wedge r\wedge\neg s)\vee(p\wedge q\wedge\neg rv\neg s)\equiv(r\vee\neg r)\wedge(p\wedge q\wedge\neg s)\equiv p\wedge q\wedge\neg s$$

$$(\neg p\wedge q\wedge r\wedge\neg s)\vee(\neg p\wedge q\wedge\neg r\wedge\neg s)\equiv(r\vee\neg r)\wedge(\neg p\wedge q\wedge\neg s)\equiv\neg p\wedge q\wedge\neg s$$

$$(\neg p\wedge q\wedge r\wedge s)\vee(\neg p\wedge q\wedge\neg r\wedge s)\equiv(r\vee\neg r)\wedge(\neg p\wedge q\wedge s)\equiv\neg p\wedge q\wedge s$$

$$(p\wedge\neg q\wedge\neg r\wedge s)\vee(p\wedge\neg q\wedge r\wedge s)\equiv(r\vee\neg r)\wedge(p\wedge\neg q\wedge s)\equiv p\wedge\neg q\wedge s$$

$$p\wedge\neg q\wedge r\wedge\neg s\equiv p\wedge\neg q\wedge r\wedge\neg s$$

Па затоа изразот (3) е еквивалентен со изразот

$$(p\wedge q\wedge s)\vee(p\wedge q\wedge\neg s)\vee(\neg p\wedge q\wedge\neg s)\vee(\neg p\wedge q\wedge s)\vee(p\wedge\neg q\wedge s)\vee(p\wedge\neg q\wedge r\wedge\neg s)\qquad(4)$$

За првите четири конјункти во (4) ја формираме соодветната Карноова мапа (цртеж 11)

	q	q	$\neg q$	$\neg q$
p	×	×		
$\neg p$	×	×		
	s	$\neg s$	$\neg s$	s

цртеж 11.

и ако ја повториме постапката по редици добиваме

$$(p \wedge q \wedge s) \vee (p \wedge q \wedge \neg s) \equiv (s \vee \neg s) \wedge (p \wedge q) \equiv p \wedge q$$
$$(\neg p \wedge q \wedge s) \vee (\neg p \wedge q \wedge \neg s) \equiv (s \vee \neg s) \wedge (\neg p \wedge q) \equiv \neg p \wedge q$$

Па затоа првите четири конјункти во (4) се редуцираат на

$$(p \wedge q) \vee (\neg p \wedge q) \equiv (p \vee \neg p) \wedge q = q\ .$$

Според тоа, за изразот (4) добиваме:

$$q \vee (p \wedge \neg q \wedge s) \vee (p \wedge \neg q \wedge r \wedge \neg s) \equiv [(q \vee \neg q) \wedge (q \vee (p \wedge s))] \vee (p \wedge \neg q \wedge r \wedge \neg s) \equiv$$
$$q \vee (p \wedge s) \vee (p \wedge \neg q \wedge r \wedge \neg s) \equiv (p \wedge s) \vee q \vee (\neg q \wedge p \wedge r \wedge \neg s) \equiv$$
$$(p \wedge s) \vee [(q \vee \neg q) \wedge (q \vee (p \wedge r \wedge \neg s)) \equiv (p \wedge s) \vee q \vee (p \wedge r \wedge \neg s) \equiv$$
$$q \vee [p \wedge (s \vee (r \wedge \neg s))] \equiv q \vee [p \wedge [(s \vee \neg s) \wedge (s \vee r)]] \equiv$$
$$q \vee [p \wedge (s \vee r)] \equiv q \vee (p \wedge s) \vee (p \wedge r),$$

што значи дека изразот (3) се сведува на $q \vee (p \wedge s) \vee (p \wedge r)$. ♦

8. ПРЕДИКАТИ И КВАНТИФИКАТОРИ

8.1. Реченицата

$$x + 3 = 8 \qquad (1)$$

не е исказ, бидејќи за вредноста на променливата $x = 5$ таа е вистинита, а за останатите вредности на x не е вистинита.

Исто така реченицата

Градот x е поголем од Прилеп (2)

е реченица со променлива. Притоа, ако на местото на x ставиме било кој град таа ќе стане исказ. Ваквите реченици ги нарекуваме исказни функции или предикати. Поточно ја имаме следнава дефиниција.

8.2. Дефиниција. *Исказната функција* или *предикат* е реченица со променлива, која што станува исказ за секоја вредност на променливата од некое дадено множество D . Притоа, множеството D се вика *дефиниционо област на предикатот*, а елементите на тоа множество - допуштени вредности на променливата.

8.3. Пример. а) За предикатот " $x - 5 = 0, x \in \mathbf{N}$ " множеството D е множеството на природни броеви.

б) За предикатот $\frac{1}{x-6}=2, x\in\mathbf{R}\setminus\{6\}$ имаме $D=\mathbf{R}\setminus\{6\}$

в) За предикатот $\frac{4}{x^2-5x+6}>1, x\in\mathbf{R}\setminus\{2,3\}$ имаме $D=\mathbf{R}\setminus\{2,3\}$. ♦

8.4. Предикатите дадени во 8.3. содржат една променлива. Меѓутоа, можеме да зборуваме и за предикати со две, три и повеќе променливи. Да дадеме еден пример.

8.5. Пример. а) Предикатот "$x^2+y^2=2, x, y\in\mathbf{R}$" е со две променливи.

б) Предикатот "$xy+yz+zx=4, x, y, z\in\mathbf{Q}$" е со три променливи.

в) Предикатот "$x+y^2+z^3+t^4+r^5=7,\ x, y, z, t, r\in\mathbf{R}$" е со пет променливи. ♦

8.6. Предикатите ќе ги означуваме со големите букви од латиницата $P, Q, R, S, \ldots$ со означување на променливите во загради. Така, со $P(x), Q(x), R(x), \ldots$ ги означуваме предикатите со една променлива кои уште ги нарекуваме предикати со должина еден или *унарни предикати*, со $P(x,y), Q(x,y), \ldots$ ги означуваме предикатите со две променливи кои уште ги нарекуваме предикати со должина два или *бинарни предикати*, итн.

8.7. Пример. Предикатот "$xy=5, x, y\in\mathbf{Z}$" е со должина два и истиот можеме да го запишеме во видот

$$P(x,y): xy=5,\ \ x, y\in\mathbf{Z}.$$

Предикатот $P(x,y)$ за $x=1, y=5$ преминува во исказот

$$P(1,5): 1\cdot 5=5$$

кој е вистинит исказ. Меѓутоа за $x=y=2$ овој предикат преминува во исказот $P(2,2): 2\cdot 2=5$, кој не е вистинит. ♦

8.8. Видовме дека даден предикат со дефиниционa област D, за некои вредности на променливата станува вистинит исказ, а за други вредности – невистинит исказ. Последното е причина за воведување на следнава дефиниција.

Дефиниција. Нека е даден предикатот P. *Решение на предикатот* P е секоја вредност на променливата (променливите) за која предикатот P станува вистинит исказ. Множеството M, така да $M\subseteq D$ од сите такви вредности го нарекуваме *множество решенија на предикатот* P.

8.9. Да ги разгледаме предикатите

$$P(x): x>3 \text{ и } Q(x): 2x<2.$$

Лесно се заклучува дека и реченицата

$$x>3\wedge 2x<2$$

е предикат, т.е. дека $P(x) \wedge Q(x)$ е предикат. Воопшто земено, ако се дадени предикатите P и Q, тогаш предикати се и:

$$P \wedge Q,\ P \vee Q,\ P \Rightarrow Q,\ P \Leftrightarrow Q,\ P \underline{\vee} Q \text{ и } \neg P .$$

8.10. Пример. а) Да го разгледаме предикатот

$$P(x) : |\sin x| \leq 1,\ x \in \mathbf{R} .$$

Забележуваме дека предикатот $P(x)$ е точен за секој реален број, т.е. за секоја вредност на променливата x. Притоа пишуваме

$$\text{за секој } x,\ P(x)$$

т.е.

$$\forall x,\ \ P(x) .$$

б) Да го разгледаме предикатот

$$Q(x, y, z) : x^2 + y^2 \geq z^2,\ \ x, y, z \in \mathbf{Z}$$

Лесно се гледа дека исказот $Q(1,2,3)$ не е точен, меѓутоа исказот $Q(3,2,1)$ е точен. Според тоа, постои $x_0 \in Z$ и постои $y_0 \in Z$ и постои $z_0 \in Z$ такви што $Q(x_0, y_0, z_0)$ е точен исказ. Последното симболички го запишуваме на следниот начин

$$(\exists x)(\exists y)(\exists z)\ Q(x, y, z) . \ \blacklozenge$$

8.11. Претходно разгледаниот пример е непосредна причина за воведување на следната дефиниција.

Дефиниција. Симболот $\forall x$ го нарекуваме *универзален квантификатор* и го читаме: за секој x или за сите вредности на x.

Симболот $\exists x$ го нарекуваме *егзистенцијален квантификатор* и го читаме: постои x или за некој x.

Симболот $\exists! x$ го нарекуваме *егзистенцијален квантификатор* и го читаме: постои еден и само еден x.

8.12. Ако е $D(x)$ предикат, тогаш исказот $\forall x\, D(x)$ е точен ако и само ако за секоја вредност на променливата x предикатот $D(x)$ е точен. Логично е да се запрашаме што значи кога ќе кажеме дека исказот $\forall x\, D(x)$ не е точен? Јасно, негирањето на исказот $\forall x\, D(x)$ можеме да го изразиме со

$$\neg(\forall x\, D(x)) .$$

Понатаму, за да докажеме дека исказот $\forall x\, D(x)$ не е точен доволно е да најдеме една вредност на променливата x, за која $D(x)$ не е точен, т.е. за која $\neg D(x)$ е точен. Според тоа, исказот $\forall x\, D(x)$ не е точен ако и само ако исказот

$$\exists x(\neg D(x))$$

е точен. Значи,

$$\neg(\forall x D(x)) \Leftrightarrow \exists x(\neg D(x)) .$$

8.13. Ако $G(x)$ е предикат, на следниот начин ќе извршиме негација дека постои вредност на променливата x, за која $G(x)$ е точен, т.е.

$$\neg(\exists x G(x))$$

Јасно, ако не постои вредност x, за која предикатот $G(x)$ е точен, тогаш за сите вредности на променливата x предикатот $G(x)$ мора да биде неточен. Во овој случај, $\neg G(x)$ ќе биде точно за сите вредности на x или еквивалентно на тоа

$$\forall x(\neg G(x)) .$$

Значи,

$$\neg(\exists x G(x)) \Leftrightarrow \forall x(\neg G(x)) .$$

8.14. Пример. а) Ќе го негираме предикатот $(\forall x)(\forall y)R(x, y)$. Последователно имаме

$$\neg[(\forall x)(\forall y)R(x, y)] \Leftrightarrow (\exists x)\neg[\forall y R(x, y)] \Leftrightarrow (\exists x)(\exists y)[\neg R(x, y)]$$

б) Ќе го негираме предикатот $(\exists x)(\forall y)(\exists z)Q(x, y, z)$. Последователно добиваме

$$\neg[(\exists x)(\forall y)(\exists z)Q(x, y, z)] \Leftrightarrow (\forall x)\neg[(\forall y)(\exists z)Q(x, y, z)] \Leftrightarrow (\forall x)(\exists y)\neg[\exists z Q(x, y, z)]$$
$$\Leftrightarrow (\forall x)(\exists y)(\forall z)\neg Q(x, y, z) \quad . \blacklozenge$$

8.15. Во претходните разгледувања се осврнавме на универзалниот и егзистенцијалниот квантификатор и нивната поврзаност со предикатите. Овде ќе забележиме дека користењето на квантификаторите и предикатите најчесто се сведува на следниве четири случаи, чија точност е очигледна.

1. **Универзална партикуларизација.** Од точноста на исказот $\forall x P(x)$ може да се заклучи дека исказот $P(a)$ е точен за произволно избрана вредност a.
2. **Универзална генерализација.** Од фактот дека за произволно избрана вредност a исказот $P(a)$ е точен, можеме да заклучиме дека е точен исказот $\forall x P(x)$.
3. **Егзистенционална партикуларизација.** Од точноста на исказот $\exists x P(x)$ можеме да заклучиме дека постои некоја вредност a за која е точен исказот $P(a)$.
4. **Егзистенционална генерализација.** Од фактот дека за некоја избрана вредност a исказот $P(a)$ е точен, можеме да заклучиме дека е точен исказот $\exists x P(x)$.

8.16. Теорема. За произволни предикати $P(x)$ и $Q(x)$, определени над ист домен важи:

а) $\forall x(P(x) \wedge Q(x)) \Leftrightarrow \forall xP(x) \wedge \forall xQ(x)$.

б) $\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists xP(x) \vee \exists xQ(x)$.

в) Од исказот $\forall xP(x) \vee \forall xQ(x)$ следува исказот $\forall x(P(x) \vee Q(x))$.

г) Од исказот $\exists x(P(x) \wedge Q(x))$ следува исказот $\exists xP(x) \wedge \exists xQ(x)$.

Доказ. а) Нека е точен исказот $\forall x(P(x) \wedge Q(x))$. Сега, користејќи ја универзалната партикуларизација, може да се заклучи дека за произволна вредност на променливата a, исказот $P(a) \wedge Q(a)$ е точен. Според тоа, исказот $P(a)$ е точен за произволна вредност a и исказот $Q(a)$ е точен за произволна вредност a. Сега користејќи ја универзалната генерализација, заклучуваме дека исказите $\forall x\, P(x)$ и $\forall x\, Q(x)$ се точни. Но тоа значи дека исказот $\forall xP(x) \wedge \forall xQ(x)$ е точен.

Обратно, нека претпоставиме дека исказот $\forall xP(x) \wedge \forall xQ(x)$ е точен. Тоа значи дека исказите $\forall x\, P(x)$ и $\forall x\, Q(x)$ се точни. Понатаму, користејќи ја универзалната партикуларизација можеме да заклучиме дека, за произволна вредност на променливата a, исказите $P(a)$ и $Q(a)$ се точни. Според тоа, за произволна вредност на променливата a, исказот $P(a) \wedge Q(a)$ е точен, па ако ја искористиме универзалната генерализација заклучуваме дека исказот $\forall x(P(x) \wedge Q(x))$ е точен. ♦

9. ДИЈАГРАМИ НА ДИГИТАЛНИ КОЛА

9.1. Вообичаено е исказите кои соодветствуваат на дијаграмите на дигиталните кола да се изразуваат со користење на Булова алгебра, на која покасно ќе се навратиме. Согласно со тоа пред да почнеме да ги проучуваме дијаграмите на колата, ќе се префрлиме од логичко на Булово означување. Симболите $\wedge, \vee$ и $\neg$ ќе ги замениме со симболите $\cdot$, $+$ и $'$, соодветно. Според тоа, исказот $(p \wedge q) \vee \neg r$ го запишуваме во видот $(p \cdot q) + r'$, а исказот

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r)$$

во видот

$$(p \cdot q \cdot r') + (p \cdot q' \cdot r) + (p' \cdot q \cdot r'). \qquad (1)$$

Како и во обичната алгебра, вообичаено е симболот за производ да има приоритет и се смета дека операцијата множење се реализира пред операцијата собирање, па изразот (1) може да се запише како

$$pqr' + pq'r + p'qr'.$$

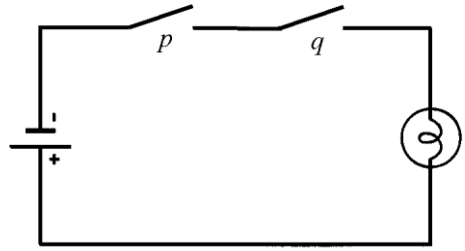
Понатаму, во таблицата на вистинитост вредноста T се заменува со бројот 1 и вредноста $\perp$ со бројот 0, па таблицата на вистинитост

p	q	r	$\neg q$	$\neg q \wedge r$	$p \vee (\neg q \wedge r)$
$\top$	$\top$	$\top$	$\bot$	$\bot$	$\top$
$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$

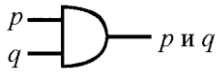
го добива видот

p	q	r	q'	$q'r$	$p+q'r$
1	1	1	0	0	1
1	1	0	0	0	1
1	0	1	1	1	1
1	0	0	1	0	1
0	1	1	0	0	0
0	1	0	0	0	0
0	0	1	1	1	1
0	0	0	1	0	0

9.2. Сега да го разгледаме електричното коло дадено на цртеж 12, во кое постојат компоненти кои претставуваат батерија и сијалица. Вредност 1 им доделуваме на прекинувачите p и q кога се затворени (т.е. ако низ нив тече струја), а во спротивно им доделуваме вредност 0. На колото му доделуваме вредност 1 кога сијалицата е вклучена, т.е. кога низ него тече струја. Јасно, кај овој тип на коло сијалицата свети и колото има вредност 1 само ако и двата прекинувачи се затворени, т.е. прекинувачите p и q имаат вредност 1. Според тоа, на ова коло му соодвествува исказот $p \cdot q$. Ваквиот распоред на прекинувачите ќе го нарекуваме p и q коло и ова коло ќе го означуваме како на цртеж 13.

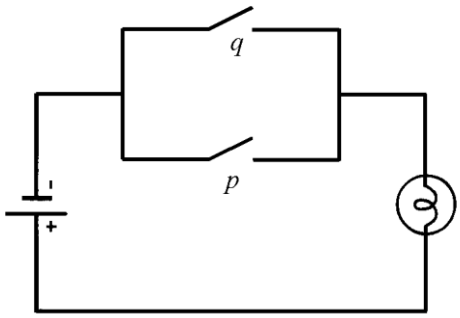


Цртеж 12

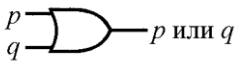


Цртеж 13

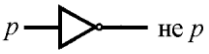
9.3. Да го разгледаме електричното коло дадено на цртеж 14, во кое прекинувачите p и q се врзани паралелно. Сијалицата свети и колото има вредност 1 ако кој било од двата прекинувачи p или q е затворен, т.е. ако $p=1$ или $q=1$. Ова коло соодветствува на исказот $p+q$, ваквиот распоред на прекинувачите го нарекуваме p или q коло и ова коло ќе го означуваме како на цртеж 15.



Цртеж 14

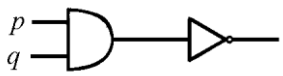


Цртеж 15



Цртеж 16

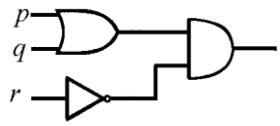
9.4. Нека претпоставиме дека постои коло (кое нема да се обидеме да го нацртаме) со еден прекинувач p, во кое сијалицата свети ако и само ако p е отворено. Според тоа, колото има вредност 1 кога p има вредност 0 и има вредност 0 кога p има вредност 1. Такво коло соодветствува на исказот p' и него го нарекуваме *не* p коло или *invertor*. Ќе го означуваме со симболот даден на цртеж 16.



Цртеж 17

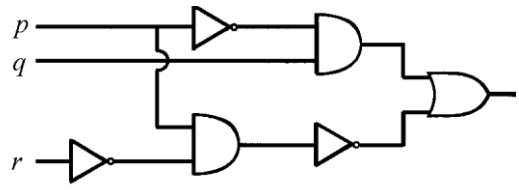
9.5. Пример. Колото на цртеж 17 се состои од p и q коло и *invertor*, што соодвествува на исказот $(p \cdot q)'$. Да забележиме дека *invertor* го негира целото коло кое му претходи.

9.6. Пример. Колото на цртеж 18 се состои од p или q коло поврзано со колото не r со помош на i коло. Според тоа, на ова коло му соодветствува исказот $(p+q)\cdot r'$.

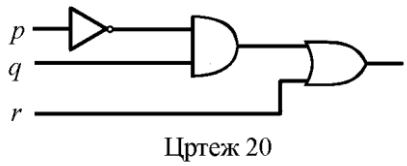


Цртеж 18

9.7. Пример. Буловиот израз за колото дадено на цртеж 19 гласи $(p'\cdot q)+(p\cdot r')'$.

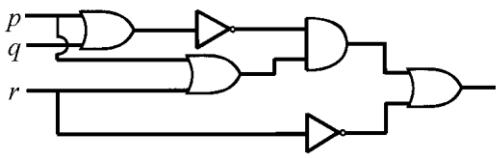


Цртеж 19



Цртеж 20

9.8. Пример. Дијаграмот на колото кој соодветствува на исказот $(p'\cdot q)+r$ е даден на цртеж 20.



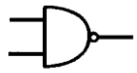
Цртеж 21

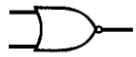
9.9. Пример. Дијаграмот на колото кој соодветствува на исказот

$$((p+q)'\cdot(p+r))+r'$$

е даден на цртеж 21.

9.10. Коментар. Во претходните разгледувања рековме дека Шеферовата црта, која се претставува со симболот $\uparrow$, има иста таблица на вистинитост како и изразот $(pq)'$, во Булова нотација, и затоа се нарекува *ni* коло. Понатаму, Пирсовата стрелка, која се преставува со симболот $\downarrow$, има иста таблица како и изразот $(p+q)'$ и затоа се нарекува *nili* коло.


Цртеж 22


Цртеж 23

Затоа на колата *ni* и *nili* им соодветствуваат симболи дадени на цртежите 22 и 23, соодветно.

9.11. Пример. Полусобирач собира два дадени бинарни броја, 1 и 0, и му соодветствува следнава таблица на собирање

+	0	1
0	0	1
1	1	10

Се нарекува полусобирач, бидејќи ако сакаме да собереме два бинарни броја кои имаат повеќе од една цифра, можеме да ги собереме само нивните крајни десни цифри, затоа што не може да се собира број кој се "пренесува". Сепак, понекогаш е згодно да се има сумата на два едноцифрени бинарни броја, така што таблица за собирање се трансформира во

+	0	1
0	00	01
1	01	10

Ако исказите p и q ги преставуваат броевите кои ги собираме, а d_1 и d_0 првата и втората цифра на збирот, ќе ја добиеме следнава таблица на вистинитост:

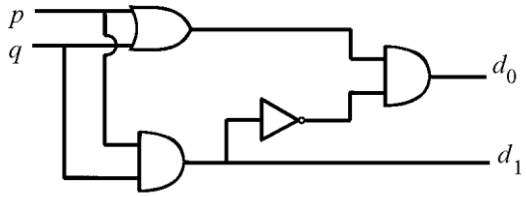
p	q	d_0
1	1	0
1	0	1
0	1	1
0	0	0

p	q	d_1
1	1	1
1	0	0
0	1	0
0	0	0

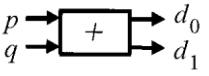
Според тоа,

$$d_0 \Leftrightarrow pq'+p'q \Leftrightarrow (p+q)\cdot(p\cdot q)'.$$

Исто така $d_1 \Leftrightarrow p\cdot q$. Дијаграмот на колото за полусобирач е даден на цртеж 24.



Цртеж 24



Цртеж 25

Бидејќи полусобирач претставува збир на два броја, ќе го означиме со симболот прикажан на цртеж 25.

9.12. Пример. Потполниот собирач собира три едноцифрени бинарни броеви. Според тоа, тој може да собере два бинарни броја и број кој се "пренесува". Овде ќе го разгледаме само случајот на три едноцифрени бинарни броеви. Ако исказите p, q и r ги претставуваат едноцифрените бинарни броеви кои ги собираме и ако се $d_1^{\#}$ и $d_0^{\#}$ првата и втората цифра на збирот, ќе ја добиеме следната таблица на вистинитост.

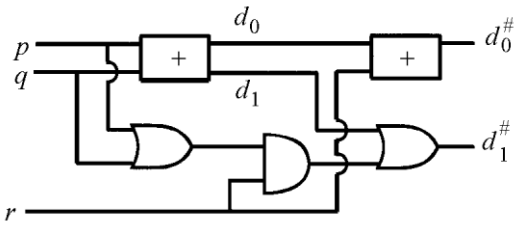
p	q	r	$d_1^{\#}$	$d_0^{\#}$
1	1	1	1	1
1	1	0	1	0
1	0	1	1	0
1	0	0	0	1
0	1	1	1	0
0	1	0	0	1
0	0	1	0	1
0	0	0	0	0

Овде $d_0^{\#}$ всушност е резултатот на собирањето на бројот d_0 добиен како збир на броевите p и q и собран со бројот r. Според тоа, неговото коло лесно се опишува. Вредноста $d_1^{\#}$, според горната таблица на вистинитост е

$$d_1^{\#} = pqr + pqr' + pq'r + p'qr .$$

Со користење на Карноовата мапа добиваме:

	q	q	$\neg q$	$\neg q$
p	x	x		x
$\neg p$	x			
	r	$\neg r$	$\neg r$	r



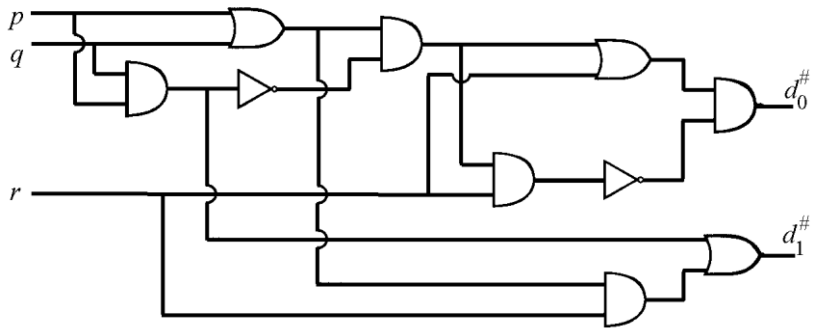
Цртеж 26

Според тоа

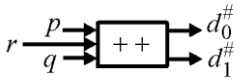
$$d_1^{\#} \Leftrightarrow pq + pr + qr = pq + (p+q)r$$

па колото може да се прикаже како на цртеж 26. Конечно, ако ова коло се детализира, тогаш за истото го добиваме цртежот 27. Бидејќи потполниот собирач се користи за собирање на три броеви истиот го означуваме со симболот

даден на цртеж 28.



Цртеж 27



Цртеж 28

ЗАДАЧИ

1. Нека p, q и r се следниве искази:

   p: Големата дога е големо куче.

   q: Јас имам мала куќа.

   r: Јас имам голема дога.

   Напишете ги следните симболички искази како реченици во обичен говорен јазик:

   а) $p \wedge q \wedge \neg r$ б) $p \wedge (\neg q \vee \neg r)$

   в) $(p \vee \neg q) \wedge r$ г) $(p \wedge r) \vee (q \wedge \neg r)$

2. Составете ги таблиците на вистинитост на исказите од задача 1.

3. Нека p, q, r и s се следниве искази:

   p: Таа сака да го цитира Конески

   q: Тој ги сака драмите со Петре Прличко

   r: Петре Прличко не сакаше да го цитира Конески

   s: Тие одат во кино

   Напишете ги следните симболички изрази како реченици во обичен говорен јазик:

   а) $\neg(((p \wedge q) \wedge \neg r) \vee \neg s)$

   б) $((p \wedge \neg q) \wedge \neg r) \vee (((p \wedge q) \wedge \neg r) \wedge \neg s)$

4. Составете ги таблиците на вистинитост на исказите од задача 3.

5. Составете ги таблиците на вистинитост на следниве искази:

а) $p \wedge (q \vee \neg r)$ б) $(q \wedge \neg r) \vee (\neg p \wedge r)$

в) $\neg(p \wedge r) \vee (\neg q \wedge r)$ г) $\neg(\neg p \vee (q \wedge \neg r))$

д) $(p \wedge r) \vee (p \wedge \neg q)$ ѓ) $(p \vee q) \wedge (r \vee q)$

е) $(\neg q \wedge r) \vee \neg(p \wedge r)$ ж) $\neg((p \wedge r) \vee \neg q)$

з) $\neg(\neg p \wedge (q \vee \neg r))$ ѕ) $(p \vee \neg r) \wedge \neg(p \vee \neg q)$

и) $(p \veebar q) \wedge (q \veebar r)$ ј) $\neg((p \wedge \neg q) \vee (p \wedge \neg r)) \veebar (q \wedge \neg r)$

к) $\neg(p \veebar q) \vee \neg(\neg(p \veebar r) \vee \neg(q \veebar r))$ љ) $(p \wedge (q \vee \neg r)) \veebar ((p \wedge \neg q) \vee r)$

6. а) Негирајте го исказот: На фармата одгледуваме крави и овци.
б) Нека p и q се следниве искази:

p : На фармата одгледуваме крави

q : На фармата одгледуваме овци

Симболички запишете го оригиналниот исказ под а).
в) Најдете таблица на вистинитост за оригиналниот и негираниот исказ под а) и проверете дали правилно сте ја извршиле негацијата,

7. а) Негирајте го исказот: Овој град и валкан и бучен.
б) Нека p и q се следниве искази:

p : Овој град е валкан

q : Овој град е бучен

Симболички запишете го оригиналниот исказ под а).
в) Најдете ги таблиците на вистинитост за оригиналниот и негираниот исказ под а) и проверете дали правилно сте ја извршиле негацијата,

8. Нека p, q и r се следниве искази:

p : Тој ќе купи нов компјутер.

q : Тој ќе слави цела ноќ.

r : Тој ќе добие на лотарија.

Напишете ги следниве реченици како симболички изрази:
a) Ако добие на лотарија, тогаш ќе купи нов компјутер и ќе слави цела ноќ.
b) Ако не купи нов компјутер, тогаш нема да слави цела ноќ.
c) Ако добие на лотарија тогаш ќе слави цела ноќ, и ако не добие на лотарија, тогаш нема да купи нов компјутер.
d) Ако не добие на лотарија или не купи нов компјутер, тогаш нема да слави цела ноќ.

9. Нека p, q и r се следниве искази:

p : Тој чита стрипови.

q : Тој сака научна фантастика.

r : Тој е информатичар

Напишете ги следниве реченици како симболички изрази:
a) Ако тој чита стрипови и сака научна фантастика, тогаш тој е информатичар
b) Ако тој не чита стрипови и не сака научна фантастика, тогаш тој не е информатичар

в) Ако тој чита стрипови, тогаш тој сака научна фантастика; и ако тој не чита стрипови, тогаш тој е информатичар

10. Нека p, q и r се следниве искази:

p: Тој сака адидас патики

q: Тој е популарен.

r: Тој има чудни пријатели

Напишете ги следниве симболички изрази како реченици:

а) $(p \wedge q) \Rightarrow r$ б) $q \Rightarrow \neg r$

в) $p \Rightarrow (q \vee r)$ г) $(p \Rightarrow \neg q) \wedge (q \Rightarrow r)$

11. Нека p, q и r се следниве искази:

p: Тој е успешен

q: Тој е популарен.

r: Тој е богат.

Напишете ги следниве симболички изрази како реченици:

а) $\neg(p \Rightarrow q)$ б) $(p \vee r) \Rightarrow q$

в) $q \Leftrightarrow (p \wedge r)$ г) $(p \Rightarrow q) \wedge (\neg r \Rightarrow (\neg p \vee \neg q))$

12. Нека p, q, r и s се следниве искази:

p: x е помал од 5

q: x е помал од 1

r: $x = 2$

s: $x = 6$

Напишете ги следниве симболички изрази како реченици:

а) $(p \wedge q) \Rightarrow (r \wedge \neg s)$ б) $(r \Rightarrow p) \wedge (s \Rightarrow q)$

в) $\neg((p \Rightarrow r) \wedge (q \Rightarrow s))$ г) $(r \veebar s) \Leftrightarrow (((p \Rightarrow r) \vee (q \Rightarrow s)) \wedge (p \vee q))$

13. Состави ги таблиците на вистинитост за следниве искази:

а) $(p \Rightarrow q) \Rightarrow r$ б) $p \Rightarrow (q \Rightarrow r)$

в) $(q \Rightarrow (p \wedge r)) \Leftrightarrow ((q \Rightarrow p) \wedge (q \Rightarrow r))$ г) $((p \Rightarrow q) \vee r) \Rightarrow (\neg p \vee \neg q)$

д) $(p \Rightarrow q) \Rightarrow (q \Rightarrow r)$ ѓ) $(p \Rightarrow q) \vee \neg(r \wedge q)$

е) $(p \vee r) \Rightarrow (p \wedge q)$ ж) $\neg((p \Rightarrow q) \wedge \neg r) \Rightarrow (p \vee \neg r)$

з) $(p \vee q) \Rightarrow q$ s) $(\neg(p \Rightarrow q) \Rightarrow (q \Rightarrow r))$

и) $(p \vee q) \wedge (p \Rightarrow r)$.

14. Одредете дали следниве искази се вистинити или невистинити:

а) Ако $2^2 = 4$, тогаш $3^2 = 9$ б) Ако $2^2 = 5$, тогаш $3^2 = 9$

в) Ако $2^2 = 5$, тогаш $3^2 = 10$ г) Ако $2^2 = 4$, тогаш $3^2 = 10$

15. Одредете ги вистинитосните вредности на исказите p, q, r и s за кои следниов исказ c е точен:

а) $((p \vee q) \vee r) \Rightarrow s$ б) $(p \vee q) \Rightarrow (r \wedge s)$

в) $(p \Rightarrow q) \wedge (r \Rightarrow s)$ г) $(p \Rightarrow s) \Rightarrow (r \veebar s)$

16. Одредете кои од следните искази се логички закони:

а) $(p \wedge q) \Rightarrow p$ б) $(p \vee q) \Rightarrow p$

в) $((p \vee q) \wedge \neg p) \Rightarrow q$ г) $(p \Rightarrow q) \wedge (p \wedge \neg q)$

д) $(((p \Rightarrow q) \wedge (q \Rightarrow r)) \wedge r) \Rightarrow p$ ѓ) $(((p \Rightarrow q) \wedge (q \Rightarrow r)) \wedge \neg r) \Rightarrow p$

е) $((p \Leftrightarrow q) \wedge (p \veebar q)$ ж) $((p \Leftrightarrow q) \vee (p \veebar q)$

17. Користејќи ги својствата на еквиваленциите покажете, без користење таблици на вистинитост, дека следниве парови искази се еквивалентни:

а) $p \Rightarrow (q \wedge r)$ и $(p \Rightarrow q) \wedge (p \Rightarrow r)$

б) $p \Rightarrow (q \vee r)$ и $(p \Rightarrow q) \vee (p \Rightarrow r)$

в) $(p \vee q) \Rightarrow r$ и $(p \Rightarrow r) \wedge (q \Rightarrow r)$

г) $(p \wedge q) \Rightarrow r$ и $(p \Rightarrow r) \vee (q \Rightarrow r)$

д) $(p \wedge q) \Rightarrow r$ и $p \Rightarrow (q \Rightarrow r)$

18. Одреди искази во дисјунктивна нормална форма, кои соодветствуваат на следниве таблици на вистинитост:

а)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊤
⊤	⊥	⊤	⊥
⊤	⊥	⊥	⊥
⊥	⊤	⊤	⊥
⊥	⊤	⊥	⊤
⊥	⊥	⊤	⊥
⊥	⊥	⊥	⊤

б)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊥
⊤	⊥	⊤	⊤
⊤	⊥	⊥	⊥
⊥	⊤	⊤	⊥
⊥	⊤	⊥	⊤
⊥	⊥	⊤	⊥
⊥	⊥	⊥	⊤

в)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊥
⊤	⊥	⊤	⊤
⊤	⊥	⊥	⊤
⊥	⊤	⊤	⊥
⊥	⊤	⊥	⊥
⊥	⊥	⊤	⊥
⊥	⊥	⊥	⊤

19. Одреди искази во конјунктивна нормална форма, кои соодветствуваат на следниве таблици на вистинитост

а)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊥
⊤	⊥	⊤	⊥
⊤	⊥	⊥	⊤
⊥	⊤	⊤	⊥
⊥	⊤	⊥	⊤
⊥	⊥	⊤	⊤
⊥	⊥	⊥	⊥

б)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊥
⊤	⊥	⊤	⊤
⊤	⊥	⊥	⊤
⊥	⊤	⊤	⊤
⊥	⊤	⊥	⊥
⊥	⊥	⊤	⊤
⊥	⊥	⊥	⊥

в)

p	q	r	
⊤	⊤	⊤	⊤
⊤	⊤	⊥	⊤
⊤	⊥	⊤	⊥
⊤	⊥	⊥	⊥
⊥	⊤	⊤	⊤
⊥	⊤	⊥	⊤
⊥	⊥	⊤	⊥
⊥	⊥	⊥	⊤

20. Поедноставете ги исказите дадени со следниве Карноови мапи

а)

	q	q	$\neg q$	$\neg q$
p	x		x	x
$\neg p$	x			x
	r	$\neg r$	$\neg r$	r

б)

	q	q	$\neg q$	$\neg q$
p	x		x	
$\neg p$	x		x	x
	r	$\neg r$	$\neg r$	r

21. Користејќи ја Карноовата мапа, поедноставете го следниот израз:

а) $(p \wedge q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r)$

б) $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$

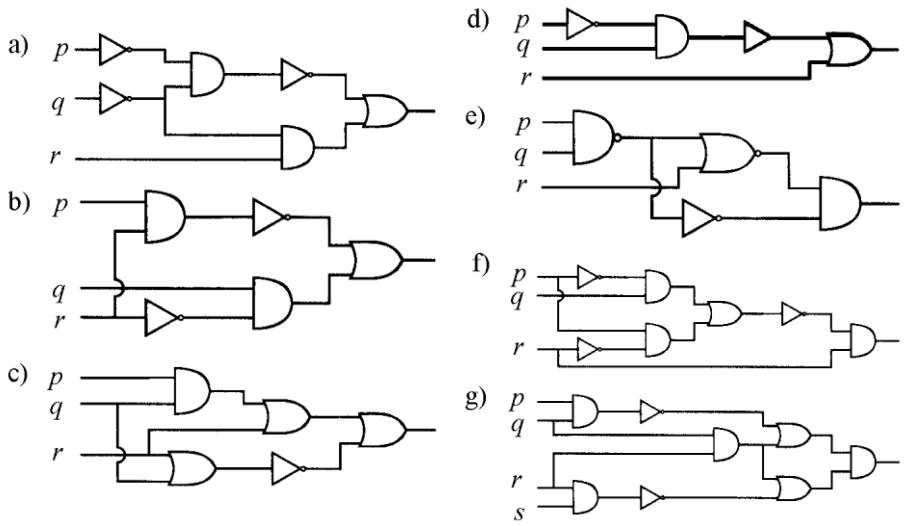
22. Запишете ги следните искази од логичка нотација во нотација на Булова алгебра:

а) $(p \wedge q) \wedge (q \vee \neg r)$ б) $\neg(\neg p \vee (q \wedge \neg r))$

в) $(p \vee q \vee \neg r) \wedge \neg(r \vee \neg q)$ г) $(\neg q \wedge r) \vee \neg(p \wedge r)$

д) $\neg((p \wedge r) \vee \neg q)$ ѓ) $(p \wedge r) \vee (p \wedge \neg q) \wedge (p \vee r \vee \neg s)$

23. Одредете ги Буловите изрази кои соодветствуваат на следниве дијаграми на кола:



24. Направете дијаграми на кола кои соодветствуваат на следниве Булови изрази:

а) $(p'+q)(p+(qr))$ б) $(pq')+((qr')+(p'r))$

в) $(pq')'+(qr)'$ г) $((p+q)r)'$

д) $(p'q+(q'r))'+ps'$ ѓ) $((pq')'+(r's))(p+r')$

25. Одредете ги колата соодветни за секоја од следниве Булови изрази:

а) $(p+q)(q'+pr)$ б) $(ps+qt)(rq+ps)$

в) $(pq+rs)(q+p)$ г) $((pq)(p'q+r))+(r+s)$

26. Дадени се предикатите

$P(x,y,z): x^2+y^2 \geq z^2$ $Q(x,y): y = \frac{x-4}{x+4}$

$R(x,r): |x-1| \leq r$ $S(n,y): y = n!$

Напишете го следниве искази:

а) $P(3,4,5)$ б) $Q(8,2)$

в) $R(3,7)$ г) $S(4,24)$

27. Дадени се предикатите

$P(x,y,z): x^2 + y^2 = z^2$ $Q(x,y):$ ако $x^2 = y^2$, тогаш $x = y$

$R(x): [[x]] = [x]$ $S(a,b,x): a \le x^2 \le b$

Напишете ги следните искази:

а) $P(3,4,5)$ б) $Q(-2,2)$

в) $R(3{,}14,16)$ г) $S(0,4,-3)$

28. За предикатот $Q(x,y,z): x^2 + y^2 \ge z^2$ доменот се состои од множеството на природни броеви. Што може да се каже за вистинитоста на исказите:

а) $\forall x \forall y \exists z\, Q(x,y,z)$ б) $\forall x \exists y \exists z\, Q(x,y,z)$

в) $\exists x \forall y \exists x\, Q(x,y,z)$ г) $\exists x \exists y \exists z\, Q(x,y,z)$

д) $\exists x \exists y \forall z\, Q(x,y,z)$?

29. Докажете дека:

$$\exists x(P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$$

30. Докажете дека од исказот $\forall x P(x) \vee \forall x Q(x)$ може да се изведе дека исказот $\forall x(P(x) \vee Q(x))$ е точен.

31. Докажете дека од исказот $\exists x(P(x) \wedge Q(x))$ може да се изведе дека исказот $\exists x P(x) \wedge \exists x Q(x)$ е точен.

32. Негирајте ги следниве искази:

a) Сите го сакаат Симе.

b) Некои кошаркари не се високи.

c) Сите луѓе се раѓаат.

d) Некои луѓе сакаат грозје.

e) $\exists x$ таков што $x^2 = 9$.

f) $\forall x \exists y$ таков што $x + y = 5$.

g) $\exists x \exists y \forall z \forall n$ $x^n + y = z^n$.

h) $\forall x,\ x \ge 0$.

II ГЛАВА
ЕЛЕМЕНТАРНА ТЕОРИЈА НА БРОЕВИ

1. ПОИМ ЗА ДЕЛИВОСТ

1.1. Познати ни се множествата

$$\mathbf{N}=\{1,2,3,...,n,...\},\ \mathbf{N}_0=\mathbf{N}\cup\{0\}=\{0,1,2,3,...,n,...\} \text{ и}$$
$$\mathbf{Z}=\{...,-4,-3,-2,-1,0,1,2,3,4,...\}.$$

Операциите собирање и множење во овие множества се секогаш изводливи, т.е.

ако $m,n\in\mathbf{N}$, тогаш $m+n\in\mathbf{N}$ и $mn\in\mathbf{N}$;

ако $m,n\in\mathbf{N}_0$, тогаш $m+n\in\mathbf{N}_0$ и $mn\in\mathbf{N}_0$; и

ако $m,n\in\mathbf{Z}$, тогаш $m+n\in\mathbf{Z}$ и $mn\in\mathbf{Z}$.

Понатаму, за одземањето знаеме дека

ако $m,n\in\mathbf{N}$, тогаш $m-n\in\mathbf{N}$ ако и само ако $m>n$;

ако $m,n\in\mathbf{N}_0$, тогаш $m-n\in\mathbf{N}_0$ ако и само ако $m\geq n$; и

ако $m,n\in\mathbf{Z}$, тогаш $m-n\in\mathbf{Z}$.

Останува да ја разгледаме операцијата делење, која не е секогаш изводлива во множествата $\mathbf{N},\mathbf{N}_0$ и $\mathbf{Z}$. Имено, ако m и $n\neq 0$ се природни или цели броеви, тогаш количникот $m:n$ не е секогаш природен или цел број. И токму тоа, прашањето кога бројот m е делив со бројот $n\neq 0$, т.е. прашањето за деливоста во множествата $\mathbf{N},\mathbf{N}_0$ и $\mathbf{Z}$ лежи во основата на теоријата на броевите.

1.2. Дефиниција. За бројот $a\in\mathbf{Z}$ ќе велиме дека е *делив* со бројот $b\in\mathbf{Z}$, $b\neq 0$, ако постои број $q\in\mathbf{Z}$ така што е исполнето равенството $a=bq$. Притоа ќе велиме дека b е *делител* на a, односно дека a е *содржател* на b и ќе пишуваме $b\mid a$.

Ако бројот $b\in\mathbf{Z}$, $b\neq 0$ не е делител на бројот $a\in\mathbf{Z}$, т.е. ако не постои број $q\in\mathbf{Z}$ така што е исполнето равенството $a=bq$, тогаш ќе пишуваме $b\nmid a$.

Ќе велиме дека b е *вистински делител* на a ако $b\mid a$ и $b\neq a$.

1.3. Пример. а) Бидејќи $15=5\cdot 3$, од дефиниција 1.2 следува дека $3\mid 15$ и $5\mid 15$. Според тоа, броевите 1, 3 и 5 се вистински делители на 15.

б) За броевите 17 и 3 имаме $17=5\cdot 3+2$ и бидејќи $5\cdot 3<5\cdot 3+2<6\cdot 3$, заклучуваме дека не постои природен број q таков што $17=3q$ што значи дека $3\nmid 17$.

в) Ќе ги определиме сите делители на броевите 84 и 56. Имаме

$$\frac{1\quad 2\quad 3\quad 4\quad 6\quad 7}{84\quad 42\quad 28\quad 21\quad 14\quad 12} \quad \text{и} \quad \frac{1\quad 2\quad 4\quad 7}{56\quad 28\quad 14\quad 8}.$$

Следствено, сите делители на бројот 84 се: 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 и 84. Притоа за два различни делители чиј производ е еднаков на 84 ќе велиме дека се *заемно комплементарни делители*. Такви се паровите 1 и 84, 2 и 42, 3 и 28, 4 и 21, 6 и 14, 7 и 12.

Повтори ја претходната дискусија за бројот 56. ♦

1.4. Забележуваме дека ако $a,b \in \mathbf{N}$, тогаш и $q \in \mathbf{N}$. Понатаму, ако $b \mid a$, тогаш од $a = bq$ непосредно следуваат равенствата

$$a = (-b)(-q),\ -a = b(-q) \text{ и } -a = (-b)q,$$

од што согласно дефиницијата 1.2 следува дека

$$(-b) \mid a,\ b \mid (-a) \text{ и } (-b) \mid (-a).$$

Претходно изнесеното ни дава за право, при разгледувањето на деливоста, да се ограничиме на ненегативните цели броеви, т.е. на множеството $\mathbf{N}_0$.

Едно од клучните прашања во теоријата на броеви е прашањето за бројот на делителите на даден природен број. На ова прашање ќе се навратиме во натамошните разгледувања, а овде само ќе забележиме дека од равенството $a = a \cdot 1$ непосредно следува дека секој цел број различен од 0 е делив со бројот 1 и со самиот себе, т.е. $1 \mid a$ и $a \mid a$ ако $a \neq 0$. Исто така, од равенството

$$0 = 0 \cdot q, \text{ за секој } q \in \mathbf{N}$$

следува дека бројот 0 има бесконечно многу делители, т.е. $a \mid 0$ ако $a \neq 0$. Да забележиме дека бројот 0 е единствен цел број кој има бесконечно многу делители. Навистина, ако $a \neq 0$ и $b \mid a$, тогаш од дефиниција 1.2 имаме $a = bq$, $a,b,q \in \mathbf{N}$, па затоа

$$a = bq \geq b \cdot 1 = b,$$

што значи дека сите делители на бројот a се помали или еднакви на a и таквите броеви се конечно многу.

1.5. Пример. а) Докажи дека збирот на кои било три последователни природни броеви е делив со бројот 3.

б) Докажи дека збирот на три последователни степени на бројот 2, чии степенови показатели се природни броеви, е делив со бројот 7.

Решение. а) Ако со k го означиме најмалиот од три последователни природни броеви, тогаш другите два броја се броевите $k+1$ и $k+2$. За збирот на овие броеви имаме

$$k + (k+1) + (k+2) = 3k + 3 = 3(k+1),$$

па од дефиниција 1.2 следува $3 \mid [k + (k+1) + (k+2)]$, што и требаше да се докаже.

б) Според условот на задачата имаме дека степеновите показатели се $k, k+1$ и $k+2$, $k \in \mathbf{N}$. Затоа, за бараниот збир имаме:

$$2^k + 2^{k+1} + 2^{k+2} = 2^k + 2 \cdot 2^k + 2^2 \cdot 2^k = 2^k (1 + 2 + 2^2) = 7 \cdot 2^k,$$

што според дефиниција 1.2 значи дека

$$7 \mid (2^k + 2^{k+1} + 2^{k+2}) \,.\ \blacklozenge$$

1.6. Теорема. Нека $a,b \in \mathbf{N}$. Ако $a \mid b$ и $b \mid a$, тогаш $a = b$.

Доказ. Нека $a,b \in \mathbf{N}$, $a \mid b$ и $b \mid a$. Од $a \mid b$ следува дека постои $q \in \mathbf{N}$ таков што $b = aq$, а од $b \mid a$ следува дека постои $p \in \mathbf{N}$ таков што $a = bp$. Понатаму, од равенствата $b = aq$ и $a = bp$ добиваме

$$b = aq = (bp)q = b(pq), \quad \text{т.е.} \quad b = b(pq) \,.$$

Ако последното равенството го поделиме со $b \neq 0$ го добиваме равенството $pq = 1$. Но, $p,q \in \mathbf{N}$ па затоа од последното равенство следува $p = q = 1$. Конечно, $a = bp = b \cdot 1 = b$. $\blacklozenge$

1.7. Теорема. Нека $a,b,c \in \mathbf{N}$. Ако $a \mid b$ и $b \mid c$, тогаш $a \mid c$.

Доказ. Нека $a,b,c \in \mathbf{N}$, $a \mid b$ и $b \mid c$. Од $a \mid b$ следува дека постои $q \in \mathbf{N}$ таков што $b = aq$, а од $b \mid c$ следува дека постои $p \in \mathbf{N}$ таков што $c = bp$. Понатаму, од равенствата $c = bp$ и $b = aq$ следствено добиваме $c = bp = (aq)p = a(qp)$, што според дефиниција 1.2 значи дека $a \mid c$. $\blacklozenge$

1.8. Пример. Докажи дека разликата на бројот $\overline{xabx}$ и бројот запишан со истите цифри, но по обратен редослед е делива со 9.

Решение. За бројот $\overline{xabx}$ имаме

$$\overline{xabx} = 1000x + 100a + 10b + x \,,$$

а за бројот запишан со истите цифри, но по обратен редослед, имаме

$$\overline{xbax} = 1000x + 100b + 10a + x \,.$$

Од последните две равенства наоѓаме

$$\overline{xabx} - \overline{xbax} = 1000x + 100a + 10b + x - (1000x + 100b + 10a + x) = 90(a - b) \,,$$

што значи дека $90 \mid (\overline{xabx} - \overline{xbax})$. Понатаму, од $90 = 9 \cdot 10$ следува $9 \mid 90$ и бидејќи $90 \mid (\overline{xabx} - \overline{xbax})$, од теорема 1.7 следува дека $9 \mid (\overline{xabx} - \overline{xbax})$. $\blacklozenge$

2. ОПШТИ ПРИЗНАЦИ ЗА ДЕЛИВОСТ

2.1. Честопати се јавува потреба да оцениме дали еден број е делив со друг број - без да го извршиме делењето на тие броеви. Притоа ги користиме таканаречените признаци за деливост на природните броеви. Тоа се тврдења преку кои заклучуваме кога еден број е делив со друг број, без да го вршиме делењето.

Познати ни се признаците за деливост на природен број со 2, 3, 4, 5, 8 и 9, за кои во натамошните разгледувања ќе дадеме докази. Во овој дел ќе се задржиме на признаците за деливост на збир, разлика и производ, кои со едно име ги нарекуваме општи признаци за деливост.

2.2. Теорема. Ако $b \mid a$, тогаш $b \mid (ac)$, за секој $c \in \mathbf{N}$.

Доказ. Навистина, ако $b \mid a$, тогаш постои $q \in \mathbf{N}$ таков што $a = bq$. Сега, за секој $c \in \mathbf{N}$ добиваме $ac = (bq)c = b(qc)$. Значи, за бројот $ac \in \mathbf{N}$ постои број $qc \in \mathbf{N}$ таков што $ac = b(qc)$, па од дефиниција 1.2 имаме дека $b \mid (ac)$. ♦

2.3. Пример. Докажи дека $8 \mid (9^8 - 1)$.

Решение. Задачата можеме да ја решиме со пресметување на бројот $9^8 - 1$ и потоа директно да провериме дали $8 \mid (9^8 - 1)$.

Меѓутоа "поелегантно" решение можеме да дадеме со примена на теорема 2.2. Јасно, $8 \mid 8$. Од теорема 2.2 имаме

$$8 \mid 8 \cdot (9^7 + 9^6 + 9^5 + 9^4 + 9^3 + 9^2 + 9 + 1) = (9-1)(9^7 + 9^6 + 9^5 + 9^4 + 9^3 + 9^2 + 9 + 1)$$
$$= 9^8 + 9^7 + 9^6 + 9^5 + 9^4 + 9^3 + 9^2 + 9 - 9^7 - 9^6 - 9^5 - 9^4 - 9^3 - 9^2 - 9 - 1 = 9^8 - 1$$

што и требаше да се докаже. ♦

2.4. Теорема. Нека $a = b + c$ и $d \mid b$. Тогаш $d \mid a$ ако и само ако $d \mid c$.

Доказ. Нека $a = b + c$ и $d \mid b$, т.е. постои q таков што $b = dq$. Ако $d \mid c$, тогаш постои p таков што $c = dp$. Според тоа,

$$a = b + c = dq + dp = d(q + p),$$

што според дефиниција 1.2 значи дека $d \mid a$. Ако $d \mid a$, тогаш постои r таков што $a = dr$. Според тоа,

$$c = a - b = dr - dq = d(r - q),$$

што според дефиниција 1.2 значи дека $d \mid c$. ♦

2.5. Теорема. Ако $a \mid b$ и $a \mid c$, тогаш $a \mid (bx + cy)$ за секои $x, y \in \mathbf{Z}$.

Доказ. Нека $a \mid b$ и $a \mid c$. Од теорема 2.2 имаме дека $a \mid (bx)$ и $a \mid (cy)$ за секои $x, y \in \mathbf{Z}$. Сега од теорема 2.4 следува дека $a \mid (bx + cy)$ за секои $x, y \in \mathbf{Z}$. ♦

2.6. Забелешка. Од теорема 2.5 непосредно следува тврдењето.

Ако $a \mid b$ *и* $a \mid c$, *тогаш* $a \mid (b + c)$ *и* $a \mid (b - c)$.

Навистина, за да докажеме дека $a \mid (b + c)$, доволно е во теорема 2.5 да земеме $x = y = 1$, а за да докажеме дека $a \mid (b - c)$, доволно е да земеме $x = 1$ и $y = -1$. ♦

2.7. Пример. Ако a и b се цели броеви такви што $31|(6a+11b)$, тогаш $31|(a+7b)$. Докажи!

Решение. Од $31|(6a+11b)$ следува дека постои m таков што

$$6a+11b=31m.$$

Но, тоа значи дека

$$30a+55b=5(6a+11b)=5\cdot 31m,$$

т.е. $31|(30a+55b)$. Од друга страна имаме

$31a+62b=31(a+2b)=31n$, т.е. $31|(31a+62b)$.

Конечно, од забелешка 2.6 следува дека

$$31|[31a+62b-(30a+55b)]=a+7b,$$

што и требаше да се докаже. ♦

2.8. Теорема. Ако $m|a$ и $n|b$, тогаш $mn|(ab)$.

Доказ. Од $m|a$ и $n|b$ следува дека постојат p и q такви што $a=mp$ и $b=nq$. Според тоа, $ab=(mp)(nq)=(mn)(pq)$, што значи дека $mn|(ab)$. ♦

2.9. Пример. Докажи дека ако бројот n е делив со броевите 2 и 3, тогаш тој е делив со бројот 6.

Решение. Бидејќи $3|3$ и $2|n$ од теорема 2.8 следува дека $2\cdot 3|3n$, т.е. $6|3n$. Аналогно, $2|2$ и $3|n$, па од теорема 2.8 имаме $2\cdot 3|2n$, т.е. $6|2n$. Конечно, од забелешка 2.6 следува дека $6|(3n-2n)=n$. ♦

2.10. Забелешка. На крајот од овој дел да забележиме дека теорема 2.8 може да се воопшти, т.е. дека важат следниве тврдења, кои ќе ги усвоиме без доказ.

а) Ако $m_1|a_1, m_2|a_2,..., m_k|a_k$, тогаш $m_1m_2...m_k|a_1a_2...a_k$.

б) Ако $m|a$, тогаш $m^k|a^k$, за секој $k\in\mathbf{N}$.

3. ДЕЛЕЊЕ СО ОСТАТОК

3.1. На почетокот рековме дека операцијата делење не е секогаш изводлива во множествата $\mathbf{N}$ и $\mathbf{Z}$. Меѓутоа, знаеме дека во множеството $\mathbf{N}$ за операцијата делење важи таканаречената *теорема за делење со остаток*.

Ако $a,b\in\mathbf{N}$, *тогаш постојат* $q,r\in\mathbf{N}_0$ *такви што*

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

Притоа, како што знаеме, бројот a го нарекуваме *деленик*, b *-делител*, q *-количник* и r *-остаток*.

Така, на пример, за броевите $a=17$ и $b=3$ имаме $17=3\cdot 5+2$, што значи дека $q=5$ и $r=2$, а за броевите $a=342$ и $b=38$ имаме $342=38\cdot 9+0$, што значи дека $q=9$ и $r=0$.

Претходно искажаната теорема за делење со остаток важи и во следниот поопшт облик.

3.2. Теорема (за делење со остаток). За секој $a\in\mathbf{Z}$ и секој $b\in\mathbf{N}$ постојат единствени цели броеви q и r такви што

$$a=bq+r,\quad 0\le r<b. \tag{1}$$

Доказ. Да го разгледаме множеството

$$A=\{...,a-3b,a-2b,a-b,a,a+b,a+2b,a+3b,...\}.$$

Ова множество содржи како негативни така и ненегативни цели броеви. Да го разгледаме множеството B од ненегативни цели броеви кои се содржат во множеството A. Како што знаеме, множеството B има најмал елемент кој е природен број или е еднаков на нула. Нека е тоа бројот $a-qb$ и да го означиме со r. Тогаш важи (1), бидејќи во спротивно, ако $r\ge b$ тогаш бројот $a-(q+1)b$, кој е помал од $a-qb$, ќе биде природен број или еднаков на нула. Со тоа докажавме дека броевите q и r постојат и дека го задоволуваат условот (1).

Ќе докажеме дека броевите q и r се единствени. Да претпоставиме дека за броевите q_1 и r_1 важи

$$a=bq_1+r_1,\quad 0\le r_1<b. \tag{2}$$

Ако од (1) го извадиме (2), добиваме

$$0=b(q-q_1)+(r-r_1). \tag{3}$$

Според тоа, $b\mid(r-r_1)$ и $b\mid(r_1-r)$, при што или $r-r_1\ge 0$ или $r_1-r\ge 0$. Нека $r-r_1\ge 0$. Ако $r-r_1>0$, тогаш од $b\mid(r-r_1)$ и $0<r-r_1<b$ добиваме дека природен број е делив со природен број кој е поголем од него, што не е можно. Значи $r-r_1=0$, т.е. $r=r_1$. Сега, од (3) добиваме $0=b(q-q_1)$ и бидејќи $b\ne 0$ имаме $q-q_1=0$ т.е. $q=q_1$, што значи дека броевите q и r се единствени. ♦

3.3. Забелешка. Од теорема 3.2 непосредно следува дека $b\mid a$ ако и само ако остатокот r од делењето на a со b е 0, т.е. $r=0$.

Количникот q од теоремата 3.2 може да биде кој било цел број, а r е некој број од множеството $\{0,1,...,b-1\}$, кое го нарекуваме *множество на остатоци на бројот* b.

Очигледно, $\{0,1\}$ е множеството на остатоци на бројот 2, бидејќи при делење со 2 се добива остаток 0 или 1. Според тоа, секој цел број можеме да го претставиме во видот

$$2k \text{ или } 2k+1,\quad k\in\mathbf{Z}.$$

Броевите од видот $2k$ ги нарекуваме *парни броеви*, а оние од видот $2k+1$ ги нарекуваме *непарни броеви*.

Слично, при делењето со 3, можни се следниве остатоци: или 0 или 1 или 2, па затоа секој цел број може да се запише во видот:

$$3k \text{ или } 3k+1 \text{ или } 3k+2, \quad k \in \mathbf{Z}.$$

Во првата група (велиме уште и класа), спаѓаат сите цели броеви деливи со 3, во втората се оние кои при делење со 3 даваат остаток 1, а во третата оние кои при делење со 3 даваат остаток 2. Честопати видот $3k+2$ го запишуваме како $3m-1$, бидејќи

$$3k+2 = 3k+3-1 = 3(k+1)-1 = 3m-1.$$

Аналогно, при делењето со 6, можни се следниве остатоци: или 0, или 1, или 2, или 3, или 4, или 5, па затоа секој цел број може да се запише во видот: $6k$, или $6k+1$, или $6k+2$, или $6k+3$, или $6k+4$, или $6k+5$, $k \in \mathbf{Z}$, односно во еден од видовите

$$6k,\ 6k \pm 1,\ 6k \pm 2,\ 6k+3,\ k \in \mathbf{Z}.$$

Ќе решиме неколку задачи користејќи ја теоремата за делење со остаток.

3.4. Пример. а) Најди најголем природен број кој при делење со 31 ќе дава количник 17.

б) При делење на бројот 170 е добиен остаток 11. Со кој број е делено и колкав е соодветниот количник?

в) При делење на бројот 237 е добиен количник 13. Со кој број е делен бројот 237 и кои остатоци се добиваат?

Решение. а) Во случајот се дадени $b=31$ и $q=17$, а се бараат a и r. Бројот a, кој при делење со 31 дава количник 17, можеме да го запишеме во видот

$$a = 31 \cdot 17 + r,\ 0 \le r < 31.$$

Тој ќе биде најголем, ако остатокот r е најголем, т.е. ако $r=30$. Значи

$$a = 31 \cdot 17 + 30 = 557.$$

б) Дадено: $a=170, r=11$; се бараат b и q. Треба да важи

$$170 = bq + 11 \text{ или } bq = 159.$$

Бидејќи $159 = 1 \cdot 159$ и $159 = 3 \cdot 53$, постојат четири можности:

$$b=159, q=1 \text{ или } b=53, q=3 \text{ или } b=3,\ q=53 \text{ или } b=1, q=159.$$

Последните две можности отпаѓаат, бидејќи остатокот треба да биде помал од делителот $(0 \le r < b)$. Затоа задачата има две решенија $b=159, q=1$ и $b=53$, $q=3$.

в) Дадено е $a=237, q=13$; се бараат b и r. Треба да важи

$$237 = 13b + r, \quad 0 \le r < b$$

и оттука заклучуваме дека $237 \geq 13b$ и $237 < 14b$, т.е. $\frac{237}{13} \geq b$ и $\frac{237}{14} < b$. Единствени природни броеви кои ги задоволуваат последните две неравенства се броевите 17 и 18, па затоа

$$b = 17,\ r = 237 - 13 \cdot 17 = 16 \text{ или } b = 18,\ r = 237 - 13 \cdot 18 = 3 .$$ ♦

3.5. Пример. а) Докажи дека збирот на четири последователни природни броеви при делење со 4 дава остаток 2.

б) Природниот број a не е делив со бројот 5. Најди го остатокот кој се добива при делење на бројот a^4 со бројот 5.

Решение. а) Нека $k, k+1, k+2$ и $k+3$ се четири последователни природни броеви. За нивниот збир имаме

$$k + (k+1) + (k+2) + (k+3) = 4(k+1) + 2 .$$

Од теоремата за делење со остаток следува дека остатокот при делење на $4(k+1)+2$ со 4 е единствен и е еднаков на 2.

б) Бројот a кој не е делив со 5 може да се запише како $5k \pm 1$ или $5k \pm 2,\ k \in \mathbf{N}$. Квадратот на ваков број е

$$a^2 = (5k \pm 1)^2 = 25k^2 \pm 10k + 1 = 5(5k^2 \pm 2k) + 1 = 5m + 1$$

или

$$a^2 = (5k \pm 2)^2 = 25k^2 \pm 20k + 4 = 5(5k^2 \pm 4k + 1) - 1 = 5m - 1 .$$

Ако последните две равенства ги квадрираме уште еднаш добиваме

$$a^4 = (5m \pm 1)^2 = 25m^2 \pm 10m + 1 = 5(5m^2 \pm 2m) + 1 = 5n + 1 .$$

Значи, остатокот при делење на бројот a^4 со бројот 5 е 1. ♦

3.6. Теорема. Збирот на природните броеви a и b е делив со природниот број c ако и само ако збирот на остатоците на броевите a и b при делење со бројот c е делив со c.

Доказ. Според теоремата за делење со остаток, за броевите a и b имаме $a = cq_1 + r_1$ и $b = cq_2 + r_2$. Според тоа,

$$a + b = (cq_1 + r_1) + (cq_2 + r_2) = c(q_1 + q_2) + r_1 + r_2 ,$$

што значи дека $a+b$ е делив со c ако и само ако $r_1 + r_2$ е делив со c. ♦

3.7. Пример. Нека $a, b, c \in \mathbf{N}$. Докажи дека $a^2 + b^2 + c^2$ при делење со 8 не може да даде остаток 7.

Решение. Од теоремата за делење со остаток следува дека секој природен број може да се запише во видот $4k, 4k+1, 4k+2$ или $4k+3$, $k \in \mathbf{N}_0$. Во секој од овие случаи квадратот на бројот може да се запише како

$$16k^2 = 8 \cdot 2k^2, \quad 16k^2 + 8k + 1 = 8(2k^2 + k) + 1,$$

$$16k^2+16k+4=8(2k^2+2k)+4,\quad 16k^2+24k+9=8(2k^2+3k+1)+1.$$

Според тоа, квадратот на произволен природен број при делење со 8 може да има остаток 0, 1 или 4. Собирајќи кои било три остатоци од наведениот вид не можеме да добиеме збир 7, па од теоремата 3.6 заклучуваме дека збирот $a^2+b^2+c^2$ при делење со 8 не може да даде остаток 7. ♦

4. ПОСЕБНИ ПРИЗНАЦИ ЗА ДЕЛИВОСТ

4.1. Познати ни се признаците за деливост на природен број со 2, 3, 4, 5, 8 и 9, кои спаѓаат во групата на посебните признаци за деливост. Најчесто посебните признаци за деливост се применуваат без за истите да се даде прецизен доказ. Во овој дел ќе се навратиме на примената на некои посебни признаци, кои и ќе ги докажеме.

Во пример 1.8 го искористивме таканаречениот декаден запис на природен број. Да се потсетиме: секој двоцифрен број $a=\overline{xy}$ можеме да го запишеме во облик $a=10x+y$; секој трицифрен број $b=\overline{xyz}$ можеме да го запишеме во облик $b=100x+10y+z$ итн. Слично, ако природниот број m е составен од $(n+1)-$на цифра, т.е. $m=\overline{a_n a_{n-1}...a_2 a_1 a_0}$, тогаш истиот можеме да го запишеме во развиена форма:

$$m=10^n a_n+10^{n-1}a_{n-1}+...+10^2 a_2+10a_1+a_0. \qquad (1)$$

Така, на пример

$$13245=1\cdot 10^4+3\cdot 10^3+2\cdot 10^2+4\cdot 10+5 \text{ и}$$
$$457245=4\cdot 10^5+5\cdot 10^4+7\cdot 10^3+2\cdot 10^2+4\cdot 10+5.$$

4.2. ***Признак за деливост со 2.*** Природниот број m е делив со 2 ако и само ако цифрата на единиците на бројот m е 0, 2, 4, 6 или 8.

Доказ. Нека бројот m е запишан во развиена форма (1). Броевите 10, $10^2, ..., 10^n$ се деливи со 2, па од теорема 2.5 следува дека бројот

$$10^n a_n+10^{n-1}a_{n-1}+...+10^2 a_2+10a_1$$

е делив со 2. Според тоа, од теорема 2.4 следува дека $2\mid m$ ако и само ако $2\mid a_0$, т.е. ако и само ако цифрата на единиците на бројот m е 0, 2, 4, 6 или 8. ♦

4.3. ***Признак за деливост со 4.*** Природниот број

$$m=10^n a_n+10^{n-1}a_{n-1}+...+10^2 a_2+10a_1+a_0$$

е делив со 4 ако и само ако $4\mid(2a_1+a_0)$.

Доказ. Имаме

$$m = 10^n a_n + \ldots + 10^2 a_2 + 10a_1 + a_0 = (10^n a_n + \ldots + 10^2 a_2 + 8a_1) + (2a_1 + a_0) .$$

Броевите $8, 10^2, 10^3, \ldots, 10^n$ се деливи со 4, па од теорема 2.5 следува дека бројот

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 8a_1$$

е делив со 4. Конечно, од теорема 2.4 следува дека $4 \mid m$ ако и само ако $4 \mid (2a_1 + a_0)$. ♦

4.4. Пример. Која цифра треба да стои на местото на ѕвездичката за бројот 434548*6 да биде делив со 4?

Решение. Од признакот за деливост со 4 следува дека даден број е делив со 4 ако и само ако $4 \mid (2a_1 + 6)$, каде што a_1 е цифрата која стои на местото на ѕвездичката. Со непосредна проверка наоѓаме $a_1 \in \{1, 3, 5, 7, 9\}$. ♦

4.5. ***Признак за деливост со 8.*** Природниот број

$$m = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0$$

е делив со 8 ако и само ако $8 \mid (4a_2 + 2a_1 + a_0)$.

Доказ. Имаме

$$\begin{aligned} m &= 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 \\ &= (10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^3 a_3 + 96a_2 + 8a_1) + (4a_2 + 2a_1 + a_0). \end{aligned}$$

Броевите $8, 96, 10^3, \ldots, 10^n$ се деливи со 8, па од теорема 2.5 следува дека бројот

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^3 a_3 + 96a_2 + 8a_1$$

е делив со 8. Според тоа, од теорема 2.4 следува дека $8 \mid m$ ако и само ако

$$8 \mid (4a_2 + 2a_1 + a_0) . \blacklozenge$$

4.6. Пример. Која цифра треба да стои на местото на ѕвездичката за бројот 4341903*6 да биде делив со 8?

Решение. Од признакот за деливост со 8 следува дека даден број е делив со 8 ако и само ако $8 \mid (4 \cdot 3 + 2a_1 + 6)$, каде што a_1 е цифрата што стои на местото на ѕвездичката. Со непосредна проверка наоѓаме $a_1 \in \{3, 7\}$. ♦

4.7. ***Признак за деливост со 5.*** Природниот број m е делив со 5 ако и само ако цифрата на единиците на бројот m е 0 или 5.

Доказ. Нека бројот m е запишан во развиена форма (1). Броевите

$$10, 10^2, 10^3, \ldots, 10^n$$

се деливи со 5, па од теорема 2.5 следува дека бројот

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1$$

е делив со 5. Конечно, од теорема 2.4 следува дека $5 \mid m$ ако и само ако $5 \mid a_0$, т.е. ако и само ако цифрата на единиците на бројот m е 0 или 5. ♦

4.8. Пример. Докажете дека бројот n^2+n+1 не е делив со 5 за ниту еден природен број n.

Решение. Според признакот за деливост со бројот 5, доволно е да докажеме дека за секој природен број n цифрата на единиците на бројот n^2+n+1 е различна од 0 и 5. За таа цел ќе ја составиме следнава табела:

број	цифра на единици									
n	0	1	2	3	4	5	6	7	8	9
n^2	0	1	4	9	6	5	6	9	4	1
n^2+n+1	1	3	7	3	1	1	3	7	3	1

од каде што гледаме дека за секој природен број n, бројот n^2+n+1 завршува на една од цифрите 1, 3 или 7, што значи дека тој не е делив со 5. ♦

4.9. ***Признак за деливост со 9.*** Природниот број

$$m = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0$$

е делив со 9 ако и само ако $9 \mid (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0)$.

Доказ. Имаме:

$$\begin{aligned} m &= 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 \\ &= (10^n - 1)a_n + \ldots + (10^2 - 1)a_2 + (10-1)a_1 + (a_n + a_{n-1} + \ldots + a_1 + a_0) \\ &= \underbrace{99..99}_{n \text{ devet.}} a_n + \underbrace{99..99}_{n-1 \text{ devet.}} a_{n-1} + \ldots + 99a_2 + 9a_1 + (a_n + a_{n-1} + \ldots + a_1 + a_0) \\ &= 9 \cdot (\underbrace{11..11}_{n \text{ edin.}} a_n + \underbrace{11..11}_{n-1 \text{ edin.}} a_{n-1} + \ldots + 11a_2 + a_1) + (a_n + a_{n-1} + \ldots + a_1 + a_0). \end{aligned}$$

Конечно, бројот m го запишавме како збир на два броја од кои едниот е делив со 9, па затоа $9 \mid m$ ако и само ако

$$9 \mid (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0). \blacklozenge$$

4.10. ***Признак за деливост со 3.*** Природниот број

$$m = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0$$

е делив со 3 ако и само ако $3 \mid (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0)$.

Доказ. Имаме:

$$\begin{aligned} m &= 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 \\ &= 9 \cdot (\underbrace{11..11}_{n \text{ edin.}} a_n + \underbrace{11..11}_{n-1 \text{ edin.}} a_{n-1} + \ldots + 11a_2 + a_1) + (a_n + a_{n-1} + \ldots + a_1 + a_0). \end{aligned}$$

Конечно, бројот m го запишавме како збир на два броја од кои едниот е делив со 9, што значи и со бројот 3, па затоа $3 \mid m$ ако и само ако

$$3 \mid (a_n + a_{n-1} + ... + a_2 + a_1 + a_0) . \blacklozenge$$

4.11. Пример. Која цифра треба да стои на местото на ѕвездичката за бројот 92357*46 да биде делив со 3, а која за бројот да биде делив со 9?

Решение. Од признакот за деливост со 3 следува дека бројот 92357*46 е делив со 3 ако и само ако збирот

$$9 + 2 + 3 + 5 + 7 + a_2 + 4 + 6 = 36 + a_2$$

е делив со 3, каде што a_2 е цифрата која стои на местото на ѕвездичката. Но, $3 \mid 36$, па затоа треба $3 \mid a_2$, од што следува дека $a_2 \in \{0, 3, 6, 9\}$.

Аналогно, од признакот за деливост со 9 следува дека бројот 92357*46 е делив со 9 ако и само ако збирот

$$9 + 2 + 3 + 5 + 7 + a_2 + 4 + 6 = 36 + a_2$$

е делив со 9, каде што a_2 е цифрата која стои на местото на ѕвездичката. Но, $9 \mid 36$ па затоа треба $9 \mid a_2$, од што следува $a_2 \in \{0, 9\}$. ♦

4.12. Пример. Даден е природен број n, кој е запишан со 60 цифри седумки и одреден број нули. Докажи дека вредноста на дропката $\frac{n-27}{3}$ е цел број, но вредноста на дропката $\frac{n-27}{9}$ не е цел број!

Решение. Збирот на цифрите на бројот n е $60 \cdot 7 = 420$, што според признакот за деливост со 3 значи дека $3 \mid n$. Но, $3 \mid 27$, па затоа $3 \mid (n-27)$, што значи дека вредноста на дропката $\frac{n-27}{3}$ е цел број.

Јасно, $9 \mid 27$ и $9 \nmid n$, па затоа $9 \nmid (n-27)$, т.е. вредноста на дропката $\frac{n-27}{3}$ не е цел број. ♦

5. НАЈГОЛЕМ ЗАЕДНИЧКИ ДЕЛИТЕЛ

5.1. За бројот 24 имаме $24 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 3$. Очигледно, броевите 1, 2, 3, 4, 6, 8, 12 и 24 се делители на бројот 24. Забележуваме дека сите делители на 24 се помали или еднакви на 24 и нив ги има конечно многу. Последното важи за секој природен број. Имено, делителите на секој природен број a се помали или еднакви на бројот a, па затоа секој природен број, а со тоа и секој цел број различен од нула, има конечно многу делители.

5.2. Дефиниција. Нека $a, b \in \mathbf{N}$. За бројот d ќе велиме дека е *заеднички делител* на броевите a и b ако $d \mid a$ и $d \mid b$.

Нека $d_1, d_2, ..., d_k$ се заеднички делители на a и b, и d е најголемиот меѓу броевите $d_1, d_2, ..., d_k$, во ознака $d = \max\{d_1, d_2, ..., d_k\}$. За бројот d ќе велиме дека е *најголем заеднички делител* на a и b.

За најголемиот заеднички делител на броевите a и b најчесто се користат ознаките (a,b) или $\mathrm{NZD}(a,b)$. Ние ќе ја користиме ознаката $\mathrm{NZD}(a,b)$.

За бројот d ќе велиме дека е заеднички делител на броевите $a_1, a_2, ..., a_n$ ако $d \mid a_1, d \mid a_2, ..., d \mid a_n$.

Нека $d_1, d_2, ..., d_k$ се заеднички делители на $a_1, a_2, ..., a_n$. Бројот $d = \max\{d_1, ..., d_k\}$ го нарекуваме *најголем заеднички делител* на $a_1, a_2, ..., a_n$ и ќе го означуваме со $\mathrm{NZD}(a_1, a_2, ..., a_n)$.

5.3. Забелешка. Како што рековме, множеството делители на природниот број a е конечно и бидејќи тоа ги содржи заедничките делители на броевите a и b, добиваме дека множеството $d_1, d_2, ..., d_k$ од заедничките делители на a и b е конечно. Но, тоа не е празно, бројот 1 е заеднички делител на a и b, па затоа истото има најголем елемент. Според тоа, за секои два природни броја a и b може да се најде $\mathrm{NZD}(a,b)$. Од наполно исти причини е јасно дека за секои n природни броеви $a_1, a_2, ..., a_n$ може да се најде $\mathrm{NZD}(a_1, a_2, ..., a_n)$.

Од досега изнесеното е јасно дека за да го најдеме најголемиот заеднички делител на броевите a и b, доволно е да ги определиме сите делители на a и сите делители на b и потоа меѓу нивните заеднички делители да го земеме најголемиот број. Јасно, ваквата постапка секогаш дава резултати, но не е секогаш ефективна. Имено, ако броевите a и b се мали тогаш сè е во ред, но ако станува збор за големи броеви, тогаш може да имаме сериозни тешкотии. Така, на пример, ако $a = 24$ и $b = 56$, тогаш лесно се гледа дека делители на 24 се 1, 2, 3, 4, 6, 8, 12 и 24, а делители на 56 се 1, 2, 4, 7, 8, 14, 28 и 56, па затоа $\mathrm{NZD}(24,56) = 8$. Меѓутоа, ако $a = 1728$ и $b = 1764$, тогаш потребен е голем број пресметувања за да со претходната постапка се констатира дека $\mathrm{NZD}(1728,1764) = 36$. Токму затоа, во овој дел ќе дадеме неколку теореми со чија помош ќе можеме полесно да наоѓаме NZD.

5.4. Теорема. Ако $a = bq$, тогаш $\mathrm{NZD}(a,b) = b$.

Доказ. Од $a = bq$ следува дека $b \mid a$ и бидејќи $b \mid b$, добиваме дека b е заеднички делител на a и b. Понатаму, бидејќи $\mathrm{NZD}(a,b) \le b$ и b е заеднички делител на a и b, добиваме дека $\mathrm{NZD}(a,b) = b$. ♦

5.5. Теорема. а) Ако $b < a$, тогаш $\mathrm{NZD}(a,b) = \mathrm{NZD}(b, a-b)$.

б) За секои $a, b \in \mathbf{N}$ важи $\mathrm{NZD}(a,b) = \mathrm{NZD}(a, a+b)$.

Доказ. а) Од теорема 2.4 имаме: ако $d \mid a$, тогаш $d \mid b$ ако и само ако $d \mid (a-b)$. Според тоа, секој заеднички делител на a и b е заеднички делител и на b и $a-b$ и, обратно, секој заеднички делител на b и $a-b$ е заеднички делител и на a и b, па затоа $\mathrm{NZD}(a,b) = \mathrm{NZD}(b, a-b)$.

б) Од тврдењето под а) имаме:

$$\text{NZD}(a, a+b) = \text{NZD}(a, a+b-a) = \text{NZD}(a, b)\,.\blacklozenge$$

5.6. Пример. а) Најди $\text{NZD}(484, 396)$.

б) Најди го најголемиот природен број за кој при делење на броевите 845 и 275 со него, и во двата случаи се добива остаток 5.

Решение. а) Од теорема 5.5 а) следува:

$$\text{NZD}(484,396) = \text{NZD}(396, 484-396) = \text{NZD}(396,88) = \text{NZD}(88, 396-88)$$
$$= \text{NZD}(88,308) = \text{NZD}(88, 308-88) = \text{NZD}(88,220) = \text{NZD}(88, 220-88)$$
$$= \text{NZD}(88,132) = \text{NZD}(88, 132-88) = \text{NZD}(88,44) = 44.$$

Последното равенство следува од теорема 5.4 бидејќи $88 = 2 \cdot 44$.

б) Бараниот број е заеднички делител на $845-5=840$ и $275-5=270$. Според тоа, треба да најдеме $\text{NZD}(840, 270)$. Од теоремата 5.5 а) имаме:

$$\text{NZD}(840,270) = \text{NZD}(270, 840-270) = \text{NZD}(270,570) = \text{NZD}(270, 570-270)$$
$$= \text{NZD}(270,300) = \text{NZD}(270, 300-270) = \text{NZD}(270,30)$$

и бидејќи $30 \mid 270$ од последното равенство и од теорема 5.4 добиваме

$$\text{NZD}(840,270) = \text{NZD}(270,30) = 30\,.$$

Значи, најголемиот број со бараното својство е 30. Притоа

$$845 = 30 \cdot 28 + 5 \text{ и } 275 = 30 \cdot 9 + 5\,.\blacklozenge$$

5.7. Во претходните разгледувања видовме дека

$$\text{NZD}(24,56) = 8 \text{ и } \text{NZD}(840,270) = 30\,.$$

Забележуваме дека и во двата случаја најголемиот заеднички делител е поголем од 1. Меѓутоа, делители на бројот 10 се 1, 2, 5 и 10, а делители на бројот 3 се 1 и 3, па затоа $\text{NZD}(10,3) = 1$. Постојат бројни примери во кои најголемиот заеднички делител на два броја е 1 и ваквите парови природни броеви се од посебна важност во теоријата на броеви, па затоа и посебно ќе ги разгледаме.

5.8. Дефиниција. За природните броеви a и b ќе велиме дека се *заемно прости* ако $\text{NZD}(a,b) = 1$.

За броевите $a_1, a_2, ..., a_n$ ќе велиме дека се *заемно прости во целина* ако $\text{NZD}(a_1, a_2, ..., a_n) = 1$.

За броевите $a_1, a_2, ..., a_n$ ќе велиме дека се *заемно прости по парови* ако $\text{NZD}(a_i, a_j) = 1$, за $i \neq j$, т.е. секои два броја се заемно прости.

Јасно, ако броевите $a_1, a_2, ..., a_n$ се заемно прости по парови, тогаш тие се заемно прости во целина. Меѓутоа, обратното не важи. Имено, за броевите 6, 15 и 35 имаме $\text{NZD}(6,15,35) = 1$, т.е. тие се заемно прости во целина, но не се заемно прости по парови бидејќи $\text{NZD}(6,15) = 3$ и $\text{NZD}(15,35) = 5$.

5.9. Пример. а) Докажи дека броевите 77 и 96 се заемно прости.

б) Докажи дека броевите $n, n+1$ и $2n+1$ се заемно прости по парови.

Решение. а) Имаме:

$$\begin{aligned}\text{NZD}(96,77) &= \text{NZD}(77,96-77) = \text{NZD}(77,19) = \text{NZD}(19,77-19)\\ &= \text{NZD}(19,58) = \text{NZD}(19,58-19) = \text{NZD}(19,39)\\ &= \text{NZD}(19,39-19) = \text{NZD}(19,20) = \text{NZD}(19,20-19) = 1,\end{aligned}$$

што значи дека броевите 77 и 96 се заемно прости.

б) Од теоремата 5.5 а) следува

$$\text{NZD}(n+1,n) = \text{NZD}(n,n+1-n) = \text{NZD}(n,1) = 1,$$

што значи дека броевите n и $n+1$ се заемно прости. Сега, од теорема 5.5 б) имаме

$$1 = \text{NZD}(n+1,n) = \text{NZD}(n+1,n+1+n) = \text{NZD}(n+1,2n+1),$$

т.е. $n+1$ и $2n+1$ се заемно прости. Конечно, од теорема 5.5 а) и од претходното равенство имаме:

$$\text{NZD}(2n+1,n) = \text{NZD}(2n+1,2n+1-n) = \text{NZD}(2n+1,n+1) = 1,$$

т.е. n и $2n+1$ се заемно прости. ♦

5.10. Теорема. Ако $\text{NZD}(a,b) = d$, $a = dx$ и $b = dy$, тогаш $\text{NZD}(x,y) = 1$.

Доказ. Да претпоставиме дека $\text{NZD}(x,y) = k > 1$. Тогаш постојат природни броеви x_1 и y_1 такви што $x = kx_1$ и $y = ky_1$. Од $a = dx$ и $b = dy$ добиваме $a = d(kx_1) = (kd)x_1$ и $b = d(ky_1) = (dk)y_1$. Според тоа $dk \mid a$ и $dk \mid b$. Значи, бројот dk е заеднички делител на a и b поголем од d, што не е можно бидејќи $\text{NZD}(a,b) = d$.

Од добиената противречност следува дека $k = 1$, т.е $\text{NZD}(x,y) = 1$. ♦

5.11. Пример. Збирот на два природни броја е 252, а нивниот најголем заеднички делител е 36. Кои се тие броеви?

Решение. Нека бараните броеви се a и b. Од условот на задачата имаме $a+b = 252$, $a = 36x$ и $b = 36y$, при што $\text{NZD}(x,y) = 1$. Според тоа,

$$36x + 36y = 252, \text{ т.е. } x + y = 7.$$

Во последното равенство ставаме $x \in \{1,2,3,4,5,6\}$ и добиваме

$$(x,y) \in \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}.$$

Конечно, со замена во равенствата $a = 36x$ и $b = 36y$ наоѓаме

$$(a,b) \in \{(36,216),(72,180),(108,144),(144,108),(180,72),(216,36)\}. \blacklozenge$$

6. ЕВКЛИДОВ АЛГОРИТАМ

6.1. Во следните неколку теореми ќе разработиме алгоритам за наоѓање на NZD. Притоа ќе ја користиме теоремата за делење со остаток, со чија помош ќе го докажеме таканаречениот *Евклидов алгоритам.*

6.2. Теорема. Ако $a = bq + r$, тогаш $\text{NZD}(a,b) = \text{NZD}(b,r)$.

Доказ. Ако $\text{NZD}(a,b) = d$, тогаш постојат x и y такви што $a = dx$ и $b = dy$. Значи, $dx = dyq + r$, па од теорема 2.4 следува $d \mid r$ и бидејќи $d \mid b$ заклучуваме дека $d \mid \text{NZD}(b,r)$.

Јасно, $d = \text{NZD}(b,r)$, бидејќи ако $d < \text{NZD}(b,r) = d_1$, тогаш според теорема 2.4, од равенството $a = bq + r$ следува $d_1 \mid a$ и бидејќи $d_1 \mid b$, добиваме дека постои заеднички делител на a и b кој е поголем од d, што е противречност. ♦

6.3. Ќе докажеме како со помош на теоремата за делење со остаток и претходната теорема може да се конструира таканаречениот Евклидов алгоритам за наоѓање на НЗД на два броја a и b. Имаме

$$\begin{array}{ll} a = bq_1 + r_1 & 0 \le r_1 < b \\ b = r_1q_2 + r_2 & 0 \le r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 \le r_3 < r_2 \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ r_{k-2} = r_{k-1}q_k + r_k & 0 \le r_k < r_{k-1} \\ r_{k-1} = r_kq_{k+1} + r_{k+1} & 0 \le r_{k+1} < r_k \\ \ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \end{array} \qquad (1)$$

Бидејќи остатоците r_i опаѓаат со секој следен чекор, т.е.

$$r_1 > r_2 > r_3 > \ldots > r_k > r_{k+1} > \ldots$$

постапката дефинирана со равенствата (1) ќе заврши по конечен број чекори, т.е. после конечен број чекори ќе добиеме равенство од вид $r_{n-1} = r_nq_{n+1} + 0$, т.е. $r_{n+1} = 0$, при што $r_n \neq 0$. Од равенството $r_{n-1} = r_nq_{n+1}$ следува $r_n \mid r_{n-1}$. Претходно кажаното и теорема 6.2 ни овозможуваат да ја докажеме следнава теорема.

6.4. Теорема. Последниот остаток r_n различен од нула, добиен со низата равенства (1) е еднаков на најголемиот заеднички делител на броевите a и b.

Доказ. Ако ги земеме предвид равенствата (1), тогаш од теоремата 6.2 непосредно ја добиваме следнава низа равенства

$$\text{NZD}(a,b) = \text{NZD}(b,r_1) = \text{NZD}(r_1,r_2) = \text{NZD}(r_2,r_3) = \ldots = \text{NZD}(r_{n-1},r_n).$$

Но, $r_n \mid r_{n-1}$ што според теорема 5.4 значи дека

$$\text{NZD}(r_{n-1},r_n) = r_n.$$

Конечно, од последните две равенства наоѓаме

$$\text{NZD}(a,b) = \text{NZD}(r_{n-1}, r_n) = r_n \ . \ \blacklozenge$$

6.5. Пример. Најди $\text{NZD}(426,312)$.

Решение. Ќе го искористиме Евклидовиот алгоритам. Имаме

$$426 = 312\cdot 1 + 114 \ ; \ 312 = 114\cdot 2 + 84 \ ; \ 114 = 84\cdot 1 + 30 \ ,$$
$$84 = 30\cdot 2 + 24 \ ; \ 30 = 24\cdot 1 + 6 \ \text{ и } \ 24 = 6\cdot 4$$

што значи $\text{NZD}(426,312) = 6$. ♦

6.6. Теорема. Ако $d = \text{NZD}(a,b)$, тогаш постојат цели броеви x и y такви што

$$d = ax + by \ .$$

Доказ. Според теоремата 6.4, во системот равенства (1) на Евклидовиот алгоритам важи $d = r_n = \text{NZD}(a,b)$, каде што r_n е последниот остаток различен од нула. Равенствата (1) ги запишуваме во видот:

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2} \\ r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3} \\ &\ldots\ldots\ldots\ldots \\ r_2 &= b - r_1 q_2 \\ r_1 &= a - b q_1 \end{aligned} \qquad (2)$$

Сега, ако во првото равенство на (2) од второто равенство замениме за r_{n-1}, потоа од третото равенство во (2) во новодобиеното равенство замениме за r_{n-2}, па во секое новодобиено равенство последователно замениме за $r_{n-3}, \ldots, r_3, r_2$ и r_1, добиваме равенство од вид $d = ax + by$. ♦

6.7. Да забележиме дека броевите x и y во претходната теорема се заемно прости, т.е. $\text{NZD}(x, y) = 1$.

Навистина, ако претпоставиме дека $\text{NZD}(x, y) = k > 1$, тогаш постојат $x_1, y_1 \in \mathbf{N}$ такви што $x = kx_1$ и $y = ky_1$. Слично, од $d = \text{NZD}(a,b)$ следува дека постојат $a_1, b_1 \in \mathbf{N}$ такви што $a = da_1$ и $b = db_1$. Ако замениме во равенството $d = ax + by,$ добиваме

$$d = (da_1)(kx_1) + (db_1)(ky_1) = kd(a_1x_1 + b_1y_1) \ ,$$

т.е. $kd \mid d$, што не е можно бидејќи $kd > d$. Од добиената противречност следува дека $\text{NZD}(x, y) = 1$.

Понатаму, ако $d = \text{NZD}(a,b)$, тогаш броевите x и y во равенството $d = ax + by$ не се еднозначно определени. Така, на пример, $\text{NZD}(8,12) = 4$ и $4 = 3\cdot 12 - 4\cdot 8 = 5\cdot 12 - 7\cdot 8$.

6.8. Пример. Запиши го $\text{NZD}(426,312)=6$ во вид

$$6=426x+312y\,.$$

Решение. Од пример 6.5 и од теорема 6.6 следува:

$$\begin{aligned}6&=30-24=30-(84-2\cdot 30)=3\cdot 30-84=3(114-84)-84=3\cdot 114-4\cdot 84\\&=3\cdot 114-4(312-2\cdot 114)=11\cdot 114-4\cdot 312=11(426-312)-4\cdot 312\\&=11\cdot 426-15\cdot 312,\end{aligned}$$

т.е. $\text{NZD}(426,312)=426\cdot 11-312\cdot 15$. ♦

6.9. Пример. Докажи дека целите броеви m и n се заемно прости ако и само ако постојат цели броеви x и y такви што

$$mx+ny=1. \tag{3}$$

Решение. Нека m и n се заемно прости т.е. $\text{NZD}(m,n)=1$. Тогаш, од теорема 6.6 следува дека постојат цели броеви x и y такви што $mx+ny=1$, т.е. важи (3).

Да претпоставиме дека за броевите m и n постојат цели броеви x и y такви што важи равенството (3). Ако $d\mid m$ и $d\mid n$, тогаш $d\mid(ma+nb)$, за секои цели броеви a и b. Земаме $a=x$ и $b=y$ и добиваме дека $d\mid(mx+ny)$, т.е. $d\mid 1$, а тоа е можно само ако $d=1$, што значи дека m и n се заемно прости. ♦

6.10. Теорема. а) Ако $c\mid a$ и $c\mid b$, тогаш $c\mid\text{NZD}(a,b)$.

б) Ако $d\mid a, d\mid b$ и $d=ax+by$, за некои цели броеви x и y, тогаш $d=\text{NZD}(a,b)$.

Доказ. а) Од теорема 6.6 следува дека постојат цели броеви x и y такви, што $\text{NZD}(a,b)=ax+by$. Понатаму, од $c\mid a$ имаме $a=cm$ за некој цел број m, а од $c\mid b$ следува $b=cn$ за некој цел број n. Заменуваме во равенството $\text{NZD}(a,b)=ax+by$ и добиваме

$$\text{NZD}(a,b)=ax+by=(cm)x+(cn)y=c(mx+ny)\,,$$

што значи $c\mid\text{NZD}(a,b)$.

б) Да претпоставиме дека $d\mid a, d\mid b$ и $d=ax+by$, за некои цели броеви x и y. Од тврдењето под а) следува дека $d\mid\text{NZD}(a,b)$. Понатаму, постојат $a_1,b_1\in\mathbf{N}$ такви што $a=a_1\cdot\text{NZD}(a,b)$ и $b=b_1\cdot\text{NZD}(a,b)$. Ако замениме во $d=ax+by$, добиваме

$$d=[a_1\cdot\text{NZD}(a,b)]x+[b_1\cdot\text{NZD}(a,b)]y=\text{NZD}(a,b)\cdot(a_1x+b_1y)$$

што значи $\text{NZD}(a,b)\mid d$.

Конечно, од $d\mid\text{NZD}(a,b)$ и $\text{NZD}(a,b)\mid d$ следува $d=\text{NZD}(a,b)$. ♦

6.11. Теорема. Ако $k > 0$, тогаш $\text{NZD}(ka, kb) = k \cdot \text{NZD}(a, b)$.

Доказ. Нека $d = \text{NZD}(a, b)$. Според тоа, $d \mid a$ и $d \mid b$ и постојат постојат x и y такви што $d = ax + by$. Но, тоа значи дека $kd \mid ka$, $kd \mid kb$ и постојат x и y такви што

$$kd = k(ax + by) = (ka)x + (kb)y .$$

Сега, од теорема 6.10 б) следува дека

$$\text{NZD}(ka, kb) = kd = k \cdot \text{NZD}(a, b) . \blacklozenge$$

6.12. Пример. Најди $\text{NZD}(765, 1080)$.

Решение. Дадените броеви завршуваат на 5 и 0, па од признакот за деливост со 5 следува дека $5 \mid 765$ и $5 \mid 1080$. Имаме, $765 = 5 \cdot 153$ и $1080 = 5 \cdot 216$, па затоа

$$\text{NZD}(765, 1080) = 5 \cdot \text{NZD}(153, 216) .$$

Збирот на цифрите на броевите 153 и 216 е еднаков на 9, па од признакот за деливост со 9 следува дека и двата броја се деливи со 9. Имаме, $153 = 9 \cdot 17$ и $216 = 9 \cdot 24$, па затоа

$$\begin{aligned} \text{NZD}(765, 1080) &= 5 \cdot \text{NZD}(153, 216) = 5 \cdot 9 \cdot \text{NZD}(17, 24) = 45 \cdot \text{NZD}(17, 7) \\ &= 45 \cdot \text{NZD}(7, 10) = 45 \cdot \text{NZD}(7, 3) = 45 \cdot \text{NZD}(3, 4) = 45 . \blacklozenge \end{aligned}$$

6.13. Теорема. а) Ако $q \mid ab$ и $\text{NZD}(q, b) = 1$, тогаш $q \mid a$.

б) Ако $q \mid a$, $p \mid a$ и $\text{NZD}(q, p) = 1$, тогаш $qp \mid a$.

Доказ. а) Според теорема 6.6, од $\text{NZD}(q, b) = 1$ следува дека постојат цели броеви m и n такви што $1 = bm + qn$. Ако последното равенство го помножиме со a, добиваме дека постојат цели броеви m и n такви што

$$a = abm + qan . \tag{4}$$

Од условот на теоремата имаме дека $q \mid ab$, т.е. постои природен број k таков што $ab = qk$. Со замена во равенството (4), добиваме

$$a = (qk)m + qan = q(km + an) .$$

Конечно, од последното равенство следува дека $q \mid a$.

б) Од $q \mid a$ и $p \mid a$ следува дека $a = qm$ и $a = pn$ за некои $m, n \in \mathbf{N}$. Според тоа, $qm = pn$ па затоа $q \mid pn$. Но, $\text{NZD}(q, p) = 1$ и бидејќи $q \mid pn$, од тврдењето под а) следува $q \mid n$, што значи дека постои $k \in \mathbf{N}$ таков што $n = qk$. Конечно, $a = pn = p(qk) = (pq)k$, од што следува дека $pq \mid a$. $\blacklozenge$

6.14. Пример. Најди ги сите природни броеви n за кои бројот $10^n + 8$ е делив со 72!

Решение. Бидејќи збирот на цифрите на бројот $10^n+8=10...08$ е еднаков на 9, заклучуваме дека $9\mid(10^n+8)$ за секој природен број n. Понатаму, од признакот за деливост со 8, имаме дека $8\mid(10^n+8)$ ако и само ако $8\mid(4a_2+2a_1+a_0)$. За $n=1$ и $n=2$ имаме

$$10^n+8=18 \text{ и } 10^n+8=108$$

и овие броеви не се деливи со 8. Ако $n\geq 3$, тогаш $a_2=a_1=0$ и $a_0=8$, па затоа $8\mid(4a_2+2a_1+a_0)$. Според тоа, за $n\geq 3$ имаме $8\mid(10^n+8)$.

Конечно, од претходно изнесеното и од фактот дека $\text{NZD}(8,9)=1$, со примена на теорема 6.13 б) добиваме дека $72\mid(10^n+8)$ за $n\geq 3$. ♦

6.15. Пример. Докажи дека од $7\mid\overline{abb}$ следува $7\mid(a+2b)$.

Решение. Имаме

$$\overline{abb}=100a+10b+b=98a+7b+2a+4b=7(14a+b)+2(a+b+b).$$

Понатаму, левата страна на последното равенство е делива со 7 и првиот собирок на десната страна е делив со 7, па затоа и вториот собирок е делив со 7, т.е. $7\mid 2(a+2b)$. Но, $\text{NZD}(7,2)=1$, па од теоремата 6.13 а) следува дека $7\mid(a+2b)$, што и требаше да се докаже. ♦

7. НАЈМАЛ ЗАЕДНИЧКИ СОДРЖАТЕЛ

7.1. При воведувањето на поимот за деливост рековме дека ако $a\mid b$, тогаш за бројот b велиме дека е содржател на бројот a. Јасно, ако b е содржател на a, тогаш и броевите $2b, 3b, 4b, ...$ се содржатели на бројот a. Така, на пример:

- содржатели на бројот 9 се:

  9, 18, 27, **36**, 45, 54, 63, **72**, 81, 90, 99, **108**, 117, 126, ...

- содржатели на бројот 12 се:

  12, 24, **36**, 48, 60, **72**, 84, 96, **108**, 120, 132, 144, ...

Како што можеме да забележиме, броевите 36, 72, 108 ... се заеднички содржатели на броевите 9 и 12. Претходно изнесеното е причина за следната дефиниција.

7.2. Дефиниција. Нека $a,b\in\mathbf{N}$. За бројот $c\in\mathbf{N}$ ќе велиме дека е *заеднички содржател* на a и b ако $a\mid c$ и $b\mid c$.

7.3. Од дефиниција 7.2 непосредно следува дека за секои $a,b\in\mathbf{N}$, броевите од видот $kab, k\in\mathbf{N}$ се заеднички содржатели на a и b. Според тоа, за секои a и b множеството од нивни заеднички содржатели е бесконечно, па затоа исто-

то нема најголем елемент. Природно е да се запрашаме дали меѓу заедничките содржатели на a и b постои најмал содржател. Одговорот на ова прашање е потврден. Навистина, бројот $c_1 = ab$ е заеднички содржател на a и b. Ако тој не е најмал, тогаш постои природен број c_2 таков што $c_2 < c_1$ и $a \mid c_2$ и $b \mid c_2$. Ако c_2 не е најмал меѓу заедничките содржатели на a и b, тогаш постои заеднички содржател c_3 на a и b таков што $c_3 < c_2$. Бидејќи природните броеви $c_1, c_2, c_3, \ldots$ се намалуваат, по конечен број чекори ќе најдеме најмал природен број c за кој важи $a \mid c$ и $b \mid c$. Јасно, ова е *најмалиот заеднички содржател* на a и b и него ќе го означуваме со $c = \text{NZS}(a,b)$. Да забележиме дека во литературата за најмалиот заеднички содржател на броевите a и b се користи и ознаката $[a,b]$.

Како што видовме, за да го определиме најмалиот заеднички содржател на два броја a и b доволно е последователно да ги испишеме содржателите на едниот и другиот број и потоа меѓу нив да го најдеме најмалиот заеднички содржател, кој сигурно е помал или еднаков на ab. Но оваа постапка може да биде долга, па затоа ќе докажеме неколку својства за најмалиот заеднички содржател.

7.4. Теорема. Ако $\text{NZS}(a,b) = s$ и S е заеднички содржател на a и b, тогаш $s \mid S$.

Доказ. Од теоремата за делење со остаток следува дека постојат q и r такви што $S = sq + r, \quad 0 \le r < s$. Ако $r \neq 0$, тогаш од $a \mid S$, $a \mid s$ и од претходното равенство следува дека $a \mid r$. Слично $b \mid r$, што значи дека најдовме заеднички содржател на a и b кој е помал од s. Последното му противречи на фактот дека $\text{NZS}(a,b) = s$. Од добиената противречност следува $r = 0$, т.е. $s \mid S$. ♦

7.5. Теорема. Ако $\text{NZD}(a,b) = 1$, тогаш $\text{NZS}(a,b) = ab$.

Доказ. Нека $\text{NZS}(a,b) = s \le ab$. Тогаш, $s = am$, за некој $m \in \mathbf{N}$. Според тоа, $b \mid am$ и бидејќи $\text{NZD}(a,b) = 1$, од теорема 6.13 а) следува дека $b \mid m$, т.е. $m = bn$, за некој $n \in \mathbf{N}$. Од досега изнесеното имаме $s = am = a(bn) = (ab)n$ и бидејќи $s \le ab$, од последното равенство следува $n = 1$, што значи дека $s = ab$, т.е. $\text{NZS}(a,b) = ab$. ♦

7.6. Пример. Најди:

а) $\text{NZS}(20,31)$ и

б) $\text{NZS}(n, 2n+1)$, $n \in \mathbf{N}$.

Решение. а) Имаме

$$\text{NZD}(20,31) = \text{NZD}(20,31-20) = \text{NZD}(20,11) = \text{NZD}(11,9) = \text{NZD}(9,2) = 1,$$

па затоа од теорема 7.5 следува дека

$$\text{NZS}(20,31) = 20 \cdot 31 = 620.$$

б) Бидејќи $\text{NZD}(n, 2n+1) = 1$, за секој $n \in \mathbf{N}$, од теоремата 7.5 заклучуваме дека $\text{NZS}(n, 2n+1) = n(2n+1)$. ♦

7.7. Теорема. а) $\text{NZS}(na, nb) = n \cdot \text{NZS}(a, b)$, за секои $n, a, b \in \mathbf{N}$.

б) $\text{NZS}(a, b) \cdot \text{NZD}(a, b) = ab$, за секои $a, b \in \mathbf{N}$.

Доказ. а) Нека $\text{NZS}(a, b) = x$. Значи, $a \mid x$ и $b \mid x$, па затоа $na \mid nx$ и $nb \mid nx$, т.е. nx е заеднички содржател на na и nb. Од теорема 7.4 следува дека

$$\text{NZS}(na, nb) \mid nx = n \cdot \text{NZS}(a, b).$$

Нека $\text{NZS}(na, nb) = s$. Тоа значи дека $na \mid s$, т.е. постои $q \in \mathbf{N}$ таков што $s = (na)q = n(aq)$, односно $s = ny$, $y = aq$. Јасно, $a \mid y$. Понатаму, $nb \mid s$, па затоа постои $k \in \mathbf{N}$ таков што $ny = s = (nb)k = n(bk)$, односно $y = bk$. Последното значи $b \mid y$, што заедно со $a \mid y$ повлекува дека y е заеднички содржател на a и b. Сега од теорема 7.4 следува дека $\text{NZS}(a, b) = x \mid y$, односно

$$n \cdot \text{NZS}(a, b) = nx \mid ny = s = \text{NZS}(na, nb).$$

Значи, $\text{NZS}(na, nb) \mid n \cdot \text{NZS}(a, b)$ и $n \cdot \text{NZS}(a, b) \mid \text{NZS}(na, nb)$ па затоа

$$\text{NZS}(na, nb) = n \cdot \text{NZS}(a, b).$$

б) Нека $\text{NZD}(a, b) = d$ и m и n се такви што $a = md, b = nd$ и $\text{NZD}(m, n) = 1$. Од теорема 7.5 и од тврдењето под а) добиваме:

$$\begin{aligned} ab &= (md)(nd) = d \cdot d(mn) = \text{NZD}(a, b) \cdot [d \cdot \text{NZS}(m, n)] \\ &= \text{NZD}(a, b) \cdot \text{NZS}(md, nd) = \text{NZD}(a, b) \cdot \text{NZS}(a, b). \end{aligned}$$ ♦

7.8. Пример. а) Најди $\text{NZS}(1155, 1232)$.

б) Стојан има повеќе од 3000 денари, а помалку од 4000 денари. Ако дневно троши или само по 150 денари или само по 180 денари, по неколку дена му остануваат 30 денари. Колку денари има Стојан?

Решение. а) Имаме,

$$\text{NZD}(1155, 1232) = \text{NZD}(1155, 1232 - 1155) = \text{NZD}(1155, 77)$$

и бидејќи $1155 = 15 \cdot 77$, добиваме дека

$$\text{NZD}(1155, 1232) = \text{NZD}(1155, 77) = 77.$$

Сега од теорема 7.7 б) следува

$$1155 \cdot 1232 = \text{NZD}(1155, 1232) \cdot \text{NZS}(1155, 1232) = 77 \cdot \text{NZS}(1155, 1232),$$

т.е. $\text{NZS}(1155, 1232) = 1155 \cdot 1232 : 77 = 18480$.

б) Стојан нека има x денари. Ако троши по 150 денари дневно по неколку дена му остануваат 30 денари, па затоа $150 \mid (x - 30)$. Слично $180 \mid (x - 30)$, што значи дека $x - 30$ е заеднички содржател на 150 и 180. Имаме,

$$\text{NZD}(150,180) = 30,$$

па ако ја искористиме теорема 7.7 б) добиваме дека

$$150 \cdot 180 = \text{NZD}(150,180) \cdot \text{NZS}(150,180) = 30 \cdot \text{NZS}(150,180)$$

што значи $\text{NZS}(150,180) = 900$. Но, $x - 30$ е заеднички содржател на 150 и 180, па затоа од теорема 7.4 следува дека $900 \mid (x-30)$, односно

$$x - 30 = 900k,\ k \in \mathbf{N}.$$

Понатаму, од условот на задачата имаме

$$3000 < x < 4000,$$

што значи

$$3000 < 900k + 30 < 4000,$$

од каде што наоѓаме $k = 4$. Конечно, Стојан имал $900 \cdot 4 + 30 = 3630$ денари. ♦

7.9. Пример. Најди ги сите природни броеви x и y, за кои

$$\text{NZD}(x,y) = 6 \text{ и } \text{NZS}(x,y) = 36.$$

Решение. Од $\text{NZD}(x,y) = 6$ имаме $x = 6m,\ y = 6n$ и $\text{NZD}(n,m) = 1$. Понатаму, од теоремите 7.5 и 7.7 а) имаме

$$36 = \text{NZS}(x,y) = \text{NZS}(6m,6n) = 6 \cdot \text{NZS}(m,n) = 6mn \text{ т.е. } mn = 6.$$

Бидејќи $\text{NZD}(n,m) = 1$, од последната равенка наоѓаме

$$(m,n) \in \{(1,6),(6,1),(2,3),(3,2)\},$$

па затоа $(x,y) \in \{(6,36),(36,6),(12,18),(18,12)\}$. ♦

7.10. Во претходните разгледувања се задржавме на најмалиот заеднички содржател на два природни броја a и b. Аналогно се дефинира и најмалиот заеднички содржател на конечно многу природни броеви $a_1, a_2, ..., a_k$. Притоа, тој може да се определи на следниов начин:

- најпрво определуваме $\text{NZS}(a_1, a_2) = s_1$,
- потоа определуваме $\text{NZS}(s_1, a_3) = s_2$ итн.

Последниот елемент s_{k-1} во низата $s_1, s_2, ..., s_{k-1}$ е *најмалиот заеднички содржател* на броевите $a_1, a_2, ..., a_k$.

7.11. Пример. Најди го најмалиот природен број кој поделен со 2 дава остаток 1, поделен со 3 дава остаток 2, поделен со 4 дава остаток 3, поделен со 5 дава остаток 4 и поделен со 6 дава остаток 5.

Решение. Ако на бараниот број му додадеме 1, тогаш новодобиениот број се дели со 2, 3, 4, 5 и 6. Бидејќи се бара најмалиот можен број со даденото својство, добиваме дека новодобиениот број е $\text{NZS}(2,3,4,5,6) = 60$. Според тоа, бараниот број е $60 - 1 = 59$. ♦

8. ПРОСТИ И СЛОЖЕНИ БРОЕВИ

8.1. Да се потсетиме дека секој природен број има барем еден делител. Поточно, бројот 1 има само еден делител, а секој друг природен број има два или повеќе делители. Така на пример, броевите 2, 3, 7 и 13 имаат точно два природни делители, а броевите 4, 6, 10, 15 и 20 имаат повеќе од два природни делители. Претходните размислувања укажуваат на можноста во множеството природни броеви **N** да извршиме поделба на дисјунктни подмножества според бројот на делителите и да ги проучуваме овие подмножества. Во таа смисла ја имаме следнава дефиниција.

8.2. Дефиниција. За природниот број p ќе велиме дека е *прост* ако p има точно два природни делители, т.е. единствени делители на p се 1 и p.

Природниот број m кој има повеќе од два природни делители го нарекуваме *сложен број*.

8.3. Значи, според бројот на делителите, разликуваме три вида на природни броеви: броеви со еден делител (тоа е бројот 1), броеви со два делители (прости броеви) и броеви со повеќе од два делители (сложени броеви).

Во врска со простите и сложените броеви од посебен интерес се прашањата:

- Колку прости броеви има, а колку сложени?
- Како да ги одредиме сите прости броеви помали од даден број?

Што се однесува до сложените броеви, одговорот на прашањето: "*Колку сложени броеви има*?" е познат. Имено, постојат бесконечно многу сложени броеви, за што доволно е да ги разгледаме броевите од видот $6k, k \geq 1$. Навистина, сите овие броеви се деливи со 1, 2, 3 и 6, што значи дека тие се сложени, а нив ги има бесконечно многу. Малку потешко е да се одговори на прашањето колку прости броеви има. На ова прашање ќе се навратиме подоцна, а сега ќе докажеме две тврдења со чија помош можеме да ги распознаваме простите и сложените броеви.

8.4. Теорема. Секој природен број n, поголем од 1, е делив барем со еден прост број.

Доказ. Ако природниот број n е прост, тогаш тврдењето е докажано. Имено, тој е делив со самиот себе, што значи барем со еден прост број.

Да претпоставиме дека n е произволен сложен број. Тогаш, тој мора да има барем еден делител различен од 1 и n, бидејќи во спротивно ќе биде прост број. Нека најмалиот од сите делители на n, различни од 1 и n, го означиме со p. Ќе докажеме дека p е прост број. Навистина, ако p е сложен број, тогаш тој има делител q, $1 < q < p$. Но, тогаш бројот q е делител на n, помал од p, што му противречи на изборот на p. Од добиената противречност следува дека p е прост број. Конечно, сложениот број n е делив со простиот број p, што значи барем со еден прост број. ♦

8.5. Според дефиниција 8.2 прости броеви се, на пример: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 и 37. Да забележиме дека единствен парен прост број е бројот 2. Имено, секој парен број поголем од 2 има најмалку три делители, и тоа 1, 2 и самиот број, значи е сложен број.

Според теорема 8.4, за да утврдиме дали еден природен број, поголем од 1, е прост или сложен, доволно е да провериме дали тој е делив со последователните прости броеви 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... Природно е да се запрашаме дали треба да делиме со сите прости броеви кои се помали од разгледуваниот број. Одговорот на ова прашање го дава следнава теорема.

8.6. Теорема. Ако природниот број p, $p>1$ не се дели со простите броеви чии квадрати се помали од p, тогаш p е прост број.

Доказ. Нека p е сложен број. Постои природен број $a \neq p$ и 1 таков што $a \mid p$. Значи, $p = ab$ каде што a и b се природни броеви помали од p. Нека $a \leq b$. Тогаш, $a^2 \leq ab = p$.

Можни се два случаи: a е прост број или a не е прост број.

Ако a е прост број, тогаш p се дели со прост број чиј квадрат е помал од p и во овој случај тврдењето е докажано.

Ако a не е прост број, тогаш постои прост број $q < a$ таков што $q \mid a$, па затоа $q \mid p$. Притоа $q^2 < a^2 \leq p$. Според тоа, p се дели со прост број чиј квадрат е помал од p, т.е. и во овој случај тврдењето е докажано. ♦

8.7. Пример. Испитај го видот на бројот:

а) 323 и б) 503.

Решение. а) Очигледно, според признаците за деливост, бројот 323 не е делив ни со 2, ни со 3, ни со 5. Со непосредно делење се убедуваме дека бројот 323 не е делив ни со 7, ни со 11, ни со 13, но е делив со 17, бидејќи $323 = 17 \cdot 19$. Според тоа, бројот 323 е сложен и неговите делители се 1, 17, 19 и 323.

б) Лесно заклучуваме дека бројот 503 не е делив ни со 2, ни со 3, ни со 5, а со непосредно делење заклучуваме дека не е делив ни со 7, 11, 13, 17 и 19. Следниот прост број е 23, но бидејќи $23^2 = 529 > 503$, од теоремата 8.6 следува дека бројот 503 е прост број. ♦

8.8. Коментар. Од решените примери гледаме дека постапката за одредување на видот на еден природен број бара до толку поголем труд, до колку е бројот поголем. Затоа се изготвуваат таблици на прости броеви. Едноставна постапка за изготвување на таблиците на прости броеви предложил Ератостен (III век пред н.е.) и според него оваа постапка е наречена *Ератостеново сито*. Таа се состои во следното.

Ги испишуваме сите природни броеви помали или еднакви на бројот N. Најпрво ја прецртуваме единицата. Бидејќи првиот прост број е 2, ги прецртуваме сите природни броеви деливи со 2 и поголеми од 2 (тие се сложени). Следниот

непрецртан број, кој е прост е бројот 3 и ги прецртуваме сите природни броеви деливи со 3 и поголеми од 3. Следниот непрецртан број е 5. Тој е прост, бидејќи ако не е ќе биде прецртан. Повторувајќи ја постапката јасно е дека можат да се определат сите прости броеви помали од даден природен број N. Според теоремата 8.6 доволно е проверката да ја направиме со прецртување на содржателите на простите броеви кои се помали или еднакви на $\sqrt{N}$.

8.9. Пример. Да се најдат простите броеви кои се помали или еднакви на 66.

Решение. Имаме

$$\cancel{1}, 2, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, \cancel{9}, \underline{10}, 11, \underline{12}, 13, \underline{14}, \cancel{15}, \underline{16}, 17, \underline{18}, 19, \underline{20}, \cancel{21}, \underline{22}, 23, \underline{24}, \cancel{25}, \underline{26}, \cancel{27}, \underline{28},$$
$$29, \underline{30}, 31, \underline{32}, \cancel{33}, \underline{34}, \cancel{35}, \underline{36}, 37, \underline{38}, \cancel{39}, \underline{40}, 41, \underline{42}, 43, \underline{44}, \cancel{45}, \underline{46}, 47, \underline{48}, \cancel{49}, \underline{50}, \cancel{51}, \underline{52},$$
$$53, \underline{54}, \cancel{55}, \underline{56}, \cancel{57}, \underline{58}, 59, \underline{60}, 61, \underline{62}, \cancel{63}, \underline{64}, \cancel{65}, \underline{66}.$$

Значи, прости броеви помали од 66 се:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 и 61. ♦

8.10. Забелешка. Како што гледаме, простите броеви се многу неправилно распоредени и единствен парен прост број е бројот 2. Меѓутоа, сепак во оваа неправилност на распоредот на простите броеви постојат некои класи на броеви кои ги содржат сите прости броеви поголеми од даден број, што може да се види од следниот пример.

8.11. Пример. Докажи дека секој прост број поголем од 3 е од видот или $6k+1$ или $6k-1$, $k \in \mathbf{N}$.

Решение. Од теоремата за делење со остаток следува дека секој природен број може да се запише во еден од следниве видови:

$$6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5\ ,\ k \in \mathbf{N}_0\ .$$

Јасно, $6 \mid 6k$, $2 \mid (6k+2)$, $3 \mid (6k+3)$ и $2 \mid (6k+4)$, па затоа овие броеви се сложени. Според тоа, ако p, $p>3$ е прост број, тогаш или $p=6k+1$ или $p=6k-1$, $k \in \mathbf{N}$.

Да забележиме, дека обратното тврдење не важи. Навистина, $25=6\cdot 4+1$ и $35=6\cdot 6-1$ се сложени броеви од видовите $6k+1$ и $6k-1$, соодветно. ♦

8.12. Теорема. Постојат бесконечно многу прости броеви.

Доказ. Да претпоставиме дека постојат конечно многу прости броеви и да ги нумерираме по растечки редослед

$$p_1=2,\ \ p_2=3,\ \ p_3=5,\ \ ...,\ p_n=p\ . \tag{1}$$

Да го разгледаме бројот $N=p_1p_2p_3...p_n+1$. Имаме, $N=p_iN_i+1$, за $i=1,\ \ 2,...,n$ од што следува дека ниеден од простите броеви во (1) не е делител на N. Значи, или бројот N е прост број или има прост делител кој не е меѓу броевите во (1). И во двата случаи заклучуваме дека постои прост број кој е поголем од најголемиот претпоставен прост број p, од што следува дека постојат бесконечно многу прости броеви. ♦

8.13. Пример. Ако p е прост број, $p>3$, тогаш $24\mid(p^2-1)$. Докажи!

Решение. Ако $p>3$ и p е прост број, тогаш $p=6k\pm1$, $k\in\mathbf{N}$ и ако искористиме дека $k(k\pm1)=2m$, добиваме:

$$p^2-1=(6k\pm1)^2-1=36k^2\pm12k+1-1=24k^2+12k^2\pm12k$$
$$=24k^2+12k(k\pm1)=24k^2+12\cdot2m=24(k^2+m)$$

што значи $24\mid(p^2-1)$. ♦

8.14. Пример. За произволен природен број k постојат k последователни сложени броеви. Докажи!

Решение. Да ги разгледаме броевите

$$a_1=(k+1)k(k-1)\cdot\ldots\cdot3\cdot2+2$$
$$a_2=(k+1)k(k-1)\cdot\ldots\cdot3\cdot2+3$$
$$a_3=(k+1)k(k-1)\cdot\ldots\cdot3\cdot2+4$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{k-1}=(k+1)k(k-1)\cdot\ldots\cdot3\cdot2+k$$
$$a_k=(k+1)k(k-1)\cdot\ldots\cdot3\cdot2+(k+1)$$

Јасно, ова се k последователни природни броеви и сите се сложени:

$$2\mid a_1,\ 3\mid a_2,\ 4\mid a_3,\ldots,\ k\mid a_{k-1},\ (k+1)\mid a_k\ .\ \blacklozenge$$

9. ОСНОВНА ТЕОРЕМА НА АРИТМЕТИКАТА

9.1. Честопати одделни аритметички задачи можеме едноставно да ги решиме ако даден природен број го разложиме на производ од прости множители. Притоа, се поставува прашањето дали секој природен број може да се претстави како производ од прости броеви. Се покажува дека секој сложен број е производ од прости броеви. За мали броеви тоа лесно се проверува: $4=2\cdot2, 12=2\cdot2\cdot3$ итн. Пред да го докажеме ова тврдење, кое е познато како *основна теорема на аритметиката,* ќе ја докажеме следнава теорема.

9.2. Теорема . Ако p е прост број и $p\mid ab$, тогаш $p\mid a$ или $p\mid b$.

Доказ. Да претпоставиме дека $p\nmid a$. Тогаш a и p се заемно прости броеви. Но, $p\mid ab$, па од теорема 6.13 а) следува дека $p\mid b$.

Аналогно се докажува дека ако $p\nmid b$, тогаш $p\mid a$. ♦

9.3. Теорема (основна теорема на аритметиката). Секој природен број N на единствен начин може да се запише како производ на прости множители, (редоследот на множителите не е битен).

Доказ. Најпрво ќе докажеме дека природниот број N може да се запише како производ на прости множители.

Ако N е прост број, тогаш $N = p$ и теоремата е докажана.

Да претпоставиме дека N не е прост број. Тогаш $N = n_1 n_2$. Ако n_1 и n_2 се прости броеви, тогаш доказот е завршен. Ако n_1 или n_2 не е прост број, тогаш постапката ја повторуваме и по конечен број чекори (според теоремата 8.6 сложен број е делив само со простите броеви чии квадрати се помали или еднакви на самиот број) го добиваме претставувањето

$$N = p_1 p_2 ... p_n \text{, каде што } p_i, i = 1,2,...,n \text{ се прости броеви.} \qquad (1)$$

Да претпоставиме дека постојат две претставувања:

$$N = p_1 p_2 ... p_n = q_1 q_2 ... q_k \text{ , } n \le k \text{ .}$$

Тогаш $p_1 \mid q_1 q_2 ... q_k$ и бидејќи два прости броеви се или меѓусебно еднакви или се заемно прости, од теоремата 9.2 следува дека $p_1 = q_j$ за некој $j = 1, \ 2,..., k$. Повторувајќи ја постапката за $p_2, ..., p_n$ добиваме дека

$$N = p_1 p_2 ... p_n = (p_1 p_2 ... p_n) q_{n+1} ... q_k \text{ ,}$$

од што следува $q_{n+1} = ... = q_k = 1$, па значи $n = k$ и претставувањето е единствено со точност до редоследот на множителите. ♦

9.4. Пример. Запиши ги броевите 6930 и 32340 како производ на прости множители.

Решение. Имаме

6930	2
3465	3
1155	3
385	5
77	7
11	11
1	

и

32340	2
16170	2
8085	3
2695	5
539	7
77	7
11	11
1	

од што добиваме $6930 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ и $32340 = 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11$. ♦

9.5. Пример. Најди ги сите природни броеви n за кои

$$n(n+1)(2n+1) = 84 \text{ .}$$

Решение. Бројот 84 го разложуваме на прости множители и наоѓаме $84 = 2 \cdot 2 \cdot 3 \cdot 7$, односно

$$84 = 3 \cdot (2 \cdot 2) \cdot 7 = 3 \cdot (3+1) \cdot (2 \cdot 3 + 1) \text{ ,}$$

од што следува $n = 3$. ♦

9.6. Како што видовме во претходните два примери, при разложувањето на даден број на прости множители, некои од множителите може повеќекратно да се повторуваат. Ако во разложувањето (1) некои од множителите се еднакви меѓу себе, на пример p_1 се јавува a_1 пати, p_2 се јавува a_2 пати итн., p_k се јавува a_k пати, тогаш за n добиваме

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \ . \qquad (2)$$

Ваквиот запис на бројот n го нарекуваме *каноничен запис*. Како што видовме во пример 9.4, каноничните записи на броевите 6930 и 32340 се

$$6930 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \text{ и } 32340 = 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \, .$$

Да забележиме дека со помош на каноничниот запис можеме да дадеме едноставен критериум кога еден природен број е полн квадрат. Имено, од теорема 9.3 и од својствата на степените, следува дека:

Природниот број n е полн квадрат ако степеновите показатели a_i, $i = 1, 2, \dots, k$ во каноничниот запис (2) *се парни броеви.*

9.7. Пример. Со кој најмал природен број k треба да се помножи бројот 720 за да добиеме точен квадрат.

Решение. Го разложуваме бројот 720 на прости множители:

$$720 = 8 \cdot 9 \cdot 10 = 2^3 \cdot 3^2 \cdot 2 \cdot 5 = 2^4 \cdot 3^2 \cdot 5 \, .$$

Простите броеви 2 и 3 имаат парни степенови показатели, а 5 има непарен степенов показател. Следствено, за да добиеме точен квадрат, треба бројот 720 да го помножиме со 5. Навистина

$$720 \cdot 5 = 2^4 \cdot 3^2 \cdot 5 \cdot 5 = (2^2 \cdot 3 \cdot 5)^2 = 60^2 \, .$$

Значи, бараниот број е $k = 5$. ♦

9.8. Со помош на каноничниот запис на дадени природни броеви n и m лесно се определуваат најголемиот заеднички делител и најмалиот заеднички содржател на n и m. Имено, ако

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \text{ и } m = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

(некои од броевите a_i и b_j можат да бидат еднакви на нула), тогаш

$\mathrm{NZD}(m,n) = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k}$, каде што $c_i = \min\{a_i, b_i\}$, $i = 1, 2, \dots, k$ и

$\mathrm{NZS}(m,n) = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$, каде што $d_i = \max\{a_i, b_i\}$, $i = 1, 2, \dots, k$.

Така на пример, ако се искористат каноничните записи на броевите

$$6930 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \text{ и } 32340 = 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \, ,$$

со помош на претходните формули наоѓаме

$$\mathrm{NZD}(6930, 32340) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 \text{ и}$$

$$\mathrm{NZS}(6930, 32340) = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 = 97020 \, .$$

10. ЛИНЕАРНА ДИОФАНТОВА РАВЕНКА

10.1. Дефиниција. Нека $a,b,c \in \mathbf{Z}$ и $ab \neq 0$. Линеарната равенка од видот

$$ax + by = c, \tag{1}$$

чии решение (x, y) се подредени парови цели броеви ја нарекуваме *линеарна Диофантова равенка со две непознати*.

10.2. Коментар. Токму барањето решенијата x и y на равенката (1) да се целобројни е клучниот проблем при решавањето на овие равенки. Така на пример, очигледно е дека равенката $x + y = 11$ има бесконечно многу решенија. Меѓутоа, равенката $6x + 15y = 17$ нема целобројни решенија. Навистина, за секои цели броеви x и y левата страна на последната равенка е делива со 3 и бидејќи $3 \nmid 17$ заклучуваме дека оваа равенка нема целобројни решенија.

Во врска со прашањето кога една линеарна Диофантова равенка со две непознати има решение ќе ја докажеме следната теорема.

10.3. Теорема. Линеарната Диофантова равенка (1) има решение ако и само ако $d \mid c$, каде што $d = \text{NZD}(a,b)$.

Доказ. Нека $d = \text{NZD}(a,b)$. Да претпоставиме дека (x_0, y_0) е решение на равенката (1). Тогаш $ax_0 + by_0 = c$ и бидејќи $d \mid a$ и $d \mid b$, добиваме $d \mid c$.

Обратно, да претпоставиме дека $d \mid c$. Тогаш постои цел број k таков што $c = kd$. Од друга страна, бидејќи $d = \text{NZD}(a,b)$ постојат цели броеви x' и y' такви што $ax' + by' = d$. Ако последното равенство го помножиме со k, добиваме $akx' + bky' = dk$, т.е. $a(kx') + b(ky') = c$. Според тоа, подредениот пар $(x_0, y_0) = (kx', ky')$ е решение на равенката (1). ♦

Очигледно, доказот на теорема 10.3 и Евклидовиот алгоритам го даваат и методот за решавање на линеарната Диофантова равенка со две непознати.

10.4. Пример. Во множеството на целите броеви реши ја равенката

$$16x - 34y = 7.$$

Решение. Бидејќи $\text{NZD}(16,34) = 2 \nmid 7$, од теорема 10.3 следува дека разгледуваната равенка нема целобројни решенија. Навистина, за секои цели броеви x и y левата страна

$$16x - 34y = 2(8x - 17y)$$

е делива со 2, а десната страна не е делива со 2, $2 \nmid 7$. ♦

10.5. Пример. Во множеството на целите броеви реши ја равенката

$$13x + 32y = 5.$$

Решение. Имаме $a=13$ и $b=32$. Бидејќи $\text{NZD}(13,32)=1$, од теоремата 10.3 следува дека равенката има решение. Сега, користејќи го Евклидовиот алгоритам, имаме

$$32=2\cdot 13+6$$
$$13=2\cdot 6+1$$
$$6=6\cdot 1$$

па затоа

$1=13-2\cdot 6=13-2\cdot(32-2\cdot 13)=5\cdot 13+(-2)\cdot 32$, т.е. $5\cdot 13+(-2)\cdot 32=1.$

Ако последното равенство го помножиме со 5, добиваме

$$13\cdot 25+32\cdot(-10)=5$$

што значи дека едно решение на равенката $13x+32y=5$ е подредениот пар (25, -10). Лесно се проверува дека решенија на равенката се и подредените парови

$(25+32t,-10-13t)$, за $t=\pm 1,\pm 2,\pm 3,\ldots$. ♦

10.6. Во претходната теорема одговоривме кога линеарна Диофантова равенка со две непознати има решение, а во пример 10.5 покажавме како се наоѓа едно нејзино решение. Во следната теорема ќе ги окарактеризираме решенијата на равенката (1) во случај кога истите постојат.

10.7. Теорема. Ако $d=\text{NZD}(a,b)$, $d\mid c$ и (x_0,y_0) е едно решение на Диофантовата равенка $ax+by=c$, тогаш сите нејзини решенија се дадени со:

$$x=x_0+\tfrac{b}{d}t,\ y=y_0-\tfrac{a}{d}t,\ t=0,\pm 1,\pm 2,\pm 3,\ldots. \qquad (2)$$

Доказ. Ако (x_0,y_0) е решение на равенката $ax+by=c$, тогаш со замена на $x=x_0+\frac{b}{d}t$ и $y=y_0-\frac{a}{d}t$ добиваме

$ax+by=a(x_0+\frac{b}{d}t)+b(y_0-\frac{a}{d}t)=ax_0+by_0=c$, за секој $t=0,\pm 1,\pm 2,\ \ldots$

т.е. со (2) се дадени решенија на равенката $ax+by=c$.

Ќе докажеме дека секое решение на равенката $ax+by=c$ е во облик (2). Ако (x,y) е произволно решение на $ax+by=c$, тогаш последователно добиваме

$$ax+by=ax_0+by_0,$$
$$a(x-x_0)=b(y_0-y),$$
$$\tfrac{a}{d}(x-x_0)=\tfrac{b}{d}(y_0-y).$$

Од $d=\text{NZD}(a,b)$ следува $\text{NZD}(\frac{a}{d},\frac{b}{d})=1$, па затоа

$$\tfrac{a}{d}\mid(y_0-y)\ \text{ и }\ \tfrac{b}{d}\mid(x-x_0),$$

т.е. $x-x_0=\frac{b}{d}t$ и $y_0-y=\frac{a}{d}t$, каде што t е цел број. Според тоа, решението (x,y) е во видот (2). ♦

10.8. Пример. Во множеството на целите броеви реши ја равенката

$$69x+111y=9000.$$

Решение. Бидејќи $\text{NZD}(69,111)=3$, дадената равенка ја делиме со 3 и ја добиваме еквивалентната равенка $23x+37y=3000$. Користејќи го Евклидовиот алгоритам наоѓаме $23\cdot(-8)+37\cdot 5=1$. Последното равенство го множиме со 3000 и добиваме

$$23\cdot(-24000)+37\cdot 15000=3000.$$

Конечно, од претходната теорема следува дека сите решенија на Диофантовата равенка $69x+111y=9000$ се дадени со

$$x=-24000+37t,\quad y=15000-23t,\quad t=0,\pm 1,\pm 2,\pm 3,\ldots. \ \blacklozenge$$

10.9. Во претходниот дел видовме кога линеарната Диофантова равенка со две непознати има решение и дадовме постапка за нејзино решавање. Овде ќе презентираме уште еден метод за решавање на ваков тип равенка. Овој метод му припаѓа на швајцарскиот математичар Леонард Ојлер (1707-1783 год.) и затоа е наречен *Ојлеров метод*. Ојлеровиот метод ќе го објасниме со следниов пример.

Пример. Во множеството на целите броеви реши ја равенката

$$738x+621y=45.$$

Решение. Нека (x,y) е решение на дадената равенка. Бидејќи $621<738$, го изразуваме y преку x. Ако ги искористиме равенствата $738=621+117$ и $45=0\cdot 621+45$, добиваме

$$y=\frac{-738x+45}{621}=-x+\frac{-117x+45}{621}.$$

Понатаму, бидејќи x и y се цели броеви добиваме дека и $\frac{-117x+45}{621}$ треба да биде цел број, односно $\frac{-117x+45}{621}=t$, од што ја наоѓаме Диофантовата равенка $621t=-117x+45$, која има помали коефициенти од почетната равенка. Ја повторуваме постапката и го изразуваме x со помош на t. Добиваме

$$x=\frac{-621t+45}{117}=-5t+\frac{-36t+45}{117},$$

односно $x=-5t+u$, каде што $u=\frac{-36t+45}{117}$. Ја повторуваме постапката и го изразуваме t со помош на u. Имаме

$$t=\frac{-117u+45}{36}=-3u+1+\frac{-9u+9}{36}=-3u+1+v,$$

каде што $v=\frac{-9u+9}{36}$. Од последното равенство добиваме $u=-4v+1$, $v\in\mathbf{Z}$. Ако сега последователно се вратиме наназад добиваме:

$$\begin{aligned}
t&=-3u+1+v=-3(-4v+1)+1+v=13v-2,\\
x&=-5t+u=-5(13v-2)+(-4v+1)=-69v+11,\\
y&=-x+t=-(-69v+11)+(13v-2)=82v-13,\quad v\in\mathbf{Z}.
\end{aligned}$$

Всушност, со последните две равенства се дадени сите решенија (x, y) на равенката $738x + 621y = 45$. ♦

10.10. Пример. Илија требало да реши 73 задачи за 19 дена. Првите 11 дена тој решавал еднаков број задачи секој ден, а останатите 8 дена повторно решавал еднаков број задачи. Колку задачи решавал Илија секој ден?

Решение. Нека бројот на задачите кои ги решавал Илија во секој од првите 11 дена го означиме со x, а бројот на задачите кои ги решавал во секој од преостанатите 8 дена со y. Од условот на задачата имаме $11x + 8y = 73$. Бидејќи $\text{NZD}(8,11) = 1$, заклучуваме дека последната равенка има решение во множеството на целите броеви.

Ако го искористиме методот на Ојлер, за решението на равенката наоѓаме

$$x = 3 - 8k, \quad y = 5 + 11k, \quad k \in \mathbf{Z}.$$

Од условот на задачата следува дека $x, y \in \mathbf{N}$, а тоа е можно само за $k = 0$. Конечно, $x = 3, y = 5$ е решение на задачата, што значи дека Илија првите 11 дена решавал по 3, а вторите 8 дена по 5 задачи дневно. ♦

11. МЕТОДИ ЗА РЕШАВАЊЕ НА НЕЛИНЕАРНИ ДИОФАНТОВИ РАВЕНКИ

11.1. Диофантовите равенки се еден од најбогатите и најразновидните делови на теоријата на броеви. Претходно видовме како се решава линеарна Диофантова равенка со две непознати. Меѓутоа, решавањето на нелинеарните Диофантови равенки не е така едноставно, па затоа не треба да нé чуди што за да се докаже дека Диофантовата равенката $x^n + y^n = z^n$, $n > 2$, која ја поставил францускиот математичар Пјер Ферма, нема решение во множеството природни броеви, биле потребни повеќе од триста години.

Што се однесува до решавањето на нелинеарните Диофантови равенки, треба да споменеме дека не постојат универзални алгоритми, но сепак да споменеме дека некои елементарни, но доста важни постапки даваат решение на голем број нелинеарни Диофантови равенки. Овие постапки најчесто се засноваат на следниве идеи:

- разложување на множители,
- дискусија на количник,
- дискусија на последната цифра и
- разгледување на остатоци при делење со даден број.

11.2. Пример. Во множеството на целите броеви реши ја Диофантовата равенка

$$x^2 + y^2 + z^2 - 2x + 4y - 6z = -11.$$

Решение. Дадената равенка ја запишуваме во видот

$$(x-1)^2+(y+2)^2+(z-3)^2=3\,.$$

Последната равенка во множеството на целите броеви има решение ако секој од квадратите е еднаков на 1, па затоа сите тројки решенија ги добиваме со комбинирање на решенијата

$$x-1=1,\quad y+2=1,\quad z-3=1,\quad x-1=-1,\quad y+2=-1,\quad z-3=-1\,.$$

Според тоа, решенија се:

$$(x,y,z)\in\{(0,-1,2);(0,-1,4);(0,-3,2);(0,-3,4);(2,-1,2);(2,-1,4);(2,-3,2);(2,-3,4)\}\,.\ \blacklozenge$$

11.3. Пример. Во множеството на целите броеви реши ги Диофантовите равенки

а) $x^2-4y^2=17$, б) $xy-4x-2y+5=0$

Решение. а) Дадената равенка ја запишуваме во видот

$$(x-2y)(x+2y)=17\,. \qquad (1)$$

Бидејќи 17 е прост број, од (1) ги добиваме системите равенки:

$$\begin{cases}x-2y=1\\x+2y=17\end{cases}\quad\begin{cases}x-2y=-1\\x+2y=-17\end{cases}\quad\begin{cases}x-2y=17\\x+2y=1\end{cases}\quad\text{и}\quad\begin{cases}x-2y=-17\\x+2y=-1\end{cases}$$

чии решенија соодветно се подредените парови:

$$(9,4)\,,\ (-9,-4)\,,\ (9,-4)\ \text{и}\ (-9,4)\,.$$

б) Дадената равенка ја запишуваме во видот $(x-2)(y-4)=3$. Бидејќи 3 е прост број, од последната равенка имаме:

$$\begin{cases}x-2=1\\y-4=3\end{cases}\quad\begin{cases}x-2=-1\\y-4=-3\end{cases}\quad\begin{cases}x-2=3\\y-4=1\end{cases}\quad\text{и}\quad\begin{cases}x-2=-3\\y-4=-1,\end{cases}$$

од што следува дека $(x,y)\in\{(3,7),(1,1),(5,5),(-1,3)\}$. $\blacklozenge$

11.4. Пример. Во множеството на целите броеви реши ги Диофантовите равенки

а) $xy+7x-3y=23$, б) $x^2-xy+2x-3y=6$

Решение. Равенките од оваа задача ќе ги решиме со дискусија на количник.

а) Последователно, еквивалентно ја трансформираме равенката и добиваме $x(y+7)=3y+23$, односно $x=\frac{3y+23}{y+7}$, од што следува $x=3+\frac{2}{y+7}$. Бидејќи x е цел број, последната равенка има решение ако и само ако $(y+7)\,|\,2$, т.е. ако и само ако $y+7\in\{-2,-1,1,2\}$, што значи $y\in\{-9,-8,-6,-5\}$. Конечно, ако најдените вредности за y ги замениме во $x=3+\frac{2}{y+7}$, за решението на почетната равенка добиваме

$$(x,y)\in\{(5,-6),(1,-8),(4,-5),(2,-9)\}\,.$$

б) Од $x^2 - xy + 2x - 3y = 6$, имаме

$$y = \frac{x^2+2x-6}{x+3} = \frac{x^2+3x-x-3-3}{x+3} = x - 1 - \frac{3}{x+3}.$$

Значи, $(x+3) \mid 3$ т.е. $x+3 \in \{-3, -1, 1, 3\}$. Според тоа, множеството решенија на дадената равенка е $\{(-2,-6), (-4,-2), (0,-2), (-6,-6)\}$. ♦

11.5. Пример. Во множеството на целите броеви реши ги Диофантовите равенки

а) $x^2 + 5y = 2002$ и

б) $1! + 2! + 3! + \ldots + x! = y^2$, каде што $k! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (k-1)k$.

Решение. а) За секој цел број y, цифрата на единиците на бројот $5y$ е 0 или 5. Понатаму, за секој цел број x, цифрата на единиците на неговиот квадрат x^2 е една од цифрите 0, 1, 4, 5, 6 или 9. Според тоа, ако $5y \geq 0$, тогаш цифрата на единиците на бројот $x^2 + 5y$ е една од цифрите 0, 1, 4, 5, 6 или 9. Аналогно се добива дека во случај кога $5y < 0$, цифрата на единиците на бројот $x^2 + 5y$ е една од цифрите 0, 1, 4, 5, 6 или 9.

Конечно, за секои $x, y \in \mathbf{Z}$ цифрата на единиците на бројот $x^2 + 5y$ е 0, 1, 4, 5, 6 или 9 и таа е различна од цифрата на единиците на бројот 2002. Значи, равенката нема решение во множеството на целите броеви.

б) Ако $x = 1$, тогаш $y = \pm 1$.

Ако $x = 2$, тогаш $y^2 = 3$, па y не е цел број.

Ако $x = 3$, тогаш $y^2 = 1 + 2 + 6$, што значи $y = \pm 3$.

Ако $x = 4$, тогаш $y^2 = 1 + 2 + 6 + 24 = 33$ па y не е цел број.

Нека $m \geq 5$. Тогаш $m!$ е делив со 10, па затоа $m! = 10t$, од што следува

$$1! + 2! + 3! + 4! + 5! + \ldots + x! = 33 + 10k.$$

Бројот $33 + 10k$ завршува на цифрата 3, а бројот y^2 завршува на една од цифрите 0, 1, 4, 5, 6 или 9, па затоа во овој случај задачата нема решение.

Конечно, единствени решенија на дадената равенка се подредените парови $(1,-1), (1,1), (3,-3), (3,3)$. ♦

11.6. Пример. Во множеството на целите броеви реши ја Диофантовата равенка

$$x^2 = 9y + 5.$$

Решение. Секој природен број може да се запише во еден од видовите

$$3k,\ 3k+1 \text{ или } 3k+2.$$

Според тоа, неговиот квадрат има вид

$$3\cdot 3k^2,\ 3(3k^2+2k)+1 \text{ или } 3(3k^2+4k+1)+1,$$

т.е. при делење со 3 дава остаток 0 или 1. Од друга страна

$$9y+5=3(3y+1)+2,$$

т.е. остатокот при делење со 3 е 2. Значи на двете страни на равенката, при делење со 3 секогаш добиваме различни остатоци, па затоа дадената равенка нема решение. ♦

12. ПОИМ ЗА КОНГРУЕНЦИЈА. ОСНОВНИ СВОЈСТВА

12.1. Во претходните разгледувања видовме дека броевите кои при делење со еден ист број даваат ист остаток се од посебен интерес во теоријата на броеви. Токму затоа тие биле предмет на разработка на многу знаменити математичари, што довело до поимот конгруенција во множеството на целите броеви, т.е. методот на конгруенции во множеството на целите броеви. Овој метод е формален аритметички метод заснован на разгледување на својствата на целите броеви кои имаат еднакви остатоци при делење со еден ист број. Методот прв го разработил германскиот математичар Гаус (1777-1855) иако многу резултати биле познати и порано.

12.2. Дефиниција. Нека $a,b\in\mathbf{Z}$ и $m\in\mathbf{N}$. Ако $m\mid(a-b)$, тогаш ќе велиме дека бројот a *е конгруентен* со бројот b по модул m и ќе пишуваме $a\equiv b\ (\mathrm{mod}\ m)$.

Ако $m\nmid(a-b)$, тогаш ќе велиме дека бројот a *не е конгруентен* со бројот b по модул m и ќе пишуваме $a\not\equiv b\ (\mathrm{mod}\ m)$.

12.3. Пример. а) Да ги разгледаме броевите $a=78, b=85$ и $m=7$. Бидејќи $a-b=78-85=-7=-7\cdot 1$, од дефиницијата 12.2 добиваме

$$78\equiv 85\ (\mathrm{mod}\ 7).$$

б) За броевите $a=123, b=97$ важи $a-b=123-97=26$ и бидејќи $3\nmid 26$ заклучуваме дека $123\not\equiv 97\ (\mathrm{mod}\ 3)$. ♦

12.4. Теорема. Нека $a,b\in\mathbf{Z}$ и $m\in\mathbf{N}$. Тогаш:

а) $a\equiv b\ (\mathrm{mod}\ m)$ ако и само ако постои цел број k таков што $a=b+km$.

б) $a\equiv b\ (\mathrm{mod}\ m)$ ако и само ако при делење со m, броевите a и b имаат еднакви остатоци.

Доказ. а) Од дефиниција 12.2 следува дека $a\equiv b\ (\mathrm{mod}\ m)$ ако и само ако $m\mid(a-b)$. Понатаму, $m\mid(a-b)$ ако и само ако постои цел број k таков што $a-b=km$, т.е. постои цел број k таков што $a=b+km$.

б) Нека $a = mp + r$ и $b = mq + s$, $p, q, r, s \in \mathbf{Z}$ и $0 \le r, s < m$. Тогаш $a \equiv b \pmod m$ ако и само ако $m \mid (a - b)$, што значи ако и само ако

$$m \mid [(mp + r) - (mq + s)].$$

Според тоа, $a \equiv b \pmod m$ ако и само ако

$$m \mid [m(p - q) + (r - s)].$$

Значи, $a \equiv b \pmod m$ ако и само ако $m \mid (r - s)$. Но, $-m < r - s < m$, па затоа $a \equiv b \pmod m$ ако и само ако $r - s = 0$, т.е. ако и само ако $r = s$. ♦

12.5. Пример. а) При делење на броевите 63, 64, 65, 66, 67, 68 и 69 со бројот 7 се добива количник 9 и остатоци 0, 1, 2, 3, 4, 5 и 6, соодветно. Од теорема 12.4 б) следува дека

$$63 \equiv 0 \pmod 7,\ 64 \equiv 1 \pmod 7,\ 65 \equiv 2 \pmod 7,\ 66 \equiv 3 \pmod 7,$$
$$67 \equiv 4 \pmod 7,\ 68 \equiv 5 \pmod 7 \text{ и } 69 \equiv 6 \pmod 7.$$

б) Од теорема 12.4 б) имаме дека $37 \equiv 25 \pmod{12}$. Навистина, при делењето на 37 и 25 со 12 се добива остаток 1. ♦

Во следниве теореми ќе докажеме неколку важни својства на конгруенциите. Притоа ќе сметаме дека бројот m е природен број.

12.6. Теорема. а) За секој $a \in \mathbf{Z}$ важи $a \equiv a \pmod m$.

б) Ако $a \equiv b \pmod m$, тогаш $b \equiv a \pmod m$.

в) Ако $a \equiv b \pmod m$ и $b \equiv c \pmod m$, тогаш $a \equiv c \pmod m$

Доказ. а) Од $a - a = 0$, за секој $a \in \mathbf{Z}$ следува $a \equiv a \pmod m$, за секој $a \in \mathbf{Z}$.

б) Ако $a \equiv b \pmod m$, тогаш $m \mid (a - b)$. Од $b - a = (-1)(a - b)$ следува $m \mid (b - a)$, па од дефиниција 12.2 заклучуваме дека $b \equiv a \pmod m$.

в) Ако $a \equiv b \pmod m$ и $b \equiv c \pmod m$, тогаш $m \mid (a - b)$ и $m \mid (b - c)$. Според тоа, $m \mid [(a - b) + (b - c)] = a - c$, па затоа $a \equiv c \pmod m$. ♦

12.7. Теорема. Ако $a \equiv b \pmod m$ и $c \equiv d \pmod m$, тогаш

$$a + c \equiv b + d \pmod m,\ a - c \equiv b - d \pmod m \text{ и } ac \equiv bd \pmod m.$$

Доказ. Нека $a \equiv b \pmod m$ и $c \equiv d \pmod m$. Од дефиниција 12.2 имаме дека $m \mid (a - b)$ и $m \mid (c - d)$. Според тоа

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

и

$$m \mid [c(a - b) + b(c - d)] = ac - bd,$$

што значи дека

$$a+c \equiv b+d \pmod m,\ a-c \equiv b-d \pmod m \text{ и } ac \equiv bd \pmod m.\blacklozenge$$

12.8. Коментар. Да забележиме дека претходната теорема всушност покажува дека релацијата $\equiv$ по даден модул е согласна со операциите собирање, одземање и множење на конгруенции.

Меѓутоа, релацијата $\equiv$ не е согласна со релацијата делење на цели броеви (дури и кога последната е дефинирана). Имено, во конгруенцијата

$$8 \equiv -4 \pmod{12}$$

броевите 8 и -4 се деливи со 2 и со 4, меѓутоа ако поделиме со 2, односно со 4 добиваме $4 \equiv -2 \pmod{12}$ односно $2 \equiv -1 \pmod{12}$, што не е точно.

Понатаму, од теоремите 12.6 а) и 12.7 непосредно следуваат следните тврдења.

12.9. Теорема. а) Ако $a \equiv b \pmod m$, тогаш

$$a+c \equiv b+c \pmod m,\ a-c \equiv b-c \pmod m \text{ и } ac \equiv bc \pmod m,$$

за секој $c \in \mathbf{Z}$.

б) Ако $a \equiv b \pmod m$, тогаш

$$a^n \equiv b^n \pmod m, \text{ за секој } n \in \mathbf{N}.\ \blacklozenge$$

12.10. Пример. Докажи дека за секои прости броеви p и q, $p,q>3$, важи или

$$p \equiv q \pmod 6 \text{ или } p+q \equiv 0 \pmod 6.$$

Решение. Како што знаеме, секој прост број поголем од 3 е од видот или $6k+1$ или $6t-1$. Ќе разгледаме три случаи:

а) ако $p=6k+1$ и $q=6t+1$, тогаш од теорема 12.4 б) следува дека $p \equiv q \pmod 6$;

б) ако $p=6k-1$ и $q=6t-1$, тогаш од теорема 12.4 б) следува дека $p \equiv q \pmod 6$; и

в) ако $p=6k+1$ и $q=6t-1$, тогаш $p \equiv 1 \pmod 6$ и $q \equiv -1 \pmod 6$ и од теорема 12.7 следува дека

$$p+q \equiv 1+(-1) \pmod 6, \text{ т.е. } p+q \equiv 0 \pmod 6.\ \blacklozenge$$

12.11. Пример. а) Докажи дека $10 \mid (3^{1988}-1)$.

б) Најди го остатокот од делењето на бројот 4^{56} со 9.

Решение. а) Од $3^4=81$ следува $3^4 \equiv 1 \pmod{10}$. Сега од теорема 12.9 б) добиваме $(3^4)^{497} \equiv 1^{497} \pmod{10}$, т.е. $3^{1998} \equiv 1 \pmod{10}$, што значи $10 \mid (3^{1988}-1)$.

б) Ќе го побараме оној степен на бројот 4 кој е конгруентен со 1 по модул 9. Последователно имаме $4 \equiv 4 \pmod 9$, $4^2 \equiv 7 \pmod 9$ бидејќи $16 = 9 \cdot 1 + 7$, $4^3 \equiv 1 \pmod 9$ бидејќи $64 = 9 \cdot 7 + 1$. Бидејќи $56 = 18 \cdot 3 + 2$, последната конгруенција ја степенуваме на 18 и добиваме $4^{54} \equiv 1 \pmod 9$. Понатаму, ако ги помножиме конгруенциите $4^2 \equiv 7 \pmod 9$ и $4^{54} \equiv 1 \pmod 9$ добиваме

$$4^{54} \cdot 4^2 \equiv 1 \cdot 7 \pmod 9, \text{ т.е. } 4^{56} \equiv 7 \pmod 9.$$

Значи, остатокот од делењето на бројот 4^{56} со 9 е 7. ♦

Како што рековме, релацијата $\equiv$ не е согласна со релацијата делење на цели броеви (дури и кога последната е дефинирана). Во следната теорема ќе докажеме кога двете страни во една конгруенција може да се поделат со некој број.

12.12. Теорема. а) Ако $\text{NZD}(a, m) = 1$ и $ab \equiv ac \pmod m$, тогаш $b \equiv c \pmod m$.

б) Ако $\text{NZD}(a, m) = d$ и $ab \equiv ac \pmod m$, тогаш $b \equiv c \pmod q$ каде што $q = \frac{m}{d}$.

в) Ако $\text{NZD}(a, m) = d$, $q = \frac{m}{d}$ и $b \equiv c \pmod q$, тогаш $ab \equiv ac \pmod m$.

Доказ. б) Нека $\text{NZD}(a, m) = d$ и $ab \equiv ac \pmod m$. Постојат цели броеви p и q такви што $m = dq$ и $a = dp$ и важи $\text{NZD}(p, q) = 1$. Од $ab \equiv ac \pmod m$ следува дека постои $k \in \mathbf{Z}$ таков што $ab = ac + mk$. Ако последното равенство го поделиме со d го добиваме равенството $pb = pc + qk$ од што следува $p(b - c) = qk$. Но, $\text{NZD}(p, q) = 1$, па затоа од последното равенство следува $q \mid (b - c)$, т.е. $b \equiv c \pmod q$, каде што $q = \frac{m}{d}$.

а) Следува од тврдењето под б) за $d = 1$.

в) Бидејќи $\text{NZD}(a, m) = d$, добиваме $a = dp$ и $m = dq$, за некои цели броеви p и q. Понатаму, од $b \equiv c \pmod q$ следува дека постои $k \in \mathbf{Z}$ таков што $b = c + qk$. Последното равенство го множиме со a и добиваме дека $ab = ac + aqk$ и ако замениме за $a = dp$ добиваме дека

$$ab = ac + (dq)(pk) = ac + m(pk),$$

односно $ab - ac = m(pk)$. Според тоа, $m \mid (ab - ac)$, т.е. $ab \equiv ac \pmod m$. ♦

12.13. Теорема. Ако $a \equiv b \pmod m$ и $a \equiv b \pmod n$ и $\text{NZS}(m, n) = k$, тогаш $a \equiv b \pmod k$.

Доказ. Нека $\text{NZD}(m, n) = t$. Тогаш $n = pt$ и $m = qt$, каде што $\text{NZD}(p, q) = 1$ и $\text{NZS}(m, n) = pqt$. Од $n \mid (a - b)$ и $m \mid (a - b)$ следува дека

$pt \mid (a-b)$ и $qt \mid (a-b)$, т.е. $a-b=ptr$ и $a-b=qts$. Значи, $ptr=qts$, т.е. $pr=qs$ и бидејќи $\text{NZD}(p,q)=1$ добиваме $p \mid s$ т.е. $s=pu$. Со замена во $a-b=qts$ добиваме $a-b=qtpu$, т.е. $pqt \mid (a-b)$. Но, $\text{NZS}(m,n)=pqt=k$, па затоа $a \equiv b \pmod{k}$. ♦

13. ПРИМЕНА НА КОНГРУЕНЦИИТЕ

13.1. При проучувањето на деливоста на целите броеви се задржавме на некои посебни признаци за деливост, а во претходниот дел ги разгледавме конгруенциите и ги докажавме нивните својства. Овде ќе покажеме како конгруенциите можат да се искористат за наоѓање на посебните признаци за деливост. За таа цел прво ќе ја докажеме следната теорема.

Теорема. Нека $f(x)=a_k x^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0$, каде што $a_0,a_1,\ldots,a_{k-1},a_k$ се цели броеви. Ако $a \equiv b \pmod{m}$, тогаш

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

Доказ. Од теорема 12.9 б) следува $a^t \equiv b^t \pmod{m}$ за $t=0,1,\ldots,k$. Сега од теорема 12.9 а) следствено добиваме

$$a_t a^t \equiv a_t b^t \pmod{m} \text{ за } t=0,1,\ldots,k$$

$$a_k a^k+a_{k-1}a^{k-1}+\ldots+a_1a+a_0 \equiv a_k b^k+a_{k-1}b^{k-1}+\ldots+a_1b+a_0 \pmod{m}$$

односно $f(a) \equiv f(b) \pmod{m}$. ♦

13.2. ***Признак за деливост со 9.*** Секој природен број е конгруентен со збирот на своите цифри по модул 9.

Доказ. Нека n е природен број чиј декаден запис е

$$n=a_k10^k+a_{k-1}10^{k-1}+\ldots+a_110+a_0,$$

каде што $a_0,a_1,\ldots,a_{k-1},a_k \in \{0,1,2,\ldots,9\}$. Ставаме

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0.$$

Тогаш, бидејќи $10 \equiv 1 \pmod{9}$ од теорема 13.1 следува

$f(10) \equiv f(1) \pmod{9}$, т.е. $n \equiv a_k+a_{k-1}+\ldots+a_1+a_0 \pmod{9}$. ♦

13.3. Пример. Од

$$56786457455 \equiv 5+6+7+8+6+4+5+7+4+5+5 \equiv 62 \equiv 6+2 \equiv 8 \pmod{9}$$

следува дека бројот 56786457455 не е делив со бројот 9. Но,

$$5673897567 \equiv 5+6+7+3+8+9+7+5+6+7 \equiv 63 \equiv 6+3 \equiv 9 \equiv 0 \pmod{9}$$

па затоа бројот 5673897567 е делив со бројот 9. ♦

13.4. ***Признак за деливост со 11.*** Ако природниот број n има декаден запис

$$n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$$

тогаш

$$n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + ... + a_4 - a_3 + a_2 - a_1 + a_0 \pmod{11}.$$

Доказ. Нека n е природен број чиј декаден запис е

$$n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0,$$

каде што $a_0, a_1, ..., a_{k-1}, a_k \in \{0,1,2,...,9\}$. Ставаме

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0.$$

Тогаш, бидејќи $10 \equiv -1 \pmod{11}$, од теорема 13.1 следува

$$f(10) \equiv f(-1) \pmod{11},$$

т.е.

$$n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + ... + a_4 - a_3 + a_2 - a_1 + a_0 \pmod{11}. \blacklozenge$$

13.5. Пример. Од

$$43419027549 \equiv 9-4+5-7+2-0+9-1+4-3+4 \equiv 18 \equiv 8-1 \equiv 7 \pmod{11}$$

следува дека бројот 43419027549 е конгруентен со 7 по модул 11, т.е. не е делив со 11.

Но, бидејќи

$$47859679 \equiv 9-7+6-9+5-8+7-4 \equiv -1 \pmod{11}$$

добиваме дека бројот 47859679 е конгруентен со -1 по модул 11, т.е. овој број не е делив со 11. ♦

13.6. ***Признак за деливост со 7.*** Ако природниот број n има декаден запис

$$n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0,$$

тогаш n е делив со 7 ако и само ако збирот

$$\{(a_0 + 3a_1 + 2a_2) + (a_6 + 3a_7 + 2a_8) + ...\} -$$
$$-\{(a_3 + 3a_4 + 2a_5) + (a_9 + 3a_{10} + 2a_{11}) + ...\}$$

е делив со 7.

Доказ. Нека n е природен број чиј декаден запис е

$$n = a_k 10^k + ... + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0,$$

каде што $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, ..., a_{k-1}, a_k \in \{0,1,2,...,9\}$. Бидејќи

$$10^0 \equiv 1 \pmod{7},\ 10^1 \equiv 3 \pmod{7},\ 10^2 \equiv 2 \pmod{7},\ 10^3 \equiv 6 \equiv (-1) \pmod{7},$$

$$10^4 \equiv 4 \equiv (-3) \pmod 7,\ 10^5 \equiv 5 \equiv (-2) \pmod 7,\ 10^6 \equiv 1 \pmod 7 \text{ итн.}$$

следува дека

$$10^{6k} \equiv 1 \pmod 7,\ 10^{6k+1} \equiv 3 \pmod 7,\ 10^{6k+2} \equiv 2 \pmod 7,$$
$$10^{6k+3} \equiv (-1) \pmod 7,\ 10^{6k+4} \equiv (-3) \pmod 7,\ 10^{6k+5} \equiv (-2) \pmod 7.$$

Според тоа,

$$\begin{aligned} n &= a_k 10^k + \ldots + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \\ &= a_0 + 10a_1 + a_2 10^2 + a_3 10^3 + a_4 10^4 + a_5 10^5 + a_6 10^6 + a_7 10^7 + \ldots \\ &\equiv a_0 + 3a_1 + 2a_2 + (-1)a_3 + (-3)a_4 + (-2)a_5 + a_6 + 3a_7 + 2a_8 + \ldots \pmod{11} \end{aligned}$$

што и требаше да се докаже. ♦

13.7. Пример. Од

$$\begin{aligned} 43419027549 &\equiv 9 + 3\cdot 4 + 2\cdot 5 - 7 - 3\cdot 2 - 2\cdot 0 + 9 + 3\cdot 1 + 2\cdot 4 - 3 - 3\cdot 4 \\ &\equiv 23 \equiv 3 + 3\cdot 2 \equiv 2 \pmod 7 \end{aligned}$$

следува дека бројот 43419027549 е конгруентен со 2 по модул 7, т.е. не е делив со 7.

Но, бидејќи

$$959679 \equiv 9 + 3\cdot 7 + 2\cdot 6 - 9 - 3\cdot 5 - 2\cdot 9 \equiv 0 \pmod 7,$$

добиваме дека бројот 959679 е конгруентен со 0 по модул 7, т.е. овој број е делив со 7. ♦

13.8. Пример. Докажи дека ако бројот n е делив со 99, тогаш збирот на неговите цифри не е помал од 18.

Решение. Нека $99 \mid n$. Тогаш $9 \mid n$, па затоа и збирот на цифрите A на n е делив со 9. Бидејќи n е природен број, $A > 0$, па единствен број кој е делив со 9 и е помал од 18 е 9. Ако $A = 9$, тогаш од

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$$

следува $A = a_k + a_{k-1} + \ldots + a_1 + a_0$. Од друга страна, бидејќи $11 \mid n$ следува

$$11 \mid \{(-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0\}$$

и бидејќи

$$-9 \le (-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0 \le 9$$

добиваме дека

$$(-1)^k a_k + (-1)^{k-1} a_{k-1} + \ldots - a_1 + a_0 = 0,$$

т.е. $a_0 + a_2 + \ldots = a_1 + a_3 + \ldots$. Според тоа

$$9 = 2(a_0 + a_2 + \ldots),$$

што е противречност. ♦

14. ЛИНЕАРНА КОНГРУЕНТНА РАВЕНКА. КИНЕСКА ТЕОРЕМА ЗА ОСТАТОЦИ

14.1. Дефиниција. Нека $a, b \in \mathbf{Z}$ и $n \in \mathbf{N}$. Равенката од облик

$$ax \equiv b \pmod{n} \tag{1}$$

ја нарекуваме *линеарна конгруентна равенка со една непозната.* За целиот број x_0 ќе велиме дека е *решение* на (1) ако $ax_0 \equiv b \pmod{n}$.

14.2. Теорема. Бројот x_0 е решение на равенката (1) ако и само ако постои цел број y_0 таков што подредениот пар (x_0, y_0) е решение на Диофантовата равенка $ax - ny = b$.

Доказ. Нека x_0 е решение на конгруентната равенка (1). Тогаш, постои цел број y_0 таков што $ax_0 - b = y_0 n$. Според тоа,

$$ax_0 - y_0 n = b$$

од што следува дека парот (x_0, y_0) е решение на Диофантовата равенка $ax - ny = b$.

Обратно, ако парот (x_0, y_0) е решение на Диофантовата равенка $ax - ny = b$, тогаш $ax_0 - y_0 n = b$, т.е. $ax_0 - b = y_0 n$. Од последното равенство следува $n \mid (ax_0 - b)$, па затоа $ax_0 \equiv b \pmod{n}$, што значи дека x_0 е решение на конгруентната равенка (1). ♦

14.3. Теорема. Линеарната конгруентна равенка (1) има решение ако и само ако $d = \mathrm{NZD}(a, n) \mid b$ и во овој случај, ако x_0 е едно решение на (1), тогаш нејзиното општо решение е дадено со

$$x \equiv x_0 \pmod{\tfrac{n}{d}}. \tag{2}$$

Доказ. Според теорема 14.2 равенката (1) има решение ако и само ако равенката $ax - ny = b$ има решение. Сега од теорема 10.3 имаме дека равенката $ax - ny = b$ има решение ако и само ако $d = \mathrm{NZD}(a, n) \mid b$. Понатаму, според теорема 10.7 сите решенија на равенката $ax - ny = b$ се дадени со

$$x = x_0 + \tfrac{n}{d}t \text{ и } y = y_0 - \tfrac{a}{d}t \text{, каде } t = 0, \pm 1, \ldots .$$

Според тоа, за сите решенија на равенката (1) важи

$$x = x_0 + \tfrac{n}{d}t \text{, каде што } t = 0, \pm 1, \ldots ,$$

а тоа значи дека тие се дадени со (2). ♦

14.4. Пример. Линеарната конгруентна равенка

$$42x \equiv 60 \pmod{91}$$

нема решение, бидејќи $\mathrm{NZD}(42, 91) = 7 \nmid 60$. ♦

14.5. Пример. Реши ја линеарната конгруентна равенка

$$42x \equiv 50 \pmod{76}.$$

Решение. Од $\text{NZD}(42,76) = 2 \mid 50$ следува дека дадената равенка има решение. Според теорема 12.12 б), можеме да скратиме со $\text{NZD}(42,76) = 2$ и добиваме

$$21x \equiv 25 \pmod{38}.$$

Понатаму, $0 \equiv 38 \pmod{38}$, па ако ги собереме последните две конгруенции наоѓаме

$$21x \equiv 63 \pmod{38}.$$

Но, $\text{NZD}(21,38) = 1$, па од теорема 12.12 а) следува дека во последната конгруенција можеме да скратиме со 21, со што добиваме

$$x \equiv 3 \pmod{38}.$$

Јасно, решенијата по модул 76 се дадени со

$$x \equiv 3 \pmod{76} \text{ и } x \equiv 41 \pmod{76}. \blacklozenge$$

14.6. Коментар. Во последниот пример добивме две решенија кои не се конгруентни по модул 76. Од теорема 14.3 непосредно следува дека линеарната конгруентна равенка (1) во случај кога има решение, таа има d неконгруентни решенија, $d = \text{NZD}(a,n)$ и ако x_0 е едно нејзино решение, тогаш сите неконгруентни решенија на (1) се дадени со: $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$.

14.7. Пример. Реши ја линеарната конгруентна равенка

$$11x \equiv 25 \pmod{60}.$$

Решение. Бидејќи $1 = \text{NZD}(11,60)$, равенката има точно едно неконгруентно решение. Решението x мора да биде деливо со 5 бидејќи

$$11x = 25 + 60k \text{ за некој } k \in \mathbf{Z}.$$

Нека $x = 5y$. Тогаш

$$55y \equiv 25 \pmod{60}$$

и ако поделиме со 5 добиваме

$$11y \equiv 5 \pmod{12}$$
$$-y \equiv 5 \pmod{12}$$
$$y \equiv -5 \pmod{12}$$
$$y \equiv 7 \pmod{12}.$$

Затоа $x \equiv 35 \pmod{60}$. $\blacklozenge$

14.8. Во претходните разгледувања се осврнавме на решавањето на равенката од видот $ax \equiv b \pmod{n}$, $a,b \in \mathbf{Z}$ и $n \in \mathbf{N}$. Во натамошните разгледувања ќе се задржиме на решавањето на системот линеарни конгруентни равенки од видот:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\ldots\ldots\ldots\ldots \\ x &\equiv b_k \pmod{m_k} \end{aligned} \tag{3}$$

со една непозната и со заемно прости модули, т.е. $\text{NZD}(m_i, m_j) = 1$, за $i \neq j$. За да го решиме системо (3) ќе ја користиме следнава теорема.

Теорема (кинеска теорема за остатоци). Нека броевите M_s и $M_s^{'}$, $s = 1, 2, ..., k$ се определени со условите

$$m_1 m_2 ... m_k = M_s m_s, \; M_s M_s^{'} \equiv 1 \pmod{m_s} \tag{4}$$

и нека

$$x_0 = M_1 M_1^{'} b_1 + M_2 M_2^{'} b_2 + ... + M_k M_k^{'} b_k .$$

Тогаш општото решение на системот (3) е дадено со

$$x \equiv x_0 \pmod{m_1 m_2 ... m_k} . \tag{5}$$

Доказ. Нека x е определено со условот (5). Од условите (4) следува дека $m_s \mid M_j$, за $j \neq s$ и $M_s M_s^{'} b_s \equiv b_s \pmod{m_s}$, па затоа за секој $s = 1, 2, ..., k$ последователно добиваме

$$\begin{aligned} x &\equiv M_1 M_1^{'} b_1 + M_2 M_2^{'} b_2 + ... + M_k M_k^{'} b_k \pmod{m_1 m_2 ... m_k}, \\ x &\equiv M_1 M_1^{'} b_1 + M_2 M_2^{'} b_2 + ... + M_k M_k^{'} b_k \pmod{m_s}, \\ x &\equiv M_s M_s^{'} b_s \pmod{m_s}, \\ x &\equiv b_s \pmod{m_s}, \end{aligned}$$

што значи дека x е решение на системот (3). Понатаму, нека x' е друго решение на системот (3). Тогаш

$$x - x' \equiv 0 \pmod{m_i} \text{, за } i = 1, 2, ..., k ,$$

и како $\text{NZD}(m_i, m_j) = 1$, за $i \neq j$ од теорема 12.3 следува:

$$x \equiv x' \pmod{m_1 m_2 ... m_k} ,$$

што значи дека решението x е единствено по модул $m_1 m_2 ... m_k$. ♦

14.9. Пример. Ќе го решиме системот линеарни конгруентни равенки

$$x \equiv b_1 \pmod 4, \quad x \equiv b_2 \pmod 5, \quad x \equiv b_3 \pmod 7.$$

Имаме $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$ и притоа важи

$$35 \cdot 3 \equiv 1 \pmod 4, \quad 28 \cdot 2 \equiv 1 \pmod 5, \quad 20 \cdot 6 \equiv 1 \pmod 7,$$

па затоа

$$x_0 = 35 \cdot 3 b_1 + 28 \cdot 2 b_2 + 20 \cdot 6 b_3 = 105 b_1 + 56 b_2 + 120 b_3 ,$$

и општото решение на дадениот систем е

$$x \equiv 105b_1 + 56b_2 + 120b_3 \pmod{140}.$$

На пример, општото решение на системот

$$x \equiv 1 \pmod 4, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7$$

е дадено со

$$x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \pmod{140},$$

општото решение на системот

$$x \equiv 3 \pmod 4, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 6 \pmod 7$$

е дадено со

$$x \equiv 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \pmod{140}. \blacklozenge$$

14.10. Кинеската теорема за остатоци може да се воопшти за модули m_1, $m_2, ...m_k$ кои не се заемно прости. Имено, точна е следнава теорема чиј доказ нема да го презентираме.

Теорема. Системот линеарни конгруентни равенки (3) има решение ако и само ако $\text{NZD}(m_i, m_j) \mid (b_i - b_j)$ за секои $i, j = 1, 2, ..., k, i \neq j$. Ако системот (3) има решение, тогаш тоа е единствено по модул $\text{NZS}(m_1, m_2, ..., m_k)$. $\blacklozenge$

14.11. Пример. Решете го системот линеарни конгруентни равенки

$$x \equiv 5 \pmod 6,$$
$$x \equiv 3 \pmod{10},$$
$$x \equiv 8 \pmod{15}.$$

Решение. Очигледно дадениот систем ги исполнува условите од теорема 14.10, па затоа тој има решение. Решението на равенката

$$x \equiv 5 \pmod 6$$

има вид $5 + 6t, t \in \mathbf{Z}$. Со замена во втората равенка ја добиваме равенката

$$5 + 6t \equiv 3 \pmod{10},$$

која е еквивалентна со равенката $6t \equiv 8 \pmod{10}$, односно со равенката

$$3t \equiv 4 \pmod 5,$$

чие решение е $t \equiv 3 \pmod 5$. Оттука $t = 3 + 5u, u \in \mathbf{Z}$, а $x = 23 + 30u, u \in \mathbf{Z}$. Со замена во третата равенка ја добиваме равенката

$$23 + 30u \equiv 8 \pmod{15}$$

која е еквивалентна со равенкта $30u \equiv 0 \pmod{15}$ и чие решение е $u = 0 + v, v \in \mathbf{Z}$, па затоа решението на дадениот систем е

$$x = 23 + 30v, v \in \mathbf{Z}. \blacklozenge$$

15. МУЛТИПЛИКАТИВНИ ФУНКЦИИ

15.1. Дефиниција. За функцијата $f : \mathbf{N} \to \mathbf{Z}$ ќе велиме дека е *мултипликативна* ако

a) постои $n_0 \in \mathbf{N}$ таков што $f(n_0) \neq 0$ и

b) ако $\text{NZD}(m,n) = 1$, тогаш $f(mn) = f(m) f(n)$.

Ако условот б) е исполнет за секои $m, n \in \mathbf{N}$, заемно прости или не, тогаш ќе велиме дека функцијата f е *потполно мултипликативна*.

15.2. Теорема. Ако f е мултипликативна функција, тогаш функцијата g дефинирана со $g(n) = \sum_{d|n} f(d)$ е мултипликативна.

Доказ. Нека $m > 1, n > 1$ и $\text{NZD}(m,n) = 1$. Имаме

$$g(n)g(m) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = \sum_{d_1|m,\, d_2|n} f(d_1) f(d_2).$$

Ако $d_1 \mid m, d_2 \mid n$ и $\text{NZD}(m,n) = 1$, тогаш $\text{NZD}(d_1, d_2) = 1$, па затоа

$$g(n)g(m) = \sum_{d_1|m,\, d_2|n} f(d_1 d_2).$$

Понатаму, множеството од сите броеви $d_1 d_2$, каде d_1 и d_2 се позитивни делители на m и n соодветно, се совпаѓа со множеството од сите позитивни делители на mn и притоа не се повторува ниту еден делител на mn. Значи,

$$g(n)g(m) = \sum_{d_1|m,\, d_2|n} f(d_1 d_2) = \sum_{d|mn} f(d) = g(mn). \ \blacklozenge$$

15.3. Дефиниција. Нека $n \in \mathbf{N}$. Со $d(n)$ го означуваме *бројот од сите природни делители* на n. Со $\sigma(n)$ го означуваме *збирот од сите природни делители* на n.

15.4. Пример. Во следнава табела се презентирани вредностите на $d(n)$ и $\sigma(n)$, за $n = 1, 2, 3, \ldots, 19$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6	2
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20

Јасно, $d(n) = 2$ и $\sigma(n) = n + 1$ ако и само ако n е прост број. $\blacklozenge$

15.5. Теорема. Функциите $d(n)$ и $\sigma(n)$ се мултипликативни.

Доказ. Функцијата $f(n) = 1$ е мултипликативна. Бидејќи

$$d(n) = \sum_{d|n} 1 = \sum_{d|n} f(d),$$

од теорема 15.2 следува дека функцијата $d(n)$ е мултипликативна.

Функцијата $f(n)=n$ е мултипликативна. Бидејќи

$$\sigma(n)=\sum_{d|n} d=\sum_{d|n} f(d),$$

од теорема 15.2 следува дека функцијата $\sigma(n)$ е мултипликативна. ♦

15.5. Теорема. Ако $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$, тогаш

$$d(n)=(1+a_1)(1+a_2)...(1+a_k),\ \sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdot...\cdot\frac{p_k^{a_k+1}-1}{p_k-1}. \qquad (1)$$

Доказ. Ако p е прост број и $a\geq 1$, тогаш делители на p^a се $1, p, p^2$, ..., p^a, па затоа

$$d(p^a)=1+a \text{ и } \sigma(p^a)=1+p+p^2+...+p^a=\frac{p^{a+1}-1}{p-1}.$$

Сега равенствата (1) следуваат од мултипликативноста на функциите $d(n)$ и $\sigma(n)$. ♦

15.6. Пример. Колку делители има бројот 1200?

Решение. Го разложуваме бројот 1200 на прости множители, т.е. го запишуваме во каноничен вид:

$$1200=12\cdot10\cdot10=4\cdot3\cdot2\cdot5\cdot2\cdot5=2^4\cdot3^1\cdot5^2,$$

па од теорема 15.5 имаме $d(1200)=(4+1)\cdot(1+1)\cdot(2+1)=5\cdot2\cdot3=30$. Значи, бројот 1200 има вкупно 30 делители. ♦

15.7. Пример. Докажи дека $d(n)$ е непарен број ако и само ако n е полн квадрат.

Решение. На секој делител d на бројот n кој е помал од $\sqrt{n}$ му соодветствува делител $\frac{n}{d}$ кој е поголем од $\sqrt{n}$ и обратно. Значи, за секој број n, бројот на неговите делители кои се различни од $\sqrt{n}$ е парен број. Според тоа, ако бројот на делителите на n е непарен број, тогаш $\sqrt{n}$ е делител и обратно, ако $\sqrt{n}$ е делител, тогаш бројот на делителите на n е непарен број. ♦

15.8. Пример. Докажи дека:

а) $\sum_{d|n} d^k=\sum_{d|n}(\frac{n}{d})^k$ и б) $d(n)<2\sqrt{n}$.

Решение. а) Равенството следува од фактот дека, ако d е делител на бројот n, тогаш и $\frac{n}{d}$ е делител на бројот n, и обратно.

б) Ако n не е полн квадрат, тогаш неговите делители ги групираме во парови од видот $(d, \frac{n}{d})$, $d < \frac{n}{d}$, кои ги има помалку од $\sqrt{n}$. Ако n е полн квадрат, тогаш

$$d(n) \le 2(\sqrt{n}-1)+1 < 2\sqrt{n}\ . \blacklozenge$$

15.9. Пример. Докажи дека $\sqrt{n} \le \frac{\sigma(n)}{d(n)}$, $n>1$.

Решение. Од

$$\sigma(p^a) = \frac{p^{a+1}-1}{p-1} = 1+p+p^2+...+p^a \ge (a+1)p^{\frac{a}{2}} = d(p^a)p^{\frac{a}{2}}$$

добиваме $\frac{\sigma(p^a)}{d(p^a)} \ge \sqrt{p^a}$ и ако ја искористиме мултипликативноста на функциите $d(n)$ и $\sigma(n)$ добиваме $\sqrt{n} \le \frac{\sigma(n)}{d(n)}$. $\blacklozenge$

16. СИСТЕМИ ОСТАТОЦИ

16.1. Од својствата на конгруенциите следува дека релацијата "... е конгруентен со ... по модул m ..." е реалција за еквиваленција. Во однос на оваа релација множеството $\mathbf{Z}$ го разбиваме на m дисјунктни класи на еквиваленција. Во врска со претходно изнесеното ја имаме следнава дефиниција.

Дефиниција. Ако $x \equiv y (\mathrm{mod}\, m)$, тогаш y го нарекуваме *остаток* од x по модул m. Множеството $y_1, y_2, ..., y_m$ го нарекуваме *комплетен систем остатоци* по модул m ако за секој $x \in \mathbf{Z}$ постои еден и само еден y_i, $i = 1, 2, ..., m$ таков што $x \equiv y_i (\mathrm{mod}\, m)$.

16.2. Теорема. Секој цел број е конгруентен по модул m со еден и само еден од броевите $0, 1, 2, ..., m-1$.

Доказ. Нека a е цел број. Јасно, $a \equiv r \ (\mathrm{mod}\, m)$ за некој r, $0 \le r < m$. Да претпоставиме дека $a \equiv r \ (\mathrm{mod}\, m)$ и $a \equiv s \ (\mathrm{mod}\, m)$, за $0 \le r, s < m$. Тогаш, $s \equiv r \ (\mathrm{mod}\, m)$, т.е. $m \mid (s-r)$ и бидејќи $-m < s-r < m$, добиваме дека $s-r = 0$, т.е. $s = r$, што и требаше да се докаже. $\blacklozenge$

16.3. За секој $r \in \{0, 1, 2, ..., m-1\}$ со $C_m(r)$ да го означиме множеството од сите цели броеви кои се конгруентни со r по модул m. Од претходната теорема следува дека $C_m(r) \cap C_m(s) = \varnothing$ за $r \ne s$ и дека

$$C_m(0) \cup C_m(1) \cup ... \cup C_m(m-1) = \mathbf{Z}.$$

Дефиниција. Множеството $C_m(r)$ го нарекуваме *класа на конгруенции по модул* m.

Од претходно изнесеното следува дека множеството

$$\{a_0, a_1, ..., a_{m-1}\}$$

е комплетен систем на остатоци по модул m ако и само ако

$$a_r \in C_m(r) \text{ за } r = 0,1,...,m-1.$$

16.4. Теорема. Нека $\text{NZD}(a,m)=1$ и $S=\{a_1, a_2, ..., a_m\}$ е комплетен систем остатоци по модул m. Тогаш, за секој $b \in \mathbf{Z}$ множеството

$$T=\{aa_1+b, aa_2+b, ..., aa_m+b\}$$

е комплетен систем остатоци по модул m.

Доказ. Од $\text{NZD}(a,m)=1$ следува дека постојат $c,k \in \mathbf{Z}$ такви што $ac+mk=1$, што значи $ac \equiv 1 (\text{mod}\, m)$. Ако $d \in \mathbf{Z}$, тогаш постои единствен $t \in \{1,2,...,m\}$ таков да $c(d-b) \equiv a_t (\text{mod}\, m)$. Но, тогаш

$$d-b \equiv ac(d-b) \equiv aa_t (\text{mod}\, m), \text{ т.е. } d \equiv (aa_t+b)(\text{mod}\, m).$$

Ако $d \equiv (aa_i+b)(\text{mod}\, m)$, тогаш $(aa_i+b) \equiv (aa_t+b)(\text{mod}\, m)$, па затоа $aa_i \equiv aa_t (\text{mod}\, m)$. Но, $\text{NZD}(a,m)=1$ и од последната конгруенција и својствата на конгруенциите следува $a_i \equiv a_t (\text{mod}\, m)$, што значи $i=t$. Според тоа, T е комплетен систем остатоци по модул m. ♦

16.5. Од теоремите 16.2 и 16.4 следува дека *секое множество од* m *последователни цели броеви е комплетен систем на остатоци по модул* m. Така на пример, множеството $\{1, 2, ..., m\}$ е комплетен системи на остатоци по модул m. Ако m е непарен број, тогаш и множеството

$$\{-\tfrac{m-1}{2}, -\tfrac{m-1}{2}+1, ..., -1, 0, 1, ..., \tfrac{m-1}{2}\}$$

е комплетен систем на остатоци по модул m.

Фактот дека $\{0, 1, ..., m-1\}$ е комплетен систем на остатоци по модул m значи дека секоја комбинација на збирови, производи и разлики од овие броеви, по модул m е повторно некој од тие броеви. Ова доведува до таканаречената *модуларна аритметика*. Во следните две табели се дадени операциите собирање и множење по модул 5.

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a+b \pmod 5$

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$ab \pmod 5$

16.6. Пример. Од таблицата за множење по модул 5 следува дека $0^2, 1^2, 2^2, 3^2$ и 4^2 се конгруентни по модул 5 само со некој од броевите 0, 1 и 4. Но, 0, 1, 2, 3 и 4 е комплетен систем на остатоци по модул 5, па затоа квадрат на природен број при делење со 5 не дава остаток 2 и 3. ♦

16.7. Пример. Докажи дека за секој природен број n, бројот n^3+5n е делив со 6.

Решение. Комплетен систем на остатоци по модул 6 е 0, 1, 2, 3, 4 и 5. Според тоа, доволно е да испитаме дали n^3+5n е делив со 6 за $n=0, 1, 2, 3, 4, 5$. При множење со модул 6 имаме

$$0^3 \equiv 0, \quad 1^3 \equiv 1, \quad 2^3 \equiv 2, \quad 3^3 \equiv 3, \quad 4^3 \equiv 4, \quad 5^3 \equiv 5 .$$

Според тоа,

$$n^3+5n \equiv n+5n \equiv 6n \equiv 0 \pmod 6 . \ ♦$$

16.8. Дефиниција. Нека $S=\{a_1, a_2, ..., a_m\}$ е комплетен систем остатоци по модул m и нека $S' \subseteq S$ се состои од сите броеви од S кои се заемно прости со m. Тогаш, S' го нарекуваме *редуциран систем остатоци* по модул m.

16.9. Теорема. Ако $\text{NZD}(a,m)=1$ и S' е редуциран систем остатоци по модул m, тогаш a е конгруентен со единствен број од S'. Ако S'' е друг редуциран систем остатоци по модул m, тогаш S' и S'' имаат ист број елементи.

Доказ. Од дефиниција 16.8 следува дека $S' \subseteq S=\{a_1, a_2, ..., a_m\}$, каде S е комплетен систем остатоци по модул m. Затоа постои единствен број $b \in S$ таков да $a \equiv b \pmod m$. Од $\text{NZD}(a,m)=1$ следува дека и $\text{NZD}(b,m)=1$, па значи $b \in S'$. Јасно, бидејќи b е единствен во S тој е единствен и во S'.

Нека S'' е друг редуциран систем остатоци по модул m. Секој елемент од S'' е конгруентен со точно еден елемент од S', а бидејќи два различни елементи од S' не се конгруентни, добиваме дека бројот на елементите на S' е поголем или еднаков со бројот на елементите на S''. Ако ги замениме местата на S'' и S' добиваме дека бројот на елементите на S'' е поголем или еднаков на бројот на елементите на S'. Значи, S' и S'' имаат ист број елементи. ♦

16.10. Теорема. Ако $m>1$ и S' е редуциран систем остатоци по модул m, тогаш бројот на сите природни броеви помали или еднакви на m и заемно прости со m е еднаков на бројот на елементите на S'.

Доказ. Бидејќи $S=\{1, 2, ..., m\}$ е комплетен систем остатоци по модул m, добиваме дека

$$S'=\{k \mid k \in S, \ \text{NZD}(m,k)=1\}$$

е редуциран систем остатоци по модул m. Сега тврдењето следува од теорема 16.9. ♦

17. ОЈЛЕРОВА ФУНКЦИЈА

17.1. Дефиниција. Функцијата $\varphi : \mathbf{N} \to \mathbf{N}$, каде $\varphi(m)$, $m \in \mathbf{N}$ е еднаков на бројот на елементите на произволен редуциран систем остатоци по модул m ја нарекуваме *Ојлерова функција*.

17.2. Пример. а) Бидејќи за секој прост број p сите елементи на множеството $\{1, 2, ..., p-1, p\}$, освен p, се заемно прости со p добиваме $\varphi(p) = p - 1$.

б) Вредностите на функцијата φ за првите 17 природни броеви се дадени во следнава табела:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Забележуваме дека $\varphi(12) = 4 = 2 \cdot 2 = \varphi(3)\varphi(4)$, што укажува на мултипликативноста на функцијата φ, која покасно ќе ја докажеме. ♦

17.3. Теорема. Ако $\text{NZD}(a, m) = 1$ и $S' = \{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m, тогаш и множеството

$$T' = \{aa_1, aa_2, ..., aa_{\varphi(m)}\}$$

е редуциран систем остатоци по модул m.

Доказ. Од дефиниција 16.8 имаме $S' \subseteq S = \{a_1, a_2, ..., a_m\}$, каде S е комплетен систем остатоци по модул m. Според теорема 16.4 при $b = 0$ множеството $T = \{aa_1, aa_2, ..., aa_m\}$ е комплетен систем остатоци по модул m. Сите броеви aa_j, $j = 1, 2, ..., m$ се различни меѓу себе, па затоа доволно е да докажеме дека $\text{NZD}(aa_j, m) = 1$, за $j = 1, 2, ..., \varphi(m)$. Последното тврдење следува од равенствата

$$\text{NZD}(a, m) = \text{NZD}(a_j, m) = 1, \text{ за } j = 1, 2, ..., \varphi(m). \ ♦$$

17.4. Теорема. Ако a и p се природни броеви и p е прост број, тогаш

$$\varphi(p^a) = p^a(1 - \tfrac{1}{p}).$$

Доказ. Единствени броеви меѓу 1 и p^a кои не се заемно прости со p се броевите што се деливи со p, а такви се: $p, 2p, 3p, ..., p^{a-1}p$ и нив ги има p^{a-1}. Според тоа,

$$\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \tfrac{1}{p}). \ ♦$$

17.5. Теорема. Ојлеровата функција φ е мултипликативна.

Доказ. Јасно $\varphi(1) = 1 \neq 0$. Нека $\text{NZD}(m, n) = 1$. Во следнава таблица ќе го определиме бројот $\varphi(mn)$ на елементите кои се заемно прости со mn. Имаме

$$\begin{array}{cccccc} 1 & 2 & 3 & \ldots & k & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & n+k & \ldots & 2n \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \ldots & (m-1)n+k & \ldots & mn \end{array}$$

Да забележиме дека ако за фиксирано k и за некој $i \in \{0,1,2,\ldots,m-1\}$ бројот $in+k$ е заемно прост со n, тогаш и за секој $j \in \{0,1,2,\ldots,m-1\}$ бројот $jn+k$ е заемно прост со n. Со други зборови, во било која колона на дадената таблица или сите елементи се заемно прости со n или ниту еден не е заемно прост со n. Колони во кои сите елементи се заемно прости со n се $\varphi(n)$. Бидејќи $\mathrm{NZD}(m,n)=1$, во секоја колона има $\varphi(m)$ елементи кои се заемно прости со m. Затоа вкупниот број елементи во табелата кои се заемно прости со m и n, односно со mn, е еднаков на $\varphi(m)\varphi(n)$, од што следува $\varphi(m)\varphi(n)=\varphi(mn)$. ♦

17.6. Пример. Бидејќи $660=5\cdot 11\cdot 12$, од претходната теорема следува

$$\varphi(660)=\varphi(5)\varphi(11\cdot 12)=\varphi(5)\varphi(11)\varphi(12)=4\cdot 10\cdot 4=160\,.\ \blacklozenge$$

17.7. Теорема. Ако $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ е каноничниот запис на број n, тогаш

$$\varphi(n)=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\ldots\left(1-\tfrac{1}{p_k}\right).$$

Доказ. Непосредно следува од теоремите 17.4 и 17.5. ♦

17.8. Последица. Ако $n>2, n\in\mathbf{N}$, тогаш $\varphi(n)$ е парен број.

Доказ. Нека $n=2^k m$, $k>1$ и m е непарен број. Тогаш

$$\varphi(n)=\varphi(2^k m)=\varphi(2^k)\varphi(m)=2^{k-1}\varphi(m)\,,$$

па затоа $\varphi(n)$ е парен број. Понатаму, ако $n=p^k m$, p е непарен прост број и $\mathrm{NZD}(p,m)=1$, тогаш

$$\varphi(n)=\varphi(p^k m)=\varphi(p^k)\varphi(m)=(p^k-p^{k-1})\varphi(m)=p^{k-1}(p-1)\varphi(m)\,,$$

па затоа $\varphi(n)$ е парен број. ♦

17.9. На крајот од оваа точка ќе докаѓеме уште едно интересно својство на Ојлеровата функција.

Теорема (Гаус). Ако $n\in\mathbf{N}$, тогаш $\sum_{d\mid n}\varphi(d)=n$, при што сумирањето е по сите позитивни делители на n.

Доказ. Нека d е позитивен делител на n и со $C(d)$ да го означиме множеството од сите природни броеви $m, m\le n$ такви што $\mathrm{NZD}(m,n)=d$. Ако $d\neq d'$, тогаш бидејќи цел број m со бројот n може да има најмногу еден најго-

лем заеднички делител добиваме дека множествата $C(d)$ и $C(d')$ немаат заеднички елементи. Понатаму, од теорема 5.10 множеството $C(d)$ е еднакво на множеството од сите природни броеви $m, m \le n$ такви што $\text{NZD}(\frac{m}{d}, \frac{n}{d}) = 1$, што значи дека тоа ги содржи позитивните цели броеви $\frac{m}{d}$ кои се помали или еднакви на $\frac{n}{d}$ и се заемно прости со $\frac{n}{d}$, па затоа бројот на елементите на множеството $C(d)$ е еднаков на $\varphi(\frac{n}{d})$. Но, унијата на сите овие множества е еднаква на множеството природни броеви помали или еднакви на n добиваме $\sum_{d|n} \varphi(\frac{n}{d}) = n$. Конечно, бидејќи за секој d делител на n бројот $\frac{n}{d}$ е делител на n и обратно, од последното равенство следува $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$, што и требаше да се докаже. ♦

18. ТЕОРЕМА НА ОЈЛЕР

18.1. Теорема. (Ојлер). Ако $\text{NZD}(a, m) = 1$, тогаш

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

Доказ. Нека $\{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m. Според теорема 17.3 и $\{aa_1, aa_2, ..., aa_{\varphi(m)}\}$ е редуциран систем остатоци по модул m. Значи, за секој a_i постои еден и само еден a_j така што $a_i \equiv aa_j (\text{mod}\, m)$. Ако ги помножиме сите конгруенции од овој вид, ги има точно $\varphi(m)$, добиваме

$$a^{\varphi(m)} a_1 a_2 ... a_{\varphi(m)} \equiv a_1 a_2 ... a_{\varphi(m)} (\text{mod}\, m).$$

Бидејќи $\text{NZD}(a_i, m) = 1$, за $i = 1, 2, ..., \varphi(m)$, од последната конгруенција добиваме $a^{\varphi(m)} \equiv 1 (\text{mod}\, m)$. ♦

18.2. Пример. Докажи дека $2^{340} - 1$ не е прост број.

Решение. Од теоремата на Ојлер следува

$$2^{10} = 2^{\varphi(11)} \equiv 1 (\text{mod} 11).$$

Значи,

$$2^{340} = (2^{10})^{34} \equiv 1^{34} (\text{mod} 11), \text{ т.е. } 11 | (2^{340} - 1).$$

Според тоа, $2^{340} - 1$ не е прост број. ♦

18.3. Пример. Докажи дека за секој природен број n бројот $N = 1 + 2^{2 \cdot 5^n}$ се дели со 5^{n+1}.

Решение. Од теоремата на Ојлер имаме

$$2^{4\cdot 5^n} \equiv 2^{\varphi(5^{n+1})} \equiv 1 \pmod{5^{n+1}}.$$

Значи, 5^{n+1} е делител на производот $(2^{2\cdot 5^n}+1)(2^{2\cdot 5^n}-1)$. Двата множители во последниот производ се заемно прости и $5 \nmid (2^{2\cdot 5^n}-1)$ (провери!), па затоа

$$5^{n+1} \mid (2^{2\cdot 5^n}+1). \blacklozenge$$

18.4. Теорема. (Ферма). Ако p е прост број и $\text{NZD}(a, p)=1$, тогаш

$$a^{p-1} \equiv 1 \pmod{p}.$$

Доказ. Од $\text{NZD}(a, p)=1$, според теорема 18.1 добиваме

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

и како $\varphi(p)=p-1$ имаме $a^{p-1} \equiv 1 \pmod{p}$. $\blacklozenge$

18.5. Последица. Ако p е прост број, тогаш за секој цел број a важи

$$a^p \equiv a \pmod{p}. \blacklozenge$$

18.6. Пример. Ако p и q се различни прости броеви, тогаш

$$p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}.$$

Докажи!

Решение. Од теоремата на Ферма имаме $q \mid (p^{q-1}-1)$ и $p \mid (q^{p-1}-1)$. Според тоа, $pq \mid (p^{q-1}-1)(q^{p-1}-1)$, т.е.

$$pq \mid (p^{q-1}q^{p-1}-p^{q-1}-q^{p-1}+1). \tag{1}$$

Бидејќи p и q се прости броеви имаме

$$pq \mid p^{q-1}q^{p-1}. \tag{2}$$

Од (1) и (2) непосредно следува дека $pq \mid (p^{q-1}+q^{p-1}-1)$, т.е.

$$p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}. \blacklozenge$$

18.7. Теорема. (Вилсон). Ако p е прост број, тогаш

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказ. За $p=2$ и $p=3$ непосредно се проверува дека тврдењето важи. Нека претпоставиме дека $p \geq 5$.

Да забележиме дека $1 \equiv 1 \pmod{p}$ и $p-1 \equiv -1 \pmod{p}$. За секој j, $2 \leq j \leq p-2$ важи $\text{NZD}(j, p)=1$, па затоа постои еден и само еден i така што

$ij \equiv 1 \pmod{p}$ и $0 \le i \le p-1$. Очигледно $i \notin \{0,1,p-1\}$, па затоа за секој j, $2 \le j \le p-2$ постои еден и само еден i така што $ij \equiv 1 \pmod{p}$ и $2 \le i \le p-2$. Притоа $i \ne j$, бидејќи за секој $j, 2 \le j \le p-2$ имаме

$$\text{NZD}(j-1, p) = \text{NZD}(j+1, p) = 1$$

и затоа

$$j^2 - 1 = (j-1)(j+1) \not\equiv 0 \pmod{p}.$$

Така, броевите $2,3,\ldots,p-2$ ги поделивме на $\frac{p-3}{2}$ дисјунктни двоелементни множества $\{i, j\}$ за кои важи $ij \equiv 1 \pmod{p}$. Ако ги помножиме овие конгруенции добиваме

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$$

и како $1 \equiv 1 \pmod{p}$ и $p-1 \equiv -1 \pmod{p}$ од последните три конгруенции следува $(p-1)! \equiv -1 \pmod{p}$. ♦

18.8. Пример. Докажи дека, ако $(m-1)! \equiv -1 \pmod{m}$, тогаш m е прост број.

Решение. Нека m не е прост број, т.е. нека $m = ks, 1 < k < m$. Тогаш, k е делител на $(m-1)!$ и како k е делител на $(m-1)!+1$ добиваме дека k е делител на 1, што е противречност. ♦

19. РЕД НА ЦЕЛ БРОЈ

19.1. Обратното тврдење на теоремата на Ферма не важи. На пример, $3^{90} \equiv 1 \pmod{91}$, меѓутоа $91 = 7 \cdot 13$ е сложен број. Од друга страна ако p е природен број и $0 < a < p$ е таков што $a^{p-1} \not\equiv 1 \pmod{p}$, тогаш p не е прост број. Затоа, теоремата на Ферма содржи парцијален тест дали бројот е прост или не, т.е. може да се искористи да се докаже дека бројот p не е прост без наоѓање на нетривијален делител на p. Во натамошните разгледувања ќе се осврнеме на конгруенцијата $a^k \equiv 1 \pmod{n}$.

19.2. Дефиниција. Нека n е природен број и a е цел број таков што НЗД$(a,n) = 1$. *Ред на бројот* a по модул n, во ознака $\text{ord}_n a$, го нарекуваме најмалиот природен број k таков што $a^k \equiv 1 \pmod{n}$.

19.3. Теорема. Нека n е природен број, НЗД$(a,n) = 1$ и нека $k = \text{ord}_n a$. Тогаш

а) ако $a^m \equiv 1 \pmod{n}$, $m \in \mathbf{N}$, тогаш $k \mid m$

б) $k \mid \varphi(n)$

в) за природните броеви r и s важи $a^r \equiv a^s \pmod{n}$ ако и само ако $r \equiv s \pmod{k}$

г) $a^i \not\equiv a^j \pmod{k}$ за $i, j \in \{1,2,...,k\}$, $i \neq j$

д) ако m е природен број тогаш редот на a^m по модул n е еднаков на $\frac{k}{\text{NZD}(k,m)}$

ѓ) редот за a^m по модул n е k ако и само ако m и k се заемно прости броеви.

Доказ. а) Ако $a^m \equiv 1 \pmod{n}$ за некој природен број m, тогаш од $m = kq + r, 0 \leq r < k,$ добиваме

$$a^m = a^{kq+r} = a^{kq} a^r$$

па затоа $a^r \equiv 1 \pmod{n}$. Последното противречи на фактот дека редот на a по модул n е k, освен во случај кога $r = 0$. Значи, $m = kq$, т.е. $k \mid m$.

б) Според теоремата на Ојлер имаме $a^{\varphi(n)} \equiv 1 \pmod{n}$ па од тврдењето под а) имаме $k \mid \varphi(n)$.

в) Нека $r > s$. Бидејќи a и n се заемно прости добиваме $a^r \equiv a^s \pmod{n}$ ако и само ако $a^{r-s} \equiv 1 \pmod{n}$, па од а) следува $k \mid (r-s)$ т.е. $r \equiv s \pmod{k}$.

г) Непосредно следува од тврдењето под в)

д) Нека $d = \text{NZD}(k,m)$. Тогаш $k = ud$ и $m = vd$, па затоа

$$(a^m)^{\frac{k}{\text{NZD}(k,m)}} = (a^m)^{\frac{ud}{d}} = a^{mu} = a^{uvd} = a^{(ud)v} = a^{kv} \equiv 1 \pmod{n}$$

Нека претпоставиме t е таков што $(a^m)^t \equiv 1 \pmod{n}$. Тогаш

$$a^{mt} \equiv 1 \pmod{n}$$

па од $\text{ord}_n a = k$ и тврдењето под а) следува $k \mid mt$. Затоа, $ud \mid vdt$ и како u и v се заемно прости добиваме $u \mid t$. Бидејќи

$$k = ud, u = \frac{k}{d} = \frac{k}{\text{NZD}(k,m)}$$

го дели произволниот број t со својството $(a^m)^t \equiv 1 \pmod{n}$ од дефиницијата на редот следува дека $\frac{k}{\text{NZD}(k,m)}$ е ред за a^m по модул n.

ѓ) Непосредно следува од тврдењето под д). ♦

19.4. Пример. Од $n = 14 = 2 \cdot 7$ следува дека $\varphi(n) = (2-1)(7-1) = 6$. Примарниот редуциран систем на остатоци за $n = 14$ е множеството $\{1,3,5,9,11,13\}$.

Да ја разгледаме следната табела во која се дадени примарните редуцирани степени на бројот $a=5$:

m	1	2	3	4	5	6	7	8	9	10	11	12	13
a^m	5	11	13	9	3	1	5	11	13	9	3	1	5

Од која согледуваме дека после $m=6$ имаме циклично повторување. Затоа $k=\text{ord}_{14}5=6.$ За $m=12$ имаме $a^m=5^{12}\equiv 1(\text{mod}14)$ и $k\,|\,m,$ што е согласно со тврдењето под а) од претходната теорема.

Проверете дали важат останатите тврдења од оваа теорема. ♦

19.5. Теорема. Ако $\text{NZD}(a,n)=\text{NZD}(b,n)=1$ и $\text{ord}_n a$ е заемно прост со $\text{ord}_n b$ тогаш

$$\text{ord}_n(ab)=\text{ord}_n a\bullet\text{ord}_n b.$$

Доказ. Нека $\text{ord}_n a=R$ и $\text{ord}_n b=S.$ Тогаш

$$(ab)^{RS}=a^{RS}b^{RS}=(a^R)^S(b^S)^R\equiv 1\cdot 1\equiv 1(\text{mod}\,n)$$

Според теорема 19.3. а) имаме $\text{ord}_n(ab)\,|\,RS$. Бидејќи R и S се заемно прости, постојат цели броеви r и s за кои е

$$\text{ord}_n(ab)=rs, rw=R \text{ и } sx=S.$$

Ќе докажеме дека $r=R$ и $s=S$. Од дефиницијата на r и s имаме

$$(ab)^{rs}=a^{rs}b^{rs}\equiv 1(\text{mod}\,n)$$
$$(a^{rs}b^{rs})^w\equiv 1(\text{mod}\,n)$$
$$(a^{rw})^s(b^{rw})^s\equiv 1(\text{mod}\,n)$$

Меѓутоа, бидејќи $a^{rw}\equiv 1(\text{mod}\,n)$ и $rw=R$ имаме

$$b^{Rs}\equiv 1(\text{mod}\,n)$$

Од теорема 19.3 а) имаме $S=\text{ord}_n b\,|\,Rs$ и како $\text{NZD}(R,S)=1$ следува $S\,|\,s.$ Но, $s\,|\,S$, па затоа $S=s$. Аналогно се докажува дека $r=R$, па затоа

$$\text{ord}_n(ab)=RS=\text{ord}_n a\cdot\text{ord}_n b\,.\ \blacklozenge$$

19.6. Пример. Нека $n=58$ и $a=25$. Имаме

$$\varphi(58)=\varphi(2\cdot 29)=(2-1)(29-1)=28=2^2\cdot 7\,.$$

Единствени позитивни делители на $2^2\cdot 7$ се $1,2,4,7,14$ и 28. Следнава табела лесно се пресметува (конгурентност на степените на 25 по модул 58)

m	1	2	4	7
25^m	25	45	53	1

Според тоа $\text{ord}_{58}25=7$ и не треба да се проверува за 14 и 28. ♦

19.7. Теорема (Лукас). Ако n е природен број и ако постои цел број a таков што

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n)$$

и

$$a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$$

за секој прост делител p на $n-1$, тогаш n е прост број.

Доказ. Од $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ следува $\mathrm{NZD}(a,n)=1$ и од теорема 19.3 а) имаме $\mathrm{ord}_n a \mid (n-1)$. Ако p е прост број таков што $p \mid (n-1)$, тогаш од $a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$ следува дека $\mathrm{ord}_n a \nmid \frac{n-1}{p}$. Навистина, ако $\mathrm{ord}_n a \mid \frac{n-1}{p}$, тогаш имаме $a^{\frac{n-1}{p}} \equiv 1 (\mathrm{mod}\, n)$, што е противречност. Меѓутоа, $\mathrm{ord}_n a \mid (n-1)$ и $\mathrm{ord}_n a \nmid \frac{n-1}{p}$, за секој p кој е делител на $n-1$ повлекува $\mathrm{ord}_n a = n-1$. Според теорема 19.3 б) имаме $\varphi(n) = n-1$, што значи дека бројот n е прост. ♦

19.8. За да ја користиме теоремата на Лукас за тестирање дали бројот n е прост, треба да можеме бројот $n-1$ да го разложиме на прости множители, што понекогаш е доста тешко. Уште повеќе треба да најдеме и соодветен цел број a.

20. МЕТОД НА ФЕРМА ЗА ФАКТОРИЗАЦИЈА

20.1.Теорема. Непарниот природен број $n>1$ не е прост ако и само ако постојат ненегативни цели броеви p и q такви што

$$n = p^2 - q^2,\ p-q>1.$$

Доказ. Нека постојат ненегативни цели броеви p и q такви што $n = p^2 - q^2,\ p-q>1$. Тогаш $p+q>1$ и од

$$n = p^2 - q^2 = (p-q)(p+q)$$

следува дека n не е прост број.

Обратно, ако $n = rs, r \geq s > 1$, тогаш n може да се запише како $(\frac{r+s}{2})^2 - (\frac{r-s}{2})^2$. Бидејќи n е непарен, добиваме дека r и s се непарни и затоа $\frac{r+s}{2}$ и $\frac{r-s}{2}$ се природни броеви. Сега за $p = \frac{r+s}{2}$ и $q = \frac{r-s}{2}$ добиваме $n = p^2 - q^2$ и $p-q = s > 1$. ♦

20.2. Претходната теорема го дава таканаречениот *Ферматов метод за факторизација*. Притоа определуваме цели броеви p и q за кои важи

$n = p^2 - q^2$, т.е. $p^2 = q^2 + n$. Понатаму, во равенството $p^2 = q^2 + n$ ставаме $q = 1, 2, 3, ..., \frac{n-1}{2}$ се додека не добиеме полн квадрат. Овде треба да забележиме дека и не треба да ги проверуваме сите вредности на q меѓу 1 и $\frac{n-1}{2}$, освен во случајот кога n е прост број.

На пример да провериме дали $n = 527$ е прост број. Нека $q = 1, 2, 3, ..., \frac{n-1}{2}$. Имаме

q	$n + q^2$
1	527+1=528
2	527+4=531
3	527+9=536
4	527+16=543
5	527+25+552
6	527+36=563
7	527+49=576= 24^2

Според тоа, $527 = 24^2 - 49 = 24^2 - 7^2 = 17 \cdot 31$ е сложен број.

ЗАДАЧИ

1. Докажи дека $12 \mid (3^n + 3^{n+1})$, за секој $n \in \mathbf{N}$.
2. Докажи дека разликата на произволен четирицифрен број и бројот запишан со истите цифри, но во обратен редослед е делива со 9.
3. Најди ги сите природни броеви n за кои вредноста на дропката $\frac{24}{3n-4}$ исто така е природен број.
4. Најди ги сите цели вредности на бројот a за кои изразот $\frac{2a-5}{a+2}$ е цел број.
5. За кои вредности на n, изразот $\frac{n^2+1}{n+2}$ е цел број?
6. На неколку листа хартија напишани се броевите +1 и -1, на секој лист по еден број. Збирот на сите броеви е 0, а нивниот производ е 1. Докажи дека бројот на листовите е делив со 4.
7. Најди го најголемиот природен број кој го задоволува условот: кои било две соседни цифри формираат број делив со 23.
8. Докажи дека за секој $n \in \mathbf{N}$,

   а) $(5n+3)^2 - 4$ е делив со 5; б) $(4n+5)^2 - 9$ е делив со 8.
9. Докажи дека:

   а) $17 \mid (6^{100} - 19^{50})$, б) $11 \mid (3^{30} - 2^{40})$
10. Докажи дека:

а) $2+2^2+2^3+...+2^{99}$ е делив со 7;

б) $6+6^2+6^3+...+6^{111}$ е делив со 43.

11. Докажи дека збирот:
а) $1+2+3+4+...+107+108+109+110$ се дели со 37.
б) $1+2+3+4+...+997+998+999+1000$ се дели со броевите 7, 11 и 13.

12. а) Докажи дека: $x^n-1=(x-1)(x^{n-1}+x^{n-2}+...+x^2+x+1)$.

б) Докажи дека: $7\mid(8^n-14n-1)$, за секој $n\in\mathbf{N}$.

в) Докажи дека: $19\mid(7\cdot5^{2n}+12\cdot6^n)$, за секој $n\in\mathbf{N}$.

13. Ако еден број се подели со 63, се добива количник n и остаток 59. Колку ќе биде остатокот при делењето на тој број со 21?

14. Најди четирицифрен број кој поделен со 131 дава остаток 112, а поделен со 132 дава ист количник и остаток 98.

15. Докажи дека производот на два последователни природни броеви е делив со 2.

16. Докажи дека квадратот на секој непарен природен број може да се запише во вид $8p+1,\ p\in\mathbf{N}_0$.

17. Докажи дека збирот на кубовите на три последователни природни броеви е делив со 9.

18. Докажи дека $6\mid(n^3-n)$, за секој $n\in\mathbf{N}$.

19. Докажи дека $3\mid n(2n^2+1)$, за секој $n\in\mathbf{N}$.

20. Докажи дека $6\mid(n^3+3n^2+2n+6)$, за секој $n\in\mathbf{N}$.

21. Докажи дека:
а) $5\mid(2^{2000}-1)$; б) $5\nmid(n^2-7)$, за секој $n\in\mathbf{N}$.

22. Докажи дека:
а) $81\mid(10^{1990}-10)$; б) $81\mid\underbrace{111...111}_{81\text{ единица}}$.

23. Ако n е природен број, тогаш и $(10^n-4):6$ е природен број. Докажи!

24. Ако n е природен број, тогаш и $(10^n+35):45$ е природен број. Докажи!

25. Дали $8\mid a$, каде што $a=\underbrace{4444...4444}_{2002\text{ четворки}}$.?

26. На местото на ѕвездичката, во бројот 63145*, стави соодветна цифра така што при делење на тој број со 3 и со 5 да се добијат еднакви остатоци. Најди ги сите решенија.

27. На местото на ѕвездичките стави цифри така што бројот 4*1* да биде делив со 12. Најди ги сите решенија.

28. На местото на ѕвездичките стави цифри така што бројот 81** биде делив со 90. Најди ги сите решенија.
29. Телефонскиот број на Самоил се состои од два трицифрени броја, од кои секој е делив со 45, а средната цифра им е 8. Најди го бројот на телефонот, ако првиот дел од бројот е помал од вториот.
30. Докажи дека четирицифрениот број $\overline{abcd}$ е делив со 11 ако и само ако бројот $a-b+c-d$ е делив со 11.
31. Кои од броевите
    а) 1324567396; б) 2619876347; в) 434548363235
    е делив со 11?
32. На местото на ѕвездичките, во бројот 1988**, стави цифри така што добиениот број да биде делив со 33. Најди ги сите решенија.
33. Најди НЗД за броевите: а) 135 и 180; б) 63, 135 и 315.
34. Нека a и b се два последователни природни броеви и нека n е произволен природен број. Докажи дека $\text{NZD}(an+b, bn+a)$ е непарен број.
35. Дали $21n+4$ и $14n+3$ имаат заеднички делител различен од 1, ако n е природен број.
36. Докажи дека се заемно прости броевите $9n+31$ и $2n+7$ за секој $n \in \mathbf{N}$.
37. Ако a и b се заемно прости броеви, тогаш $\text{NZD}(a+b, a-b) \mid 2$. Докажи!
38. Збирот на два природни броја е 150, а нивниот најголем заеднички делител е 30. Кои се тие броеви?
39. Производот на два природни броја е 8400, а нивниот најголем заеднички делител е 20. Кои се тие броеви?
40. Со помош на Евклидовиот алгоритам најди НЗД за броевите:
    а) 1001 и 7655; б) 72135 и 45360
    а потоа запиши го $\text{NZD}(1001, 7655)$ во обликот $1001x+7655y$.
41. Најди два различни парови цели броеви x и y такви што:
    а) $\text{NZD}(6,4) = 6x+4y$; б) $\text{NZD}(7,8) = 7x+8y$
42. Ако $\text{NZD}(a,c)=1$ и $\text{NZD}(b,c)=1$, тогаш $\text{NZD}(ab,c)=1$. Докажи!
43. Ако $\text{NZD}(a,c)=1$, тогаш $\text{NZD}(ab,c) \mid b$. Докажи!
44. Ако $\text{NZD}(a,b)=1$, тогаш $\text{NZD}(ac,b) \mid \text{NZD}(c,b)$. Докажи!
45. Нека a, b и c се природни броеви такви што $\text{NZD}(a,b,c)=1$ и $c=\frac{ab}{a-b}$. Докажи дека $a-b$ е квадрат на природен број.
46. Пресметај:
    а) $\text{NZS}(152, 285)$; б) $\text{NZS}(10n+9, n+1)$
47. Најди ги природните броеви x и y ако:
    а) $\text{NZD}(x,y)=4$ и $\text{NZS}(x,y)=96$; б) $xy=20$ и $\text{NZS}(x,y)=10$.
48. Пресметај:

а) $\text{NZD}(\text{NZD}(a,b),\text{NZS}(a,b))$; б) $\text{NZD}(ab,\text{NZS}(a,b))$.

49. Најди ги сите природни трицифрени броеви кои при делење со 7 даваат остаток 2, при делење со 9 даваат остаток 4 и при делење со 12 даваат остаток 7.
50. Никола има толку денари да може да ги подели на делови така, што секој дел да има или 18, или 24, или 30 денари и секогаш да му остане по еден денар. Најди колку најмалку пари треба да има Никола.
51. На бројот 1972 допиши му оддесно четири цифри така што добиениот осумцифрен број да биде делив со 5, 7 и 72.
52. Методиј ги запишал по ред природните броеви од 1 до 1000. Прво ги прецртал броевите кои се деливи со 4 и броевите кои се деливи со 6, а потоа броевите кои се деливи со 10. Колку броеви останале непрецртани?
53. Докажи дека:
    a) збирот на кои било пет последователни природни броеви не може да биде прост број.
    b) при делење на произволен прост број p со 30, остатокот е или прост број или бројот 1.
54. Ако броевите p, $p+5$ и $p+9$ се прости, тогаш $p=2$. Докажи!
55. Докажи дека:

    а) за секој $n>1$ секој број од видот n^4+4 е сложен;

    б) бројот $2^{10}+5^{12}$ е сложен.
56. За кои природни броеви p, броевите p и $3p^2+1$ се прости?
57. За кои природни броеви p, бројот p^4+p^2+1 е прост?
58. Ако p е прост број, тогаш бројот $p^{2002}-1$ е сложен. Докажи!
59. Докажи дека ако еден од броевите 2^n-1 и 2^n+1, каде што $n>2$ е прост број, тогаш вториот број е сложен.
60. Докажи дека ако p и $8p^2+1$ се прости броеви, тогаш и бројот $8p^2-1$ е прост.
61. Најди ги сите прости броеви p такви што $2p^2+1=k^5$ за некој $k\in\mathbf{N}$.
62. Најди прости броеви p, q и r за кои $p=q^3-r^3$.
63. За кои прости броеви p се прости и броевите:

    а) $p+2$ и p^2+2; б) $p+10$ и $p+20$; в) $p+10$ и $p+14$.
64. Разложи ги на множители броевите:
    а) 6600; б) 2618.
65. Со кој најмал природен број n треба да се помножи бројот 5400 за да се добие точен квадрат?
66. Најди ги сите природни броеви чиј производ на цифри е еднаков на
    а) 234; б) 105.

67. Користејќи го каноничниот запис на природните броеви, најди НЗД и НЗС за броевите a и b, ако:
    а) $a=2520$, $b=39600$; б) $a=6600, b=2618$.

68. Која од наведените Диофантови равенки има решение:
    а) $3x+7y=2002$; б) $30x+25y=174$; в) $3x+15y=1234$.

69. Реши ги Диофантовите равенки:
    а) $48x+7y=5$; б) $11x+30y=31$; в) $21x-12y=72$.

70. Продавачот Арсо треба да наполни 99 кг брашно во кеси од по 2, 3 и 5 кг. По колку кеси од секоја тежина ќе наполни Арсо, ако вкупно наполнил 22 кеси?

71. Пекарот Теодор треба да направи 100 векни леб тешки 5, 3 и 0,5 кг. Колку од кои векни леб треба да направи Теодор ако нивната вкупна тежина е 100 кг.

72. Збирот на цифрите на бројот X е Y, а збирот на цифрите на бројот Y е Z. Ако $X+Y+Z=60$, најди го бројот X.

73. Во множеството на целите броеви реши ги Диофантовите равенки:
    а) $x^2+2x+13=y^2$; б) $x^2-7xy+12y^2=7$.

74. Во множеството на целите броеви реши ги Диофантовите равенки:
    а) $x^2y=y^3+10$; б) $y^4+x=xy+9$.

75. Во множеството на природните броеви реши ги Диофантовите равенки:
    а) $x!+2y=5555$; б) $5^x+6^y=1234567$.

76. Во множеството на целите броеви реши ги Диофантовите равенки:
    а) $x^2+y^2+z^2=1988$; б) $x^2+4y^2=1988$.

77. а) Докажи дека квадратот на секој цел број е конгруентен со 0 или 1 по модул 4.
    б) Докажи дека квадратот на секој цел број е конгруентен со 0, 1 или 4 по модул 8.

78. На која цифра завршува бројот:
    а) 6^{811}; б) 2^{1000}; в) 3^{333}

79. а) Докажи дека $(a-b)\,|\,(a^k-b^k)$ за секој $k\in\mathbf{N}$ и секои $a,b\in\mathbf{Z}$.
    б) Докажи дека $(a+b)\,|\,(a^{2k+1}+b^{2k+1})$ за секој $k\in\mathbf{N}$ и секои $a,b\in\mathbf{Z}$.

80. Најди го остатокот при делењето на
    а) $(5^{100}+55)^{100}$ со 24; б) $(17^{17}+116)^{21}$ со 8.

81. Докажи дека за секој ненегативен цел број n важи:
    а) $11\,|\,(2^{6n+1}+3^{2n+2})$; б) $37\,|\,(2^{n+5}\cdot 3^{4n}+5^{3n+1})$;
    в) $57\,|\,(7^{n+2}+8^{2n+1})$; г) $17\,|\,(2^{5n+3}+5^n\cdot 3^{n+2})$.

82. Докажи дека за секој природен број n остатокот од делењето на $3\cdot 5^{2n+1}+2^{3n+1}$ со 17 е 0.

83. "Читачот на мисли" Марко му рекол на својот пријател Доротеј да замисли еден број меѓу 1 и 999, да го помножи со 143 и да го каже трицифреniот број

составен од последните три цифри од производот. Потоа, Марко на Доротеј ќе му го соопшти замисленият број. Како?

84. Која од линеарните конгруентни равенки има решение:
а) $4x+5\equiv 0 \pmod 6$; б) $2x+2\equiv 0 \pmod 3$; в) $21x\equiv 12 \pmod{15}$.

85. Со непосредна проверка на системите на остатоци најди ги сите решенија на линеарната конгруентна равенка
а) $2x+5\equiv 0 \pmod 3$; б) $2x-3\equiv 0 \pmod 6$

86. Реши ги линеарните конгруентни равенки:
а) $21x\equiv 1 \pmod{17}$; б) $72x\equiv 2 \pmod{10}$

87. Реши го системот линеарни конгруентни равенки
а) $x\equiv 5 \pmod 4$, $x\equiv 7 \pmod{11}$,
б) $x\equiv 7 \pmod{11}$, $x\equiv 4 \pmod{14}$, $x\equiv 6 \pmod 5$,
в) $x\equiv 3 \pmod 5$, $x\equiv 4 \pmod 7$, $x\equiv 2 \pmod 3$,
г) $x\equiv 4 \pmod 5$, $x\equiv 3 \pmod 4$, $x\equiv 2 \pmod 7$, $x\equiv 6 \pmod 9$.

88. Ако топчиња за пин-понг се наредат во кутија во редови од по 15, тогаш остануваат 4 топчиња. Ако топчињата се наредат во редови од по 8, тогаш остануваат 3 топчиња. Ако топчињата се наредат во редови од по 23, тогаш остануваат 10 топчиња. Колку најмалку топчиња треба да има за да се задоволени горните услови? Колку во овој случај има редови од по 15, 8 и 23 топчиња?

89. Нека претпоставиме дека имаме два запчаника, запчаник А со 25 запци и запчаник В со 54 запци. Запчаникот А има "лош" забец, а запчаникот В има лош сектор меѓу два запци. Овие два запчаника се взаптени, при што запчаникот А се наоѓа на левата страна и се врти во насока на стрелката на часовникот, додека запчаникот Б се врти во насока спротивна од стрелката на часовникот. На почетокот на вртењето запчаниците правилно налегнуваат. Лошиот забец на А е три запци пред местото на взапнување, а лошиот сектор меѓу запците на В е на 20 места пред взапнувањето. За колку запци мора да се поместат запчаниците пред лошиот забец да легне на лошиот сектор? Колку често после тоа дефектните делови ќе се сретнуваат?

90. Ако е можно, решете го секој од системите конгруенции:
а) $x\equiv 21 \pmod{36}$, $x\equiv 5 \pmod 8$,
б) $x\equiv 8 \pmod{12}$, $x\equiv 5 \pmod 9$, $x\equiv 14 \pmod{15}$,
в) $x\equiv 19 \pmod{49}$, $x\equiv 10 \pmod{14}$.

91. Најди го најмалиот природен број кој има точно 6 делители.

92. Најди природен број n така да $n=2d(n)$.

93. Докажи дека постојат бесконечно многу природни броеви n такви да $\sigma(n)=2n-1$.

94. Бројот n е совршен ако $\sigma(n)=2n$. Докажи дека
а) Ако $n=2^{k-1}(2^k-1), k>1$ и $p=2^k-1$ е прост број, тогаш n е совршен број.

b) Ако n е парен совршен број, тогаш $n = 2^{k-1}(2^k - 1), k > 1$ и $p = 2^k - 1$ е прост број.

95. Докажи дека броевите $d(m^n)$ и n се заемно прости.

96. Најди критериум за деливост со:
а) 13; б) 99; в) 17.

97. Најди ги класите на конгруенција по модул m за:
а) $m = 2$; б) $m = 3$; в) $m = 4$; г) $m = 6$.

98. Состави таблица за собирање и множење по модул m за:
а) $m = 2$; б) $m = 3$; в) $m = 4$; г) $m = 6$.

99. Докажи дека за секој природен број n броевите: $n(2n+1)(7n+1)$; $n^3 + 11n$ и $n^3 + 17n$ се деливи со 6.

100. Докажи дека за секој природен број n бројот $4n^7 + 4$ не е делив со 19.

101. Докажи дека за секој природен број n бројот $n^2(n^2 - 1)$ е делив со 4.

102. Нека m и r се заемно прости цели броеви и $m > 0$. Докажи дека множеството $\{a, a+r, a+2r, ..., a+(m-1)r\}$, $a \in \mathbf{Z}$ е потполн систем остатоци по модул m.

103. Нека $\{a_1, a_2, ..., a_m\}$ е потполн систем остатоци по модул m, $\{b_1, b_2, ..., b_n\}$ е потполн систем остатоци по модул n и $\text{NZD}(m, n) = 1$. Докажи дека множеството S од сите природни броеви од видот

$$a_i n + b_j m,\ i = 1, 2, ..., m;\ j = 1, 2, ..., n$$

е потполн систем остатоци по модул mn.

104. Нека $\{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m, $\{b_1, b_2, ..., b_{\varphi(n)}\}$ е редуциран систем остатоци по модул n и $\text{NZD}(m, n) = 1$. Докажи дека множеството S од сите природни броеви од видот

$$a_i n + b_j m,\ i = 1, 2, ..., \varphi(m);\ j = 1, 2, ..., \varphi(n)$$

е редуциран систем остатоци по модул mn.

105. Докажи

а) $\varphi(p^a) = p^{a-1}\varphi(p)$, $p, a \in \mathbf{N}$ и p е прост број.

б) $\varphi(m^a) = m^{a-1}\varphi(m)$, $m, a \in \mathbf{N}$.

106. Дадено е $\varphi(m)$. Најди $\varphi(2m)$.

107. Докажи дека

$$\varphi(4m) = \begin{cases} \varphi(2m), & \text{NZD}(m, 2) = 1, \\ 2\varphi(2m), & \text{NZD}(m, 2) = 2. \end{cases}$$

108. Нека p е прост број. Пресметај го збирот

$$\varphi(1) + \varphi(p) + \varphi(p^2) + ... + \varphi(p^a),\ a \in \mathbf{N}.$$

109. Природниот број p е прост ако и само ако $\varphi(p) = p - 1$. Докажи!

III ГЛАВА
АКСИОМИ. ТЕОРЕМИ. МЕТОДИ НА ДОКАЖУВАЊЕ

При изучувањето на елементите од математичката логика и теоријата на броеви докажувавме низа тврдења, а користевме и определени поими. Притоа заклучоците ги изведувавме според правила кои беа прифатени интуитивно, т.е. за овие правила не дававме строго логичко објаснување. Во овој дел, врз основа на елементи на математичката логика, овие правила ќе ги објасниме и ќе можеме да ги користиме во експлицитен, т.е. јавен вид. Исто така, ќе се запознаеме и со основните методи за докажување на теореми, при што примената на овие методи ќе ја илустрираме како на веќе докажани теореми, така и на нови примери.

Во овој дел, покрај со теоремите, ќе се запознаеме и со математичките поими, при што посебно внимание ќе им обрнеме на основните (првични) и изведените поими, како и на причините за ваквата поделба на поимите.

1. МАТЕМАТИЧКИ ПОИМ. СОДРЖИНА И ОБЕМ НА ПОИМ

1.1. Математиката изучува разни математички објекти: *број, точка, множество, права, рамнина, сложен број, триаголник, паралелограм* итн. При изучувањето на овие објекти неопходно е прецизно да се утврди нивното значење. Така, на пример, со реченицата:

> *"За природниот број* n *ќе велиме дека е сложен ако има најмалку три природни делители.*"

е утврдено значењето на поимот сложен број и тоа е природен број кој има најмалку три природни делители. Да видиме како е дојдено до овој поим.

Во множеството на природните броеви го разгледуваме прашањето за бројот на делителите на даден природен број. Забележуваме дека бројот 1 има само еден природен делител, броевите 2, 3, 5, 7, ... имаат точно два природни делители, а броевите 4, 6, 8, 9, 10, 12, ... имаат три или повеќе природни делители. Според тоа, во однос на бројот на делителите, заедничка карактеристика на броевите 4, 6, 8, 9, 10, 12, ... е "*тие имаат барем три природни делители*" и оваа карактеристика ги опфаќа само овие броеви, па затоа нив можеме да ги опфатиме со еден термин, во случајов со терминот *сложен број*.

Значи, *поимот* претставува мисловно репродуцирање, т.е. мисловна копија на дадена класа објекти и се искажува со реченица која содржи определен *договор* за таа класа објекти. Секој математички поим се означува со *термин* кој обично се состои од еден или од неколку збора, но може да биде претставен и со симбол (знак). Во нашиот пример класата објекти е 4, 6, 8, 9, 10, 12, ..., а терминот е *сложен број*.

Од досега изнесеното можеме да заклучиме дека секој математички поим во себе обединува множество објекти или релации, кое го нарекуваме *обем на поимот* и карактеристично својство кое го имаат само елементите на тоа множество, а кое го нарекуваме *содржина на поимот*.

Така, на пример, обемот на поимот сложен број е множеството {4, 6, 8, 9, 10, 12,...}, а неговата содржина е претставена со својството*: број што има барем три природни делители*.

Јасно, содржината и обемот на поимот се заемно поврзани. Имено, содржината строго го определува обемот на поимот и обратно, обемот во целост ја определува содржината на поимот. Зависноста меѓу содржината и обемот на поимот во извесна смисла е обратнопропорционална. Имено, ако *содржината на еден поим се збогати*, тогаш *неговиот обем се намалува*, а ако *обемот на поимот* се *зголеми*, тогаш *неговата содржина ќе се осиромаши*.

1.2. Пример. Да ја разгледаме класата: "*отсечки кои минуваат низ центарот на кружницата и чии крајни точки лежат на кружницата*". Очигледно станува збор за класата дијаметри на кружница.

Ако содржината "*минуваат низ центарот на кружницата и чии крајни точки лежат на кружницата*" се осиромаши на: "*чии крајни точки лежат на кружницата*", тогаш ќе ја добиеме класата: "*отсечки чии крајни точки лежат на кружницата*". Очигледно станува збор за класата тетиви на кружница, која ја содржат класата дијаметри на кружница.

Значи, со осиромашување на содржината се зголемува обемот на поимот. ♦

1.3. Пример. Да ја разгледаме класата: "*паралелограми, такви што во кој било од нив, сите агли се еднакви меѓу себе*". Очигледно се работи за поимот правоаголник, т.е. тоа е класата правоаголници.

Ако содржината "*сите агли се еднакви меѓу себе*" се збогати на: "*сите страни и сите агли се еднакви меѓу себе*", тогаш ќе ја добиеме класата: "*паралелограми такви, што во кој било од нив, сите страни и сите агли се еднакви меѓу себе*". Очигледно се работи за поимот квадрат, т.е. тоа е класата квадрати, која се содржи во класата правоаголници.

Значи, со збогатување на содржината се стеснува обемот на поимот. ♦

1.4. При *обопштувањето* на некој поим, неговата содржина се стеснува и обемот се проширува, додека во процесот на *специјализација* се случува обратното: содржината се проширува, а обемот се стеснува.

Како што видовме, обемот на поимот сложен број се содржи во обемот на поимот природен број.

1.5. Дефиниција. Нека поимот A има обем $O(A)$, а поимот B има обем $O(B)$. Ако $O(A) \subset O(B)$, тогаш за A ќе велиме дека е *видов поим* во однос на B, а B дека е *родов поим* во однос на A.

1.6. Пример. *Четириаголник* е многуаголник со четири страни. *Паралелограм* е четириаголник кај кој спротивните страни, две по две, се паралелни.

Според тоа, паралелограм е вид на четириаголник, а четириаголник е вид на многуаголник. Значи, поимот многуаголник е родов поим во однос на поимот паралелограм, но исто така и поимот четириаголник е родов поим во однос на поимот паралелограм. Јасно, за паралелограм поимот четириаголник е *најблискиот род*.♦

1.7. Пример. Дијаметар на кружница е тетива што минува низ центарот на кружницата.

Од множеството тетиви на една кружница ние издвоивме едно подмножество со помош на својството "тетива што минува низ центарот на кружницата". Со ова својство наполно се определени дијаметрите на кружницата, т.е. тоа е *нивно карактеристично својство*. Значи, со него се издвојува еден вид тетива, па затоа ова својство го нарекуваме *видова одлика* за поимот дијаметар. ♦

2. ДЕФИНИРАЊЕ НА ПОИМ. ВИДОВИ ПОИМИ

2.1. Реченицата со која се открива содржината на еден поим ја нарекуваме *дефиниција* на тој поим. Со други зборови, со дефиницијата се набројуваат суштинските својства со чија помош се издвојуваат сите објекти и само тие коишто ги имаат споменатите својства.

Така, со реченицата: "*Дијаметар на кружница е тетива што минува низ центарот на кружницата*." се дефинира поимот дијаметар. Таа се состои од:

- *дефиниран поим*, т.е. поимот што се дефинира, а тоа е дијаметар на кружница,
- *логичка врска*, (во примерот "е", а може да биде и "го нарекуваме", "се нарекува", "го викаме" и сл.) и
- *дефинирачки поим,* т.е. родовиот поим со видовите одлики, а тоа е: тетива што минува низ центарот на кружницата.

Како што веќе видовме, поимите најчесто се наоѓаат во родов-видов однос. Затоа *дефиницијата според најблискиот род и видовите одлики* е најдобар и најраспространет начин на дефинирање на поими. Меѓутоа, дефиницијата може да се даде и преку род што не е најблизок до дефинираниот поим, што може да се види од следниот пример.

2.2. Пример. Дијаметар на кружница е отсечка која минува низ центарот на кружницата и чии крајни точки лежат на кружницата. ♦

2.3. Јасно, во такви случаи потребни се повеќе видови признаци, чиј број може да се намали само ако се изнајде најблискиот род за дефинирање на нов вид, а тоа во даденият случај е тетива на кружница.

Се поставува прашање каков треба да биде односот меѓу дефинираниот и дефинирачкиот поим. Одговорот на ова прашање е дека тие треба да се *еквивалентни* и во тој случај велиме дека дефиницијата е *логички издржана* (*правилна*). Затоа секоја реченица којашто претставува дефиниција на некој поим, мора да се

подразбира во смисла “*ако и само ако*”, дури и тогаш кога е искажана само со условот “*ако*”. Така, на пример, дефиницијата за сложен број треба да се сфати во следнава смисла: “*Природниот број n е сложен ако и само ако има барем три природни делители*.”

2.4. Правила за дефинирање. При дефинирањето на поимите треба да се запазуваат основните правила за дефинирање. Имено, дефиницијата треба:

1. ***да биде потполна, јасна и без непотребни податоци,*** т.е. да биде логички совршена, без да вклучува својства коишто се логички зависни едно од друго како што е во примерот: "*Четириаголникот кај кој спротивните страни пар по пар се паралелни и еднакви се вика паралелограм.*" Во овој пример е вклучено својството “*за еднаквост на спротивните страни*” кое е последица од својството "*спротивните страни пар по пар се паралелни*".
2. ***да биде усогласена***, т.е. обемот на дефинираниот поим да се совпаѓа со обемот на дефинирачкиот поим. На пример, дефиницијата: “*Четириаголникот кај кој спротивните страни пар по пар се паралелни се вика паралелограм.*" е усогласена. Доколку дефиницијата не е усогласена, тогаш можни се грешки во кои обемот на дефинирачкиот поим е *поширок* од обемот на поимот што се дефинира, како на пример: "*Дијаметар на кружница е отсечка што минува низ центарот на кружницата.*", или *потесен*, како на пример: "*Ромб е правоаголник со две еднакви соседни страни.*". Така, во првиот случај обемот ги опфаќа сите отсечки кои минуваат низ центарот на кружницата, па тука спаѓаат и отсечките чии крајни точки не лежат на кружницата и тие, како што знаеме, не се нејзини дијаметри. Во вториот случај обемот ги опфаќа само квадратите, т.е. ваквата дефиниција на ромб не е согласна со класата на ромбови.
3. ***да не се влегува во логички бесмислен круг***, т.е. не смее $\boldsymbol{A}$ да се дефинира со $\boldsymbol{B}$, а потоа $\boldsymbol{B}$ да се дефинира со $\boldsymbol{A}$, како што тоа е направено во следниов случај: "*Еден агол се вика прав ако неговите краци се заемно нормални*", а потоа "*За две прави ќе велиме дека се заемно нормални ако се сечат под прав агол*".
4. ***во дефиницијата не смее да се допушта тафтологија***, т.е. објектот да се дефинира сам со себе иако се искажува со други зборови, бидејќи во тој случај ништо не се дефинира, како што е во примерот: "*За две прави ќе велиме дека се нормални ако тие се нормални една на друга.*"
5. ***да не отсуствува родовиот (дефинирачкиот) поим,*** како што е во случајот: "*сложен број е она што има барем три делители*".
6. по можност ***да не е негативна,*** како на пример: "*Ако природниот број не е прост, тогаш ќе велиме дека е сложен*" или "*Реалниот број којшто не е рационален, се нарекува ирационален.*"
7. ***да биде "минимална"***, т.е. карактеристичното својство по својата структура треба да биде минимално, на пример: "*Правоаголник е паралелограм со прав агол.*" Да забележиме дека дефиницијата е *мини-*

мална ако таа е дадена со помош на најблискиот род. Претходната дефиниција е минимална, што не е случај со следнава дефиниција на правоаголник: "*Правоаголник е четириаголник што има прав агол и два пара паралелни страни*".

8. ***да не е противречна***, т.е. при дефинирањето на еден поим неговиот обем не смее да биде празно множество, како што е во случајот на следнава "дефиниција": "*За природниот број ќе велиме дека е едноставен ако бројот на неговите делители е еднаков на нула*." Јасно, не постои природен број кој нема делители, па затоа обемот на претходната "дефиниција" е празно множество, што значи дека во случајот ништо не сме дефинирале.

2.5. Основни и изведени поими. Во досегашните разгледувања се задржавме на основните правила за дефинирање на поимите, кое може да биде правилно направено на повеќе начини. Со други зборови, постојат повеќе видови дефиниции. Пред да ги разгледаме различните видови дефиниции, ќе направиме класификација на поимите. За таа цел ќе ја разгледаме дефиницијата на поимот квадрат:

"*Квадрат е ромб со прав агол*".

Овој поим е дефиниран со родовиот поим ромб и соодветната одлика (прав агол). Поимот ромб можеме да го дефинираме со поимот паралелограм и соодветна одлика итн. Процесот на изградување на поимите доведува до една од следниве две можности:

1. или еден поим A смее да се дефинира со друг поим B за чие дефинирање е веќе употребен поимот A, т.е. ќе допуштиме логички бесмислен круг во дефиницијата,
2. или некои од поимите ќе ги прифатиме без да ги дефинираме.

Секако, втората можност е логична, па затоа таа е прифатена се со цел да не се допушти логички бесмислен круг.

Дефиниција. Поимите што не ги дефинираме, т.е. ги прифаќаме без дефиниција, ги нарекуваме *основни поими* бидејќи се во основата на науката и не можат да се изразат со други поими од таа наука.

Една математичка дисциплина обично се гради врз основа на неколку основни поими и врските меѓу нив. Тие овозможуваат да се дефинираат сите други поими од таа дисциплина, кои поими ги нарекуваме *изведени*.

Така, основни поими во геометријата се: *точка, права, рамнина и растојание,* а сите други поими се изведени. Други основни математички поими се: *множество, елемент и број*, кои се среќаваат како основни поими во сите математички дисциплини.

2.6. Видови на дефиниции. Како што веќе рековме, математичките поими може правилно да се дефинираат на повеќе начини. Во таа смисла имаме неколку видови на дефиниции. Ќе наведеме некои од нив.

1) ***Дефиниција со помош на најблискиот род и видова одлика.*** За овој начин на дефинирање веќе говоревме. Ќе наведеме неколку примери.

2.6.1. Пример. а) За природниот број n ќе велиме дека е прост ако има точно два природни делители.

б) Топка е множеството од сите точки во просторот чиешто растојание до една фиксна точка O е помало или еднакво на даден позитивен број r. ♦

Како што веќе рековме, дефиницијата со помош на најблискиот род и видова одлика е најраспространета во математиката, но сепак се користат и други видови дефиниции, како што се:

2) ***Генеричка дефиниција.*** Тоа е дефиниција со која се опишува процесот на формирање на поимот што се дефинира.

2.6.2. Пример. а) Топка е геометриско тело, кое се добива со ротација на круг околу еден негов дијаметар.

б) Конус е геометриско тело, кое се добива со ротација на правоаголен триаголник околу една негова катета. ♦

Како што можеме да забележиме, описот на процесот на формирање на поимот, даден во генеричката дефиниција на топка, го занемарува нејзиното карактеристично својство, кое доаѓа до израз во дефиницијата со помош на најблискиот род и видова одлика (пример 2.6.1 а)), и е главен недостаток на генеричката дефиниција.

3) ***Рекурзивна дефиниција.*** Тоа е дефиниција со која се задаваат:

i) почетни елементи од класата објекти што се дефинираат,

ii) правила за формирање на нови објекти од веќе формираните (тоа најчесто се рекурзивни врски) и

iii) ограничување, т.е. логичко толкување дека со *i*) и *ii*) се исцрпуваат сите објекти од разгледуваната класа.

Пример за рекурзивна дефиниција е следниот начин на дефинирање на таканаречената *Фибоначиева низа броеви*, која има посебна улога во толкувањето на низа природни процеси.

i) $a_1 = a_2 = 1$,

ii) дадено е правило: $a_n = a_{n-1} + a_{n-2}$, $n = 2,3,4,...$

iii) членови на Фибоначиевата низа се сите броеви добиени со *i)* и *ii)* и никои други.

Да забележиме дека според претходната дефиниција, членовите на Фибоначиевата низа се 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

4) ***Дефиниција искажана со симболички јазик.*** Овој вид на дефиниција честопати се користи во математиката. Така, на пример, од основното образование ти се познати следниве дефиниции искажани со симболичен јазик:

- $a^0 = 1, a \neq 0$,

- $|a| = \begin{cases} a, & \text{ако } a \geq 0 \\ -a, & \text{ако } a < 0, \end{cases}$

- $a^n = \underbrace{a \cdot a \cdot ... \cdot a}_{n \text{ пати}}$, за $a \in \mathbf{R}, n \in \mathbf{N}$ итн.

5) ***Опис на поим.*** Честопати користиме логички реченици, кои не се дефиниции, но се блиски до дефинициите. Имено, во некои случаи тие ја заменуваат дефиницијата или ја надополнуваат. Кон опис на поимот најчесто се прибегнува кога не е можно да се даде дефиниција на разгледуваниот поим. Таков е случајот со основните поими: точка, права, рамнина итн., кои најчесто ги објаснуваме со некој модел, како на пример:

- *точката* се претставува со допир на моливот до хартијата,

- *правата* ја замислуваме како бескраен затегнат конец, итн.

6) ***Индиректна (аксиоматска) дефиниција***. Тоа е дефиниција кога својствата на поимите се откриваат преку аксиоми (почетни тврдења). Така, во елементарната геометрија аксиомите ги откриваат својствата и врските меѓу основните поими: точка, права, рамнина и растојание, без да се дефинираат. Друг пример е воведувањето на множеството на природните броеви $\mathbf{N}$ кое се дефинира со Пеановите аксиоми.

Пеанови аксиоми. Множеството $\mathbf{N}$ е непразно и важи:

i) $1 \in \mathbf{N}$.

ii) За секој природен број k постои единствен природен број k^+, кој го нарекуваме *следбеник* на k.

iii) Ако $k^+ = n^+$, тогаш $k = n$.

iv) $1 \neq k^+$, за секој $k \in \mathbf{N}$.

v) Ако $S \subseteq \mathbf{N}, 1 \in S$ и од $k \in S$ следува дека $k^+ \in S$, тогаш $S = \mathbf{N}$.

3. ПОИМ ЗА ТВРДЕЊЕ. ВИДОВИ МАТЕМАТИЧКИ ТВРДЕЊА

3.1. Во математиката, на секој чекор среќаваме реченици со кои се искажува некое својство или врска на математички поими. Ваквите реченици ги нарекуваме тврдења. Попрецизно, под *тврдење* подразбираме логичка форма на мислење, со која се потврдуваат или се одрекуваат некои својства на дадени објекти, појави, процеси, или на некои релации меѓу нив. Тврдењата во кои се среќаваат својства и релации на математички објекти ги нарекуваме *математички тврдења*. Ќе дадеме неколку примери на математички тврдења.

3.2. Пример. а) Еден број е делив со 3 ако збирот на неговите цифри е делив со 3.

б) Дијагоналите на паралелограмот заемно се преполовуваат.

в) Збирот на внатрешните агли во триаголникот е еднаков на 180°.

г) Дијагоналите на ромбот се заемно нормални.

д) Ако $p \mid a$, тогаш $p \mid ab$, за секој $b \in \mathbf{Z}$.

ѓ) Ако еден број е делив со 5, тогаш неговата последна цифра мора да е 0. ♦

3.3. Како што можеме да забележиме, секое тврдење се состои од три главни елементи, и тоа:

а) *логички подмет* (или *субјект*) на мислата (S) - тоа е оној поим или објект за кој се искажува нешто во тврдењето,

б) *логички прирок* (или *предикат*) на мислата (P) - тоа што се искажува,

в) *логички сврзник* (е, има итн.).

3.4. Пример. а) Да го разгледаме тврдењето:

"*За секој природен број* n, $2^n > n^2$."

Во ова тврдење субјект е "бројот 2^n", предикат е "поголем од бројот n^2", а сврзник е "е".

б) Во тврдењето од примерот 3.2 г) субјект е "дијагоналите на ромбот", предикат е "заемно нормални", а сврзник е "се".

в) Во тврдењето од примерот 3.2 в) субјект е "збирот на внатрешните агли во триаголникот", предикат е "еднаков на 180°", а сврзник е "е". ♦

3.5. Во досегашниот дел се запознавме со поимот математичко тврдење и со неговата логичка структура. Што се однесува до поделбата на математичките тврдења, таа може да се направи според повеќе критериуми. Еден од критериумите за поделба на математичките тврдења е дали едно тврдење важи за сите објекти од дадена класа или само за некои од нив, и според овој критериум разликуваме *општо* и *делумно тврдење*. Ако, пак, на објектите од дадена класа им се припишува, односно одрекува некое својство, тогаш имаме *потврдно*, односно *одречно тврдење*. Комбинирајќи ги овие две поделби на тврдењата, ги добиваме следниве видови тврдења:

1) *Општо потврдно тврдење*, кое се искажува во обликот: "*за кој било објект* x, *ако* x *го има својството* S, *тогаш* x *го има и својството* P". Симболички овој вид на тврдење се запишува со: $(\forall x)(S(x) \Rightarrow P(x))$.

3.5.1. Пример. а) Во секој паралелограм спротивните агли се еднакви.

б) Во секој рамнокрак трапез дијагоналите се еднакви.

в) Секој природен број поголем од 1 е или прост или сложен број. ♦

2) *Делумно потврдно тврдење*, кое се искажува во обликот: "*постои објект* x, *којшто го има својството* S, *а го има и својството* P". Симболички овој вид тврдење се запишува со: $(\exists x)(S(x) \wedge P(x))$.

3.5.2. Пример. а) Некои правоаголници имаат заемно нормални дијагонали.

б) Некои триаголници имаа два еднакви агли.

в) Во некои триаголници висината и тежишната линија повлечени од едно теме се совпаѓаат. ♦

3) *Општо одречно тврдење*, кое се искажува во обликот: "*ниеден објект* x*, којшто го има својството* S*, го нема својството* P ". Симболички овој вид тврдење се запишува со: $(\forall x)(S(x) \Rightarrow \overline{P}(x))$.

3.5.3. Пример. а) Ниеден природен број не е истовремено и прост и сложен број.

б) Ниеден триаголник не е истовремено и правоаголен и тапоаголен. ♦

4) *Делумно одречно тврдење*, кое се искажува во обликот: "*постои* x*, којшто го има својството* S*, а го нема својството* P ". Симболички овој вид тврдење се запишува со: $(\exists x)(S(x) \wedge \overline{P}(x))$.

3.5.4. Пример. а) Некои трапези немаат еднакви дијагонали.

б) Некои триаголници немаат еднакви страни.

в) Некои природни броеви немаат повеќе од два природни делители. ♦

4. ТЕОРЕМИ И АКСИОМИ. УСЛОВНА И КАТЕГОРИЧКА ФОРМА НА ТЕОРЕМА

4.1. Како што знаеме, тврдењата под а), б), в), г) и д) од примерот 3.2 се вистинити, т.е. точни, а тврдењето под ѓ) не е вистинито. Јасно, како и секое тврдење, така и математичките тврдења се карактеризираат со нивната вистинитост. Вистинитите тврдења се од посебно значење во математиката. Затоа, за секое математичко тврдење се поставува задачата да се установи неговата вистинитост. Според начинот на утврдување на вистинитоста на математичките тврдења, тие се поделени во две групи, и тоа: *аксиоми* и *теореми*.

4.2. Дефиниција. Математичкото тврдење што е вистинито, а неговата вистинитост е констатирана со доказ, т.е. тоа е логичка последица од други точни тврдења го нарекуваме *теорема* или *изведено тврдење*.

Пред да преминеме на разгледување на структурата на теоремите, да забележиме дека барањето за минималност на дефиницијата е причина за појавата на теоремите. Имено, со запазувањето на ова барање, за да се утврдат другите својства на поимите, кои ги нема во дефиницијата, се појавиле теоремите.

4.3. Пример. Да ја разгледаме теоремата:

Ако еден четириаголник е паралелограм, тогаш неговите дијагонали се преполовуваат.

Во оваа теорема се разгледува, прво, математичкиот објект четириаголник при условот: "*тој четириаголник да е паралелограм*", а потоа за таквиот четириаголник се тврди дека: "*неговите дијагонали се преполовуваат*". Со други зборови, од претпоставката (условот) дека четириаголникот е паралелограм се заклучува дека неговите дијагонали се преполовуваат. ♦

4.4. Како и во претходниот пример, во секоја теорема мора да е јасно искажано:

- под кои услови се разгледува некој математички објект и
- што се тврди за тој објект, т.е. кое негово својство следува.

Условите под кои се разгледува математичкиот објект ги нарекуваме *претпоставки*, а својството кое следува за тој објект го нарекуваме *заклучок на теоремата*.

4.5. Пример. Во теоремата

"Ако четириаголникот е рамнокрак трапез, тогаш неговите дијагонали се еднакви."

претпоставката е "четириаголникот е рамнокрак трапез", а заклучокот е "дијагоналите му се еднакви". ♦

4.6. Како што рековме, теорема е математичко тврдење чија вистинитост е констатирана со доказ. Докажувањето на вистинитоста на теоремата е направено со помош на други тврдења чија вистинитост претходно е констатирана. Како и кај математичките поими, и овде постојат две можности:

- или ќе навлеземе во логички бесмислен круг;
- или некои тврдења ќе ги прифатиме за точни, без да ги докажуваме.

Јасно, од логичка гледна точка, втората алтернатива е поприфатлива, па затоа некои тврдења ги прифаќаме за точни без да ги докажуваме. Така ја имаме следнава дефиниција.

4.7. Дефиниција. Математичкото тврдење кое без доказ го прифаќаме за точно го нарекуваме *аксиома* или *основно тврдење.*

4.8. Аксиомите се тврдења кои лежат во основата на математиката, која во различни свои дисциплини користи различни системи на аксиоми. Притоа за еден систем на аксиоми ќе сметаме дека е добро осмислен ако тој е:

1) ***непротивречен***, што значи дека меѓусебно не смеат да си противречат како аксиомите, така и сите тврдења кои се докажуваат со нивна помош.

2) ***комплетен***, што значи дека при негова реализација секогаш се добива "иста" математичка структура и

3) ***независен***, што значи дека ниедна од аксиомите не смее да може да се докаже со помош на останатите аксиоми, што само по себе значи сведување на минимум на бројот на аксиомите, а со самото тоа и упростување на системот на аксиоми.

4.9. Како што можеме да забележиме, теоремите од примерите 4.3 и 4.5 се искажани со користење на формулацијата "*Ако ..., тогаш ...*". Во овој случај велиме дека теоремата е искажана во *условна форма*, т.е. во форма на импликација:

$$p \Rightarrow q,$$

и притоа јасно се разграничува условот од заклучокот, т.е. кај оваа формулација делот од реченицата p е услов, а делот од реченицата q е заклучок на теоремата.

Теоремите од примерите 4.3 и 4.5 можат да се искажат и на начин даден во следниов пример.

4.10. Пример. а) Дијагоналите кај паралелограмот се преполовуваат.

б) Дијагоналите кај рамнокракиот трапез се еднакви. ♦

4.11. Забележуваме дека во овој случај истите теореми се искажани со "категорични" реченици. При ваквото искажување на теоремите велиме, дека тие се дадени во *категорична форма*. Ќе наведеме уште неколку теореми искажани во категорична форма.

4.12. Пример. а) Дијагоналите кај ромбот се заемно нормални.

б) Збирот на внатрешните агли во триаголникот е еднаков на 180°.

в) Спротивните агли кај тетивен четириаголник се суплементни.

г) Збировите на спротивните страни кај тангентен четириаголник се еднакви. ♦

4.13. Забелешка. Категоричната форма за искажување на теоремите се одликува со краткост во формулацијата, па затоа оваа формулација честопати се применува. Меѓутоа, оваа форма има и еден сериозен недостаток, а тоа е што условот и заклучокот не се експлицитно одделени. Затоа, во случај кога една теорема е искажана во категорична форма пожелно е истата да ја искажеме во условна форма, а потоа да ја докажеме односно користиме. Обиди се теоремите од пример 4.12 да ги искажеш во условна форма.

5. ДИРЕКТНА И ОБРАТНА ТЕОРЕМА. ПОТРЕБЕН И ДОВОЛЕН УСЛОВ

5.1. Директна и обратна теорема. Како што веќе рековме кај теоремите меѓу условот (претпоставката) p и заклучокот q постои причинско-последична врска која во условна форма се искажува со импликацијата $p \Rightarrow q$. Логично е да се запрашаме што се случува ако претпоставката и заклучокот си ги заменат местата. Во оваа смисла ја имаме следната дефиниција.

5.2. Дефиниција. Ако $p \Rightarrow q$ е теорема, тогаш импликацијата $q \Rightarrow p$ ја нарекуваме *обратно тврдење* на теоремата $p \Rightarrow q$, која уште ја нарекуваме и директно тврдење.

5.3. Пример. а) За теоремата:

"Ако четириаголникот е ромб, тогаш неговите дијагонали се заемно нормални.",

обратното тврдење гласи:

"Ако дијагоналите на четириаголникот се заемно нормални, тогаш тој е ромб."

б) За теоремата:

"Дијагоналите во паралелограмот се преполовуваат."

обратното тврдење гласи:

"Четириаголникот во кој дијагоналите се преполовуваат е паралелограм.".♦

5.4. Бидејќи кај делтоидот дијагоналите се заемно нормални и делтоидот не е ромб, заклучуваме дека обратното тврдење на теоремата во примерот 5.3 а) не е точно. Меѓутоа, обратното тврдење на теоремата во примерот 5.3. б) е точно тврдење, т.е. во овој случај обратното тврдење е повторно теорема. Така, ја имаме следната дефиниција.

Дефиниција. Ако обратното тврдење на една теорема е точно, тогаш тоа го нарекуваме *обратна теорема*.

5.5. Математиката како наука тежнее записите да се колку што е можно поедноставни и пократки. Токму затоа, ако обратното тврдење $q \Rightarrow p$ на теоремата $p \Rightarrow q$ исто така е теорема, тогаш двете теореми најчесто, со помош на еквиваленција $p \Leftrightarrow q$ се запишуваат како една. Ќе разгледаме неколку примери.

5.6. Пример. а) Теоремите во примерот 5.3. б) можеме да ги искажеме на следниот начин:

"*Четириаголникот е паралелограм ако и само ако неговите дијагонали се преполовуваат"*

б) Теоремата:

"*Ако бројот* n *е делив со 3, тогаш збирот на неговите цифри е делив со 3.*"

и нејзината обратна теорема:

"*Ако збирот на цифрите на бројот* n *е делив со 3, тогаш тој е делив со 3.*"

заедно ги искажуваме на следниов начин:

"*Бројот* n *е делив со 3 ако и само ако збирот на неговите цифри е делив со 3.*"

5.7. Потребен и доволен услов. Како што веќе рековме, секоја теорема може да се искаже во условна форма, т.е. во форма на импликација $p \Rightarrow q$. Јасно при искажувањето на теоремите во форма на импликација, исказите p и q се во

причинско-последична врска, т.е. тие се меѓу себе содржински поврзани. Ваквите импликации ги нарекуваме *условни искази*.

Според тоа, секоја математичка теорема, според својата логичка структура е условен исказ:

$$\text{“Ако } p\text{, тогаш } q\text{.”}(p \Rightarrow q),$$

чијашто вистинитост е докажана за множеството објекти за кои е формулирана теоремата.

Ако имаме променлива x, тогаш условот p и заклучокот q на теоремата $p \Rightarrow q$ се предикати кои ги означуваме со $p(x)$ и $q(x)$, соодветно, и притоа импликацијата $p(x) \Rightarrow q(x)$ е вистинита за секоја вредност на променливата x, што значи дека за секој x е точен исказот $p(x) \Rightarrow q(x)$. Притоа велиме дека исказот $q(x)$ логички следува од исказот $p(x)$, односно дека заклучокот q на теоремата $p \Rightarrow q$ е *логичко следство* од условот p, што значи дека кога е вистинито p, задолжително е вистинито q. Тоа значи дека заклучокот на теоремата q е *неопходно следство* (*потребен услов*) на условот p, а условот p на истата теорема е *доволна основа* (*доволен услов*) за нејзиниот заклучок q.

Погоре споменатите термини потребен услов и доволен услов имаат посебно значење во математиката, токму поради нивната тесна врска со поимот теорема. Имено, секоја теорема може да се искаже со помош на овие два термини, па затоа на нив подетално ќе се осврнеме.

Потребен услов на некое тврдење е таков услов без чие исполнување тврдењето не може да биде точно.

5.7.1. Пример. Да ја разгледаме теоремата:

“*Ако четириаголникот е ромб, тогаш неговите дијагонали се заемно нормални*.”

Заклучокот “*дијагоналите на четириаголникот се заемно нормални*” е потребен услов за тврдењето “*четириаголникот е ромб*”, бидејќи за четириаголник кај кој дијагоналите не се заемно нормални, тврдењето “*четириаголникот е ромб*” со сигурност не е точно, како на пример кај рамнокракиот трапез.

Оваа теорема со помош на терминот потребен услов може да се искаже на следниов начин:

“Потребен услов за еден четириаголник да биде ромб е неговите дијагонали да се заемно нормални.” ♦

Од друга страна, потребниот услов на една теорема може да биде исполнет за некоја класа на математички објекти, но не мора да биде последица на претпоставката. Последново ќе го илустрираме на следниот пример.

5.7.2. Пример. Во теоремата

“Ако четириаголникот е правоаголник, тогаш неговите дијагонали се еднакви меѓу себе.”,

потребен услов е тврдењето *"четириаголникот има еднакви дијагонали"*. Меѓутоа овој услов го задоволува и секој рамнокрак трапез, а како што знаеме рамнокракиот трапез не е правоаголник, што значи дека во случајот на рамнокракиот трапез потребниот услов не е последица од претпоставката. ♦

Од досега изнесеното следува, дека ако теоремата е искажана во условна форма $p \Rightarrow q$, наместо "*Ако* p, *тогаш* q", во терминот потребен услов таа може да се искаже на еден од следниве начини:

а) "Потребен услов за p е q" или

б) "q е потребен услов за p",

што значи дека во секоја теорема *последицата е потребен услов за претпоставката.*

Доволен услов за едно тврдење е таков услов при чие исполнување даденото тврдење е задолжително вистинито.

5.7.3. Пример. Во теоремата

"*Ако збирот на цифрите на природниот број* n *е делив со 9, тогаш тој се дели со 3*."

претпоставката "*збирот на цифрите на природниот број* n *се дели со* 9" е доволен услов за тврдењето "*природниот број* n *е делив со* 3", бидејќи природен број чиј збир на цифри е делив со 9 сигурно е делив со 9, па значи и со 3.

Оваа теорема со помош на терминот доволен услов може да се искаже на следниов начин:

"*Доволен услов за природниот број* n *да се дели со* 3 *е збирот на неговите цифри да се дели со* 9." ♦

Да забележиме дека во претходниот пример доволниот услов "*збирот на цифрите на природниот број* n *се дели со* 9" не е и потребен за условот "*природниот број* n *е делив со* 3". Навистина, постојат и други броеви кои се деливи со 3, а чиј збир на цифри не се дели со 9, а тоа се сите природни броеви чиј збир на цифри се дели со 3, а не се дели со 9. Овој пример, всушност, непосредно укажува на разликата на термините потребен и доволен услов.

Од досега изнесеното следува дека ако теоремата е искажана во условна форма $p \Rightarrow q$, наместо "*Ако* p, *тогаш* q", во терминот доволен услов таа може да се искаже на еден од следниве начини:

а) "Доволен услов за q е p" или

б) "p е доволен услов за q",

што значи дека во секоја теорема *претпоставката е доволен услов за последицата.*

Како што видовме, ако теоремата е искажана во условна форма $p \Rightarrow q$, тогаш претпоставката p е *доволен услов* за заклучокот q, а заклучокот q е *потребен услов* за претпоставката p. Според тоа, една иста теорема која што е искажана со помош на потребен услов за еден поим може да се искаже со помош на доволен услов за друг поим. Последното ќе го илустрираме на следниот пример.

5.7.4. Пример. а) Теоремата од примерот 5.7.1 во терминот доволен услов се искажува на следниов начин:

"Доволен услов за еден четириаголник да има заемно нормални дијагонали е тој четириаголник да биде ромб."

б) Теоремата од примерот 4.12 в) во терминот доволен услов се искажува на следниов начин:

"*Доволен услов за спротивните агли на еден четириаголник да се суплементни е тој четириаголник да е тетивен*." ♦

Претходно кажавме дека заклучокот q не е секогаш доволен услов за претпоставката p. Меѓутоа, во низа случаи во теоремата $p \Rightarrow q$ заклучокот q е и доволен услов за p, и тогаш велиме дека q е *потребен и доволен услов* за p (или p е потребен и доволен услов за q). Всушност, во овој случај станува збор за еквиваленција, т.е. $p \Leftrightarrow q$. Последното ќе го илустрираме на следниот пример.

5.7.5 Пример. Во термините потребен и доволен услов теоремата

"Четириаголникот е паралелограм ако и само ако неговите дијагонали се преполовуваат."

можеме да ја искажеме на следниот начин:

"Потребен и доволен услов за еден четириаголник да биде паралелограм е неговите дијагонали да се преполовуваат" ♦

5.8. Во врска со поимите потребен услов, доволен услов и потребен и доволен услов може да се направи класификација на теоремите искажани за даден поим. Така ја имаме следната дефиниција.

Дефиниција. Ако со една теорема се дава потребен услов за некој поим, тогаш таа се вика *теорема-својство* за тој поим.

Ако со една теорема се искажува доволен услов за еден поим, тогаш таа се вика *теорема-признак* за тој поим.

Теорема, пак, со која се искажува потребен и доволен услов за еден поим се вика *теорема-карактеристично својство* за тој поим.

5.9. Пример. а) Теоремата "*Потребен услов за еден четириаголник да биде ромб е неговите дијагонали да се заемно нормални."* е теорема-својство.

б) Теоремите искажани во примерот 5.7.4 се теореми-признаци.

в) Теоремата искажана во примерот 5.7.5 е теорема-карактеристично својство. ♦

6. ПРАВИЛА ЗА ИЗВЕДУВАЊЕ НА ЗАКЛУЧОЦИ

6.1. При изучувањето на елементите од математичката логика се запознавме со конјункцијата, дисјункцијата, негацијата, импликацијата и еквиваленцијата. Исто така, се запознавме со исказните формули кои можат да бидат *тафто-*

логии, контрадикции или *неутрални исказни формули*. Понатаму, дека од сите логички формули тавтологиите имаат посебно значење, бидејќи секоја тавтологија е некој *логички закон* или *закон на мислењето*.

Во натамошниот дел, користејќи го претходно изнесеното, ќе се запознаеме со некои правила за изведување на заклучоци.

6.2. Модус поненс (правило за одделување). Да ја разгледаме исказната формула

$$(p \Rightarrow q) \wedge p \Rightarrow q \,. \tag{1}$$

За да утврдиме дека од $p \Rightarrow q$ и p следува заклучокот q, доволно е да докажеме дека исказната формула (1) е тавтологија. Последното ќе го направиме користејќи ја следната таблица на вистинитост.

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \wedge p$	$(p \Rightarrow q) \wedge p \Rightarrow q$
T	T	T	T	T
T	⊥	⊥	⊥	T
⊥	T	T	⊥	T
⊥	⊥	T	⊥	T

Од претходната таблица заклучуваме дека исказната формула (1) е тавтологија, што значи дека таа е логички закон кој го нарекуваме *модус поненс* или *правило за одделување*. Во случајот исказите $p \Rightarrow q$ и p се *претпоставки*, а исказот q е *заклучок*. Пред да наведеме примери во кои ќе го применуваме ова правило, да забележиме дека истото уште се запишува во вид на шема на следниов начин: $\frac{p \Rightarrow q, p}{q}$. Да споменеме дека во последната шема запирката во броителот го заменува сврзникот "и", а дробната црта зборот "заклучок" или "следува".

6.3. Пример. а) Имаме:

1) Ако $x = a$, тогаш $x^3 = a^3$.
2) $x = a$.

Заклучок. $x^3 = a^3$.

Да ја појасниме примената на модус поненс. Имаме исказ $p : x = a$ и исказ $q : x^3 = a^3$, па затоа во 1) и 2) се дадени претпоставките $p \Rightarrow q$ и p, од кои следува заклучокот q т.е. $x^3 = a^3$.

б) Имаме:

1) Ако врне дожд, тогаш улицата е мокра.
2) Врне дожд.

Заклучок. Улицата е мокра.

Да ја појасниме примената на модус поненс. Имаме исказ p: "*Врне дожд*" и исказ q: "*Улицата е мокра*", па затоа во 1) и 2) се дадени претпоставките $p \Rightarrow q$ и p, од кои следува заклучокот q, т.е. "*Улицата е мокра*". ♦

6.4. Модус толенс. Да ја разгледаме исказната формула

$$(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p\,. \qquad (2)$$

За да утврдиме дека од $p \Rightarrow q$ и $\neg q$ следува заклучокот $\neg p$, доволно е да докажеме дека исказната формула (1) е тавтологија. Последното ќе го направиме користејќи ја следната таблица на вистинитост.

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$(p \Rightarrow q) \wedge \neg q$	$(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$
Т	Т	⊥	⊥	Т	⊥	Т
Т	⊥	⊥	Т	⊥	⊥	Т
⊥	Т	Т	⊥	Т	⊥	Т
⊥	⊥	Т	Т	Т	Т	Т

Од претходната таблица заклучуваме дека исказната формула (2) е тавтологија, што значи дека таа е логички закон кој го нарекуваме *модус толенс*. Пред да наведеме примери во кои ќе го применуваме ова правило, да забележиме дека истото уште се запишува во вид на шема на следниот начин: $\frac{p \Rightarrow q, \neg q}{\neg p}$.

6.5. Пример. а) Имаме:

1) Ако $x = 1$, тогаш $x^3 = 1$.

2) $x^3 \neq 1$.

Заклучок. $x \neq 1$.

Да ја појасниме примената на модус толенс. Имаме исказ $p : x = 1$ и исказ $q : x^3 = 1$, па затоа во 1) и 2) се дадени претпоставките $p \Rightarrow q$ и $\neg q$, од кои следува заклучокот $\neg p$, т.е. $x \neq 1$.

б) Имаме:

1) Ако врне дожд, тогаш улицата е мокра.
2) Улицата не е мокра.

Заклучок. Не врне дожд.

Да ја појасниме примената на модус толенс. Имаме исказ p: "*Врне дожд*" и исказ q: "*Улицата е мокра*", па затоа во 1) и 2) се дадени претпоставките $p \Rightarrow q$ и $\neg q$, од кои следува заклучокот $\neg p$, т.е. "*Не врне дожд*".

в) Имаме:

1) Ако четириаголник е ромб, тогаш дијагоналите се нормални.
2) Дијагоналите не се нормални.

Заклучок. Четириаголникот не е ромб. ♦

6.6. Хипотетички силогизам. Да ја разгледаме исказната формула

$$(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)\,, \qquad (3)$$

за која знаеме дека е тавтологија, т.е. дека е логички закон кој го нарекуваме *хипотетички силогизам*. Пред да наведеме примери во кои ќе го применуваме ова пра-

вило, да забележиме дека истото уште се запишува во вид на шема на следниов начин: $\frac{p \Rightarrow q,\ q \Rightarrow r}{p \Rightarrow r}$.

6.7. Пример. а) Имаме:

1) Ако збирот на цифрите на бројот n е делив со 9, тогаш n е делив со 9.

2) Ако бројот n е делив со 9, тогаш n е делив со 3.

Заклучок. Ако збирот на цифрите на бројот n е делив со 9, тогаш n е делив со 3.

б) Имаме:

1) Ако дијагоналите на четириаголник $ABCD$ се преполовуваат, тогаш тој е паралелограм.

2) Ако четириаголникот $ABCD$ е паралелограм, тогаш $\overline{AB} = \overline{CD}$.

Заклучок. Ако дијагоналите на четириаголник $ABCD$ се преполовуваат, тогаш $\overline{AB} = \overline{CD}$. ♦

6.8. Коментар. Правилото за хипотетички силогизам може да се обопшти. Притоа имаме

$$\frac{p \Rightarrow p_1,\ p_1 \Rightarrow p_2,\ p_2 \Rightarrow p_3, \ldots, p_{k-1} \Rightarrow p_k,\ p_k \Rightarrow q,}{p \Rightarrow q}. \tag{4}$$

6.8. Правило на контрапозиција. Да ја разгледаме исказната формула

$$(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p), \tag{5}$$

за која знаеме дека е тавтологија, т.е. дека е логички закон кој го нарекуваме *правило за контрапозиција*. Пред да наведеме примери во кои ќе го применуваме ова правило, да забележиме дека истото уште се запишува во вид на шема на следниов начин: $\frac{p \Rightarrow q}{\neg q \Rightarrow \neg p}$.

6.9. Пример. а) Имаме:

Ако цифрата на единиците на природниот број n е 0 или 5, тогаш тој е делив со 5.

Заклучок. Ако природниот број n не е делив со 5, тогаш неговата цифра на единици е различна од 0 и 5.

б) Имаме:

Ако четириаголникот е ромб, тогаш неговите дијагонали се заемно нормални.

Заклучок. Ако дијагоналите не се заемно нормални, тогаш четириаголникот не е ромб. ♦

7. МЕТОДИ ЗА ДОКАЖУВАЊЕ НА ТЕОРЕМИ

7.1. При изучувањето на елементите од математичката логика и теоријата на броеви усвоивме и докажавме повеќе теореми. Притоа, не се осврнавме посебно на методите за докажување и правилата на логичко заклучување, иако истите прекутно ги користевме. Пред да преминеме на разгледување на методите за докажување на математички тврдења, ќе се осврнеме на прашањето што значи да се докаже една теорема.

Да се докаже една теорема значи да се установи точноста на нејзиниот заклучок со помош на логички расудувања, при што се користат: претпоставките на теоремата, правилата за изведување на заклучоци, дефиниции и други тврдења за кои е констатирано дека се вистинити.

Според тоа, *доказ на теорема* претставува конечна низа од реченици $T_1, T_2, ..., T_k$, такви што секоја од нив е или аксиома, или дефиниција, или тврдење чија вистинитост е претходно докажана според правилата за изведување на заклучоци. Ако постои една таква низа тврдења $T_1, T_2, ..., T_k$ која завршува со тврдењето T, тогаш тврдењето T всушност е теоремата која ја докажуваме.

Во натамошните разгледувања ќе се осврнеме на методите на докажување на теоремите, кои според начинот на нивното реализирање ги делиме на *директни и индиректни.*

7.2. Директни методи за докажување. Нека е дадена теоремата $A \Rightarrow B$. Под *директен метод* за докажување на теоремата $A \Rightarrow B$ го подразбираме оној метод кај кој заклучокот B се изведува со директно користење на претпоставката A. Претходно споменавме дека директниот метод по својата форма може да биде:

- *метод со напредување (синтетички метод)* при кој се поаѓа од претпоставката и се стигнува до заклучокот и
- *метод со враќање (аналитички метод),* при кој се поаѓа од заклучокот и се стигнува до претпоставката.

7.2.1. Метод со напредување (синтетички метод). Да ја разгледаме теоремата $A \Rightarrow B$. За да ја докажеме оваа теорема, треба да докажеме дека нејзиниот заклучок B е логичко следство од претпоставката A.

За да докажеме една теорема $A \Rightarrow B$, потребно е да се располага со:

1) определена фамилија $\boldsymbol{F}$ од искази $I_1, I_2, ..., I_k$, кои се вистинити за разгледуваното множество објекти и
2) правила за изведување на заклучоци.

Притоа, ако доказот на тврдењето $A \Rightarrow B$, се реализира според логичката шема:

$$(A \wedge \boldsymbol{F}) \Rightarrow B_1, \quad B_1 \Rightarrow B_2, \ ..., \quad B_{n-1} \Rightarrow B_n, \quad B_n \Rightarrow B$$

каде што $\boldsymbol{F}$ е фамилијата вистинити искази и $B_1, B_2, ..., B_{n-1}, B_n, B, A$ е конечна низа од реченици, тогаш ќе велиме дека тврдењето е докажано со методот на напредување.

Според тоа, директен доказ со напредување претставува низа од правилни расудувања, таква што заклучокот на секое од нив влегува како претпоставка на некое од следните расудувања, а заклучокот на последното расудување е заклучокот во самата теорема. Ќе разгледаме два примера.

7.2.1.1. Пример. Ќе го анализираме доказот на теоремата:

"*Ако* $a,b\in\mathbf{N}$, $a\mid b$ *и* $b\mid a$, *тогаш* $a=b$."

Претпоставки A: "$a,b\in\mathbf{N}$, $a\mid b$ и $b\mid a$". ***Заклучок*** B: "$a=b$."

Тврдење B_1: "постои $q\in\mathbf{N}$ таков што $b=aq$ и постои $p\in\mathbf{N}$ таков, што $a=bp$", (следува од претпоставките и дефиницијата за деливост).

Тврдење B_2: "$b=b(pq)$", (следува од B_1: $b=aq$, $a=bp$ и асоцијативниот закон за множење на природни броеви: $b=aq=(bp)q=b(pq)$).

Тврдење B_3: "$pq=1$, $p,q\in\mathbf{N}$", (следува од B_2: $b=b(pq)$, $b\neq 0$ и законот за кратење).

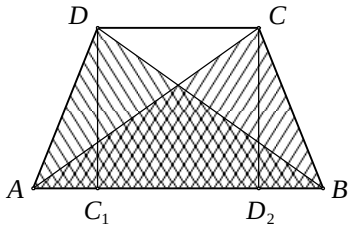
Тврдење B_4: "$p=q=1$", (следува од B_3: $pq=1$, $p,q\in\mathbf{N}$ и својствата на природните броеви),

Тврдење B: "$a=b$", (следува од B_4: "$p=q=1$ и $a=bp=b\cdot 1=b$).

Конечно, имаме $A\Rightarrow B_1$, $B_1\Rightarrow B_2$, $B_2\Rightarrow B_3$, $B_3\Rightarrow B_4$, $B_4\Rightarrow B$ од што според хипотетичкиот силогизам добиваме $A\Rightarrow B$. ♦

7.2.1.2. Пример. Ќе ја докажеме теоремата:

"*Ако еден трапез е рамнокрак, тогаш дијагоналите на тој трапез се еднакви.*"



Претпоставка p: "Трапезот $ABCD$ е рамнокрак."

Заклучок q**:** "Дијагоналите AC и BD се еднакви: $\overline{AC}=\overline{BD}$."

Од темињата C и D повлекуваме нормали CD_2 и DC_1 на страната AB (цртеж десно).

Тврдење r_1: "четириаголникот CDC_1D_2 е правоаголник", (од конструкцијата и p: трапезот $ABCD$ е рамнокрак).

Тврдење r_2: "$\angle AC_1D=\angle BD_2C=90^\circ$", (од r_1: четириаголникот CDD_1C_1 е правоаголник).

Тврдење r_3: "$\Delta AC_1D\cong\Delta BD_2C$", (од r_2: $\angle AC_1D=\angle BD_2C=90^\circ$, p: трапезот $ABCD$ е рамнокрак и признакот за складност ССА).

Тврдење r_4: "$\angle C_1AD=\angle D_2BC$", (од r_3: $\Delta AC_1D\cong\Delta BD_2C$).

Тврдење r_5: "$\Delta ABD\cong\Delta BAC$", (од r_4: $\angle C_1AD=\angle D_2BC$, p: трапезот $ABCD$ е рамнокрак и признакот за складност САС).

Тврдење q: "дијагоналите AC и BD се еднакви: $\overline{AC}=\overline{BD}$", (од r_5: $\Delta ABD\cong\Delta BAC$).

Конечно, имаме

$$p \Rightarrow r_1,\ r_1 \Rightarrow r_2, (r_2 \wedge p) \Rightarrow r_3, r_3 \Rightarrow r_4, (r_4 \wedge p) \Rightarrow r_5, r_5 \Rightarrow q$$

од што според хипотетичкиот силогизам добиваме $p \Rightarrow q$. ♦

7.3. Метод со враќање (аналитичен метод). Процесот на размислување при докажување на теоремата $A \Rightarrow B$ со аналитичкиот метод се одвива на следниов начин:

Се тргнува од заклучокот на теоремата B и се избира доволен услов B_1 таков што импликацијата $B_1 \Rightarrow B$ и B_1 да се вистинити. Потоа се избира доволен услов B_2 за B_1 таков што импликацијата $B_2 \Rightarrow B_1$ и B_2 да се вистинити. Постапката се продолжува сè додека не се добие доволен услов B_n за B_{n-1} таков што импликацијата $B_n \Rightarrow B_{n-1}$ и B_n да се вистинити и притоа да е вистинита и импликацијата $A \Rightarrow B_n$. Јасно, при докажувањето на теоремата се користат како условот A, така и фамилијата $\boldsymbol{F}$ од вистинити искази.

Симболички, процесот на размислување со аналитичкиот метод може да се запише со помош на шемата:

$$B_1 \Rightarrow B,\ \ B_2 \Rightarrow B_1,\ \ ...,\ B_n \Rightarrow B_{n-1},\ \ (A \wedge \boldsymbol{F}) \Rightarrow B_n$$

Претходната шема е еквивалентна на шемата

$$(A \wedge \boldsymbol{F}) \Rightarrow B_n,\ B_n \Rightarrow B_{n-1},\ \ ...,\ \ B_2 \Rightarrow B_1,\ \ B_1 \Rightarrow B,$$

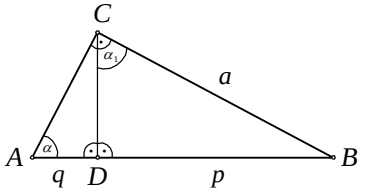
што значи дека секој доказ добиен со аналитичкиот метод може да се запише во вид на доказ добиен со синтетичкиот метод, од што следува дека доказите добиени со аналитичкиот метод се коректни и строги.

7.4. Пример. Да ја докажеме теоремата:

"*Ако во правоаголен триаголник со хипотенуза c ортогоналната проекција на катетата a врз хипотенузата е p, тогаш* $a^2 = pc$."

Дадено е (A): ΔABC е правоаголен со прав агол во темето C, $c = \overline{AB}$, $p = \overline{BD}$ и $a = \overline{BC}$. Треба да докажеме:

$$a^2 = pc \qquad (B)$$



Да тргнеме од равенството (B), кое е еквивалентно на равенството:

$$\overline{BC}^2 = \overline{AB} \cdot \overline{DB},$$

односно на равенството:

$$\overline{BC} : \overline{DB} = \overline{AB} : \overline{BC} \qquad (B_1)$$

кое е пропорција на четири отсечки, па затоа постои можност да имаме слични триаголници за кои овие отсечки се нивни страни. Разгледувањето на цртежот нè

доведува до ΔABC и ΔCDB. Значи за да биде точно тврдењето (B_1), доволно е да биде исполнето

$$\Delta ABC \sim \Delta CDB . \qquad (B_2)$$

Понатаму, за да биде исполнето тврдењето (B_2) доволно е овие два триаголника да имаат по два еднакви агли, а за тоа да биде исполнето доволно е да биде исполнето (види цртеж)

$$\angle CAB = \angle DCB . \qquad (B_3)$$

Последното тврдење е точно ако е исполнето тврдењето:

$$CD \perp AB \text{ и } AC \perp BC , \qquad (B_4)$$

кое е очигледно точно бидејќи ΔABC е правоаголен и CD е неговата висина.

Според тоа, важи $B_1 \Rightarrow B, B_2 \Rightarrow B_1, B_3 \Rightarrow B_2, B_4 \Rightarrow B_3, A \Rightarrow B_4$, односно важи

$$A \Rightarrow B_4 \Rightarrow B_3 \Rightarrow B_2 \Rightarrow B_1 \Rightarrow B ,$$

со што теоремата е докажана. ♦

7.5. Индиректни методи за докажување. *Индиректен метод* за докажување на теоремата $A \Rightarrow B$ го нарекуваме оној метод при кој вистинитоста на теоремата се докажува со помош на тврдење кое е еквивалентно на теоремата. Од индиректните методи најчесто се користи методот за докажување од спротивното, при кој се докажува дека тврдењето $\neg B$ не е вистинито.

Понекогаш откривањето на импликациите

$$(A \wedge \boldsymbol{F}) \Rightarrow B_1, \quad B_1 \Rightarrow B_2, \ ..., \quad B_n \Rightarrow B_{n-1}, \quad B_n \Rightarrow B$$

при синтетичкиот метод, или на импликациите

$$(A \wedge \boldsymbol{F}) \Rightarrow B_n, \ B_n \Rightarrow B_{n-1}, \quad ..., \quad B_2 \Rightarrow B_1, \quad B_1 \Rightarrow B$$

при аналитичкиот метод на докажување, е доста тешко или речиси невозможно. Во вакви случаи најчесто се користи некоја од следниве еквиваленции:

$$\begin{aligned} &(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A) \\ &(A \Rightarrow B) \Leftrightarrow (\neg B \wedge A \Rightarrow \neg A) \\ &(A \Rightarrow B) \Leftrightarrow (\neg B \wedge A \Rightarrow B) \\ &(A \Rightarrow B) \Leftrightarrow (\neg B \wedge A \Rightarrow C \wedge \neg C) \end{aligned} \qquad (1)$$

и потоа преку докажување на импликациите кои се наоѓаат на левата страна од овие еквиваленции се докажува теоремата $A \Rightarrow B$. Всушност овие еквиваленции се и основата на индиректните методи за докажување на теоремите, кои се реализираат со докажување дека негацијата на теоремата не е вистинита.

7.6. Пример. Да го анализираме доказот на теоремата:

"Ако $d = \mathrm{NZD}(a,b)$, $a = \alpha d$ *и* $b = \beta d$, *тогаш* $\mathrm{NZD}(\alpha, \beta) = 1$."

Претпоставка A**:** "$d = \mathrm{NZD}(a,b)$, $a = \alpha d$ и $b = \beta d$."

Заклучок B**:** "$\mathrm{NZD}(\alpha, \beta) = 1$."

Го негираме заклучокот $\neg B$: $\mathrm{NZD}(\alpha,\beta)=k>1$.

Тврдење B_1: "постојат природни броеви α_1 и β_1, такви што $\alpha=k\alpha_1$ и $\beta=k\beta_1$." (следува од $\neg B$).

Тврдење B_2: "$(kd)\,|\,a$ и $(kd)\,|\,b$", (следува од A и B_1).

Тврдење $\neg A$: "kd е заеднички делител на a и b, кој е поголем од d", (следува од B_2).

Значи, $\neg B \Rightarrow B_1$, $B_1 \Rightarrow B_2$, $B_2 \Rightarrow \neg A$, па од правилото хипотетички силогизам имаме $\neg B \Rightarrow \neg A$. Според тоа, за теоремата искажана во условна форма $A \Rightarrow B$, ја докажавме импликацијата $\neg B \Rightarrow \neg A$, па од првата еквиваленција во (1) следува точноста на теоремата. ♦

7.7. Пример. Да го анализираме доказот на теоремата:

"*Постојат бесконечно многу прости броеви*."

Тврдење p: "Постојат бесконечно многу прости броеви."

Тврдење $\neg p$: "Постојат конечно многу прости броеви и тоа се броевите:

$$p_1=2,\ p_2=3,\ \ldots,\ p_n=p\ .\text{"} \tag{2}$$

Тврдење q: "Бројот $N=p_1p_2p_3\ldots p_n+1$ е прост или има прост делител различен од $p_1=2,\ p_2=3,\ \ldots,\ p_n=p$." (следува од $\neg p$ и дефиницијата за деливост).

Тврдење $\neg\neg p$: "Постои прост број кој не се содржи во низата (2)." (следува од q).

Точноста на теоремата следува од тафтологијата $p \Leftrightarrow \neg\neg p$. ♦

8. МАТЕМАТИЧКА ИНДУКЦИЈА

8.1. Како што знаеме, во множеството природни броеви $\mathbf{N}=\{1,2,\ldots,n,\ldots\}$ операциите собирање и множење се целосно изводливи, а додека одземањето и делењето се делумни операции во $\mathbf{N}$. Во оваа точка нема да го разгледуваме воведувањето на множеството природни броеви и операциите во него, но ќе ги искористиме Пеановите аксиоми кои го дефинираат множеството $\mathbf{N}$, за да го воведеме принципот на математичка индукција, кој е еден од најчесто користените методи за докажување тврдења во множествата природни и цели броеви.

На значењето на Пеановите аксиоми нема посебно да се задржуваме, меѓутоа да забележиме дека со првата и четвртата аксиома се обезбедува бројот 1 да припаѓа на множеството природни броеви и тој да е "првиот" природен број. Понатаму, со втората аксиома се задаваат броевите $2=1^+$, $3=2^+$ итн., а нивната единственост ја овозможуваат третата и четвртата аксиома. За нашите разгледувања, од посебно значење е петтата аксиома, која уште е позната како *аксиома за*

индукција и која всушност обезбедува единственост на множеството природни броеви. Всушност, единствеността на множеството природни броеви лежи во основата на *принципот на математичка индукција* (ПМИ), кој е еден од основните методи за докажување на математички тврдења и кој гласи:

Ако треба да ја докажеме точноста на некое математичко тврдење T, кое зависи од природниот број n, и ако за T знаеме дека:

i) T е точно за природниот број 1;

ii) од претпоставката дека T е точно за некој природен број $k \geq 1$, следува дека T е точно и за $k+1$;

тогаш ова тврдење T е точно за секој природен број n.

8.2. Пример. Докажете дека збирот на првите n природни броеви е еднаков на

$$\frac{n(n+1)}{2}.$$

Решение. Да означиме $S_1 = 1;\ S_2 = 1+2;\ \ldots,\ S_n = 1+2+\ldots+n$, т.е. S_n е збирот на првите n природни броеви. Треба да докажеме дека

$$S_n = \frac{n(n+1)}{2}. \tag{1}$$

Прв чекор. Да провериме дека оваа формула е точна за бројот 1. Навистина $S_1 = 1$, а од (1) добиваме дека $S_1 = \frac{1(1+1)}{2} = 1$.

Втор чекор. Да претпоставиме дека за некој природен број $k \geq 1$ формулата (1) е точна, т.е. за збирот на првите k природни броеви знаеме дека $S_k = \frac{k(k+1)}{2}$.

Ќе докажеме дека формулата (1) важи и за следниот природен број $k+1$, т.е. дека

$$S_{k+1} = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}.$$

Имаме:

$$S_{k+1} = \underbrace{(1+2+\ldots+k)}_{S_k} + (k+1) = S_k + (k+1).$$

Сега од претпоставката во вториот чекор следува

$$S_{k+1} = S_k + (k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)[\frac{k}{2}+1] = (k+1)\frac{k+2}{2} = \frac{(k+1)(k+2)}{2}.$$

Според тоа, во првиот чекор докажавме дека условот *i*) од ПМИ е исполнет, а во вториот чекор дека условот *ii*) од ПМИ е исто така исполнет. Следствено, согласно со ПМИ формулата (1) важи за секој природен број $n \geq 1$. ♦

8.3. Забелешка. Често пати проверката во првиот чекор се нарекува *база на индукцијата* (БИ), а претпоставката во вториот чекор *индуктивна претпоставка* (ИП). ♦

8.4. Забелешка. Со помош на аксиомата за индукција може да се докаже и *вториот принцип на математичка индукција*, кој гласи:

Ако треба да ја докажеме точноста на некое математичко тврдење T, кое зависи од природниот број n, и ако за T знаеме дека:

iii) T е точно за некој конкретен природен број m;

iv) од претпоставката дека T е точно за некој природен број $k \geq m$, следува дека T е точно и за $k+1$;

тогаш ова тврдење е точно за секој природен број $n \geq m$. ♦

8.5. Пример. За секој природен број m означуваме $m! = 1 \cdot 2 \cdot ... \cdot m$ и по дефиниција ставаме $0! = 1$. Докажи дека

$$(2n)! < 2^{2n}(n!)^2, \text{ за } n > 1.$$

Решение. Чекор 1. БИ: За $n = 2$ имаме

$$(2 \cdot 2)! = 4! = 24 < 64 = 2^{2 \cdot 2}(2!)^2,$$

т.е. неравенството важи.

Чекор 2. ИП: Нека претпоставиме дека за некој природен број $k \geq 2$ важи $(2k)! < 2^{2k}(k!)^2$.

Од ИП за $k+1$ имаме

$$\begin{aligned}[2(k+1)]! &= (2k)!(2k+1)(2k+2) < 2^{2k}(k!)^2(2k+1)2(k+1) \\ &< 2^{2k+1}k!(k+1)k!2(k+1) = 2^{2(k+1)}[(k+1)!]^2,\end{aligned}$$

т.е. неравенството важи и за $k+1$, што значи важи за секој $n > 1$. ♦

8.6. Забелешка. При докажувањето на некои тврдења се користи и таканаречената *индукција со двојна основа*, која симболички е искажана на следниов начин:

v) T е точно за природните броеви m и $m+1$;

vi) од претпоставката дека T е точно за некои природни броеви k и $k+1$, $k \geq m$, следува дека T е точно и за $k+2$;

тогаш ова тврдење е точно за секој природен број $n \geq m$. ♦

8.7. Пример. Броевите $a_n, n = 0,1,...$ се зададени со формулите $a_0 = 2$, $a_1 = \frac{5}{2}$ и

$$a_n = \tfrac{5}{2}a_{n-1} - a_{n-2}, \text{ за } n > 1. \tag{2}$$

Докажи дека за секој $n = 0,1,2,3,...$ важи

$$a_n = 2^n + 2^{-n}. \tag{3}$$

Решение. Чекор 1. БИ: За $n = 0$ и $n = 1$ имаме

$$a_0 = 2 = 1+1 = 2^0 + 2^{-0} \text{ и } a_1 = \tfrac{5}{2} = 2 + \tfrac{1}{2} = 2^1 + 2^{-1}$$

што значи дека формулата (3) важи за $n = 0$ и $n = 1$.

Чекор 2. ИП: Нека претпоставиме дека формулата (3) важи за $n = k$ и $n = k+1$, т.е. дека важи $a_k = 2^k + 2^{-k}$ и $a_{k+1} = 2^{k+1} + 2^{-(k+1)}$.

Ако ја искористиме релацијата (2) и индуктивната претпоставка, тогаш за $n = k+2$ добоваме

$$\begin{aligned} a_{k+2} &= \tfrac{5}{2} a_{k+2-1} - a_{k+2-2} = \tfrac{5}{2} a_{k+1} - a_k = \tfrac{5}{2}(2^{k+1} + 2^{-(k+1)}) - (2^k + 2^{-k}) \\ &= 5 \cdot 2^k + 5 \cdot 2^{-k-2} - 2^k - 2^{-k} = 4 \cdot 2^k + 2^{-k-2} + 4 \cdot 2^{-k-2} - 2^{-k} \\ &= 2^2 2^k + 2^{-(k+2)} + 2^2 2^{-k-2} - 2^{-k} = 2^{k+2} + 2^{-(k+2)} + 2^{-k} - 2^{-k} \\ &= 2^{k+2} + 2^{-(k+2)}, \end{aligned}$$

т.е. формулата (3) важи за $n = k+2$, па од забелешка 8.6 следува дека формулата (3) важи за секој $n = 0, 1, 2, 3, \ldots$. ♦

8.8. Лема. (неравенство на Бернули). Ако $x > -1$, тогаш

$$(1+x)^n \geq 1 + nx \text{, за секој } n \in \mathbf{N}. \tag{4}$$

Доказ. За $n = 1$ имаме $1 + x \geq 1 + x$, т.е. неравенството важи.

Нека претпоставиме дека за $n = k$, важи $(1+x)^k \geq 1 + kx$.

Нека $n = k+1$. Од индуктивната претпоставка и бидејќи $1 + x > 0$ имаме

$$\begin{aligned} (1+x)^{k+1} &= (1+x)^k (1+x) \geq (1+kx)(1+x) = 1 + kx + x + kx^2 \\ &= 1 + (k+1)x + kx^2 \geq 1 + (k+1)x \end{aligned}$$

т.е. неравенството (4) важи и за $n = k+1$, па од принципот на математичка индукција добиваме дека важи за секој $n \in \mathbf{N}$ и секој реален број $x > -1$. ♦

8.9. Лема. ако $x_i > 0$, $i = 1, 2, \ldots, n$ и $x_1 x_2 \ldots x_n = 1$ тогаш

$$x_1 + x_2 + \ldots + x_n \geq n,$$

при што $x_1 + x_2 + \ldots + x_n = n$ ако и само ако $x_1 = x_2 = \ldots = x_n = 1$.

Доказ. Даденото неравенство ќе го докажеме со математичка индукција по n.

i) За $n = 1$ неравенството е точно и притоа важи знак на равенство.

Ако $n = 2$ и $x_1 x_2 = 1$, тогаш едниот број е поголем или еднаков на 1, а другиот е помал или еднаков на 1, на пример $x_1 \leq 1$ и $x_2 \geq 1$. Според тоа,

$$x_1 + x_2 = 1 + x_1 x_2 + (x_2 - 1)(1 - x_1) = 2 + (x_2 - 1)(1 - x_1) \geq 2$$

и знак за равенство важи ако и само ако $x_2 - 1 = 0$ или $1 - x_1 = 0$, што заедно со $x_1 x_2 = 1$ дава $x_1 = x_2 = 1$.

ii) Нека претпоставиме дека за $n=k$ и произволни реални броеви x_i, $i=1,2,...,k$, чиј производ е единица, точно е неравенството

$$x_1+x_2+...+x_k \geq k$$

при што знак за равенство важи ако и само ако $x_i=1,\ i=1,2,...,k$.

Нека $n=k+1$ и $x_1,...,x_{k+1}$ се позитивни реални броеви за кои $x_1x_2...x_kx_{k+1}=1$. Ако сите x_i не се еднакви на 1, тогаш имаме броеви поголеми од 1, но и помали од 1. Без ограничување на општоста можеме да земеме $x_1<1$ и $x_2>1$. Тогаш имаме k позитивни броеви $x_1x_2, x_3,..., x_{k+1}$ чиј производ е еднаков на 1, па според индуктивната претпоставка добиваме

$$x_1x_2+x_3+...+x_k+x_{k+1} \geq k$$

при што знак за равенство важи ако и само ако

$$x_1x_2=x_3=...=x_k=x_{k+1}=1.$$

Но, тогаш

$$x_1+x_2+...+x_k+x_{k+1}=1+x_1x_2+x_3+x_4+...+x_k+x_{k+1}+(x_2-1)(1-x_1)$$
$$\geq k+1+(x_2-1)(1-x_1) \geq k+1$$

при што знак за равенство важи ако и само ако

$$x_1x_2=x_3=...=x_k=x_{k+1}=1$$

и при тоа $(x_2-1)(1-x_1)=0$, т.е. $x_1=x_2=x_3=...=x_k=x_{k+1}=1$. ♦

8.10. Дефиниција. Нека се дадени n позитивни реални броеви $a_1, a_2,...,$ a_n. Броевите

$$\frac{1}{n}\sum_{i=1}^{n} a_i\ ,\ (\prod_{i=1}^{n} a_i)^{1/n}\ ,\ \frac{n}{\sum_{i=1}^{n} a_i^{-1}}$$

ги нарекуваме *аритметичка, геометриска и хармониска средина* на броевите $a_1, a_2,..., a_n$, соодветно.

8.11. Теорема (Неравенство на Коши). За аритметичката, геометриската и хармониската средина на позитивните реални броеви $a_1, a_2,..., a_n$ важи

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geq (\prod_{i=1}^{n} a_i)^{1/n} \geq \frac{n}{\sum_{i=1}^{n} a_i^{-1}}$$

при што знак за равенство важи ако и само ако $a_1=a_2=...=a_n$.

Доказ. Означуваме $\beta_n=(\prod_{i=1}^{n} a_i)^{1/n}$. Да ги разгледаме следниве n позитивни реални броеви $y_i=\frac{a_i}{\beta_n}$, $i=1,2,...,n$. За броевите y_i, $i=1,2,...,n$ важи $\prod_{i=1}^{n} y_i=1$, што според лема 8.9 значи $y_1+y_2+...+y_n \geq n$, т.е.

$$\frac{a_1}{\beta_n}+\frac{a_2}{\beta_n}+\ldots+\frac{a_n}{\beta_n}\geq n$$

односно $\frac{1}{n}\sum_{i=1}^{n}a_i\geq(\prod_{i=1}^{n}a_i)^{1/n}$. Притоа, знак за равенство важи ако и само ако $y_1=y_2=\ldots=y_n$, т.е. ако и само ако $a_1=a_2=\ldots=a_n$.

Од претходно изнесеното имаме:

$$\frac{1}{(\prod_{i=1}^{n}a_i)^{1/n}}=(\frac{1}{a_1}\cdot\frac{1}{a_2}\cdot\ldots\cdot\frac{1}{a_n})^{1/n}\leq\frac{\frac{1}{a_1}+\frac{1}{a_2}+\ldots+\frac{1}{a_n}}{n}=\frac{1}{\frac{n}{\sum_{i=1}^{n}a_i^{-1}}}$$

односно $(\prod_{i=1}^{n}a_i)^{1/n}\geq\frac{n}{\sum_{i=1}^{n}a_i^{-1}}$, при што знак за равенство важи ако и само ако $\frac{1}{a_1}=\frac{1}{a_2}=\ldots=\frac{1}{a_n}$, т.е. ако и само ако $a_1=a_2=\ldots=a_n$. ♦

8.12. Пример. Докажи дека за секој $x>0$ и за секој $n\in\mathbf{N}$ важи неравенството

$$1+\frac{x}{n}\geq\sqrt[n]{1+x}$$

Решение. Прв начин. За $x>0$ и $n\in\mathbf{N}$ имаме $\frac{x}{n}>-1$. Од неравенството на Бернули добиваме:

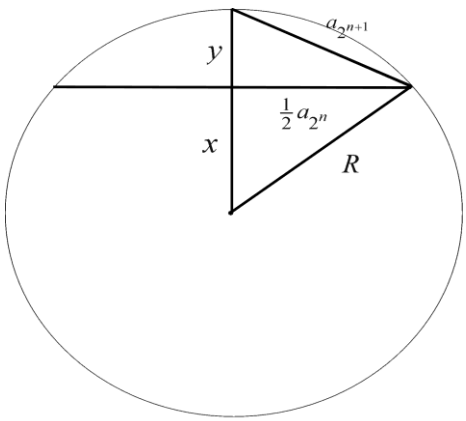
$$(1+\frac{x}{n})^n\geq1+n\cdot\frac{x}{n}=1+x \text{ т.е. } 1+\frac{x}{n}\geq\sqrt[n]{1+x}.$$

Втор начин. Од неравенството помеѓу аритметичка и геометриска средина, при $x_1=x_2=\ldots=x_{n-1}=1$ и $x_n=1+x$ добиваме

$$\frac{x_1+x_2+\ldots+x_n}{n}\geq\sqrt[n]{1\cdot1\cdot1\cdot\ldots\cdot1\cdot(1+x)}$$

односно $1+\frac{x}{n}\geq\sqrt[n]{1+x}$. ♦

8.13. Во претходните разгледувања се запознавме со методот на математичка индукција и разгледавме некои негови примени во алгебрата. Во натамошните разгледувања ќе покажеме како математичката индукција може да се примени во геометријата. Ќе разгледаме неколку примери.



Цртеж 1

8.14. Пример. Пресметај ја страната a_{2^n} на правилен 2^n – аголник, впишан во кружница со радиус R.

Решение. За $n=2$ правилниот

2^n – аголник е квадрат, па затоа неговата страна е $a_4 = R\sqrt{2}$. Понатаму, ако го искористиме цртеж 1) наоѓаме:

$$\begin{aligned} a_{2^{n+1}} &= \sqrt{\frac{a_{2^n}^2}{4} + y^2} = \sqrt{\frac{a_{2^n}^2}{4} + (R-x)^2} \\ &= \sqrt{\frac{a_{2^n}^2}{4} + (R - \sqrt{R^2 - \frac{a_{2^n}^2}{4}})^2} \\ &= \sqrt{2R^2 - 2R\sqrt{R^2 - \frac{a_{2^n}^2}{4}}}. \end{aligned} \tag{1}$$

Од претходно изнесеното следува дека страната на правилниот осумаголник впишан во кружница со радиус R е

$$a_8 = \sqrt{2R^2 - 2R\sqrt{R^2 - \frac{(R\sqrt{2})^2}{4}}} = \sqrt{2R^2 - 2R\sqrt{\frac{2R^2}{4}}} = \sqrt{2R^2 - R^2\sqrt{2}} = R\sqrt{2-\sqrt{2}}.$$

Аналогно се покажува дека страните на правилниот шеснаесетаголник и правилниот 32-аголник впишан во кружница со радиус R се:

$$a_{16} = R\sqrt{2-\sqrt{2+\sqrt{2}}} \quad \text{и} \quad a_{32} = R\sqrt{2-\sqrt{2+\sqrt{2+\sqrt{2}}}},$$

соодветно. Затоа природно е да претпоставиме, дека за секој $n \geq 2$ страната a_{2^n} на правилниот 2^n – аголник, впишан во кружница со радиус R е дадена со формулата

$$a_{2^n} = R\underbrace{\sqrt{2-\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n-1 \text{ корен}}. \tag{2}$$

Користејќи го принципот на математичка индукција ќе докажеме дека формулата (2) е точна за секој $n \geq 2$.

а) Јасно, формулата (2) важи за $n = 2$.

б) Нека претпоставиме дека (2) важи за некој природен број $n \geq 2$. Сега, од (1) следува

$$a_{2^{n+1}} = \sqrt{2R^2 - 2R\sqrt{R^2 - \frac{a_{2^n}^2}{4}}} = \sqrt{2R^2 - 2R\sqrt{R^2 - \tfrac{1}{4}(R\underbrace{\sqrt{2-\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n-1 \text{ корен}})^2}}$$

$$= R\sqrt{2-2\sqrt{1-\tfrac{1}{4}(2-\underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}_{n-2 \text{ корени}})}} = R\underbrace{\sqrt{2-\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n \text{ корени}},$$

па од принципот на математичка индукција следува дека формулата (2) важи за секој природен број $n \geq 2$. ♦

8.15. Забелешка. Ако земеме предвид дека должината на кружниците со радиус R е $L = 2\pi R$ и дека кога $n \to \infty$ истата е граница на периметрите на впишаните 2^n – аголници добиваме дека

$$2\pi R = \lim_{n\to\infty} 2^n a_{2^n} = \lim_{n\to\infty} 2^n R \underbrace{\sqrt{2-\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n-1 \text{ корен}}$$

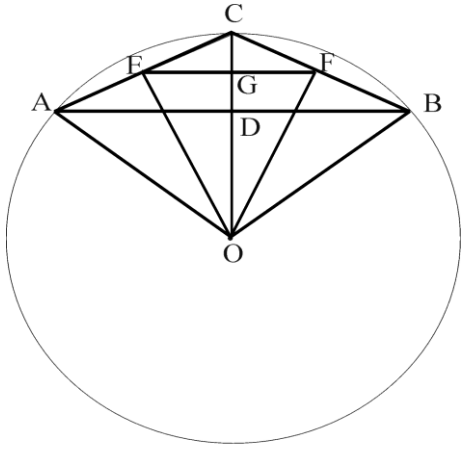
т.е.

$$\pi = \lim_{n\to\infty} 2^{n-1} \underbrace{\sqrt{2-\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n-1 \text{ корен}} . \blacklozenge$$

8.16. Пример. Најди правило за пресметување на радиусите r_n и R_n на впишаната и опишаната кружница околу правилен 2^n – аголник со даден периметар p.

Решение. а) Лесно се пресметува дека $r_2 = \frac{p}{8}$ и $R_2 = \frac{p\sqrt{2}}{8}$.

б) Нека се дадени радиусите r_n и R_n на впишаната и опишаната кружница околу правилен 2^n – аголник со даден периметар p. Ќе ги пресметаме радиусите r_{n+1} и R_{n+1} на впишаната и опишаната кружница околу правилен 2^{n+1} – аголник со истиот периметар. Нека AB е страната на правилниот 2^n – аголник со периметар p, O е неговиот центар, C е средината на лакот AB и D е средината на тетивата AB (црт. 2). Понатаму, нека EF е средната линија на триаголникот ABC паралелна на страната AB и G е средината на отсечката EF. Од



Цртеж 2

$$\measuredangle EOF = \measuredangle EOC + \measuredangle FOC = \tfrac{1}{2}\measuredangle AOC + \tfrac{1}{2}\measuredangle BOC = \tfrac{1}{2}\measuredangle AOB$$

следува дека отсечката EF е еднаква на страната на правилниот 2^{n+1} – аголник впишан во кружница со радиус OE, при што периметарот на овој 2^{n+1} – аголник е еднаков на

$$2^{n+1}\overline{EF} = 2^{n+1}\,\frac{\overline{AB}}{2} = 2^n \overline{AB} = p .$$

Според тоа, $r_{n+1} = \overline{OG}$ и $R_{n+1} = \overline{OE}$. Понатаму е јасно дека

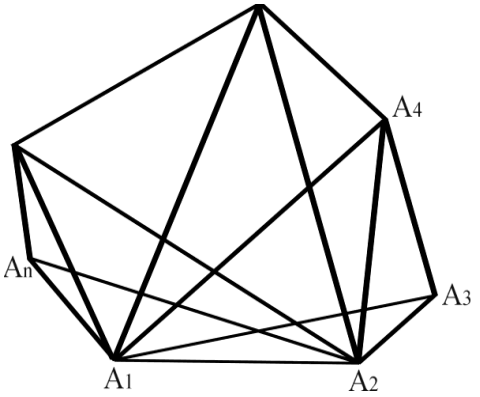
$$\overline{OC} - \overline{OG} = \overline{OG} - \overline{OD}, \text{ т.е. } R_n - r_{n+1} = r_{n+1} - r_n ,$$

од каде наоѓаме $r_{n+1} = \frac{R_n + r_n}{2}$. Конечно, од правоаголниот триаголник OEC имаме $\overline{OE}^2 = \overline{OC}\cdot\overline{OG}$, т.е. $R_{n+1}^2 = R_n r_{n+1}$ па затоа $R_{n+1} = \sqrt{R_n r_{n+1}}$. Конечно

$$r_{n+1} = \frac{R_n + r_n}{2} \text{ и } R_{n+1} = \sqrt{R_n r_{n+1}} . \blacklozenge$$

8.17. Пример. Најди правило за пресметување на бројот $P(n)$ на начините, со кои конвексен $n-$аголник може да биде поделен на триаголници со негови дијагонали кои не се сечат.

Решение. За триаголник овој број очигледно е еднаков на еден, т.е. $P(3)=1$.



Нека претпоставиме дека сме ги определиле броевите $P(k)$, $k<n$. За да го определиме бројот $P(n)$ ќе го разгледаме конвексниот $n-$аголник $A_1A_2...A_n$. При секоја негова поделба на триаголници страната A_1A_2 ќе биде страна на еден од добиените триаголници, чие трето теме може да се совпадне со секоја од точките $A_3, A_4, ..., A_n$. Притоа, бројот на начините на поделба на $n-$аголникот, при кои третото теме на триаголникот ќе се совпадне со точката A_3 е еднаков на бројот на начините на поделбата на $(n-1)-$аголникот $A_1A_3A_4...A_n$, т.е. тој е еднаков на $P(n-1)$. Бројот на начините на поделба, при кои третото теме ќе се совпадне со точката A_4 е еднаков на бројот на начините $P(n-2)$ на поделба на $(n-2)-$аголникот $A_1A_4...A_n$ помножен со бројот на поделба $P(3)$ на триаголникот $A_2A_3A_4$ (зошто?). Бројот на начините на поделба, при кои третото теме се совпаѓа со точката A_5 е еднаков на $P(n-3)P(4)$, бидејќи секоја поделба на $(n-3)-$аголникот $A_1A_5...A_n$ се комбинира со секоја поделба на четириаголникот $A_2A_3A_4A_5$. Продолжувајќи ја постапката ја наоѓаме релацијата:

$$P(n)=P(n-1)+P(n-2)P(3)+P(n-3)P(4)+...+P(3)P(n-2)+P(n-1)\ . \quad (3)$$

Ако ја искористиме релацијата (3) последователно наоѓаме:

$$P(4)=P(3)+P(3)=2,$$
$$P(5)=P(4)+P(3)P(3)+P(4)=5,$$
$$P(6)=P(5)+P(4)P(3)+P(3)P(4)+P(5)=14,$$
$$P(7)=P(6)+P(5)P(3)+P(4)P(4)+P(3)P(5)+P(6)=42,$$
$$P(8)=P(7)+P(6)P(3)+P(5)P(4)+P(4)P(5)+P(3)P(6)+P(7)=132 \quad \text{итн.}$$

8.18. Забелешка. Користејќи ја формулата (3) може да се докаже, дека за секој $n\geq 3$ важи

$$P(n)=\frac{2(2n-5)!}{(n-1)!(n-3)!}\ .$$

Последната формула нема да ја докажуваме, бидејќи истата излегува надвор од рамките на нашите разгледувања. ♦

8.19. Во геометријата принципот на математичка индукција може да се искористи и за пресметувања според димензијата во која се разгледува задачата, т.е. задачата последователно да се разгледува на права, во рамнина и во простор.

Пример. а) На колку делови n точки ја делат правата.

б) На колку делови ја делата рамнината n прави такви што секои две од нив се сечат и никои три немаат заедничка точка (прави во општа положба)

в) На колку делови го делат просторот n рамнини такви што секои три рамнини се сечат и никои четири рамнини немаат заедничка точка (рамнини во општа положба).

Решение. а) Ако со $F_1(n)$ го означиме бараниот број, тогаш очигледно $F_1(n)=n+1$.

б) Една права ја дели рамнината на два дела.

Нека претпоставиме, дека е познат бројот $F_2(n)$ на деловите, на кои n прави во општа положба ја делат рамнината и нека се дадени $n+1$ права во општа положба. Првите n прави ја делат рамнината на $F_2(n)$ делови, а според условот $(n+1)-$та права p ги сече останатите n прави во n различни точки. Според задачата под а) овие n точки ја делат правата p на $F_1(n)=n+1$ делови. Според тоа, правата p сече $F_1(n)=n+1$ од веќе добиените делови на кои првите n прави ја делат рамнината и истите ги удвојува, што значи дека таа на веќе добиените $F_2(n)$ додава нови $F_1(n)=n+1$ делови. Значи, за бројот на деловите на кој $n+1$ права во општа положба ја делат рамнината важи

$$F_2(n+1)=F_2(n)+F_1(n)=F_2(n)+(n+1)\,. \tag{4}$$

Ако во равенството (4), наместо n последователно ставиме

$$n-1, n-2, n-3, ..., 2, 1$$

добиваме

$$\begin{aligned}
&F_2(n)=F_2(n-1)+n,\\
&F_2(n-1)=F_2(n-2)+n-1,\\
&F_2(n-2)=F_2(n-3)+n-2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&F_2(3)=F_2(2)+3,\\
&F_2(2)=F_2(1)+2.
\end{aligned}$$

Ако ги собереме последните равенства и земеме предвид дека $F_2(1)=2$ наоѓаме

$$F_2(n)=F_2(1)+[n+(n-1)+\ldots+3+2]=1+[n+(n-1)+(n-2)+\ldots+2+1]=1+\tfrac{n(n+1)}{2}\,.$$

в) Една рамнина го дели просторот на два дела.

Нека претпоставиме, дека е познат бројот $F_3(n)$ на деловите, на кои n рамнини во општа положба го делат просторот и нека се дадени $n+1$ рамнини во општа положба. Првите n рамнини го делат просторот на $F_3(n)$ делови, а според

условот $(n+1)-$та рамнина π ги сече останатите n рамнини во n различни прави, кои се наоѓаат во општа положба (зошто?). Според задачата под б) овие n прави ја делат рамнината π на

$$F_2(n)=1+\frac{n(n+1)}{2}=\frac{n^2+n+2}{2}$$

делови. Според тоа, рамнината π сече $F_2(n)=\frac{n^2+n+2}{2}$ од веќе добиените делови на кои првите n рамнини го делат просторот и истите ги удвојува, што значи дека таа на веќе добиените $F_3(n)$ додава нови $F_2(n)=\frac{n^2+n+2}{2}$ делови. Значи, за бројот на деловите на кој $n+1$ рамнина во општа положба го делат просторот важи

$$F_3(n+1)=F_3(n)+F_2(n)=F_3(n)+\frac{n^2+n+2}{2}. \qquad (5)$$

Ако во равенството (5), наместо n последователно ставиме

$$n-1, n-2, n-3, ..., 2, 1$$

добиваме

$$F_3(n)=F_3(n-1)+\frac{(n-1)^2+(n-1)+2}{2},$$

$$F_3(n-1)=F_3(n-2)+\frac{(n-2)^2+(n-2)+2}{2},$$

.....

$$F_3(3)=F_3(2)+\frac{2^2+2+2}{2}$$

$$F_3(2)=F_3(1)+\frac{1^2+1+2}{2}.$$

Ако ги собереме последните равенства и земеме предвид дека $F_3(1)=2$ наоѓаме

$$F_3(n)=F_3(1)+\tfrac{1}{2}[(n-1)^2+...+2^2+1^2]+\tfrac{1}{2}[(n-1)+...+2+1]+\tfrac{1}{2}[\underbrace{2+...+2+2}_{(n-1)-\text{на двојка}}]$$

$$=2+\frac{n(n-1)(2n-1)}{12}+\frac{(n-1)n}{4}+(n-1),$$

од каде после средувањето наоѓаме $F_3(n)=\frac{(n+1)(n^2-n+6)}{6}$. ♦

8.20. Пример. Најди го бројот на деловите на кои е поделена рамнината од n кружници кои лежат на неа и такви што секои две од нив се сечат меѓу себе.

Решение. Нека е даден бројот $\Phi_2(n)$ на делови на кои е поделена рамнината со n кружници кои лежат на неа и такви што секои две од нив се сечат меѓу себе. Бидејќи n кружници ја сечат $(n+1)-$та кружница во n парови точки и тие истата ја делат на $\Phi_1(n)=2n$, добиваме дека $(n+1)-$та кружница сече $\Phi_1(n)=2n$ од $\Phi_2(n)$ деловите на кои е поделена рамнината со n кружници кои лежат на неа и такви, што секои две од нив се сечат меѓу себе. Оттука го добиваме равенството

$$\Phi_2(n+1)=\Phi_2(n)+\Phi_1(n)=\Phi_2(n)+2n. \qquad (6)$$

Ако во равенството (6), наместо n последователно ставиме $n-1, n-2$, ..., 2, 1 со аналогна постапка како во пример 8 наоѓаме

$$\Phi_2(n) = n^2 - n + 2\,.\ \blacklozenge$$

8.21. Пример. На колку делови го делат просторот n сфери такви, што секои две се сечат меѓу себе.

Решение. Бидејќи n сфери ја сечат $(n+1)-$та сфера во n кружници и како тие нејзината површина ја делат на

$$\Phi_2(n) = n^2 - n + 2$$

делови добиваме дека ако n сфери од кои секои две се сечат меѓу себе го делат просторот на $\Phi_2(n)$ делови, тогаш $n+1$ сфера просторот го делат на

$$\Phi_3(n+1) = \Phi_3(n) + \Phi_2(n) = \Phi_3(n) + (n^2 - n + 2)$$

делови. Сега постапувајќи аналогно како во решението на пример 8.19 наоѓаме

$$\Phi_3(n+1) = \frac{n(n^2-3n+8)}{3}\,.\ \blacklozenge$$

ЗАДАЧИ

1. Одреди го обемот и содржината на следниве поими:
   а) паралелограм, б) ромбоид,
   в) ромб, г) трапез,
   д) рамнокрак триаголник, ѓ) средна линија на триаголник
   е) инјективно пресликување и ж) прост број.
2. За секој од поимите од претходната задача наведи го неговиот најблизок род. За кои од тие поими можеш да укажеш на “род” што не е “најблизок”? За секој од овие поими наведи и по еден вид (ако има).
3. Определи ги видовите одлики на поимот квадрат, ако тој се смета за:
   а) вид паралелограм; б) вид ромб; в) вид правоаголник.
4. Запиши ја дефиницијата на поимот
   а) симетрала на отсечка; б) тежишна линија.
   Потоа, одреди го дефинирачкиот поим.
5. Усоврши ја следнава дефиниција: “Ромб е паралелограм кај кој сите страни се еднакви.”
6. Дадена е дефиницијата: “Паралелограм е четириаголник кај кој спротивните страни пар по пар се паралелни и еднакви”. Анализирај ја и најди минимална дефиниција.
7. Искажи ја дефинцијата на поимот трапез. Дали според неа, паралелограмите се трапези?
8. Тргнувајќи од дефиницијата на поимот отсечка, наведи ги последователно дефинициите на дефинирачките поими сè додека не дојдеш до некои првични поими.

9. Два прости броја p и q се викаат *близнаци*, ако $|p-q|=2$. Такви се на пример, 11 и 13, 17 и 19 итн. По аналогија дефинираме: "Три прости броја p, q и r ги нарекуваме тризнаци ако $|p-q|=|q-r|=2$". Дали оваа дефиниција е противречна?
10. Определи ги субјектот и предикатот за тврдењата од примерот 3.5.1.
11. Определи ги субјектот и предикатот за тврдењата од примерот 3.5.3.
12. Запиши ги симболички тврдењата од примерите 3.5.1 в), 3.5.3 а) и 3.5.4 в).
13. Наведи по два примера за секој вид тврдења.
14. Дали е теорема следново тврдење:
    а) Во секој правоаголник дијагоналите се заемно нормални.
    б) Во секој паралелограм аглите што лежат на иста страна се суплементни.
15. Определи ги претпоставките и заклучокот на теоремата:
    а) Ако еден број е делив со 2 и со 5, тогаш тој е делив со 10.
    б) Агли со нормални краци се еднакви или суплементни.
16. Определи ги условот и заклучокот на следнава теорема:
    а) Цел број чијашто последна цифра е 0, е делив со 5.
    б) Еднаквите тетиви во една кружница се на исто растојание од центарот на кружницата.
    в) Дијагоналите на квадратот се еднакви меѓу себе.
17. Определи ја формата во која е искажана теоремата, а потоа искажи ја во другата форма.
    а) Ако два агли се напоредни, тогаш тие се суплементни.
    б) Агли со заемно паралелни краци се еднакви или суплементни.
    в) Наизменичните агли на трансферзалата на две паралелни прави се еднакви.
    г) Ако еден број е делив со 6, тогаш тој е делив со 2 и со 3.
    д) Во рамнокрак триаголник, висината и тежишната линија повлечени од врвот се совпаѓаат.
18. Избери една теорема и искажи ја во условна форма, а потоа во категорична форма.
19. Дадени се теоремите:
    а) Во секој правоаголник дијагоналите заемно се преполовуваат.
    б) Во секој паралелограм аглите што лежат на иста страна се суплементни.
    в) Ако еден број е делив со 2 и со 5, тогаш тој е делив со 10.
    г) Агли со нормални краци се еднакви или суплементни.
    Формулирај го обратното тврдење; дали и тоа е теорема?
20. Дадени се теоремите:
    а) Ако два агли се напоредни, тогаш тие се суплементни.
    б) Ако два агли имаат заемно паралелни краци, тогаш тие се еднакви или суплементни.
    в) Ако два агли се наизменични агли на трансверзалата на две паралелни прави, тогаш тие се еднакви.
    Запиши ги во категоричка форма, а потоа искажи ги во терминот доволен услов.
21. Дадени се теоремите:

а) Цел број чијашто последна цифра е 0 е делив со 5.
б) Еднаквите тетиви во една кружница се на исто растојание од центарот на кружницата.
в) Дијагоналите на квадратот се еднакви меѓу себе.
г) Број што е делив со 6 е делив со 2 и со 3.
Запиши ги во условна форма, а потоа искажи ги во терминот потребен услов.

22. а) Дали во теоремите од задачата 20 доволниот услов е и потребен?
б) Дали во теоремите од задачата 21 потребниот услов е и доволен?

23. Утврди кои од следните заклучоци се правилно изведени и врз основа на кое правило.
а) 1) Ако бројот n завршува со нула, тогаш n е делив со 2.
2) Бројот n завршува со нула.
Заклучок. Бројот n е делив со 2.
б) 1) Ако бројот n завршува со нула, тогаш n е делив со 2.
2) Бројот n не е делив со 2.
Заклучок. Бројот n не завршува со нула.
в) 1) Ако бројот n завршува со нула, тогаш n е делив со 2.
2) Бројот n не завршува со нула.
Заклучок. Бројот n не е делив со 2.
г) 1) Ако четириаголникот $ABCD$ е делтоид, тогаш неговите дијагонали се заемно нормални.
2) Четириаголникот $ABCD$ е делтоид.
Заклучок. Дијагоналите на четириаголникот $ABCD$ се заемно нормални.
д) 1) Ако четириаголникот $ABCD$ е ромб, тогаш неговите дијагонали се заемно нормални.
2) Дијагоналите на четириаголникот $ABCD$ се заемно нормални.
Заклучок. Четириаголникот $ABCD$ е ромб.

24. Утврди кои од следните заклучоци се правилно изведени и врз основа на кое правило.
а) Ако четириаголникот $ABCD$ е делтоид, тогаш неговите дијагонали се заемно нормални.
Заклучок. Ако дијагоналите на четириаголникот $ABCD$ не се заемно нормални, тогаш тој не е делтоид.
б) Ако четириаголникот $ABCD$ е ромб, тогаш неговите дијагонали се заемно нормални.
Заклучок. Ако четириаголникот $ABCD$ не е ромб, тогаш неговите дијагонали не се заемно нормални.
в) Ако бројот n завршува со една од цифрите 0, 2, 4, 6 или 8, тогаш n е делив со 2.
Заклучок. Ако бројот n не е делив со 2, тогаш n не завршува на цифрата 0, 2, 4, 6 и 8.

25. Утврди кои од следните заклучоци се правилно изведени и врз основа на кое правило.
а) 1) Ако во четириаголникот $ABCD$ аглите што лежат на иста страна се

суплементни, тогаш тој е паралелограм.
2) Ако четириаголникот $ABCD$ е паралелограм, тогаш негови дијагоналите се преполовуваат.
Заклучок. Ако во четириаголникот $ABCD$ аглите што лежат на иста страна се суплементни, тогаш неговите дијагонали се преполовуваат.

b) 1) Ако дијагоналите на делтоидот $ABCD$ се преполовуваат, тогаш тој е ромб.
2) Ако четираголникот $ABCD$ е ромб, тогаш триаголниците BDA и BDC се рамнокраки.
Заклучок. Ако дијагоналите на делтоидот $ABCD$ се преполовуваат, тогаш триаголниците BDA и BDC се рамнокраки.

в) 1) Ако $a \mid b$ и $a \mid c$, тогаш $a \mid (bx)$ и $a \mid (cy)$ за секои $x, y \in \mathbf{Z}$.
2) Ако $a \mid (bx)$ и $a \mid (cy)$, за секои $x, y \in \mathbf{Z}$, тогаш $a \mid (bx+cy)$ за секои $x, y \in \mathbf{Z}$.
Заклучок. Ако $a \mid b$ и $a \mid c$, тогаш $a \mid (bx+cy)$ за секои $x, y \in \mathbf{Z}$.

26. Користејќи го синтетичкиот метод, докажи ја теоремата:
a) *Ако четириаголникот $ABCD$ е ромб, тогаш неговите дијагонали се заемно нормални.*
b) *Ако производот на два природни броја е непарен природен број, тогаш нивниот збир е парен природен број.*

27. Користејќи го аналитичкот метод, докажи ја теоремата:
а) *Во паралелограм дијагоналите заемно се преполовуваат.*
б) *Ако $a, b \in \mathbf{R}^+$ и $a \neq b$, тогаш $\frac{a+b}{2} > \sqrt{ab}$.*
в) *Ако a и b се реални броеви со ист знак, тогаш $\frac{a}{b} + \frac{b}{a} \geq 2$.*
г) *Ако $a, b \in \mathbf{R}$, тогаш $a^2 + b^2 \geq 2 \mid ab \mid$.*

28. Со индиректен метод, докажи ја теоремата:
a) *Ако четириаголникот $ABCD$ е паралелограм, тогаш симетралите на прилегнатите агли на иста страна од тој четириаголник се сечат под прав агол.*
b) *Производот на два непарни природни броја е непарен природен број.*
c) *Ако квадратот на некој реален број е 2, тогаш тој број не е рационален.*

29. Докажи, дека за секој $n \in \mathbf{N}$ се точни равенствата:
а) $1+3+\ldots+(2n-3)+(2n-1)=n^2$, б) $1^2+2^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$,
в) $1^3+2^3+\ldots+n^3=[\frac{n(n+1)}{2}]^2$, г) $1\cdot 2+2\cdot 3+\ldots+(n-1)n=\frac{n(n^2-1)}{3}$,
д) $\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)\cdot(2n+1)}=\frac{n}{2n+1}$, ѓ) $(1-\frac{1}{4})(1-\frac{1}{9})\cdot\ldots\cdot(1-\frac{1}{(n+1)^2})=\frac{n+2}{2n+2}$.

30. Докажи дека $\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}}_{n \text{ корени}} = 2\cos\frac{\pi}{2^{n+1}}$, за секој $n \in \mathbf{N}$.

31. Докажи дека $\frac{1}{n+1}+\frac{1}{n+2}+...+\frac{1}{3n+1}>1$, за секој $n\in\mathbf{N}$.

32. Докажи дека за секој $n>1$ се исполнети неравенствата:
    а) $\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdot...\cdot\frac{2n-1}{2n}<\frac{1}{\sqrt{3n+1}}$, б) $\frac{n}{2}<1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{2^n-1}<n$.

33. Докажи дека за секој природен број $n>3$ важи $n!>2^n$.

34. Броевите $a_n, n=1,2,3,...$ се зададени со $a_1=1, a_2=1$ и $a_n=a_{n-1}+a_{n-2}$, за $n>2$. Докажи дека $a_n=\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n-(\frac{1-\sqrt{5}}{2})^n]$, за секој $n=1,2,3,....$

35. Докажи дека се точни неравенствата:
    а) $n!<(\frac{n+1}{2})^n$, за $n>1$ б) $(n!)^2<(\frac{(n+1)(2n+1)}{6})^n$, за $n>1$

36. Да се најде збирот на внатрешните агли на $n-$аголник (не задолжително конвексен).

37. На колку триаголници е поделен $n-$аголник (не задолжително конвексен) со неговите дијагонали.

38. Определи го бројот N на дијагоналите кои не се сечат и кои го делат $n-$аголникот на триаголници.

39. На колку начини со своите дијагонали може да се подели конвексен $n-$аголник, ако ниедни три дијагонали не се сечат во една точка.
    Одговор. $F(n)=\frac{(n-1)(n-2)(n^2-3n+12)}{24}$.

40. На колку делови ја делат правата n парови точки, кои лежат на таа права?
    Одговор. $2n$ точки ја делат правата на $2n+1$ делови.

41. Да се најде бројот $\Phi_1(n)$ на деловите, на кои е поделена кружница со n парови точки кои се наоѓаат на таа кружница!
    Одговор. $\Phi_1(n)=2n$.

42. На колку делови ја делат сферата n кружници кои лежат на сферата и такви, што секои две од нив се сечат меѓу себе?
    Одговор. Бараниот број е $\Phi_2(n)=n^2-n+2$.

IV ГЛАВА
МНОЖЕСТВА И ПРЕСЛИКУВАЊА

1. ПОИМ ЗА МНОЖЕСТВО

1.1. Поимот *множество* е основен поим во современата математика и него не го дефинираме, туку сметаме дека интуитивно е јасно што е тоа множество.

Како синоним на зборот множество ќе ги користиме зборовите: *севкупност и класа*. Објектите од кои е составено едно множество ги нарекуваме негови *елементи* или *точки*.

За означување на множествата најчесто ги користиме големите букви од латинската азбука: $A, B, C, D, \ldots$, а за означување на елементите на едно множество ги користиме малите букви од латинската азбука: $a, b, c, d, e, x, y, z, \ldots$.

За едно множество ќе сметаме дека е определено, ако за секој објект можеме да кажеме дали му припаѓа или не му припаѓа на тоа множество. Во врска со припадноста на даден елемент на едно множество ги воведуваме следните ознаки.

Нека A е множество. Ако елементот x му припаѓа на множеството A, тогаш пишуваме $x \in A$, а ако елементот x не му припаѓа на множеството A, тогаш пишуваме $x \notin A$.

1.2. *Задавање на множествата со помош на набројување на неговите елементи*. При овој начин елементите на дадено множество се наведуваат во големи загради и притоа редоследот на елементите во заградите не е битен.

Пример. а) Ако множеството A е составено од арапските цифри, тогаш тоа го запишуваме на следниот начин: $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

б) Записот на множеството B составено од самогласките на македонската азбука е: $B = \{$а, е, и, о, у$\}$. ♦

1.3. *Задавање на множествата со наведување на својството на неговите елементи*. Во секоја математичка задача најчесто ги разгледуваме елементите на точно определено множество A, кое понекогаш го нарекуваме основно множество. Притоа потребно е да ги одделиме елементите кои задоволуваат одредено својство P (пишуваме $P(x)$), или не го задоволуваат својството P. Со помош на својството P одделуваме множество од сите елементи на A, кои го имаат својството P. Ова множество го означуваме со $\{x \in A \mid P(x)\}$ или $\{x \mid P(x)\}$.

Пример. а) Нека M е множеството од сите природни броеви кои при делење со 3, даваат остаток 2. Според тоа, во овој случај својството P е природни броеви кои при делење со 3, даваат остаток 2. Ова множество можеме да го запишеме на следниот начин:

$$M = \{n \in \mathbf{N} \mid n \text{ при делење со } 3 \text{ дава остаток } 2\}$$

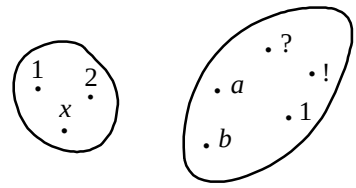
или кратко

$$M = \{n \in \mathbf{N} \mid \ n = 3k + 2, k \in \mathbf{N}\}.$$

б) Множеството X од сите рационални броеви кои се поголеми од $\frac{1}{2}$ и се помали од $\frac{4}{3}$ го запишуваме на следниот начин:

$$X = \{p \in \mathbf{Q} \mid \tfrac{1}{2} < p < \tfrac{4}{3}\}. \ \blacklozenge$$

1.4. *Претставување на множествата со помош на Венови дијаграми.* Заради полесно расудување во геометријата, а исто така и во алгебрата, се користат цртежи, шеми, скици и слично. Слично се постапува и во теоријата на множествата, каде што множествата се претставуваат како дел од рамнината ограничен со затворена линија. Ваквите цртежи ги нарекуваме *Венови дијаграми*.



Пример. За множествата $A = \{1, 2, x\}$ и $B = \{a, b, ?, 1, !\}$ Веновите дијаграми се дадени на цртежот десно. ♦

1.5. Дали постојат природни броеви кои се поголеми од 1 и се помали од 2? Јасно, не постои ниту еден таков природен број. Слично, не постојат квадрати кои не се паралелограми, а исто така не постојат луѓе кои се повисоки од 6 *m* итн.

Претходните разгледувања природно иницираат да воведеме множество без елементи, кое го нарекуваме *празно множество*. Притоа сметаме дека постои само едно празно множество, кое го означуваме со симболот $\varnothing$.

Да ги разгледаме множествата

$$A = \{a, b, c\}, \ B = \{1, 2, 3, a, b, c\} \ \text{и} \ C = \{b, c, a\}.$$

Забележуваме дека секој елемент на множеството A е елемент и на множеството B, а множествата A и C се составени од исти елементи. Во математиката, а и во природата воопшто, имаме низа вакви ситуации, па затоа природна е следнава дефиниција.

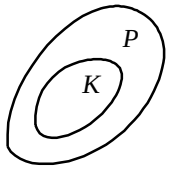
1.6. Дефиниција. За множеството A ќе велиме дека е *подмножество* од множеството B ако од $x \in A$ следува $x \in B$. Притоа означуваме $A \subseteq B$ или $B \supseteq A$.

За множествата A и B ќе велиме дека се *еднакви* ако $A \subseteq B$ и $B \subseteq A$. Притоа пишуваме $A = B$.

Ако $A \subseteq B$ и B содржи елемент кој не му припаѓа на A, тогаш ќе велиме дека A е *вистинско подмножество* од B и пишуваме $A \subset B$ или $B \supset A$.

1.7. Забелешка. За празното множество сметаме дека е подмножество од секое множество A. Од претходната дефиниција непосредно следува дека $A \subseteq A$, но A не е вистинско подмножество на самото себе.

1.8. Пример. а) Со K да го означиме множеството од сите квадрати, а со P множеството од сите правоаголници. Бидејќи секој квадрат е правоаголник, но не секој правоаголник е квадрат, добиваме дека $K \subset P$. Со помош на Венов дијаграм, последново е прикажано на цртежот десно.



б) Множествата $A = \{1\}$ и $B = \{1, 1\}$ се еднакви, бидејќи елементот 1 е единствен елемент како на множеството A, така и на множеството B. Слично, $\{1, 2, 2, 3, 3, 3, 4\} = \{1, 2, 3, 4\}$.

Последното е во согласност со претходно кажаното дека *множеството е целина на различни елементи*, односно дека *секој елемент во множеството се смета само по еднаш*. ♦

1.9. Теорема. За секои множества A, B и C точни се следниве тврдења.

i) $A = A$,

ii) Ако $A = B$, тогаш $B = A$.

iii) Ако $A \subseteq B$ и $B \subseteq C$, тогаш $A \subseteq C$.

iv) Ако $A = B$ и $B = C$, тогаш $A = C$.

Доказ. Ќе го докажеме тврдењето *iii*).

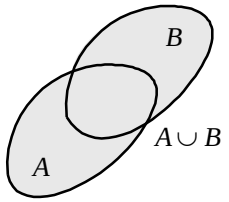
Да претпоставиме дека $A \subseteq B$ и $B \subseteq C$. Ако $x \in A$, тогаш според дефиниција 1.6 од $A \subseteq B$ следува дека $x \in B$. Понатаму, бидејќи $B \subseteq C$, повторно од дефиниција 1.6 добиваме дека $x \in C$. Според тоа, од $x \in A$ следува дека $x \in C$, а тоа значи дека $A \subseteq C$.

Слично се докажуваат и останатите три тврдења. Деталите ги оставаме на читателот за вежба. ♦

2. ОПЕРАЦИИ СО МНОЖЕСТВА

2.1. Во досегашните разгледувања се осврнавме на поимите множество, подмножество и еднакви множества. Во практиката најчесто се среќаваме со проблеми во кои треба истовремено да ги разгледуваме елементите кои им припаѓаат на две или повеќе множества, потоа заедничките елементи на две или повеќе множества, па елементите кои му припаѓаат на едно, а не му припаѓаат на друго множество и слично. Претходно кажаното природно ги наметнува операциите со множествата на кои подетално ќе се осврнеме.

2.2. Дефиниција. *Унија* на множествата A и B го нарекуваме множеството C, кое се состои од сите елементи кои припаѓаат барем на едно од множествата A и B. Притоа означуваме $C = A \cup B$.



Според тоа,

$$A \cup B = \{x \mid x \in A \text{ или } x \in B\}.$$

Претставувањето на унијата на множествата A и B со Венов дијаграм е дадено на горниот цртеж. Јасно, $x \notin A \cup B$ ако и само ако $x \notin A$ и $x \notin B$.

2.3. Пример. Најди ја унијата на множествата

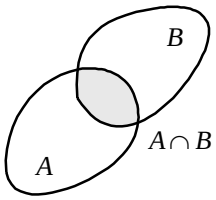
$$A = \{n \mid n \in \mathbf{N} \text{ и } n < 9\} \text{ и } B = \{n \mid n \in \mathbf{N} \text{ и } n \geq 5\}.$$

Решение. За дадените множества имаме

$$A = \{1, 2, 3, 4, 5, 6, 7, 8\} \text{ и } B = \{5, 6, 7, 8, ..., k, ...\},$$

па затоа $A \cup B = \mathbf{N}$. ♦

2.4. Дефиниција. *Пресек* на множествата A и B го нарекуваме множеството C, кое се состои од сите елементи кои припаѓаат на секое од множествата A и B. Притоа означуваме $C = A \cap B$.



Според тоа,

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}.$$

Претставувањето на пресекот на множествата A и B со Венов дијаграм е дадено на цртежот десно. Јасно, $x \notin A \cap B$ ако и само ако $x \notin A$ или $x \notin B$.

2.5. Пример. Најди го пресекот на множествата

$$A = \{n \mid n \in \mathbf{N} \text{ и } n < 9\} \text{ и } B = \{n \mid n \in \mathbf{N} \text{ и } n \geq 5\}.$$

Решение. За дадените множества имаме

$$A = \{1, 2, 3, 4, 5, 6, 7, 8\} \text{ и } B = \{5, 6, 7, 8, ..., k, ...\},$$

па затоа $A \cap B = \{5, 6, 7, 8\}$. ♦

2.6. Дефиниција. За множествата A и B ќе велиме дека се *дисјунктни* ако $A \cap B = \varnothing$.

2.7. Пример. а) Множествата $A = \{1, 2, 3, 4\}$ и $B = \{n \mid n \geq 5, n \in \mathbf{N}\}$ се дисјунктни.

б) Множествата A и B од примерот 2.5 не се дисјунктни. На пример $5 \in A \cap B$. ♦

2.8. Теорема. За секои множества A, B и C точни се следниве тврдења.

i) $A \cup \varnothing = A$; $A \cap \varnothing = \varnothing$,

ii) $A \cap B \subseteq A$; $A \cap B \subseteq B$; $A \subseteq A \cup B$; $B \subseteq A \cup B$,

iii) $A \cap A = A$; $A \cup A = A$, (закони за идемпотентност),

iv) $A \cap B = B \cap A$; $A \cup B = B \cup A$, (комутативни закони),

v) $A \cap (B \cap C) = (A \cap B) \cap C$;
$A \cup (B \cup C) = (A \cup B) \cup C$, (асоцијативни закони),

vi) $A\cap(A\cup B)=A$; $A\cup(A\cap B)=A$, (закони за апсорпција).

Доказ. Ќе го докажеме првото равенство во *v)*. Имаме

$$x\in A\cap(B\cap C)\Rightarrow(x\in A \text{ и } x\in B\cap C)\Rightarrow(x\in A \text{ и } (x\in B \text{ и } x\in C))$$
$$\Rightarrow((x\in A \text{ и } x\in B) \text{ и } x\in C)\Rightarrow(x\in A\cap B \text{ и } x\in C)\Rightarrow x\in(A\cap B)\cap C$$

што значи $A\cap(B\cap C)\subseteq(A\cap B)\cap C$.

Од друга страна имаме

$$x\in(A\cap B)\cap C\Rightarrow(x\in A\cap B \text{ и } x\in C)\Rightarrow((x\in A \text{ и } x\in B) \text{ и } x\in C)$$
$$\Rightarrow(x\in A \text{ и } (x\in B \text{ и } x\in C))\Rightarrow(x\in A \text{ и } x\in B\cap C)\Rightarrow x\in A\cap(B\cap C)$$

што значи $(A\cap B)\cap C\subseteq A\cap(B\cap C)$.

Конечно, од $(A\cap B)\cap C\subseteq A\cap(B\cap C)$ и $A\cap(B\cap C)\subseteq(A\cap B)\cap C$ следува

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

Слично се докажуваат останатите тврдења. Деталите ги оставаме на читателот за вежба. ♦

2.9. Теорема (дистрибутивни закони). За секои множества A,B и C точни се следниве тврдења:

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

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

Доказ. *i*) Нека $x\in(A\cup B)\cap C$. Според тоа, $x\in A\cup B$ и $x\in C$, т.е. $x\in A$ или $x\in B$, и $x\in C$. Затоа, $x\in A$ и $x\in C$ или $x\in B$ и $x\in C$. Но, тоа значи дека $x\in A\cap C$ или $x\in B\cap C$, т.е. $x\in(A\cap C)\cup(B\cap C)$. Конечно,

$$(A\cup B)\cap C\subseteq(A\cap C)\cup(B\cap C).$$

Ако $x\in(A\cap C)\cup(B\cap C)$, тогаш $x\in A\cap C$ или $x\in B\cap C$. Затоа, $x\in A$ и $x\in C$ или $x\in B$ и $x\in C$, што значи дека $x\in A$ или $x\in B$ и $x\in C$, односно $x\in A\cup B$ и $x\in C$. Но, тоа значи дека $x\in(A\cup B)\cap C$. Конечно,

$$(A\cap C)\cup(B\cap C)\subseteq(A\cup B)\cap C.$$

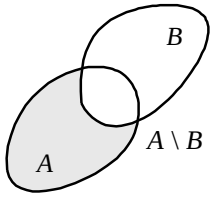
Бидејќи

$$(A\cup B)\cap C\subseteq(A\cap C)\cup(B\cap C) \text{ и } (A\cap C)\cup(B\cap C)\subseteq(A\cup B)\cap C,$$

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

Равенството под *ii*) се докажува аналогно. ♦

2.10. Дефиниција. *Разлика* на множествата A и B го нарекуваме множеството C, кое се состои од сите елементи на множеството A кои не му припаѓаат на множеството B. Означуваме $C=A\setminus B$.



Според тоа,

$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}.$$

Претставувањето на разликата на множествата A и B со Венов дијаграм е дадено на претходниот цртеж.

2.11. Пример. Најди ја разликата на множествата

$$A = \{n \mid n > 4, n \in \mathbf{N}\} \text{ и } B = \{n \mid n < 14, n \in \mathbf{N}\}.$$

Решение. Имаме

$$A = \{5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, ...\} \text{ и}$$
$$B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\},$$

па затоа $A \setminus B = \{14, 15, 16, 17, ...\} = \{n \mid n \geq 14, n \in \mathbf{N}\}$. ♦

2.12. Тврдењата искажани во следнава теорема непосредно следуваат од дефиницијата на разликата на множествата. Обиди се самостојно да ги докажеш.

Теорема. За секои множества A и B важи:

i) $A \setminus \varnothing = A, \quad A \setminus A = \varnothing, \quad \varnothing \setminus A = \varnothing$.

ii) $x \notin A \setminus B$ ако и само ако $x \notin A$ или $x \in B$.

iii) Ако $A \subseteq B$, тогаш $A = B \setminus (B \setminus A)$.

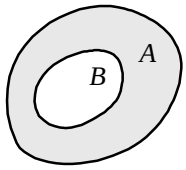
iv) $A \setminus B = \varnothing$ ако и само ако $A \subseteq B$.

v) $A \setminus B = A$ ако и само ако $A \cap B = \varnothing$. ♦

2.13. Дефиниција. Нека е дадено множеството A и $B \subseteq A$. *Комплемент* на B во однос на A го нарекуваме множеството ${}^{c}B = A \setminus B$.

Според тоа,

$${}^{c}B = \{x \mid x \in A \text{ и } x \notin B\}.$$



Претставувањето на комплементот на множеството B во однос на множеството A со Венов дијаграм е дадено на цртежот десно. Јасно, $x \notin {}^{c}B$ ако и само ако $x \in B$.

2.14. Пример. а) Најди го комплементот на множеството $A = \{3, 4, 5\}$ во однос на множеството $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

б) Најди го комплементот на множеството $A = \{n \mid n = 2k, k \in \mathbf{N}\}$ во однос на множеството $\mathbf{N}$.

Решение. а) Од дефиницијата 2.13 имаме ${}^{c}A = U \setminus A = \{1, 2, 6, 7, 8\}$.

б) Имаме

$${}^{c}A = \mathbf{N} \setminus A = \mathbf{N} \setminus \{n \mid n = 2k, k \in \mathbf{N}\} = \{n \mid n \neq 2k, k \in \mathbf{N}\} = \{n \mid n = 2k - 1, k \in \mathbf{N}\}.$$ ♦

2.15. Во врска со поимот комплемент на множество ќе ја докажеме следнава теорема. Тврдењата искажани под *iii*) и *iv*) во оваа теорема се познати како *Де Морганови закони*.

Теорема. Нека $A, B \subseteq X$. Тогаш, точни се равенствата:

i) $^c(^cA) = A$,

ii) $A \subseteq B$ ако и само ако $^cB \subseteq {}^cA$,

iii) $^c(A \cup B) = {}^cA \cap {}^cB$,

iv) $^c(A \cap B) = {}^cA \cup {}^cB$,

v) $A \setminus B = A \cap {}^cB$.

Доказ. Ќе го докажеме првото и третото тврдење.

i) Равенството $^c(^cA) = A$ следува од $x \in {}^c(^cA) \Leftrightarrow x \notin {}^cA \Leftrightarrow x \in A$.

iii) Имаме

$$x \in {}^c(A \cup B) \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \text{ и } x \notin B \Leftrightarrow x \in {}^cA \text{ и } x \in {}^c B \Leftrightarrow x \in {}^cA \cap {}^cB \text{ . } \blacklozenge$$

2.16. Дефиниција. *Декартов производ* на множествата A и B го нарекуваме множеството C, во ознака $C = A \times B$, кое се состои од сите подредени парови (x, y), каде што $x \in A,\ y \in B$. Притоа, $(x_1, y_1) = (x_2, y_2)$ ако и само ако $x_1 = x_2,\ y_1 = y_2$.

Според тоа, $C = \{(x, y) |\ x \in A, y \in B\}$.

Декартовиот производ на непразното множество A со самото себе го нарекуваме *Декартов квадрат* на множеството A и го означуваме A^2.

Аналогно дефинираме Декартов производ на множествата A_i, $i = 1, 2, ..., n$. Имено,

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) |\ a_i \in A_i,\ i = 1, 2, ..., n\}.$$

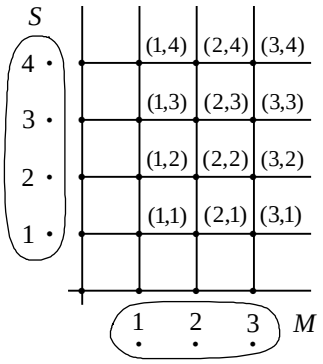
2.17. Пример. а) За множествата

$$M = \{1, 2, 3\} \text{ и } S = \{1, 2, 3, 4\}$$

Декартовиот производ е

$$M \times S = \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,1), (3,2), (3,3), (3,4)\}.$$

На цртежот десно е даден графички приказ на Декартовиот производ на множествата M и S.



б) За множеството $A = \{x, y, z\}$ Декартовиот квадрат е

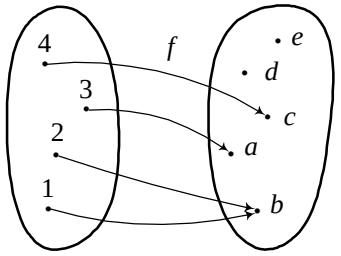
$$A^2 = \{(x,x), (x,y), (x,z), (y,x), (y,y), (y,z), (z,x), (z,y), (z,z)\} \text{ . } \blacklozenge$$

3. ПРЕСЛИКУВАЊА (ФУНКЦИИ)

3.1. Дефиниција. Нека A и B се две непразни множества. Ако на секој елемент $x \in A$ му е придружен, по некое правило f, еднозначно определен елемент $y \in B$, тогаш велиме дека f е *пресликување* (*функција*) од A во B и пишуваме $f : A \to B$.

За елементот $y \in B$ велиме дека е *слика на елементот* $x \in A$ и пишуваме $y = f(x)$. Множеството A го нарекуваме *домен*, а множеството B - *кодомен* на пресликувањето f.

Според тоа, едно пресликување е зададено ако се зададени неговиот домен, кодомен и правилото со кое на секој елемент од доменот му се придружува единствен елемент од кодоменот. Да разгледаме неколку примери.



3.2. Пример. а) Ако

$$A = \{1, 2, 3, 4\},\ B = \{a, b, c, d, e\},$$

тогаш со

$$f(1) = b,\ f(2) = b,\ f(3) = a,\ f(4) = c \qquad (1)$$

е зададено пресликување $f : A \to B$.

Во многу случаи пожелно е пресликувањата графички да се претставуваат. Така, даденото пресликување графички можеме да го претставиме како на цртежот лево.

Исто така, наместо правилото на пресликувањето да го запишуваме во обликот (1), тоа можеме да го направиме со помош на записот

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ b & b & a & c \end{pmatrix}, \qquad (2)$$

што значи дека во првиот ред ги запишуваме елементите на доменот A, а во вториот ред нивните слики кои му припаѓаат на кодоменот B.

Според тоа, ако $f : A \to B$ и $y_1 = f(x_1), y_2 = f(x_2), y_3 = f(x_3), \ldots$, тогаш за правилото f можеме да го користиме и записот

$$f = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots \\ y_1 & y_2 & y_3 & \cdots \end{pmatrix}.$$

б) Нека A е произволно непразно множество. Тогаш, со $I_A(x) = x$, за секој $x \in A$ е определено пресликување $I_A : A \to A$ кое го нарекуваме *идентично* пресликување.

в) Нека се дадени множествата $\mathbf{N}$ и $M = \{2n \mid n \in \mathbf{N}\}$. Јасно, со правилото $f(k) = 2k$, е зададено пресликување $f : \mathbf{N} \to M$. ♦

3.3. Дефиниција. За две пресликувања $f : A \to B$ и $g : C \to D$ ќе велиме дека *се еднакви* ако $A = C,\ B = D$ и $f(x) = g(x)$ за секој $x \in A$.

3.4. Пример. а) Да ги разгледаме пресликувањата

$f : A \to B$, каде што $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3, 4\}$, $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 1 & 3 \end{smallmatrix}\right)$

и

$g : C \to D$, кадешто $C = \{1, 2, 3, 4, 5\}$, $D = \{1, 2, 3\}$, $g = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 1 & 3 \end{smallmatrix}\right)$

Како што забележуваме, $A = C$ и $f(x) = g(x)$ за секој $x \in A$, но бидејќи $B \neq D$ според дефиниција 3.3 имаме дека овие пресликувања не се еднакви.

б) За пресликувањата

$f : A \to B$, каде што $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 3\}$, $f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 1 & 3 \end{smallmatrix}\right)$

и

$g : C \to D$, каде што $C = \{1, 2, 3, 4, 5\}$, $D = \{1, 2, 3\}$, $g = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 2 & 1 & 3 \end{smallmatrix}\right)$

имаме $A = C$, $B = D$, но $f(2) = 1 \neq 2 = g(2)$, па затоа тие не се еднакви. ♦

3.5. Дефиниција. Нека $f : A \to B$. *График* на пресликувањето (функцијата) f го нарекуваме множеството

$$G(f) = \{(x, y) \mid (x, y) \in A \times B,\ y = f(x)\}.$$

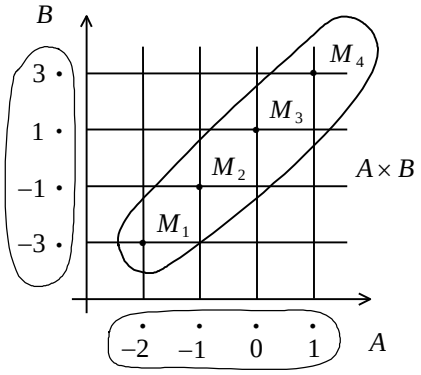
Јасно, $G(f) \subseteq A \times B$.

3.6. Пример. а) Графикот на пресликувањето f од пример 3.4 а) е множеството

$$G(f) = \{(1,1), (2,1), (3,2), (4,1), (5,3)\}.$$

б) Графикот на пресликувањето f од пример 3.2 в) е множеството

$$G(f) = \{(k, 2k) \mid k \in \mathbf{N}\}.$$



в) Нека

$$A = \{-2, -1, 0, 1\},\ B = \{-3, -1, 1, 3\}$$

и нека правилото f е дадено со формулата $f(x) = 2x + 1$, $x \in A$. Имаме

$$f(-2) = -3,\ f(-1) = -1,\ f(0) = 1 \text{ и } f(1) = 3,$$

па затоа

$$G(f) = \{(-2, -3), (-1, -1), (0, 1), (1, 3)\}.$$

На претходниот цртеж е даден шематски приказ на графикот на ова пресликување. ♦

3.7. Дефиниција. Нека $f : A \to B$ и $g : B \to C$ се две пресликувања. За секој $x \in A$ ставаме $h(x) = g(f(x))$ и добиваме пресликување $h : A \to C$ кое го нарекуваме *композиција на пресликувањата* f и g и го означуваме со $h = g \circ f$.

3.8. Пример. Нека $A=B=C=\mathbf{R}$ и пресликувањата $f:A\to B$ и $g:B\to C$ нека се дадени со $f(x)=2x+5$ и $g(x)=5x+3$. Јасно, композициите $g\circ f$ и $f\circ g$ се дефинирани и притоа имаме

$$(g\circ f)(x)=g(f(x))=g(2x+5)=5(2x+5)+3=10x+28$$

и

$$(f\circ g)(x)=f(g(x))=f(5x+3)=2(5x+3)+5=10x+11.$$

Последното покажува дека дури и во случај кога и двете композиции на пресликувања $g\circ f$ и $f\circ g$ се дефинирани, не важи $f\circ g=g\circ f$. ♦

3.9. Теорема. а) Ако $f:A\to B$, тогаш $f\circ I_A=f$ и $I_B\circ f=f$.

б) Ако $f:A\to B$, $g:B\to C$ и $h:C\to D$, тогаш

$$h\circ(g\circ f)=(h\circ g)\circ f.$$

Доказ. а) Пресликувањата $f\circ I_A$ и f имаат исти домени и кодомени и притоа за секој $x\in A$ важи $(f\circ I_A)(x)=f(I_A(x))=f(x)$, па затоа $f\circ I_A=f$.

Аналогно се докажува дека $I_B\circ f=f$.

б) Пресликувањата $h\circ(g\circ f)$ и $(h\circ g)\circ f$ имаат ист домен A и кодомен D и притоа за секој $x\in A$ важи

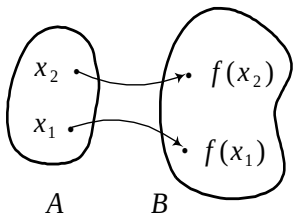
$$(h\circ(g\circ f))(x)=h((g\circ f)(x))=h(g(f(x)))=(h\circ g)(f(x))=((h\circ g)\circ f)(x)$$

од што следува $h\circ(g\circ f)=(h\circ g)\circ f$. ♦

3.10. Дефиниција. Нека $f:A\to B$ и $A_1\subset A$. Пресликувањето $h:A_1\to B$ определено со $h(x)=f(x)$ за секој $h\in A_1$ го нарекуваме *рестрикција на пресликувањето* f на множеството A_1 и го означуваме со $h=f_{|A_1}$.

4. ИНЈЕКЦИЈА, СУРЈЕКЦИЈА И БИЕКЦИЈА. ИНВЕРЗНО ПРЕСЛИКУВАЊЕ

4.1. Дефиниција. За пресликувањето $f:A\to B$ ќе велиме дека е *инјекција* ако од $x_1\neq x_2$ следува $f(x_1)\neq f(x_2)$, т.е. различни елементи имаат различни слики (цртеж десно).



4.2. Пример. а) Нека $A=\{a,b,c,d\}$ и пресликувањата $f:A\to A$ и $g:A\to A$ се определени со $f=\begin{pmatrix}a&b&c&d\\b&a&d&c\end{pmatrix}$ и $g=\begin{pmatrix}a&b&c&d\\c&a&a&d\end{pmatrix}$. Јасно, пресликувањето f е инјекција, но пресликувањето g не е инјекција бидејќи $b\neq c$, но $g(b)=a=g(c)$.

б) Нека се дадени множествата $\mathbf{N}$ и $M=\{2n \mid n\in\mathbf{N}\}$ и нека пресликувањето $f:\mathbf{N}\to M$ е определено со $f(k)=2k$, за секој $k\in\mathbf{N}$. Ќе докажеме дека ова пресликување е инјекција.

Навистина, за секои $k,n\in\mathbf{N}$ такви што $k\neq n$ важи $2k\neq 2n$ што значи $f(k)\neq f(n)$, т.е. f е инјекција. ♦

4.3. Теорема. Ако $f:A\to B$ и $g:B\to C$ се инјекции, тогаш и $g\circ f$ е инјекција.

Доказ. Нека f и g се инјекции. Ако $x_1,x_2\in A$ се такви што $x_1\neq x_2$, тогаш бидејќи f е инјекција, добиваме $f(x_1)\neq f(x_2)$. Понатаму, од $f(x_1)\neq f(x_2)$ и фактот дека g е инјекција имаме

$$g(f(x_1))\neq g(f(x_2)),$$

односно

$$(g\circ f)(x_1)\neq (g\circ f)(x_2),$$

што значи дека $g\circ f$ е инјекција. ♦

4.4. Дефиниција. За пресликувањето $f:A\to B$ ќе велиме дека е *сурјекција* ако за секој $y\in B$ постои $x\in A$ таков што $y=f(x)$, т.е. секој елемент на B е слика на барем еден елемент на A.

4.5. Пример. а) Нека $A=\{a,b,c,d\}$ и $B=\{1,2,3\}$ и пресликувањата $f:A\to B$ и $g:B\to A$ се определени со $f=\left(\begin{smallmatrix}a & b & c & d\\ 1 & 3 & 3 & 2\end{smallmatrix}\right)$ и $g=\left(\begin{smallmatrix}1 & 2 & 3\\ c & a & b\end{smallmatrix}\right)$. Јасно, пресликувањето f е сурјекција, но пресликувањето g не е сурјекција бидејќи d не е слика на ниту еден елемент од множеството B.

б) Нека се дадени множествата $\mathbf{N}$ и $M=\{2n-1 \mid n\in\mathbf{N}\}$ и нека пресликувањето $f:\mathbf{N}\to M$ е определено со $f(k)=2k-1$, за секој $k\in\mathbf{N}$. Ќе докажеме дека ова пресликување е сурјекција.

Нека $2k-1\in M$. Тогаш $k\in\mathbf{N}$ и притоа важи $f(k)=2k-1$. Според тоа, за произволен елемент во M најдовме k од $\mathbf{N}$ чија слика е елементот од M, што значи дека f е сурјекција. ♦

4.6. Теорема. Ако $f:A\to B$ и $g:B\to C$ се сурјекции, тогаш и $g\circ f$ е сурјекција.

Доказ. Нека f и g се сурјекции и нека $z\in C$ е произволен. Бидејќи g е сурјекција, добиваме дека за секој $z\in C$ постои барем еден $y\in B$ таков што $z=g(y)$. Може да постојат и повеќе елементи во B со ова својство. Избираме еден од овие елементи y и бидејќи f е сурјекција, следува дека постои елемент $x\in A$ таков што $y=f(x)$. Според тоа, за секој $z\in C$ постои $x\in A$ таков што $g(f(x))=g(y)=z$, што значи дека $g\circ f$ е сурјекција. ♦

4.7. Дефиниција. За пресликувањето $f: A \to B$ ќе велиме дека е *биекција* ако тоа е и инјекција и сурјекција.

Според тоа, f е биекција ако секој елемент $y \in B$ е слика на барем еден елемент $x \in A$ и различни елементи од A со f се пресликуваат во различни елементи од B.

4.8. Пример. Нека $a, b \in \mathbf{R}$ и $a \neq 0$. Да го разгледаме пресликувањето $f: \mathbf{R} \to \mathbf{R}$ определено со $f(x) = ax + b$.

Ако $x_1 \neq x_2$, тогаш од $a \neq 0$ следува $ax_1 \neq ax_2$, па затоа

$$f(x_1) = ax_1 + b \neq ax_2 + b = f(x_2),$$

што значи дека f е инјекција. Понатаму, за секој $y \in \mathbf{R}$ важи $x = \frac{y-b}{a} \in \mathbf{R}$ и притоа

$$f(x) = f(\tfrac{y-b}{a}) = a \cdot \tfrac{y-b}{a} + b = y - b + b = y,$$

т.е. f е сурјекција.

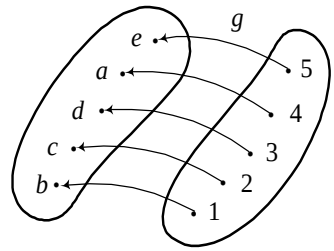
Конечно, f е сурјекција и инјекција, па значи е биекција. ♦

4.9. Теорема. Ако пресликувањата $f: A \to B$ и $g: B \to C$ се биекции, тогаш и нивната композиција $g \circ f$ е биекција.

Доказ. Нека f и g се биекции. Тоа значи дека f и g се инјекции, па од теорема 4.3 следува дека $g \circ f$ е инјекција. Понатаму, f и g се сурјекции, па од теорема 4.6 следува дека $g \circ f$ е сурјекција.

Конечно, $g \circ f$ е инјекција и сурјекција, па значи тоа е биекција. ♦

4.10. Пример. Нека $A = \{a, b, c, d, e\}$, $B = \{1, 2, 3, 4, 5\}$ и $f: A \to B$ е дадено со $f = \left(\begin{smallmatrix} a & b & c & d & e \\ 4 & 1 & 2 & 3 & 5 \end{smallmatrix}\right)$. Ова пресликување е биекција. Во врска со пресликувањето f да го разгледаме пресликувањето $g: B \to A$ зададено со $g = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ b & c & d & a & e \end{smallmatrix}\right)$. Како што можеме да забележиме, "старите" слики сега се оригинали, а "старите" оригинали сега се "нови" слики (цртеж десно). Во овој случај велиме дека пресликувањето g е инверзно пресликување за пресликувањето f. ♦



4.11. Претходно разгледаниот пример непосредно ја иницира следнава дефиниција за инверзно пресликување.

Дефиниција. Ако $f: A \to B$ е биекција, тогаш со $g(y) = x$, за секој $y \in B$ ако и само ако $y = f(x)$ е определено пресликување $g: B \to A$ кое го наре-

куваме *инверзно* на пресликувањето f. За инверзното пресликување ја прифаќаме ознаката $g = f^{-1}$.

4.12. Пример. Нека $a,b \in \mathbf{R}$ и $a \neq 0$. Во пример 4.8 докажавме дека пресликувањето $f : \mathbf{R} \to \mathbf{R}$ определено со $f(x) = ax + b$ е биекција. Според тоа, постои инверзното пресликување f^{-1}.

За да го најдеме f^{-1}, ставаме $y = ax + b$ и добиваме $x = \frac{y-b}{a}$. Сега, од равенството $f^{-1}(y) = x$ добиваме

$$f^{-1}(y) = \tfrac{1}{a}(y-b) = \tfrac{1}{a}y - \tfrac{b}{a}.$$

Конкретно, за пресликувањето $f(x) = 2x - 1$ имаме $a = 2$ и $b = -1$, па со замена добиваме дека неговото инверзно пресликување е

$$f^{-1}(y) = \tfrac{1}{2}y + \tfrac{1}{2}. \blacklozenge$$

4.13. Теорема. Ако $f : A \to B$ е биекција, тогаш инверзното пресликување $f^{-1} : B \to A$ е биекција.

Доказ. Од дефиниција 4.11 следува дека f^{-1} е пресликување од B во A.

Ако $y_1 \neq y_2$, тогаш $f^{-1}(y_1) \neq f^{-1}(y_2)$ бидејќи во спротивно еден ист елемент од A со f ќе се преслика во два различни елементи од B, што не е можно бидејќи f е пресликување. Значи f^{-1} е инјекција.

Ако $x \in A$, тогаш $x = f^{-1}(y)$ каде што $y = f(x)$, што значи дека f^{-1} е сурјекција.

Конечно, f^{-1} е инјекција и сурјекција, па значи е биекција. $\blacklozenge$

5. БУЛОВА АЛГЕБРА

5.1. Ако ги споредиме основните својства на множествата и исказната логика, забележуваме дека многу од нив се слични. Последното е непосредна причина за воведување поопшта теорија, која во математиката е позната како Булова алгебра. Меѓутоа, пред да преминеме на разгледување на основните својства на Буловите алгебри ќе ги воведеме поимите за унарна и бинарна операција.

5.2. Дефиниција. Ако G е множество, тогаш секое пресликување $f : G \times G \to G$ го нарекуваме *внатрешна бинарна операција* на G.

Според тоа со секоја бинарна операција на G на секој подреден пар $(x, y) \in G \times G$ еднозначно му се придружува елемент $z \in G$. Притоа пишуваме $z = xfy$ или $f : (x, y) \to z$. Вообичаено операцијата f ќе ја означуваме со еден од

следниве симболи: $*, \circ, \otimes, \oplus, \Delta, +, -, \cdot, :, \cap, \cup, \setminus, \ldots$. Во оваа смисла ќе пишуваме $x*y, x+y, x-y, x\cdot y, \ldots$.

Заради пократко искажување, наместо терминот внатрешна бинарна операција овде ќе го користиме терминот *операција*.

5.3. Пример. а) Нека G е множеството природни броеви $\mathbf{N}$. Собирањето и множењето на природни броеви се примери на операции во ова множество. Од друга страна одземањето и делењето не се операции во множеството природни броеви бидејќи, на пример, не постои природен број z таков што $z = 2-3$ и не постои природен број t таков што $t = 2:3$.

Меѓутоа, во множеството $\mathbf{N}$ одземањето и делењето се изводливи за некои парови природни броеви. Во ваков случај велиме дека станува збор за *делумна операција*.

б) Нека G е множеството природни броеви $\mathbf{N}$. Бидејќи за секои $x, y \in \mathbf{N}$ важи $\mathrm{NZD}(x,y) \in \mathbf{N}$, $\mathrm{NZS}(x,y) \in \mathbf{N}$, $\min\{x,y\} \in \mathbf{N}$, $x+y+xy \in \mathbf{N}$ заклучуваме дека со

$$x*y = \mathrm{NZD}(x,y),\ x\circ y = \mathrm{NZS}(x,y),\ x\Delta y = \min\{x,y\} \text{ и } x\bullet y = x+y+xy$$

се дефинирани операции на $\mathbf{N}$. На пример,

$$6*15 = 3,\ 6\circ 15 = 30,\ 6\Delta 15 = 6,\ 6\bullet 15 = 111.$$

Пресметај: $12*14,\ 12\circ 14,\ 12\Delta 14,\ 12\bullet 14$. ♦

5.4. Пример. Да се потсетиме, ако $M_4 = \{0,1,2,3\}$ е множеството на остатоци при делење на природните броеви со 4, тогаш збирот и производот по модул 4 на кои било елементи од ова множество повторно е елемент од истото множеството, што значи дека собирањето и множењето по модул 4 се операции на M_4. Ако со $\oplus$ го означиме собирањето по модул 4, а со $\otimes$ множењето по модул 4, тогаш овие операции можеме да ги претставиме со помош на следните таблици.

$\oplus$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Честопати операциите над множествата можеме да ги дефинираме со таблици, како што тоа го направивме во случајот со собирањето и множењето по модул 4. Таблиците од овој вид ги нарекуваме *Келиеви шеми* и тие најчесто се користат кога множеството над кое ја дефинираме операцијата е конечно. ♦

5.5. Дефиниција. Ако G е множество, тогаш секое пресликување $f : G \to G$ го нарекуваме *унарна операција* на G.

5.6. Дефиниција. Нека B е множество такво што $1, 0 \in B$ и на B се дефинирани бинарни операции + и $\cdot$ и унарна операција $'$. Ако за секои $x, y, z \in B$ се исполнети својствата

а) Комутативни закони

$$x \cdot y = y \cdot x$$
$$x + y = y + x$$

б) Асоцијативни закони

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
$$x + (y + z) = (x + y) + z$$

в) Дистрибутивни закони

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$x + (y \cdot z) = (x + y) \cdot (x + z)$$

г) Својства на идентитети

$$x + 0 = x$$
$$x \cdot 1 = x$$

д) Закони за комплемент

$$x + x' = 1$$
$$x \cdot x' = 0,$$

Тогаш подредената четворка $(B, +, \cdot, ')$ ја нарекуваме *Булова алгебра*. Елементот 1 го нарекуваме *единица*, елементот 0 го нарекуваме *нула*, а елементот x' го нарекуваме *комплемент* на елементот x.

5.7. Забелешка. Заради поедноставно запишување често пати наместо $x \cdot y$ ќе ја користиме ознаката xy.

5.8. Теорема. Нека $(B, +, \cdot, ')$ е Булова алгебра. Тогаш, за секои $x, y \in B$ важи:

а) Закони за идемпотетност

$$x + x = x$$
$$x \cdot x = x$$

б) Закони за единицата и нулата

$$x + 1 = 1$$
$$x \cdot 0 = 0$$

в) Закони за апсорпција

$$x + (x \cdot y) = x$$
$$x \cdot (x + y) = x.$$

Доказ. а) За секој $x \in B$ имаме

$$x + x = (x + x) \cdot 1 = (x + x) \cdot (x + x') = x + (x \cdot x') = x + 0 = x.$$

Второто равенство се докажува аналогно.

б) За секој $x \in B$ имаме

$$x + 1 = (x + 1) \cdot 1 = (x + 1) \cdot (x + x') = x + (1 \cdot x') = x + (x' \cdot 1) = x + x' = 1.$$

Второто равенство се докажува аналогно.

в) За секои $x, y \in B$ имаме

$$x+(x\cdot y)=(x\cdot 1)+(x\cdot y)=x\cdot(1+y)=x\cdot(y+1)=x\cdot 1=x\,.$$

Второто равенство се докажува аналогно. ♦

5.9. Теорема (единственост на комплементот). Нека $(B,+,\cdot,')$ е Булова алгебра. Ако $x\cdot x'=0,\ x+x'=1,\ x\cdot x^*=0,\ x+x^*=1,$ тогаш $x'=x^*.$

Доказ. Ако $x+x'=1$ и $x+x^*=1$, тогаш

$$x'=x'\cdot 1=x'\cdot(x+x^*)=x'\cdot x+x'\cdot x^*=x\cdot x'+x'\cdot x^*=0+x'\cdot x^*=x'\cdot x^*+0=x'\cdot x^*$$

па затоа

$$x^*=x^*\cdot 1=x^*\cdot(x+x')=x^*\cdot x+x^*\cdot x'=x\cdot x^*+x'\cdot x^*=0+x'\cdot x^*$$
$$=x'\cdot x^*+0=x'\cdot x^*=x'\,.\ \blacklozenge$$

5.10. Теорема. Нека $(B,+,\cdot,')$ е Булова алгебра. Тогаш за секои $x, y \in B$ важи:

а) Закон за инволуторност: $(x')'=x$,

б) Закони за комплемент на неутралните елементи: $1'=0$ и $0'=1$

в) Де Морганови закони: $(x+y)'=x'\cdot y'$ и $(x\cdot y)'=x'+y'.$

Доказ. а) Имаме: $x'+x=x+x'=1$ и $x'\cdot x=x\cdot x'=0$, што значи дека x е комплемент на x', т.е. $(x')'=x$, (теорема 5.9).

б) Непосредно следува од тврдењето под а). Деталите ги оставаме на читателот за вежба.

в) За секои $x, y \in B$ важи

$$(x+y)+x'\cdot y'=((x+y)+x')\cdot((x+y)+y')=((y+x)+x')\cdot((x+y)+y')$$
$$=(y+(x+x'))\cdot(x+(y+y'))=(y+1)\cdot(x+1)=1\cdot 1=1$$

и

$$(x+y)\cdot(x'\cdot y')=(x'\cdot y')\cdot(x+y)=((x'\cdot y')\cdot x)+((x'\cdot y')\cdot y)$$
$$=(x\cdot(x'\cdot y'))+(x'\cdot(y'\cdot y))=((x\cdot x')\cdot y')+(x'\cdot(y\cdot y'))$$
$$=(0\cdot y')+(x'\cdot 0)=(y'\cdot 0)+(x'\cdot 0)=0+0=0.$$

Сега од теорема 5.9 следува дека $(x+y)'=x'\cdot y'$.

Понатаму $(x'+y')'=(x')'\cdot(y')'=x\cdot y$, па затоа

$$(x\cdot y)'=((x'+y')')'=x'+y'.\ \blacklozenge$$

5.11. Теорема. Нека $(B,+,\cdot,')$ е Булова алгебра. Тогаш $x+y=y$ ако и само ако $xy=x$.

Доказ. Нека претпоставиме дека $x+y=y$. Од законот за апсорпција имаме $x=(x+y)x$, па затоа $xy=x(x+y)=(x+y)x=x.$

Обратната импликација се докажува аналогно. Деталите ги оставаме на читателот за вежба. ♦

5.12. Коментар. Секоја од аксиомите за Булова алгебра се состои од пар равенства кои се заемно дуални во следнава смисла: ако во едното од равенствата симболот + го замениме со симболот ·, · со +, 1 со 0 и 0 со 1, го добиваме другото равенство. Непосредна последица од ова својство е дека ако во која било теорема симболот + го замениме со симболот ·, · со +, 1 со 0 и 0 со 1, тогаш се добива нова теорема.

5.13. Пример. Нека A е произволно множество и B е партитивното множество на A. Лесно се докажува дека $(B,\cup,\cap,')$, каде $X' = A \setminus X$ за секој $X \in B$ е Булова алгебра во која $\cup$ соодветствува на +, а $\cap$ соодветствува на ·. ♦

6. ЕКВИВАЛЕНТНИ МНОЖЕСТВА

6.1. Дефиниција. За множествата A и B велиме дека се *еквивалентни*, со ознака $A \sim B$, ако постои биекција f од A во B.

6.2. Пример. Ќе докажеме дека $[0,1] \sim [a,b]$, за секои $a,b \in \mathbf{R}$, $b > a$. За таа цел да го разгледаме пресликувањето $f(x) = b + (b-a)(x-1)$.

Ако $x_1 \neq x_2$, тогаш последователно добиваме

$$x_1 - 1 \neq x_2 - 1,$$
$$(b-a)(x_1-1) \neq (b-a)(x_2-1),$$
$$b + (b-a)(x_1-1) \neq b + (b-a)(x_2-1),$$

што значи $f(x_1) \neq f(x_2)$, т.е. f е инјекција. Од друга страна, за секој $y \in [a,b]$ имаме $0 \leq y-a \leq b-a$ и ако поделиме со $b-a > 0$ добиваме $0 \leq \frac{y-a}{b-a} \leq 1$, па затоа

$$f\left(\frac{y-a}{b-a}\right) = b + (b-a)\left(\frac{y-a}{b-a} - 1\right) = b + (b-a)\frac{y-b}{b-a} = b + (y-b) = y,$$

што значи дека f е и сурјекција.

Според тоа, f е инјекција и сурјекција, па е биекција, што според дефиниција 6.1 значи $[0,1] \sim [a,b]$. ♦

6.3. Теорема. За секои множества A, B и C важи:
i) $A \sim A$,
ii) Ако $A \sim B$, тогаш $B \sim A$, и
iii) Ако $A \sim B$ и $B \sim C$, тогаш $A \sim C$.

Доказ. *i)* Јасно, идентичното пресликување $I_A : A \to A$ е биекција, па затоа $A \sim A$.

ii) Нека $A \sim B$. Тоа значи дека постои биекција $f : A \to B$. Сега, од теорема 4.13 следува дека инверзното пресликување $f^{-1} : B \to A$ е биекција, па затоа $B \sim A$.

iii) Нека $A \sim B$ и $B \sim C$. Тоа значи дека постојат биекции $f : A \to B$ и $g : B \to C$. Сега, од теорема 4.9 следува дека композицијата $g \circ f : A \to C$ е биекција, па затоа $A \sim C$. ♦

6.4. Пример. Нека $a, b, c, d \in \mathbf{R}$ се такви што $a < b$ и $c < d$. Според пример 6.2 имаме $[0,1] \sim [a,b]$ и $[0,1] \sim [c,d]$. Сега од теоремата 6.3 *iii*) следува дека $[a,b] \sim [c,d]$. ♦

6.5. Во следнава дефиниција ќе го воведеме поимот за конечно множество и во натамошните разгледувања под поимот множество ќе ги подразбираме конечните множества. За таа цел, за секој природен број k нека $\mathbf{N}_k = \{1, 2, 3, ..., k\}$.

Дефиниција. Нека $k \in \mathbf{N}$. За множеството M ќе велиме дека се состои од k елементи ако $M \sim \mathbf{N}_k$. Притоа ќе пишуваме $|M| = k$. По дефиниција земаме дека $|\varnothing| = 0$.

За множеството M ќе велиме дека е *конечно* ако постои $k \in \mathbf{N}$ таков што $|M| = k$. Во спротивно ќе велиме дека множеството M е *бесконечно*.

6.6. Забелешка. Според теорема 6.3 *i*) имаме $\mathbf{N}_k \sim \mathbf{N}_k$, за секој $k \in \mathbf{N}$, па затоа од дефиниција 6.5 следува $|\mathbf{N}_k| = k$.

6.7. Теорема. Нека $k \neq 0$. Тогаш, $|M| = k$ ако и само ако M може да се запише во видот $M = \{a_1, a_2, ..., a_k\}$.

Доказ. Нека $|M| = k$. Тоа значи дека $M \sim \mathbf{N}_k$, т.е. постои биекција $f : \mathbf{N}_k \to M$. Да означиме

$$f(1) = a_1,\ f(2) = a_2, ...,\ f(k) = a_k .$$

Тогаш,

$$M = \{f(1),\ f(2), ...,\ f(k)\} = \{a_1, a_2, ..., a_k\} .$$

Обратно, нека $M = \{a_1, a_2, ..., a_k\}$. Тогаш пресликувањето $f : \mathbf{N}_k \to M$ определено со $f(i) = a_i$, $i = 1, 2, ..., k$ е биекција. Навистина, за секој $a_i \in M$ постои $i \in \mathbf{N}_k$ таков што $f(i) = a_i$, што значи дека f е сурјекција. Понатаму, од $i \neq j$ следува $a_i \neq a_j$, па затоа $f(i) \neq f(j)$, т.е. f е и инјекција. Според тоа, $|M| = k$. ♦

7. ПРИНЦИП НА ЕДНАКВОСТ, ЗБИР, ПРОИЗВОД, ВКЛУЧУВАЊЕ И ИСКЛУЧУВАЊЕ

7.1. Теорема (принцип на еднаквост). а) Ако $|M|=k$ и $M \sim L$, тогаш $|L|=k$.

б) Ако $|M|=|L|=k$, тогаш $M \sim L$.

Доказ. а) Од $|M|=k$ имаме $\mathbf{N}_k \sim M$. Понатаму, бидејќи $\mathbf{N}_k \sim M$ и $M \sim L$, од теорема 6.3 *iii*) следува дека $\mathbf{N}_k \sim L$, што значи дека $|L|=k$.

б) Нека $|M|=|L|=k$. Тогаш $\mathbf{N}_k \sim M$ и $\mathbf{N}_k \sim L$, па од теорема 6.3 *iii*) следува дека $M \sim L$. ♦

Од теорема 6.7 непосредно следува дека конечните множества M и L се еквивалентни ако и само ако имаат ист број на елементи.

7.2. Пример. На колку начини на тројца студенти може да им се поделат 8 исти моливи, така што секој од нив да добие барем еден молив?

Решение. Осумте моливи ќе ги наредиме во низа и на празните места меѓу нив, кои ги има 7, ќе поставуваме две "прегради" како на следниов цртеж.

$$\bullet^{1} \quad \bullet^{2}| \quad \bullet^{3} \quad \bullet^{4} \quad \bullet^{5} \quad \bullet^{6}| \quad \bullet^{7} \quad \bullet$$

Празните места да ги означиме со броевите 1, 2, 3, 4, 5, 6, 7. Поделбата на цртежот е определена со броевите 2 и 6, т.е. со бројот 26. Сите поделби се определени со следниве броеви:

12 13 14 15 16 17
23 24 25 26 27
34 35 36 37
45 46 47
56 57
67

Вакви двоцифрени броеви има 21, па од принципот на еднаквост следува дека бројот на поделбите на 8 исти моливи на тројца студенти така што секој од нив да добие барем по еден молив е 21. ♦

7.3. Теорема (принцип на збир). Ако A и B се конечни множества такви што $A \cap B = \varnothing$, тогаш $|A \cup B| = |A| + |B|$.

Доказ. Нека $A \cap B = \varnothing$ и $f : A \to \mathbf{N}_n$, $g : B \to \mathbf{N}_m$ се биекции. Ќе докажеме дека пресликувањето $h : A \cup B \to \mathbf{N}_{n+m}$ определено со $h(a) = f(a)$, $a \in A$ и $h(b) = g(b) + n$, $b \in B$ е биекција. Нека $x, y \in A \cup B$ и $x \neq y$. Можни се два случаи и тоа:

а) x и y му припаѓаат на едно од множествата A и B, да кажеме A. Тогаш, од дефиницијата на пресликувањето h следува дека $h(x) = f(x)$ и $h(y) = f(y)$ и бидејќи f е биекција, имаме $f(x) \neq f(y)$, што значи $h(x) \neq h(y)$.

б) x и y му припаѓаат на различни множества, да кажеме $x \in A$ и $y \in B$. Тогаш $h(x) = f(x) \le n < n+1 \le g(y)+n = h(y)$, т.е. $h(x) \ne h(y)$.

Според тоа, во секој случај од $x \ne y$ следува $h(x) \ne h(y)$, т.е. h е инјекција.

Нека $p \in \mathbf{N}_{n+m}$. Можни се два случаја и тоа:

а) $p \le n$ и во тој случај бидејќи f е биекција, постои $z \in A$ таков што $f(z) = p$. Но тоа, значи дека постои $z \in A \cup B$ таков што $h(z) = f(z) = p$.

б) $p > n$ и во овој случај $1 \le p-n \le m$. Но g е биекција, па затоа постои $z \in B$ таков што $g(z) = p-n$. Значи постои $z \in A \cup B$ таков што

$$p = (p-n)+n = g(z)+n = h(z).$$

Според тоа, во секој случај постои $z \in A \cup B$ таков што $h(z) = p$, т.е. h е сурјекција.

Конечно, h е инјекција и сурјекција, па значи е биекција. Значи, $A \cup B \sim \mathbf{N}_{n+m}$ од што следува $|A \cup B| = n+m = |A|+|B|$. ♦

7.4. Да забележиме дека принципот на збир важи и во случај кога имаме k, $k \ge 2$ по парови дисјунктни множества. Имено, точна е следново тврдење.

Последица. Ако $A_1, A_2, ..., A_k$ е фамилија од k, $k \ge 2$ по парови дисјунктни конечни множества, т.е. множества за кои важи $A_i \cap A_j = \varnothing$, за $i \ne j$, тогаш

$$|A_1 \cup A_2 \cup ... \cup A_k| = |A_1|+|A_2|+...+|A_k|. \blacklozenge$$

7.5. Пример. Во пример 7.2 дадовме решение на проблемот на поделба на 8 еднакви моливи на тројца студенти, при што секој студент добива барем по еден молив. Истата задача ќе ја решиме користејќи го принципот на збир.

Нека сите поделби на моливите на тројца студенти го формираат множеството A. Ова множество ќе го разбиеме на подмножества $A_1, A_2, A_3, A_4, A_5, A_6$, при што подмножеството A_1 ги содржи поделбите при кои првиот студент добива еден молив, A_2 поделбите при кои првиот студент добива два молива итн. Така, за множествата $A_1, A_2, A_3, A_4, A_5, A_6$ ја имаме следнава табела

i	A_i	$\lvert A_i \rvert$
1	(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)	6
2	(1,5), (2,4), (3,3), (4,2), (5,1)	5
3	(1,4), (2,3), (3,2), (4,1)	4
4	(1,3), (2,2), (3,1)	3
5	(1,2), (2,1)	2
6	(1,1)	1
Вкупно		21

Сега од принципот на збир имаме

$$|A| = |A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6| = |A_1| + |A_2| + |A_3| + |A_4| + |A_5| + |A_6| = 21 . \blacklozenge$$

7.6. Теорема (принцип на производ). За секои конечни множества A и B важи $|A \times B| = |A| \cdot |B|$.

Доказ. Нека A и B се конечни множества такви што $|A| = m$ и $|B| = n$. Тогаш, од теорема 6.7 имаме $A = \{a_1, ..., a_m\}$ и $B = \{b_1, ..., b_n\}$.

За множеството $A \times B$ имаме

$$\begin{aligned} A \times B &= \{(a_1, b_1), ..., (a_m, b_1), (a_1, b_2), ..., (a_m, b_2), ..., (a_1, b_n), ..., (a_m, b_n)\} \\ &= \{(a_1, b_1), ..., (a_m, b_1)\} \cup \{(a_1, b_2), ..., (a_m, b_2)\} \cup ... \cup \{(a_1, b_n), ..., (a_m, b_n)\} \quad (1) \\ &= (A \times \{b_1\}) \cup (A \times \{b_2\}) \cup ... \cup (A \times \{b_n\}). \end{aligned}$$

Понатаму, $A \times \{b_i\} \cap A \times \{b_j\} = \emptyset$, за $i \neq j$ и бидејќи $|A \times \{b_i\}| = m$ за секој $i = 1, 2, ..., n$ од (1) и од принципот на збир добиваме

$$|A \times B| = |A \times \{b_1\}| + |A \times \{b_2\}| + ... + |A \times \{b_n\}| = \underbrace{m + m + ... + m}_{n \text{ пати}} = mn = |A| \cdot |B| . \blacklozenge$$

7.7. Принципот на производ го има следново обопштување.

Последица. Нека $k \geq 2$. Тогаш

$$|A_1 \times A_2 \times ... \times A_k| = |A_1| \cdot |A_2| \cdot ... \cdot |A_k|$$

за секои конечни множества A_i, $i = 1, 2, ..., k$. $\blacklozenge$

7.8. Пример. Меѓу градовите *A* и *B* има три директни патишта, меѓу градовите *B* и *C* има два директни пата, а меѓу градовите *C* и *D* има пет директни патишта. На колку различни начини може да се стигне од градот *A* во градот *D*, ако треба само по еднаш да се влезе во секој од градовите *B* и *C*?

Решение. Со X, Y, Z да ги означиме множествата патишта меѓу градовите *A* и *B*, *B* и *C*, *C* и *D* соодветно. Тогаш, секоја можност за патување од *A* до *D* при наведените услови е елемент на множеството $X \times Y \times Z$ и елементите на ова множество ги даваат сите можности за патување. Од принципот на производ (последица 7.7) следува дека бараниот број е

$$|X \times Y \times Z| = |X| \cdot |Y| \cdot |Z| = 3 \cdot 2 \cdot 5 = 30 . \blacklozenge$$

7.9. Теорема. а) (принцип на исклучување). Ако M е конечно множество и $A \subseteq M$, тогаш $|M \setminus A| = |M| - |A|$.

б) (принцип на вклучување). За произволни конечни множества A и B важи $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказ. а) Од $M = A \cup (M \setminus A)$ и $A \cap (M \setminus A) = \emptyset$, според принципот на збир следува $|M| = |A| + |M \setminus A|$, односно $|M \setminus A| = |M| - |A|$.

б) Нека $M = A \cup B$. Тогаш од принципот на исклучување следува дека $|M| = |A| + |M \setminus A|$. Но, бидејќи $M \setminus A = B \setminus (A \cap B)$, т.е.

$$B = (M \setminus A) \cup (B \cap A) \text{ и } (M \setminus A) \cap (A \cap B) = \varnothing$$

од принципот на збир следува дека $|B| = |M \setminus A| + |A \cap B|$. Според тоа,

$$|A \cup B| = |A| + |M \setminus A| = |A| + |B| - |A \cap B|. \blacklozenge$$

7.10. Забелешка. Во случај на три и четири множества, принципот на вклучување го има следниов облик:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

и

$$\begin{aligned} |A \cup B \cup C \cup D| = {} & |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| \\ & - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| \\ & + |B \cap C \cap D| - |A \cap B \cap C \cap D|. \end{aligned}$$

7.11. Пример. Во една студиска група има 35 студенти. Од нив, десет студенти имаат оценка осум по алгебарски структури, 20 студенти имаат оценка осум по калкулус, додека 27 студенти имаат барем една оценка осум по предметите алгебарски структури и калкулус. Колку студенти имаат оценка осум по двата предмети?

Решение. Нека A е множеството студенти кои што имаат оценка осум по алгебарски структури и B е множеството студенти кои што имаат оценка осум по калкулус. Од условите на задачата имаме $|A| = 10, |B| = 20$ и $|A \cup B| = 27$, а се бара $|A \cap B|$. Од принципот на вклучување имаме

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

односно $27 = 10 + 20 - |A \cap B|$, па затоа $|A \cap B| = 3$. $\blacklozenge$

7.12. Пример. Најди го бројот на природните броеви помали од 100 кои не се деливи ниту со 2, ниту со 3, ниту со 7.

Решение. Нека $M = \{n \mid 1 \le n < 100, n \in \mathbf{N}\}$ и со A, B и C да ги означиме множествата од природните броеви помали од 100 кои се деливи со 2, 3 и 7 соодветно. Тогаш,

$$\begin{aligned} & |A| = 49, |B| = 33, |C| = 14, |A \cap B| = 16, \\ & |A \cap C| = 7, |B \cap C| = 4 \text{ и} |A \cap B \cap C| = 2. \end{aligned}$$

Прво од принципот на исклучување, а потоа од принципот на вклучување имаме

$$\begin{aligned} |M \setminus (A \cup B \cup C)| &= |M| - |A \cup B \cup C| = \\ &= |M| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C| \\ &= 99 - 49 - 33 - 14 + 16 + 7 + 4 - 2 = 28. \end{aligned}$$

Според тоа, природни броеви кои се помали од 100 и не се деливи ниту со 2, ниту со 3, ниту со 7 има вкупно 28. $\blacklozenge$

8. ПРИНЦИП НА ДИРИХЛЕ

8.1. Принципот на Дирихле е еден од наједноставните комбинаторни принципи, но тој често се користи во решавањето на разни комбинаторни задачи, па затоа истиот посебно ќе го разгледаме. Наједноставно кажано, овој принцип тврди дека ако, на пример, четири зајаци се сместени во три кафези, тогаш барем во еден кафез ќе има два зајаци.

Во следната теорема ќе дадеме прецизна формулација на принципот на Дирихле.

8.2. Теорема (принцип на Дирихле - елементарен случај). Нека n е природен број. Ако $n+1$ предмети се распоредени на произволен начин во n кутии, тогаш барем во една кутија има два предмета.

Доказ. Да претпоставиме дека во секоја кутија има најмногу по еден предмет. Бидејќи има само n кутии, добиваме дека во нив се распоредени најмногу $n \cdot 1 = n$ предмети, што и противречи на претпоставката дека се распоредени $n+1$ предмети. ♦

8.3. Забелешка. Принципот на Дирихле кажува дека постои кутија во која има барем два предмети, но не дава начин, односно алгоритам како таа кутија да се најде. Ќе разгледаме неколку примери.

8.4. Пример. Докажи дека во група од 367 луѓе секогаш има барем двајца што имаат роденден во ист ден.

Решение. Годината има најмногу 366 денови (предвид ја земаме и преступната година) и роденденот на секој од групата луѓе е во некој од овие денови. Бидејќи $367 = 366 + 1$, од принципот на Дирихле следува дека барем двајца луѓе од групата имаат роденден во ист ден. ♦

8.5. Пример. Дали може броевите $-1, 0, 1$ да се распоредат во квадратна 5×5 таблица така што збирот на броевите во секој ред, секоја колона и секоја дијагонала да биде различен.

Решение. Збирот на пет броеви од множеството $\{-1, 0, 1\}$ може да биде број a таков што $-5 \le a \le 5$, што значи дека збирот може да прими најмногу 11 различни вредности. Но, квадратната 5×5 таблица има вкупно 12 колони, редови и дијагонали, па од принципот на Дирихле (теорема 8.2) следува дека барем два збира на броевите во секој ред, секоја колона и секоја дијагонала мораат да бидат еднакви. ♦

8.6. Пример. Дадени се пет произволни броеви. Докажи дека меѓу нив постојат барем два броја такви што нивната разлика е делива со 4.

Решение. Секој природен број при делење со 4 дава остаток 0, 1, 2 или 3. Значи постојат само четири можности. Според тоа, меѓу пет природни броеви мора да има барем два кои имаат ист остаток при делење со 4. Јасно, разликата на овие два броја е делива со 4. ♦

8.7. Пример. Нека $a_1, a_2, ..., a_n$ се цели броеви. Докажи дека постојат $p, q \in \{0,1,2,...,n\}$, $p < q$ такви што $n \mid (a_{p+1} + a_{p+2} + ... + a_q)$.

Решение. Ги формираме збировите

$$b_1 = a_1$$
$$b_2 = a_1 + a_2$$
$$.....$$
$$b_n = a_1 + a_2 + ... + a_n.$$

Ако еден од овие збирови е делив со n, да кажеме b_k, тогаш земаме $p = 0, q = k$ и задачата е решена. Нека ниеден од овие збирови не е делив со n. Од теоремата за делење со остаток имаме $b_i = ns_i + r_i$, $0 < r_i < n$ за секој $i = 1,2,...,n$. Бидејќи имаме n остатоци $r_1, r_2, ..., r_n$ и тие примаат $n-1$ вредности $1,2,...,n-1$, според принципот на Дирихле заклучуваме дека барем два од овие остатоци се еднакви, т.е. постојат p и q такви што $r_p = r_q$ и тоа е бараното решение, бидејќи

$$a_{p+1} + a_{p+2} + ... + a_q = b_q - b_p = n(s_q - s_p).\blacklozenge$$

8.8. Принципот на Дирихле може да се искаже и во поопшта форма, со чија помош можеме да решаваме посложени комбинаторни проблеми. Тоа ќе го направиме во следната теорема.

Теорема (принцип на Дирихле - општ случај). Нека $kn + r$ предмети $r \geq 1$ се сместени во n кутии. Тогаш, барем во една кутија се сместени најмалку $k+1$ предмети.

Доказ. Да претпоставиме дека во секоја кутија има најмногу по k предмети. Бидејќи има само n кутии добиваме дека во нив се распоредени најмногу nk предмети, што и противречи на претпоставката дека се распоредени $kn + r > nk$ предмети. ♦

8.9. Пример. Во Република Македонија има повеќе од 2150000 жители и на главата на секој од нив има најмногу по 300000 влакна. Докажи дека во Македонија има барем 8 луѓе со ист број влакна на главата.

Решение. Сите жители ќе ги поделиме во групи според бројот на влакната на главата. Вакви групи има 300001, т.е. група со 0 влакна, група со 1 влакно, ..., група со 300000 влакна, а луѓе има најмалку 2150000. Бидејќи

$$2150000 = 7 \cdot 300001 + 49993,$$

од обопштениот принцип на Дирихле следува дека мора да постои група во која има најмалку 8 луѓе со ист број влакна на главата. Доколку тоа не е случај, во секоја група ќе има најмногу по 7 луѓе, па нивниот број ќе биде 2100007, а тоа му противречи на бројот на жителите во Републиката. ♦

8.10. Пример. Во едно одделение 40 ученици правеле три писмени задачи. Никој не добил оценка помала од 3 и секој добил по три различни оценки. Ха-

ралампие забележал дека во одделението има најмалку 7 ученици кои имаат иста оценка на секоја од трите писмени задачи. Дали Хараламие е во право?

Решение. За секој ученик постојат 6 можности, т.е. секој ученик ја добил следната подредена тројка оценки:

(3, 4, 5), (3, 5, 4), (4, 3, 5), (4, 5, 3), (5, 3, 4) и (5, 4, 3).

Затоа, учениците според добиените оценки можеме да ги поделиме на 6 групи. Во одделението има 40 ученици, а според добиените оценки се поделени во 6 групи. Од принципот на Дирихле следува дека постои група во која има најмалку 7 ученици, што значи дека Хараламие е во право. ♦

8.11. Пример. Дадени се 10 различни природни броеви помали од 26. Докажи дека меѓу сите можни разлики на паровите различни броеви од дадените 10 броеви, постојат барем три еднакви разлики.

Решение. Дадените 10 броеви да ги подредиме по големина, т.е. нека

$$1 \le n_1 < n_2 < n_3 < n_4 < n_5 < n_6 < n_7 < n_8 < n_9 < n_{10} < 26.$$

Ќе докажеме дека меѓу следните девет разлики

$$n_2 - n_1, n_3 - n_2, n_4 - n_3, n_5 - n_4, n_6 - n_5, n_7 - n_6, n_8 - n_7, n_9 - n_8, n_{10} - n_9$$

има барем три еднакви броеви, со што задачата ќе биде решена. Ако меѓу овие 9 разлики нема барем три еднакви, тогаш меѓу нив има најмногу 2 единици, 2 двојки, 2 тројки, 2 четворки и 2 петки. Одовде добиваме дека

$$\begin{aligned} n_{10} - n_1 &= (n_{10} - n_9) + (n_9 - n_8) + (n_8 - n_7) + (n_7 - n_6) + (n_6 - n_5) \\ &\quad + (n_5 - n_4) + (n_4 - n_3) + (n_3 - n_2) + (n_2 - n_1) \\ &\ge 1+1+2+2+3+3+4+4+5 = 25, \end{aligned}$$

т.е. дека $n_{10} \ge n_1 + 25 \ge 26$, што му противречи на фактот дека $n_{10} < 26$. Значи, меѓу посочените 9 разлики мора да има барем три еднакви. ♦

8.12. Принципот на Дирихле е познат и во таканаречената *геометриска форма*. Во овој случај нема да дадеме некои посебни теориски објаснувања, туку истиот ќе го објасниме со примери.

8.13. Пример. Во квадрат со страна $1m$ на произволен начин се сместени 51 точка. Докажи дека меѓу овие 51 точка, постојат три точки кои можат да се покријат со круг чиј радиус е $\frac{1}{7}m$.

Решение. Квадратот да го поделиме на 25 еднакви квадрати со страна $0,2m$. Според принципот на Дирихле, постои квадрат со страна $0,2m$ кој содржи барем 3 од дадените 51 точка. Земаме 3 точки кои лежат во еден квадрат со страна $0,2m$. Но, $\frac{2}{7} > 0,2\sqrt{2}$, што значи дека дијагоналата на квадратот е помала од дијаметарот на круг со радиус $\frac{1}{7}m$, па затоа квадратот може да се покрие со круг со радиус $\frac{1}{7}m$, т.е. 3 од дадените 51 точка можат да се покријат со круг со радиус $\frac{1}{7}m$. ♦

8.14. Пример. Во круг со радиус $1m$ на произволен начин се распоредени 51 точка така што кои било 3 од нив не се колинеарни. Докажи дека постојат 3 точки меѓу нив кои формираат триаголник чија плоштина е помала од $12,6dm^2$.

Решение. Кругот го делиме на 25 складни исечоци чиј централен агол е $360^\circ : 25 = 14,4^\circ$. Според принципот на Дирихле, постои исечок во кој се наоѓаат барем три точки. Избираме произволни три од тие точки. Плоштината на триаголникот формиран од овие три точки е помала од плоштината на кружниот исечок. Плоштината на кружниот исечок е $\frac{\pi}{25}m^2 < 0,126m^2 = 12,6dm^2$. ♦

9. ГРУПИРАЊЕ НА ЕЛЕМЕНТИ НА КОНЕЧНО МНОЖЕСТВО

9.1. Дефиниција. Нека е дадено конечното множество од n елементи $A = \{a_1, a_2, ..., a_n\}$ и нека $k \in \{1, 2, ..., n\}$. Секоја подредена $k-$торка од видот

$(a_{i_1}, a_{i_2}, ..., a_{i_k})$, каде што $a_{i_p} \neq a_{i_t}$, за $p \neq t$ и $a_{i_p} \in A$, за $p = 1, 2, ..., k$

ја нарекуваме *варијација без повторување од n елементи од класа k*.

Според тоа, варијација без повторување од n елементи од класа k е подредена $k-$торка составена од елементи од множеството $A = \{a_1, a_2, ..., a_n\}$ во која сите елементи се различни.

9.2. Забелешка. Во практиката, скоро сите проблеми поврзани со варијациите без повторување се сведуваат на определување на нивниот број, па затоа во следната теорема ќе ја докажеме формулата за определување на бројот на варијациите без повторување од n елементи од класа k, кој го означуваме со V_n^k, $n = 1, 2, ...;\ k = 1, 2, ..., n$.

9.3. Теорема. а) Ако $k < n$, тогаш

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

б) Ако $n \in \mathbf{N}$, тогаш

$$V_n^k = n(n-1)...(n-k+1), \text{ за } k = 1, 2, ..., n. \tag{2}$$

Доказ. а) Од секоја варијација без повторување од n елементи од класа k, т.е. од секоја подредена $k-$ка од облик $(a_{i_1}, a_{i_2}, ..., a_{i_k})$, со додавање на уште еден елемент

$$a_{i_{k+1}} \neq a_{i_p}, \text{ за } p \neq k+1,\ p = 1, 2, ..., k,$$

кои вкупно ги има $n-k$, може да се добијат $n-k$ варијации без повторување од n елементи од класа $k+1$ од вид $(a_{i_1}, a_{i_2}, ..., a_{i_k}, a_{i_{k+1}})$. Притоа се добиваат сите варијации од n елементи од класа $k+1$ и секоја од новодобиените варијациии се добива само по еднаш, па затоа од принципот на производ следува формулата (1).

б) Очигледно е дека $V_n^1 = n$. Нека за $k = i < n$ важи формулата (2), т.е.

$$V_n^i = n(n-1)...(n-i+1).$$

Сега, од (1) и од претпоставката добиваме

$$V_n^{i+1} = (n-i)V_n^i = n(n-1)...(n-i+1)(n-i),$$

т.е. формулата важи и за $k = i+1$. Конечно, од принципот на математичка индукција следува дека формулата (2) важи за $k = 1,2,...,n$. ♦

9.4. Пример. Колку трицифрени броеви, кај кои цифрите не се повторуваат, можат да се составаат од цифрите $1,2,3,4,5$ и 7 ?

Решение. Очигледно, бидејќи сите цифри се различни од цифрата 0, за да го определиме бројот на трицифрените броеви, кај кои цифрите не се повторуваат и кои можат да се составаат од цифрите $1,2,3,4,5$ и 7, треба да го најдеме бројот на варијациите без повторување од 6 елементи од класа 3 (зошто?). Ако ја искористиме формулата (2), за бараниот број добиваме

$$V_6^3 = 6 \cdot 5 \cdot 4 = 120. \blacklozenge$$

9.5. Пример. Реши ја равенката

а) $V_n^2 = 380$, б) $V_{2n+4}^3 : V_{n+4}^4 = 2:3$

Решение. а) Од формулата (2) следува дека дадената равенка е еквивалентна на равенката

$$n(n-1) = 380,\ n \in \mathbf{N}.$$

Решенија на квадратната равенка

$$n^2 - n - 380 = 0$$

се $n_1 = 20$ и $n_2 = -19$. Но, $n \in \mathbf{N}$, па затоа решение на дадената равенка е само $n_1 = 20$.

б) Од формулата (2) следува дека дадената равенка е еквивалентна на равенката

$$(2n+4)(2n+3)(2n+2) : (n+4)(n+3)(n+2)(n+1) = 2:3,\ n \in \mathbf{N},$$

т.е. на равенката

$$n^2 - 5n - 6 = 0,\ n \in \mathbf{N}.$$

Решенија на квадратната равенка $n^2 - 5n - 6 = 0$ се $n_1 = 6$ и $n_2 = -1$. Но, $n \in \mathbf{N}$, па затоа решение на дадената равенка е само $n_1 = 6$. ♦

9.6. Дефиниција. Нека е дадено конечното множество од n елементи $A = \{a_1,...,a_n\}$ и нека $k \in \mathbf{N}$. Секоја подредена $k-$торка од облик

$(a_{i_1}, a_{i_2},..., a_{i_k})$, каде што $a_{i_p} \in A$, за $p = 1,2,...,k$

ја нарекуваме *варијација со повторување од n елементи од класа k*.

Според тоа, варијација со повторување од n елементи од класа k е подредена k – ка составена од елементи од множеството $A=\{a_1,...,a_n\}$.

9.7. Забелешка. Во практиката, скоро сите проблеми поврзани со варијациите со повторување се сведуваат на определување на нивниот број, па затоа во следната теорема ќе ја докажеме формулата за определување на бројот на варијациите со повторување од n елементи од класа k, кој го означуваме со $\overline{V}_n^k$, $n,k\in\mathbf{N}$.

9.8. Теорема. Ако $n,k\in\mathbf{N}$, тогаш

$$\overline{V}_n^k=n^k. \tag{3}$$

Доказ. Нека е дадено множеството $A=\{a_1,...,a_n\}$ и нека

$$(a_{i_1},a_{i_2},...,a_{i_k})$$

е произволна варијација со повторување од класа k од неговите елементи. Тогаш, на местото на првата координата може да се запише секој од елементите на множеството A, т.е. имаме n можности. За секоја од овие можности за местото на втората координата имаме n можности, па затоа за првите две координати имаме $n\cdot n=n^2$ можности. Продолжувајќи ја постапката со секоја нова координата бројот на можностите се зголемува n пати и како имаме k координати од принципот на производ следува дека $\overline{V}_n^k=n^k$, т.е. точна е формулата (3). ♦

9.9. Пример. Колку Морзеови знаци може да се формираат од двата елементарни знака – и • ако еден знак се состои од најмногу четири елементарни знаци?

Решение. Имаме множество $A=\{-,\bullet\}$ од два елементи и можеме да формираме Морзеови знаци од $1,2,3$ и 4 елементарни знаци. Според тоа, елементарните знаци ќе бидат варијации со повторување од 2 елемента од класа $1,2,3$ и 4, соодветно. Значи, бројот на Морзеовите знаци кои во случајот можеме да ги формираме е:

$$\overline{V}_2^1+\overline{V}_2^2+\overline{V}_2^3+\overline{V}_2^4=2^1+2^2+2^3+2^4=30\,.\ \blacklozenge$$

9.10. Пример. Реши ја равенката: $9V_n^3=5\overline{V}_n^3$.

Решение. Ако ги искористиме формулите (2) и (3) добиваме дека дадената равенка е еквивалентна на равенката

$$9n(n-1)(n-2)=5n^3,\ n\in\mathbf{N},$$

т.е. на равенката

$$4n^2-27n+18=0,\ n\in\mathbf{N}.$$

Решенијата на равенката $4n^2-27n+18=0$ се $n_1=6$ и $n_2=\frac{3}{4}$ и како n е природен број добиваме дека решение на почетната равенка е $n_1=6$. ♦

9.11. Дефиниција. Нека е дадено конечното множество од n елементи $A=\{a_1,a_2,...,a_n\}$. Секоја варијација без повторување од n елементи од класа n ја нарекуваме *permutacija bez povtorување od n elementi*.

9.12. Според тоа, пермутација без повторување од n елементи на множеството $A=\{a_1,a_2,...,a_n\}$ е подредена $n-$торка во која сите елементи се различни меѓу себе. Понатаму, бројот на пермутациите без повторување од n елементи го означуваме со P_n. Од теорема 9.3 б) добиваме

$$P_n=V_n^n=n(n-1)(n-2)\cdot...\cdot(n-n+1)=n(n-1)(n-2)\cdot...\cdot1=n!,$$

т.е. точна е следнава теорема.

Теорема. Бројот на пермутациите без повторување од n елементи е

$$P_n=n!. \text{ ♦} \tag{4}$$

9.13. Пример. Колку петцифрени броеви можат да се формираат од цифрите $1,3,5,7$ и 9?

Решение. Бидејќи секоја од цифрите $1,3,5,7$ и 9 е различна од 0, бројот на петцифрените броеви е еднаков на бројот на пермутациите од 5 елементи, т.е. тој е еднаков на $5!=5\cdot4\cdot3\cdot2\cdot1=120$. ♦

9.14. Пример. На колку начини можат да се распоредат броевите $1, 2, 3, ..., 2n-1, 2n$, така што секој парен број се наоѓа на непарно место?

Решение. Меѓу дадените броеви има n парни и n непарни броеви. Според тоа, треба да распоредиме n парни броеви на n непарни места, па затоа секое вакво распоредување е пермутација без повторување од n елементи и нивниот број $P_n=n!$. Понатаму, при секое распоредување на парните броеви на непарните места ни останууваат празни парните места, кои ги има n и на нив треба да распоредиме n непарни броеви, па затоа секое вакво распоредување е пермутација без повторување од n елементи и нивниот број $P_n=n!$. Конечно, бидејќи распоредувањето на парните и распоредувањето на непарните броеви не зависи едно од друго добиваме дека вкупниот број на распоредувања на броевите

$$1, 2, 3, ..., 2n-1, 2n$$

така што секој парен број се наоѓа на непарно место е еднаков на

$$P_n\cdot P_n=n!\cdot n!=(n!)^2. \text{ ♦}$$

9.15. Пример. Колку пермутации без повторување од елементите 1,2,3, 4,5,6,7 и 8 почнуваат со:

а) 5, б) 123, в) 8642.

Решение. а) Бидејќи пермутациите треба да почнуваат со цифрата 5, секоја од бараните пермутации може да се добие ако останатите седум цифри произволно се распоредат на останатите седум места. Според тоа, бројот на бараните пермутации е еднаков на бројот на пермутациите од 7 елементи, т.е. тој е еднаков на $P_7 = 7! = 5040$.

На потполно ист начин наоѓаме:

б) $P_5 = 5! = 120$ и в) $P_4 = 4! = 24$. ♦

9.16. Дефиниција. Нека е дадено множеството $A = \{a_1, ..., a_n\}$. Секое подмножество од k елементи, $k \le n$ на множеството A го нарекуваме *комбинација без повторување од n елементи од класа k*.

Бројот на комбинациите без повторување од n елементи од класа k го означуваме со C_n^k, $n = 1, 2, 3, 4, ...,$ $k = 1, 2, ..., n$.

9.17. Теорема. За бројот на комбинациите без повторување од n елементи од класа k точна е формулата

$$C_n^k = \frac{V_n^k}{P_k}, \tag{5}$$

каде што $n = 1, 2, 3, 4, ...,$ $k = 1, 2, ..., n$, т.е. формулата

$$C_n^k = \frac{n(n-1)(n-2)...(n-k+1)}{k!}. \tag{6}$$

Доказ. Нека $\{a_1, a_2, ..., a_k\}$ е една комбинација без повторување од n елементи од класа k. Ако оваа комбинација ја пермутираме, ќе добиеме $P_k = k!$ пермутации, кои воедно се и сите варијации без повторување од n елементи од класа k кои се составени од елементите $a_1, a_2, ..., a_k$. Понатаму, од сите варијации без повторување на n елементи од класа k кои се составени од елементите $a_1, a_2, ..., a_k$ со занемарување на редоследот на елементите се добива единствената комбинација без повторување $\{a_1, a_2, ..., a_k\}$ од n елементи од класа k. Според тоа, бројот на варијациите без повторување V_n^k од n елементи од класа k е $P_k = k!$ пати поголем од бројот C_n^k на комбинациите без повторување на n елементи од класа k, па затоа важи формулата $V_n^k = C_n^k P_k$, која е еквивалентна на формулата (5).

Точноста на формулата (6) непосредно следува од формулите (4) и (5) и фактот дека

$$V_n^k = n(n-1)(n-2)...(n-k+1). \text{ ♦}$$

9.18. Забелешка. Ако броителот и именителот на десната страна во формулата (6) ги помножиме со $(n-k)!$, ја добиваме формулата

$$C_n^k = \frac{n(n-1)(n-2)...(n-k+1)\cdot(n-k)(n-k-1)\cdot...\cdot 2\cdot 1}{k!\cdot(n-k)(n-k-1)\cdot...\cdot 2\cdot 1} = \frac{n!}{k!(n-k)!}. \quad (7)$$

Понатаму, за секој $k = 0,1,2,...,n$ од формулата (7) имаме

$$C_n^{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{(n-k)!k!} = C_n^k, \quad (8)$$

што значи дека за секој $k = 0,1,2,...,n$ бројот на комбинациите без повторување од n елементи од класа k е еднаков на бројот на комбинациите без повторување од n елементи од класа $n-k$.

Нека е дадено множеството $A, |A| = n$ и нека $P(A)$ е партитивното множество на множеството A. Тогаш, од дефиниција 9.16 и од претходно изнесеното, користејќи го принципот на збир со помош на Њутновата биномна формула непосредно наоѓаме дека

$$|P(A)| = C_n^0 + C_n^1 + C_n^2 + ... + C_n^n = 2^n.$$

9.19. Пример. Во една паралелка има 35 ученици. На колку начини може да се избере нејзиното раководство кое брои 3 члена?

Решение. Јасно, секое раководство на паралелката е подмножество од множеството ученици, па затоа вкупниот број на начини на избори на раководството на паралелката е еднаков на бројот на комбинациите без повторување од 35 елементи од класа 3, т.е. тој е еднаков на

$$C_{35}^3 = \frac{35\cdot 34\cdot 33}{3\cdot 2\cdot 1} = 6545. \blacklozenge$$

9.20. Пример. Во еден сад се наоѓаат 7 топчиња означени со броевите од 1 до 7. На колку начини можат да се извлечат 5 топчиња, ако топчињата се влечат одеднаш и без гледање?

Решение. Имаме 7 топчиња и одеднаш без гледање влечеме 5. Очигледно станува збор за комбинации без повторување од 7 елементи од класа 5, па затоа тоа може да се направи на $C_7^5 = \frac{7\cdot 6\cdot 5\cdot 4\cdot 3}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 21$ начини. $\blacklozenge$

9.21. Пример. а) Докажи дека $\frac{(2n)!}{(n!)^2} \in \mathbf{N}$, за секој $n \in \mathbf{N}$.

б) Пресметај ги n и k ако $C_n^k = 4$ и $V_n^k = 24$.

Решение. а) Нека $n \in \mathbf{N}$ и да разгледаме произволно множеството A со $2n$ елементи. Јасно, бројот на сите $n-$елементни подмножества на множеството A е природен број и ако ја искористиме формулата (7) добиваме

$$\frac{(2n)!}{(n!)^2} = \frac{(2n)!}{n!(2n-n)!} = C_{2n}^n \in \mathbf{N}.$$

б) Од формулата (5) наоѓаме $P_k = \frac{V_n^k}{C_n^k} = \frac{24}{4} = 6$, што значи $6 = P_k = k!$ и како $1\cdot 2\cdot 3 = 6$ добиваме дека $k = 3$. Понатаму,

$$24 = V_n^3 = n(n-1)(n-2)$$

и како бројот 24 како производ на три последователни природни броја може да се запише на единствен начин и тоа $24=4\cdot 3\cdot 2$, добиваме дека $n=4$. ♦

9.22. Дефиниција. Нека е дадено множеството $A=\{a_1,...,a_m\}$, $k_i\in\mathbf{N}$, за $i=1,...,m$ и $n=k_1+k_2+...+k_m$. Подредената $n-$торка елементи на множеството A во која за секој $i\in\{1,2,...,m\}$ елементот a_i се јавува точно k_i пати, ја нарекуваме *пермутација од n елементи од тип $(k_1,k_2,...,k_m)$* или *пермутација со повторување*.

За бројот на пермутациите од n елементи од тип $(k_1,k_2,...,k_m)$, кој го означуваме со $P_n^{k_1,k_2,...,k_m}$ точна е следнава теорема.

9.23. Теорема. Ако $k_i\in\mathbf{N}$, за $i=1,2,...,m$ и $n=k_1+k_2+...+k_m$, тогаш

$$P_n^{k_1,k_2,...,k_m}=\frac{n!}{k_1!k_2!...k_m!}. \ \blacklozenge \tag{9}$$

Доказ. Од $n-$те места во подредената $n-$торка избираме k_1 места, што може да се направи на $C_n^{k_1}=\frac{n!}{k_1!(n-k_1)!}$ начини и на нив го ставаме елементот a_1, потоа од преостанатите $n-k_1$ места избираме k_2 места, што може да се направи на $C_{n-k_1}^{k_2}=\frac{(n-k_1)!}{k_2!(n-k_1-k_2)!}$ начини и на нив го ставаме елементот a_2 итн., во $(m-1)-$от чекор од преостанатите $n-k_1-k_2-...-k_{m-2}$ места избираме k_{m-1}, што може да се направи на

$$C_{n-k_1-k_2-...-k_{m-2}}^{k_{m-1}}=\frac{(n-k_1-k_2-...-k_{m-2})!}{k_{m-1}!(n-k_1-k_2-...-k_{m-2}-k_{m-1})!}=\frac{(n-k_1-k_2-...-k_{m-2})!}{k_{m-1}!k_m!}$$

начини и на нив го ставаме елементот a_{m-1}, за да на крајот на преостанатите k_m места го ставиме елементот a_m. Од досега изнесеното следува дека

$$\begin{aligned}P_n^{k_1,k_2,...,k_m}&=C_n^{k_1}C_{n-k_1}^{k_2}C_{n-k_1-k_2}^{k_3}...C_{n-k_1-k_2-...-k_{m-2}}^{k_{m-1}}\\&=\frac{n!}{k_1!(n-k_1)!}\cdot\frac{(n-k_1)!}{k_2!(n-k_1-k_2)!}\cdot\frac{(n-k_1-k_2)!}{k_3!(n-k_1-k_2-k_3)!}\cdot...\cdot\frac{(n-k_1-k_2-...-k_{m-2})!}{k_{m-1}!k_m!}=\frac{n!}{k_1!k_2!...k_m!}. \ \blacklozenge\end{aligned}$$

9.24. Пример. На колку начини може да се разместат 8 гости во три хотелски соби: еднокреветна, трикреветна и четирикреветна.

Решение. Сместувањето во еднокреветната соба да го означиме со a, во трикреветната со b и во четирикреветната со c. Според тоа, секое сместување определува подредена $8-$торка во која a се јавува еднаш, b се јавува трипати и c се јавува четири пати, на пример со (a,b,b,b,c,c,c,c) и обратно. Значи станува збор за пермутации од 8 елементи од тип $(1,3,4)$, па од теорема 9.23 следува дека бројот на сместувањата е еднаков на

$$P_8^{1,3,4}=\frac{8!}{1!3!4!}=280. \ \blacklozenge$$

9.25. Пример. Колку различни низи од букви може да се направат со разместување на буквите на зборот "*математика*"? (Низите не мора да имаат значење.)

Решение. Во зборот математика вкупно има 10 букви, при што буквата *м* се повторува двапати и $k_1 = 2$, буквата *а* се повторува трипати и $k_2 = 3$, буквата *т* се повторува двапати и $k_3 = 2$ пати, буквата *е* се повторува еднаш и $k_4 = 1$, буквата *и* се повторува еднаш и $k_5 = 1$ и буквата *к* се повторува еднаш и $k_6 = 1$. Затоа бројот на низите од букви кои можат да се направат од зборот "*математика*" е еднаков на

$$P_{10}^{3,2,2,1,1,1} = \frac{10!}{3!2!2!1!1!1!} = 151200 . \blacklozenge$$

9.26. Пример. Колку пермутации од елементите

$$1,2,2,2,3,3,3,3,4,4,4$$

почнуваат со:

а) 22, б) 313, в) 1234?

Решение. а) Имаме пермутации од 11 елементи од тип $(1,3,4,3)$ и како елементите 2 и 2 се фиксирани на првите две места, за да го определиме бараниот број на пермутации потребно е да го определиме бројот на пермутациите од 9 елементи од тип $(1,1,4,3)$ и тој е еднаков на

$$P_9^{1,1,4,3} = \frac{9!}{1!1!4!3!} = 2520 .$$

б) $P_8^{3,2,3} = \frac{8!}{3!2!3!} = 560$ и в) $P_7^{2,3,2} = \frac{7!}{2!3!2!} = 210 . \blacklozenge$

9.27. Пример. На колку различни начини, без да се користат загради, може да се запише $a^3b^2c^3$ како производ од 8 множители?

Решение. Очигледно станува збор за пермутации од 8 елементи од тип $(3,2,3)$, па затоа бараниот број на запишувања е $P_8^{3,2,3} = \frac{8!}{3!2!3!} = 560 . \blacklozenge$

Нека е дадено множеството $A = \{a,b,c\}$. Тогаш множеството

$$\{(a,a),(a,b),(a,c),(b,b),(b,c),(c,c)\}$$

го нарекуваме множество комбинации со повторување од 3 елементи од класа 2. Во практиката често пати записот на комбинациите со повторување може да се сретне во скратен облик, при што комбинациите со повторување во примерот се запишуваат во облик *aa, ab, ac, bb, bc, cc* . Да забележиме дека во дадениот случај за елементите на множеството A треба да знаеме кој е прв, кој е втор итн. и тоа го означуваме со $a < b < c$. Во општ случај ја имаме следнава дефиниција.

9.28. Дефиниција. Нека е дадено множеството $A = \{a_1, a_2, ..., a_n\}$ и нека за неговите елементи знаеме кој е прв, кој е втор итн., т.е. нека $a_1 < a_2 < ... < a_n$. За

подредената $k-$торка $(b_1,b_2,...,b_k)$, $b_i \in A$ ќе велиме дека е *комбинација со повторување од* n *елементи од класа* k ако $b_i \le b_j$, за $i<j$. Бројот на комбинациите со повторување од n елементи од класа k ќе го означуваме со $\overline{C}_n^k$.

9.29. Теорема. Бројот на комбинациите со повторување од n елементи од класа k е

$$\overline{C}_n^k = C_{n+k-1}^k. \tag{10}$$

Доказ. Да земеме една комбинација со повторување од n елементи од класа k и на истата да и ја придружиме низата од нули и единици формирана со следнава постапка: запишуваме онолку единици колку што во комбинацијата се јавува елементот a_1, потоа запишуваме една 0, па запишуваме онолку единици колку што во комбинацијата се јавува елементот a_2, па запишуваме една 0 итн., за на крајот да запишеме онолку единици колку што во комбинацијата се јавува елементот a_n, а во случај кога во комбинацијата не се јавува некој елемент a_i наместо единици запишуваме една нула. На овој начин на секоја комбинација ќе и соодветствува единствена низа составена од k единици и $n-1$ нула и обратно, на секоја ваква низа ќе и соодветствува единствена комбинација со повторување од n елементи од класа k.

Секоја од конструираните низи е со должина $n+k-1$ и истата е определена со распоредот на $n-1$ нула на $n+k-1$ место, односно со распоредот на k единици на $n+k-1$ место. Според тоа, бројот на сите низи од разгледуваниот вид е еднаков на $C_{n+k-1}^{n-1} = C_{n+k-1}^k$ и како тој е еднаков на бројот на комбинациите со повторување од n елементи од класа k, добиваме дека важи формулата (10). ♦

9.30. Пример. На колку начини може да се изберат три од дванаесетте букви

$$a,a,a,t,t,t,g,g,g,c,c,c\ ?$$

Решение. Во случајов имаме множество $A=\{a,t,g,c\}$ со четири елементи. Според условот на задачата, секој елемент на множеството A може да биде избран најмногу три пати, па затоа бројот на начините на избор на три од наведените дванаесет букви е еднаков на бројот на комбинациите со повторување од 4 елементи од класа 3, т.е. е еднаков на

$$\overline{C}_4^3 = C_{4+3-1}^3 = C_6^3 = \tfrac{6!}{3!3!} = 20\,.\ \blacklozenge$$

9.31. Пример. Колку елементи се потребни за да се добијат 276 комбинации од втора класа со повторување?

Решение. Од условот на задачата ја добиваме равенката $\overline{C}_n^2 = 276$, која е еквивалентна на равенката $C_{n+2-1}^2 = 276$, т.е. на равенката

$$\frac{n(n+1)}{2} = 276,\ n \in \mathbf{N}.$$

Решенијата на равенката $\frac{n(n+1)}{2} = 276$ се $n_1 = 23$ и $n_2 = -24$ и како $n \in \mathbf{N}$ добиваме дека за да се добијат 276 комбинации од втора класа со повторување се потребни 23 елементи. ♦

10. РЕШЕНИ ПРИМЕРИ

10.1. Пример. Нека се $a_1, a_2, ..., a_n$ ненегативни цели броеви. Докажете дека $a_1!a_2!...a_n! \le (a_1 + a_2 + ... + a_n)!$.

Решение. Бројот на пермутациите од $a_1 + a_2 + ... + a_n$ елементи од тип $(a_1, a_2, ..., a_n)$ е поголем или еднаков на еден. Според тоа, точно е неравенството $\frac{(a_1+a_2+...+a_n)!}{a_1!a_2!...a_n!} \ge 1$, кое е еквивалентно со бараното неравенство. ♦

10.2. Пример. Колку нули има во записите на броевите $1, 2, 3, ..., 10^9$.

Решение. k-цифрени броеви има $10^k - 10^{k-1} = 9 \cdot 10^{k-1}$. Во нивниот запис има $9k \cdot 10^{k-1}$ цифри. Бројот на нулите во записите на сите k-цифрени броеви е еднаков на $(9k \cdot 10^{k-1} - 9 \cdot 10^{k-1}) / 10 = 9(k-1) \cdot 10^{k-2}$. Според тоа, бројот на нулите во записите на броевите $1, 2, 3, ..., 10^9$ е

$$\sum_{k=1}^{9} 9(k-1) \cdot 10^{k-2} + 9, \text{ (зошто?). } ♦$$

10.3. Пример. Дадени се $3n+1$ предмети, така да n од овие предмети не се разликуваат меѓу себе, а сите останати предмети се разликуваат и меѓу себе и од првите n предмети. На колку начини можат да се изберат n предмети?

Решение. Бројот на изборите на n предмети, кај кои се избрани точно k од множеството од n исти предмети, е еднаков на $\binom{2n+1}{n-k}$. Значи, бројот на сите избори на n предмети е:

$$\binom{2n+1}{n} + \binom{2n+1}{n-1} + ... + \binom{2n+1}{0} = \frac{1}{2}\left[\binom{2n+1}{0} + \binom{2n+1}{1} + ... + \binom{2n+1}{n} + \binom{2n+1}{n} + ... + \binom{2n+1}{2n+1}\right]$$
$$= \frac{1}{2}(1+1)^{2n+1} = 2^{2n}.$$

10.4. Пример. Во сенатот има 30 сенатори. Секој од сенаторите е скаран со точно шест други сенатори. На колку начини може да биде формирана тричлена комисија така да секои два члена на комисијата се скарани меѓу себе или никои два члена на комисијата не се скарани.

Решение. Нека x е бројот на тричлените комисии за кои важи условот на задачата (таквите комисии ќе ги нарекуваме добри), а y е бројот на тричлените комисии за кои условот не важи. Тогаш

$$x+y=\binom{30}{3}=4060.$$

Да претпоставиме дека секој сенатор прави список од сите комисии чиј член е, но така што тој е скаран со секој од останатите два члена или не е скаран со ниту еден од останатите два члена. Тогаш, секој таков список содржи $\binom{23}{2}+\binom{6}{2}=268$ комисии. Според тоа, секоја добра комисија ќе биде запишана точно во три списоци, а секој комисија која не е добра ќе биде запишана само во еден од тие списоци. Затоа важи

$$3x+y=30\cdot 268=8040.$$

Така, го добивме системот

$$\begin{cases} x+y=4060 \\ 3x+y=8040 \end{cases}$$

од каде наоѓаме $x=1990$. ♦

10.5. Пример. На колку начини n особи можат да застанат во редица, а притоа две фиксирани особи да не бидат една до друга?

Решение. Нека се воочени особите a и b. Прво ќе го определиме бројот на распоредите (пермутациите) во кои особите a и b се една до друга. Во овој случај постојат две можности: особата a да е лево од особата b и особата a да е десно од особата b. Во двата случаи бројот на пермутациите е $(n-1)!$, бидејќи парот од двете особи може да се смета како еден елемент во пермутација од $n-1$ елементи. Според тоа, вкупниот број пермутации во кои особите a и b се една до друга е $2(n-1)!$. Конечно, бараниот број распоредувања е

$$n!-2(n-1)!=n\cdot(n-1)!-2(n-1)!=(n-1)!(n-2). \blacklozenge$$

10.6. Пример. На колку начини може да се потполни правоаголна таблица со m редици и n колони (вкупно mn полиња) со броевите $+1$ и -1 така што производот на броевите во секој ред и секоја колона да биде еднаков на 1?

Решение. Сите таблици кои го имаат саканото својство можат да се состават на следниов начин. Во сите полиња со исклучок на последниот ред и последната колона на произволен начин ќе ги запишеме броевите $+1$ и -1. Јасно, тоа може да се направи на $2^{(m-1)(n-1)}$ начини. Сега со p да го означиме производот на сите запишани броеви. Понатаму, во секој од првите $m-1$ редови, во пресекот со $n-$тата колона ќе запишеме $+1$ или -1 така да производот во секој ред да биде еднаков на 1. Сега во пресекот на секоја од првите $n-1$ колона со $m-$от ред ќе запишеме $+1$ или -1 така да производот на броевите во секоја колона да биде еднаков на 1. Нека b е производот на броевите запишани во $m-$тата редица и a е производот на броевите запишани во $n-$тата колона.

Бидејќи $pa=1$ и $pb=1$ добиваме $p^2ab=1$, т.е. $ab=1$. Значи, броевите a и b се со ист знак, па затоа ако во пресекот на $m-$тата редица и $n-$тата колона го запишеме бројот $a=b$, добиваме дека вака конструираната таблица ги има саканите својства. Според тоа, имаме $2^{(m-1)(n-1)}$ таблици со саканите својства. ♦

10.7.Пример. Најди го бројот на подмножествата на множеството $\{1,2,...,2n\}$ во кои равенката $x+y=2n+1$ нема решение?

Решение. Елементите на множеството $\{1,2,...,2n\}$ ќе ги поделиме на n парови, така што збирот на броевите во секој пар е $2n+1$. При формирањето на подмножествата во кои равенката $x+y=2n+1$ нема решение, за секој од овие парови постојат три можности: ниеден не е во подмножеството, само помалиот е во подмножеството и само поголемиот е во подмножеството. Според тоа, бараниот број е 3^n. ♦

10.8.Пример. Најди го бројот на пермутациите на цифрите $1,2,...,9$ такви што единицата не е на првото место, двојката не е на првите две места и тројката не е на првите три места.

Решение. Тројката може да се стави на едно од последните 6 места, двојката на едно од последните 7 места на кои не е тројката (6 можности) и единицата на едно од последните 8 места на кои не е ниту двојката ниту тројката (6 можности). Останатите 6 цифри се распоредуваат на 6 слободни места. Значи, бројот на бараните пермутации е $6\cdot 6\cdot 6\cdot 6!=155520$. ♦

10.9.Пример. Докажете дека за секој природен број n кој не е делив ниту со 2 ниту со 5, постои природен број N чии цифри се сите единици и кој е делив со n.

Решение. Да ги разгледаме броевите

$$1,\ 11,\ 111,\ 1111,\ ...,\ \underbrace{111...11}_{n+1}.$$

Во оваа низа постојат два броја кои при делењето со n даваат ист остаток, па затоа нивната разлика се дели со n. Според тоа, постои природен број

$$\underbrace{111...11}_{h}\underbrace{000...00}_{s}=\underbrace{111...11}_{h}\cdot 10^s=\underbrace{111...11}_{h}\cdot 2^s5^s$$

кој се дели со n. Но, n не се дели со 2 и со 5, па затоа бројот $N=\underbrace{111...11}_{h}$ се дели со n. ♦

10.10. Пример. Дали за некој природен број n, бројот 3^n може да завршува на 000001?

Решение. Да ги разгледаме 10^6 различни степени на бројот 3:

$$3, 3^2, 3^3, ..., 3^{10^6}$$

и остатоците при делењето на секој степен со 10^6. Секој од овие броеви при делење со 10^6 дава остаток различен од нула. Значи, бројот на различни остатоци е еднаков на $10^6 - 1$, а броеви има 10^6. Според тоа, постојат два различни степени 3^m и 3^n, $m > n$ со ист остаток. Нивната разлика $3^m - 3^n = 3^n(3^{m-n} - 1)$ е делива со 10^6. Но, броевите 3^n и 10^6 немаат заеднички делител, па затоа бројот $3^{m-n} - 1$ се дели со 10^6, т.е. $3^{m-n} - 1 = 10^6 k$, односно

$$3^{m-n} = 10^6 k + 1 = \overline{...a000001}. \ \blacklozenge$$

11. БИНОМНА ФОРМУЛА

11.1 Нека $a, b \in \mathbf{R}$ и да ги разгледаме степените на биномот $a + b$. Знаеме дека

$$(a+b)^0 = 1,$$
$$(a+b)^1 = a + b,$$
$$(a+b)^2 = a^2 + 2ab + b^2 \text{ и}$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Ако ги пресметаме четвртиот и петтиот степен на $a + b$ ќе добиеме

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \text{ и}$$
$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Коефициентите на првите шест степени на биномот $a + b$ ќе ги запишеме во следнава шема

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

која во литературата е позната како *Паскалов триаголник*. Забележуваме дека сите редови во Паскаловиот триаголник започнуваат и завршуваат со бројот 1, но останатите броеви се различни и некако неповрзани. Меѓутоа, ако добро погледнеме ќе забележиме дека, на пример, за броевите во четвртиот и петтиот ред важи $4 = 1 + 3, 6 = 3 + 3, 4 = 3 + 1$, а за броевите во петтиот и шестиот ред важи $5 = 1 + 4$, $10 = 4 + 6, 10 = 6 + 4, 5 = 4 + 1$. Логично е да се запрашаме дали на ист начин од броевите во шестиот ред можеме да ги добиеме броевите во седмиот ред. Ако послед-

ното е точно, тогаш броевите во седмиот ред на Паскаловиот триаголник треба да бидат

$$1, 1+5=6, 5+10=15, 10+10=20, 10+5=15, 5+1=6 \text{ и } 1,$$

па затоа треба да важи формулата

$$(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6,$$

во чија точност можеме да се убедиме со непосредна проверка.

Претходно изнесеното ни дава за право да претпоставиме дека за пресметување на степените на биномот $a+b$ постои формула која треба да ја најдеме. За таа цел прво ќе се потсетиме на комбинациите без повторување. Имено, за комбинациите без повторување од 2 елемента од класа 0,1 и 2 соодветно имаме:

$$C_2^0 = \frac{2!}{0!2!} = 1, \quad C_2^1 = \frac{2!}{1!1!} = 2 \text{ и } C_2^2 = \frac{2!}{2!0!} = 1,$$

а за комбинациите без повторување од 3 елементи од класа 0,1,2 и 3 соодветно имаме:

$$C_3^0 = \frac{3!}{0!3!} = 1, \quad C_3^1 = \frac{3!}{1!2!} = 3, \quad C_3^2 = \frac{3!}{2!1!} = 3 \text{ и } C_3^3 = \frac{3!}{3!0!} = 1,$$

па затоа ако ја воведеме ознаката $C_n^k = \binom{n}{k}$, тогаш за вториот и третиот степен на биномот $a+b$ имаме

$$(a+b)^2 = \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2 \text{ и}$$

$$(a+b)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3.$$

Следејќи ја оваа идеја, логично е да претпоставиме дека формулата за наоѓање на $n-$ от степен на биномот $a+b$ е

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{k}a^{n-k}b^k + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n. \quad (1)$$

Пред да преминеме на доказот на оваа формула повторно да се навратиме на коефициентите во Паскаловиот триаголник. Од претходно изнесеното за коефициентот C_3^2 имаме $C_3^2 = 3 = 2+1 = C_2^1 + C_2^2$, т.е. $\binom{3}{2} = \binom{2}{1} + \binom{2}{2}$. Ќе докажеме дека за дел од коефициентите во Паскаловиот триаголник важи формула аналогна на формулата најдена за C_3^2, т.е. ќе ја докажеме следнава теорема.

11.2. Теорема. За секој $k \geq 2$ и за секој $i \in \{2, 3, \ldots, k\}$ важи

$$\binom{k}{i-1} + \binom{k}{i} = \binom{k+1}{i}. \quad (2)$$

Доказ. Нека $k \geq 1$. Тогаш, за секој $i \in \{1, 2, 3, \ldots, k\}$ имаме

$$\binom{k}{i-1} + \binom{k}{i} = \frac{k!}{(i-1)!(k-i+1)!} + \frac{k!}{i!(k-i)!} = \frac{k!}{(i-1)!(k-i)!}\left[\frac{1}{k-i+1} + \frac{1}{i}\right]$$

$$= \frac{k!}{(i-1)!(k-i)!} \cdot \frac{i+k-i+1}{i(k+1-i)} = \frac{(k+1)!}{i!(k+1-i)!} = \binom{k+1}{i}$$

што и требаше да се докаже. ♦

11.3. Сега користејќи ја претходната теорема, принципот на математичка индукција и фактот дека за секој $k \in \mathbf{N}$ важи

$$\binom{k}{0} = \binom{k+1}{0} = 1 = \binom{k}{k} = \binom{k+1}{k+1},$$

(провери!), ќе ја докажеме формулата (1), т.е ќе ја докажеме следнава теорема.

11.4. Теорема. За секои $a, b \in \mathbf{R}$ и секој $n \in \mathbf{N}$ точна е формулата (1).

Доказ. За $n = 1$ имаме $(a+b)^1 = a + b = \binom{1}{0}a + \binom{1}{1}b$, т.е. формулата (1) е точна.

Нека претпоставиме дека формулата (1) е точна за $n = k$, т.е. дека важи

$$(a+b)^k = \binom{k}{0}a^k + \binom{k}{1}a^{k-1}b + \binom{k}{2}a^{k-2}b^2 + \ldots + \binom{k}{i}a^{k-i}b^i + \ldots + \binom{k}{k-1}ab^{k-1} + \binom{k}{k}b^k . \quad (3)$$

Тогаш, од индуктивната претпоставка и од равенството (2) за $n = k+1$ имаме

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)^k (a+b) \\
&= [\binom{k}{0}a^k + \binom{k}{1}a^{k-1}b + \binom{k}{2}a^{k-2}b^2 + \ldots + \binom{k}{i}a^{k-i}b^i + \ldots + \binom{k}{k-1}ab^{k-1} + \binom{k}{k}b^k](a+b) \\
&= a^{k+1} + \binom{k}{1}a^k b + \binom{k}{2}a^{k-1}b^2 + \ldots + \binom{k}{i}a^{k+1-i}b^i + \ldots + \binom{k}{k}ab^k + \\
&\quad + \binom{k}{0}a^k b + \binom{k}{1}a^{k-1}b^2 + \ldots + \binom{k}{i-1}a^{k+1-i}b^i + \ldots + \binom{k}{k-1}ab^k + b^{k+1} \\
&= \binom{k+1}{0}a^{k+1} + \binom{k+1}{1}a^k b + \binom{k+1}{2}a^{k-1}b^2 + \ldots + \binom{k+1}{i}a^{k+1-i}b^i + \ldots + \binom{k+1}{k}ab^k + \binom{k+1}{k+1}b^{k+1}
\end{aligned}$$

т.е. формулата (1) важи и за $n = k+1$.

Конечно, од принципот на математичка индукција следува дека биномната формула е точна за секои $a, b \in \mathbf{R}$ и секој $n \in \mathbf{N}$. ♦

11.5. Забелешка. Формулата (1) во литературата е позната како *биномна формула* или *Њутнова биномна формула*, а коефициентите $\binom{n}{k}$, $k = 0, 1, 2, \ldots, n$ како *биномни коефициенти*.

11.6. Пример. Докажи дека за секој $n \in \mathbf{N}$ важи:

а) $2^n = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n-1} + \binom{n}{n}$,

б) $0 = \binom{n}{0} - \binom{n}{1} + \ldots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n}$.

Решение. а) Равенството непосредно следува од биномната формула при $a = b = 1$.

б) Непосредно следува од биномната формула при $a = 1, b = -1$. ♦

11.7. Пример . а) Степенувај го биномот $(2x+5)^4$.

б) Користејќи ја биномната формула пресметај $1{,}03^{10}$ со точност до четвртото децимално место.

Решение. а) Имаме

$$(2x+5)^4 = \binom{4}{0}(2x)^4 + \binom{4}{1}(2x)^3 5 + \binom{4}{2}(2x)^2 5^2 + \binom{4}{3}(2x)5^3 + \binom{4}{4}5^4$$
$$= 16x^4 + 160x^3 + 600x^2 + 1000x + 625.$$

б) Имаме

$$1,03^{10} = (1+0,03)^{10} = 1 + \binom{10}{1}\cdot 0,03 + \binom{10}{2}\cdot 0,03^2 + \binom{10}{3}\cdot 0,03^3 + \binom{10}{4}\cdot 0,03^4 + \binom{10}{5}\cdot 0,03^5 + \ldots$$
$$= 1 + 0,3 + 0,0405 + 0,00324 + 0,0001701 + 0,0000061236 + \ldots \approx 1,3439162236$$

т.е. со точност до четири децимални места важи $1,03^{10} \approx 1,3439$. Обиди се да објасниш зошто е доволно да се соберат само првите шест членови во развојот. ♦

11.8. Пример. Определи го членот кој не го содржи x во развојот на степенот

$$\left(x^2 - \frac{1}{x}\right)^9.$$

Решение. Имаме

$$T_{k+1} = \binom{9}{k}(x^2)^{9-k}\left(-\frac{1}{x}\right)^k = \binom{9}{k}\cdot x^{18-2k}(-1)^k x^{-k} = \binom{9}{k}\cdot(-1)^k x^{18-3k}$$

па за да не се содржи x потребно е $18-3k=0$. Според тоа, $k=6$ и значи седмиот член не го содржи x и $T_{6+1} = \binom{9}{6}\cdot(-1)^6 = 84$. ♦

11.9. Пример. Најди го средниот член во развојот на биномот

$$\left(a^{-2}\sqrt{a} - \sqrt[5]{\frac{a^{-2}}{\sqrt{a}}}\right)^n$$

ако коефициентот на петтиот член спрема коефициентот на третиот член се однесува како $14:3$.

Решение. Бидејќи биномот не содржи константи добиваме дека коефициентот на петтиот член е $\binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{24}$ а коефициентот на третиот член е $\binom{n}{2} = \frac{n(n-1)}{2}$. Од условот на задачата ја добиваме равенката

$$\binom{n}{4} : \binom{n}{2} = 14:3,$$

која е еквивалентна на равенката

$$\frac{n(n-1)(n-2)(n-3)}{24} : \frac{n(n-1)}{2} = 14:3, \quad n \in \mathbf{N},$$

т.е. на равенката $n^2 - 5n - 50 = 0, \quad n \in \mathbf{N}$. Решенијата на равенката $n^2 - 5n - 50 = 0$ се $n_1 = -5$ и $n_2 = 10$ и како $n \in \mathbf{N}$ добиваме дека степенот на биномот е $n = 10$. Според тоа, развојот содржи 11 члена и треба да го определиме шестиот. Значи, бараниот член е

$$T_{5+1} = \binom{10}{5}(a^{-2}\sqrt{a})^5\left(-\sqrt[5]{\frac{a^{-2}}{\sqrt{a}}}\right)^5 = -252a^{-10}. \ \blacklozenge$$

12. ПРЕБРОЈЛИВИ МНОЖЕСТВА. КАРДИНАЛНИ БРОЕВИ

12.1. Пред да го воведеме поимот за пребројливо множество ќе дадеме дефиниција за низа, поим кој во нашите натамошните разгледувања ќе има важна улога.

Дефиниција. Нека е дадено непразното множество A. Секое пресликување $a:\mathbf{N}\to A$ ќе го наречеме *низа во множеството* A.

Притоа, наместо $a(i)$ пишуваме a_i, за секој $i\in\mathbf{N}$ и a_i го нарекуваме $i-$ти член на низата. За низата $a:\mathbf{N}\to A$ ќе ги користиме ознаките $a_i, i=1,2,3,...$ или $\{a_i\}_{i=1}^{\infty}$.

12.2. Дефиниција. За множеството A ќе велиме дека е *пребројливо* ако $A\sim\mathbf{N}$. За множеството A ќе велиме дека е *најмногу пребројливо* ако тоа е конечно или пребројливо.

12.3. Лема. Множеството A е пребројливо ако и само ако

$$A=\{a_i \mid i\in\mathbf{N},\ a_k\neq a_j \text{ за } k\neq j\}.$$

Доказ. Нека A е пребројливо множество и нека $f:\mathbf{N}\to A$ е биекција. За секој $i\in\mathbf{N}$ важи $f(i)=a_i\in A$ и за $k\neq j$ имаме

$$a_k=f(k)\neq f(j)=a_j,$$

што значи дека $A=\{a_i \mid i\in\mathbf{N},\ a_k\neq a_j \text{ за } k\neq j\}$.

Обратно, ако

$$A=\{a_i \mid i\in\mathbf{N},\ a_k\neq a_j \text{ за } k\neq j\}$$

тогаш пресликувањето $g(n)=a_n$ е биекција од $\mathbf{N}$ во A, што значи дека A е пребројливо множество. ♦

12.4. Забелешка. Од лема 12.3 следува дека множеството A е пребројливо ако и само елементите на множеството A можат да се запишат во низа $a_1,...,a_n,...$, каде што $a_i\neq a_j$, за $i\neq j$. Користејќи го записот на пребројливо множество во облик на низа $a_1,...,a_n,...$, каде $a_i\neq a_j$, за $i\neq j$, лесно се докажува дека унијата на пребројливо и конечно множество е пребројливо множество. Доказот на ова тврдење го оставаме на читателот за вежба.

Претходно кажаното често пати ќе го користиме во натамошните излагања на овој дел.

12.5. Теорема. Секое бесконечно множество содржи пребројливо множество.

Доказ. Нека A е бесконечно множество. Тогаш, $A\neq\varnothing$, па затоа постои $a_1\in A$. Бидејќи A е бесконечно множество добиваме дека множеството $A\setminus\{a_1\}$ не е празно, па затоа постои $a_2\in A\setminus\{a_1\}$. Продолжувајќи ја постапката, при што

се користи фактот дека множеството A е бесконечно конструираме низа $a_1, a_2, ..., a_n, ...$, каде што $a_i \neq a_j$, за $i \neq j$. Пресликувањето $f(i) = a_i$, $i \in \mathbf{N}$ е биекција, па затоа множеството $A_0 = \{a_1, a_2, ..., a_n, ...\} \subseteq A$ е пребројливо. ♦

12.6. Теорема. Секое бесконечно подмножество на пребројливо множество е пребројливо.

Доказ. Нека елементите на пребројливото множество A се запишани во бесконечна низа $a_1, ..., a_n, ...$, каде што $a_i \neq a_j$, за $i \neq j$ и A' е бесконечно подмножество на A. Нека a_{n_1} е елемент на A' со најмал индекс, a_{n_2} е елемент на $A' \setminus \{a_{n_1}\}$ со најмал индекс, a_{n_3} е елемент на $A' \setminus \{a_{n_1}, a_{n_2}\}$ со најмал индекс итн. Така елементите на множеството A' се запишани во бесконечна низа

$$a_{n_1}, a_{n_2}, a_{n_3}, ..., a_{n_k}, ...,$$ каде $a_{n_i} \neq a_{n_j}$, за $i \neq j$,

што значи дека пресликувањето $f : \mathbf{N} \to A'$ дефинирано со $f(i) = a_{n_i}$ е биекција, т.е. A' е пребројливо множество. ♦

12.7. Теорема. Унија од пребројлива фамилија пребројливи множества е пребројливо множество.

Доказ. Нека $A_1, A_2, A_3, ...$ е пребројлива фамилија пребројливи множества. Тогаш, за секој $k \geq 1$ имаме $A_k = \{a_{k1}, a_{k2}, a_{k3}, ..., a_{kn}, ...\}$, а унијата $\bigcup_{n \geq 1} A_n$ е множеството составено од сите елементи во табелава

$$\begin{array}{ccccccc}
a_{11} & a_{12} & a_{13} & a_{14} & \ldots & a_{1n} & \ldots \\
a_{21} & a_{22} & a_{23} & a_{24} & \ldots & a_{2n} & \ldots \\
a_{31} & a_{32} & a_{33} & a_{34} & \ldots & a_{3n} & \ldots \\
a_{41} & a_{42} & a_{43} & a_{44} & \ldots & a_{4n} & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
a_{k1} & a_{k2} & a_{k3} & a_{k4} & \ldots & a_{kn} & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

кои одејќи по дијагоналите од десно горе кон лево надолу, ги запишуваме во бесконечна низа, при што веќе појавените елементи ги испуштаме. Значи елементите на $\bigcup_{n \geq 1} A_n$ можеме да ги запишеме како бесконечна низа на следниот начин

$$b_1 = a_{11}, b_2 = a_{12}, b_3 = a_{21}, b_4 = a_{13}, b_5 = a_{22}, b_6 = a_{31}, b_7 = a_{14}, b_8 = a_{23}, b_9 = a_{32}, ...$$

и како што рековме веќе појавените елементи ги испуштаме. Според тоа, множеството $\bigcup_{n \geq 1} A_n$ е пребројливо. ♦

12.8. Последица. Декартовиот производ на две пребројливи множества е пребројливо множество.

Доказ. Нека

$$A=\{a_1,a_2,....,a_n,....\} \text{ и } B=\{b_1,b_2,....,b_k,....\}$$

се пребројливи множества. Тогаш, множествата $C_i=A\times\{b_i\}, i=1,2,3,...$ се пребројливи (зошто?) и притоа важи $A\times B=\underset{i\geq 1}{\cup} C_i$. Сега тврдењето следува од теорема 12.7. ♦

12.9. Последица. За секој $n\in\mathbf{N}$ Декартовиот производ $A_1\times...\times A_n$ на пребројливите множества $A_1,...,A_n$ е пребројливо множество.

Доказ. Непосредно следува од последица 12.8 и принципот на математичка индукција. Деталите ги оставаме на читателот за вежба. ♦

12.10. Последица. Нека A е пребројливо множество и за секој $n\in\mathbf{N}$ да го определиме множеството

$$A^n=\{(a_1,...,a_n)\mid a_i\in A, \text{ за } i=1,2,...,n\}.$$

Тогаш множеството $B=\underset{n\geq 1}{\cup} A^n$ е пребројливо.

Доказ. Од последица 12.9 следува дека за секој $n\in\mathbf{N}^+$ множеството

$$A^n=\{(a_1,...,a_n)\mid a_i\in A, \text{ за } i=1,2,...,n\}$$

е пребројливо. Сега тврдењето следува од теорема 12.7. ♦

12.11. Последица. Унија на конечно многу пребројливи множества е пребројливо множество.

Доказ. Нека се дадени пребројливите множества $A_1,A_2,...,A_n$. Множествата $A_k=A_n$, за $k>n$ се пребројливи, па така множеството

$$\bigcup_{i=1}^{n} A_i=\bigcup_{i\geq 1} A_i$$

е унија на пребројлива фамилија пребројливи множества. Според теорема 12.7 ова множество е пребројливо, што и требаше да се докаже. ♦

12.12. Пример. а) Множеството цели броеви $\mathbf{Z}$ е пребројливо.

б) Множеството рационални броеви $\mathbf{Q}$ е пребројливо.

Решение. а) Пресликувањето $f:\mathbf{N}\to\mathbf{Z}^-\cup\{0\}$, дефинирано со

$$f(n)=1-n, \text{ за секој } n\in\mathbf{N},$$

е биекција, па затоа множеството $\mathbf{Z}^-\cup\{0\}$ е пребројливо. Сега тврдењето следува од $\mathbf{Z}=\mathbf{N}\cup\mathbf{Z}^-\cup\{0\}$ и од последица 12.11.

б) Од пребројливоста на множеството $\mathbf{Z}$ следува дека за секој $i=1,2,...$ множествата

$$\mathbf{Q}_i = \{\frac{m}{i} \mid \ m \in \mathbf{Z}\}$$

се пребројливи (зошто?). Но,

$$\mathbf{Q} = \underset{i \geq 1}{\cup} \mathbf{Q}_i ,$$

па од теорема 12.7 следува дека множеството $\mathbf{Q}$ е пребројливо. ♦

12.13. Теорема. Постои бесконечно множество кое е *непребројливо*.

Доказ. Нека A е множеството од сите низи во множеството $B = \{0,1\}$, т.е. множеството од сите низи $\{a_i\}_{i=1}^{\infty}$, каде $a_i = 0$ или $a_i = 1$, за секој $i \in \mathbf{N}$. Очигледно множеството A е бесконечно. Ќе докажеме дека тоа не е пребројливо.

Нека допуштиме дека множеството A е пребројливо, т.е дека неговите елементи можат да се запишат во бесконечна низа

$$\begin{aligned} a_1 &= (a_{11}, a_{12}, a_{13}, a_{14}, ..., a_{1n}, ...) \\ a_2 &= (a_{21}, a_{22}, a_{23}, a_{24}, ..., a_{2n}, ...) \\ &..... \\ a_k &= (a_{k1}, a_{k2}, a_{k3}, a_{k4}, ..., a_{kn}, ...) \\ &..... \end{aligned} \qquad (1)$$

од различни елементи, каде што $a_{ij} = 0$ или 1, за секои $i, j \in \mathbf{N}$ и дека сите елементи на множеството A се содржат во низата (1). Наоѓаме елемент $b = (b_1, ..., b_n, ...)$ каде што $b_i = 0$ или 1 и притоа важи $b_i \neq a_{ii}$, за секој $i \in \mathbf{N}$. Јасно, $b \in A$, но тој е различен од сите елементи во низата (1), што е противречност. Од добиената противречност следува дека множеството A не е пребројливо. ♦

12.14. Забелешка. Методот со кој е докажана претходната теорема е познат под името *Канторов дијагонален метод*. Претходната теорема ни беше потребна за да ги докажеме следните две тврдења. Но, претходно да кажеме дека за множествата A и B ќе велиме дека имаат *еднакви кардинални броеви* ако тие се еквивалентни и ќе пишуваме $k(A) = k(B)$. Понатаму, ако постои инјекција од множеството A во множеството B, тогаш ќе велиме дека кардиналниот број на множеството A е *помал или еднаков* на кардиналниот број на множеството B и ќе пишуваме $k(A) \leq k(B)$. Ако $k(A) \leq k(B)$ и $k(A) \neq k(B)$, тогаш ќе велиме дека кардиналниот број на множеството A е помал од кардиналниот број на множеството B и ќе пишуваме $k(A) < k(B)$.

Кардиналниот број на пребројливите множества ќе го означуваме со $\aleph_0$, (*алеф нула*).

12.15. Теорема. Кардиналниот број на бесконечното множество A не се менува ако кон него додадеме најмногу пребројливо множество B.

Доказ. Нека множеството A е бесконечно. Тогаш, тоа содржи пребројливо подмножество C. Множеството $B \cup C$ е пребројливо, па затоа постои биекција $f : B \cup C \to C$. Дефинираме пресликување $g : A \cup B \to A$ со

$$g(x)=\begin{cases} f(x); & x\in B\cup C \\ x; & x\in A\setminus C \end{cases}$$

кое е биекција од $A\cup B$ во A, па затоа $A\cup B\sim A$, т.е. $k(A\cup B)=k(A)$. ♦

12.16. Теорема. Кардиналниот број на бесконечно непребројливо множество не се менува ако од него извадиме најмногу пребројливо множество.

Доказ. Нека A е бесконечно непребројливо множество и нека B е негово најмногу пребројливо множество. Множеството $C=A\setminus B$ е бесконечно и е непребројливо, бидејќи во спротивен случај множеството A би било пребројливо. Според претходната теорема имаме

$$k(C)=k(C\cup B)=k((A\setminus B)\cup B)=k(A),$$

што и требаше да докажеме. ♦

12.17. На крајот од овој дел во врска со кардиналните броеви на множествата ќе докажеме уште неколку тврдења за кои сметаме дека можда не се погодни за обработка со студентите од прва година.

Теорема А. Нека A е произволно множество и $P(A)$ е неговото партитивно множество (Булеан). Тогаш

$$k(P(A))>k(A).$$

Доказ. Пресликувањето $f:A\to P(A)$ определено со $f(a)=\{a\}$ е инјекција, па затоа $k(A)\le k(P(A))$.

Ќе докажеме дека меѓу A и $P(A)$ не може да се воспостави биекција, т.е. дека $k(A)\ne k(P(A))$. Нека $f:A\to P(A)$ е произволно пресликување. Ќе докажеме дека постои барем еден елемент во $P(A)$ кој со пресликувањето f не е слика на ниеден елемент од A, па од произволноста на f ќе следува дека не постои биекција меѓу A и $P(A)$. Нека B е подмножество од A кое ги содржи сите оние елементи $a\in A$ кои не лежат во својата слика, т.е. $B=\{a\in A\mid a\notin f(a)\}$. Ако B е слика на некој $b\in A$, т.е. $f(b)=B$, тогаш или $b\notin f(b)$, па затоа $b\in B$, т.е. $b\in f(b)$, што е противречност или $b\in f(b)$, па затоа $b\in B$, т.е. $b\notin f(b)$, што повторно е противречност, од што следува дека f не е биекција, т.е

$$k(A)\ne k(P(A)).$$ ♦

Теорема Б. Ако $k(S)\le k(T)$ и $k(T)\le k(S)$, тогаш $k(S)=k(T)$, т.е. множествата S и T се еквивалентни.

Доказ. Нека претпоставиме дека $k(S)\le k(T)$ и $k(T)\le k(S)$ и нека $f:S\to T$ и $g:T\to S$ се инјекции. Нека $s\in S$ и да го определиме елементот $g^{-1}(s)$ ако тој постои. Понатаму го определуваме елементот $f^{-1}g^{-1}(s)$ ако тој

постои, па го определуваме елементот $g^{-1}f^{-1}g^{-1}(s)$ ако тој постои итн. Постапката ја повторуваме за секој $s \in S$. Можни се три случаи:

(1) Постапката ќе се повторува бесконечно многу пати.

(2) Постапката ќе заврши, бидејќи за некој s_i во постапката не постои $g^{-1}(s_i)$.

(3) Постапката ќе заврши бидејќи за некој t_i во постапката не постои $f^{-1}(t_i)$.

Нека со S_1 го означиме множеството елементи од S за кои се добива првиот резултат, со S_2 го означиме множеството елементи од S за кои се добива вториот резултат и со S_3 го означиме множеството елементи од S за кои се добива третиот резултат. Јасно, множествата S_1, S_2 и S_3 се заемно дисјунктни. На сличен начин, поаѓајќи од елементите на множеството T ги конструираме множествата T_1, T_2 и T_3 кои се заемно дисјунктни. Лесно се гледа дека пресликувањето $f_{|S_1}$ е биекција од S_1 на T_1, пресликувањето $f_{|S_2}$ е биекција од S_2 на T_2 и пресликувањето $g^{-1}_{|S_3}$ е биекција од S_3 на T_3 (проверете). Но, множествата S_1, S_2, S_3 и се заемно дисјунктни и $S = S_1 \cup S_2 \cup S_3$, а множествата T_1, T_2, T_3 се заемно дисјунктни и притоа важи $T = T_1 \cup T_2 \cup T_3$, па затоа пресликувањето $h: S \to T$ определено со

$$h(s) = \begin{cases} f(s), & s \in S_1 \cup S_2, \\ g^{-1}(s), & s \in S_3, \end{cases}$$

е биекција, што значи $k(S) = k(T)$. ♦

Теорема В. Нека $m, n \in \mathbf{N}$. Тогаш постои биекција меѓу природните броеви кои се помали или еднакви на бројот m и вистинско подмножество на природните броеви кои се помали или еднакви од бројот n ако и само ако $m < n$.

Доказ. Јасно, ако $m < n$, тогаш пресликувањето $f : \{1, 2, ..., m\} \to \{1, 2, ..., n\}$ определено со $f(i) = i$ е инјекција и како $\{1, 2, ..., m\} \subset \{1, 2, ..., n\}$ добиваме дека постои биекција од $\{1, 2, ..., m\}$ на вистинско подмножество на $\{1, 2, ..., n\}$.

За да го докажеме обратното тврдење ќе користиме индукција по бројот m. Ако $m = 1$ и ако f е биекција меѓу природните броеви кои се помали или еднакви на бројот 1 (според тоа, само природниот број 1) и вистинско подмножество на природните броеви кои се помали или еднакви на бројот n, тогаш очигледно е дека $n > 1$.

Нека претпоставиме дека тврдењето важи за $m = k - 1$ и нека постои биекција f меѓу природните броеви кои се помали или еднакви на бројот $m = k$ и вистинско подмножество на природните броеви кои се помали или еднакви од бројот n. Сакаме да најдеме биекција g меѓу природните броеви кои се помали или еднакви на бројот $k - 1$ и вистинско подмножество на множеството природни

броеви кои се помали или еднакви на бројот $n-1$. За таа цел дефинираме пресликување g на множеството $\{1,2,...,\ k-1\}$ на следниов начин:

$$g(i)=\begin{cases} f(i), & \text{ако } f(i)\neq n,\\ f(k), & \text{ако } f(i)=n. \end{cases}$$

Пресликувањето g е биекција меѓу множеството $\{1,2,...,k-1\}$ и вистинско подмножество на множеството цели броеви кои се помали или еднакви на $n-1$ (зошто?). Од индуктивната претпоставка следува $k-1<n-1$, што значи дека $k<n$. ♦

13. НЕПРЕБРОЈЛИВИ МНОЖЕСТВА

13.1. Во претходната точка ги разгледавме пребројливите множества и докажавме дека множеството од сите низи од нули и единици е непребројливо. Во овој дел ќе се осврнеме на *непребројливите множества*, т.е. на множествата кои не се конечни или пребројливи.

13.2. Теорема (Кантор). Множеството реални броеви е непребројливо.

Доказ. Доволно е да докажеме дека интервалот $(0,1)$ е непребројливо множество (зошто?).

Нека претпоставиме дека интервалот $(0,1)$ е пребројливо множество и дека елементите на $(0,1)$ се подредени во низа. Тогаш, користејќи ги десетичните дропки имаме

$$d_1=0,\alpha_{11}\alpha_{12}...\alpha_{1n}...$$
$$d_2=0,\alpha_{21}\alpha_{22}...\alpha_{2n}...$$
$$.....$$
$$d_n=0,\alpha_{n1}\alpha_{n2}...\alpha_{nn}...$$
$$.....$$

и $(0,1)=\{d_i \mid \ i=1,2,...\}$. За реалниот број $d=0,b_1b_2...b_n...$ таков што

$$b_i=\begin{cases} 1, & \text{ако } \alpha_{ii}\neq 1\\ 2, & \text{ако } \alpha_{ii}=1 \end{cases}$$

важи $d\in(0,1)$ и $d\neq d_i$ за секој $i=1,2,...$, т.е. $d\notin\{d_i \mid \ i=1,2,...\}$, што е противречност. Од добиената противречност следува дека интервалот $(0,1)$ е непребројливо множество. Значи, множеството реални броеви е непребројливо. ♦

13.3. Дефиниција. За множеството A ќе велиме дека има кардинален број *континиум* c ако тоа е еквивалентно со множеството реални броеви.

13.4. Забелешка. Од лема 12.16 непосредно следува дека множеството ирационални броеви $\mathbf{I}$ е непребројливо и дека $k(\mathbf{I})=c$.

Во врска со непребројливите подмножества на $\mathbf{R}$ Кантор ја дал следната хипотеза, позната како *хипотеза на континиум*:

Ако B е бесконечно непребројливо подмножество на $\mathbf{R}$, тогаш B е еквивалентно со $\mathbf{R}$.

Интересно е да забележиме дека оваа хипотеза не е ниту потврдена, ниту е негирана, но за истата Гедел и Коен докажале дека таа е независна од аксиомите за реални броеви.

13.5. Лема. За секои $a,b \in \mathbf{R}$, $a<b$ важи $(a,b) \sim \mathbf{R}$.

Доказ. Да го разгледаме пресликувањето $f:(a,b)\to(-1,1)$ определено со

$$f(t)=\tfrac{2t-a-b}{b-a}, \text{ за } t\in(a,b).$$

Лесно се гледа дека ова пресликување е биекција, па затоа $(a,b)\sim(-1,1)$.

Сега, пресликувањето $g:(-1,1)\to\mathbf{R}$ определено со $g(x)=\frac{x}{1-|x|}$, за $x\in(-1,1)$ е биекција, па затоа $(-1,1)\sim\mathbf{R}$, што заедно со $(a,b)\sim(-1,1)$ дава $(a,b)\sim\mathbf{R}$. ♦

13.6. Лема. Унија на најмногу пребројливо многу множества A_k, $k=1,2,...$ со кардинален број континиум има кардинален број на континиум.

Доказ. Без ограничување на општоста можеме да сметаме дека множествата A_k, $k=1,2,...$ се дисјунктни по парови, што значи дека за секој $k=1,2,...$ важи $A_k\sim(k-1,k)$, (зошто?). Според тоа, $\bigcup_{k=1}^{\infty}A_k\sim(0,+\infty)\setminus\mathbf{N}$, па од лема 12.16 следува дека $\bigcup_{k=1}^{\infty}A_k\sim(0,+\infty)$.

Аналогно како во лема 13.5, се докажува дека $(0,+\infty)\sim(0,1)$ и, бидејќи $(0,1)\sim(-1,1)\sim\mathbf{R}$ добиваме $(0,+\infty)\sim\mathbf{R}$, т.е. $k(\bigcup_{k=1}^{\infty}A_k)=c$. ♦

13.7. Природно се поставува прашањето: Дали сите непребројливи множества се еквивалентни на множеството реални броеви, т.е. дали сите овие множества имаат кардинален број континиум? Одговорот на ова прашање е негативен. Овде ќе дадеме пример на непребројливо множество чиј кардинален број е поголем од c.

Пример. Ќе докажеме дека множеството

$$F=\{f \mid f:[0,1]\to\mathbf{R} \text{ е пресликување}\}$$

има кардинален број поголем од c.

Навистина, пресликувањето $g:\alpha\to f_\alpha$ дефинирано со

$$g(\alpha) = f_\alpha(x) = x + \alpha,\ \alpha \in [0,1]$$

е инјекција од $[0,1]$ во F, па затоа $k(F) \geq c$.

Нека претпоставиме дека $F \sim [0,1]$. Тоа значи дека меѓу функциите $f \in F$ и броевите $\alpha \in [0,1]$ може да се воспостави биекција. Според тоа, за секоја функција $f \in F$ постои индекс $\alpha \in [0,1]$, т.е.

$$f(x) = f_\alpha(x) \text{ и } F = \bigcup_{\alpha \in [0,1]} \{f_\alpha\}.$$

Да го разгледаме пресликувањето $g : [0,1] \times [0,1] \to \mathbf{R}$ дефинирано со $g(x,\alpha) = f_\alpha(x)$. Со помош на ова пресликување конструираме функција $\varphi : [0,1] \to \mathbf{R}$, $\varphi(x) = g(x,x) + 1$. Но, $\varphi \in F$, па затоа постои $\alpha_0 \in [0,1]$ таков, што $\varphi(x) = f_{\alpha_0}(x)$, за секој $x \in [0,1]$. Сега, за $x = \alpha_0 \in [0,1]$ добиваме

$$g(\alpha_0, \alpha_0) = g(\alpha_0, \alpha_0) + 1$$

што е противречност. Од добиената противречност следува дека множествата $[0,1]$ и F не се еквивалентни, т.е. $k(F) > c$. ♦

13.8. Забелешка. Да забележиме дека одговорот на поставеното прашање непосредно следува и од теорема 12.17 во која покажавме дека за секое множество A важи $k(P(A)) > k(A)$. Имено, според оваа теорема за множеството $\mathbf{R}$ важи $k(P(\mathbf{R})) > k(\mathbf{R}) = c$.

ЗАДАЧИ

1. Со набројување на неговите елементи запиши го:
   a) множеството од сите цели броеви меѓу 3 и 12;
   b) множеството од сите природни броеви деливи со 3 и помали од 25;
2. Со помош на својството кое го има, запиши го секое од множествата во задачата 1.
3. Запиши ги со набројување на нивните елементи множествата:
   a) $A = \{2^x \mid x \in \mathbf{N} \text{ i } x < 7\}$;
   b) $B = \{n \mid 3n = 7\}$;
4. Кои од множествата:
   $$A = \{1, 3, 7, 15, 31\},\ B = \{5, 11, 23, 47, 95\},\ C = \{2^x - 1 \mid x \in \mathbf{N},\ x \leq 5\} \text{ и}$$
   $$D = \{3 \cdot 2^x - 1 \mid x \in \mathbf{N},\ x \leq 5\}$$
   се меѓусебно еднакви?
5. Дадени се множествата: $\mathbf{N}$, $P = \{n \mid n = 2k, k \in \mathbf{N}\}$, $M = \{n \mid n = 2k - 1, k \in \mathbf{N}\}$. Каков однос постои меѓу множествата:
   a) $\mathbf{N}$ и P;

b) $\mathbf{N}$ и M;
c) M и P.

6. Најди ја унијата на множествата:
   a) $A=\{x\mid -1\le x<2,\ x\in\mathbf{R}\}$ и $B=\{x\mid 2\le x<4,\ x\in\mathbf{R}\}$;
   b) $A=\{x\mid x\le -2,\ x\in\mathbf{R}\}$ и $B=\{x\mid x\ge 2,\ x\in\mathbf{R}\}$.

7. Најди го пресекот на множествата:
   a) $A=\{x\mid -1\le x<2,\ x\in\mathbf{R}\}$ и $B=\{x\mid 0<x<4,\ x\in\mathbf{R}\}$;
   b) $A=\{x\mid x>-2,\ x\in\mathbf{R}\}$ и $B=\{x\mid x<2,\ x\in\mathbf{R}\}$;
   c) $A=\{x\mid x<-2,\ x\in\mathbf{R}\}$ и $B=\{x\mid x\ge -2,\ x\in\mathbf{R}\}$.

8. Најди непразни множества A,B и C такви, што
   a) $A\cup B=A\cup C$, но $B\ne C$;
   b) $A\cap B=A\cap C$, но $B\ne C$.

9. Најди ги елементите на множеството $G=\{(x,y)\mid 2x-y=1,\ x\in A,\ y\in B\}$, каде што $A=\{-1,\ 2,\ 3\}$ и $B=\{-3,\ -1,\ 2,\ 5,\ 7\}$.

10. Докажете дека од $A\subseteq B$ и $A\subseteq C$ следува $A\subseteq B\cap C$.

11. Докажете дека од $A,B\subset C$ следува $A\cup B\subseteq C$.

12. Нека A и B се две множества. За множеството C определено со
$$C=(A\cup B)\setminus(A\cap B)$$
ќе велиме дека е *симетрична разлика на множествата* A и B. Притоа пишуваме $C=A\dot{-}B$. Докажете дека:
   a) Множеството $A\dot{-}B$ се состои од елементите кои припаѓаат на едно и само едно од множествата A и B.
   b) $A\dot{-}B=B\dot{-}A$.
   c) $A\dot{-}A=\varnothing$.
   d) $A\dot{-}\varnothing=A$.
   e) $A\dot{-}(B\dot{-}C)=(A\dot{-}B)\dot{-}C$.
   f) $A\cap(B\dot{-}C)=(A\cap B)\dot{-}(A\cap C)$.

13. Докажи дека од $A\subseteq B$ и $C\subseteq D$ следува $A\times C\subseteq B\times D$.

14. Нека $A=\{1,\ 2,\ 3,\ 4,\ 5\}$ и f и g се пресликувања од A во A определени со $f=\begin{pmatrix}1&2&3&4&5\\1&1&2&1&3\end{pmatrix}$ и $g=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$.
   a) Пресметај $f(f(1)),\ f(g(2)),\ g(f(4))$ и $f(g(4))$.
   b) Најди ги графиците на f и g.
   c) Дали постои $x\in A$ таков, што $f(x)=g(x)$?

15. Нека $A=B=C=\mathbf{R}$ и нека пресликувањата $f:A\to B$ и $g:B\to C$ се дадени со $f(x)=2x+1$ и $g(x)=x^2+1$. Најди ги формулите на пресликувањата $f\circ g$, $g\circ f$ и $g\circ g$.

16. Нека $A=B=C=\mathbf{R}$ и нека пресликувањата $f:A\to B$ и $g:B\to C$ се дадени со $f(x)=3x-2$ и $g(x)=x+3$.
    1) Најди ги пресликувањата $f\circ g$ и $g\circ f$, а потоа пресметај $(f\circ g)(7)$ и $(g\circ f)(2)$.
    2) Определи ги графиците на пресликувањата f, g, $f\circ g$ и $g\circ f$.
    3) Дали постои $x\in\mathbf{R}$ таков што $g(x)=x$?

17. Докажи дека пресликувањето $f:\mathbf{R}\to[1,+\infty)$, $f(x)=x^2+1$ е сурјекција, но не е инјекција.

18. Нека M и N се непразни множества и F е подмножество од $M\times N$ со следниве својства:
    a) $(\forall x\in M)$ $(\exists y\in N)$ таков што $(x,y)\in F$,
    b) $(\forall x\in M)$ $(\forall y_1,y_2\in N)$ ако $(x,y_1),(x,y_2)\in F$, тогаш $y_1=y_2$.

    Нека ставиме $y=f(x)$ ако и само ако $(x,y)\in F$. Докажете дека f е пресликување од M во N. Какви својства треба да има множеството F за да f биде:
    1) инјекција,
    2) сурјекција.

19. Ако $f:M\to N$ и $g:N\to M$ се такви што $gf=I_M$, тогаш f е инјекција, а g е сурјекција. Докажете!

20. Ако $f:M\to N$ е инјекција, тогаш:
    a) од $A_1\subseteq A_2$ следува $f(A_1)\subseteq f(A_2)$,
    b) $f(A_1\cap A_2)=f(A_1)\cap f(A_2)$.

21. За пресликувањето $f:\mathbf{R}\to\mathbf{R}$ најди го инверзното пресликување ако
    a) $f(x)=\frac{1}{2}x+4$;
    b) $f(x)=-\frac{5}{4}x-\frac{2}{3}$;
    c) $f(x)=4x-\frac{1}{12}$.

22. Нека A,B и C се произволни множества. Докажете дека:
    a) $A\times B\sim B\times A$,
    b) $A\times(B\times C)\sim(A\times B)\times C$.

23. Ако $A\sim B$ и $C\sim D$, тогаш $A\times C\sim B\times D$. Докажете!

24. Докажете дека множествата
$$A=\{3k\mid k\in\mathbf{N}\},\ B=\{3k+1\mid k\in\mathbf{N}\}\ \text{и}\ C=\{3k+2\mid k\in\mathbf{N}\}$$
се еквивалентни меѓу себе.

25. Докажете дека множествата $A=\{3k\mid k\in\mathbf{N}\}$ и $B=\{3^k\mid k\in\mathbf{N}\}$ се еквивалентни.

26. Докажете дека множествата $A=\{3, 6, 9, 12, 15, 18, \ldots\}$ и $B=\{1, 5, 9, 13, 17, 21, \ldots\}$ се еквивалентни.

27. Докажете дека $[0,1) \sim (0,1]$.
28. На колку начини на тројца ученици можат да им се поделат 10 исти тетратки, така што секој од нив да добие барем една тетратка?
29. Колку четирицифрени броеви има, кои се деливи со 5 и во чиј декаден запис нема повторување на цифрите?
30. Во рамнината се дадени 7 точки, така што никои три не се колинеарни. Колку прави се определени со овие точки?
31. На колку начини може да се поделат 8 исти моливи, 9 исти тетратки и 10 исти книги на тројца ученици, така што секој од нив да добие барем по еден предмет од секој вид?
32. Во едно одделение има 30 ученици. На колку начини може да се избере претседател, благајник и секретар на одделенската заедница, под услов еден ученик да нема две задолженија?
33. Колку петцифрени броеви има, кои се запишуваат со помош на пет различни цифри?
34. Во едно одделение има 30 ученици. Секој ученик има оценка пет по географија или по математика. Од нив: 5 ученици имаат пет по математика и по географија; 16 ученици имаат пет по историја и по географија; 20 ученици имаат пет по географија и 25 ученици имаат пет по историја. Колку ученици имаат пет по историја или по географија, а колку ученици имаат пет по математика?
35. Од 100 ученици: 24 не учат ниту еден од јазиците: англиски, руски и германски; 48 учат англиски; 8 и англиски и руски; 26 учат германски; 8 учат и германски и англиски; 13 учат и германски и руски; и 28 учат руски јазик. Колку ученици ги учат сите три јазици?
36. Од 45 студенти во една паралелка, 30 говорат англиски јазик, 23 германски а 13 англиски и германски. Колку студенти не говорат ниту еден од двата јазици?
37. На колку начини тројца Турци, тројца Грци и тројца Бугари може да се наредат во низа така да тројца луѓе со иста националност не стојат во низата последователно?
38. Бројот на елементите спрема бројот на варијациите од класа 3 се однесува како $1:20$. Најди го бројот на елментите!
39. Најди го бројот на елементите, ако бројот на варијациите од четврта класа без повторување е 1680.
40. Реши ја равенката:
    a) $V_n^2 = 72$,
    b) $V_n^2 = 56n$,
    c) $V_n^4 : V_{n-1}^5 = 1:3$.
41. Колку елементи има основното множество, ако бројот на варијациите од четврта класа со повторување е 50625?
42. При потполнување на талонот за спортска прогноза за означување на нерешен резултат, победа на домаќинот и победа на гостинот се користат знаците 0,1 и 2, соодветно. На талонот се наоѓаат 12 натпревари.

a) Колку различно пополнети колони треба да имаме за да со сигурност добиеме 12 погодоци?
b) Колку колони треба да се пополнат, ако се "знае" резултатот на 3 натпревари?
c) Колку колони треба да се пополнат, ако се "знае" дека 7 натпревари ќе завршат нерешено?

43. Колку петцифрени броеви може да се формираат од цифрите 0, 1, 3, 5, 7 и 9 такви, што цифрата 0 да не се наоѓа ниту на првото ниту на последното место и цифрите да не се повторуваат?

44. На колку различни начини можат да седнат 12 лица на маса, околу која се распоредени 12 столици така, што на секоја столица седи по едно лице?

45. Колку пермутации почнуваат со цифрата 5 меѓу сите пермутации кои можат да се формираат од елементите 3, 4, 5 и 6?

46. Во колку пермутации на елементите 1, 2, 3,4 и 5 цифрите 4 и 5 се наоѓаат на првото и последното место?

47. Бројот на пермутациите без повторување од n елементи спрема бројот на пермутациите без повторување од $n+2$ елемента се однесува како $1:30$. Најди го бројот n.

48. Бројот на пермутациите без повторување од $n+2$ елемента е 56 пати поголем од бројот на пермутациите без повторување од n елементи. Најди го бројот n.

49. Во колку пермутации без повторување на елементите 1, 2, 3, 4, 5, 6, 7 и 8, елементите 2,4,5 и 6 стојат еден до друг и тоа:
a) во дадениот редослед,
b) во произволен редослед?

50. Реши ги равенките:
a) $C_n^2 = 15n$,
b) $6C_n^2 = C_n^4$,
c) $30C_n^2 = C_{n+2}^3$.

51. Ако $C_n^8 = C_n^{12}$, пресметај C_n^{17}.

52. Најди ги n и k, ако
$$C_{n+1}^{k+1} : C_{n+1}^{k} : C_{n+1}^{k-1} = 5:5:3.$$

53. Кои класи даваат еднаков број комбинации без повторување од 12 елементи? За секоја класа најди го бројот на комбинациите.

54. На колку начини може да се разместат 9 гости во три хотелски соби: двокреветна, трикреветна и четирикреветна.

55. Колку различни низи од букви може да се направат со разместување на буквите на зборот "*статистика*"? (Низите не мора да имаат значење.)

56. Колку пермутации од елементите a,a,a,a,a,b,b,b,c:
a) почнуваат со буквата a,
b) почнуваат со буквата b,

c) почнуваат со буквата c ?

57. На колку различни начини, без да се користат загради може да се запише a^5b^3 како производ од 8 множители?

58. Најди го бројот на седумцифрените броеви запишани со цифрите 0,0,0,0,0, 1,2,3 не земајќи ги во предвид броевите кои почнуваат со цифрата 0 .

59. На колку начини можат да се изберат четири од следниве дванаесет букви a,a,a,a,b,b,b,b,c,c,c,c ?

60. Колку елементи се потребни за да се добијат 2600 комбинации од трета класа со повторување?

61. Во колку пермутации на броевите 1, 2, 3, 4, 5, 6, 7 и 8 елементите 2, 4, 5 и 6 стојат еден по друг и тоа:
    1) во дадениот редослед
    2) во произволен редослед.

62. Определи го бројот на пермутации на цифрите 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9 во кои цифрите 0, 1, 2, 3 се четири последователни цифри:
    1) во растечки редослед,
    2) во произволен редослед.

63. Определи го бројот на пермутации на елементите на множеството $\{1,2,3,4,5\}$ во кои цифрите 4 и 5 се наоѓаат на прво и последно место.

64. Определи го бројот на петцифрени броеви кои имаат пет различни цифри.

65. Определи го бројот на четирицифрени броеви кои се деливи со 5 и во чиј што декаден запис нема повторување на цифрите.

66. Колку пермутации од елементите 1, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4 :
    a) почнуваат со 22
    b) почнуваат со 313
    c) почнуваат со 1234.

67. На колку начини можеме да избереме две дисјунктни подмножества од дадено множество $S, |S| = n$.

68. Определи го бројот на четирицифрени броеви кај кои секоја цифра
    1) е помала од претходната,
    2) е поголема од претходната

69. На една забава учествувале 10 девојки и 7 момчиња. Ако на еден валцер играат сите момчиња, на колку различни начини може да ги поканат девојките.

70. Определи го бројот на десетоцифрени броеви кај кои сите цифри се меѓу себе различни и меѓу цифрите 2 и 3 стојат точно три цифри.

71. Во простор се дадени $n, n \geq 4$ точки $A_1, A_2, A_3, A_4, ..., A_n$ такви што било кои четири од нив не лежат во една рамнина.
    a) Определи го бројот на рамнини определен со овие точки.
    b) Определи го бројот на триаголни пирамиди определен со овие точки.

72. Секоја n -торка броеви ќе ја нарекуваме вектор. Определи ги сите вектори $x = (x_1, x_2, ..., x_n)$ за кои:
    a) $x_i \in \{0,1,2,3,...,k-1\}$, $i = 1,2,....,n$,

b) $x_i \in \{0,1,2,3,...,k_i-1\}$, $i=1,2,...,n$

c) $x_i \in \{0,1\}$, $i=1,2,3,...,n$ и $x_1+x_2+...+x_n=r$, каде r е природен број.

73. Нека $p_n(k)$ е бројот на пермутации на множеството $S=\{1,2,3,...,n\}$ со точно k неподвижни точки ($k \geq 0$). Докажете дека

$$\sum_{k=1}^{n} k p_n(k) = n!.$$

74. Определи го бројот на пермутации $a_1a_2....a_n$ на множеството $S=\{1,2,3,..., n\}$ за кои што $a_1-a_2>1$.

75. Определи го бројот на пермутации $a_1a_2....a_n$ на множеството $S=\{1,2,3,..., n\}$ такви што $a_i < a_{i+2}$, за $1 \leq i \leq n-2$.

76. Определи го бројот на пермутации $a_1a_2....a_n$ на множеството $S=\{1,2,3,..., n\}$ такви што $a_i < a_{i+3}$, за $1 \leq i \leq n-3$.

77. Правоаголник $1 \times n$ е поделен на единични квадрати. Во квадратите се запишуваат броевите од множеството $S=\{1,2,3,...,n\}$ на начинот кој е опишан. Прво го запишуваме бројот 1 во некој квадрат. Потоа го запишуваме бројот 2 во еден од соседните квадрати на квадратот во кој е запишан бројот 1. Потоа го запишуваме бројот 3 во празен квадрат кој е соседен на квадратите во кои се запишани броевите 1 и 2 итн. Определи го бројот на различни пермутации кои може да се добијат на овој начин.

78. На колку начини можеме да распоредиме n различни писма во m различни поштенски сандачиња?

79. Определи го бројот на комбинациите без повторување од трета класа $\{x_1, x_2, x_3\}$ од елементите $1,2,3,4,...,3n-1,3n$ такви што збирот $x_1+x_2+x_3$ е делив со 3.

80. Докажи дека помеѓу било кои $n+1$ различни помеѓу себе природни броеви $a_1, a_2, ..., a_n, a_{n+1}$ кои не се поголеми од $2n$, постојат два броја такви што едниот е делив со другиот.

81. Определи го бројот на пермутации од елементите 1, 2, 3, 4, 5, 6, 7 и 8 за кои:
   a) Бројот 8 е на прво место а бројот 1 е на последното место.
   b) Бројот 5 е на прво место, бројот 1 е на петто место.
   c) Почетни елементи на пермутацијата се 4 3 2 1.

82. Определи го бројот на парни броеви кои можат да се запишат со цифрите 1, 3, 4, 6 и 7, такви што две соседни цифри да не се еднакви.

83. Определи го максималниот број на триелементни подмножества од множеството $\{1,2,3,4,...,n\}$, такви што било кои два од нив да имаат точно по еден заеднички елемент.

84. Определи го бројот на парни шестцифрени броеви, такви што во нивниот декаден запис сите цифри им се различни.

85. На колку начини може да се изберат три различни броеви од 1 до 30 така што нивниот збир е парен број.

86. Определи го бројот на пермутации $(p_1, p_2, ..., p_n)$ на множеството $\{1, 2, 3, ..., n\}$ за кои збирот
$$|p_1 - 1| + |p_2 - 2| + ... + |p_n - n|$$
има максимална вредност.

87. На една забава биле присутни 15 девојки и 12 момчиња. На колку начини може да се формираат четири пара момче со девојка за да играат танго?

88. Определи го бројот на пермутациите $i_1 i_2 ... i_n j_1 j_2 ... j_n$ на множеството $\{1, 2, 3, 4, ..., 2n-1, 2n\}$ за кои што $i_1 < j_1, i_2 < j_2, ..., i_n < j_n$.

89. На колку начини може да се поклонат 10 различни гердани на 5 девојки, така што секоја од нив да добие по два ѓердани.

90. Докажи дека за бесконечно многу тројки природни броеви (m, k, r) такви што $m! \cdot k! = r!$.

91. Секоја страна на даден квадрат е поделена со точки на n отсечки. Определи го бројот на триаголници чии темиња се делбените точки, ако темињата на квадратот не се делбени точки.

92. Определи го бројот на шестцифрени броеви во кои што парните и непарните цифри се распоредени наизменично (до парна цифра стојат непарни цифри и обратно, до непарни цифри стојат парни цифри.

93. Определи го максималниот број на пермутации на множество $\{1, 2, ..., n\}$, така што било кои два елементи се соседни во најмногу една од пермутациите.

94. Определи го бројот на пермутации на цифрите 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9 во кои што помеѓу цифрите 2 и 3 стојат точно три цифри.

95. Ако $n \geq 2$, најди го бројот на пермутации на множеството $\{1, 2, 3, 4, ..., n\}$ во кои елементите 1 и 2 се соседни.

96. Ако $n \geq k + 2$, најди го бројот на пермутации на множеството $\{1, 2, 3, ..., n\}$ во кои помеѓу единицата и двојката има точно k елементи.

97. Даден е конвексен n-аголник. Определи го бројот на триаголници на кои темињата му се темињата на n-аголникот, а ниту една страна на n-аголникот не е страна на триаголник.

98. Нека $n \geq 2$. Определи го бројот на пермутации на множеството $\{1, 2, 3, ..., n\}$ во кои двојката се наоѓа после единицата.

99. На колку начини шаховска табла 8×8 може да се обои со 8 различни бои, така што во секоја редица се појавува секоја боја и во секоја колона две соседни полиња да не се обоени со иста боја.

100. Определи го бројот на n цифрени броеви $c_1 c_2 c_3 ... c_n$ за кои што
$$1 \leq c_1 \leq c_2 \leq c_3 \leq ... \leq c_n \leq 9 ?$$

101. Провери ја точноста на равенствата:

a) $C_1^1 + C_1^2 + ... + C_1^n = C_1^{n+1}$,

b) $C_2^2 + C_2^3 + ... + C_2^n = C_3^{n+1}$,

c) $C_k^k + C_k^{k+1} + ... + C_k^n = C_{k+1}^{n+1}$, $0 \le k \le n$.

102. Определи го бројот на пермутациите $(a_1, a_2, ..., a_n)$ на множеството $\{1, 2, 3, ..., n\}$ за кои што $a_j \neq j$ за секој $j \in \{1, 2, 3, ..., n\}$.

103. Дадени се две конечни низи броеви со должина n: $a_1, a_2, ..., a_n$; $b_1, b_2, ..., b_n$. Сите $2n$ броеви се различни меѓу себе. На колку различни начини може да се формира низа со должина $2n$ која ги содржи сите членови на двете низи, во кои не е променет редоследот ниту на членовите на првата низа ниту членовите на втората низа.

104. На колку начини може да се одберат три различни природни броеви кои што се помали од 100, такви што нивниот збир е број кој е делив со 3?

105. На колку начини n_1-плави, n_2-жолти и n_3-црвени топчиња може да се распоредат во m различни кутии, ако топчињата не се разликуваат меѓусебно.

106. Определи го бројот на $2n$-варијации на елементите од множеството $\{1, 2, ..., n\}$ такви што секој негов елемент се појавува точно 2 пати и било кои два соседни елементи не се меѓусебно еднакви?

107. На колку начини $n = n_1 + n_2 + ... + n_k$ различни топчиња може да се распоредат во k различни кутии, така што за секое $i \in \{1, 2, 3, ..., k\}$, во i-тата кутија се наоѓаат n_i топчиња.

108. Со поставување на загради во изразот $x_1 : x_2 : ... : x_n$ се добива израз од обликот

$$\frac{x_{i_1} x_{i_2} ... x_{i_k}}{x_{j_1} x_{j_2} ... x_{j_{n-k}}}.$$

Колку различни изрази може да се добијат со поставување на загради?

109. Развиј ги биномите:

a) $(a^{-2} + b^{3/2})^4$;

b) $(x + \frac{1}{x})^5$.

110. Користејќи ја биномната формула, пресметај со точност до петтото децимално место:

a) $0,98^6$;

b) $2,1^6$;

c) $1,005^6$.

111. Најди го седмиот член од развојот на биномот

$$(\tfrac{3}{4}\sqrt[3]{a^2} - \tfrac{2}{\sqrt{a}})^9.$$

112. Најди го тринаесеттиот член во развојот на биномот $(9x-\frac{1}{\sqrt{3x}})^n$, ако биномниот коефициент на неговиот трет член е еднаков на 105.

113. Во развојот на биномот $(\frac{3}{4}\sqrt[3]{a^2}+\frac{2}{3}\sqrt{a})^{12}$ определи го членот кој содржи a^7.

114. Најди го оној член од развојот на биномот $(\sqrt[3]{x^2}+\frac{1}{\sqrt[4]{x^3}})^{17}$ што не го содржи x.

115. Најди го оној член од развојот на биномот $(\sqrt[3]{x^2}+\sqrt{y})^{14}$ што ги содржи x и y на еднаков степен.

116. Во една банкарска експозитура треба да стигнат n особи. На колку можни начини, според времето на доаѓање, можат да стигнат во експозитурата?

117. Одредете ги изразите кои се дуални на следниве изрази:
   1) $xy'+xz'+yx'$
   2) $xyz'+xy'z$
   3) $xy(x+0+z1)$
   4) $(x+y')(z'+y)'$
   5) $(1+x)y+xy'z$
   6) $(xy+1)(0+x)z$.

118. Опишете ја Буловата алгебра со два елементи: 0 и 1.

119. Нека B_n го означува множеството од сите низи со должина n, кои се состојат од 0 и 1. На пример, 10010101 е елемент на множеството B_8. За константно n, најдете операции ·, + и ' над B_n, така да множеството B_n е Булова алгебра.

120. Нека множеството B се состои од сите делители на 30. За броевите $a,b\in B$ нека $ab=\mathrm{NZD}(a,b)$ и $a+b=\mathrm{NZS}(a,b)$. Докажете дека множеството B, заедно со вака дефинираните операции, претставува Булова алгебра. Што е нула, а што единица? Што е комплемент за бројот a?

121. Нека B е Булова алгебра и $x,y,z\in B$. Докажете дека од $xy=xz$ и $x'y=x'z$ следува $y=z$.

122. Формулирајте дуалното тврдење на тврдењето од претходната задача.

123. Нека B е Булова алгебра и $x,y\in B$. Докажете дека $xy'=0$ ако и само ако $xy=x$.

124. Формулирајте го дуалното тврдење на тврдењето од претходната задача.

125. Нека $S=\{a+bi\mid a,b\in\mathbf{Z}\}$, каде $i^2=-1$. Докажете дека множеството S е пребројливо.

126. Докажете дека множеството од сите полиноми со целобројни коефициенти од петта степен е пребројливо.

127. Докажете дека множеството од сите полиноми со целобројни коефициенти и степен помал или еднаков на n е пребројливо.

128. Користејќи ја теорема 12.17 В, докажете дека не постои биекција меѓу множеството $\{1, 2, 3, ..., n\}$ и произволно негово подмножество.

129. Користејќи го резултатот од претходниот проблем, докажете дека множеството S е бесконечно ако и само ако постои биекција меѓу S и некое негово вистинско подмножество.

V ГЛАВА
БИНАРНИ РЕЛАЦИИ

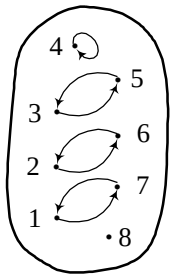
1. ПОИМ ЗА БИНАРНА РЕЛАЦИЈА

1.1. При изучувањето на множествата го разгледавме поимот подмножество и притоа видовме дека $A \subseteq B$ ако и само ако од $x \in A$ следува $x \in B$. Последното значи дека за произволни множества X и Y не мора да важи $X \subseteq Y$ или $Y \subseteq X$. Аналогно, при изучувањето на деливоста на природните броеви видовме дека за секои природни броеви a и b не мора да важи $a \mid b$ или $b \mid a$. Претходните два примери на прв поглед немаат ништо заедничко. Меѓутоа, тоа е само на прв поглед, бидејќи овие два примери имаат некои заеднички карактеристики со кои ќе се запознаеме при изучувањето на таканаречените бинарни релации.

1.2. Дефиниција. Ако M е непразно множество, тогаш секое подмножество α од $M \times M$ го нарекуваме *бинарна релација* во M. Притоа наместо $(x, y) \in \alpha$ честопати ќе пишуваме $x \alpha y$ и ќе читаме "x е во релација α со y". Ако $(x, y) \notin \alpha$, т.е. ако x не е во релација α со y, ќе пишуваме $x \not\alpha y$. Множеството од сите $x \in M$ такви што $(x, y) \in \alpha$ за некој $y \in M$ го нарекуваме *домен* на релацијата α. Множеството од сите $y \in M$ такви што $(x, y) \in \alpha$ за некој $x \in M$ го нарекуваме *кодомен* на релацијата α.

Да забележиме дека ако $x \alpha y$, тогаш тоа графички се прикажува така што x и y се поврзуваат со стрелка која е насочена од x кон y (види го цртежот во примерот 1.3).

1.3. Пример. а) Да го разгледаме множеството $M = \{1, 2, 3, 4, 5, 6, 7, 8\}$ и во него да дефинираме бинарна релација α на следниов начин: $x \alpha y$ ако и само ако $x + y = 8$.



Значи, ако $x \alpha y$, тогаш $x + y = 8$, па затоа $x + y = 8$, од што следува дека $y \alpha x$. Понатаму, од претходно изнесеното и од

$$1+7 = 2+6 = 3+5 = 4+4 = 8$$

следува дека

$$\alpha = \{(1,7), (2,6), (3,5), (4,4), (5,3), (6,2), (7,1)\}.$$

Да забележиме дека $1 \not\alpha 6,\ 7 \not\alpha 2, \ldots,\ 8 \not\alpha x,$ за $x = 1, 2, \ldots, 8$ бидејќи

$$1+6 \neq 8,\ 7+2 \neq 8, \ldots, 8+x \neq 8, \text{ за } x = 1, 2, \ldots, 8.$$

Графичкиот приказ на релацијата α е даден на цртежот горе десно.

б) Дадено е множеството A чии елементи се имињата на една група ученици:

$$A = \{\text{Ana, Eva, Adam, Marko, Obren, Ivana, Nikola, Meri}\}.$$

Во ова множество е дефинирана релацијата α на следниов начин:

$x \alpha y$ ако и само ако почетната буква на
името на x е крајна буква на името на y,

за секои $x, y \in A$. Од условот имаме дека дадената релација е:

$$\alpha = \{(\text{Ana, Ana}), (\text{Ana, Eva}), (\text{Ana, Ivana}), (\text{Ana, Nikola}), (\text{Adam, Ana}),$$
$$(\text{Adam, Eva}), (\text{Adam, Ivana}), (\text{Adam, Nikola}), (\text{Marko, Adam}),$$
$$(\text{Meri, Adam}), (\text{Obren, Marko}), (\text{Ivana, Meri}), (\text{Nikola, Obren})\}.$$

в) За секое непразно множество M релациите

$$\Delta_M = \{(x, x) \mid x \in M\} \text{ и } \alpha = M \times M$$

ги нарекуваме *дијагонална* и *универзална релација* во M, соодветно. ♦

1.4. Дефиниција. Нека α е релација на непразното множество M. За релацијата α^{-1} на множеството M определена со

$$\alpha^{-1} = \{(y, x) \mid (x, y) \in \alpha\}$$

ќе велиме дека е *инверзна* на релацијата α.

1.5. Пример. Нека на множеството $M = \{1, 3, r, s\}$ е дадена релацијата $\alpha = \{(1, r), (1, s), (3, s)\}$. Тогаш инверзната релација е

$$\alpha^{-1} = \{(r, 1), (s, 1), (s, 3)\}. \blacklozenge$$

1.6. Дефиниција. Нека α и β се релации на непразното множество M. *Композиција на релациите* α и β ја нарекуваме релација

$$\gamma = \{(x, z) \mid \text{postoi } y \in M \text{ takov } \{\text{to } (x, y) \in \alpha \text{ i } (y, z) \in \beta\}.$$

Притоа ја користиме ознаката $\gamma = \beta \circ \alpha$.

1.7. Пример. Нека α и β се релации во множеството природни броеви $\mathbf{N}$ определени со

$$\alpha = \{(x, x+2) \mid x \in \mathbf{N}\} \text{ и } \beta = \{(x, x^2) \mid x \in \mathbf{N}\}.$$

Тогаш $\alpha \circ \beta = \{(x, x^2 + 2) \mid x \in \mathbf{N}\}$ и $\beta \circ \alpha = \{(x, (x+2)^2) \mid x \in \mathbf{N}\}$, што значи дека за композицијата на релации не важи комутативниот закон. ♦

1.8. Теорема. Нека M е непразно множество и α, β и γ се релации во M. Тогаш $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$, т.е. за композицијата на релации важи асоцијативниот закон.

Доказ. Нека $(a, d) \in \gamma \circ (\beta \circ \alpha)$. Тоа значи дека постои $c \in M$ таков што $(a, c) \in \beta \circ \alpha$ и $(c, d) \in \gamma$. Од $(a, c) \in \beta \circ \alpha$ следува дека постои $b \in M$ таков што

$(a,b)\in\alpha$ и $(b,c)\in\beta$. Според тоа, $(b,c)\in\beta$ и $(c,d)\in\gamma$, па затоа $(b,d)\in\gamma\circ\beta$ и како $(a,b)\in\alpha$ добиваме дека $(a,d)\in(\gamma\circ\beta)\circ\alpha$. Значи

$$\gamma\circ(\beta\circ\alpha)\subseteq(\gamma\circ\beta)\circ\alpha\,.$$

Аналогно се докажува дека

$$(\gamma\circ\beta)\circ\alpha\subseteq\gamma\circ(\beta\circ\alpha)\,.$$

Конечно, од последните две инклузии следува

$$(\gamma\circ\beta)\circ\alpha=\gamma\circ(\beta\circ\alpha)\,.\ \blacklozenge$$

2. РЕФЛЕКСИВНА, СИМЕТРИЧНА, ТРАНЗИТИВНА И АНТИСИМЕТРИЧНА РЕЛАЦИЈА

2.1. Дефиниција. За бинарната релацијата α определена на непразното множество M ќе велиме дека е *рефлексивна* ако $x\alpha x$, за секој $x\in M$.

2.2. Пример. а) Од $(x,x)\in\Delta_M$, за секој $x\in M$ непосредно следува дека дијагоналата на секое непразно множество е рефлексивна релација.

б) Дадено е множеството $M=\{1,2\}$ и релацијата $\alpha=\{(1,1),(1,2),(2,2)\}$. Бидејќи $(1,1)\in\alpha$ и $(2,2)\in\alpha$, заклучуваме дека $x\alpha x$ за секој $x\in M$, т.е. релацијата α е рефлексивна.

в) Во множеството природни броеви $\mathbf{N}$ да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x=y$. Јасно, $x=x$ за секој $x\in\mathbf{N}$, што значи дека оваа релација е рефлексивна.

г) Во множеството природни броеви $\mathbf{N}$ да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x<y$. Бидејќи $x\not<x$ за секој $x\in\mathbf{N}$ заклучуваме дека оваа релација не е рефлексивна.

Меѓутоа, ако земеме $x\alpha y$ ако и само ако $x\le x$, тогаш релацијата е рефлексивна.

д) Нека n е фиксиран природен број. Во множеството природни броеви $\mathbf{N}$ да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x\equiv y\,(\mathrm{mod}\,n)$. Од својствата на конгруенциите имаме $x\equiv x\,(\mathrm{mod}\,n)$ за секој $x\in\mathbf{N}$, што значи дека оваа релација е рефлексивна.

ѓ) Во множеството природни броеви $\mathbf{N}$ да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x\mid y$. Од својствата на деливоста имаме $x\mid x$ за секој $x\in\mathbf{N}$, што значи дека оваа релација е рефлексивна. $\blacklozenge$

2.3. Забелешка. Од дефиницијата на рефлексивноста лесно се гледа дека една релација определена на непразно множество M е рефлексивна ако и само ако ја содржи дијагоналата Δ_M.

2.4. Дефиниција. За бинарната релацијата α определена на непразното множество M ќе велиме дека е *симетрична* ако од $x\alpha y$ следува $y\alpha x$.

2.5. Пример. а) Дадено е множеството $M=\{1,2\}$ и релацијата $\alpha=\{(1,1),(1,2),(2,1)\}$. Од $(1,1)\in\alpha$, $(2,1)\in\alpha$ и $(1,2)\in\alpha$ заклучуваме дека релацијата α е симетрична.

б) Нека $x,y\in\mathbf{N}$. Ако $x=y$, тогаш $y=x$. Според тоа, релацијата од примерот 2.2 в) е симетрична.

в) Бидејќи $2<4$ и $2\le 4$, но $4\not<2$ и $4\not\le 2$ заклучуваме дека релациите од примерот 2.2 г) не се симетрични.

г) Нека $x\equiv y\pmod n$. Тогаш, $y\equiv x\pmod n$ што значи дека релацијата од примерот 2.2 д) е симетрична.

д) Бидејќи $2\mid 4$, но $4\nmid 2$ заклучуваме дека релацијата од примерот 2.2 ѓ) не е симетрична. ♦

2.6. Дефиниција. За бинарната релацијата α определена на непразното множество M ќе велиме дека е *транзитивна* ако од $x\alpha y$ и $y\alpha z$ следува $x\alpha z$.

2.7. Пример. а) Дадено е множеството $M=\{1,2\}$ и релацијата

$$\alpha=\{(1,1),(1,2),(2,1)\}.$$

Оваа релација не е транзитивна бидејќи $2\alpha 1$ и $1\alpha 2$, но 2 не е во релација α со 2.

б) Нека $x,y,z\in\mathbf{N}$. Ако $x=y$ и $y=z$, тогаш $x=z$. Според тоа, релацијата од примерот 2.2 в) е транзитивна.

в) Нека $x,y,z\in\mathbf{N}$. Од $x<y$ и $y<z$ следува дека $x<z$, што значи дека првата релација во примерот 2.2 г) е транзитивна. Аналогно се докажува дека и втората релација од истиот пример е транзитивна.

г) Нека $x\equiv y\pmod n$ и $y\equiv z\pmod n$. Тогаш, $x\equiv z\pmod n$ што значи дека релацијата од примерот 2.2 д) е транзитивна.

д) Бидејќи од $x\mid y$ и $y\mid z$ следува $x\mid z$ за секои $x,y,z\in\mathbf{N}$, заклучуваме дека релацијата од примерот 2.2 ѓ) е транзитивна. ♦

2.8. Дефиниција. За бинарната релацијата α определена на непразното множество M ќе велиме дека е *антисиметрична* ако од $x\alpha y$ и $y\alpha x$ следува $x=y$.

2.9. Пример. а) Дадено е множеството $M=\{1,2\}$ и релацијата

$$\alpha=\{(1,1),(1,2),(2,1)\}.$$

Оваа релација не е антисиметрична бидејќи $2\alpha 1$ и $1\alpha 2$, но $2\neq 1$.

б) Нека $x,y\in\mathbf{N}$. Од $x\le y$ и $y\le x$ следува дека $x=y$, што значи дека втората релација во примерот 2.2 г) е антисиметрична.

в) Нека $x, y \in \mathbf{N}$. Порано докажавме дека од $x \mid y$ и $y \mid x$ следува $x = y$, што значи дека релацијата од примерот 2.2 ѓ) е антисиметрична. ♦

2.10. Дефиниција. Нека α е релација во множеството M. Најмалата рефлексивна релација во множеството M која ја содржи, како подмножество, релацијата α ја нарекуваме *рефлексивно затворање* на α. Најмалата симетрична релација во множеството M која ја содржи, како подмножество, релацијата α ја нарекуваме *симетрично затворање* на α. Најмалата транзитивна релација во множеството M која ја содржи, како подмножество, релацијата α ја нарекуваме *транзитивно затворање* на α.

2.11. Теорема. Нека α е релација во множеството M. Тогаш

a) рефлексивното затворање на релацијата α е релацијата $\alpha \cup \Delta_M$,

b) симетричното затворање на релацијата α е релацијата $\alpha \cup \alpha^{-1}$ и

c) ако M е конечно множество кое содржи n елементи, тогаш транзитивното затворање на релацијата α е релацијата $\alpha \cup \alpha^2 \cup ... \cup \alpha^n$, каде $\alpha^2 = \alpha \circ \alpha, ..., \alpha^{k+1} = \alpha \circ \alpha^k$.

Доказ. c) Нека $\overline{\alpha}$ е транзитивното затворање на релацијата α. Со индукција ќе докажеме дека $\alpha \cup \alpha^2 \cup \alpha^3 \cup ... \cup \alpha^n \subseteq \overline{\alpha}$.

За $k = 1$ имаме $\alpha \subseteq \overline{\alpha}$, што е очигледно точно.

Нека претпоставиме дека за $k < n$ важи $\alpha \cup \alpha^2 \cup ... \cup \alpha^k \subseteq \overline{\alpha}$. Треба да докажеме дека $\alpha \cup \alpha^2 \cup ... \cup \alpha^{k+1} \subseteq \overline{\alpha}$, што согласно со индуктивната претпоставка значи да докажеме дека $\alpha^{k+1} \subseteq \overline{\alpha}$. Нека $(a,c) \in \alpha^{k+1}$. Тогаш постои $b \in M$ таков што $(a,b) \in \alpha$ и $(b,c) \in \alpha^k$ и како $\alpha, \alpha^k \subseteq \overline{\alpha}$ добиваме дека $(a,b), (b,c) \in \overline{\alpha}$. Но, релацијата $\overline{\alpha}$ е тразитивна, па затоа $(a,c) \in \overline{\alpha}$, т.е. $\alpha^{k+1} \subseteq \overline{\alpha}$, односно $\alpha \cup \alpha^2 \cup ... \cup \alpha^{k+1} \subseteq \overline{\alpha}$.

За да докажеме дека $\overline{\alpha} \subseteq \alpha \cup \alpha^2 \cup ... \cup \alpha^n$, согласно со минималноста на релацијата $\overline{\alpha}$ доволно е да докажеме дека $\alpha \cup \alpha^2 \cup ... \cup \alpha^n$ е транзитивна релација. Нека $(a,b), (b,c) \in \alpha \cup \alpha^2 \cup ... \cup \alpha^n$. Тогаш, постојат $i, k \in \{1, 2, ..., n\}$ такви што $(a,b) \in \alpha^i$ и $(b,c) \in \alpha^k$. Но, тоа значи дека $(a,c) \in \alpha^{i+k}$. Ако $a = b$ или $b = c$, тогаш елементот (a,c) е еднаков на (b,c) или (a,b), па затоа припаѓа на $\alpha \cup \alpha^2 \cup ... \cup \alpha^n$. Во спротивно, од дефиницијата на композиција на релации следува дека постојат $b_2, b_3, ..., b_{i+k-1} \in M$ такви што

$$(a,b_2), (b_2,b_3), ..., (b_{i+k-2}, b_{i+k-1}), (b_{i+k-1}, c) \in \alpha .$$

Да ставиме $b_1 = a$ и $b_{i+k} = c$. Ако кои било од елементите b_t се меѓусебно еднакви, на пример $b_p = b_q$, тогаш од горната низа можеме да ги отстраниме паровите

$$(b_p, b_{p+1}), (b_{p+1}, b_{p+2}), ..., (b_{q-1}, b_q)$$

и да ги оставиме елементите

$$a = b_1, b_2, ..., b_{p-1}, ..., b_q, ..., b_{i+k-1}, b_{i+k} = c \in M \ ,$$

при што секој елемент во низата е во релација α со следниот елемент. Постапката ја повторуваме се додека сите елементи во низата не се меѓусебно различни и секој елемент е во релација со следниот. Бидејќи множеството M има n различни елементи, добиваме дека $(a,c) \in \alpha^m$, за некој $m \le n$, што значи дека релацијата $\alpha \cup \alpha^2 \cup ... \cup \alpha^n$ е транзитивна. ♦

3. РЕЛАЦИЈА НА ЕКВИВАЛЕНЦИЈА

3.1. Дефиниција. За релацијата α ќе велиме дека е *релација на еквиваленција* (*еквивалентност*) ако таа е рефлексивна, симетрична и транзитивна.

Симболот ~ (читај: *тилда*) најчесто се користи како симбол за означување на еквивалентностите.

3.2. Пример. а) Дадено е множеството $M = \{1, 2\}$ и релацијата $\alpha = \{(1,1), (1,2), (2,1)\}$. Бидејќи $(2,2) \notin \alpha$, заклучуваме дека оваа релација не е рефлексивна, па затоа не е ниту релација на еквиваленција.

б) Во множеството природни броеви **N** да ја разгледаме релацијата α определена со $x \alpha y$ ако и само ако $x = y$. Од примерите 2.2 в), 2.5 б) и 2.7 б) следува дека оваа релација е релација на еквиваленција.

в) Во множеството природни броеви **N** да ја разгледаме релацијата α определена со $x \alpha y$ ако и само ако $x < y$. Според примерот 2.5 в) оваа релација не е симетрична, па затоа таа не е релација на еквиваленција.

Повторно од примерот 2.5 в) следува дека релацијата $x \alpha y$ ако и само ако $x \le y$, не е симетрична, што значи дека таа не е релација на еквиваленција.

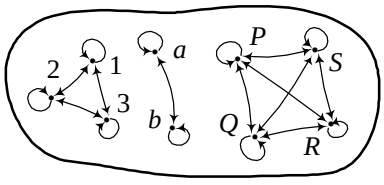
г) Нека n е фиксиран природен број. Во множеството природни броеви **N** да ја разгледаме релацијата α определена со $x \alpha y$ ако и само ако $x \equiv y \pmod{n}$. Од примерите 2.2 д), 2.5 г) и 2.7 г) следува дека оваа релација е релација на еквиваленција.

д) Во множеството природни броеви **N** да ја разгледаме релацијата α определена со $x \alpha y$ ако и само ако $x \mid y$. Во примерот 2.5 д) докажавме дека оваа релација не е симетрична, па затоа не е релација на еквиваленција. ♦

3.3. Да го разгледаме множеството

$$A = \{1, 2, 3, a, b, P, Q, R, S\}$$

и бинарната релација ~ прикажана со наведениот граф лево. Лесно се проверува дека оваа

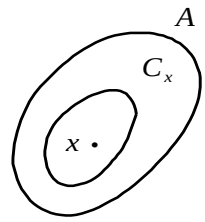


релација е рефлексивна, симетрична и транзитивна, односно дека е релација на еквиваленција. На цртежот забележуваме дека елементите на множеството A со оваа релација се распределени во три класи. Едната класа ја сочинуваат елементите $1,2,3$; втората класа елементите a,b; третата класа елементите P,Q,R,S. Како што можеме да забележиме, кои било два елементи од една класа се во релација меѓу себе, при што велиме дека се еквивалентни.

Во каков однос се елементите од различните класи, да кажеме 1 и a, a и Q? Очигледно $1 \not\sim a$, $Q \not\sim a$ и воопшто, кој било елемент од една класа не е во релација ~ со кој било елемент од друга класа, односно елементите од различните класи не се еквивалентни.

Претходно кажаното важи за која било релација на еквиваленција. Имено, како што понатаму ќе докажеме, на секоја релација на еквиваленција и соодветствува поделба на елементите на класи, кои ги нарекуваме класи на еквиваленција. Така ја имаме следната дефиниција.

3.4. Дефиниција. Нека A е непразно множество и ~ е релација на еквиваленција во A. Ако $x \in A$, тогаш множеството елементи од A кои се еквивалентни со x го нарекуваме *класа на еквиваленција на елементот* x и го означуваме со C_x (цртеж десно). Според тоа,



$$C_x = \{y \mid y \sim x \text{ i } y \in A\}. \qquad (1)$$

За претходно дадената релација на еквиваленција имаме

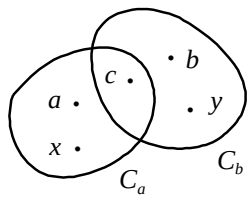
$$C_1 = C_2 = C_3 = \{1,2,3\}, \quad C_a = C_b = \{a,b\}, \quad C_P = C_Q = C_R = C_S = \{P,Q,R,S\}.$$

3.5. Нека C_x е класата на еквиваленција на елементот x и нека $y,z \in C_x$. Од дефиницијата на класата на еквиваленција имаме $y \sim x$ и $z \sim x$. Но, ~ е симетрична па затоа од $z \sim x$ следува $x \sim z$. Според тоа, $y \sim x$ и $x \sim z$ и бидејќи ~ е транзитивна, добиваме $y \sim z$.

Со тоа ја докажавме следнава теорема.

Теорема. Ако A е непразно множество и ~ е релација на еквиваленција во A, тогаш кои било два елементи од една класа на еквиваленција се еквивалентни меѓу себе. ♦

3.6. Нека сега C_a и C_b се две произволни класи на еквиваленција (цртеж десно). Јасно, тие имаат или барем еден заеднички елемент или се дисјунктни, т.е. $C_a \cap C_b \neq \varnothing$ или $C_a \cap C_b = \varnothing$.



Нека $C_a \cap C_b \neq \varnothing$ и нека c е еден од заедничките елементи, т.е. $c \in C_a$ и $c \in C_b$, што значи $c \sim a$ и $c \sim b$. Нека $x \in C_a$. Но, $c \in C_a$ па од теоремата 3.5 сле-

дува дека $x \sim c$. Понатаму, $c \sim b$ и бидејќи ~ е релација на еквиваленција добиваме дека $x \sim b$, што значи $x \in C_b$. Според тоа, од $x \in C_a$ следува $x \in C_b$, па затоа $C_a \subseteq C_b$. Аналогно се докажува дека $C_b \subseteq C_a$. Конечно, од $C_a \subseteq C_b$ и $C_b \subseteq C_a$ следува $C_b = C_a$.

Со тоа ја докажавме следнава теорема.

Теорема. Нека A е непразно множество и ~ е релација на еквиваленција во A. Ако две класи на еквиваленција имаат барем еден заеднички елемент, тогаш тие се еднакви. ♦

3.7. Коментар. Од претходно изнесеното следува дека кои било две класи на еквиваленција C_a и C_b или се еднакви или немаат заеднички елементи, т.е. или $C_a = C_b$ или $C_a \cap C_b = \varnothing$.

Заради последното својство на класите на еквиваленција, множеството A со класите на еквиваленција е поделено на меѓусебно дисјунктни множества. Од овие множества формираме ново множество и го добиваме таканаречената *фактор-множество*, кое обично го означуваме со $A_{/\sim}$. Според тоа, $A_{/\sim}$ е множеството од сите класи на еквиваленција.

Во последниот пример класите на еквиваленција се: $\{1,2,3\}, \{a,b\}$ и $\{P,Q,R,S\}$. Според тоа, фактор-множеството е дадено со

$$A_{/\sim} = \{\{1,2,3\}, \{a,b\}, \{P,Q,R,S\}\}.$$

3.8. Пример. а) Според примерот 3.2 б) во множеството природни броеви $\mathbf{N}$ релацијата α определена со $x \alpha y$ ако и само ако $x = y$ е релација на еквиваленција. Лесно се гледа дека за секој $x \in \mathbf{N}$ важи $C_x = \{x\}$, т.е. оваа релација има бесконечно многу класи на еквиваленција.

б) Според примерот 3.2 г) во множеството природни броеви $\mathbf{N}$ релацијата α определена со $x \alpha y$ ако и само ако $x \equiv y \pmod 3$ е релација на еквиваленција. Како што знаеме $x \equiv y \pmod 3$ ако и само ако x и y при делење со 3 даваат исти остатоци. Според тоа, класите на еквиваленција се

$$\{3k+1 \mid k \in \mathbf{N}_0\}, \quad \{3k+2 \mid k \in \mathbf{N}_0\}, \quad \{3k+3 \mid k \in \mathbf{N}_0\}$$

што значи фактор-множеството е

$$\mathbf{N}_{/\alpha} = \{\{3k+1 \mid k \in \mathbf{N}_0\}, \{3k+2 \mid k \in \mathbf{N}_0\}, \{3k+3 \mid k \in \mathbf{N}_0\}\}. \blacklozenge$$

4. РЕЛАЦИЈА ЗА ПОДРЕДУВАЊЕ

4.1. Дефиниција. Нека A е непразно множество. За релацијата α ќе велиме дека е *релација на подредување (подредување)* на A ако таа е рефлексивна, антисиметрична и транзитивна.

Нека α е релација на подредување на A. Ако за елементите $x, y \in A$ важи $x\alpha y$ или $y\alpha x$, тогаш ќе велиме дека тие се *споредливи*.

Ако секои два елементи на A се споредливи, ќе велиме дека релацијата α е *потполно подредување* во A и дека множеството A е *потполно подредено множество*, а во спротивно ќе велиме дека релацијата α е релација на *делумно подредување* и множеството A е *делумно подредено множество*.

4.2. Пример. а) Во множеството природни броеви **N** да ја разгледаме релацијата α определена $x\alpha y$ ако и само ако $x \le y$. Во примерите 2.2 г), 2.7 в) и 2.9 б) докажавме дека оваа релација е рефлексивна, транзитивна и антисиметрична, што значи таа е релација на подредување. Јасно, вака дефинираната релација на подредување е потполно подредување во **N**, што значи дека **N** е потполно подредено множество.

б) Во множеството природни броеви **N** да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x \mid y$. Во примерите 2.2 ѓ), 2.7 д) и 2.9 в) докажавме дека оваа релација е рефлексивна, транзитивна и антисиметрична, па затоа таа е релација на подредување. Јасно, со оваа релација множеството **N** не е потполно подредено бидејќи, на пример, ниту $2 \mid 3$ ниту $3 \mid 2$, односно во ова множество постојат елементи кои не се споредливи со оваа релација.

в) Во множеството цели броеви **Z** да ја разгледаме релацијата α определена со $x\alpha y$ ако и само ако $x \mid y$. Како и кај природните броеви се докажува дека оваа релација е рефлексивна и транзитивна. Меѓутоа, таа не е антисиметрична, бидејќи, на пример, $2 \mid (-2)$ и $(-2) \mid 2$, но $2 \ne -2$. Според тоа, релацијата "x е делител на y" не е релација за подредување. ♦

4.3. Теорема. Ако α е подредување на множеството M и ако релацијата α_1 е определена со

$$x\alpha_1 y \text{ ако и само ако } x\alpha y \text{ и } x \ne y \qquad (1)$$

тогаш α_1 не е рефлексивна и е транзитивна релација во M.

Доказ. Од (1) следува дека релацијата α_1 не е рефлексивна. Нека $x\alpha_1 y$ и $y\alpha_1 z$. Од (1) добиваме $x\alpha y$, $x \ne y$, $y\alpha z$, $y \ne z$. Од транзитивноста на α следува дека $x\alpha z$ и притоа не може да биде $x = z$, бидејќи тогаш од $x\alpha y$ и $y\alpha x$ ќе следува $x = y$. Значи, $x\alpha_1 z$, т.е. релацијата α_1 е транзитивна. ♦

4.4. Во натамошните разгледувања за релација на подредување наместо ознаката $x\alpha y$ обично ќе ја користиме ознаката $x \le y$. Според тоа, имаме

i) $x \le x$, за секој $x \in M$,

ii) ако $x \le y$ и $y \le x$, тогаш $x = y$ и

iii) ако $x \le y$ и $y \le z$, тогаш $x \le z$.

Соодветната релација α_1 дефинирана со (2) ќе ја означуваме се $<$, т.е.

$$x < y \text{ ако и само ако } x \le y \text{ и } x \ne y. \tag{2}$$

4.5. Во натамошните разгледувања под подредување ќе подразбираме потполно подредување, и во таа смисла за едно множество M ќе велиме дека е подредено ако соодветното подредување е потполно. Така, важи следново тврдење.

Теорема. Ако M е подредено множество и ако $x, y \in M$, тогаш еден и само еден од следните три услови е исполнет

$$x < y,\ x = y,\ y < x. \blacklozenge \tag{3}$$

4.6. На крајот од овој дел, во врска со подредените множества, ќе воведеме уште два поими.

Дефиниција. Нека M е подредено множество и A е непразно подмножество од M. За елементот $a \in A$ ќе велиме дека е *најмал елемент* на A ако $a \le x$, за секој $x \in A$.

За множеството M ќе велиме дека е *добро подредено* ако секое непразно множество има најмал елемент.

Дефиниција. Нека M е подредено множество и A е непразно подмножество од M. За елементот $a \in A$ ќе велиме дека е *најголем елемент* на A ако $x \le a$, за секој $x \in A$.

ЗАДАЧИ

1. Дадено е множеството $M = \{-2, -1, 0, 1, 2, 3\}$ и во него е дефинирана релација α на следниов начин: $x \alpha y$ ако и само ако $x^2 = y^2$, за $x, y \in M$.
   a) Запиши ја релацијата α како множество од подредени парови.
   b) Прикажи ја графички релацијата α.
2. Дадено е множеството $M = \{-3, -2, -1, 0, 1, 2, 3, 4\}$ и во него е дефинирана релација α на следниов начин: $x \alpha y$ ако и само ако $x - y = -1$ за $x, y \in M$.
   a) Запиши ја релацијата α како множество од подредени парови.
   b) Прикажи ја графички релацијата α.
3. Нека е дадено множеството $A = \{a, b, c, d, e\}$ и во него релациите

   $\alpha = \{(a,a),(a,b),(b,c),(b,d),(c,e),(e,d),(c,a)\}$,

   $\beta = \{(a,b),(b,a),(b,c),(b,d),(e,e),(d,e),(c,b)\}$,

   $\gamma = \{(a,b),(a,a),(b,c),(b,b),(e,e),(b,a),(c,b),(c,c),(d,d),(a,c),(c,a)\}$ и

   $\delta = \{(a,b),(b,c),(b,b),(e,e),(b,a),(c,b),(d,d),(a,c),(c,a)\}$.
   a) Кои од овие релации се симетрични?
   b) Кои од овие релации се рефлексивни?

c) Кои од овие релации се транзитивни?
d) Кои од овие релации се антисиметрични?
e) Опишете ги релациите $\gamma \cap \delta$, $\alpha \cup \beta$, $\gamma \setminus \delta$ и $\gamma \Delta \alpha$.

4. Докажете дека пресек на рефлексивни релации е рефлексивна релација.
5. Докажете дека пресек на симетрични релации е симетрична релација.
6. Нека е дадено множеството $A = \{a, b, c, d, e\}$.
   1) Најдете релација на множеството A која е рефлексивна, но не е ниту симетрична, ниту транзитивна.
   2) Најдете релација на множеството A која е симетрична, но не е ниту рефлесивна, ниту транзитивна.
   3) Најдете релација на множеството A која е транзитивна, но не е ниту рефлексивна, ниту симетрична.
   4) Најдете релација на множеството A која е рефлексивна и симетрична, но не е транзитивна.
   5) Најдете релација на множеството A која е симетрична и транзитивна, но не е рефлексивна.
   6) Најдете релација на множеството A која е рефлексивна и транзитивна, но не е симетрична.
7. Во множеството природни броеви **N** релацијата α е дефинирана на следниов начин: $x \alpha y$ ако и само ако $3 \mid x$ и $3 \mid y$. Докажи дека оваа релација е симетрична и транзитивна.
8. Нека A е множеството прави во рамнината. Испитај ги својствата на релацијата α во множеството A дефинирана со:
   a) $a \alpha b$ ако и само ако $a \parallel b$;
   b) $a \alpha b$ ако и само ако $a \perp b$.
9. Дадено е множеството $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ и во него релациите:
   a) α_1 определена со $x \alpha_1 y$ ако и само ако $x + y = 10$;
   b) α_2 определена со $x \alpha_2 y$ ако и само ако $x + y$ е парен број;
   c) α_3 определена со $x \alpha_3 y$ ако и само ако $x \cdot y$ е парен број.

   Испитај ги својствата на секоја од овие релации.
10. Определете дали следниве искази се вистинити или не се вистинити. За секој исказ кој е невистинит дадете контрапример.
    a) Ако релациите α и β се симетрични, тогаш и релацијата $\alpha \cap \beta$ е симетрична.
    b) Ако релациите α и β се симетрични, тогаш и релацијата $\alpha \cup \beta$ е симетрична.
    c) Ако релациите α и β се симетрични, тогаш и релацијата $\alpha \circ \beta$ е симетрична.
    d) Ако релациите α и β се симетрични, тогаш и релацијата $\alpha \setminus \beta$ е симетрична.
    e) Ако релациите α и β се симетрични, тогаш и релацијата $\alpha \dot{-} \beta$ е симетрична.

11. Определете дали следниве искази се вистинити или не се вистинити. За секој исказ кој е невистинит дадете контрапример.
    a) Ако релациите α и β се антисиметрични, тогаш и релацијата $\alpha \cap \beta$ е антисиметрична.
    b) Ако релациите α и β се антисиметрични, тогаш и релацијата $\alpha \cup \beta$ е антисиметрична.
    c) Ако релациите α и β се антисиметрични, тогаш и релацијата $\alpha \circ \beta$ е антисиметрична.
    d) Ако релациите α и β се антисиметрични, тогаш и релацијата $\alpha \setminus \beta$ е симетрична.
    e) Ако релациите α и β се антисиметрични, тогаш и релацијата $\alpha \dot{-} \beta$ е антисиметрична.
12. Определете дали следниве искази се вистинити или не се вистинити. За секој исказ кој е невистинит дадете контрапример.
    a) Ако релациите α и β се рефлексивни, тогаш и релацијата $\alpha \cap \beta$ е рефлексивни.
    b) Ако релациите α и β се рефлексивни, тогаш и релацијата $\alpha \cup \beta$ е рефлексивни.
    c) Ако релациите α и β се рефлексивни, тогаш и релацијата $\alpha \circ \beta$ е рефлексивни.
    d) Ако релациите α и β се рефлексивни, тогаш и релацијата $\alpha \setminus \beta$ е рефлексивни.
    e) Ако релациите α и β се рефлексивни, тогаш и релацијата $\alpha \dot{-} \beta$ е рефлексивни.
13. Определете дали следниве искази се вистинити или не се вистинити. За секој исказ кој е невистинит дадете контрапример.
    a) Ако релациите α и β се транзитивни, тогаш и релацијата $\alpha \cap \beta$ е транзитивни.
    b) Ако релациите α и β се транзитивни, тогаш и релацијата $\alpha \cup \beta$ е транзитивни.
    c) Ако релациите α и β се транзитивни, тогаш и релацијата $\alpha \circ \beta$ е транзитивни.
    d) Ако релациите α и β се транзитивни, тогаш и релацијата $\alpha \setminus \beta$ е транзитивни.
    e) Ако релациите α и β се транзитивни, тогаш и релацијата $\alpha \dot{-} \beta$ е транзитивни.
14. Во множеството цели броеви $\mathbf{Z}$ е дефинирана релација α на следниов начин: $x \alpha y$ ако и само ако $x^2 + x = y^2 + y$. Испитај дали α е релација на еквиваленција.
15. Во множеството цели броеви $\mathbf{Z}$ е дефинирана релација α на следниов начин: $x \alpha y$ ако и само ако $4 \mid (x - y)$.

a) Докажи дека α е релација на еквиваленција.

b) Најди го фактор-множеството $\mathbf{Z}_{|\alpha}$.

16. Најди ја релацијата на еквиваленција α на множеството A ако нејзиното фактор-множество е $A_{|\alpha} = \{\{a,b,c,d,e\},\{f,g,h\}\}$.

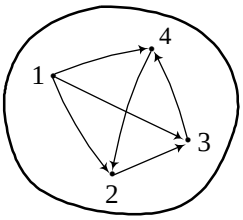
17. Докажи дека релацијата

$$\alpha = \{(a,a),(b,b),(c,c),(d,d),(a,b),(a,c),(b,c),(b,a),(c,a),(c,b)\}$$

дефинирана во множеството $A = \{a,b,c,d\}$ е релација на еквиваленција.

Најди го фактор-множеството $A_{|\alpha}$.

18. а) На цртежот десно во множеството $A = \{1,2,3,4\}$ графички е прикажана релацијата α. Запиши ја како подмножество од $A \times A$ и определи ги нејзините својства.



б) Во множеството цели броеви $\mathbf{Z}$ е дефинирана релација α на следниот начин: $x \alpha y$ ако и само ако

$$3x^2 + 2x = 3y^2 + 2y.$$

Испитај дали е α релација на еквиваленција.

19. За множеството $A = \{a,b,c,d,e,f,g\}$ најди барем една релација на еквиваленција која има три класи на еквиваленција такви што едната има три елементи, а останатите две имаат по два елементи.

20. Нека функцијата $f(x) = x^2 + 1$ е определена на множеството $A = [-2,4]$. На множеството A дефинираме релација α на следниов начин:

$(a,b) \in \alpha$ ако и само ако $f(a) = f(b)$.

1) Докажете дека α е релација на еквиваленција.

2) Определете ги следниве класи на еквиваленција: $C_1, C_2, C_0, C_3, C_{\frac{-1}{2}}, C_4$.

21. На множеството $\mathbf{N} \times \mathbf{N}$ е определена релација α на следниов начин:

$(a,b)\alpha(c,d)$ ако и само ако $a + d = b + c$.

Дали α е релација на еквиваленција (докажете или наведете контрапример). Кои елементи се во релација со $(1,2)$, а кои се во релација со $(6,3)$?

22. Нека A е множеството зборови составени од кириличното писмо и нека на множеството A е дефинирана релација α на следниов начин

$u \alpha v$ ако и само ако во двата збора u и v првите четири букви се еднакви.

Дали α е релација на еквиваленција?

23. Нека A е множеството зборови составени од кириличното писмо и нека на множеството A е дефинирана релација α на следниов начин:

$u \alpha v$ ако и само ако во двата збора u и v првата и последната буква се еднакви.

Дали α е релација на еквиваленција?

24. Нека A е множеството низи кои се состојат од броевите 0 и 1 и нека на множеството A е дефинирана релација α на следниов начин:

$u \alpha v$ ако и само ако низите u и v содржат ист број нули.

Дали α е релација на еквиваленција?

25. Дадено е множеството $A = \{a, b, c, d, e\}$ и во него релацијата

$$\alpha = \{(a,a), (b,b), (c,b), (d,e), (e,e), (d,d), (c,c), (b,e), (d,b), (c,e)\}.$$

а) Докажи дека α е релација на подредување во множеството A.

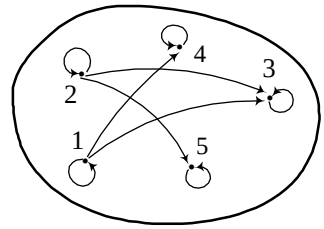
б) Претстави ја шематски релацијата α.

26. Дадено е множеството $A = \{1, 2, 3\}$.

a) Најди го неговото партитивно множество $\mathbf{P}(A) = \{X \mid X \subseteq A\}$.

b) Докажи дека релацијата α определена со $X \alpha Y$ ако и само ако $X \subseteq Y$ е релација за подредување во $\mathbf{P}(A)$.

27. Во множеството $A = \{1, 2, 3, 4, 5\}$ релацијата α е дадена со шемата на цртежот десно.



а) Запиши ја релацијата α како множество од подредени парови.

b) Докажи дека α е релација за подредување во множеството A.

28. Која од следниве релации е делумно подредување на множеството $A = \{a, b, c, d\}$:

1) $\alpha = \{(a,a), (b,b), (c,c), (d,d), (a,c), (b,c), (c,d), (a,d), (b,d)\}$,

2) $\alpha = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,c), (c,d), (d,a)\}$,

3) $\alpha = \{(b,b), (c,c), (d,d), (a,c), (b,c), (c,d), (a,d), (b,d)\}$ и

4) $\alpha = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,c), (a,c), (a,d), (b,d), (c,d)\}$.

29. Нека B е Булова алгебра. За $x, y \in B$ дефинираме $x \leq y$ ако $xy = x$. Докажете дека множеството $(B, \leq)$ е делумно подредено множество.

30. Нека B е Булова алгебра со делумното подредување дадено во задача 25. Елементот $x \in B$ го нарекуваме *атом* на алгебрата B ако за секој $y \in B$ од $y \leq x$ следува $y = 0$ или $y = x$. Докажете дека ако елементот $x \in B$ е атом на алгебрата B и $y \in B$, тогаш $xy = 0$ или $xy = x$.

31. Докажете дека ако елементите $x, y \in B$ се атоми на алгебрата B, тогаш $xy = 0$.

VI ГЛАВА
ГРУПИ. ПРСТЕНИ И ПОЛИЊА

1. ГРУПОИД. ПОЛУГРУПА

1.1. Во дефиниција IV 5.2 го воведовме поимот за внатрешна бинарна операција определена на непразно множество и разгледавме неколку примери во врска со овој поим. Токму изучувањето на непразните множества со некои операции е основна задача на современата алгебра. Секако, наједноставен случај е кога имаме непразно множество со една операција. Во оваа смисла ја имаме следната дефиниција.

Дефиниција. Ако $*$ е бинарна операција на непразното множеството G, тогаш подредениот пар $(G,*)$ го нарекуваме *групоид*. Притоа G го нарекуваме *носител* на групоидот, а $*$ - негова *операција*.

Ако бинарната операција е означена со $\cdot$, тогаш ќе велиме дека ознаката е *мултипликативна*, а ако операцијата е означена со +, тогаш ќе велиме дека ознаката е *адитивна*. Притоа, за групоидот $(G,\cdot)$ ($(G,+)$) ќе велиме дека се *мултипликативно* (*адитивно*) *означен*.

1.2. Пример. а) Нека $\mathbf{N}$ е множеството природни броеви. Бидејќи збир и производ на два броја е природен број, заклучуваме дека $(\mathbf{N},+)$ и $(\mathbf{N},\cdot)$ се групоиди.

Од друга страна, одземањето и делењето не се операции во множеството природни броеви $\mathbf{N}$, па затоа $(\mathbf{N},-)$ и $(\mathbf{N},:)$ не се групоиди.

б) Нека M е произволно непразно множество и $\mathbf{P}(M)=\{X \mid X \subseteq M\}$ е неговото *партитивно множество* (*булеан*). Од дефинициите на унија, пресек и разлика на множества следува дека $(\mathbf{P}(M),\cup)$; $(\mathbf{P}(M),\cap)$ и $(\mathbf{P}(M),\setminus)$ се групоиди, чиј заеднички носител е $\mathbf{P}(M)$, а операциите се $\cup,\cap$ и $\setminus$, соодветно.

в) $(\mathbf{N},*)$, $(\mathbf{N},\circ)$, $(\mathbf{N},\Delta)$ и $(\mathbf{N},\bullet)$ каде

$$x*y=\mathrm{NZD}(x,y),\ x\circ y=\mathrm{NZS}(x,y),\ x\Delta y=\min\{x,y\} \text{ и } x\bullet y=x+y+xy$$

се групоиди.

г) Ако со $M_n=\{1,2,...,n-1,n\}$ го означиме комплетниот систем на остатоци по модул n и со $\oplus$ и $\otimes$ ги означиме операциите собирање и множење по модул n соодветно, тогаш $(M_n,\oplus)$ и $(M_n,\otimes)$ се групоиди. Како и во случаите $n=4$ и $n=5$, точноста на ова тврдење непосредно следува од фактот дека при наведените операции збир и производ на елементи од M_n резултатот е елемент од M_n. ♦

1.3. При проучувањето на множествата видовме дека за операциите пресек и унија на произволни множества A, B и C важи

$$(A\cap B)\cap C = A\cap(B\cap C) \text{ и } (A\cup B)\cup C = A\cup(B\cup C).$$

Исто така, знаеме дека за операциите собирање и множење на природни броеви важи

$$(x+y)+z = x+(y+z) \text{ и } (x\cdot y)\cdot z = x\cdot(y\cdot z), \text{ за секои } x,y,z\in\mathbf{N}.$$

Меѓутоа, за операцијата разлика на множества равенствата од наведениот облик не се исполнети. Така, на пример, ако

$$A=\{1,2,3,4\},\ B=\{1,4,5\}, C=\{1,2,4\},$$

тогаш

$$(A\setminus B)\setminus C = \{2,3\}\setminus\{1,2,4\} = \{3\} \neq \{1,2,3,4\} = \{1,2,3,4\}\setminus\{5\} = A\setminus(B\setminus C).$$

Претходно изнесеното е една од причините за проучувањето на групоидите чии операции го задоволуваат асоцијативниот закон. Така ја имаме следнава дефиниција.

Дефиниција. За групоидот $(G,*)$ ќе велиме дека е *асоцијативен* (*полугрупа*) ако за секои $x,y,z\in G$ важи

$$x*(y*z) = (x*y)*z. \tag{1}$$

1.4. Пример. а) Од својствата на операциите пресек и унија на множества следува дека групоидите $(\mathbf{P}(M),\cup)$ и $(\mathbf{P}(M),\cap)$ од примерот 1.2 б) се полугрупи. Меѓутоа, од погоре изнесеното следува дека групоидот $(\mathbf{P}(M),\setminus)$ не е полугрупа.

б) Од својствата на природните и целите броеви следува дека групоидите $(\mathbf{N},+)$, $(\mathbf{N},\cdot)$, $(\mathbf{Z},+)$ и $(\mathbf{Z},\cdot)$ се полугрупи.

Групоидот $(\mathbf{Z},-)$ не е полугрупа. Навистина,

$$6-(4-3) = 5 \neq -1 = (6-4)-3,$$

што значи дека асоцијативниот закон за операцијата одземање во множеството цели броеви не важи.

в) Лесно се покажува дека групоидите $(M_n,\oplus)$ и $(M_n,\otimes)$ од примерот 1.2 г) се полугрупи. Обиди се да докажеш дека за операциите собирање и множење по модул n важи асоцијативниот закон.

г) Да го разгледаме групоидот $(\mathbf{N},\bullet)$ каде што $x\bullet y = x+y+xy$ за секои $x,y\in\mathbf{N}$. За секои $x,y,z\in\mathbf{N}$ важи

$$\begin{aligned}(x\bullet y)\bullet z &= (x+y+xy)\bullet z = x+y+xy+z+z(x+y+xy)\\ &= x+y+z+xy+yz+zx+xyz\\ &= x+y+z+yz+x(y+z+yz) = x\bullet(y+z+yz) = x\bullet(y\bullet z)\end{aligned}$$

што значи дека $(\mathbf{N},\bullet)$ е полугрупа. ♦

1.5. За операциите унија и пресек на множества знаеме дека за секои множества A и B важи $A\cup B = B\cup A$, $A\cap B = B\cap A$. Исто така, за собирањето и множењето на целите броеви знаеме дека

$$x+y=y+x,\ x\cdot y=y\cdot x,$$

за секои $x,y\in\mathbf{Z}$. Меѓутоа, за одземањето на целите броеви и за разликата на множествата не важат равенства од наведениот облик. Имено,

$$3-4=-1\neq 1=4-3 \text{ и } \{1,2,3\}\setminus\{4,3,2\}=\{1\}\neq\{4\}=\{4,3,2\}\setminus\{1,2,3\}\ .$$

Претходно изнесеното е една од причините за проучувањето на групоидите чии операции го задоволуваат комутативниот закон. Така ја имаме следнава дефиниција.

Дефиниција. За групоидот $(G,*)$ ќе велиме дека е *комутативен* ако за операцијата * важи комутативниот закон, т.е. ако за секои $x,y\in G$ важи

$$x*y=y*x. \tag{2}$$

Полугрупата $(G,*)$ ја нарекуваме *комутативна* ако таа е е комутативен групоид.

1.6. Пример. а) Од својствата на операциите пресек и унија на множества следува дека полугрупите $(\mathbf{P}(M),\cup)$ и $(\mathbf{P}(M),\cap)$ од примерот 1.2 б) се комутативни. Меѓутоа, од погоре изнесеното следува дека групоидот $(\mathbf{P}(M),\setminus)$ не е комутативен.

б) Од својствата на природните и целите броеви следува дека полугрупите $(\mathbf{N},+)$, $(\mathbf{N},\cdot)$, $(\mathbf{Z},+)$ и $(\mathbf{Z},\cdot)$ се комутативни. Но, како што веќе видовме групоидот $(\mathbf{Z},-)$ не е комутативен.

в) Полугрупите $(M_n,\oplus)$ и $(M_n,\otimes)$ од пример 1.2 г) се комутативни. Последното може да се заклучи и од Келиевите шеми. Имено, еден групоид е комутативен ако и само ако неговата Келиева шема е симетрична во однос на главната дијагонала повлечена од левиот горен агол (зошто?).

г) Да ја разгледаме полугрупата $(\mathbf{N},\bullet)$ каде што $x\bullet y=x+y+x\cdot y$ за секои $x,y\in\mathbf{N}$. Бидејќи

$$x\bullet y=x+y+x\cdot y=y+x+y\cdot x=y\bullet x \text{ за секои } x,y\in\mathbf{N},$$

заклучуваме дека полугрупата $(\mathbf{N},\bullet)$ е комутативна. ♦

1.7. Лема. Ако $(G,*)$ е комутативен групоид, тогаш

1) $a*(a*a)=(a*a)*a$, за секој $a\in G$,

2) $a*(b*a)=(a*b)*a$, за секои $a,b\in G$,

3) Ако $a*(b*c)=(a*b)*c$, тогаш $c*(b*a)=(c*b)*a$.

Доказ. 2) Бидејќи групоидот G е комутативен добиваме дека за секои $a,b\in G$ важи:

$$a*(b*a)=(b*a)*a=(a*b)*a\ .$$

1) Непосредно следува од 2) за $b=a$.

3) Бидејќи групоидот G е комутативен од $a*(b*c)=(a*b)*c$ следува:

$$c*(b*a)=(b*a)*c=(a*b)*c=a*(b*c)=(b*c)*a=(c*b)*a\ .\ \blacklozenge$$

1.8. Од својствата на целите броеви знаеме дека од $x+y=z+y$ следува $x=z$. Претходно докажавме дека $(\mathbf{Z},+)$ е полугрупа, па логично се наметнува прашањето дали законот за кратење важи за секоја полугрупа. Пред да дадеме одговор на ова прашање ќе дефинираме што значи групоид со кратење.

Дефиниција. За групоидот $(G,*)$ ќе велиме дека е *групоид со кратење* ако од $x*z=y*z$ или $z*x=z*y$ следува $x=y$.

1.9. Пример. а) Од својствата на природните броеви следува дека $(\mathbf{N},\cdot)$ и $(\mathbf{N},+)$ се групоиди со кратење.

б) Нека M е непразно множество. Да го разгледаме групоидот $(\mathbf{P}(M),\cup)$. Ако A е произволно непразно подмножество од M, тогаш $A\cup M={}^{c}A\cup M$, но $A\neq {}^{c}A$. Според тоа, и $(\mathbf{P}(M),\cup)$ не е групоид со кратење. Сега да го разгледаме групоидот $(\mathbf{P}(M),\cap)$. За секое непразно подмножество A од M важи $A\cap\varnothing={}^{c}A\cap\varnothing$, но $A\neq {}^{c}A$. Според тоа, $(\mathbf{P}(M),\cap)$ не е групоид со кратење. ♦

2. ПОДГРУПОИДИ. ПОТПОЛУГРУПИ

2.1. Дефиниција. За групоидот (полугрупата) $(H,\bullet)$ ќе велиме дека е *подгрупоид* (*потполугрупа*) од групоидот $(G,*)$ ако $H\subseteq G$ и $x\bullet y=x*y$, за секои $x,y\in H$.

2.2. Тврдењата од следнава теорема се очигледни. Деталите ги оставаме на читателот за вежба.

Теорема. Нека $(H,\bullet)$ е подгрупоид на $(G,*)$. Ако $(G,*)$ е

а) комутативен,

б) полугрупа,

в) групоид со кратење,

тогаш соодветното својство го има и $(H,\bullet)$. ♦

2.3. Степени со природни експоненти. Нека $(G,\cdot)$ е мултипликативно означена полугрупа. Дефинираме пресликување $(n,a)\to a$ од $\mathbf{N}\times G$ во G со:

$$a^{n}=\underbrace{aa...a}_{n},\ n\geq 1\ .$$

Јасно, бидејќи $(G,\cdot)$ е полугрупа пресликувањето е добро дефинирано. Елементот a^{n} го нарекуваме *степен* со основа a и *степенов показател* (*експонент*) n. Лесно се докажува дека

$$a^1 = a,\ \ a^n a^m = a^{m+n},\ (a^n)^m = a^{mn}$$, за секои $a \in G,\ m,n \in \mathbf{N}$,

а ако полугрупата G е комутативна, тогаш $(ab)^n = a^n b^n$, за секои $a,b \in G$ и $n \in \mathbf{N}_0$, (проверете!). Понатаму, од равенството $a^n a^m = a^{m+n}$ следува дека множеството $A = \{a, a^2, a^3, ...\} \subseteq S$ е полугрупа, која ја нарекуваме *циклична потполугрупа на* S *генерирана од елементот* a.

Во случај на адитивно означена полугрупа $(G,+)$ наместо a^n ќе пишуваме na. Јасно, притоа

$$na = \underbrace{a + a + ... + a}_{n},\ n \geq 1.$$

и се исполнети равенствата:

$$1a = a,\ ma + na = (m+n)a,\ m(na) = (mn)a$$, за секои $a \in G,\ m,n \in \mathbf{N}$,

а ако полугрупата G е комутативна, тогаш $n(a+b) = na + nb$, за секои $a,b \in G$ и $n \in \mathbf{N}$. ♦

2.4. Теорема. Нека $(G,\cdot)$ е полугрупа,

$$a_1, a_2, ..., a_k \in S,\ A = \{a_1, a_2, ..., a_k\}$$

и A^* е множеството кое се состои од сите конечни производи на елементите од A. Тогаш A^* е најмалата потполугрупа од G која го содржи множеството A.

Доказ. Доволно е да докажеме дека производ на два елементи од A^* е елемент на A^*. Деталите ги оставаме на читателот за вежба. ♦

2.5. Дефиниција. Полугрупата A^* од теорема 2.4 ја нарекуваме *полугрупа генерирана од множеството* A. Ако за секое вистинско подмножество B на множеството A важи $B^* \neq A^*$, тогаш за множеството A ќе велиме дека е *минимално генерирачко множество на полугрупата* A^*.

2.6. Дефиниција. Нека $(G,*)$ и $(H,\bullet)$ се групоиди. За пресликувањето $f : G \to H$ ќе велиме дека е *хомоморфизам* од G во H ако за секои $a,b \in G$ важи $f(a*b) = f(a) \bullet f(b)$. Ако хомоморфизмот $f : G \to H$ е биекција, тогаш ќе велиме дека f е *изоморфизам* од G во H.

2.7. Теорема. Ако групоидот $(G,*)$ е:

а) комутативен,
б) асоцијативен (полугрупа), и
в) групоид со кратење,

тогаш соодветното својство го има и секој групоид $(H,\bullet)$ изоморфен со G.

Доказ. Нека f е изоморфизам од G во H. Ако $a', b', c' \in H$, тогаш бидејќи f е биекција постојат $a,b,c \in G$, такви што $a' = f(a), b' = f(b), c' = f(c)$.

а) Нека групоидот G е комутативен. Тогаш за секои $a',b' \in H$ важи

$$a' \bullet b' = f(a) \bullet f(b) = f(a*b) = f(b*a) = f(b) \bullet f(a) = b' \bullet a',$$

т.е. групоидот H е комутативен.

б) Нака групоидот G е асоцијативен. Тогаш за секои $a',b',c' \in H$ важи

$$a' \bullet (b' \bullet c') = f(a) \bullet (f(b) \bullet f(c)) = f(a) \bullet f(b*c) = f(a*(b*c)) = f((a*b)*c)$$
$$= f(a*b) \bullet f(c) = (f(a) \bullet f(b)) \bullet f(c) = (a' \bullet b') \bullet c',$$

т.е. групоидот H е асоцијативен.

в) Нека G е групоид со кратење. Ако $a' \bullet b' = a' \bullet c'$, тогаш

$$f(a) \bullet f(b) = f(a) \bullet f(c), \text{ т.е. } f(a*b) = f(a*c)$$

и како f е биекција следува дека $a*b = a*c$. Но, G е групоид со кратење, па од последното равенство следува $b = c$, што значи $f(b) = f(c)$, односно $b' = c'$. Аналогно се докажува дека од $a' \bullet b' = c' \bullet b'$ следува $a' = c'$, што значи дека H е групоид со кратење. ♦

2.8. Теорема. а) Нека $(S,\cdot)$ и $(T,\circ)$ се полугрупи и нека $f : S \to T$ е хомоморфизам од S во T. Ако $\overline{S}$ е потполугрупа од S, тогаш $f(\overline{S})$ е потполугрупа од T.

б) Нека $(S,\cdot)$ и $(T,\circ)$ се полугрупи и нека $f : S \to T$ е хомоморфизам од S во T. Ако $\overline{T}$ е потполугрупа од T, тогаш $f^{-1}(\overline{T})$ е потполугрупа од S.

Доказ. а) Нека $t_1, t_2 \in f(\overline{S})$. Тогаш, постојат $s_1, s_2 \in \overline{S}$ такви што $t_1 = f(s_1), t_2 = f(s_2)$. Но, $\overline{S}$ е потполугрупа од S, па затоа $s_1 \cdot s_2 \in \overline{S}$, што значи

$$t_1 \circ t_2 = f(s_1) \circ f(s_2) = f(s_1 \cdot s_2) \in f(\overline{S}),$$

т.е. $f(\overline{S})$ е потполугрупа од T. ♦

б) Постапете аналогно на доказот под а). ♦

2.9. Теорема. а) Идентичното пресликување е изоморфизам од $(G,*)$ во $(G,*)$.

б) Ако $f : G \to H$ е изоморфизам од $(G,*)$ во $(H,\bullet)$, тогаш инверзното пресликување $f^{-1} : H \to G$ е изоморфизам.

в) Нека $(G,*), (H,\bullet)$ и $(R,\circ)$ се групоиди. Ако $f : G \to H$ и $g : H \to R$ се изоморфизми, тогаш $h = gf : G \to R$ е изоморфизам.

Доказ. а) Ако $a,b \in G$, тогаш $I_G(ab) = ab = I_G(a)I_G(b)$ и I_G е биекција.

б) Според теорема IV 4.13 инверзното пресликување f^{-1} е биекција. Нека $a',b' \in H$ и $f^{-1}(a') = a,\ f^{-1}(b') = b$, т.е. $f(a) = a',\ f(b) = b'$. Тогаш имаме

$$f^{-1}(a')*f^{-1}(b')=a*b=f^{-1}f(a*b)=f^{-1}(f(a)\bullet f(b))=f^{-1}(a'\bullet b'),$$

што значи дека f^{-1} е изоморфизам.

в) Според теорема IV 4.9 пресликувањето $h=gf$ е биекција и притоа важи

$$h(a*b)=g(f(a*b))=g(f(a)\bullet f(b))=g(f(a))\circ g(f(b))=h(a)\circ h(b)$$

што значи дека $h=gf$ е изоморфизам. ♦

3. КОНГРУЕНЦИИ НА ГРУПОИДИ

3.1. Дефиниција. Нека $(G,\cdot)$ е групоид и α е релација на еквиваленција над G. Ако од $(u,v)\in\alpha$ и $(x,y)\in\alpha$ следува $(u\cdot x,v\cdot y)\in\alpha$, за секои $x,y,u,v\in G$, тогаш за релацијата α ќе велиме дека е *релација на конгруенција* над G.

3.2. Теорема. Нека $(S,\cdot)$ и $(T,\circ)$ се групоиди и нека $f:S\to T$ е хомоморфизам од S во T. Релацијата α на групоидот $(S,\cdot)$ определена со $(s,s')\in\alpha$ ако и само ако $f(s)=f(s')$ е релација на конгруенција.

Доказ. За секој $s\in S$ важи $f(s)=f(s)$, па затоа релацијата α е рефлексивна. Понатаму, ако $(s,s')\in\alpha$, тогаш $f(s)=f(s')$, па затоа $f(s')=f(s)$, т.е. $(s',s)\in\alpha$, т.е. релацијата α е симетрична. Нека $(s,s')\in\alpha$ и $(s',s'')\in\alpha$. Имаме:

$$f(s)=f(s')=f(s''),$$

па затоа $(s,s'')\in\alpha$, т.е. релацијата α е транзитивна, што значи дека α е релација на еквиваленција.

Нека претпоставиме дека $(u,v)\in\alpha$ и $(x,y)\in\alpha$. Тогаш $f(u)=f(v)$ и $f(x)=f(y)$. Но, f е хомоморфизам, па затоа

$$f(u\cdot x)=f(u)\circ f(x),\ \ f(v)\circ f(y)=f(v\cdot y)$$

и

$$f(u\cdot x)=f(u)\circ f(x)=f(v)\circ f(y)=f(v\cdot y),$$

т.е. $(u\cdot x,v\cdot y)\in\alpha$, што значи дека α е релација на конгруенција. ♦

3.3. Теорема. Класите на еквиваленција на конгруенцијата α на групоидот $(G,\cdot)$ формираат групоид во која операцијата е определена со

$$C_a\circ C_b=C_{ab}. \tag{1}$$

Доказ. Доволно е да докажеме дека десната страна на (1) зависи само од класите C_a и C_b, а не и од нивните претставници. Навистина нека α е конгруенција на $(G,\cdot)$. Тогаш, ако $C_a=C_x$ и $C_b=C_y$ имаме $(a,x)\in\alpha$ и $(b,y)\in\alpha$ и како

α е конгруенција добиваме $(ab, xy) \in \alpha$, што значи дека $C_{ab} = C_{xy}$, т.е. десната страна на (1) зависи само од класите C_a и C_b, а не и од нивните претставници. ♦

3.4. Дефиниција. Групоидот формиран од класите на еквиваленција на релацијата на конгруенција α на групоидот $(G, \cdot)$ ја нарекуваме *факторгрупоид* и ќе го означуваме со $G_{|\alpha}$.

3.5. Пример. Од својствата на конгруенциите во множеството цели броеви следува дека за секој природен број n релацијата α_n определена со

$$(x, y) \in \alpha_n \text{ ако и само } x \equiv y \pmod{n}$$

е релација на конгруенција во групоидите $(\mathbf{Z}, +)$ и $(\mathbf{Z}, \cdot)$. Притоа соодветните факторгрупоиди се $(M_n, \oplus)$ и $(M_n, \otimes)$, соодветно. ♦

3.6. Теорема. Ако групоидот $(G, \cdot)$ е: а) комутативен, б) полугрупа, тогаш соодветното својство го има и секој факторгрупоид на G.

Доказ. Нека α е конгруенција на G.

а) Нека G е комутативен групоид. Тогаш, за секои $a, b \in G$ важи

$$C_a \circ C_b = C_{ab} = C_{ba} = C_b \circ C_a,$$

што значи дека групоидот $G_{|\alpha}$ е комутативен.

б) Нека G е полугрупа. Тогаш, за секои $a, b, c \in G$ важи

$$\begin{aligned}(C_a \circ C_b) \circ C_c &= C_{ab} \circ C_c = C_{(ab)c} = C_{a(bc)} \\ &= C_a \circ C_{bc} = C_a \circ (C_b \circ C_c),\end{aligned}$$

што значи дека групоидот $G_{|\alpha}$ е полугрупа. ♦

4. НЕУТРАЛЕН И ИНВЕРЗЕН ЕЛЕМЕНТ

4.1. Нека M е дадено множество и $\mathbf{P}(M)$ е неговото партитивно множество. Во групоидот $(\mathbf{P}(M), \cup)$ важи $A \cup \varnothing = \varnothing \cup A = A$ за секое множество $A \in \mathbf{P}(M)$. Слично, во групоидот $(\mathbf{P}(M), \cap)$ важи $A \cap M = M \cap A = A$ за секое множество $A \in \mathbf{P}(M)$.

Од друга страна, во групоидот $(\mathbf{P}(M), \setminus)$ важи $A \setminus \varnothing = A$ за секое множество $A \in \mathbf{P}(M)$, но за секое множество B важи $B \setminus M = \varnothing$, што значи дека равенството $B \setminus M = M$ не е исполнето за ниту едно множество $B \in \mathbf{P}(M)$.

Понатаму, како што знаеме, во групоидот $(\mathbf{N}, \cdot)$ важи $1 \cdot n = n \cdot 1 = n$ за секој $n \in \mathbf{N}$, но во групоидот $(\mathbf{N}, +)$ не постои елемент k таков што $k + n = n + k = n$ за

кој било $n \in \mathbf{N}$. Последното не е точно за групоидот $(\mathbf{N}_0, +)$. Имено, во овој групоид важи $n + 0 = 0 + n = n$ за секој $n \in \mathbf{N}_0$.

Како што можеме да видиме, кај некои групоиди постојат елементи кои во извесна смисла се неутрални во однос на операциите во тие групоиди, додека кај некои групоиди тоа не е случај. Ваквата ситуација е непосредна причина за воведување на нов апстрактен поим и тоа е поимот за единичен (неутрален) елемент. Така ја имаме следната дефиниција.

4.2. Дефиниција. Нека е даден групоидот $(G, *)$. Елементот $e_l \in G$ го нарекуваме *лева единица* на G ако

$$e_l * x = x, \text{ за секој } x \in G. \tag{1}$$

Елементот $e_d \in G$ го нарекуваме *десна единица* на G ако

$$x * e_d = x, \text{ за секој } x \in G. \tag{2}$$

Елементот $e \in G$ го нарекуваме *единица* на G ако тој е и лева и десна единица на G.

4.3. Коментар. Да забележиме дека ако групоидот $(G, *)$ е комутативен, тогаш левата единица истовремено е и десна единица и обратно. Навистина, ако e_l е лева единица, тогаш $e_l * x = x$, за секој $x \in G$. Ако во последното равенство го примениме комутативниот закон добиваме

$$x = e_l * x = x * e_l, \text{ за секој } x \in G,$$

што значи дека e_l е и десна единица. Случајот со десната единица се разгледува аналогно.

Покрај термините лева единица, десна единица и единица, кои се вообичаени за мултипликативните групоиди (на пример, групоид со операција множење на броеви), кога станува збор за адитивни групоиди (на пример, групоид со операција собирање на броеви, т.е. кога наместо $x * y$ пишуваме $x + y$), ќе го користиме терминот *нулти елемент* (*нула*). Во овој случај единицата ќе ја нарекуваме *нула* и ќе ја означуваме со 0. Според тоа, 0 е нула на групоидот $(G, +)$ ако $x + 0 = x = 0 + x$, за секој $x \in G$.

4.4. Пример. а) На почетокот од овој дел видовме дека групоидот $(\mathbf{N}, +)$ нема нулти елемент, додека бројот 1 е единица за групоидот $(\mathbf{N}, \cdot)$.

Меѓутоа, како за групоидот $(\mathbf{N}_0, +)$, така и за групоидот $(\mathbf{Z}, +)$ бројот 0 е нулти елемент, т.е. $x + 0 = 0 + x = x$ за секој $x \in \mathbf{Z}$. Што се однесува до групоидот $(\mathbf{Z}, \cdot)$, имаме $1 \cdot x = x \cdot 1 = x$ за секој $x \in \mathbf{Z}$, што значи дека бројот 1 е единица во $(\mathbf{Z}, \cdot)$.

Што се однесува до групоидот $(\mathbf{Z}, -)$, тој има десна единица и тоа е бројот 0. Навистина, од својствата на целите броеви знаеме дека $x - 0 = x$ за секој $x \in \mathbf{Z}$. Од друга страна, за овој групоид да има лева единица, потребно е да по-

стои цел број y таков што $y-x=x$ за секој $x\in\mathbf{Z}$. Последното не е можно, бидејќи за $x=0$ добиваме дека $y=0$, од што ќе следува дека $0-x=x$ за секој $x\in\mathbf{Z}$, што е противречност.

б) Да ја разгледаме полугрупата $(M_n,\oplus)$. Имаме $x\oplus 0=0\oplus x=x$ за секој $x\in M_n$, што значи дека 0 е нулти елемент во оваа полугрупа.

Во полугрупата $(M_n,\otimes)$ е исполнето равенството $x\otimes 1=1\otimes x=x$ за секој $x\in M_n$, што значи дека 1 е единичен елемент во оваа полугрупа.

в) Да ја разгледаме полугрупата $(\mathbf{N},\bullet)$, каде што $x\bullet y=x+y+x\cdot y$ за секои $x,y\in\mathbf{N}$. Како што знаеме, оваа полугрупа е комутативна, па затоа ако таа има лева единица, ќе има и десна единица, т.е. ќе има единица. Нека e е единица во $(\mathbf{N},\bullet)$. Тогаш $x=x\bullet e=x+e+x\cdot e$ за секој $x\in\mathbf{N}$. Во множеството природни броеви равенството $x=x+(e+e\cdot x)$ не е можно, бидејќи кога на природниот број x се додаде природниот број $e+e\cdot x$, добиваме број кој е поголем од бројот x. Од досега изнесеното следува дека полугрупата $(\mathbf{N},\bullet)$ нема единица.

г) Од операциите собирање и множење на целите броеви следува дека $(\mathbf{Z},\bullet)$, каде што $x\bullet y=x+y+x\cdot y$, за секои $x,y\in\mathbf{Z}$ е комутативна полугрупа. Ќе провериме дали оваа полугрупа има неутрален елемент. Нека e е неутрален елемент во $(\mathbf{Z},\bullet)$. Тогаш,

$x=x\bullet e=x+e+x\cdot e$ за секој $x\in\mathbf{Z}$, т.е. $0=e\cdot(1+x)$ за секој $x\in\mathbf{Z}$.

Во множеството $\mathbf{Z}$ последното равенство е можно ако и само ако $e=0$. Според тоа, бројот 0 е неутрален елемент во полугрупата $(\mathbf{Z},\bullet)$. Навистина,

$$x\bullet 0=x+0+x\cdot 0=x \text{ за секој } x\in\mathbf{Z}. \blacklozenge$$

4.6. Пример. а) Во примерот 4.4 б) видовме дека $(M_n,\oplus)$ и $(M_n,\otimes)$ имаат нула и единица, соодветно. Како што знаеме, за $n=4$ тие ги имаат следниве *Келиеви шеми*:

$\oplus$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Забележуваме дека во Келиевата шема на $(M_4,\oplus)$ редот и колоната кои соодветствуваат на 0 се идентични со главниот ред и колона, соодветно. Слично, во Келиевата шема на $(M_4,\otimes)$ редот и колоната кои соодветствуваат на 1 се идентични со главните ред и колона, соодветно.

Претходно изнесеното, всушност, важи за секоја Келиева шема. Имено, елементот x е лева единица во групоидот $(G,*)$ ако и само ако редот која му соодветствува на x е идентичен со главниот ред во Келиевата шема на $(G,*)$.

Елементот y е десна единица во групоидот $(G,*)$ ако и само ако колоната која му соодветствува на y е идентична со главната колона во Келиевата шема на $(G,*)$.

б) Да ги разгледаме групоидите $(G,\bullet)$ и $(G,\circ)$ чии Келиеви шеми се:

$\bullet$	***a***	***b***	***c***	***d***
a	*d*	*a*	*b*	*c*
b	*c*	*d*	*a*	*b*
c	*b*	*c*	*d*	*a*
d	*a*	*b*	*c*	*d*

$\circ$	***a***	***b***	***c***	***d***
a	*d*	*c*	*b*	*a*
b	*a*	*d*	*c*	*b*
c	*b*	*a*	*d*	*c*
d	*c*	*b*	*a*	*d*

Од Келиевата шема гледаме дека елементот d е лева единица за $(G,\bullet)$, меѓутоа овој групоид нема десна единица. Слично, елементот d е десна единица за $(G,\circ)$, меѓутоа овој групоид нема лева единица. ♦

4.7. Како што видовме, еден групоид може да има десна или лева единица, но не мора да има единица. Логично е да се запрашаме дали еден групоид може да има различни десна и лева единица. Одговорот на ова прашање го дава следната теорема.

Теорема. Ако e_l е лева, а e_d десна единица на групоидот $(G,*)$, тогаш $e_l = e_d$.

Доказ. Нека e_l и e_d се соодветно лева и десна единица на групоидот $(G,*)$. Бидејќи e_l е лева единица, за елементот e_d добиваме $e_d = e_l * e_d$. Но, e_d е десна единица, па за елементот e_l добиваме $e_l * e_d = e_l$. Конечно, од последните две равенства следува дека $e_d = e_l * e_d = e_l$. ♦

4.8. Последица. Во еден групоид G има најмногу една единица.

Доказ. Непосредно следува од теоремата 4.7 и фактот дека секоја единица е истовремено и лева и десна единица. ♦

4.9. Да се вратиме на групоидот $(M_4,\oplus)$ во кој 0 е нултиот елемент. Забележуваме дека $1\oplus 3 = 2\oplus 2 = 0\oplus 0 = 0$. Слично, за групоидот $(M_4,\otimes)$ во кој 1 е единичниот елемент имаме $1\otimes 1 = 3\otimes 3 = 1$, но не постојат елементи x и y такви што $x\otimes 2 = y\otimes 0 = 1$.

Последното укажува на потребата, при проучувањето на групоид $(G,*)$ со неутрален елемент e да се најдат сите оние елементи x за кои постои елемент y таков што $x*y = y*x = e$. Во таа смисла ја имаме следнава дефиниција.

4.10. Дефиниција. Нека $(G,*)$ е групоид со неутрален елемент e. За еден елемент $x\in G$ ќе велиме дека е *инверзибилен* ако постои $x'\in G$ таков што $x*x' = x'*x = e$. Притоа елементот x' го нарекуваме *инверзен елемент* на x.

Јасно, единицата e е инверзен елемент на самата себе.

4.11. Пример. а) Бројот 1 е единица за групоидот $(\mathbf{N},\cdot)$ и е единствен инверзибилен елемент. Навистина, од својствата на природните броеви имаме дека $xy=1$ ако и само ако $x=y=1$.

За групоидот $(\mathbf{Z},\cdot)$ бројот 1 е единица. За да ги најдеме инверзибилните елементи во овој групоид треба во множеството $\mathbf{Z}$ да ја решиме равенката $xy=1$. Решенија на последната равенка се $x=y=1$ и $x=y=-1$. Според тоа, во овој групоид единствени инверзибилни елементи се 1 и -1.

За групоидот $(\mathbf{Z},+)$ бројот 0 е нулти елемент и бидејќи $x+(-x)=0$ за секој $x\in\mathbf{Z}$, добиваме дека секој елемент во овој групоид е инверзибилен.

б) Како што видовме во групоидот $(M_4,\oplus)$ важи

$$1\oplus 3=2\oplus 2=0\oplus 0=0,$$

што значи дека 1 е инверзен на 3, 2 е инверзен на самиот себе и 0 е инверзен на самиот себе. Заради комутативноста добиваме дека 3 е инверзен на 1. Слично, за секој природен број n секој елемент на групоидот $(M_n,\oplus)$ има инверзибилен (зошто?).

За групоидот $(M_4,\otimes)$ видовме дека 1 и 3 се инверзни на самите себе, но 0 и 2 не се инверзибилни. Понатаму, од множењето по модул 5 следува дека во групоидот $(M_5,\otimes)$ секој елемент различен од 0 е инверзибилен и тоа: 1 и 4 се инверзибилни сами на себе, 2 на 3 се заемно инверзибилни.

Забележуваме дека 5 е прост број, а 4 е сложен број. Провери дали за бројот $n=7$ во групоидот $(M_n,\otimes)$ секој елемент различен од 0 е инверзибилен. Дали ова важи за $n=6$?

в) Во примерот 4.4 г) видовме дека 0 е неутрален елемент на комутативниот групоид $(\mathbf{Z},\bullet)$, каде што $x\bullet y=x+y+x\cdot y$ за секои $x,y\in\mathbf{Z}$. За да ги најдеме инверзибилните елементи, треба во множеството $\mathbf{Z}$ да ја решиме равенката $x+y+x\cdot y=0$. Јасно, $y\neq -1$. Последната равенка ја трансформираме и добиваме $x=-\frac{y}{1+y}$, што значи дека $(1+y)\mid y$. Но, броевите y и $1+y$ се заемно прости, па затоа последниот услов е можен ако и само ако $y=0$ и притоа $x=0$. Конечно, единствен инверзибилен елемент во групоидот $(\mathbf{Z},\bullet)$ е 0. ♦

4.12. Од дефиницијата 4.10 имаме дека ако во групоидот $(G,*)$ со неутрален елемент e елементот x' е инверзен на x, тогаш x е инверзен на x'. Логично е да се запрашаме дали производ на инверзибилни елементи е инверзибилен елемент. Одговорот на ова прашање го дава следната теорема.

4.13. Теорема. Ако x и y се инверзибилни елементи во полугрупата $(G,*)$ со единица e, тогаш и $x*y$ е инверзибилен во $(G,*)$ и притоа важи дека неговиот инверзен елемент е $y'*x'$, каде што x' и y' се инверзните елементи на x и y, соодветно.

Доказ. Нека x и y се инверзибилни елементи во полугрупата $(G,*)$ со единица e. Тогаш

$$(x*y)*(y'*x') = x*(y*y')*x' = x*e*x' = x*x' = e$$
$$(y'*x')*(x*y) = y'*(x'*x)*y = y'*e*y = y'*y = e$$

од што следува точноста на тврдењето. ♦

4.14. Забелешка. Имајќи ја предвид аналогијата на инверзибилниот елемент со инверзното пресликување во натамошните разгледувања инверзибилниот елемент на елементот x ќе го означуваме со x^{-1}.

4.15. Теорема. Ако $(G,*)$ е групоид со единица, тогаш соодветното својство го има и секој групоид $(H,\bullet)$ изоморфен со G.

Доказ. Нека f е изоморфизам од G во H. Ако $a' \in H$, тогаш бидејќи f е биекција постои $a \in G$ таков што $a' = f(a)$. Ако e е единица на G и ако $e' = f(e)$, тогаш за секој $a' \in H$ важи:

$$a'\bullet e' = f(a)\bullet f(e) = f(a*e) = f(a) = a' \text{ и}$$
$$e'\bullet a' = f(e)\bullet f(a) = f(e*a) = f(a) = a',$$

од што следува дека e' е единица на H. ♦

4.16. Теорема. Ако групоидот $(G,\cdot)$ има единица, тогаш и секој факторгрупоид на G има единица.

Доказ. Нека α е конгруенција на G. Ако e е единица во G, тогаш за секој $a \in G$ важи

$$C_e C_a = C_{ea} = C_a \text{ и } C_a C_e = C_{ae} = C_a,$$

што значи дека C_e е единица на факторгрупоидот $G_{|\alpha}$. ♦

5. ПОИМ ЗА ГРУПА. ПОДГРУПА

5.1. Во претходните разгледувања се запознавме со поимите групоид, асоцијативен и комутативен групоид, неутрален и инверзибилен елемент и разгледавме повеќе примери во врска со овие поими. Притоа дадовме примери на групоиди во кои важат комутативниот и асоцијативниот закон, кои имаат неутрален елемент и секој елемент е инверзибилен. Вакви примери се групоидите $(M_5,\oplus)$ и $(\mathbf{Z},+)$. Токму ваквите примери лежат во основата на посложените алгебарски структури, како што се група и прстен, кои се од посебно значење во математиката.

5.2. Дефиниција. За групоидот $(G,*)$ ќе велиме дека е *група* ако е полугрупа со единица, во која секој елемент е инверзибилен, т.е. ако

i) $(x*y)*z = x*(y*z)$, за секои $x, y, z \in G$,

ii) постои $e \in G$ таков што $x*e = e*x = x$ за секој $x \in G$ и

iii) за секој $x \in G$ постои еднозначно определен елемент $x^{-1} \in G$ таков што $x*x^{-1} = x^{-1}*x = e$.

За групата ќе велиме дека е *комутативна* (*Абелова*) ако е комутативна како групоид, т.е. ако $x*y = y*x$ за секои $x, y \in G$.

5.3. Пример. а) Од примерот 4.11 а) непосредно следува дека групоидите $(\mathbf{N}, \cdot)$ и $(\mathbf{Z}, \cdot)$ не се групи. Имено, во $(\mathbf{N}, \cdot)$ единствен инверзибилен елемент е 1, а во $(\mathbf{Z}, \cdot)$ единствени инверзибилни елементи се 1 и -1. Исто така, групоидот $(\mathbf{N}, +)$ не е група, бидејќи нема неутрален елемент.

Од примерите 1.6 б), 4.4 а) и 4.11 а) непосредно следува дека групоидот $(\mathbf{Z}, +)$ е група и таа според примерот 4.10 б) е комутативна.

б) Од примерите 1.6 в), 1.8 в), 4.4 б) и 4.11 б) следува дека за секој $n \in \mathbf{N}$ групоидот $(M_n, \oplus)$ е комутативна група.

За секој $n \in \mathbf{N}$ елементот 0 не е инверзибилен во групоидот $(M_n, \otimes)$ (зошто?). Тоа значи дека за секој $n \in \mathbf{N}$ групоидот $(M_n, \otimes)$ не е група. Меѓутоа, ако на множеството $M_5 \setminus \{0\}$ множењето по модул 5 го дефинираме како и во групоидот $(M_5, \otimes)$, забележуваме дека во овој случај добиваме нов групоид $(M_5 \setminus \{0\}, \otimes)$ (провери?). Дали ова е исполнето за групоидот $(M_4, \otimes)$? А за групоидите $(M_6, \otimes)$ и $(M_7, \otimes)$?

Со непосредна проверка добиваме дека на претходно опишаниот начин при $n = 7$ добиваме нов групоид $(M_7 \setminus \{0\}, \otimes)$, а при $n = 6$ не добиваме групоид. Јасно, Келиевите шеми на групоидите $(M_5 \setminus \{0\}, \otimes)$ и $(M_7 \setminus \{0\}, \otimes)$ се добиваат од Келиевите шеми на групоидите $(M_5, \otimes)$ и $(M_7, \otimes)$ со бришење на редот и колоната во кои главен елемент е 0. Сега лесно може да се провери дека групоидите $(M_5 \setminus \{0\}, \otimes)$ и $(M_7 \setminus \{0\}, \otimes)$ се комутативни групи.

Какви се броевите 5 и 7? На каков заклучок наведуваат претходните разгледувања? Провери го својот заклучок за $n = 11$!

в) Нека е дадено множеството A чии елементи се сите биекции од множеството $\{1, 2, 3\}$ во множеството $\{1, 2, 3\}$, а операцијата $\circ$ нека е композицијата на пресликувања. Ќе покажеме дека $(A, \circ)$ е група, но не е Абелова група.

Јасно, ако $f : \{1, 2, 3\} \to \{1, 2, 3\}$ и $g : \{1, 2, 3\} \to \{1, 2, 3\}$ се биекции, тогаш, композиција на биекции е биекција, што значи дека $(A, \circ)$ е групоид. Понатаму, за композицијата на пресликувања важи асоцијативниот закон, т.е. $(A, \circ)$ е полугрупа. Но, за идентичното пресликување I имаме дека важи $f \circ I = I \circ f = f$ за секој $f \in A$, што значи дека I е единица во полугрупата $(A, \circ)$. Конечно, инверзното пресликување на секоја биекција f е биекција, што значи дека секој елемент

f е инверзибилен. Значи, $(A,\circ)$ е полугрупа со единица во која секој елемент е инверзибилен, т.е. $(A,\circ)$ е група.

Лесно се наоѓа дека елементи на множеството A се биекциите:

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ f_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ f_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ f_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ f_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ f_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

Со непосредна проверка наоѓаме дека

$$f_2\circ f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=f_3,\ f_1\circ f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=f_4$$

што значи дека групата $(A,\circ)$ не е комутативна.

г) Нека n е природен број. Тогаш класите на конгруенција S на произволен редуциран систем на остатоци формираат комутативна група во однос на множење по модул n.

Навистина, ако $\mathrm{NZD}(a,n)=\mathrm{NZD}(b,n)=1$, тогаш $\mathrm{NZD}(ab,n)=1$, па затоа операцијата множење по модул n е добро дефинирана во множеството S. Јасно, операцијата множење по модул n е комутативна и асоцијативна во множеството S. Понатаму, од $\mathrm{NZD}(1,n)=1$ следува $1\in S$. Конечно, од $\mathrm{NZD}(a,n)=1$ и од теорема II 14.3 следува конгруенцијата дека $ax\equiv 1\,(\mathrm{mod}\,n)$ има единствено решение во множеството S, што значи дека секој елемент a има инверзен. ♦

5.4. Теорема. Секоја група е групоид со кратење.

Доказ. Нека $(G,*)$ е група, e е единица во G и со z^{-1} да го означиме инверзниот елемент на z. Ако $x*z=y*z$, тогаш,

$$x=x*e=x*(z*z^{-1})=(x*z)*z^{-1}=(y*z)*z^{-1}=y*(z*z^{-1})=y*e=y.$$

Аналогно се докажува дека од $z*x=z*y$ следува $x=y$, т.е. секоја група е групоид со кратење. ♦

5.5. Теорема. Нека $(G,*)$ е група и $a,b\in G$. Тогаш, постои единствен елемент $x\in G$ таков што $a*x=b$ и постои единствен елемент $y\in G$ таков што $y*a=b$.

Доказ. Нека e е неутралниот елемент на G. Со a^{-1} да го означиме инверзниот елемент на a и да го разгледаме елементот $x=a^{-1}*b$. Имаме

$$a*x=a*(a^{-1}*b)=(a*a^{-1})*b=e*b=b,$$

т.е. постои елемент $x\in G$ со саканото својство. Единствеността на елементот $x\in G$ следува од единствеността на инверзниот елемент a^{-1} и ако во $a*x=b$ помножиме од лево со a^{-1}.

Аналогно се докажува дека постои единствен елемент $y\in G$ таков што $y*a=b$. Навистина, да го разгледаме $y=b*a^{-1}$. Имаме

$$y*a=(b*a^{-1})*a=b*(a^{-1}*a)=b*e=b,$$

т.е. постои елемент $y\in G$ со саканото својство. Единствеността на елементот $y\in G$ следува од единствеността на инверзниот елемент a^{-1} и ако во $y*a=b$ помножиме од десно со a^{-1}. ♦

5.6. Забелешка. Непосредно од теорема 5.4 следува дека ако a е елемент од групата $(G,*)$ таков што $a*a=a$, тогаш $a=e$, т.е. a е единицата на групата $(G,*)$.

5.7. Дефиниција. За групоидот $(H,\bullet)$ ќе велиме дека е *подгрупа* од групата $(G,*)$ ако $H\subseteq G$, $x\bullet y=x*y$, за секои $x,y\in H$ и $(H,\bullet)$ е група.

5.8. Пример. а) Нека $(\mathbf{Z},+)$ е групата цели броеви во однос на операцијата собирање и $m\mathbf{Z}=\{mk\,|\,k\in\mathbf{Z}\}$. Лесно се докажува дека $(m\mathbf{Z},+)$ е подгрупа на групата $(\mathbf{Z},+)$.

б) Нека $(\mathbf{R},+)$ е групата реални броеви во однос на операцијата собирање. Групата $(\mathbf{Q},+)$ рационални броеви со операцијата собирање е подгрупа $(\mathbf{R},+)$.

в) Нека $(\mathbf{R}^+,\cdot)$ е групата позитивни реални броеви во однос на операцијата множење. Тогаш, $(\mathbf{Q}^+,\cdot)$ е подгрупа од $(\mathbf{R}^+,\cdot)$. ♦

5.9. Теорема. Непразното подмножество H на групата $(G,\cdot)$ е подгрупа ако и само ако $xy^{-1}\in H$, за секои $x,y\in H$.

Доказ. Нека претпоставиме дека H е подгрупа од G и нека $x,y\in H$. Тогаш, H го содржи инверзниот елемент на секој свој елемент, па затоа $y^{-1}\in H$. Но, $x\in H$ и $y^{-1}\in H$ па затоа $xy^{-1}\in H$.

Обратно, нека претпоставиме дека $xy^{-1}\in H$, за секои $x,y\in H$. Од $x\in H$ следува $e=xx^{-1}\in H$, т.е. H има единица. Понатаму, од $e,y\in H$ следува дека $y^{-1}=ey^{-1}\in H$, т.е. H ја содржи инверзијата на секој свој елемент. Конечно, ако $x,y\in H$, тогаш $y^{-1}\in H$, па затоа $xy=x(y^{-1})^{-1}\in H$, што значи дека H е подгрупа на G. ♦

5.10. Теорема. Нека $(G,\cdot)$ е полугрупа со единица e. Ако H се состои од сите инверзибилни елементи на G, тогаш $(H,\cdot)$ е потполугрупа на G и H е група.

Доказ. Според теорема 3.13 H е подгрупоид, па значи е потполугрупа на G. Понатаму, бидејќи единицата e на G е инверзибилна ($e^{-1}=e$) заклучуваме

дека $e \in H$, т.е. H е полугрупа со единица. Конечно, бидејќи за секој $a \in H$ важи $a^{-1} \in H$, т.е. секој елемент од H има инверзија заклучуваме дека H е група. ♦

5.11. Теорема. Ако $(G,\cdot)$ е група, тогаш и секој фактор групоид на G е група.

Доказ. Нека α е конгруенција на G. Ако G е група, тогаш според теоремите 4.16 и 3.6 б) $G_{|\alpha}$ е полугрупа со единица C_e, каде e е единицата на G. Понатаму, за секој $a \in G$ важи $C_a C_{a^{-1}} = C_{aa^{-1}} = C_e$, од каде следува дека секој елемент на $G_{|\alpha}$ е инверзибилен, што значи дека $G_{|\alpha}$ е група. ♦

5.12. Степени со цели експоненти. Нека $(G,\cdot)$ е мултипликативно означена полугрупа со единица e. Ако a е инверзибилен елемент во G и $n \in \mathbf{N}$, тогаш a^{-n} го определуваме со:

$$a^{-n} = (a^{-1})^n .$$

Според тоа, ако a е инверзибилен елемент во G, тогаш за секој цел број n е определен степенот a^n. Понатаму, ако G е група, тогаш секој елемент е инверзибилен, што значи дека за секој цел број n и за секој $a \in G$ важи $a^n \in G$. Притоа, како и претходно елементот a^n го нарекуваме *степен* со основа a и *степенов показател* (*експонент*) n. Притоа, ако G е група, тогаш

$$a^n a^m = a^{m+n},\ (a^n)^m = a^{mn},\ a^n a^{-n} = e = a^0,\ (a^{-n})^{-1} = a^n ,$$

за секои $a \in G$, $m,n \in \mathbf{Z}$. Според тоа, ако $A = \{a^n \mid n \in \mathbf{Z}\}$, тогаш $A \subseteq G$ и A е подгрупа од G, за која ќе велиме дека е *генерирана* од елементот $a \in G$. Понатаму, ако групата G е комутативна , тогаш

$$(ab)^n = a^n b^n , \text{ за секои } a,b \in G \text{ и } n \in \mathbf{Z},$$

Во случај на адитивно означена комутативна група $(G,+)$ наместо a^n пишуваме na. Според тоа, во овој случај, имаме

$$ma + na = (m+n)a,\ m(na) = (mn)a,\ m(a+b) = ma + mb,$$
$$ma - na = (m-n)a,\ ma - mb = (m-n)b,\ 1a = a,\ (-1)a = -a,\ 0a = 0,$$

за секои $a,b \in G$ и $m,n \in \mathbf{Z}$. ♦

6. КОНЕЧНИ ГРУПИ

6.1. Дефиниција. Бројот на елементите на една група G, во ознака $|G|$, го нарекуваме *ред на групата* G. Ако $|G|$ е конечен број, тогаш за групата G ќе велиме дека е *конечна*.

6.2. Пример. Во пример 4.3 в) разгледавме една некомутативна група. Овде ќе забележиме дека тоа всушност е наједноставната некомутативна група, која има ред 6. Ако ги поедноставиме ознаките, тогаш нејзината Келиева шема е следнава:

	1	***a***	***b***	***c***	***d***	***e***
1	1	*a*	*b*	*c*	*d*	*e*
a	*a*	*b*	1	*e*	*c*	*d*
b	*b*	1	*a*	*d*	*e*	*c*
c	*c*	*d*	*e*	1	*a*	*b*
d	*d*	*e*	*c*	*b*	1	*a*
e	*e*	*c*	*d*	*a*	*b*	1

.♦

6.3. Ако G е конечна група и $a \in G$, тогаш и подгрупата A од G генерирана од a е конечна, што значи постојат $m, n \in \mathbf{Z}$, $m \neq n$ такви што $a^m = a^n$. Но, тогаш $a^n a^{-m} = a^m a^{-m} = 1$, т.е. $a^{n-m} = 1, m - n \neq 0$. Слично се покажува дека $a^{m-n} = 1, m - n \neq 0$. Нека r е најмалиот природен број со својство $a^r = 1$. Од теоремата за делење со остаток имаме дека за секој $m \in \mathbf{Z}$ важи $m = kr + t$, $k \in \mathbf{Z}$, $t \in \{0,1,2,...,r-1\}$. Значи, за секој $m \in \mathbf{Z}$ важи

$$a^m = a^{kr+t} = (a^r)^k a^t = a^t \in \{1, a, a^2, ..., a^{r-1}\}.$$

Според тоа, $A = \{1, a, a^2, ..., a^{r-1}\}$, па затоа редот на A е r, кој уште го нарекуваме *ред на елементот* a.

6.4. Теорема (Лагранж). Ако G е конечна група со ред n и $a \in G$, тогаш $a^n = 1$.

Доказ. Нека r е редот на a. Тогаш $A = \{1, a, a^2, ..., a^{r-1}\}$ е подгрупа од G и уште повеќе таа е комутативна. Ако $r = n$, тогаш $a^n = 1$. Затоа, нека $r \neq n$. Ако $b \in G \setminus A$, тогаш сите елементи $b, ba, ba^2, ..., ba^{r-1}$ се различни меѓу себе и притоа секој од нив е различен од секој елемент од A. Навистина, бидејќи секоја група е групоид со кратење, од $ba^i = ba^j$, за $0 \leq i < j < r$, добиваме $a^i = a^j$, т.е. $a^{i-j} = 1$, од што следува дека редот на a е помал од r, а ако $ba^i = a^j$, за $0 \leq i \neq j < r$ добиваме $b = a^{j-i} \in A$, што е противречност. Нека $B = \{b, ba, ba^2, ..., ba^{r-1}\}$. Ако $G = A \cup B$, тогаш од принципот на збир следува $n = |A| + |B| = 2r$, па затоа $a^n = a^{2r} = (a^r)^2 = 1$. Ако $G \neq A \cup B$, тогаш постои $c \in G \setminus (A \cup B)$. Аналогно се докажува дека сите елементи $c, ca, ca^2, ..., ca^{r-1}$ се различни меѓу себе и дека $C \cap (A \cup B) = \varnothing$, каде $C = \{c, ca, ca^2, ..., ca^{r-1}\}$. Продолжувајќи ја постапката, која заради конечноста на групата G мора да заврши после конечен број чекори, наоѓаме дека $G = A \cup B \cup C \cup ... \cup H$, каде $|A| = |B| = |C| = ... = |H| = r$ и сите множества

во претходната унија се по парови заемно дисјунктни. Ако такви множества има k, тогаш $n = |G| = kr$, па затоа $a^n = a^{kr} = (a^r)^k = 1^k = 1$. ♦

6.5. Последица. Ако $|G| = n$ и $a \in G$ има ред r, тогаш $r \mid n$.

Доказ. Нека редот на $a \in G$ е r и нека $A = \{1, a, a^2, ..., a^{r-1}\}$ е подгрупата од G во доказот на теоремата на Лагранж. Од доказот на теоремата на Лагранж следува дека постои $k \in \mathbf{N}$ таков што $n = |G| = kr$, па значи $r \mid n$. ♦

7. ХОМОРФИЗМИ, ИЗОМОРФИЗМИ И ДИРЕКТНИ ПРОИЗВОДИ НА ГРУПИ

7.1. Ако ги разгледаме Келиевите шеми на групите $(M_4, \oplus)$ и $(M_5^*, \otimes)$ за која Келиевата шема е:

$\otimes$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

можеме да забележиме дека ако во втората шема замениме секаде 1 со 0, 2 со 1, 4 со 2, тогаш ќе ја добиеме првата шема. Со други зборови, можеме да речеме дека групата $(M_5^*, \otimes)$ е всушност друг запис на групата $(M_4, \oplus)$. Ваквите групи ги нарекуваме изоморфни групи.

7.2. Дефиниција. Нека G и H се две групи. За пресликувањето $f : G \to H$ ќе велиме дека е *хомоморфизам* од G во H ако за секои $a, b \in G$ важи $f(ab) = f(a) f(b)$. Ако хомоморфизмот $f : G \to H$ е биекција, тогаш ќе велиме дека f е *изоморфизам* од G во H.

7.3. Лема. а) Ако $f : G \to H$ е хоморфизам од групата $(G, *)$ во групата $(H, \bullet)$, тогаш $f(e) = e'$, каде e е единицата во G, а e' е единицата во H.

б) Ако $f : G \to H$ е хомоморфизам од групата $(G, *)$ во групата $(H, \bullet)$, тогаш за секој $a \in G$ важи $f(a^{-1}) = (f(a))^{-1}$.

в) Ако $(G, *)$ е група, тогаш секој групоид $(H, \bullet)$ изоморфен со G е група.

Доказ. а) Ако во равенството $f(e) = f(e * e) = f(e) \bullet f(e)$ помножиме со $(f(e))^{-1}$ добиваме $f(e) = e'$.

б) Од $e' = f(e) = f(a * a^{-1}) = f(a) \bullet f(a^{-1})$ следува $f(a^{-1}) = (f(a))^{-1}$.

в) Ако G е група, тогаш според теоремите 2.7 и 3.15 H е полугрупа со единица $e' = f(e)$, каде e е единицата на G. Значи, останува да покажеме дека секој елемент $a' \in H$ е инверзибилен во H. Навистина, ако $a' = f(a)$, тогаш имаме

$$a' \bullet f(a^{-1}) = f(a) \bullet f(a^{-1}) = f(a * a^{-1}) = f(e) = e',$$

од што следува дека $f(a^{-1})$ е инверзија на $f(a)$ во H. ♦

7.4. Пример. Да ги разгледаме групите $(M_4, \oplus)$ и $(M_5^*, \otimes)$. Лесно се гледа дека со

$$f(1) = 0,\ f(2) = 1,\ f(4) = 2 \text{ и } f(3) = 3$$

е дефиниран изоморфизам $f : M_5^* \to M_4$.

Понатаму, со

$$g(0) = 1, g(1) = 2, g(2) = 4, g(3) = 3$$

е дефиниран изоморфизам $g : M_4 \to M_5^*$. ♦

7.5. Дефиниција. Нека $f : G \to H$ е хомоморфизам. Множеството $\{x \mid x \in G,\ f(x) = e'\}$, каде $e \in H$ е единичниот елемент, го нарекуваме *јадро* на f и го означуваме со $\ker f$.

7.6. Теорема. Ако $f : G \to H$ е хомоморфизам, тогаш $\ker f$ е подгрупа од G.

Доказ. Од дефиницијата на $\ker f$ следува дека $\ker f \subseteq G$. Нека $a, b \in \ker f$. Тогаш

$$f(a * b) = f(a) \bullet f(b) = e' \bullet e' = e',$$

т.е. $ab \in \ker f$, т.е. $\ker f$ е подгрупоид од G. Понатаму, според теорема 2.2 $\ker f$ е полугрупа, а според лема 6.3 имаме дека $e \in \ker f$. Конечно, ако $a \in \ker f$, тогаш

$$e' = f(e) = f(a * a^{-1}) = f(a) \bullet f(a^{-1}) = e' \bullet f(a^{-1}) = f(a^{-1}),$$

од што следува $a^{-1} \in \ker f$, т.е. $\ker f$ е подгрупа од G. ♦

7.7. Лема. Хомоморфизмот $f : G \to H$ е инјекција ако и само ако $\ker f = \{e\}$.

Доказ. Нека f е инјекција и $a \in \ker f$, т.е. $f(a) = e'$. Но, $f(e) = e'$, па затоа $f(a) = f(e)$ и како f е инјекција добиваме $a = e$, т.е. $\ker f = \{e\}$.

Обратно, нека $\ker f = \{e\}$ и нека $f(x) = f(y)$. Тогаш,

$$f(x * y^{-1}) = f(x) \bullet f(y^{-1}) = f(y) \bullet f(y^{-1}) = f(y * y^{-1}) = f(e) = e'$$

па затоа $x*y^{-1} \in \ker f = \{e\}$, т.е. $xy^{-1} = e$ од што следува $x = y$. Според тоа, f е инјекција. ♦

7.8. Теорема. Нека G и H се две групи и нека на множеството $G \times H$ дефинираме операција со:

$$(a,c)\bullet(b,d) = (ab,cd).$$

Тогаш $G \times H$ со оваа операција е група, која ја нарекуваме *директен производ* на групите G и H. Притоа, ако и двете групи G и H се комутативни, тогаш и групата $G \times H$ е комутативна.

Доказ. За секои $a,b \in G$ и $c,d \in H$ важи $ab \in G$ и $cd \in H$, па затоа $(a,c)\bullet(b,d) \in G \times H$, т.е. $(G \times H, \bullet)$ е групоид.

Ако $a,b,c \in G$ и $d,e,f \in H$, тогаш

$$((a,d)\bullet(b,e))\bullet(c,f) = (ab,de)\bullet(c,f) = (abc,def) = (a,d)\bullet(bc,ef) = (a,b)\bullet((b,e)\bullet(c,f)),$$

т.е. $(G \times H, \bullet)$ е полугрупа.

Нека $e \in G$ и $e' \in H$ се единичните елементи во G и H. Тогаш, за секој $(a,b) \in G \times H$ важи

$$(e,e')\bullet(a,b) = (ea,e'b) = (a,b) = (ae,be') = (a,b)\bullet(e,e'),$$

т.е. (e,e') е единичен елемент во $G \times H$. Конечно, ако $(a,b) \in G \times H$, тогаш $(a^{-1},b^{-1}) \in G \times H$ и притоа важи

$$(a,b)\bullet(a^{-1},b^{-1}) = (aa^{-1},bb^{-1}) = (e,e') = (a^{-1}a,b^{-1}b) = (a^{-1},b^{-1})\bullet(a,b),$$

т.е. (a^{-1},b^{-1}) е инверзен елемент на (a,b) во $G \times H$. Според тоа, $(G \times H, \bullet)$ е група.

Нека G и H се комутативни групи. Тогаш за секои $(a,b);(c,d) \in G \times H$ важи

$$(a,b)\bullet(c,d) = (ac,bd) = (ca,db) = (c,d)\bullet(a,b),$$

т.е. групата $(G \times H, \bullet)$ е комутативна. ♦

8. ЦИКЛИЧНИ И КОНЕЧНИ АБЕЛОВИ ГРУПИ

8.1. Дефиниција. За групата G ќе велиме дека е *циклична* ако постои $a \in G$ таков што $G = \{a^n \mid n \in \mathbf{Z}\}$. Ако за секој $n \in \mathbf{Z} \setminus \{0\}$ важи $a^n \neq 1$, тогаш за G ќе велиме дека е *бесконечна циклична група*. Во спротивно ќе велиме дека G е *конечна циклична група*.

8.2. Коментар. Нека G е бесконечна циклична група. Пресликувањето $f : G \to \mathbf{Z}$ дефинирано со $f(a^n) = n$ е изоморфизам од G во $(\mathbf{Z},+)$. Според тоа, $(\mathbf{Z},+)$ е бесконечна циклична група.

Ако G е конечна циклична група со ред r, тогаш $G=\{1,a,...,a^{r-1}\}$ и таа е комутативна. Конечната циклична група со ред r ќе ја означуваме со C_r. Очигледно, пресликувањето $f:C_r\to M_r$ е изоморфизам од групата C_r во групата $(M_r,\oplus)$. Во натамошните разгледувања за групата $(M_r,\oplus)$ ќе ја користиме ознаката $(\mathbf{Z}_r,\oplus)$.

8.3. Теорема. Нека $m,n\in\mathbf{N}$ и $\mathrm{NZD}(m,n)=1$. Тогаш $\mathbf{Z}_n\times\mathbf{Z}_m=\mathbf{Z}_{mn}$, т.е. $C_n\times C_m=C_{mn}$.

Доказ. Нека $C_n=\{1,a,...,a^{n-1}\}$, $C_m=\{1,b,...,b^{m-1}\}$ и $G=C_n\times C_m$. Бидејќи редот на групата C_n е n и редот на групата C_m е m, добиваме дека редот на групата G е mn. Според тоа, редот r на елементот $(a,b)\in G$ е делител на mn. Понатаму, од

$$(a^r,b^r)=(a,b)^r=(1,1)$$

следува $a^r=1$ и $b^r=1$, па затоа редот n на a е делител на r и редот m на b е делител на r. Нека $r=np=mq$. Од $\mathrm{NZD}(m,n)=1$ и $np=mq$ следува $n\mid q$ и $m\mid p$. Понатаму, бидејќи $r\mid mn$ добиваме $np\mid mn$ и $mq\mid mn$, т.е. $p\mid m$ и $q\mid n$, што заедно со $m\mid p$ и $n\mid q$ дава $n=q$ и $m=p$. Конечно, од $r=np=mq$ следува $r=nm$, т.е. редот на $(a,b)\in G$ е еднаков на mn, па значи $G=C_n\times C_m$ е циклична група со ред mn, т.е. $C_n\times C_m=C_{mn}$. ♦

8.4. Теорема. Ако $C_n\times C_m=C_{mn}$, тогаш $\mathrm{NZD}(m,n)=1$.

Доказ. Нека $\mathrm{NZD}(m,n)=d\neq 1$. Тогаш $n=pd, m=qd$ и $pqd<mn$. Ако $(a,b)\in C_n\times C_m$, тогаш

$$(a,b)^{pqd}=(a^{pqd},b^{pqd})=((a^{pd})^q,(b^{qd})^p)=((a^n)^q,(b^m)^p)=(1^q,1^p)=(1,1),$$

од што следува дека секој елемент на $G=C_n\times C_m$ има ред помал од mn, што противречи на претпоставката дека $C_n\times C_m=C_{mn}$. ♦

8.5. Следнава теорема која нема да ја докажуваме дава карактеризација на конечните комутативни групи.

Теорема. Секоја конечна комутативна група G е изоморфна со директен производ на конечни циклични групи, чии редови се степени на прости броеви. Притоа, низата од степените на тие прости броеви е единствена за G, со точност до пермутација на нејзините елементи, т.е. ако

$$G=\mathbf{Z}_{p_1^{a_1}}\times\mathbf{Z}_{p_2^{a_2}}\times...\times\mathbf{Z}_{p_k^{a_k}}=\mathbf{Z}_{q_1^{b_1}}\times\mathbf{Z}_{q_2^{b_2}}\times...\times\mathbf{Z}_{q_s^{b_s}},$$

каде $p_i, i=1,2,...,k$ и $q_j, j=1,2,...,s$ се прости броеви, тогаш $k=s$ и $(q_1^{b_1},q_2^{b_2},...,q_s^{b_s})$ е пермутација на $(p_1^{a_1},p_2^{a_2},...,p_k^{a_k})$. ♦

8.6. Дефиниција. Степените на простите броеви од теорема 8.5 ги нарекуваме *елементарни делители на групата* G.

8.7. Пример. Бројот на неизоморфните Абелови групи со ред 24 е три, бидејќи $24 = 2\bullet 2\bullet 2\bullet 3$ може да се запише како

$$8\bullet 3,\ 4\bullet 2\bullet 3 \text{ и } 2\bullet 2\bullet 2\bullet 3 .$$

Тие групи се

$$\mathbf{Z}_8 \times \mathbf{Z}_3 = \mathbf{Z}_{24},\ \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_3 = \mathbf{Z}_2 \times \mathbf{Z}_{12} = \mathbf{Z}_4 \times \mathbf{Z}_6 \text{ и}$$
$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 = \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_6 . \blacklozenge$$

8.8. Пример. Бројот на неизоморфните Абелови групи со ред 36 е 4, бидејќи 36 може да се запише како

$$2\bullet 2\bullet 3\bullet 3,\ 2^2\bullet 3^2,\ 2^2\bullet 3\bullet 3 \text{ и } 2\bullet 2\bullet 3^2 .$$

Тие групи се

$$\mathbf{Z}_4 \times \mathbf{Z}_9 = \mathbf{Z}_{36},\ \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 = \mathbf{Z}_6 \times \mathbf{Z}_6 = \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_6 ,$$
$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_9 = \mathbf{Z}_2 \times \mathbf{Z}_{18} \text{ и } \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_3 = \mathbf{Z}_3 \times \mathbf{Z}_{12} . \blacklozenge$$

8.9. Пример. Дали се изоморфни групите:

а) $\mathbf{Z}_4 \times \mathbf{Z}_{15}$ и $\mathbf{Z}_6 \times \mathbf{Z}_{10}$,

б) $\mathbf{Z}_6 \times \mathbf{Z}_{60}$ и $\mathbf{Z}_{12} \times \mathbf{Z}_{30}$.

Решение. а) Имаме

$$\mathbf{Z}_4 \times \mathbf{Z}_{15} = \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \text{ и } \mathbf{Z}_6 \times \mathbf{Z}_{10} = \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_5$$

но $\mathbf{Z}_4$ и $\mathbf{Z}_2 \times \mathbf{Z}_2$ не се изоморфни, па затоа и разгледуваните групи не се изоморфни.

б) Имаме

$$\mathbf{Z}_6 \times \mathbf{Z}_{60} = (\mathbf{Z}_2 \times \mathbf{Z}_3) \times (\mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_5) = (\mathbf{Z}_3 \times \mathbf{Z}_4) \times (\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5) = \mathbf{Z}_{12} \times \mathbf{Z}_{30} ,$$

т.е. разгледуваните групи се изоморфни. $\blacklozenge$

8.10. Во дефиниција II 19.2 го воведовме поимот ред на бројот a по модул n, како најмалиот природен број k таков што $a^k \equiv 1 (\mathrm{mod}\, n)$. На крајот од овој дел во врска со редот на бројот a по модул n ќе докажеме едно важно тврдење. Така ја имаме следнава дефиниција.

Дефиниција. Нека $n \in \mathbf{N}$ и нека $\mathrm{NZD}(a, n) = 1$. Ако редот на елементот a по модул n е еднаков на $\varphi(n)$, тогаш ќе велиме дека a е *примитивен корен на* n.

8.11. Теорема. Ако a е примитивен корен од n, тогаш $\{a, a^2, ..., a^{\varphi(n)}\}$ е редуциран систем на остатоци по модул n, т.е. е конечна циклична група.

Доказ. Според дефиниција 8.10 имаме $\text{NZD}(a,n)=1$. Оттука следува дека $\text{NZD}(a^i,n)=1$, за секој $1\le i\le \varphi(n)$. Понатаму, од теорема II 19.3 следува дека броевите a^i, $i\in\{1,2,...,\varphi(n)\}$ не се меѓусебно конгруентни. Бидејќи имаме само $\varphi(n)$ природни броеви помали од n кои се заемно прости со n, заклучуваме дека елементите на множеството $\{a,a^2,...,a^{\varphi(n)}\}$ мора да се конгруентни со нив. Според тоа, $\{a,a^2,...,a^{\varphi(n)}\}$ е редуциран систем на остатоци по модул n, па од пример 4.3 г) следува дека тој е група. Јасно, оваа група е циклична. ♦

На крајот од оваа точка без доказ ќе наведеме некои својства на примитивните корени:

a) Нека p е прост број. Имаме точно $\varphi(p-1)$ примитивни корени на p.

b) Ако m и n се заемно прости природни броеви поголеми од 2, тогаш бројот mn нема примитивни корени.

c) Природниот број $2^k m$, каде $k>1$ и m е непарен цел број нема примитивни корени.

d) Постојат примитивни корени од 2^n ако и само ако n е природен број помал од 3.

e) Ако p непарен прост број, тогаш p^k има примитивен корен за секој $k\in\mathbf{N}$.

9. СТРУКТУРА НА ГРУПАТА S_n

9.1. Нека со S_n го означиме множеството од сите природни броеви помали од n и заемно прости со n, т.е

$$S_n=\{m\mid m\in\mathbf{N},\ m<n,\ \text{NZD}(m,n)=1\}.$$

Во S_n дефинираме операција $\otimes$ на следниов начин:

$$\text{ако } k,p\in S_n, \text{ тогаш } k\otimes p=m \text{ ако } kp\equiv m(\text{mod } n),$$

т.е. $\otimes$ е множење со модул n.

9.2. Лема. $(S_n,\otimes)$ е комутативна група со ред $\varphi(n)$.

Доказ. Множеството S_n е редуциран систем на остатоци по модул n, па затоа бројот на неговите елементи е $\varphi(n)$.

Операцијата $\otimes$ е добро дефинирана. Навистина, лесно се гледа дека од $\text{NZD}(k,n)=1$ и $\text{NZD}(p,n)=1$ следува $\text{NZD}(kp,n)=1$, па од теорема II 16.9 следува дека kp е конгруентен, по модул n, со единствен елемент m од S_n.

Исполнетоста на асоцијативниот, односно комутативниот закон непосредно следува од следниве конгруенции

$$(kp)r \equiv k(pr)(\mathrm{mod}\, n) \text{ и } kp \equiv pk(\mathrm{mod}\, n),$$

соодветно.

Бројот 1 е очигледно единечен елемент на $(S_n, \otimes)$.

Нека $m \in S_n = \{m_1, m_2, ..., m_{\varphi(n)}\}$. Аналогно како во доказот на теорема II 16.4 може да се докаже дека броевите $mm_1, mm_2, ..., mm_{\varphi(n)}$ формираат редуциран систем на остатоци по модул n, а според теорема II 16.9 секој од нив е конгруентен со еден и единствен елемент од S_n. Освен тоа, ако $mm_i \equiv m'(\mathrm{mod}\, n)$ и $mm_j \equiv m'(\mathrm{mod}\, n)$, тогаш $n \mid m(m_i - m_j)$, т.е. $n \mid (m_i - m_j)$. Но, тоа значи $m_i = m_j$. Според тоа, за секој $m' \in S_n$ постои единствен $m_i \in S_n$ таков што $mm_i \equiv m'(\mathrm{mod}\, n)$, односно $m \otimes m_i = m'$. Значи, постои $m_k \in S_n$ таков што $m \otimes m_k = 1$, т.е. $m^{-1} = m_k$ и од произволноста на $m \in S_n$ следува дека секој елемент на S_n има инверзен.

Конечно, $(S_n, \otimes)$ е комутативна група со ред $\varphi(n)$. ♦

9.3. Структурата на групата S_n е определена со следнава теорема, чиј доказ заради тежината нема да го презентираме.

Теорема. Ако $n = 2^a p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$, $p_i > 2$, за $i = 1, 2, ..., s$ се прости броеви, тогаш

- ако $a \geq 3$, тогаш $S_n = \mathbf{Z}_2 \times \mathbf{Z}_{2^{a-2}} \times \mathbf{Z}_{p_1^{a_1} - p_1^{a_1 - 1}} \times ... \times \mathbf{Z}_{p_s^{a_s} - p_s^{a_s - 1}}$,
- ако $a = 2$, тогаш $S_n = \mathbf{Z}_2 \times \mathbf{Z}_{p_1^{a_1} - p_1^{a_1 - 1}} \times ... \times \mathbf{Z}_{p_s^{a_s} - p_s^{a_s - 1}}$,
- ако $a \in \{0, 1\}$, тогаш $S_n = \mathbf{Z}_{p_1^{a_1} - p_1^{a_1 - 1}} \times ... \times \mathbf{Z}_{p_s^{a_s} - p_s^{a_s - 1}}$. ♦

9.4. Забелешка. Всушност структурата на групата S_n се определува на следниов начин. Ако $n = 2^a p_1^{a_1} p_2^{a_2} ..., p_s^{a_s}$, тогаш

$$\varphi(n) = 2^{a-1}(p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1})...(p_s^{a_s} - p_s^{a_s - 1})$$

и ако $a \geq 3$, тогаш факторот 2^{a-1} го запишуваме во видот $2 \cdot 2^{a-2}$, а ако $a \leq 2$, тогаш ништо не се менува. Сега, бројот $\varphi(n)$ е запишан како производ на броеви $a_1, a_2, ..., a_t$, па затоа $S_n = \mathbf{Z}_{a_1} \times \mathbf{Z}_{a_2} \times ... \times \mathbf{Z}_{a_t}$.

9.5. Пример. Определете ја структурата на групата S_n, ако

а) $n = 4$, б) $n = 15$, в) $n = 16$,

г) $n=17$, д) $n=24$, ѓ) $n=63$.

Решение. а) $\varphi(4)=\varphi(2^2)=2$, па затоа $S_4=\mathbf{Z}_2$.

б) $\varphi(15)=\varphi(3\cdot 5)=\varphi(3)\varphi(5)=2\cdot 4$, па затоа $S_{15}=\mathbf{Z}_2\times\mathbf{Z}_4$.

в) $\varphi(16)=\varphi(2^4)=2\cdot 2^2$, па затоа $S_{16}=\mathbf{Z}_2\times\mathbf{Z}_4$.

г) $\varphi(17)=16$, па затоа $S_{17}=\mathbf{Z}_{16}$.

д) $\varphi(24)=\varphi(2^3\cdot 3)=2\cdot 2\cdot 2$, па затоа $S_{24}=\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$.

ѓ) $\varphi(63)=\varphi(3^2\cdot 7)=6\cdot 6$, па затоа $S_{63}=\mathbf{Z}_6\times\mathbf{Z}_6$. ♦

9.6. Пример. Дали групите S_{104} и S_{105} се изоморфни.

Решение. Од $\varphi(104)=\varphi(2^3\cdot 13)=2\cdot 2\cdot 12$ и $\varphi(105)=\varphi(3\cdot 5\cdot 7)=2\cdot 4\cdot 6$ следува

$$\begin{aligned} S_{104}&=\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_{12}=\mathbf{Z}_2\times\mathbf{Z}_2\times(\mathbf{Z}_3\times\mathbf{Z}_4)\\ &=\mathbf{Z}_2\times(\mathbf{Z}_2\times\mathbf{Z}_3)\times\mathbf{Z}_4=\mathbf{Z}_2\times\mathbf{Z}_6\times\mathbf{Z}_4=S_{105}\end{aligned}$$

т.е. групите S_{104} и S_{105} се изоморфни. ♦

9.7. Пример (Гаус). Најдете ги сите природни броеви n за кои групата S_n е циклична.

Решение. Нека $n=2^a p_1^{a_1}p_2^{a_2}...,p_s^{a_s}$, $p_i>2$, за $i=1,2,...,s$ се прости броеви. Ќе докажеме дека ако $s\geq 2$, тогаш групата S_n не е циклична. Навистина, ако $s\geq 2$, тогаш факторите $p_1^{a_1}-p_1^{a_1-1}$ и $p_2^{a_2}-p_2^{a_2-1}$ не се заемно прости, па затоа $S_n\neq\mathbf{Z}_{\varphi(n)}$. Нека $s\leq 1$. За $s=1$ факторот $p_1^{a_1}-p_1^{a_1-1}$ е парен, па ако $a\geq 2$, тогаш $\varphi(n)$ го запишуваме како производ на два или три парни броеви, што значи дека групата S_n не е циклична. Лесно се докажува дека за $s=1$ и $a\in\{0,1\}$ групата S_n е циклична. Нека претпоставиме дека $s=0$, т.е. $n=2^a$. Ако $a\geq 3$, тогаш $\varphi(n)=2\cdot 2^{a-2}$ и групата S_n не е циклична. Понатаму, за $a=2$ групата S_4 е циклична, а случајот $n=2$ е тривијален. ♦

10. ПЕРМУТАЦИОНИ ГРУПИ

10.1. Да ги разгледаме пермутациите без повторување на множеството $X=\{1,2,...,n\}$. Од дефиниција IV 9.11 непосредно следува дека множеството пермутации без повторување на X се совпаѓа со множеството биекции од X во X. Понатаму, секоја пермутација $p:X\to X$ можеме да ја претставиме со помош на

$2\times n$ табела, при што во првиот ред се дадени елементите на множеството X, а во вториот ред се дадени сликите на елементите, соодветно, т.е.

$$p=\begin{bmatrix} 1 & 2 & \ldots & n \\ p(1) & p(2) & \ldots & p(n) \end{bmatrix}.$$

Но, според теорема IV 9.12 бројот на пермутациите p на множеството X е еднаков на $n!$. Нека во множеството

$$P_n=\{p \mid p \text{ е пермутација на } X\}$$

воведеме множење на елементи дефинирано како производ (композиција) на пресликувања. Според теорема IV 4.9 композиција на пермутации е пермутација, што значи дека $(P_n,\circ)$ е групоид. Понатаму, од теорема IV 3.9 следува дека $(P_n,\circ)$ е полугрупа со единица, а од теорема IV 4.13 следува дека секој елемент на P_n е инверзибилен, што значи дека $(P_n,\circ)$ е група.

Групата $(P_n,\circ)$ ја нарекуваме *симетрична група* од $n-$ти ред и истата ќе ја означуваме со E_n. Јасно, редот на групата E_n е $n!$.

10.2. Пример. Нека $X=\{1,2,3,4,5\}$. Производот на пермутациите

$$p_1=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{bmatrix} \text{ и } p_2=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{bmatrix}$$

е пермутацијата

$$p_2\circ p_1=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{bmatrix}.$$

Понатаму,

$$p_1^{-1}=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{bmatrix} \text{ и } p_2^{-1}=\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{bmatrix}. \blacklozenge$$

10.3. Теорема (Кели). Секоја конечна група е изоморфна со некоја група пермутации.

Доказ. Нека е дадена конечната група $(G,\circ)$ каде $G=\{x_1,\ldots,x_n\}$. За секој $x_i\in G$ ќе ја формираме пермутацијата p_{x_i} на множеството G дефинирана на следниов начин

$$p_{x_i}=\begin{bmatrix} x_1 & x_2 & \ldots & x_n \\ x_1\circ x_i & x_2\circ x_i & \ldots & x_n\circ x_i \end{bmatrix}.$$

Нека $P_G=\{p_{x_i} \mid x_i\in G\}$. Структурата $(P_G,\circ)$, каде со $\circ$ е означена композицијата на пресликувања, е изоморфна на групата $(G,\circ)$, бидејќи пресликувањето $f:G\to P_G$ дефинирано со $f(x)=p_x$ е изоморфизам. Навистина, f е биекција и важи

$$f(x_i \circ x_j) = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ x_1 \circ x_i \circ x_j & x_2 \circ x_i \circ x_j & \dots & x_n \circ x_i \circ x_j \end{bmatrix}$$
$$= \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ x_1 \circ x_i & x_2 \circ x_i & \dots & x_n \circ x_i \end{bmatrix} \circ \begin{bmatrix} x_1 \circ x_i & x_2 \circ x_i & \dots & x_n \circ x_i \\ x_1 \circ x_i \circ x_j & x_2 \circ x_i \circ x_j & \dots & x_n \circ x_i \circ x_j \end{bmatrix}$$
$$= \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ x_1 \circ x_i & x_2 \circ x_i & \dots & x_n \circ x_i \end{bmatrix} \circ \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ x_1 \circ x_j & x_2 \circ x_j & \dots & x_n \circ x_j \end{bmatrix}$$
$$= f(x_i) \circ f(x_j),$$

т.е. $(P_G, \circ)$ е група пермутации изоморфна на конечната група $(G, \circ)$. ♦

10.4. Пример. Пермутацијата $p_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$ ги заменува местата на броевите 1 и 3. Геометриски гледано, таа ја опишува симетријата на квадратот околу дијагоналата низ темињата 2 и 4. Слично, пермутацијата $p_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}$ ги заменува местата на 2 и 4. Понатаму, пермутацијата $p_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$ ја опишува симетријата на квадратот околу хоризонталната права која минува низ средината на квадратот, а пермутацијата $p_4 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$ ја опишува симетријата на квадратот околу вертикалната права која минува низ средината на квадратот. Нека

$$\rho_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \ \rho_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \text{ и } \rho_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}.$$

Лесно се гледа дека ρ_1, ρ_2 и ρ_3 го ротираат квадратот во насока на стрелките на часовникот за $90^\circ, 180^\circ$ и 270°, соодветно. Ако со I ја означиме идентичната пермутација тогаш со множење на елементите

$$I, p_1, p_2, p_3, p_4, \rho_1, \rho_2, \rho_3$$

ја добиваме следнава Келиева шема:

$\circ$	I	ρ_1	ρ_2	ρ_3	p_1	p_2	p_3	p_4
I	I	ρ_1	ρ_2	ρ_3	p_1	p_2	p_3	p_4
ρ_1	ρ_1	ρ_2	ρ_3	I	p_3	p_4	p_2	p_1
ρ_2	ρ_2	ρ_3	I	ρ_1	p_2	p_1	p_4	p_3
ρ_3	ρ_3	I	ρ_1	ρ_2	p_4	p_3	p_1	p_2
p_1	p_1	p_4	p_2	p_3	I	ρ_2	ρ_3	ρ_1
p_2	p_2	p_3	p_1	p_4	ρ_2	I	ρ_1	ρ_3
p_3	p_3	p_1	p_4	p_2	ρ_1	ρ_3	I	ρ_2
p_4	p_4	p_2	p_3	p_1	ρ_3	ρ_1	ρ_2	I

Оваа група ја нарекуваме *октална група* или *група симетрии на квадратот.* Множеството $H = \{I, \rho_1, \rho_2, \rho_3\}$ е подгрупа на октална група. ♦

10.5. Теорема. Нека A е конечно множество со n елементи и со P_n да ја означиме групата пермутации над множеството A, која содржи $n!$ елементи. За фиксна пермутација p дефинираме релација α над A така што $a\alpha b$ ако и само ако $b = p^k(a)$ за некој $k > 0$.

Релацијата α е релација на еквиваленција над A.

Доказ. Групата $(P_n, \circ)$ е конечна, па од последица 5.5 следува дека постои $m \le n$ таков што $p^m = 1$. Затоа, $p^m(a) = a$, т.е. $a\alpha a$, за секој $a \in A$. Значи релацијата α е рефлексивна. Нека $a\alpha b$, т.е. $b = p^k(a)$ за некој $k > 0$. Бидејќи $p^k p^{m-k} = 1$ добиваме дека p^{m-k} е инверзен на p^k, т.е. важи $p^{m-k}(b) = a$, што значи $b\alpha a$. Значи релацијата α е симетрична. Нека $a\alpha b$ и $b\alpha c$. Тогаш $b = p^k(a)$ за некој $k > 0$ и $c = p^i(b)$ за некој $i > 0$. Според тоа, $c = p^{i+k}(a)$ за $i + k > 0$, т.е. $a\alpha c$, што значи дека релацијата α е транзитивна.

Конечно, α е рефлексивна, симетрична и транзитивна, т.е. таа е релација на еквиваленција. ♦

10.6. Нека земеме $A = \{1, 2, 3, ..., n\}$. Бидејќи релацијата α од претходната теорема е релација на еквиваленција, таа го дели множеството A на класи на еквиваленција. На пример, ако $A = \{1, 2, 3, ..., 8\}$ и $p_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 7 & 8 & 6 & 1 & 5 \end{bmatrix}$, тогаш лесно се гледа дека множеството класи на еквиваленција е $\{\{1,4,7\},\{2,3\},\{5,8\},\{6\}\}$. Множеството класи на еквиваленција добиено со претходната постапка го нарекуваме *орбита на пермутацијата* p.

11. НОРМАЛНИ ПОДГРУПИ

11.1. Дефиниција. Нека H и K се подмножества на групата $(G, \circ)$. *Производ на подмножествата* H и K го нарекуваме множеството

$$H \circ K = \{h \circ k \mid h \in H, k \in K\}.$$

11.2. Теорема. Ако H е подгрупа од групата $(G, \circ)$, тогаш $H \circ H = H$.

Доказ. Нека H е подгрупа од групата G и $z \in H \circ H$. Според тоа, постојат $x, y \in H$ такви што $z = x \circ y \in H$, т.е. $H \circ H \subseteq H$. Обратно, ако $x \in H$, тогаш $x = x \circ e \in H \circ H$, т.е. $H \subseteq H \circ H$. ♦

11.3. Забелешка. Обратното тврдење на теорема 11.2 не важи. Навистина, за множеството природни броеви $\mathbf{N}$ кое е подмножество од групата $(\mathbf{Q}, \cdot)$ важи $\mathbf{N} \cdot \mathbf{N} = \mathbf{N}$, но $\mathbf{N}$ не е подгрупа од $(\mathbf{Q}, \cdot)$.

11.4. Дефиниција. Нека H е подгрупа од групата G и $x \in G$. Множеството

$$xH = \{xz \mid z \in H\} \subseteq G$$

го нарекуваме *лев комплекс* на H во G, а елементот x го нарекуваме *преставник* на тој комплекс. Множеството

$$Hx = \{zx \mid z \in H\} \subseteq G$$

го нарекуваме *десен комплекс* на H во G, а елементот x го нарекуваме *преставник* на тој комплекс.

11.5. Лема. Нека H е подгрупа од групата G. Кои било два леви (десни) комплекси xH и yH на подгрупата H се или еднакви, или пак дисјунктни.

Доказ. Непосредно следува од доказот на теоремата на Лагранж. ♦

11.6. Дефиниција. Нека H е подгрупа на групата G. За H ќе велиме дека е нормална подгрупа на G ако $gHg^{-1} = H$, за секој $g \in G$.

11.7. Теорема. Нека $f : G \to H$ е хомоморфизам од групата G во групата H. Тогаш јадрото на $f : G \to H$ е нормална подгрупа на групата G.

Доказ. Нека $g \in G$ и $J = \{x \mid x \in G,\ f(x) = 1'\}$ е јадрото на $f : G \to H$. Имаме

$$gJg^{-1} = \{gxg^{-1} \mid x \in G,\ f(x) = 1'\}.$$

Ако $y \in gJg^{-1}$, тогаш постои $x \in J$ таков што $y = gxg^{-1}$ и $f(x) = 1'$. Но, f е хомоморфизам, па затоа

$$f(y) = f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)(f(g))^{-1} = 1',$$

т.е. $y \in J$, што значи $gJg^{-1} \subseteq J$, за секој $g \in G$.

Обратната инклузија се докажува аналогно. Деталите ги оставаме на читателот за вежба. ♦

11.8. Теорема. Нека H е подгрупа од групата G. H е нормална подгрупа од G ако и само ако $gH = Hg$, за секој $g \in G$.

Доказ. Нека претпоставиме дека H е нормална подгрупа на G, т.е. дека $gHg^{-1} = H$, за секој $g \in G$. Нека $gh \in gH$. Од $gHg^{-1} = H$ следува дека $ghg^{-1} = h'$ за некој $h' \in H$, т.е. $gh = h'g$ за некој $h' \in H$ и како $h'g \in Hg$ добиваме $gH \subseteq Hg$. Слично се докажува дека $Hg \subseteq gH$, што значи $gH = Hg$, за секој $g \in G$.

Нека $gH = Hg$, за секој $g \in G$. Тогаш

$$gHg^{-1} = (Hg)g^{-1} = \{xg \mid x \in H\}g^{-1} = \{xgg^{-1} \mid x \in H\} = \{x \mid x \in H\} = H,$$

т.е. H е нормална подгрупа на G. ♦

11.9. Теорема. Нека H е нормална подгрупа на група G. Тогаш $abH = (aH)(bH)$, за секои $a, b \in G$.

Доказ. За секои $a, b \in G$ важи

$$abH = a(bH) = a(b(HH)) = a(bH)H = a(Hb)H = (aH)(bH)\,.$$ ♦

11.10. Последица. Ако H е нормална подгрупа на група G, тогаш комплексите од H во G во однос на операцијата $(aH)(bH) = abH$ формираат група, која ја нарекуваме *фактор-група* и ја означуваме се G/H.

Доказ. Фактот дека G/H е групоид непосредно следува од теорема 10.9. Останатите својства следуваат од фактот дека G е група. Деталите ги оставаме на читателот за вежба. ♦

11.11. Теорема. Нека $f : G \to H$ е сурјективен хомоморфизам од групата G во групата H со јадро K. Тогаш групите H и G/K се изоморфни.

Доказ. Да го разгледаме пресликувањето $\varphi : G/K \to H$ определено со $\varphi(gK) = f(g)$, за секој $g \in G$. Прво ќе докажеме дека ова пресликување е добро дефинирано, т.е. дека од $gK = g'K$ следува $\varphi(gK) = \varphi(g'K)$. Нека $gK = g'K$ и $f(g) = \varphi(gH), f(g') = \varphi(g'H)$. Од $gK = g'K$ следува $g = g'k$ за некој $k \in K$, па затоа

$$\varphi(gH) = f(g) = f(g'k) = f(g')f(k) = f(g') \circ 1' = f(g') = \varphi(g'H)\,.$$

Сега ќе докажеме дека φ е хомоморфизам. Имаме

$$\varphi(gHg'H) = \varphi(gg'H) = f(gg') = f(g)f(g') = \varphi(gH)\varphi(g'H)\,.$$

Ќе докажеме дека φ е биекција. Нека $h \in H$. Бидејќи f е сурјекција, за $h \in H$ постои $g \in G$ таков што $f(g) = h$, па затоа постои $gK \in G/H$ таков што $\varphi(gK) = f(g) = h$, т.е. φ е сурјекција. Нека $\varphi(gK) = \varphi(g'K)$. Тогаш $f(g) = f(g')$ па, затоа $f(g)f(g)^{-1} = f(g')f(g)^{-1}$, односно

$$f(1) = f(gg^{-1}) = f(g'g^{-1})\,,$$

од што следува дека $g'g^{-1} \in K$, па затоа $gK = g'K$, т.е. φ е инјекција. ♦

12. ПРСТЕНИ

12.1. Дефиниција. Нека на множеството G е определена низа операции: $\bullet, *, \oplus, \otimes, \ldots$. Тогаш, велиме дека $(G, \bullet, *, \oplus, \otimes, \ldots)$ е *алгебарска структура со носител* G.

За алгебарската структура $(G,*,\circ)$ ќе велиме дека е *прстен* ако

а) групоидот $(G,*)$ е комутативна група;

б) групоидот $(G,\circ)$ е полугрупа; и

в) важат левиот и десниот дистрибутивен закон на операцијата $\circ$ во однос на операцијата $*$, т.е. важи

$$x\circ(y*z)=(x\circ y)*(x\circ z) \text{ и} \tag{1}$$

$$(x*y)\circ z=(x\circ z)*(y\circ z), \tag{2}$$

за секои $x,y,z\in G$. Ако полугрупата $(G,\circ)$ е комутативна, ќе велиме дека $(G,*,\circ)$ е *комутативен прстен*. Ако $(G,\circ)$ е полугрупа со единица, ќе велиме дека $(G,*,\circ)$ е *прстен со единица*.

12.2. Пример. а) Претходно видовме дека $(\mathbf{Z}_5,\oplus)$ е комутативна група. Понатаму, $(\mathbf{Z}_5,\otimes)$ е комутативна полугрупа со единица, а од својствата на конгруенциите непосредно следува дека за собирањето и множењето по модул 5 важи

$$x\otimes(y\oplus z)=(x\otimes y)\oplus(x\otimes z)\text{, за секои } x,y,z\in\mathbf{Z}_5,$$

(провери!). Според тоа, алгебарската структура $(\mathbf{Z}_5,\oplus,\otimes)$ е комутативен прстен со единица.

Претходно кажаното, всушност, важи за секој $n\in\mathbf{N}$. Според тоа, за секој $n\in\mathbf{N}$ алгебарската структура $(\mathbf{Z}_n,\oplus,\otimes)$ е комутативен прстен со единициа.

б) Како што знаеме $(\mathbf{N},+)$ не е група, па затоа алгебарската структура $(\mathbf{N},+,\cdot)$ не е прстен. Но, групоидот $(\mathbf{Z},+)$ е комутативна група, а групоидот $(\mathbf{Z},\cdot)$ е комутативна полугрупа со единица. Понатаму, од својствата на целите броеви знаеме дека за секои $x,y,z\in\mathbf{Z}$ важи

$$(x+y)\cdot z=x\cdot z+y\cdot z.$$

Од досега изнесеното следува дека алгебарската структура $(\mathbf{Z},+,\cdot)$ е комутативен прстен со единица и тоа е прстенот на целите броеви. Аналогно се проверува дека $(\mathbf{Q},+,\cdot)$ и $(\mathbf{R},+,\cdot)$ се прстените на рационални и реални броеви. ♦

12.3. Теорема. Нека $(G,+,\cdot)$ е прстен. Тогаш

а) $a0=0a=0$, за секој $a\in G$,

б) $a(-b)=(-a)b=-(ab)$, за секои $a,b\in G$,

в) $(-a)(-b)=ab$, за секои $a,b\in G$,

г) $a(b-c)=ab-ac,(a-b)c=ac-bc$, за секои $a,b,c\in G$.

Доказ. а) За секој $a\in G$ важи

$$a0+0=a0=a(0+0)=a0+a0,$$

од што по кратење со $a0$ се добива $a0=0$. Аналогно се докажува дека $0a=0$.

б) Имаме

$$0 = a0 = a(b + (-b)) = ab + a(-b)$$

од што следува дека $a(-b) = -(ab)$. Аналогно се докажува дека $(-a)b = -(ab)$.

в) Според б) добиваме $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

г) Имаме

$$a(b-c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac .$$

Второто равенство се докажува аналогно. ♦

12.4. Теорема. Нека $(G, +, \cdot)$ е прстен. Тогаш $n(ab) = (na)b = a(nb)$, за секој $n \in \mathbf{Z}$ и за секои $a, b \in G$.

Доказ. Од $1a = a, (-1)a = -a, 0a = 0$ следува дека горните равенства се точни за $n = 1, 0, -1$. Нека претпоставиме дека равенствата се точни за $n = k \in \mathbf{N}$. Тогаш за $n = k + 1$ имаме

$$(na)b = ((k+1)a)b = (ka + a)b = (ka)b + ab = k(ab) + ab = (k+1)(ab) = n(ab),$$

$$a(nb) = a((k+1)b) = a(kb + b) = a(kb) + ab = k(ab) + ab = (k+1)ab = n(ab),$$

па од принципот на математичка индукција следува дека равенствата се точни за секој $n \in \mathbf{N}$. Ако $n < 0$, тогаш $-n \in \mathbf{N}$, па затоа

$$n(ab) = -((-n)(ab)) = -(((-n)a)b) = (-(-n)a)b = (na)b .$$

Аналогно се докажува дека $n(ab) = a(nb)$. ♦

12.5. Дефиниција. Нека $(G, +, \cdot)$ е прстен и $H \subseteq G$. За H ќе велиме дека е *потпрстен* од G ако $(H, +, \cdot)$ е прстен.

12.6. Пример. а) Од пример 11.2 б) и фактот дека $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$ следува дека $(\mathbf{Z}, +, \cdot)$ е потпрстен од $(\mathbf{Q}, +, \cdot)$ и $(\mathbf{R}, +, \cdot)$ и $(\mathbf{Q}, +, \cdot)$ е потпрстен од $(\mathbf{R}, +, \cdot)$.

б) $\{0, 2, 4\}$ е потпрстен од $(\mathbf{Z}_6, \oplus, \otimes)$. Проверете!

в) Ако $(G, +, \cdot)$ е прстен, тогаш $\{0\} = O$ и G се негови потпрстени. ♦

12.7. Теорема. Нека $(G, +, \cdot)$ е прстен. Тогаш $H \subseteq G$ е потпрстен од G ако и само ако се исполнети следниве услови:

1) $0 \in H$,

2) од $a, b \in H$ следува $-a, a + b, ab \in H$.

Доказ. Ако $(H, +, \cdot)$ е потпрстен, тогаш $(H, +)$ е подгрупа од $(G, +)$, $(H, \cdot)$ е потполугрупа од $(G, \cdot)$, па затоа се исполнети условите 1) и 2).

Обратно, ако се исполнети условите 1) и 2), тогаш $(H, +)$ е подгрупа од $(G, +)$, $(H, \cdot)$ е потполугрупа од $(G, \cdot)$. Јасно, групата $(H, +)$ е комутативна, бидејќи таква е групата $(G, +)$. Конечно, дистрибутивните закони (1) и (2) се точни

за сите елементи на H бидејќи тие се точни за сите елементи на G, па затоа H е потпрстен од G. ♦

12.8. Дефиниција. Нека се $(G,+,\cdot)$ и $(H,+,\cdot)$ алгебарски структури. За пресликувањето $f:G\to H$ ќе велиме дека е *хомоморфизам* од $(G,+,\cdot)$ во $(G,+,\cdot)$ ако за секои $a,b\in G$ важи

$$f(a+b)=f(a)+f(b) \text{ и } f(ab)=f(a)f(b),$$

и притоа ќе велиме дека алгебарските структури G во H се *хомоморфни*. Ако хомоморфизмот $f:G\to H$ е биекција, тогаш ќе велиме дека f е *изоморфизам* од G во H, а за алгебарските структури G во H ќе велиме дека се *изоморфни*.

12.9. Пример. Прстените $(\mathbf{Z},+,\cdot)$ и $(\mathbf{Z}_5,\oplus,\otimes)$ се хомоморфни. Навистина пресликувањето $f:\mathbf{Z}\to\mathbf{Z}_5$ определено со $f(n)=m$, $m\in\mathbf{Z}_5$ и $m\equiv n \pmod 5$ е хомоморфизам (зошто?). Јасно, овие два прстени не се изоморфни. ♦

12.10. Теорема. Нека $(G,+,\cdot)$ и $(H,+,\cdot)$ се две изоморфни структури. Ако едната од нив е прстен, тогаш и другата е прстен.

Доказ. Нека $(G,+,\cdot)$ е прстен. Тогаш $(G,+)$ е комутативна група, па од теоремите 2.2 и 6.3 следува дека $(H,+)$ е комутативна група. Аналогно, $(G,\cdot)$ е полугрупа, па од теорема 2.2 следува дека $(H,\cdot)$ е полугрупа. Останува да се докажат дистрибутивните закони. Ако $a',b',c'\in H$ и $f:G\to H$ е изоморфизам тогаш постојат $a,b,c\in G$ такви што $a'=f(a), b'=f(b), c'=f(c)$, па затоа

$$\begin{aligned} a'(b'+c') &= f(a)(f(b)+f(c)) = f(a)f(b+c) = f(a(b+c)) = f(ab+ac) \\ &= f(ab)+f(ac) = f(a)f(b)+f(a)f(c) = a'b'+a'c'. \end{aligned}$$

Аналогно се докажува и вториот дистрибуривен закон, што значи дека $(H,+,\cdot)$ е прстен.

Конечно, тврдењето следува од теорема 2.9 б). ♦

12.11. На крајот од овој дел ќе го воведеме поимот изоморфно сместување, кој може да се дефинира за произволни алгебарски структури, но ние ќе се задржиме само на изоморфното сместување на прстен во прстен.

Дефиниција. Нека $(G,+,\cdot)$ и $(H,+,\cdot)$ се два прстена. Ако $f:G\to H$ е инјекција таква што

$$f(a+b)=f(a)+f(b) \text{ и } f(ab)=f(a)f(b), \tag{3}$$

тогаш ќе велиме дека f е *изоморфно сместување* од G во H.

12.12. Теорема. Ако f е изоморфно сместување од прстенот $(G,+,\cdot)$ во прстенот $(H,+,\cdot)$, тогаш $G_1=f(G)$ е потпрстен од H и притоа G и G_1 се изоморфни.

Доказ. Нека $a', b' \in G_1$. Тогаш $a' = f(a), b' = f(b)$ за некои $a, b \in G$. Сега од (3) следува дека

$$a'b' = f(a)f(b) = f(ab) \in G_1,$$
$$a' + b' = f(a) + f(b) = f(a+b) \in G_1,$$
$$-a' = f(-a) \in G_1,$$

и како $0' = f(0) \in G_1$, од теорема 11.7 следува дека G_1 е потпрстен од H. Јасно, G и G_1 се изоморфни. ♦

12.13. Теорема. Нека f е изоморфно сместување од прстенот $(G, +, \cdot)$ во прстенот $(H, +, \cdot)$, при што $G \cap H = \varnothing$. Постои прстен $R(+', \cdot')$ таков што

1) R е изоморфен со H и
2) G е потпрстен од R.

Доказ. Ако f е биекција, тогаш прстенот G ги има бараните својства на R. Затоа ќе претпоставиме дека f не е биекција, т.е. дека $f(G) = G_1 \subset H$. Го разгледуваме множеството $R = G \cup (H \setminus G_1)$ и дефинираме пресликување $g : R \to H$ со:

$$g(x) = \begin{cases} f(a), & a \in G, \\ a, & a \in H \setminus G_1. \end{cases} \tag{4}$$

Имаме

$$g(R) = g(G \cup (H \setminus G_1)) = g(G) \cup g(H \setminus G_1) = f(G) \cup (H \setminus G_1) = G_1 \cup (H \setminus G_1) = H,$$

т.е. g е сурјекција. Но, f е инјекција, па од (4) следува дека g е инјекција, што значи дека g е биекција.

Во R дефинираме операции: собирање во ознака $+'$ и множење $\cdot'$ со:

$$\begin{aligned} a +' b &= g^{-1}(g(a) + g(b)), \\ a \cdot' b &= g^{-1}(g(a) \cdot g(b)). \end{aligned} \tag{5}$$

Од (5) следува

$$\begin{aligned} g(a +' b) &= g(a) + g(b), \\ g(a \cdot' b) &= g(a) \cdot g(b), \end{aligned} \tag{5'}$$

што значи дека g е изоморфизам од R во H. Сега од теорема 11.10 следува дека $R(+', \cdot')$ е прстен.

Останува уште да докажеме дека $(G, +, \cdot)$ е потпрстен од $R(+', \cdot')$. Нека $a, b \in G$. Од (4) и (5') и фактот дека f е изоморфизам следува

$$\begin{aligned} g(a +' b) &= g(a) + g(b) = f(a) + f(b) = f(a+b), \\ g(a \cdot' b) &= g(a) \cdot g(b) = f(a) \cdot f(b) = f(ab), \end{aligned} \tag{6}$$

па затоа ако се земе предвид дека g е изоморфизам добиваме

$$a+'b=g^{-1}(g(a+'b))=g^{-1}(f(a+b))=f^{-1}(f(a+b))=a+b\in G,$$
$$a\cdot'b=g^{-1}(g(a\cdot'b))=g^{-1}(f(ab))=f^{-1}(f(ab))=ab\in G, \qquad (7)$$

што значи дека $(G,+,\cdot)$ е потпрстен од $R(+',\cdot')$. ♦

12.14. Забелешка. Равенствата (7) ни дозволуваат операциите во R да ги означуваме со стандардните ознаки, што значи дека равенствата (5) можеме да ги запишеме во обликот:

$$a+b=g^{-1}(g(a)+g(b)),$$
$$a\cdot b=g^{-1}(g(a)\cdot g(b)). \qquad (5'')$$

13. ИНТЕГРАЛНИ ДОМЕНИ

13.1. Дефиниција. За комутативниот прстен со единица $(G,+,\cdot)$ ќе велиме дека е *интегрален домен* ако од $ab=0$ следува $a=0$ или $b=0$.

13.2. Пример. а) Од својствата на множењето на реалните броеви и од следува дека $(\mathbf{Z},+,\cdot)$, $(\mathbf{Q},+,\cdot)$ и $(\mathbf{R},+,\cdot)$ се интегрални домени.

б) Во пример 12.2 б) констатиравме дека $(\mathbf{Z}_n,\oplus,\otimes)$ е прстен за секој $n\in\mathbf{N}$. Меѓутоа, ако n не е прост број, на пример $n=pq$, тогаш $p\otimes q=0$, но $p\neq 0$ и $q\neq 0$, па затоа $(\mathbf{Z}_n,\oplus,\otimes)$ не е интегрален домен.

Од друга страна, ако n е прост број, тогаш според теорема II 14.3 за секој $a\neq 0$ конгруенцијата $ax\equiv 1\,(\mathrm{mod}\,n)$ има решение a', па затоа $a\otimes a'=1$, што значи дека секој елемент $a\neq 0$ има инверзен. Сега, ако $a\otimes b=0$, тогаш

$$b=1\otimes b=(a'\otimes a)\otimes b=a'\otimes(a\otimes b)=a'\otimes 0=0,$$

што значи дека во случај кога n добиваме дека $(\mathbf{Z}_n,\oplus,\otimes)$ е интегрален домен. ♦

13.3. Теорема. Нека $(G,+,\cdot)$ е комутативен прстен со единица. G е интегрален домен ако и само ако

$$\text{од } ab=ac \text{ следува } b=c \text{, за секои } a,b,c\in G,\ a\neq 0. \qquad (1)$$

Доказ. Нека G е интегрален домен и нека

$$ab=ac,\ a,b,c\in G,\ a\neq 0.$$

Последователно добиваме

$$ab-ac=0,\ a(b-c)=0$$

и како $a\neq 0$ од дефиниција 11.3 следува $b-c=0$, односно $b=c$.

Нека G е комутативен прстен со единица таков што е исполнет условот (1) и нека $ab=0$. Ако $a=0$, тогаш нема што да се докажува, па затоа нека претпоставиме дека $a\neq 0$. Тогаш последователно добиваме

$$ab = 0,\quad a(b-0) = 0,\quad ab - a0 = 0,\quad ab = a0,$$

и ако го искористиме условот (1) добиваме $b = 0$, што значи дека G е интегрален домен. ♦

13.4. Дефиниција. Нека $(G,+,\cdot)$ е интегрален домен и $H \subseteq G$. За H ќе велиме дека е *поддомен* од G ако $(H,+,\cdot)$ е интегрален домен.

13.5. Теорема. Потпрстенот $(H,+,\cdot)$ од интегралниот домен $(G,+,\cdot)$ е поддомен од G ако и само ако $e \in H$, каде e е единицата на G.

Доказ. Непосредно следува од дефинициите на домен и поддомен. Деталите ги оставаме на читателот за вежба. ♦

13.6. Теорема. Нека $(G,+,\cdot)$ и $(H,+,\cdot)$ се две изоморфни структури. Ако едната од нив е интегрален домен, тогаш и другата е интегрален домен.

Доказ. Нека G е интегрален домен. Јасно, H е комутативен прстен со единица. Понатаму, ако $f : G \to H$ е изоморфизам, тогаш $f(0) = 0'$, $f(e) = e'$, каде 0 и e се нулата и единицата во G, а $0'$ и e' се нулата и единицата во H.

Ако $a'b' = 0'$, тогаш имаме

$$f(ab) = f(a)f(b) = a'b' = 0' = f(0),$$

па затоа $ab = 0$. Но, G е интегрален домен и од последното равенство следува $a = 0$ или $b = 0$, што значи $a' = 0'$ или $b' = 0'$, т.е. H е интегрален домен. ♦

14. ПОЛИЊА

14.1. Дефиниција. За комутативниот прстен $(G,+,\cdot)$ со единица $e \neq 0$ ќе велиме дека е *поле* ако секој ненулти елемент е инверзибилен во мултипликативната полугрупа $(G,\cdot)$.

14.2. Теорема. Ако $(G,+,\cdot)$ е поле, тогаш $(G,+,\cdot)$ е интегрален домен.

Доказ. Нека G е поле и нека $ab = 0$. Ако $a \neq 0$, тогаш

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0,$$

што значи дека G е интегрален домен.

14.3. Теорема. Ако $(G,+,\cdot)$ е конечен интегрален домен, тогаш $(G,+,\cdot)$ е поле.

Доказ. Нека $G = \{0, e, a_3, a_4, ..., a_n\}$ е интегрален домен со n елементи и нека $a \in G \setminus \{0\}$. Да го разгледаме множеството $A = \{ae, aa_3, aa_4, ..., aa_n\} \subset G$. Ако $aa_i = aa_k$, тогаш $a(a_i - a_k) = 0$ и како $a \in G \setminus \{0\}$ и G е интегрален домен добива-

ме дека $a_i - a_k = 0$, т.е. $a_i = a_k$, што значи дека A има $n-1$ елемент, па затоа $A = \{e, a_3, a_4, ..., a_n\}$. Според тоа, постои $a_i \in G$ таков што $aa_i = e$, т.е. $a_i = a^{-1}$. Конечно, од произволноста на $a \in G \setminus \{0\}$ следува дека $(G, +, \cdot)$ е поле. ♦

14.4. Последица. За секој прост број p алгебарската структура $(\mathbf{Z}_p, \oplus, \otimes)$ е поле.

Доказ. Непосредно следува од теорема 14.3 и пример 13.2 б). ♦

14.5. Дефиниција. Нека $(G, +, \cdot)$ е поле и $H \subseteq G$. За H ќе велиме дека е *потполе* од G ако $(H, +, \cdot)$ е поле.

14.6. Теорема. Подпрстенот H од полето $(G, +, \cdot)$ е потполе ако и само ако

$$e \in H,\ a \in H \setminus \{0\} \Rightarrow a^{-1} \in H.$$

Доказ. Непосредно следува од претходните разгледувања. Деталите ги препуштаме на читателот за вежба. ♦

14.7. Теорема. Нека $(G, +, \cdot)$ и $(H, +, \cdot)$ се две изоморфни структури. Ако едната од нив е поле, тогаш и другата е поле.

Доказ. Нека G е поле. Тогаш G е интегрален домен, па од теорема 12.8 следува дека H е интегрален домен. Останува да покажеме дека секој ненулти елемент a' во H е инверзибилен.

Нека $a' \neq 0'$ и $f : G \to H$ е изоморфизам. Тогаш $a \neq 0$, па затоа

$$a' f(a^{-1}) = f(aa^{-1}) = f(e) = e',$$

па затоа $a'^{-1} = f(a^{-1})$ во H, што значи дека H е поле. ♦

14.8. Забелешка. Како што претходно рековме $(\mathbf{Z}, +, \cdot)$ е интегрален домен, но лесно се проверува дека не е поле. Значи, сите интегрални не се домени полиња. Меѓутоа, во натамошните разгледувања ќе докажеме дека секој интегрален домен се содржи во некое поле, односно дека секој интегрален домен може изоморфно да се смести во некое поле.

14.9. Нека $(G, +, \cdot)$ е интегрален домен и во множеството

$$P = \{(a, b) \mid (a, b) \in G \times G, b \neq 0\} \tag{1}$$

дефинираме релација $\sim$ на следниов начин: за секои $(a, b), (c, d) \in P$ важи

$$(a, b) \sim (c, d) \text{ ако и само ако } ad = bc. \tag{2}$$

Во врска со релацијата $\sim$ точна е следнава теорема, чиј доказ го препуштаме на читателот за вежба.

Теорема. Нека $(G,+,\cdot)$ е интегрален домен и нека ~ е релацијата во множеството P определена со (2). Тогаш ~ е релација на еквиваленција во P. ♦

14.10. Пример. Ако $G=\mathbf{Z}$, тогаш класата на еквиваленции $(2,3)$ од теорема 14.9 ги содржи подредените парови

$$(2,3),(-2,-3),(4,6),(-4,-6),(6,9),(-6,-9),...$$

кои соодветствуваат на рационалните броеви $\frac{2}{3},\frac{-2}{-3},\frac{4}{6},\frac{-4}{-6},\frac{6}{9},\frac{-6}{-9},...$ и тоа се различни начини на запишување на ист рационален број $(2,3)$. ♦

14.11. Теорема. Нека $(G,+,\cdot)$ е интегрален домен и нека F е множеството класи на еквиваленција од теорема 14.9 при што класата на еквиваленција која го содржи елементот $(a,b)\in P$ ја означуваме со $\frac{a}{b}$. Дефинираме операции

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\text{, за секој }\frac{a}{b},\frac{c}{d}\in F, \tag{3}$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}\text{, за секој }\frac{a}{b},\frac{c}{d}\in F. \tag{4}$$

Тогаш $(F,+,\cdot)$ е комутативен прстен со неутрален елемент (нула) во однос на собирањето $\frac{0}{1}$ и неутрален елемент (единица) во однос на множењето $\frac{1}{1}$.

Доказ. Ќе докажеме дека операциите $+$ и $\cdot$ во F се добро дефинирани. Нека $\frac{a}{b}$ и $\frac{a'}{b'}$ се два претставници од класата на еквиваленција (a,b), а $\frac{c}{d}$ и $\frac{c'}{d'}$ се два претставници од класата (c,d). Тогаш од (2) следува дека $ab'=a'b$ и $cd'=c'd$.

а) G е интегрален домен, па затоа

$$b'd'(ad+bc)=b'add'+ad'bb'=a'bdd'+c'dbb'=bd(a'd'+b'c'),$$

па од (2) и (3) следува дека

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}=\frac{a'}{b'}+\frac{c'}{d'},$$

што значи дека резултатот во (3) не зависи од изборот на претставниците на класата на еквиваленција, т.е. операцијата $+$ е добро дефинирана на F.

б) G е интегрален домен, па затоа

$$acb'd'=ab'cd'=a'bc'd=a'c'bd,$$

па од (2) и (4) следува дека

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{a'c'}{b'd'}=\frac{a'}{b'}\cdot\frac{c'}{d'},$$

што значи дека резултатот во (4) не зависи од изборот на претставниците на класата на еквиваленција, т.е. операцијата $\cdot$ е добро дефинирана на F.

Сега непосредно се проверува дека $(F,+,\cdot)$ е комутативен прстен со единица $\frac{1}{1}$ и нула $\frac{0}{1}$. Деталите ги оставаме на читателот за вежба. ♦

14.12. Лема. Нека $(G,+,\cdot)$ е интегрален домен и $(F,+,\cdot)$ е комутативниот прстен од теорема 14.11. Тогаш $\frac{a}{b}=\frac{0}{1}, b\neq 0$ ако и само ако $a=0$, а $\frac{a}{b}=\frac{1}{1}, b\neq 0$ ако и само ако $a=b$.

Доказ. Јасно, $\frac{a}{b}=\frac{0}{1}, b\neq 0$ ско и само ако $a=a\cdot 1=b\cdot 0=0$, а $\frac{a}{b}=\frac{1}{1}, b\neq 0$ ако и само ако $a=a\cdot 1=b\cdot 1=b$. ♦

14.13. Теорема. Комутативниот прстен $(F,+,\cdot)$ е поле, кое го нарекуваме *поле на дропки* од $(G,+,\cdot)$.

Доказ. Согласно со дефиниција 14.1 доволно е да докажеме дека секој ненулти елемент во F е инверзибилен. Од лема 14.12 следува дека $\frac{a}{b}\neq\frac{0}{1}$ ако и само ако $a\neq 0$, па затоа $\frac{b}{a}\in F$. Сега од (4) и од лема 14.12 добиваме

$$\frac{a}{b}.\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=\frac{1}{1},$$

т.е. $(F,+,\cdot)$ е поле. ♦

14.14. Пример. Ако G е множеството цели броеви $\mathbf{Z}$, тогаш F е множеството рационални броеви $\mathbf{Q}$. Јасно, $(\mathbf{Q},+,\cdot)$ е *полето на рационални броеви*. ♦

14.15. Теорема. Нека $(F,+,\cdot)$ е полето дропки на интегралниот домен $(G,+,\cdot)$. Тогаш пресликувањето $f:G\to F$ определено со $f(x)=\frac{x}{1}$ е хоморфизам и е инјекција. Притоа ќе велиме дека интегралниот домен G е *вграден* во полето F или дека F го *содржи* G.

Доказ. За секои $x,y\in G$ важи

$$f(x+y)=\frac{x+y}{1}=\frac{x}{1}+\frac{y}{1}=f(x)+f(y) \text{ и } f(xy)=\frac{xy}{1}=\frac{x}{1}\cdot\frac{y}{1}=f(x)f(y),$$

што значи дека f е хомоморфизам од G во F. Јасно, ако $f(x)=f(y)$, тогаш $\frac{x}{1}=\frac{y}{1}$, па затоа $x=x\cdot 1=y\cdot 1=y$, што значи дека f е инјекција. ♦

ЗАДАЧИ

1. Во множеството $\mathbf{N}$ дефинираме $m*n=m^n$. Докажете дека $(\mathbf{N},*)$ е групоид! Пресметајте $2*3$, $3*2$, $(2*2)*3$ и $2*(2*3)$! Што заклучувате?
2. Во множеството природни броеви $\mathbf{N}$ дефинираме операции $*,\circ$ и Δ со:
$$x*y=\mathrm{NZD}(x,y),\ x\circ y=\mathrm{NZS}(x,y),\ x\Delta y=\min\{x,y\}.$$
   a) Дали групоидите $(\mathbf{N},*),(\mathbf{N},\circ),(\mathbf{N},\Delta)$ се полугрупи?
   b) Дали групоидите $(\mathbf{N},*),(\mathbf{N},\circ),(\mathbf{N},\Delta)$ се комутативни?

3. Во множеството цели броеви $\mathbf{Z}$ дефинираме операција $*$ со: $x*y=x+y+1$ за секои $x,y\in\mathbf{Z}$. Дали $(\mathbf{Z},*)$ е групоид? Во случај на потврден одговор проверете дали овој групоид е:
   a) полугрупа,
   b) комутативен.
4. Нека M е произволно непразно множество и $\mathbf{P}(M)=\{X \mid X\subseteq M\}$ е неговото партитивно множество. Докажете дека $(\mathbf{P}(M),\dot{-})$ е комутативна полугрупа.
5. Даден е групоидот $(\mathbf{Z},*)$, каде $x*y=x+2y-3$ за секои $x,y\in\mathbf{Z}$.
   a) Пресметај $[2*(-3)]*1$, $(4*1)*(2*3)$.
   b) Дали овој групоид е полугрупа? Дали групоидот е комутативен?
   c) Решете ги равенките $3*x=10$, $(-2*x)*(x*3)=2$.
6. Даден е групоидот $(\mathbf{Z},*)$, каде што $x*y=2xy+3(x+y)+3$ за секои $x,y\in\mathbf{Z}$.
   a) Пресметајте $[4*(-12)]*2$, $[(4*(-3))*(2*7)]*(-1)$.
   b) Дали овој групоид е полугрупа? Дали групоидот е комутативен?
7. Докажете дека за групоидот $(\mathbf{N},*)$ каде што $m*n=m^n$ за секои $m,n\in\mathbf{N}$ бројот 1 е десна единица!
8. Докажете дека за групоидот $(\mathbf{P}(M),\setminus)$ празното множество $\varnothing$ е десна единица.
9. Дали групоидите $(\mathbf{N},*)$, $(\mathbf{N},\circ)$, $(\mathbf{N},\Delta)$, каде $*,\circ$ и Δ се операциите од задача 2, имаат неутрални елементи? Во случај на потврден одговор најдете ги инверзибилните елементи во овие групоиди.
10. Во множеството $\mathbf{Z}\setminus\{0\}$ дефинираме $m*n=m^n$. Докажете дека $(\mathbf{Z}\setminus\{0\},*)$ е групоид! Пресметај $2*3$, $3*2$, $(2*2)*3$ и $2*(2*3)$! Што заклучувате?
11. Докажете дека $(\mathbf{Z},*)$, каде што $x*y=x\cdot y+3x-2y-3$ за секои $x,y\in\mathbf{Z}$ е групоид. Дали овој групоид е:
    1) комутативен,
    2) асоцијативен.
12. Нека $(G,\cdot)$ е групоид. Докажете дека од $xy=x$, за секои $x,y\in G$ следува дека секоја еквивалентност на G е конгруенција на G.
13. Ако α е конгруенција на полугрупата $(\mathbf{N},+)$, тогаш α е конгруенција и на полугрупата $(\mathbf{N},\cdot)$. Докажете!
14. Еквивалентноста α е конгруенција на групоидот $(G,\cdot)$ ако и само ако од $(x,y)\in\alpha$ следува $(xz,yz)\in\alpha$ и $(zx,zy)\in\alpha$, за секој $z\in G$. Докажете!
15. Нека a е фиксен елемент од множеството G и нека операцијата $*$ е определена со $x*y=a$, за секои $x,y\in G$. Докажете дека добиениот групоид е комутативна полугрупа и дека $(G,*)$ има единица ако и само ако $G=\{a\}$.
16. Нека α е релација во $\mathbf{N}$ определена со: $(x,y)\in\alpha$ ако и само ако

$$x = y \text{ или } x \geq 3,\ y \geq 3,\ 4 \mid (x-y).$$

Докажете дека α е конгруенција на $(\mathbf{N},+)$ и на $(\mathbf{N},\cdot)$ и најдете ги факторполугрупите $(\mathbf{N}_{|\alpha},+)$ и $(\mathbf{N}_{|\alpha},\cdot)$.

17. Нека G е множество и да дефинираме операција * со $x*y=y$, за секои $x,y\in G$. Докажете дека $(G,*)$ е полугрупа во која секој елемент е лева единица и дека $(G,*)$ е комутативна ако и само ако G нема повеќе од еден елемент.

18. Нека $(G,*)$ е групоид и да дефинираме операција $\circ$ со: $x\circ y = y*x$, за секои $x,y\in G$. Тогаш $(G,\circ)$ е групоид кој го нарекуваме *спротивен групоид* на групоидот $(G,*)$. Докажете дека $(G,*)$ е:
    a) комутативен групоид,
    b) полугрупа,
    c) групоид со единица,
    d) групоид со кратење,

    ако и само ако соодветното својство го има неговиот спротивен групоид $(G,\circ)$.

19. Даден е групоидот $(\mathbf{Z},*)$, каде што $x*y=x+y+1$ за секои $x,y\in\mathbf{Z}$. Дали овој групоид има неутрален елемент? Во случај на потврден одговор најди ги инверзибилните елементи на групоидот.

20. Докажете дека за комутативната полугрупа $(\mathbf{P}(M),\dot{-})$ празното множество $\varnothing$ е неутрален елемент и дека секој елемент е инверзибилен на самиот себе.

21. Докажете дека $(\mathbf{N},*)$ каде $m*n = |x-y|$, за секои $x,y\in\mathbf{N}$ е комутативен групоид со единица, но не е група.

22. Со A да го означиме множеството од сите парни цели броеви и $x*y=x+y$, за секој $x,y\in A$. Докажете дека $(A,*)$ е комутативна група.

23. Докажете дека, ако a е елемент на групата $(G,\circ)$ таков што $a\circ a = a$, тогаш a е единичниот елемент на групата G.

24. Во множеството $\mathbf{Q}\setminus\{0\}$ е дефинирана операција $\circ$ на следниов начин: $x\circ y = 2xy$, за секои $x,y\in\mathbf{Q}\setminus\{0\}$. Докажете дека $(\mathbf{Q}\setminus\{0\},\circ)$ е комутативна група.

25. Дадени се пресликувањата
$$f_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ f_2=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\ f_3=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$
и нека $S=\{f_1,f_2,f_3\}$. Докажете дека $(S,\circ)$ е група, каде што со $\circ$ е означена композицијата на пресликувања.

26. Дадени се пресликувањата
$$f_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ f_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ f_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\ f_4=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$
и нека $S=\{f_1,f_2,f_3,f_4\}$. Докажете дека $(S,\circ)$ е група, каде со $\circ$ е означена композицијата напресликувања. Дали оваа група е комутативна?

27. Даден е групоидот $(\mathbf{Z},*)$, што каде $x*y=x+y+3$ за секои $x,y\in\mathbf{Z}$. Дали овој групоид е комутативна група? Одговорот да се образложи!

28. Нека $A=\{1,3,\frac{1}{3},9,\frac{1}{9},27,\frac{1}{27},...,3^n,\frac{1}{3^n},...\}$ и $x*y=xy$, за секои $x,y\in A$. Докажете дека $(A,*)$ е комутативна група.

29. Нека f и g се пресликувања од $\mathbf{R}$ во $\mathbf{R}$ дефинирани со $f(x)=x$, $g(x)=1-x$, за секој $x\in\mathbf{R}$. Докажете дека $(S,\circ)$ е група, каде што $S=\{f,g\}$ и со $\circ$ е означена композицијата на пресликувања.

30. Нека $(G,*)$ е група и a е фиксен елемент од G. На G дефинираме операција $\circ$ со: $x\circ y=x*a*y$, за секои $x,y\in G$. Докажете дека $(G,\circ)$ е група.

31. Нека $(G,\cdot)$ е група. Докажете дека следниве искази се еквивалентни:
    a) G е комутативна,
    b) $(xy)^{-1}=x^{-1}y^{-1}$, за секои $x,y\in G$,
    c) $(xy)^2=x^2y^2$, за секои $x,y\in G$.

32. Ако во групата $(G,\cdot)$ важи $x^{-1}=x$, за секој $x\in G$, тогаш таа е комутативна. Докажете!

33. Групоидот $(G,\cdot)$ е група ако и само ако соодветниот спротивен групоид е група. Докажете!

34. Докажете дека секоја конечна непразна полугрупа со кратење е група.

35. Докажете дека, ако α е конгруенција во групата G, тогаш $(x,y)\in\alpha$ ако и само ако $(x^{-1},y^{-1})\in\alpha$.

36. Најдете една група пермутации изоморфна на групата $(\{1,i,-1,-i\},\bullet)$.

37. Докажете дека во секоја група $(G,\cdot)$ важи:
    1) елементите ab и ba имаат ист ред.
    2) ако елементите a и b пермутираат, тогаш пермутираат и елементите a^m и b^n, m и n се произволни цели броеви.

38. Нека G е множеството реални или комплексни броеви и нека во G е дефинирана операција $\circ$: $a\circ b=\frac{a+b}{2}$. Докажете дека групоидот $(G,\circ)$ не е асоцијативен, е комутативен и дека нема единечен елемент.

39. Ако редовите на подгрупите $(H,\cdot)$ и $(K,\cdot)$ на конечната група $(G,\cdot)$ се заемно прости броеви, докажете дека $H\cap K=\{e\}$, каде e е единичниот елемент на групата $(G,\cdot)$.

40. Ако цикличната група G е генерирана од елементот $a\in G$ со ред n, докажете дека елементот a^m ја генерира групата G ако и само ако $\mathrm{NZD}(m,n)=1$.

41. Ако G е подгрупа од H и H е подгрупа од K, докажете дека G е подгрупа од K.

42. Докажете дека пресек на две подгрупи од групата G е подгрупа од групата G.
43. Дали унија на две групи е група?
44. *Центар на групата* е множеството од сите $g \in G$ такви, што $gh = hg$ за секој $h \in G$. Докажете дека центарот на групата G е подгрупа од G.
45. Докажете, дека ако $f : G \to H$ е хомоморфизам од групата G во групата H и ако K е подгрупа од H, тогаш $f^{-1}(K)$ е подгрупа од G.
46. Докажете, дека ако $f : G \to H$ е хомоморфизам од групата G во групата H и ако K е подгрупа од G, тогаш $f(K)$ е подгрупа од H.
47. Докажете, дека ако H, J и K се подмножества од групата $(G, \circ)$, тогаш
$$(H \circ J) \circ K = H \circ (J \circ K).$$
48. Нека G е група. Секој изморфизам од G на G го нарекуваме а*втоморфизам* на G. Докажете дека за секој елемент $a \in G$ функцијата $T_a : G \to G$ определена со $T_a(g) = a^{-1}ga$ е автоморфизам на G.
49. Докажете дека секоја подгрупа на циклична група е циклична. Ако $m \mid n$, докажете дека постои подгрупа со ред m на циклична група со ред n.
50. Докажете дека сите групи со ред не поголем од 5 се комутативни.
51. Докажете дека конечна група со парен ред содржи непарен број елементи со ред 2.
52. Ако редот на секој елемент на една група, освен единичниот, е еднаков на 2, докажете дека групата е комутативна. Докажете, дека редот на оваа група е степен на бројот 2.
53. Нека a е генератор на конечната група G, $|G| = n$. Докажете дека редот на елементот $b = a^i$ е еднаков на $\frac{n}{\text{NZD}(i,n)}$.
54. Нека H, K и M се подгрупи од G, при што H е нормална во G, а K е нормална во M. Докажете дека HK е нормална подгрупа во HM.
55. Елементите на групата G од видот $x^{-1}y^{-1}xy$ ги нарекуваме *комутатори.* Докажете дека групата генерирана од множеството C од сите комутатори на G е нормална подгрупа на G.
56. Нека C е нормална подгрупа која го содржи множеството од сите комутатори на групата G. Докажете, дека фактор групата G/C е комутативна.
57. Ако $(G, +, \cdot)$ е прстен со единица e и ако G има барем два различни елементи, тогаш $e \neq 0$. Докажете!
58. Нека $G = \mathbf{P}(A)$ и нека ставиме
$$XY = X \cap Y,\ X + Y = X \dot{-} Y,$$

за секои $X, Y \in \mathbf{P}(A)$. Докажете дека $(G, +, \bullet)$ е прстен, кој го нарекуваме *Булов прстен* над множеството A.

59. Дадено е множеството $A = \{2k \mid k \in \mathbf{Z}\}$ и во него операции собирање и множење на цели броеви. Дали алгебарската структура $(A, +, \cdot)$ е комутативен прстен?

60. Докажете дека ниедна од алгебарските структури $(\mathbf{Z}, \cdot, +), (\mathbf{Z}, +, -), (\mathbf{Z}, -, \cdot), (\mathbf{Z}, \cdot, -)$ не е прстен.

61. Нека $(G, +, \cdot)$ е прстен. Докажете дека следниве тврдења се еквивалентни:
    a) G е комутативен,
    b) $(a+b)^2 = a^2 + 2ab + b^2$, за секои $a, b \in G$,
    c) $(a+b)(a-b) = a^2 - b^2$, за секои $a, b \in G$.

62. Нека $(G, +, \cdot)$ е комутативен прстен со единица. Докажете дека за секој $n \in \mathbf{N}$ и за секои $a, b \in G$ важи формулата

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{n-1}ab^{n-1} + b^n,$$

    која како и претходно ја нарекуваме *Њутнова биномна формула*.

63. Ако R е комутативен прстен со единица, тогаш
    a) $a^{n+1} - b^{n+1} = (a-b)(a^n + a^{n-1}b + \ldots + ab^{n-1} + b^n)$,
    b) $a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \ldots - ab^{2k-1} + b^{2k})$.

64. Докажете дека пресек на подпрстени е подпрстен.

65. Во кој случај унија на два подпрстени е подпрстен?

66. Со $\mathbf{Z}[x]$ да го означиме множеството полиноми по x со целобројни коефициенти. Ако со $+$ и $\cdot$ ги означиме операциите собирање и множење на полиноми, тогаш $(\mathbf{Z}[x], +, \cdot)$ е комутативен прстен со единица. Докажете!

67. Дадено е множеството

$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$$

    и во него операциите собирање и множење на реални броеви. Докажете дека алгебарската структура $(\mathbf{Q}(\sqrt{2}), +, \cdot)$ е поле.

68. Дадено е множеството

$$\mathbf{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\}$$

    и во него операциите собирање и множење на реални броеви. Докажете дека алгебарската структура $(\mathbf{Q}(\sqrt{3}), +, \cdot)$ е поле.

69. Дадено е множеството

$$\mathbf{Q}(\sqrt{6}) = \{a + b\sqrt{6} \mid a, b \in \mathbf{Q}\}$$

    и во него операциите собирање и множење на реални броеви. Докажете дека алгебарската структура $(\mathbf{Q}(\sqrt{6}), +, \cdot)$ е поле.

70. Дали алгебарската структура $(\mathbf{Z}[x], +, \cdot)$ од задачата 66 е поле? Одговорот да се образложи.

71. Дали алгебарската структура $(\mathbf{P}(M), \dot{-}, \cap)$ од задачата 58 е поле? Одговорот да се образложи.

ЛИТЕРАТУРА

1. Anderson, J. A.; Lewis, J.; Saylor, O. D.: *Discrete Mathematics with Combinatorics*, Pearson Education, Inc., 2004
2. Berge, C.: *Principles of Combinatorics*, Academic Press, New York, 1971
3. Burton, D. M.: *Elementary Number Theory*, Wm. C. Brown, Dubuque, Iowa, 1994
4. Cvetković, D.: *Diskretne matematčke strukture*, Naučna knjiga, Beograd, 1995
5. Cvetković, D.; Simić, S.: *Diskretna matematika*, Prosveta, Niš, 1995
6. Devide, V.: *Zadaci iz apstraktne algebre* I, Beograd, 1964
7. Friendlander, J. B.; Heath-Brown, D. R.; Iwaniec, H.; Kaczorowski, J.: *Analytic Number Theory*, Springer, Berlin, 2006
8. Garnier, R.; Taylor, J.: *Discrete mathematics for New Technology*, Institute of Physics Publishing, Bristol, 2002
9. Gilbert, J.; Gilbert, L.: *Elements of Modern Algebra*, PWS, Boston, 1995
10. Marshall, H. Jr.: *The Theory of Groups*, Chelsea Publishing Company, 1976
11. Mićić, V.; Kadelburg, Z.: *Uvod u teoriju brojeva*, DMS, Beograd, 1989
12. Niven, I.; Zuckerman, H. S.: *An introduction to the Theory of Numbers*, John Wiley & Sons, Inc., New York - London, 1962
13. Olmsted, J. M. N.: *The Real Number System*, Appleton-Century-Crofts, New York, 1962
14. Rosen, K.; Michaels, J.; Gross, J.; Grossman, J.; Shier, D.: *Discrete and Combinatorial Mathematics*, CRC Pres, New York, 2000
15. Shoup, V.: *A Compuaitional to Number Theory and Algebra*, Cambridge University Press, 2005
16. Stojanović, Z.; Paunić, Dj.: *Zbirka zadataka iz algebre*, Gradjevinska knjiga, Beograd, 1984
17. Tošić, R.; Vukoslavčević, V.: *Elementi teorije brojeva*, Alef, Novi Sad, 1995
18. Аляев, Ю. А.; Тюрин, С. Ф.: *Дискретная математика и математическая логика*, Финансы и статистика, Москва, 2006
19. Димовски, Д.; Тренчевски, К.; Малчески, Р.; Јосифовски, Б.: *Практикум по елементарна математика,* Просветно дело, Скопје, 1993
20. Дирихле, П. Г. Л.: *Лекции по теория на числата,* Наука и изкуство, София, 1980
21. Ерусалимский, Я. М.: *Дискретная математика,* Вуовская книга, Москва, 2004
22. Кудреватов, Г. А.: *Сборник задач по теории чисел*, Просвещение, Москва, 1970
23. Малчески, Р.: *Елементарна алгебра*, Просветно дело, Скопје, 2002
24. Малчески, Р.: *Методика на наставата по математика,* Просветно дело, Скопје, 2002
25. Малчески, Р.: *Мултипликативни функции и теорема на Ојлер,* Сигма 64, 2004

26. Малчески, Р.; Димовски, Д.; Тренчевски, К.: *Вовед во теоријата на броеви*, МММ, Скопје, 1993
27. Малчески, Р.; Малчески, А.; Аневска, К.: *Вовед во елементарна теорија на броеви*, СММ, Скопје, 2014
28. Михелович, Ш. Х.: *Теория чисел,* Высшая школа, Москва, 1967
29. Младеновиќ, П.: *Комбинаторика*, ДМС, Београд, 2001
30. Нагел, Т.: *Увод в теорията на числата,* Наука и изкуство, София, 1971
31. Плотников, А. Д.: *Дискретная математика,* ООО Новое знание, Москва, 2005
32. Самарџиски, А.; Целакоски, Н.: *Збирка задачи по алгебра, множества,* Уни. Св. Кирил и Методиј, Скопје, 1996
33. Самарџиски, А.; Целакоски, Н.: *Решени задачи по алгебра* II, (неиздаден ракопис), Скопје, 1971
34. Чупона, Ѓ.: *Алгебарски структури и реални броеви*, Просветно дело, 1976
35. Чупона, Ѓ.; Трпеновски, Б.: *Алгебра*, Унив. Св. Кирил и Методиј, Скопје

ИНДЕКС НА ПОИМИ