Мостови аритметике и алгебре

Први кораци

Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.

London 1941
G. H. Hardy

Author 1 name
Department name
email1@example.com

Author 2 name
Department name
email2@example.com

Садржај

5 Глава 1
Увод

7 Глава 2
Природни и остали бројеви

1 Релације 12
2 Функције 18
3 Операције 20
4 На почетку бјеше природан број... 22
5 ВЈЕЖБАНКА 25
6 Пребројивост и непребројивост 26

31 Глава 3
Релације, операције, пресликавања

1 Бинарне релације 33
2 Операције 34
1 Операције над скуповима 35

37 Глава 4
Дјељивост

1 Вјежбанка 41
2 Функције заокруживања 41
3 Највећи заједнички дјелилац 42
4 Еуклидов алгоритам 47
5 Бланкиншип метода 50
6 Најмањи заједнички садржалац 53
7 Представљање цијелих бројева у одређеној бази 55

59 Глава 5
Диофантове једначине

61 Глава 6
Конгруенције - рачун остатака

1 Остаци квадрата 67
2 Кинеска теорема о остацима 68
3 Примјене конгруенција 69

71 Глава 7
Увод у алгебарске структуре

1 Својства операција 74
2 Групе 81
1 Групе пермутација 87
2 Групе изометрија 89
3 Коначне групе 96
4 Мултипликативна група $\mathcal{I}_n$ 100
5 Прстени и поља 101

103 Глава 8
Прости бројеви

1 Теорема о дистрибуцији простих бројева 109

115 Глава 9
Прстен остатака модуло n

1 Ојлерова функција. Фермаова и Ојлерова теорема 115

125 Глава 10
Примитивни коријени

129 Глава 11
Упуства и рјешења

1 Увод

POGLEDATI I: Давид Буртон - ЕЛЕМЕНТАРНА ТЕОРИЈА БРОЈЕВА

Теорија бројева је дисциплина математике која се бави својствима цијелих бројева:

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Један од највећих математичара у историји математике, Карл Фридрих Гаус је рекао:

> ”Математика је краљица наука, а аритметика краљица математике.”

С обзиром на то да се са аритметиком срећемо веома рано у школи, неко би неоправдано помислио да је то зато што је ова математичка дисциплина једноствна. Напротив, она је је једна од комплекснијих, али неопходна као темељ за опште математичко образовање.

Бројеви су вјероватно прва лаичка асоцијација на математику. Леополд Кронекер, чувени њемачки математичар, рекао је

> Бог је створио цијеле бројеве, а све остало човјек.

У оригиналу, на њемачком *Die ganze Zahl schuf der liebe Gott, alles Übrige ist Menschenwerk.* Примјетимо да је *Zahl* на њемачком *број*, а то је разлог што данас користимо ознаку $\mathbb{Z}$ за скуп цијелих бројева.

Ова књига је писана са жељом да читалац успјешно прати њен ток, ослањајући се на елементарни ниво математичке писмености, постигнут у средњој школи. Наравно, основни циљ књиге би требало да буде продубљивање читалачког знања и разумијевања ове математичке дисциплине.

ПРЕПОРУЧЕНЕ КЊИГЕ ЗА НАСТАВАК РАДА У ТЕОРИЈИ БРОЈЕВА.

Као што је то урађено у Кларковој књизи, наводимо неке неријешене проблеме из Теорије бројева. Многи од наведених су дуго на тој листи и многи математичари су ”јуришали” на њих. То значи да би свако рјешење неког од њих било веома запажено у математичком универзуму, а и ван њега. Многи од тох проблема се тичу простих бројева. Подсјетимо се да је *прост број* цијели број већи од 1 који је дјељив само са 1 и самим собом.

1. (*Голдбахова хипотеза*) Сваки паран цио број $n > 2$ је сума нека два проста броја.

2. (*Хипотеза о простим бројевима - близанцима*) Постоји бесконачно много простих бројева - близанаца. [Ако су p и $p + 2$ прости бројеви, кажемо да су *близанци.*]

3. Постоји ли бесконачно много простих бројва облика $n^2 + 1$?

4. Постоји ли бесконачно много простих бројва облика $2^n - 1$? Прости бројеви овог облика се називају *Мерсенови бројеви*.

5. Постоји ли бесконачно много простих бројва облика $2^{2^n} + 1$? Прости бројеви овог облика се називају *Фермаови бројеви*.

Clark - NAVESTI

2 Природни и остали бројеви

У математици, у свим њеним дисциплинама, сусрећемо се са **скупом** као основним, градивним појмом из кога настају остали математички појмови. У описном смислу, кажемо да је скуп *колекција* објеката које називамо **елементима скупа**. Наравно, математички чистунци ће одмах поставити питање *Шта је то колекција?*. Ипак, ослонићемо се, у овом случају, на *саморазумљивост* тог појма.

Скуп се може задати конкретним навођењем његових елемената унутар витичастих заграда, као $B = \{a, b, c, 4, 5, *\}$. Често не постоји нека "везивна" карактеристика за елементе неког скупа, већ је њихово заједничко својство управо припадност том скупу. Скупове обично означавамо великим, а њихове елементе малим словима.

Напомињемо да није важан редослед навођења елемената тако да су скупови $\{1, a, b\}$ и $\{1, b, a\}$ једнаки. Такође, на скуп нема утицаја уколико вишеструко наводимо исти елемент, па је тако

$$\{a, b, c\} = \{a, a, b, b, c\} = \{c, a, a, a, a, b\}.$$

Примјер 2.1 *Скуп $A = \{a, b, c, d\}$ се састоји од четири елемента, као и скуп $B = \{1, \{1, 2, 3\}, \{1, 4\}, \{7\}\}$ чија су три елемента такође скупови.*

Међутим, за неке скупове није могуће конкретно навести све његове елементе, јер их има бесконачно

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

У опису скупа $\mathbb{N}$ је са три тачке заправо дато упуство како наставити низ. Извјесно, сви очекују да 4 долази након 3, па потом 5, 6, 7 и тако редом. Наравно, препознајемо да се ради о скупу природних бројева. Овај скуп има изузетан значај за математику уопште, а посебно за теме којима се бавимо у овој књизи.

За скуп

$$E = \{2, 4, 6, \ldots\},$$

три тачке симболизују листу свих парних природних бројева.

Сем набрајања елемената неког скупа, он се може задати и помоћу одређеног правила, попут

$$A = \{n \mid n \in \mathbb{N} \text{ и збир цифара броја } n \text{ једнак } 11\}.$$

Примјер 2.2 *Скуп природних бројева се може дефинисати на следећи начин:*

1. $1 \in \mathbb{N}$.
2. *Ако је* $x \in \mathbb{N}$, *онда је* $x + 1 \in \mathbb{N}$.
3. $\mathbb{N}$ *садржи искључиво оне бројеве који се могу добити примјеном правила 1 и 2.*

Примјећујемо да се правилима 1 и 2 генеришу сви бројеви који припадају скупу $\mathbb{N}$, *док се правилом 3 обезбјеђује да ништа друго не може наћи у скупу* $\mathbb{N}$. *Да није правила 3, не би знали да ли је било који други број, али и не само број, у скупу* $\mathbb{N}$.

Једна од опсежнијих расправа која дијели математички свијет је питање да ли нула припада скупу природних бројева. У овој књизи подразумијевамо да нула није природан број, а користимо ознаку

$$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$$

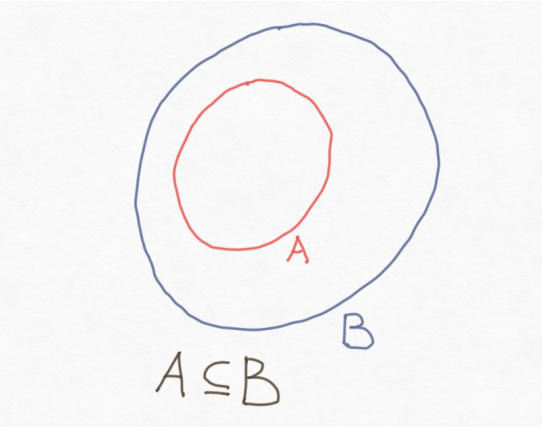
за скуп природних бројева проширен нулом. Кључни скуп за теорију бројева којом се бавимо је скуп цијелих бројева

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Скупови рационалних

$$\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z},\, n \in \mathbb{N}\},$$

к реалних бројева $\mathbb{R}$ немају посебан значај у темама ове књиге. Реални бројеви $\mathbb{R}$ могу припадати скупу рационалних $\mathbb{Q}$ или скупу $\mathbb{I}$, *ирационалних бројева*. Ирационални бројеви су они које није могуће представити у облику разломка датог у дефиницији скупа $\mathbb{Q}$, као што је на примјер $\sqrt{2}$. Доказ да је $\sqrt{2}$ ирационалан се доказује математичким средствима које остављамо за касније.



Слика 2.1: A је подскуп B

Ако је A скуп и x елемент скупа A, то записујемо $x \in A$, дочим кад x није елемент скупа A, онда пишемо $x \notin A$.

Скупове, као и односе међу њима често илуструјемо помоћу Венових дијаграма.

Ако је сваки елемент скупа A уједно и елемент скупа B, онда кажемо да је A **подскуп** скупа B и означавамо $A \subseteq B$. У овом случају кажемо да је B **надскуп** скупа A.

Два скупа A и B су једнака, пишемо $A = B$, ако је $A \subseteq B$ и $B \subseteq A$. У случају да није $A = B$, то записујемо $A \neq B$.

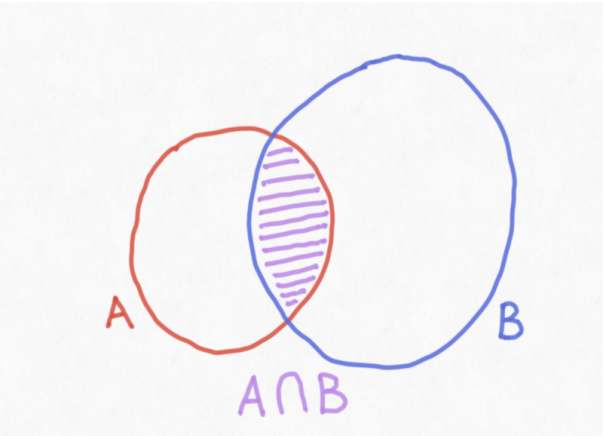
Уколико је $A \subseteq B$, али $A \neq B$, онда кажемо да је A **прави подскуп** скупа B, а то означавамо са $A \subset B$. Тривијални подскупови скупа S су празан скуп $\emptyset$ и сам скуп S. Ако A није подскуп B, пишемо $A \not\subseteq B$.

На примјер, за наведене скупове бројева, знамо да важи

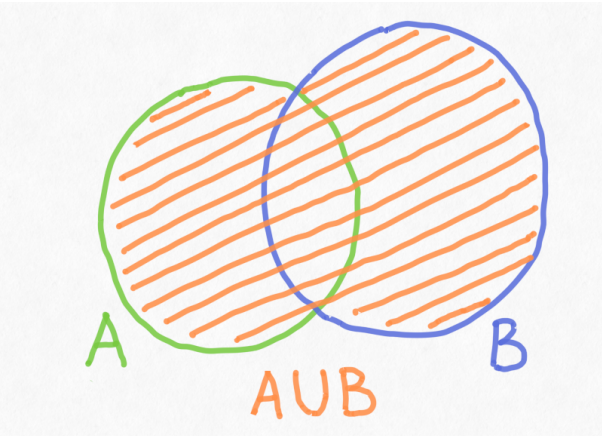
$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Пресјек два скупа A и B је скуп који садржи елементе који припадају скупу A и скупу B, а означавамо га са $A \cap B$.

Унија два скупа A и B је скуп који обухвата све елементе из скупа A и све елементе скупа B, а означавамо је са $A \cup B$. Јасно, тиме су обухваћени и елементи из пресјека ова два скупа.



(a) пресјек скупова



(b) унија скупова

Слика 2.2

Дакле,

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}, \ A \cup B = \{x \mid x \in A \text{ или } x \in B\}.$$

Примјер 2.3 *Нека је* $A = \{\star, a, 4, 12\}$, $B = \{2, 4, a, b, c, d\}$. *Онда је*

$$A \cap B = \{2, a\}, \ A \cup B = \{\star, a, b, c, d, 2, 4, 12\}.$$

Видимо да је унија два скупа увијек скуп, који обухвата све њихове елементе. Међутим, може се десити да нека два скупа немају заједничких елемената. Шта је у том случају пресјек таква два скупа? Ако захтјевамо да и пресјек два скупа обавезно буде скуп, онда би то значило да морамо да уведемо појам скупа без елемената.

Скуп који нема елемената се назива **празан скуп** и означава са $\emptyset$. У неком смислу, празан скуп међу скуповима је аналогија нуле међу бројевима. Скуп који није празан је **непразан** скуп.

Примјер 2.4 *Нека је A скуп. Пошто празан скуп нема елемената, онда је јасно да је празан скуп подскуп скупа A, као што је и сваки скуп подскуп самог себе, односно*

$$\emptyset \subseteq A \text{ и } A \subseteq A.$$

Такође, вриједи да је

$$A \cup \emptyset = A, \text{ и } A \cap \emptyset = \emptyset.$$

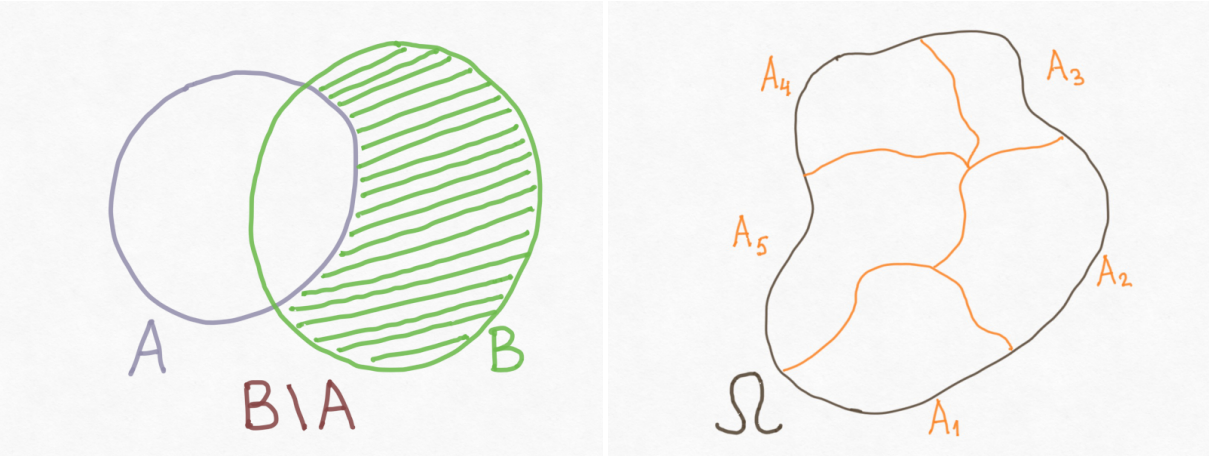
За неки природан број n, аналогно претходној дефиниције пресјека, односно уније два скупа, можемо дефинисати пресјек

$$A_1 \cap \cdots \cap A_n = \Big\{x \mid x \in A_i \text{ за свако } i \in \{1, \ldots, n\}\Big\},$$

односно унију коначног броја скупова

$$A_1 \cup \cdots \cup A_n = \Big\{x \mid x \in A_i \text{ за неко } i \in \{1, \ldots, n\}\Big\}.$$

Два скупа су **дисјунктна** ако је њихов пресјек празан скуп. За дисјунктну унију скупова A и B користимо ознаку $A \uplus B$. Општије, колекција скупова је **међусобно дисјунктна** ако су било која два члана те колекције дисјунктна.



(a) разлика скупова (b) партиција скупа

Слика 2.3

Разлику два скупа B и A чине сви елементи скупа B који се не налазе у скупу A. Дакле,

$$B \setminus A = \{x \mid x \in B \text{ и } x \notin A\}.$$

Примјер 2.5 *Нека је S скуп свих парних природних бројева, а T скуп свих рјешења једначине*

$$(x-2)^2(x-6)(3x-21)(x-11) = 0.$$

Очигледно, $T = \{2, 6, 7, 11\}$. Из овог слиједи $S \cap T = \{2, 6\}$, $S \cup T = \{7, 11, 2, 4, 6, \ldots\}$, $S \setminus T = \{4, 8, 10, \ldots\}$.

Колекција скупова је **партиција скупа** S ако је међусобно дисјунктна и ако је унија те колекције једнака скупу S. На примјер, на Слици 2.3 видимо да је

$$\Omega = A_1 \uplus A_2 \uplus A_3 \uplus A_4 \uplus A_5.$$

Нека је A подскуп скупа Ω. **Комплемент** скупа A у односу на Ω је заправо скуп $\Omega \setminus A$, што што означавамо са

$$A^c = \{x \in \Omega \mid x \notin A\}.$$

Примјетимо да кад користимо ознаку A^c, онда из контекста знамо у односу на који надскуп рачунамо комплемент датог скупа A. Такође, лако закључујемо да је $\Omega = A \cup A^c$.

Примјер 2.6 *Скупови E и O, парних и непарних природних бројева, представљају једну партицију скупа приодних бројева, јер*

$$E \cap O = \emptyset \text{ и } E \cup O = \mathbb{N}.$$

Декартов производ, $S \times T$, непразних скупова S и T се састоји од елемената облика (s,t), при чему је $s \in S$, а $t \in T$. Елемент s зовемо *прва компонента* или *прва координата*, а елемент t *друга компонента* или *друга координата* уређеног пара. За ове елементе користимо други тип заграде у односу на скупове, чиме истичемо једну важну разлику. За разлику од скупа у ком редослед није битан, па је $\{s,t\} = \{t,s\}$, за уређене парове, редослед елемената је важан и $(s,t) \neq (t,s)$. Такве елементе називамо **уређени парови**. Атрибут *уређени* долази отуд што знамо шта је на првој, а шта је на другој позицији у (s,t). Дакле,

$$S \times T = \{(s,t) \mid s \in S,\ t \in T\}.$$

Примјер 2.7 *Нека је $S = \{a,b,c\}$, $T = \{1,2\}$. Онда је*

$$S \times T = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}.$$

Није тешко закључити да је за произвољан скуп A

$$A \times \emptyset = \emptyset \times A = \emptyset.$$

Дефиницију Декартовог производа можемо уопштити на произвољан број скупова. Нека су $A_1, A_2, \ldots, A_n$ непразни скупови. Онда је

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ i = 1,2,\ldots,n\}.$$

Елементе Декартовог производа $A_1 \times A_2 \times \cdots \times A_n$ називамо **уређеним $n-$торкама.** Ако је $A_1 = A_2 = \cdots = A_n = A$, тада умјесто $A_1 \times A_2 \times \cdots \times A_n = A \times A \times \cdots \times A$ пишемо само A^n.

Примјер 2.8 *Нека је $A_1 = A_2 = \mathbb{R}$. Онда је*

$$\mathbb{R}^2 = \{(x,y) \mid x \in \mathbb{R},\ y \in \mathbb{R}\}.$$

*Скуп $\mathbb{R}^2$ представља оно што у елементарној геометрији зовемо **раван**, док скуп $\mathbb{R}^3$ представља **простор**.*

Користећи неки скуп као основ, можемо градити нове скупове на различите начине. С тим у вези, интересантан је концепт дат у следећем примјеру.

Примјер 2.9 *Нека је скуп* $A = \{1, 2, 3\}$. *Посматрајмо скуп* Ω *који се састоји од свих подскупова скупа* A. *Није тешко утврдити да је*

$$\Omega = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}.$$

Скуп свих подскупова скупа A, као у претходном примјеру, се назива **партитивни скуп** и означава са $\mathcal{P}(A)$.

На крају овог одјељка, понављамо ознаке за скупове бројеве које смо истакли:

$\mathbb{N}$ - скуп природних бројева,

$\mathbb{N}_0$ - скуп природних бројева уз укључивање нуле, односно $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

$\mathbb{Z}$ - скуп цијелих бројева,

$\mathbb{Q}$ - скуп рационалних бројева,

$\mathbb{I}$ - скуп ирационалних бројева,

$\mathbb{R}$ - скуп реалних бројева.

Међутим, ми ћемо се у овој књизи углавном бавити природним и цијелим бројевима.

2.1. Релације

Није ријетка ситуација да елементе неког скупа A *асоцирамо* са неким елементим скупа B, чиме се успоставља одређена *релација* та два скупа. Овај концепт илуструјемо у следећем примјеру.

Примјер 2.10 *Нека је* A *скуп ријека, а* B *скуп држава. Задајемо релацију* ρ *као:* $(a, b) \in \rho$ *ако и само ако ријека* $a \in A$ *протиче кроз земљу* $b \in B$. *Онда:*

1° *(Дунав, Србија)* $\in \rho$, *(Дунав, Мађарска)* $\in \rho$, *(Зета, Црна Гора)* $\in \rho$.

2° *(Волга, Италија)* $\notin \rho$, *(Лим, Данска)* $\notin \rho$.

Нека је P *скуп људи, а* S *скуп улица у неком граду. Дефинишемо релацију* θ *тако што* $p \in P$ *и* $s \in S$ *повежемо на очекивани начин*

$$(p, s) \in \theta \text{ ако и само ако особа } p \text{ станује у улици } s.$$

Претходно описани концепт, релације два скупа, могуће је дефинисати на коначном броју скупова.

Дефиниција 2.1 *Нека су $A_1, A_2, \ldots, A_n$ скупови.*

1° ***Релација*** *ρ дужине (арности) n над скуповима $A_1, A_2, \ldots, A_n$ је било који подскуп скупа $A_1 \times A_2 \times \cdots \times A_n$. Специјално, ако је $n = 2$, онда је ρ* ***бинарна релација*** *над скуповима A_1 и A_2.*

2° *Умјесто $(a_1, a_2, \ldots, a_n) \in \rho$ пишемо $\rho(a_1, a_2, \ldots, a_n)$ и кажемо да су $(a_1, a_2, \ldots, a_n)$ у релацији ρ.*

3° *Ако је ρ бинарна релација, онда умјесто $\rho(a_1, a_2)$ пишемо $a_1 \, \rho \, a_2$ и кажемо да је a_1 у релацији ρ са a_2. У супротном, ако $(a_1, a_2) \notin \rho$ кажемо да a_1 није у релацији ρ са a_2.*

Примјер 2.11 *Нека је A_1 скуп становника, A_2 скуп градова у Црној Гори, а A_3 скуп марки аутомобила. Нека је $a_1 \in A_1$, $a_2 \in A_2$ и $a_3 \in A_3$.*

За тројку (a_1, a_2, a_3) кажемо да је у релацији θ ако особа a_1 живи у граду a_2 и посједује возило марке a_3.

На примјер,

$$(\text{Урош Павићевић, Даниловград, Пежо}) \in \theta.$$

Примјер 2.12 *Нека је ρ подскуп од $\mathbb{R}^3$ дефинисан на следећи начин*

$$(x, y, z) \in \rho \text{ ако и само ако } x + y + z = 1.$$

Скуп ρ можемо представити као

$$\{(a, b, 1 - a - b) \mid a, b \in \mathbb{R}\}.$$

Јасно, у питању је раван у простору $\mathbb{R}^3$.

Бинарне релације имају посебну важност и њима посвећујемо нарочиту пажњу.

Дефиниција 2.2 *Нека је $\rho \subseteq A^2$ бинарна релација.*

1° *Ако је за свако $x \in A$, $x \, \rho \, x$, онда кажемо да је ρ* ***рефлексивна*** *релација.*

2° *Ако за свако $x, y \in A$ за које је $x \, \rho \, y$ вриједи да $y \, \rho \, x$ онда кажемо да је ρ* ***симетрична*** *релација.*

3° *Ако за свако $x, y \in A$ за које је $x \, \rho \, y$ и $y \, \rho \, x$ вриједи да $x = y$ онда кажемо да је ρ* ***антисиметрична*** *релација.*

4° *Ако за свако $x, y, z \in A$ тако да $x \, \rho \, y$ и $y \, \rho \, z$, вриједи да $x \, \rho \, z$, онда кажемо да је ρ* ***транзитивна*** *релација.*

Дефиниција 2.3 *Нека је ρ бинарна релација на супу A. Онда је ρ релација*

1° ***еквиваленције*** *ако и само ако је рефлексивна, симетрична и транзитивна,*

2° ***парцијалног уређења или поретка*** *ако и само ако је рефлексивна, антисиметрична и транзитивна,*

3° ***тоталног уређења или линеарног поретка*** *ако и само ако је то релација парцијалног уређења за коју вриједи да за свако $x, y \in A$ имамо да је $x \rho y$ или $y \rho x$.*

Примјер 2.13 *У скупу цијелих бројева, дефинисана је релација ρ на следећи начин*

$$a \rho b \Leftrightarrow a^2 + 7b = b^2 + 7a.$$

Релација ρ, за свако $a, b, c \in \mathbb{Z}$ је

1° *Рефлексивна, јер је $a^2 + 7a = a^2 + 7a$;*

2° *Симетрична. Из $a \rho b$ имамо да је $a^2 + 7b = b^2 + 7a$, па је $b^2 + 7a = a^2 + 7b$, што значи да је $b \rho a$;*

3° *Транзитивна. Из $a \rho b$ и $b \rho c$ слиједи $a^2 + 7b = b^2 + 7a$, као и $b^2 + 7c = c^2 + 7b$. Ако додамо $7c$ на обје стране једнакости у првом идентитету и замијенимо $b^2 + 7c$ са $c^2 + 7b$, имамо $a^2 + 7b + 7c = b^2 + 7c + 7a = c^2 + 7b + 7a$, одакле је $a^2 + 7c = c^2 + 7a$. Дакле, $a \rho c$.*

Тиме је показано да је ρ релација еквиваленције. Било би интересантно одредити класе еквиваленције. На примјер, није тешко закључити да ако је $a + b = 7$, онда је $a \rho b$ за цијеле бројеве a и b. Да ли вриједи обратно?

Примјер 2.14 1° *Релација сличност троуглова је релација еквиваленције у скупу свих троуглова.*

2° *Релација паралелност правих је релација еквиваленције у скупу свих правих у једној равни.*

Дефиниција 2.4 *За дату бинарну релацију θ над скуповима A и B, кажемо да је*

1° *универзална, ако је $\theta = A \times B$*

2° *празна, ако је $\theta = \emptyset$*

3° *идентитет, ако је $\theta = \{(a, b) \mid a = b\}$*

Инверзна релација релацији θ је подскуп скупа $B \times A$, а дефинишемо је као

$$\theta^{-1} = \{(b, a) \mid (a, b) \in \theta\}.$$

Примјер 2.15 *Нека је $A = B = \mathbb{Z}$, а ρ бинарна релација дефинисана на $A \times B$ као*

$$a \,\rho\, b \Leftrightarrow a^2 + b^2 + 1 > 0.$$

Очигледно, сваки пар цијелих бројева задовољава релацију ρ, па је у питању универзална релација.

Релација θ на $A \times B$ дефинисана

$$a \,\theta\, b \Leftrightarrow a + b = 0.5$$

је очигледно празна релација, јер не постоји пар цијелих бројева који задовољава задати услов.

Релација ψ на $A \times B$ дефинисана

$$a \,\psi\, b \Leftrightarrow a - b = 0$$

је идентитет.

Примјер 2.16 *У скупу X дефинисана је релација ρ на следећи начин*

$$x \,\rho\, y \Leftrightarrow x - y \in X$$

Испитати врсту релације ρ у скупу X ако је
а. $X = \mathbb{N}_0$; ***б.*** $X = \mathbb{Z}$

Примјер 2.17 *Нека је дат непразан скуп A. Посматрамо бинарну релацију "подскуп од", $\subseteq$, на партитивном скупу $P(A)$ скупа A, односно на скупу свих његових подскупова. То значи да су два подскупа S и скупа A "у релацији" ако и само ако је $S \subseteq T$.*

Пошто је релација "подскуп од" рефлескивна, антисиметрична и транзитивна, онда је то релација (парцијалног) поретка. Међутим, ово није релација линеарног поретка јер S и T могу бити подскупови, такви да нити је $S \subseteq T$ нити је $T \subseteq S$.

На примјер, ако је $A = \{a, b\}$, онда је $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. У овом случају јасно је да $\{a\}$ није подскуп од $\{b\}$, као ни обратно.

Примјер 2.18 *Посматрајмо бинарну релацију θ на скупу $A = \{1, 2, \ldots, 100\}$ дефинисану са*

$$(k, m) \in \theta \Leftrightarrow k \text{ дијели } m,$$

за $(k, m) \in A \times A$. Лако се закључује да је релација θ релација парцијалног поретка. Међутим, $(2, 3) \notin \theta$ као и $(3, 2) \notin \theta$, па ово није релација тоталног поретка.

Да ли је релација θ дефинисана на скупу $\mathbb{N}$ релација парцијалног поретка? А на скупу $\mathbb{Z}$?

Дефиниција 2.5 *Нека је ρ релација еквиваленције на скупу A. За елемент $a \in A$, скуп*

$$[a]_\rho = \{x \in A \mid a \,\rho\, x\}$$

*називамо **класом еквиваленције** елемента a у односу на задату релацију ρ.*

***Количнички скуп** или **скуп класа еквиваленције** за релацију ρ је*

$$A/\rho = \{[a] \mid a \in A\}.$$

Уколико је из контекста јасно о којој релацији се ради, онда се умјесто ознаке $[a]_\rho$ користи само $[a]$.

Примјер 2.19 *У скупу $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ дефинисана је релација*

$$x \,\rho\, y \Leftrightarrow xy > 0, x, y \in \mathbb{Z} \setminus \{0\}.$$

Показати да је ρ релација еквиваленције. Одредити класе еквиваленције елемената -1 и 1.

$$[-1] = \{x \mid x \in \mathbb{Z},\, x < 0\} = \{-1, -2, -3, \ldots\}$$

$$[1] = \{x \mid x \in \mathbb{Z},\, x > 0\} = \{1, 2, 3, \ldots\}$$

Очигледно, ово двије класе еквиваленције покривају цијели скуп на ком је релација дефинисана, па је

$$\mathbb{Z}^*/\rho = \{[-1], [1]\}.$$

Лема 2.1 *Нека је ρ релација еквиваленцијена скупу A, а a и b два различита елемента из A. Онда*

1. $[a] = [b]$ *ако и само ако* $(a, b) \in \rho$.
2. $[a] = [b]$ *ако и само ако* $(a, b) \notin \rho$.

$$[a] = [b] \text{ или } [a] \cap [b] = \emptyset.$$

Доказ. Разликујемо два случаја

1. Елементи a и b су у релацији ρ. Ако је $x \in [a]$, односно $a \rho x$, односно $x \rho a$ због симетричности релације ρ. Онда из својства транзитивности релације ρ слиједи да је $x\rho b$, што значи да је $x \in [b]$. Дакле, $[a] \subseteq [b]$. Аналогно, закључујемо да је и $[b] \subseteq [a]$, из чега слиједи да је $[a] = [b]$.

2. Елементи a и b нису у релацији ρ. Претпоставимо да је $x \in [a] \cap [b]$. Слиједи да је $a \rho x$ као и $b \rho x$, односно $x \rho b$ због симетричности релације ρ. На основу транзитивности, из $a \rho x$ и $x \rho b$, закључујемо да је ρb, што је контрадикција у односу на претпоставку. Дакле, $[a] \cap [b] = \emptyset$.

■

Како је $a \rho a$, за свако $a \in A$, онда су елементи скупа A/ρ, иначе подскупови A, непразни. На основу овог имамо следеће тврђење.

Лема 2.2 *Нека је дата ρ релација еквиваленције на скупу A. Онда је A дисјунктна унија класа еквиваленције у односу на дату релацију ρ.*

Доказ. Доказујемо да је A/ρ партиција скупа A. Пошто за свако $a \in A$ вриједи да је $a \in [a]$, онда

$$\bigcup_{a \in A} \{a\} \subseteq \bigcup_{[a] \in A/\rho} [a].$$

С друге стране, имамо да је $[a] \subseteq A$, за свако $a \in A$, па је

$$A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{[a] \in A/\rho} [a] \subseteq A.$$

Како су, на основу Леме 2.1, елементи A/ρ дисјунктни подскупови A, имамо да је

$$A = \dot{\bigcup_{[a] \in A/\rho}} [a].$$

■

Претходна теорема нам указује да класе еквиваленције на скупу A у односу на дату релацију еквиваленције ρ чине заправо партицију тог скупа. Ово тврђење је од изузетног значаја и примјенљиво је у многим областима математике.

2.2. Функције

Појам *функције* или *пресликавања* је један од основних у математици. Функција представља неко *правило придруживања* елемената скупа A елементима скупа B. Свака функција је заправо бинарна релација над скуповима A и B, али која задовољава одређена својства наведена у следећој дефиницији.

Дефиниција 2.6 *Нека је $A \neq \emptyset$ и $B \neq \emptyset$, а f релација, подскуп од $A \times B$ која задовољава својство да за свако $x \in A$ постоји тачно један $y \in B$ тако да $(x, y) \in f$.*

Тада f називамо ***пресликавање*** *из A у B и означавамо $f : A \to B$. Уколико је $(x, y) \in f$, то записујемо са $f(x) = y$. Елемент x називамо* ***оригинал****, док за елемент $y = f(x)$ кажемо да је* ***слика*** *елемента x при пресликавању f, односно вриједност funkcije у тачки x.*

Ако је $f : A \to B$, онда A зовемо **домен**, а B **кодомен** пресликавања f. **Слика функције**, у ознаци $Im(f)$ или $f(A)$ је скуп $\{f(x) \mid x \in A\}$. Скуп свих функција из скупа A у скуп B означавамо са B^A.

За пресликавања $f : A \to B$ и $g : C \to D$ кажемо да су једнака, а записјемо $f = g$, уколико су $A = C$, $B = D$ и за свако $x \in A$ вриједи $f(x) = g(x)$.

Идентичка функција на скупу A, $id_A \subseteq A \times A$ је дефинисана sa $id_A(x) = x$, за сваки $x \in A$.

Примјер 2.20 *Као што је истакнуто у претходној дефиницији, свака функција јесте релација, али обратно не мора да важи.*

1° *Бинарна релација $\{(1, a), (2, b), (3, b)\}$ је функција дефинисана на скупу $A = \{1, 2, 3\}$. Скуп слика, односно вриједности ове функције је скуп $\{a, b\}$.*

2° *Бинарна релација над скупом $\mathbb{Q}$*

$$\chi = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x = y^2\}$$

није функција. Наиме, за $x = 4$, постоје $y = 2$ и $y = -2$ за које су $(4, 2)$, $(4, -2) \in \chi$.

3° *Релација $\{x, x^2 + x + 1) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$ је функција јер из $x = u$ слиједи*

$$x^2 + x + 1 = u^2 + u + 1$$

и за свако $x \in \mathbb{R}$ постоји $x^2 + x + 1 \in \mathbb{R}$. Дакле, овдје се ради о функцији $x \to f(x) = x^2 + x + 1$ која пресликава $\mathbb{R}$ у $\mathbb{R}$. Скуп слика је $f(\mathbb{R}) = [3/4, \infty)$.

Дефиниција 2.7 *Нека је $f : A \to B$ пресликавање. Ако је $f(A) = B$, онда кажемо да је f* ***на*** *или* ***сирјективно****, односно да је f* ***сирјекција****.*

Ако за свако $a_1, a_2 \in A$ и $a_1 \neq a_2$ вриједи да је $f(a_1) \neq f(a_2)$, онда кажемо да је f ***1-1*** *или* ***инјективно*** *пресликавање, односно да је f* ***инјекција****.*

Уколико је f сирјективно и инјективно, онда за f кажемо да је f ***бијективно****, односно да је f* ***бијекција****.*

Бијекције скупа A у себе називамо ***пермутације****.*

Примјер 2.21 *Нека је $f : \mathbb{Z} \to \mathbb{N}$ пресликавање дефинисано са*

$$f(x) = x^2.$$

Ово пресликавање није инјективно, јер је, на примјер, $f(-1) = f(1)$. Такође, f није ни сирјективно јер 2 није у скупу $Im(f)$. Заправо, уочавамо да је слика функције $Im(f) = \{1, 4, 9, \ldots\}$ прави подскуп кодомена $\mathbb{N}$.

Дефиниција 2.8 *Нека су дате функције $f : A \to B$ и $g : B \to C$. Композиција функција f и g, у ознаци $g \circ f$ је скуп*

$$(g \circ f) = \{(x, z) \mid \text{ постоји } y \in B \text{ за које је } f(x) = y \text{ и } g(y) = z\}.$$

С обзиром на то да су f и g функције, лако се показује да је и композиција функција $(g \circ f)$ такође функција, и то

$$(g \circ f) : A \to C,$$

за коју је $(g \circ f)(x) = g(f(x))$. Наиме за сваки $x \in A$ постоји тачно један $y \in B$ за који је $f(x) = y$, а такође за тај $y \in B$ тачно један $z \in C$ такав да је $g(y) = z$, одакле је испуњен услов из Дефиниције 2.6 да за сваки $x \in A$ постоји тачно један $z \in C$ такав да је $(x, z) \in g \circ f$. Следећа теорема истиче важно својство *асоцијативности* композиције пресликавања.

Теорема 2.1 *Нека су $f : A \to B$, $g : B \to C$ и $h : C \to D$ пресликавања.*
Онда је

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Доказ. За произвољно $x \in A$ вриједи

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$$

одакле слиједи тврђење. ■

2.3. Операције

Са појмом операција смо се сусрели још у основној школи говорећи о сабирању, одузимању, множењу и дијељењу. Овај појам проширујемо следећом дефиницијом.

Дефиниција 2.9 *Нека је A непразан скуп, а $n \in \mathbb{N}$. Функција $f : A^n \to A$ се назива $n-$арна операција или операција* ***арности*** *n на скупу A.*

У случају кад је $n = 1$, кажемо да је у питању ***унарна****, а кад је $n = 2$* ***бинарна*** *операција.*

Примјер 2.22 *Функција $f : \mathbb{Z} \to \mathbb{Z}$, дефинисана са*

$$f(a) = -a$$

је унарна операција на $\mathbb{Z}$. Функција $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ дефинисана са

$$g(z_1, z_2) = z_1 z_2 + z_1^2 - 1$$

је бинарна операција на $\mathbb{Z}$.

У случају бинарних операција, $\star : A^2 \to A$, слично као и код релација, користи се другачија нотација, па умјесто $\star(x, y)$ обично пишемо $x \star y$.

Примјер 2.23 *Помоћу стандардних бинарних операција (сабирање, одузимање, множење) на скупу цијелих бројева, можемо уводити нове операције на скупу цијелих бројева. На примјер,*

$$a \star b = ab + a - 1.$$

Очигледно, могућности за увођење нових операција има бесконачно, али је питање мотивације, односно смисла за тако конструисане операције.

Наводимо и примјер јерне опрације арности 4, односно пресликавање из $\mathbb{R}^4$ у $\mathbb{R}$. Користимо познату, детерминантну фунцкцију

$$(a_1, a_2, a_3, a_4) \to \det \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

Примјер 2.24 *Посматрајмо скуп $A = \{1, 2, 3\}$ и скуп свих пермутација на овом скупу. Као што знамо, ради се о бијективним пресликавањима скупа $\{1, 2, 3\}$ у себе, те их можемо на природан начин представити у облику*

$$f = \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix},$$

гдје су i, j, k различити елементи скупа $\{1, 2, 3\}$. На примјер,

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

*је **идентичка** пермутација, у којој се сваки елемент пресликава у себе. Скуп свих пермутација над скупом од 3 елемента означавамо као S_3 и знамо да их има $3 \cdot 2 \cdot 1 = 6$. Скуп $S_3 = \{id, f_1, f_2, f_3, f_4, f_5\}$, гдје су*

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{pmatrix}$$

Посматрајмо композиције пермутација на S_3, попут:

$$f_3 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_1$$

Дакле, композиција двије функције је очигледно бинарна операција на скупу S_3. У следећој табели су дате све операције на посматраном скупу:

$\circ$	id	f_1	f_1	f_1	f_1	f_1
id	id	f_1	f_1	f_1	f_1	f_1
f_1	id	f_1	f_1	f_1	f_1	f_1
f_2	id	f_1	f_1	f_1	f_1	f_1
f_3	id	f_1	f_1	f_1	f_1	f_1
f_4	id	f_1	f_1	f_1	f_1	f_1
f_5	id	f_1	f_1	f_1	f_1	f_1

Примјер 2.25 *Нека је S непразан скуп, а $\mathcal{P}(S)$ његов партитивни скуп. На партитивном посматрамо **пресјек**, **унију**, **разлику** скупова као бинарне операције*

$$(A_1, A_2) \to A_1 \cap A_2, \ (A_1, A_2) \to A_1 \cup A_2, \ (A_1, A_2) \to A_1 \setminus A_2.$$

*гдје су A_1, $A_2 \in \mathcal{P}(S)$. С друге стране, **комплемент** је унарна операција на $\mathcal{P}(S)$*

$$A \to A^c,$$

за $A \in \mathcal{P}(S)$.

2.4. На почетку бјеше природан број...

На почетку математичке Библије *скуп цијелих бројева* $\mathbb{Z}$ има снагу Ријечи, као што је то рекао Кронекер: *Бог је створио цијеле бројеве, све остало човјек.*

Сматрамо да су основне особине $\mathbb{N}$ и $\mathbb{Z}$ општепознате, те их нећемо посебно истицати. Два еквивалентна принципа, принцип доброг уређења и принцип математичке индукције, су посебно важна за доказивање тврђења која су у вези са природним бројевима.

Принцип доброг уређења за скуп природних бројева $\mathbb{N}$: *Сваки непразни подскуп скупа* $\mathbb{N}$ *садржи најмањи елемент.*

Иако овај принцип јесте усаглашен са већ формираним представама о природним бројевима, узима се као полазни, онај из ког се изводе сложенији закључци. Илуструјемо га у наредном примјеру.

Примјер 2.26 *Најмањи елемент скупа* $A = \{14, 5, 8, 16777, 64, 6\}$ *је број* 5.

Најмањи елемент скупа B*, свих природних бројева чији је збир цифара* 10*, је број* 19*. Скуп* B *је бесконачан. На примјер, сви бројеви облика* $10\ldots09$ *припадају* B*.*

Као што је истакнуто, принцип доброг уређења је еквивалентан принципу математичке индукције. То значи да је, аксиоматским усвајањем једног од ова два принципа, могуће доказати онај други.

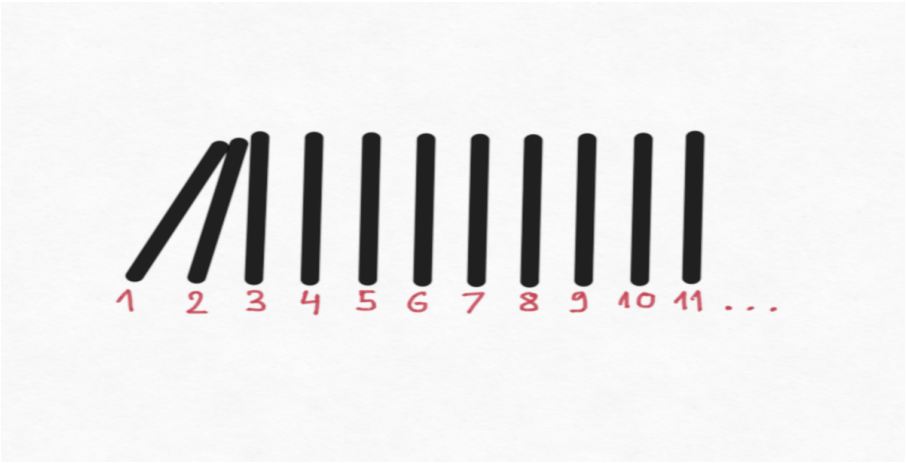
Принцип математичке индукције: Нека је $P(n)$ тврђење које се односи на природан број n. Ако су испуњени услови

(а) $P(n_0)$ је тачно;

(б) Под претпоставком да је $P(i)$ тачно за природне бројеве $n_0 \leq i \leq k$ за неки природан број k (**индуктивна претпоставка**), тачан је исказ $P(k+1)$;

онда је тврђење $P(n)$ тачно за свако $n \geq n_0$.

Дакле, *принцип математичке индукције* или скраћено индукција је средство којим доказујемо тврђења која се односе на природне бројеве, претпостављамо почевши од одређеног природног броја n_0. Уколико успијемо да докажемо да тачност неког тврђења $P(n)$ за почетни случај $P(n_0)$, тиме смо закључили **ПМИ (а)**. Други дио индукције који означавамо са **ПМИ (б)** је доказ да из претпоставке о тачности тврђења за природне бројеве закључно са неким природним бројем k слиједи и тврђење за $k+1$, при чему је $k \geq n_0$. Након што се комплетира **ПМИ (а)** и **ПМИ (б)**, закључујемо да је исказ $P(n)$ тачан за све природне бројеве $n \geq n_0$.



Слика 2.4: домине - илустрација математичке индукције

Сликовито, принцип математичке индукције илуструјемо тако што што замислимо бесконачан низ поређаних домина. Претпоставимо да је *оборена* прва домина у низу, односно да је остварен корак **ПМИ (а)**. Ако су домине тако поређане да је пад првих k обавезно узрокује пад $(k+1)-$е, што одговара кораку **ПМИ (б)**, онда је јасно да ће обарањем прве у низу *пасти* цијели низ.

Примјер 2.27 *За сваки природни број n, вриједи тврђење*

$$\underbrace{1+2+\cdots+n=\frac{n(n+1)}{2}}_{\text{тврђење } P(n)}$$

Очигледно, можемо провјеравати тачност исказа за појединачне вриједности као што су $P(1)$, $P(4)$, $P(12),\ldots$ Међутим, тако не постижемо општост, не утврђујемо важење тврђења $P(n)$ за сваки природан број. Потребан нам је приступ који то обезбјеђује, од појединачног ка општем, а који је садржан у представљеном принципу математичке индукције.

- *Видимо да је за $n=1$ тврђење тачно, јер*

  $$1=\frac{1(1+1)}{2},$$

  чиме је потврђен први корак, ***ПМИ (а)****.*

- *Други корак,* ***ПМИ (б)****, почиње индуктивном претпоставком да је $P(k)$ тачно, односно да вриједи*

  $$1+2+\cdots+k=\frac{k(k+1)}{2}.$$

  Користећи претходно, можемо лијевој и десној страни додати $k+1$. Тиме добијамо

  $$1+2+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1),$$

  одакле је

  $$1+2+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2},$$

  што значи да је $P(k+1)$ потврђено. Тиме смо испунили и други услов индукције, ***ПМИ (б)****, па је тврђење $P(n)$ доказано за свако n.*

Примјер 2.28 *Ако $n\geq 5$ онда $2^n>5n$.*

Доказ. Јасно, овдје је $P(n)$ исказ да је $2^n>5n$, за $n\geq 5$, па је $n_0=5$. Дакле, пишемо

$$P(n)=2^n>5n \text{ и } n_0=5.$$

Као што је наведено у самој дефиницији, $P(n)$ увијек представља *исказ*, обично неједнакост или једнакост, а повремено и неку компликованију тврдњу.

У овом случају, ако је $n=4$ онда $P(n)$ постаје исказ $2^4>5\cdot 4$ који је нетачан! Међутим, за $n=5$, $P(n)$ је исказ $2^5>5\cdot 5$ или $32>25$ што је тачно, па смо тиме установили тачност корака **ПМИ (а)**.

У циљу да докажемо дио који се односи на **ПМИ (б)** *подразумијевамо* да је

$$P(n) \text{ тачно за } 5\leq n\leq k.$$

Дакле, индуктивна претпоставка је да

$$2^i > 5i \text{ за } \ 5 \leq i \leq k. \tag{2.1}$$

Доказујемо тачност $P(k+1)$. Како је по индутивној претпоставци тачно $P(k)$, односно

$$2^k > 5k,$$

онда множењем лијеве и десне стране неједнакости са 2 добијамо

$$2^{k+1} > 10k. \tag{2.2}$$

Не губимо из вида да је наш циљ да покажемо да је тачно $P(k+1)$ односно $2^{k+1} > 5(k+1)$. Јасно, $5(k+1) = 5k+5$, па ако покажемо да је $10k \geq 5k+5$ онда можемо искористити неједнакост (2.2) за комплетирање доказа.

Како је $10k = 5k + 5k$ и $k \geq 5$ по (2.1), онда $k \geq 1$ и зато $5k \geq 5$. Слиједи

$$10k = 5k + 5k \geq 5k + 5 = 5(k+1).$$

Дакле,

$$2^{k+1} > 10k \geq 5(k+1),$$

па

$$2^{k+1} > 5(k+1). \tag{2.3}$$

што значи да је $P(i)$ тачно кад је $i = k+1$. Према томе, користежи индуктивну претпоставку (2.1) доказали смо (2.3). Тиме је доказан и корак ПМИ (б), а то значи да је методом математичке индукције доказано да $P(n)$ важи за $n \geq 5$. Коначо, слиједи да $2^n > 5n$ за $n \geq 5$. ■

2.5 ВЈЕЖБАНКА

1

Доказати да је $2^n > 6n$ за $n \geq 5$.

2

Доказати да је

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$

за $n \geq 1$.

3

Доказати да је

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

ако $n \geq 1$.

4

Доказати да ако $0 < a < b$ онда $0 < a^n < b^n$ за свако $n \in \mathbb{N}$.

Рјешење. аааа ■

5

Доказати да $n! < n^n$ за $n \geq 2$.

6

Доказати да ако су a and r реални бројеви и $r \neq 1$, онда за $n \geq 1$

$$a + ar + ar^2 + \cdots + ar^n = \frac{a\left(r^{n+1} - 1\right)}{r - 1}.$$

7

Доказати да $\underbrace{111\cdots1}_{n} = \dfrac{10^n - 1}{9}$ за $n \geq 1$.

8

Доказати да ако је $n \geq 12$ онда n може бити написано као збир бројева 4 и 5. На примјер, $23 = 5 + 5 + 5 + 4 + 4 = 3 \cdot 5 + 2 \cdot 4$.

2.6. Пребројивост и непребројивост

У општем случају, скуп може имати **коначно** или **бесконачно** много елемената. У случају да је S непразан и има коначно много елемената, то записујемо

$$S = \{x_1, x_2, \ldots, x_n\},$$

гдје n означава број елемената тог скупа. Код бесконачних скупова имамо додатну класификацију. Наиме, бесконачност скупа може бити **пребројива** или **непребројива**. За заснованији, прецизнији увид у ове појмове би било неопходно направити озбиљнију математичку припрему. Покушаћемо да ове појмове освијетлимо кроз неколико упечатљивих примјера.

За скуп S ћемо рећи да је **пребројив** уколико постоји начин да елементе тог скупа поставимо у низ

$$x_1, x_2, \ldots, x_m, \ldots,$$

односно да за сваки елемент $a \in S$ одредимо његову тачну позицију у низу. Парни бројеви мањи од 20 се могу поређати у низ

$$2, 4, 6, 8, 10, 12, 14, 16, 18.$$

Дакле, у питању је коначан скуп са 9 елемената. Међутим, могуће је да у низ смјестимо и бесконачне скупове. На примјер, скуп цијелих бројева је могуће ставити у низ

$$0, 1, -1, 2, -2, \ldots$$

чиме обезбјеђујемо да се тачно зна позиција сваког цијелог броја. Рецимо, број 426 је на 952-ој позицији, док је -125 на 249-ој позицији. Очигледна је функција којом се одређује позиција појединих цијелих бројева.

Ако пажљивије посматрамо концепт пребројивости, онда разликујемо случај кад је посматрани скуп S

1. **Коначан**. У овом случају елементе скупа S можемо поређати у низ на позицијама

   $$1, \ldots, n,$$

   гдје је n број елемената у скупа S.

2. **Бесконачан.** Елементе скупа S у овом случају ређамо на позицијама

   $$1, 2, \ldots.$$

Изражавајући се језиком пресликавања, видимо да у првом случају постоји бијекција скупа $\{1, \ldots, n\}$ са скупом S. Интересантно је да је и скуп рационалних бројева бесконачно пребројив. У следећем дијаграму је представљена техника пребројавања рационалних бројева.

$$
\begin{tikzcd}
\frac{1}{1} \arrow[d] & \frac{1}{2} \arrow[r] & \frac{1}{3} & \frac{1}{4} \arrow[r] & \frac{1}{5} & \cdots \\
\frac{2}{1} \arrow[ur] & \frac{2}{2} \arrow[dl] & \frac{2}{3} \arrow[ul] & \frac{2}{4} \arrow[dl] & \frac{2}{5} \arrow[ul] & \cdots \\
\frac{3}{1} \arrow[d] & \frac{3}{2} \arrow[ur] & \frac{3}{3} \arrow[dl] & \frac{3}{4} \arrow[ul] & \frac{3}{5} \arrow[dl] & \cdots \\
\frac{4}{1} \arrow[ur] & \frac{4}{2} \arrow[dl] & \frac{4}{3} \arrow[ul] & \frac{4}{4} \arrow[dl] & \frac{4}{5} \arrow[ul] & \cdots \\
\frac{5}{1} \arrow[d] & \frac{5}{2} \arrow[ur] & \frac{5}{3} \arrow[dl] & \frac{5}{4} \arrow[ul] & \frac{5}{5} \arrow[dl] & \cdots \\
\vdots \arrow[ur] & \vdots \arrow[dl] & \vdots \arrow[ul] & \vdots \arrow[dl] & \vdots \arrow[ul] &
\end{tikzcd}
$$

Као што се види из дијаграма, полазећи од лијевог ћошка и редом *бројимо* све елементе из скупа рационалних бројева. Наравно, неки елементи попут 1 и 2/2, или 1/3 и 2/6, се понављају, али прескачемо све оне које смо већ видјели, односно претходно уврстили у низ. Они су прецртани. Тако долазимо до низа

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{1}{3}, \cancel{\frac{2}{2}}, \frac{3}{1}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{1}{5}, \cancel{\frac{2}{4}}, \cancel{\frac{3}{3}}, \cancel{\frac{4}{2}}, \frac{1}{5}, \ldots$$

За разлику од скупова који се могу *спаковати* у низ, постоје они скупови за које то није могуће. У тим случајевима, само задавање скупа обично вршимо на алтернативан начин, користећи одређено својство P које одређује елементе скупа

$$\{x \mid x \text{ задовољава } P\}.$$

На примјер, скуп реалних бројева из интервала $[0, 1]$ се може записати као $\{x \mid 0 \leq x \leq 1\}$. За разлику од, на примјер, скупа рационалних бројева, овај скуп није могуће спаковати у низ. Претпоставимо супротно, да постоји низ којим су обухваћени сви бројеви из датог скупа

$$
\begin{array}{cccccc}
0. & d_{11} & d_{12} & d_{13} & d_{14} & \ldots \\
0. & d_{21} & d_{22} & d_{23} & d_{24} & \ldots \\
0. & d_{31} & d_{32} & d_{33} & d_{34} & \ldots \\
0. & d_{41} & d_{42} & d_{43} & d_{44} & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

Посматрајмо реални број који је конструисан на следећи начин

$$x = 0.b_1 b_2 b_3 b_4 \ldots$$

при чему је b_i изабран тако да се разликује од цифре d_{ii}, што значи да се x сигурно разликује од $i-$тог броја у претходном низу, за $i = 1, 2, \ldots$. Дакле, x се по конструкцији

разликује од сваког броја из претходног низа, а ипак припада интервалу $[0, 1]$. То значи да претходним низом нису обухваћени сви бројеви из датог интервала, па је посматрани скуп **непребројив**.

3 Релације, операције, пресликавања

Дефиниција 3.1 *Нека је $A \neq \emptyset$.*

1° *Скуп ρ, подскуп скупа A^n, називамо n-**арна релација или релација дужине** n скупа A. Специјално, ако је $n = 2$, онда је ρ **бинарна релација** скупа A;*

2° *Умјесто $(a_1, a_2, \ldots, a_n) \in \rho$ пишемо $\rho(a_1, a_2, \ldots, a_n)$ и кажемо да су елементи $n-$торке $(a_1, a_2, \ldots, a_n)$ **у релацији** ρ.*

3° *Ако је ρ бинарна релација, онда умјесто $\rho(a_1, a_2)$ пишемо $a_1 \, \rho \, a_2$.*

Примјер 3.1 *Нека је ρ подскуп од $\mathbb{R}^3$ дефинисан на сљедећи начин*

$$(x, y, z) \in \rho \text{ ако и само ако } x + y + z = 1.$$

Да ли можете рећи о каквом подскупу простора $\mathbb{R}^3$ се ради? Да ли је $\rho = \mathbb{R}^3$?

Они који имају неко ретходно искуство из дијела математике која се зове аналитичка геометрија ће лако препознати да се ради о равни у простору $\mathbb{R}^3$. Такође, врло се лако утврђује да $\rho \neq \mathbb{R}^3$, јер, на примјер, координатни почетак, односно тачка $(0, 0, 0)$ извјесно не припада релацији ρ.

Дефиниција 3.2 *Нека је $A \neq \emptyset$ и $B \neq \emptyset$, а f подскуп од $A \times B$ који задовољава својство да за свако $x \in A$ постоји тачно један $y \in B$ тако да $(x, y) \in f$.*

*Тада f називамо **пресликавање** из A у B и означавамо $f : A \to B$. Уколико је $(x, y) \in f$, то записујемо са $f(x) = y$.*

*Ако је $f : A \to B$, онда A зовемо **домен**, а B **кодомен** пресликавања f.*

Примјер 3.2 *Нека је* $A = \{1, 2, 3, 4, 5\}$, *а* $B = \{x, y, z, w\}$. *Релација*

$$f = \{(1, x), (2, x), (2, y), (3, w), (4, z), (5, z)\}$$

није пресликавање јер за $2 \in A$ *постоје два елемента из* $y, w \in B$, *тако да* $(2, x), (2, y) \in f$.

Примјер 3.3 *Нека је* $A = \{1, 2, 3, 4, 5\}$, *а* $B = \{x, y, z, w\}$. *Релација*

$$g = \{(1, x), (2, x), (3, w), (4, z)\}$$

није пресликавање јер за $5 \in A$ *не постоји елемент* y *из* B *тако да* $(5, y) \in B$.

Примјер 3.4 *Нека је* $A = \{1, 2, 3, 4, 5\}$, *а* $B = \{x, y, z, w\}$. *Релација*

$$h = \{(1, x), (2, x), (3, w), (4, z), (5, z)\}$$

јесте пресликавање јер за свако $x \in A$ *постоји тачно један* y *из* B *тако да* $(x, y) \in B$.

Претпоставимо да је дато пресликавање $f : A \to B$, а $A' \subseteq A$. Онда је скуп

$$f(A') := \{f(a) \mid a \in A'\}$$

слика подскупа A' пресликавањем f. У Примјеру 3.4, видимо да је

Сходно томе, можемо посматрати и рестрикцију пресликавања f на скуп A', коју означавамо са $f|_{A'}$, а то значи да је домен пресликавања

$$f|_{A'} : A' \to B$$

скуп A', док је кодомен $f(A') \subseteq B$.

Примјер 3.5 *Посматрајмо пресликавање* $f : \mathbb{Z} \to \mathbb{Q}$ *дефинисано као*

$$f(x) = x/2.$$

Нека је скуп свих парних природних бројева, односно $A = \{2n \mid n \in \mathbb{N}\}$. *Јасно је,* $A \subseteq \mathbb{Z}$. *Није тешко закључити да је* $f(A) = \mathbb{N}$.

Дефиниција 3.3 *Нека је* $f : A \to B$.

а. Ако је $f(A) = B$, *онда кажемо да је* f ***сирјекција*** *или* ***на***.

б. Ако за свако $a_1, a_2 \in A$ *и* $a_1 \neq a_2$ *вриједи да је* $f(a_1) \neq f(a_2)$, *онда* f *зовемо* ***инјекција*** *или* ***1-1***.

в. Уколико је f *сирјекција и инјекција, онда за* f *кажемо да је* ***бијекција***.

Најједноставнији примјер бијекције је идентичко пресликавање $I_A : A \to A$ дефинисано са

$$I_A(a) = a,$$

за свако $a \in A$.

НАЦРТАТИ НЕКЕ ПРИМЈЕРЕ!

Нека је $f : A \to B$ бијективно пресликавање. Установимо пресликавање $f^{-1} : B \to A$ тако што за $b \in B$ дефинишемо

$$f^{-1}(b) := a,$$

при чему је a јединствени елемент скупа A тако да $f(a) = b$. Свакако, јединственост елемента a проситиче из чињенице да је f бијекција. Овако дефинисано пресликавање f^{-1} називамо инверзно пресликавање у односу на пресликавање f. Очигледно, оно је једнозначно одређено пресликавањем f.

Ако је $f : A \to B$ и $g : B \to C$, онда можемо дефинисати и композицију пресликавања $g \circ f$ које представља пресликавање из A u C, а дефинишемо га као

$$g \circ f(a) := g(f(a)).$$

Лема 3.1 *Нека је $f : A \to B$ бијекција.*

а. Инверзно пресликавање $f^{-1} : B \to A$ је бијекција.

б. Композиција $f^{-1} \circ f = I_A$ док је $f \circ f^{-1} = I_B$.

Примјер 3.6 *Нека је $A = \mathbb{R}$ и $B = \{y \mid y \in \mathbb{R} \text{ и } y \geq 0\}$. Онда је*

$$f = \{(x, x^2) \mid x \in \mathbb{R}\}$$

пресликавање које називамо парабола.

3.0.1. Бинарне релације

Дефиниција 3.4 *Нека је ρ бинарна релација скупа A.*

*Ако је за свако $x \in A$, $x \,\rho\, x$, онда кажемо да је ρ **рефлексивна** релација.*

*Ако за свако $x, y \in A$ за које је $x \,\rho\, y$ вриједи да $y \,\rho\, x$ онда кажемо да је ρ **симетрична** релација.*

*Ако за свако $x, y \in A$ за које је $x \,\rho\, y$ вриједи да $y \,\rho\, x$ онда кажемо да је ρ **симетрична** релација.*

*Ако за свако $x, y, z \in A$ тако да $x \,\rho\, y$ и $y \,\rho\, z$, вриједи да $x \,\rho\, z$, онда кажемо да је ρ **транзитивна** релација.*

Дефиниција 3.5 *Бинарну релацију која је рефлексивна, симетрична и транзитивна зовемо* ***релација еквиваленције****.*

Бинарну релацију која је рефлексивна, асиметрична и транзитивна зовемо ***релација поретка*** *.*

Примјер 3.7 *Нека је ρ бинарна релација на $\mathbb{Z}$ дефинисана са*

$$a \,\rho\, b \text{ ако и само ако } 2 \mid a - b.$$

Онда је ρ релација еквиваленције.

Примјер 3.8 *Нека је ρ бинарна релација на $\mathbb{N}$ дефинисана са*

$$a \,\rho\, b \text{ ако и само ако } a \mid b.$$

Онда је ρ заправо релација ***дјељивости****, а која је релација поретка.*

3.0.2. Операције

Дефиниција 3.6 *Нека је S непразан скуп и n природан број. Тада пресликавање $f : S^n \to S$ зовемо* ***операција дужине*** *n скупа S. Специјално, уколико је $n = 1$, онда је f* ***унарна****, а ако је $n = 2$, онда је f* ***бинарна операција*** *скупа S.*

Примјер 3.9 *Нека је f бинарна релација на скупу S. Умјесто $f((x, y)) = z$, у принципу користимо запис $x \, f \, y = z$.*

Тако је, на примјер, операција сабирања, $+$, бинарна операција на $\mathbb{R}$ и користимо уобичајени запис $x + y = z$ умјесто формалног $+((x, y)) = z$.

Примјер 3.10 *Нека је $f : S \to S$ пресликавање. Тада је f операацијa дужине 1 коју зовемо унарна операција.*

На примјер, пресликавање $f : \mathbb{Z} \to \mathbb{Z}$ дефинисано као $f(x) = -x$ је унарна операција којом се, за свако x одређује елемент $f(x)$ са својством да $x + f(x) = 0$.

Дефиниција 3.7 *Нека је $*$ бинарна операција скупа S.*

- *Ако је за све x, y, z из S*
$$x * (y * z) = (x * y) * z,$$
кажемо да је операција асоцијативна.

- *Ако за све x, y из S важи*
$$x * y = y * x$$
кажемо да је операција комутативна.

Примјер 3.11 *На скупу $\mathbb{Z}$, операција сабирања је и асооцијативна и комутативна, док одузимање није ни једно ни друго, јер у општем случају не важи*
$$x - (y - z) = (x - y) - z, \ x - y = y - x.$$

Примјер 3.12 *Нека је $S = \{1, -1\}$. Сабирање и одузимање нису операције скупа S јер $1 + 1 \notin S$ и $1 - 1 \notin S$.*

Са друге стране, није тешко утврдити да су и множење и дијељење асоцијативне и комутативне операције на S.

3.1. Операције над скуповима

У одређеним ситуацијама, разматрамо и пресјек, односно унију бесконачно много скупова, најчешће неке пребројиве колекције скупова. На примјер, ако нам је за свако $n \in \mathbb{N}$ дат скуп S_n, онда

$$\bigcap_{n=1}^{\infty} S_n = S_1 \cap S_2 \cap \cdots = \{x \mid x \in S_k \text{ за свако } k \in \mathbb{N}\},$$
$$\bigcup_{n=1}^{\infty} S_n = S_1 \cup S_2 \cup \cdots = \{x \mid x \in S_k \text{ за неко } k \in \mathbb{N}\}.$$

Два посебно корисна тврђења за скуповне операције су **Де Морганови закони**

$$\left(\bigcup_n S_n\right)^c = \bigcap_n S_n^c, \qquad \left(\bigcap_n S_n\right)^c = \bigcup_n S_n^c.$$

Наводимо неке основне особине скуповних операција

а. $S \cap T = T \cap S$, $S \cup T = T \cup S$,

б. $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$,

в. $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$,

г. $(S^c)^c = S$,

д. $S \cap S^c = \emptyset$, $S \cup S^c = \Omega$,

ђ. $S \cap \Omega = S$, $S \cup \Omega = \Omega$.

4 Дјељивост

У Теорији бројева, од посебног интереса су својства скупа природних бројева

$$\mathbb{N} = \{1, 2, \ldots\},$$

као и скупа цијелих бројева

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Појам дјељивости је основни и један од најважнијих у теорији бројева.

Дефиниција 4.1 *Нека су a и b цијели бројеви, $a \neq 0$. Уколико постоји цио број m такав да*

$$b = am,$$

онда кажемо да је b ***дјељив са*** *a. То записујемо са $a \mid b$, а читамо a* ***дијели*** *b. Ако b није дјељив са a, онда пишемо $a \nmid b$ и читамо a* ***не дијели*** *b.*

Специфичан случај из претходне дефиниције је кад је $b = 0$. За било који цио број a различит од нуле, видимо да је $m = 0$. Тачније, закључујеммо да сваки цијели број a различит од нуле дијели 0. Такође, видимо да је 1 дијели сваки цијели број.

Уколико $b \neq 0$, онда закључујемо да b има само ненулте дјелиоце. У том случају, ако је a дјелилац, онда је то и $-a$. Дакле, за $b \neq 0$, дјелиоци се могу груписати у паровима $(a, -a)$.

Лако се уочавају и остала основна својства дјељивости.

Лема 4.1 *Нека су a, b, c, m, n цијели бројеви такви да је $c \mid a$ и $c \mid b$. Онда*

$$c \mid am + bn.$$

Доказ. Пошто је $a = ck_1$ и $b = ck_2$ за $k_1, k_2 \in \mathbb{Z}$, то је онда

$$am + bn = ck_1m + ck_2n = c(k_1m + k_2n),$$

што значи да $c \mid am + bn$. ■

Лема 4.2 *Нека су a, b, c цијели бројеви.*

1. *Ако $a \mid b$ и $b \mid c$, онда*
$$a \mid c.$$

2. *Ако $a \mid b$ и $b \mid a$, онда*
$$a = b \text{ или } a = -b.$$

Доказ.

1. Из $a \mid b$ слиједи $b = ak_1$, за $k_1 \in \mathbb{Z}$, а из $b \mid c$, слиједи $c = bk_2$, за $k_2 \in \mathbb{Z}$. Дакле,
$$c = bk_2 = (ak_1)k_2 = a(k_1k_2),$$
што значи да $a \mid c$.

2. Из $a \mid b$ и $b \mid a$, онда
$$a = bk_1 \text{ и } b = ak_2,$$
за $k_1, k_2 \in \mathbb{Z}$, одакле је $a = a(k_1k_2)$, што значи да су $k_1k_2 = 1$, односно
$$k_1 = k_2 = 1 \text{ или } k_1 = k_2 = -1,$$
чиме је тврђење доказано.

■

Примјер 4.1 *Нека су $a, b, m \in \mathbb{Z}$.*

(а) Ако је $m \neq 0$, онда $a \mid b$ ако и само ако $ma \mid mb$.

(б) Ако $a \mid b$ и $b \neq 0$, онда $|a| \leq |b|$.

Рјешење

Тврђење под (а) слиједи директно из
$$b = ka \text{ ако и само ако } mb = mka, \text{ за } m \neq 0.$$

У тврђењу под (б), слиједи да су и a и b ненулти цијели борјеви за које вриједи да је $b = ka$, за неко $k \in \mathbb{Z}$ које је такође различито од нуле. Како је $|ka| = |k||a| \geq |a|$, тиме је и доказано тврђење.

Иако су сама дефиниција, као и основна својства дјељивости једноставни, поступак тражења дјелилаца датог броја може бити изузетно тежак. Наиме, не постоје ефикасни поступци, односно они који у разумном времену рјешавају овај задатак у општем случају. Ово

се посебно односи на велике бројеве. Наравно, постоје изузетно велики бројеви чији се дјелиоци лако налазе. На примјер, $a = 2^{65536}$ има дјелиоце облика 2^i, гдје је $i = 0, 1, \ldots, 65536$. Међутим, налажење дјелилаца броја $a + 1 = 2^{65536} + 1$ који има 19729 цифара је изузетно тешко, па се овакви проблеми најчешће рјешавају коришћењем рачунара. Тако се добило да је, на примјер, $m = 825753601$ један од дјелилаца $+1$.
Следећа теорема је једна од кључних у Теорији бројева, па се препоручује наставнику да са пажњом и детаљно изведе њен доказ.

Теорема 4.1 *(Теорема о дијељењу са остатком). Нека су a и b цијели бројеви, при чему је $b > 0$. Онда постоје јединствени цијели бројеви,* ***количник*** *q и* ***остатак*** *r, такви да је*

$$a = qb + r \quad \text{и} \quad 0 \leq r < b.$$

Доказ. Једна могућност је да је a дјељиво са b, па је у том случају $a = bq$, из чега слиједи да је $r = 0$. Претпоставимо да то није случај, односно да a није дјељиво са b. Посматрајмо скуп

$$S = \{a - bm \ : m \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \ldots\}.$$

Ако је $m = -|a| - 1$, онда је израз $a - bm = a + |a|b + b$ природан број, па скуп S садржи и природне бројеве. По принципу доброг уређења скупа природних бројева (сваки непразан подскуп у $\mathbb{N}$ садржи минималан елемент), скуп $S \cap \mathbb{N}$ садржи најмањи елемент, који је облика $r = a - bq$, за неки цијели број q, одакле је

$$a = bq + r, \quad \text{уз услов} \quad r > 0.$$

Доказујемо да је $r < b$. Претпоставимо супротно, да је $r \geq b$. Случај $r = b$ искључујемо, јер би тада a било дјељиво са b. Онда је $r > b$. Међутим, у том случају је $r - b < r$ и $r - b \in S \cap \mathbb{N}$, што би било у супротности са претпоставком о минималности елемента r. Дакле, $r < b$.

Докажимо јединственост пара бројева q, r. Претпоставимо супротно, да постоји q_1, r_1 који задовољава исте услове као q, r. Нека је, не умањујући општост да је $r_1 > r$. Из

$$qb + r = q_1 b + r_1,$$

слиједи

$$b(q - q_1) = r_1 - r.$$

Како је лијева страна претходне једнакости већа од нуле, а b је природан број, то је онда $q - q_1 \in \mathbb{N}$ такође природан број. Међутим, то повлачи да је $r_1 - r > b$, односно да је $r_1 > b$. Ово је контрадикција у односу на чињеницу да је r_1 мањи од b.

■

Сада можемо обрадити и случај $b < 0$, јер је у том случају $-b > 0$, па према претходној теореми постоје јединствени q^* и r, тако да је

$$a = -bq^* + r \; 0 \leq r < -b.$$

За $q = -q^*$, имамо $a = bq + r$. Комбинујући ово и резултат претходне теореме, слиједи:

Посљедица 4.1 *Нека су a и b цијели бројеви, при чему је $b \neq 0$. Онда постоје јединствени цијели бројеви, q и r, такви да је*

$$a = qb + r \quad \text{и} \quad 0 \leq r < |b|.$$

Претходна теорема има изузетан значај у Теорији бројева и бројне примјене у доказу комплекснијих тврђења. Једна од основних последица је и подјела скупа цијелих бројева у класе у односу на дјељивост према неком задатом броју k. Наиме, сви цијели бројеву у односу на дјељивост према броју 5 се могу класификовати у оне који дају остатак 0, 1, 2, 3 или 4 приликом дјељења са 5. Дакле, имамо 5 класа у конкретном случају, а k у општем, када посматрамо цкуп цијелих бројева у односу на дијељење са бројем k.

Примјер 4.2 *Доказати да је број $m^5 - m$, $m \in \mathbb{N}$, дјељив са 30.*

Рјешење. Како је $m^5 - m = m(m-1)(m+1)(m^2+1)$, видимо да на десној страни имамо производ три узастопна природна броја, па је онда дати израз дјељив са 6. Остало је још да се покаже да је број дјељив са 5.

Произвољан цијели број m има облик $5k$, $5k+1$, $5k+2$, $5k+3$, или $5k+4$. Ако је m облика $5k$, $5k+1$ или $5k+4$, онда је јасно да је m, $m-1$, односно $m+1$ дјељиво са 5. У преосталим случајевима, ако је m једнако $5k+2$ или $5k+3$, израз m^2+1 је дјељив са 5. ■

Примјер 4.3 *Доказати да ни за један цио број n, број $n^2 + 3n + 5$ није дјељив са 121.*

Рјешење. Како је $n^2 + 3n + 5 = (n-4)(n+7) + 33$, онда видимо да су бројеви $n-4$ и $n+7$ оба дјељива са 11 или ниједан. Оба су дјељива са 11 ако и само ако n даје остатак 4 при дијељењу са 11. Стога, или је $(n-4)(n+7)$ дјељиво са 121 или није ни са 11. Како је 33 дјељиво са 11, али није са 121, онда је закључак очигледан. ■

Примјер 4.4 *Доказати да $n^2 + 2$ није дјељиво са 4 ни за један цијели број n.*

Рјешење. Ако је n непаран број, онда је и n^2 непаран, па је такав и $n^2 + 2$. Стога, не може бити дјељив са 4.

Уколико је n паран број, онда је n^2 дјељив са 4, али $n^2 + 2$ даје остатак 2 при дјељењу са 4. ■

Примјер 4.5 *Наћи три последње цифре броја 7^{9999}.*

Рјешење. Најприје, примјетимо да је

$$7^{9999} = 7^{4\cdot 2499+3} = 7^{4\cdot 2499} \cdot 7^3,$$

што истиче важност израза облика 7^{4n} у датом контексту. Пошто је $7^4 = 2401$, онда је

$$7^{4n} = (1+2400)^n = 1 + n \cdot 2400 + \binom{n}{2} 2400^2 + \cdots .$$

Из претходне суме уочавамо да се сви сабирци почевши од трећег члана завршавају са најмање четири нуле, што значи да не утичу на последње три цифре посматраног броја. Дакле, да би одредили последње три цифре броја 7^{4n} довољно је посматрати израз
$1 + n \cdot 2400$. Пошто је

$$1 + n \cdot 2400 = 24n \cdot 100 + 1 = (\ldots m) \cdot 100 + 1 = \ldots m01,$$

гдје је са $(\ldots m)$ заправо представљен број $24n$, а m његова последња цифра. У нашем, конкретном случају, за посматрано $n = 2499$, слиједи $24n = 59976$, па је $m = 6$. Значи, број 7^{4n} се завршава са 601. На крају,

$$7^{9999} = 7^{4\cdot 2499} \cdot 7^3 = (\ldots 601)(343) = (\ldots 143),$$

што значи да се тражени број завршава са 143. ■

Вјежбанка

4.1. Вјежбанка

1. Да ли постоје цијели бројеви a, b и c такви да $a \mid bc$, али $a \nmid b$ и $a \nmid c$?
2. Показати да за непарне бројеве a и b постоје цијели бројеви s и t, такви да $a = bs + t$, гдје је t непаран и $|t| < b$.
3. Ако су a и b природни бројеви, онда је $a!b! \mid (a+b)!$.
4. Доказати да је за природан број k, производ $P = (a+1)(a+2)\cdots(a+k)$ дјељив са $k!$.
5. Доказати

4.2. Функције заокруживања

Нека је a реалан број. Функција *доње цјелобројно*, у ознаци $\lfloor a \rfloor$, је највећи цио број који је мањи или једнак датом броју a.

Слично, функција *горње цјелобројно*, у ознаци $\lceil a \rceil$ је најмањи цио број који је већи или једнак датом броју a.

Ове дефиниције можемо дати и у скуповном облику:

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\},$$

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

Из саме дефиниције ових функција, закључујемо да за произвољан реалан број a вриједи

$$\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1 \text{ и } \lceil a \rceil - 1 < a \leq \lceil a \rceil.$$

Ако је x реалан број, онда је функција $\{x\}$, коју називамо *разломљени дио* од x, дефинисана са

$$\{x\} = x - \lfloor x \rfloor.$$

У следећој леми су дате неке од основних особина ових функција.

Лема 4.3 *Нека је x реалан, а k цио број. Вриједе следеће особине*

1. $\lfloor k \rfloor = k = \lceil k \rceil$.
2. $\lceil x \rceil = \lfloor x \rfloor + 1$, *ако* $x \notin \mathbb{Z}$.
3. $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.
4. $\lceil x + k \rceil = \lceil x \rceil + k$.
5. $\left\lfloor \frac{k}{2} \right\rfloor = \frac{k-1}{2}$, *ако је k непаран.*
6. $\left\lceil \frac{k}{2} \right\rceil = \frac{k+1}{2}$, *ако је k непаран.*
7. $\lfloor 2x \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor$.
8. $\{x + k\} = \{x\}$.

4.3. Највећи заједнички дјелилац

Дефиниција 4.2 *Нека су a и b цијели бројеви од којих је бар један различит од нуле. Цијели број d зовемо* ***заједнички дјелилац*** *од a и b ако $d \mid a$ и $d \mid b$. Највећи међу њима се зове* ***највећи заједнички дјелилац*** *и означава се са* **нзд**(a, b) *или* (a, b).

Посебно, дефинишемо **нзд**$(0, 0) = 0$.

Слично дефинишемо и највећи заједнички дјелилац цијелих бројева $b_1, b_2, \ldots, b_n$, од којих је бар један различит од нуле, а означавамо са

$$\textbf{нзд}(b_1, b_2, \ldots, b_n) \text{ или } (b_1, b_2, \ldots, b_n).$$

Бројеви $b_1, b_2, \ldots, b_n$ су ***релативно прости*** *ако је*

$$\textbf{нзд}(b_1, b_2, \ldots, b_n) = 1.$$

Бројеви $b_1, b_2, \ldots, b_n$ су ***релативно прости у паровима*** *ако је* **нзд**$(b_i, b_j) = 1$ *за свако i, j за које је $1 \leq i < j \leq n$.*

Примјер 4.6 *Бројеви $12, 8, 15$ су релативно прости, али нису релативно прости у паровима, јер на примјер,* **нзд**$(12, 8) = 4$.

Напомена Убудуће, кад год напишемо **нзд**$(b_1, b_2, \ldots, b_n)$, подразумијеваћемо да је услов из претходне дефиниције, да је бар један од бројева b_i различит од нуле, испуњен.

Теорема 4.2 *Нека је $d =$* **нзд**$(a_1, a_2, \ldots, a_n)$. *Онда је d најмањи позитивни елемент скупа*

$$S = \{a_1t_1 + a_2t_2 + \cdots + a_nt_n \mid t_1, t_2, \ldots, t_n \in \mathbb{Z}\},$$

па постоје цијели бројеви $t'_1, t'_2, \ldots, t'_n$ тако да је

$$d = a_1t'_1 + a_2t'_2 + \ldots + a_nt'_n.$$

Доказ. Нека је s најмањи позитивни елемент скупа S. Показујемо да је $d = s$. Најприје, докажимо да је сваки елемент из S дјељив са s. Лако се уочава да за произвољно $x \in S$ вриједи $x - ls \in S$, за свако $l \in \mathbb{Z}$. Тиме је и

$$x - \left\lfloor \frac{x}{s} \right\rfloor s \in S.$$

Пошто је

$$\left\lfloor \frac{x}{s} \right\rfloor \leq \frac{x}{s} < \left\lfloor \frac{x}{s} \right\rfloor + 1,$$

онда је

$$0 \leq x - \left\lfloor \frac{x}{s} \right\rfloor s < s.$$

Из последње неједнакости, уважавајући чињеницу да је s најмањи позитивни елемент скупа S, слиједи да је $x - \lfloor x/s \rfloor s = 0$, што значи да $s \mid x$. Слиједи да $s \mid a_i$ за $i = 1, 2, \ldots, n$, па је стога $s \leq d$. Са друге стране, знамо да је

$$s = a_1 u_1 + a_2 u_2 + \ldots + a_n u_n,$$

за неке одговарајуће $u_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$. Из услова да $d \mid a_i$, $i = 1, 2, \ldots, n$, слиједи да $d \leq s$. Стога, закључујемо да је $d = s$. ■

Дакле, претходна теорема установљава могућност приказа за највећег заједничког дјелиоца **нзд**$(a_1, a_2, \ldots, a_n)$ цијелих бројева $a_1, a_2, \ldots, a_n$ у облику цјелобројне линеарне комбинације

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = a_1 u_1 + a_2 u_2 + \ldots a_n u_n,$$

за одговарајуће $u_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$. Ово представљање највећег заједничког дјелиоца скупа бројева се у литератури назива Безуов идентитет.

Примјетимо да **нзд**$(a_1, a_2, \ldots, a_n) \geq 1$. Такође, елементарном анализом закључујемо да је

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = \textbf{нзд}(\pm a_1, \pm a_2, \ldots, \pm a_n),$$

што значи да су само апсолутне вриједности бројева битне за највећи заједнички дјелилац датог скупа бројева.

Посљедица 4.2 *Сваки заједнички дјелилац цијелих бројева $a_1, a_2, \ldots, a_n$ дијели* **нзд**$(a_1, a_2, \ldots, a_n)$.

Доказ. Пошто сваки заједнички t дјелилац бројева $a_1, a_2, \ldots, a_n$ уједно дијели и сваку цјелобројну линеарну комбинацију ових бројева, онда $t \mid d$, гдје је, према претходној Теореми 4.2,

$$d = \textbf{нзд}(a_1, a_2, \ldots, a_n) = a_1 u_1 + a_2 u_2 + \ldots + a_n u_n,$$

за одговарајуће $u_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$.

■

Посљедица 4.3 *За цијеле бројеве $a_1, a_2, \ldots, a_n$ вриједи*

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = \textbf{нзд}(a_1, a_2, \ldots, a_{n-2}, \textbf{нзд}(a_{n-1}, a_n))$$

Доказ. Сваки заједнички дјелилац a_{n-1} и a_n је уједно и дјелилац **нзд**(a_{n-1}, a_n). Такође, сваки дјелилац **нзд**(a_{n-1}, a_n) је уједно дјелилац a_{n-1} и a_n. Закључујемо да скупови

$$\{a_1, a_2, \ldots, a_n\} \text{ и } \{a_1, a_2, \ldots, a_{n-2}, \textbf{нзд}(a_{n-1}, a_n)\}$$

имају исти скуп заједничких дјелилаца. Стога, имају и заједнички највећи заједнички дјелилац **нзд**. ■

Примјер 4.7 *Доказати да се разломци*

$$\frac{12n+1}{30n+2} \text{ и } \frac{21n+4}{14n+3}$$

не могу скратити ни за један природан број.

Рјешење. Претпоставимо да d дијели бројеве $12n+1$ и $30n+2$. Тада d дијели и сваку линеарну комбинацију ова два броја, па специјално

$$d \mid 5(12n+1) - 2(30n+2) = 1,$$

одакле слиједи да је $d = 1$, чиме је доказано да се дати разломак не може даље скратити.

Слично се доказује и за други разломак, јер је

$$d \mid 3(14n+3) - 2(21n+4) = 1.$$

■

Лема 4.4 *Нека је* $d = \textbf{нзд}(a_1, a_2, \ldots, a_n)$, *гдје су* $a_1, a_2, \ldots, a_n$ *цијели бројеви. Онда је*

$$\textbf{нзд}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1.$$

Такође, вриједи

$$\textbf{нзд}(ma_1, ma_2, \ldots, ma_n) = md,$$

за сваки цио број $m > 0$.

Доказ. Претпоставимо да је

$$\textbf{нзд}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = k$$

и $k > 1$. Слиједи да је

$$a_1 = kdt_1, a_2 = kdt_2, \ldots, a_n = kdt_n$$

па је

$$\textbf{нзд}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) \geq kd > d,$$

што је контрадикција у односу на претпоставку. На основу Теореме 4.2 закључујемо да је $\textbf{нзд}(ma_1, ma_2, \ldots, ma_n)$ најмањи позитивни број облика

$$ma_1x_1 + ma_2x_2 + \cdots + ma_nx_n = m(a_1x_1 + a_2x_2 + \cdots + a_nx_n),$$

гдје су $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. Како је најмањи природан број облика $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ управо d, слиједи да је

$$\textbf{нзд}(ma_1, ma_2, \ldots, ma_n) = md.$$

■

Лема 4.5 *Нека a, b, q и r цијели бројеви за које вриједи $a = bq + r$. Онда је*

$$\textbf{нзд}(a, b) = \textbf{нзд}(b, r).$$

Доказ. Ако цијели број d дијели бројеве a и b, онда, на основу Леме 4.1, слиједи да d дијели и $a - bq$ односно r. Дакле, d дијели b и r. То значи да

$$\textbf{нзд}(a, b) \leq \textbf{нзд}(b, r). \tag{1}$$

Обрнуто, ако d дијели b и r, слиједи да d дијели a, из чега закључујемо да d дијели и a и b. Тиме смо показали да је

$$\textbf{нзд}(b, r) \leq \textbf{нзд}(a, b). \tag{2}$$

Из (1) и (2), слиједи тврђење

$$\textbf{нзд}(a, b) = \textbf{нзд}(b, r).$$

■

Лема 4.6 *Нека су a, b, m цијели бројеви такви да* $\textbf{нзд}(a, m) = \textbf{нзд}(b, m) = 1$. *Тада је* $\textbf{нзд}(ab, m) = 1$.

Доказ. Из претпоставки, а на основу Теореме 4.2, слиједи

$$1 = ax_0 + my_0$$
$$1 = bx_1 + my_1$$

Из претходне двије једнакости добијамо

$$abx_0x_1 = (1 - my_0)(1 - my_1) = 1 - mt,$$

гдје је $t = y_0 + y_1 - my_0y_1$. Сада, из

$$abx_0x_1 + mt = 1$$

закључујемо да је $\textbf{нзд}(ab, m) = 1$. ■

Лема 4.7 *Нека су a и b узајамно прости цијели бројеви.*

(а) Ако $a \mid c$ и $b \mid c$, онда $ab \mid c$.

(б) Ако $a \mid bc$, онда $a \mid c$.

Доказ.

(а) Како је $1 = ax + by$ за неке цијеле бројеве, онда је $c = cax + cby$. Међутим, $c = as$ и $c = bt$, па је $c = abtx + absy = ab(tx + sy)$.

(б) Као и под (а), имамо да је $c = cax + cby$. Пошто $a \mid a$ и $a \mid bc$, онда из дате једнакости слиједи $a \mid c$.

■

1. Ако су $a \neq 0$ и $b \neq 0$, онда је

$$0 < \textbf{нзд}(a, b) \leq \min\{|a|, |b|\}$$

4.4. Еуклидов алгоритам

У следећој теореми је описана конструктивна, практична процедура за тражење највећег заједничког дјелиоца два цијела броја.

Теорема 4.3 *(Еуклидов алгоритам). Нека су a и $b > 0$ цијели бројеви. Претпоставимо да је узастопном примјеном Теореме 4.1 добијен низ једнакости*

$$\begin{array}{rcll} b & = & aq_1 + r_1, & 0 < r_1 < a \\ a & = & r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3, & 0 < r_3 < r_2 \\ & \dots & & \\ r_{j-2} & = & r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_jq_{j+1}. & \end{array}$$

Тада је **нзд**(a, b) *једнак r_j, односно последњем ненултом остатку.*

Доказ. Уочавамо да у општем случају, ред у Еуклидовом алгоритму изгледа

$$r_i = r_{i+1}q_{i+2} + r_{i+2},\ 0 \leq r_{i+2} < r_{i+1},\ \text{за } i \geq -1,$$

уколико дефинишемо да је $r_{-1} = b$, а $r_0 = a$. Како је низ остатака r_i строго опадајући, онда је извјесно да ће за неки природан број j бити r_j последњи ненулти остатак, односно $r_{j+1} = 0$. На основу Леме 4.5 закључујемо да је

$$\textbf{нзд}(r_i, r_{i+1}) = \textbf{нзд}(r_{i+1}, r_{i+2}),$$

из чега произилази низ једнакости

$$\textbf{нзд}(r_{-1}, r_0) = \ldots = \textbf{нзд}(r_j, r_{j+1}) = \textbf{нзд}(r_{j+1}, 0) = r_j.$$

■

Algorithm 1 Еуклидов алгоритам

```
procedure EUCLID(a, b)                                  ▷ нзд(a, b)
    r ← a mod b
    while r ≠ 0 do                                      ▷ Имамо одговор ако је r једнако 0
        a ← b
        b ← r
        r ← a mod b
    end while
    return b                                            ▷ нзд је b
end procedure
```

Лема 4.8 *За остатке у Еуклидовом алгоритму важи релација*

$$r_{i+2} < \frac{1}{2} r_i \quad i = -1, 0, 1, 2, \ldots.$$

За број корака j у Еуклидовом алгоритму вриједи $j < 2\log_2 a$.

Доказ. Могућа су два случаја:

I $r_{i+1} \leq 1/2 r_i$
Како је $r_{i+2} < r_{i+1}$, онда је $r_{i+2} < 1/2 r_i$.

II $r_{i+1} > 1/2 r_i$
Ово значи да је у кораку дијељења r_i са r_{i+1}, количник једнак 1, односно

$$r_i = 1 \cdot r_{i+1} + r_{i+2}.$$

Одавде је

$$r_{i+2} = r_i - r_{i+1} < r_i - 1/2 r_i = 1/2 r_i.$$

На основу претходног, закључујемо

$$1 \leq r_j < \frac{r_{j-2}}{2} < \frac{r_{j-4}}{4} < \cdots < \frac{r_0}{2^{j/2}},$$

ако је j парно. Како је $r_{j-1} > r_j \geq 1$, то је за непарно j

$$2 \leq r_{j-1} < \frac{r_{j-3}}{2} < \frac{r_{j-5}}{4} < \cdots < \frac{r_0}{2^{(j-1)/2}}.$$

Дакле, у сваком случају је $a = r_0 > 2^{j/2}$, па је $j < 2\log_2 a$. ■

Користећи Еуклидов алгоритам, могуће је највећи заједнички дјелилац два броја изразити као њихову линеарну комбинацију. У следећем примјеру је дат поступак како је то могуће урадити.

Проширени Еуклидов алгоритам. Рјешења једначине

$$ax + by = \textbf{нзд}(a, b)$$

могу се ефикасно добити у следећем поступку. Ако је

$$\begin{array}{lll} r_{-1} = a, & r_0 = b; & r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} = 1, & x_0 = 0; & x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} = 0, & y_0 = 1; & y_i = y_{i-2} - q_i y_{i-1}; \end{array}$$

онда је

$$ax_i + by_i = r_i, \quad i = -1, 0, 1, \ldots, j+1,$$

гдје је j индекс везан за Еуклидов алгоритам, представљен у Теореми 4.3.

Примјер 4.8 *Одредити највећи заједнички дјелилац за бројеве* 4056 *и* 1848 *и приказати га као њихову линеарну комбинацију.*

Рјешење.

$$\begin{aligned} 4056 &= 1848 \cdot 2 + 360 \\ 1848 &= 360 \cdot 5 + 48 \\ 360 &= 48 \cdot 7 + 24 \\ 48 &= 24 \cdot 2 + 0 \end{aligned}$$

i	q_i	x_i	y_i
-1		1	0
0		0	1
1	2	1	-2
2	5	-5	11
3	7	36	-79

Дакле, имамо да је

$$36 \cdot 4056 - 79 \cdot 1848 = 24.$$

■

Из Еуклидовог алгоритму дијељења видимо да, за природне бројеве a, b постоје јединствени бројеви q, r тако да

$$a = bq + r_0, \ 0 \leq r < b.$$

Јасно је да је $q = \lfloor a/b \rfloor$. Међутим, трансформацијом претходног записа можемо обезбиједити форму у којој је остатак увијек мањи од $b/2$. Наиме, ако је $r > b/2$, онда

$$a = bq + b - r_1$$

при чему $r_1 \leq b/2$. Дакле, у сваком случају, за произвољна два броја a, b имамо

$$a = bq + r \text{ или } a = b(q+1) - r_1 = bq_1 - r_1$$

при чему су $0 \leq r, r_1 \leq b/2$. Уочимо да овим поступком обезбјеђујемо јединственост пара q, r односно q_1, r_1. Тако добијамо модификовани Еуклидов алгоритам у ком су остаци најмањи по апсолутној вриједности.

Лема 4.9 *За дате цијеле бројеве a и $b > 0$, постоји јединствен пар q, r, тако да*

$$a = bq + r, \text{ при чему вриједи } -\frac{b}{2} < r \leq \frac{b}{2}.$$

4.5. Бланкиншип метода

У чланку Америчког математичког мјесечника из 1963. године, Бланкиншип (W.A. Blankinship) је дао веома једноставан метод за налажење најмањег заједничког садржаоца два броја, као и коефицијената одговарајуће линеарне комбинације. Примјери и опис метода који слиједе су преузети из књиге Кларка, Елементарна теорија бројева. (НАВЕСТИ ЦИТАТ!!!)

За дате цијеле бројеве $a > b > 0$ почињемо са матрицом

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Изводимо *елементарне матричне операције над врстама* тако што једној врсти додајемо другу, претходно помножену са неким бројем, а са циљем да добијемо једну од двије форме

$$\begin{bmatrix} 0 & x_1 & x_2 \\ d & y_1 & y_2 \end{bmatrix}$$

или

$$\begin{bmatrix} d & y_1 & y_2 \\ 0 & x_1 & x_2 \end{bmatrix}$$

Дакле, крајњи циљ је да се добије нула у првој колони. Овај метод гарантује да је $d = \textbf{нзд}(a, b) = y_1 a + y_2 b$.

Примјер 4.9 *Нека је* $a = 35$, $b = 15$.

$$\begin{bmatrix} 35 & 1 & 0 \\ 15 & 0 & 1 \end{bmatrix}$$

Примјетимо да је $35 = 15 \cdot 2 + 5$, *па је*

$$35 + 15(-2) = 5.$$

Ако помножимо другу врсту са -2 *и додамо је првој врсти, добијамо*

$$\begin{bmatrix} 5 & 1 & -2 \\ 15 & 0 & 1 \end{bmatrix}$$

Како је $3 \cdot 5 = 15$ *или* $15 + (-3)5 = 0$, *онда множимо прву врсту са* -3 *и додајемо је другој врсти, при чему добијамо*

$$\begin{bmatrix} 5 & 1 & -2 \\ 0 & -3 & 7 \end{bmatrix}.$$

Сада, можемо рећи да је

$$\textbf{нзд}(35, 15) = 5$$

и

$$5 = 1 \cdot 35 + (-2) \cdot 15.$$

Како ради Бланкшип метод:

Почевши од матрице

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

имамо да

$$a = 1 \cdot a + 0 \cdot b$$
$$b = 0 \cdot a + 1 \cdot b.$$

У $i-$том кораку Бланкиншип методе, имамо матрицу

$$\begin{bmatrix} a_i & u_i & v_i \\ b_i & s_i & t_i \end{bmatrix}$$

и при том вриједи да

$$a_i = u_i a + v_i b,$$
$$b_i = s_i a + t_i b.$$

Уочавамо да $\textbf{нзд}(a, b) \mid \textbf{нзд}(a_i, b_i)$. Такође, увиђамо да, у складу са датим трансформацијама на врстама, увијек вриједи

$$u_i t_i - v_i s_i = 1.$$

Посматрајмо крајњу матрицу

$$\begin{bmatrix} 0 & x_1 & x_2 \\ d & y_1 & y_2 \end{bmatrix}.$$

Из

$$x_1y_2 - x_2y_1 = 1,\ x_1a + x_2b = 0 \text{ и } y_1a + y_2b = d,$$

слиједи да је $b = x_1d$ и $a = -x_2d$. Закључујемо да $d \mid \textbf{нзд}(a, b)$. Како је већ показано да $\textbf{нзд}(a, b) \mid \textbf{нзд}(a_i, b_i)$, онда $\textbf{нзд}(a, b) \mid \textbf{нзд}(0, d)$, односно $\textbf{нзд}(a, b) \mid d$. Стога, $d = \textbf{нзд}(a, b)$.

Задатак 4.1 *Искористити Бланкиншип методу за порналажење највећег заједничког дјелиоца и одговарајуће линеарне комбинације у Безуовом идентитету за*

(1) $a = 267,\ b = 112$

(2) $a = 216,\ b = 135$

(3) $a = 11312,\ b = 11321$

Примјер 4.10 *Доказати да је* $a^{2^n} + 1$ *дјелилац броја* $a^{2^m} - 1$ *за* $m > n$, *а да је за* $a, m, n \in \mathbb{N}$, $m \neq n$

$$\textbf{нзд}\left(a^{2^m} + 1, a^{2^n} + 1\right) = \begin{cases} 2, & \text{ако је } a \text{ непаран,} \\ 1, & \text{ако је } a \text{ паран.} \end{cases}$$

Рјешење. Прво тврђење у задатку се доказује индукцијом по $m > n$. Како је $(a^{2^n} + 1)(a^{2^n} - 1) = a^{2^{n+1}} - 1$, слиједи да $a^{2^n} + 1 \mid a^{2^{n+1}} - 1$. Дакле, ако $a^{2^n} + 1 \mid a^{2^k} - 1$, онда

$$a^{2^n} + 1 \mid \left(a^{2^k} - 1\right)\left(a^{2^k} + 1\right) = a^{2^{k+1}} - 1,$$

чиме је први дио тврђења доказан.

Ако је $m \neq n$, онда је један од бројева m, n већи. Нека је то, на примјер, број m. Користећи претходну тврдњу, имамо да је

$$a^{2^m} - 1 = k(a^{2^n} + 1),$$

што значи да је

$$a^{2^m} + 1 = k(a^{2^n} + 1) + 2,$$

одакле слиједи да је $\textbf{нзд}\left(a^{2^m} + 1,\ a^{2^n} + 1\right)$ дјелилац броја 2. То значи да су једине двије могућности 1 или 2. У случају, да је a паран, онда су бројеви $a^{2^m} + 1, a^{2^n} + 1$ непарни, па највећи заједнички дјелилац мора бити 1. У случају да је a непаран, онда су посматрани бројеви парни, па је највећи заједнички дјелилац 2.

Напомињемо да се у доказу ништа суштински не би промијенило ни да смо претпоставили да је n већи, сем што би m и n у претходном поступку замијенили мјеста.

■

1. Испитати да ли вриједи да ако $a \mid (b+c)$ онда $a \mid b$ или $a \mid c$, гдје су a, b и c цијели бројеви.
2. Доказати да је бар један од бројева a, $a+2$ или $a+4$, $a \in \mathbf{Z}$ дјељив са 3.
3. Доказати да за природан број n и цио број a, вриједи да **нзд**$(a, a+n)$ дијели n.
4. Доказати следећа тврђења

   а. Ако је a непаран цио број, онда $24 \mid a(a^2-1)$.

   б. Ако су a и b непарни цијели бројеви, онда $8 \mid a^2-b^2$.

   в. Ако је a цио број који није дјељив ни са 2 ни са 3, онда $24 \mid (a^2+3)$.

   г. Ако је a цио број онда $360 \mid a^2(a^2-1)(a^2-4)$.

4.6. Најмањи заједнички садржалац

Дефиниција 4.3 ***Заједнички садржалац*** *два ненулта броја, a и b, је цио број c, такав да $a \mid c$ и $b \mid c$. Ако су оба броја, a и b, ненулта, онда увијек постоји позитивни заједнички садржалац, као на примјер $|ab|$. Сагласно томе, постоји и* ***најмањи заједнички садржалац****,* **нзс**(a,b)*, односно најмањи позитивни број l који задовољава два услова*

(1) Ако $a \mid l$ и $b \mid l$.

(2) Ако $a \mid c$ и $b \mid c$, при чему је $l > 0$, онда $l \leq c$.

Често се умјесто **нзс**(a,b) *користи и ознака $[a,b]$.*

Слично, дефинишемо најмањи заједнички садржалац ненултих бројева $a_1, a_2, \ldots a_n$ и означавамо са $[a_1, a_2, \ldots, a_n]$.

Својства најмањег заједничког садржаоца су у одређеном смислу везана за својства највећег заједничког дјелиоца, што се потврђује и следећом теоремом. Пошто је **нзд**$(a,b) =$ **нзд**$(|a|,|b|)$, а **нзс**$(a,b) =$ **нзс**$(|a|,|b|)$, онда без умањења општости можемо сматрати да су a и b природни бројеви.

Теорема 4.4 *Ако су a и b природни бројеви, онда је*

$$\textbf{нзд}(a,b)\,\textbf{нзс}(a,b) = ab.$$

Доказ. Нека је $d =$ **нзд**(a,b) и $l =$ **нзс**(a,b). Доказујемо да је $\dfrac{ab}{d}$ најмањи заједнички садржалац бројева a и b. Ако је $e = a/d$ и $f = b/d$, онда

$$\frac{ab}{d} = \frac{(de)(df)}{d} = def.$$

Очигледно, добијени број def је позитиван, па је потребно доказати да је то заправо најмањи заједнички садржалац датих бројева. Прво,

$$def = (de)f = af \text{ и } def = (df)e = be,$$

што значи да је $a \mid def$ и $b \mid def$, па је def заједнички садржалац бројева a и b. Доказујемо да је то заправо најмањи заједнички садржалац.

Претпоставимо да $a \mid c$ и $b \mid c$, за $c > 0$. Потребно је показати да је $def \leq c$. На основу Теореме 4.2 имамо да је $d = au + bv$, за цијеле бројеве u и v. На основу тога имамо

$$\frac{c}{def} = \frac{cd}{(de)(df)} = \frac{cd}{ab} = \frac{c(au+bv)}{ab} = \frac{c}{b}u + \frac{c}{a}v,$$

што је цио број, па закључујемо да је $def \mid c$, односно $def \leq c$. ■

Лема 4.10 *Сваки заједнички садржалац бројева $a_1, a_2, \ldots, a_n$ је дјељив са* **нзс**$(a_1, a_2, \ldots, a_n)$.

Доказ. Нека је $N = \textbf{нзс}(a_1, a_2, \ldots, a_n)$. Претпоставимо да постоји заједнички садржалац M датих бројева који није дјељив са N. Онда је

$$M = qN + r,$$

гдје је r природан број и $r < N$. Дакле, $r = M - qN$. Нека је i произвољан број из скупа $1, 2, \ldots, n$. Пошто су M и N садржаоци броја a_i, онда је $M = x_i a_i$ и $N = y_i a_i$. Одатле је

$$r = M - qN = (x_i - qy_i)a_i,$$

одакле закључујемо да $a_i \mid r$ за $i = 1, 2, \ldots, n$. Слиједи да је r заједнички садржалац за бројеве $a_1, a_2, \ldots, a_n$, мањи од N. То је супротно претпоставвци да је N најмањи заједнички садржалац бројева $a_1, a_2, \ldots, a_n$. Значи, $N \mid M$. ■

Лема 4.11 *За природне бројеве $a_1, a_2, \ldots, a_n$ вриједи*

$$\textbf{нзд}(a_1, a_2, \ldots, a_n) = \textbf{нзд}(\textbf{нзд}(a_1, a_2, \ldots, a_{n-1}), a_n)$$

Доказ. Нека је $t = \textbf{нзд}(a_1, a_2, \ldots, a_{n-1})$, а

$$s = \textbf{нзд}(\textbf{нзд}(a_1, a_2, \ldots, a_{n-1}), a_n) = \textbf{нзд}(t, a_n).$$

Пошто је s дјелитељ t и a_n, а t дјелитељ сваког од посматраних бројева $a_1, a_2, \ldots, a_{n-1}$, онда је s заједнички дјелитељ $a_1, a_2, \ldots, a_n$. Нека је s' произвољан дјелитељ бројева $a_1, a_2, \ldots, a_n$. На основу Последице 4.2, слиједи да $s' \mid t$. Како $s' \mid a_n$, онда $s' \mid \textbf{нзд}(t, a_n)$, односно $s' \mid s$. То значи да је s заједнички дјелитељ бројева $a_1, a_2, \ldots, a_n$ са особином да је дјељив са произвољним заједничким дјелиоцем посматраних бројева. То управо значи да је $s = \textbf{нзд}(a_1, a_2, \ldots, a_n)$. ■

Лема 4.12 *За природне бројеве $a_1, a_2, \ldots, a_n$ вриједи*

$$\textbf{нзс}(a_1, a_2, \ldots, a_n) = \textbf{нзс}(\textbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n)$$

Доказ. Нека је $N = \textbf{нзс}(\textbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n)$. Очигледно, N је садржалац бројева $a_1, a_2, \ldots, a_n$. Нека је M произвољан садржалац бројева $a_1, a_2, \ldots, a_n$. Пошто

$$\textbf{нзс}(a_1, a_2, \ldots, a_{n-1}) \mid M \text{ и } a_n \mid M,$$

онда на основу Леме 4.10 слиједи да

$$\textbf{нзс}(\textbf{нзс}(a_1, a_2, \ldots, a_{n-1}), a_n) \mid M,$$

односно $N \mid M$. Дакле, N је заједнички садржалац $a_1, a_2, \ldots, a_n$ такав да дијели сваки други заједнички садржалац датих бројева. Слиједи, по дефиницији, да је $N = \textbf{нзс}(a_1, a_2, \ldots, a_n)$. ■

4.7. Представљање цијелих бројева у одређеној бази

Подразумијеван облик представљања бројева је у *децималном* облику, што значи да запис неког броја користимо *основу* или *базу* 10, па запис одређеног броја, на примјер 3567, значи:

$$3 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10^1 + 7 \cdot 10^0.$$

Не постоји јасан разлог због чега би за представљање бројева користили основу 10, изузев то што имамо 10 прстију на рукама. Познато је да су Вавилонци користили основу 60, док су Маје користиле основу 20. У свијету рачунара, користимо основу 2.

Следећа теорема указује да сваки природан број већи од 1 може бити база представљања.

Теорема 4.5 *Нека је b природан број већи од 1. Сваки природан број n се може написати у облику*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

гдје су a_j цијели бројеви такви да $0 \leq a_j \leq b - 1$ за $j = 0, 1, \ldots, k$ и $a_k \neq 0$.

Посљедица 4.4 *Сваки природан број је могуће, на јединствен начин, представити као суму степена броја 2.*

Примјер 4.11 *Наћи све природне бројеве a такве да је $a^{10} + 1$ дјељиво са 10.*

Рјешење. Нека је r остатак при дијељењу природног броја са 10. Лако је видјети да је $a^{10}+1$ дјељиво са 10 ако и само ако је $r^{10}+1$ дјељиво са 10. Пошто су могућности за r из скупа $0,1,\ldots,9$ онда директном провјером закључујемо да су само

$$3^{10}+1 \text{ и } 7^{10}+1$$

дјељиви са 10. Дакле, сви бројеви a облика $10k+3$ и $10k+7$, за $k=0,1,2,\ldots$ су они за које вриједи да је $a^{10}+1$ дјељиво са 10. ■

Примјер 4.12 *Доказати да постоји бесконачан скуп бројева облика* $t_n=\dfrac{1}{2}n(n+1)$, $n=1,2,\ldots$ *такав да су свака два елемента тог скупа релативно проста.*

Рјешење. Показаћемо заправо да постоји бесконачан растући низ траженог облика у ком су свака два елемента релативно проста.

Најприје показујемо да ако постоји m таквих бројева

$$t_{k_1}<t_{k_2}<\cdots<t_{k_m},$$

који су релативно прости, онда постоји $t\in\mathbb{N}$, такође облика $\frac{1}{2}n(n+1)$ за неко $n\in\mathbb{N}$, такав да је релативно прост са свим бројевима

$$t_{k_1},t_{k_2},\ldots,t_{k_m}.$$

Нека је $s=t_{k_1}t_{k_2}\cdots t_{k_m}$. Посматрајмо број

$$t=\frac{(2s+1)(2s+2)}{2}=(s+1)(2s+1).$$

Очигледно, број t је одговарајућег облика и производ је фактора $s+1$ и $2s+1$ који су релативно прости са s, а тиме и са сваким од бројева $t_{k_1},t_{k_2},\ldots,t_{k_m}$ који учествују у производу. Тиме смо показали да постојећи скуп од m бројева можемо проширити са новим $t_{k_{m+1}}=t$, а да остану задовољене све тражене особине. На описани начин, поступак се наставља за $m+2,m+3,\ldots$

На примјер, ако почнемо са најмањим бројем $t_1=1$ имамо низ

$$t_1=1,t_2=3,t_4=10,t_{13}=91,t_{22}=253,\ldots$$

у ком су свака два броја релативно проста. ■

Примјер 4.13 *Ако су a и b два различита цијела броја, онда постоји бесконачно много природних бројева $n\in\mathbb{N}$ таквих да су $a+n$ и $b+n$ релативно прости.*

Рјешење. Нека су a и b два различита цијела броја и нека је $a<b$. Посматрајмо број

$$n=(b-a)k+1-a.$$

За довољно велико k, n је природан број. Тиме су и

$$a+n=(b-a)k+1,\ \ b+n=(b-a)(k+1)+1$$

такође природни броеви. Ако $d \mid a+n$ и $d \mid b+n$, онда $d \mid b-a$. Даље, из $d \mid a+n$ и $d \mid b-a$, слиједи да $d \mid 1$, одакле је $d=1$. Дакле,

$$\textbf{нзд}(a+n, b+n)=1.$$

Значи, одабиром довољно великог броја k добијамо одговарајући број n за који вриједи да су $a+n$ и $b+n$ релативно прости. ■

1. Представити највећи заједнички дјелилац бројева 93 и 81 у облику њихове линеарне комбинације.
2. Доказати да су n и $n+1$ релативно прости за свако $n \in \mathbb{N}$.
3. Доказати да су $n!+1$ и $(n+1)!+1$ релативно прости за свако $n \in \mathbb{N}$.
4. Нека су a и b узастопни цијели бројеви и n природан број. Доказати да је $\textbf{нзд}(an+b, bn+a)$ непаран број.
5. Нека су a и b цијели бројеви. Ако је $\textbf{нзд}(a,b)=1$, доказати да је $\textbf{нзд}(a+b, a-b) \leq 2$.
6. Доказати да је $mn(m^4-n^4)$ дјељив са 30 за свако $m, n \in \mathbb{N}$.
7. Ако су a, b и c цијели бројеви такви да је $\textbf{нзд}(a,b)=1$ и $c \mid a+b$, доказати да је $\textbf{нзд}(a,c)=\textbf{нзд}(b,c)=1$.
8. Ако су a, b и m цијели бројеви такви да је $\textbf{нзд}(a,b)=1$ и $m \mid a$, доказати да је $\textbf{нзд}(m,b)=1$.
9. Нека су m, n и a природни бројеви, при чему је $a>1$. Показати да је

$$\textbf{нзд}(a^m-1, a^n-1)=a^{\textbf{нзд}(m,n)}-1.$$

10. Ако су x и y реални бројеви, онда је $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor$ једнако 0 или 1, доказати да је

$$\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor,\ \ \{x+y\} \leq \{x\}+\{y\}.$$

5 Диофантове једначине

Теорема 5.1 *Нека су a, b и c цијели бројеви. Једначина*

$$ax + by = c$$

има цјелобројна рјешења ако и само ако $d|c$, гдје је $d = \textbf{нзд}(a, b)$.

Ако је пар x^*, y^* рјешење једначине, онда су сва рјешења дата формулом

$$x = x^* + \frac{b}{d}t$$
$$y = y^* - \frac{a}{d}t,$$

гдје је $t \in \mathbb{Z}$.

Примјетимо да се пар (x^*, y^*) може добити као

$$(x^*, y^*) = \left(\frac{c}{d}x_0, \frac{c}{d}y_0\right),$$

гдје је (x_0, y_0) рјешење једначине

$$ax + by = d$$

Доказ. Ако $d|a$ и $d|b$, онда је $d|ax + by$, односно $d|c$.

Обрнуто, нека $d|c$ и $c = kd$. Из Еуклидовог алгоритма слиједи да постоје цијели бројеви r, s тако да

$$d = ra + sb.$$

Одавде слиједи да $kd = (kr)a + (ks)b$, што значи да је $x^* = kr, y^* = ks$ рјешење дате једначине.

Остало је још да покажемо да се преко једног пара рјешења могу генерисати сва остала. Најприје, лако се изводи да ако је x^*, y^* рјешење једначине, онда су и x, y, датим формулама

$$x = x^* + \frac{b}{d}t$$
$$y = y^* - \frac{a}{d}t,$$

такође рјешења исте једначине.

Са друге стране, ако је

$$ax + by = ax^* + by^* = c,$$

онда вриједи

$$a(x - x^*) = b(y^* - y), \text{ односно } \frac{a}{d}(x - x^*) = \frac{b}{d}(y^* - y).$$

Пошто је

$$\textbf{нзд}(\frac{a}{d}, \frac{b}{d}) = 1, \text{ онда је } \frac{a}{d} \mid y^* - y.$$

Одавде слиједи да је $y = y^* - \frac{a}{d}t$. Замјеном овог израза за y у почетну једначину, као и замјеном $c = ax^* + by^*$, добијамо тражени израз $x = x^* + \frac{b}{d}t$.

На крају, очигледно је да ако је (x_0, y_0) рјешење једначине

$$ax + by = d,$$

онда је и пар

$$(x^*, y^*) = \left(\frac{c}{d}x_0, \frac{c}{d}y_0\right),$$

рјешење почетне једначине

$$ax + by = c.$$

■

Примјер 5.1 *Ријешити једначину* $27x + 59y = 20$.

Рјешење. Како је **нзд**$(27, 59) = 1$, онда се из проширеног Еуклидовог алгоритма добија $x_0 = -24$, $y_0 = 11$ као рјешења једначине

$$27x + 59y = 1.$$

На основу Теореме 5.1 слиједи да је опште рјешење почетне једначине дато са

$$x = -480 + 59t,\ y = 220 - 27t,\ t \in \mathbb{Z}.$$

■

6 Конгруенције - рачун остатака

Теорију конгруенција је увео Карл Фридрих Гаус (1777-1855), један од највећих математичара свих времена. Он је такође увео и ознаку за конгруенције коју и данас користимо.

Дефиниција 6.1 *Ако цијели број $m \neq 0$ дијели разлику $a - b$, онда кажемо да је a конгруентан b модуло m и пишемо $a \equiv b \pmod{m}$. У противном, кажемо да a није конгруентан b модуло m и пишемо $a \not\equiv b \pmod{m}$.*

Лема 6.1 *Релација конгруенције по модулу m је релација еквиваленције на скупу цијелих бројева.*

Доказ.

Релација је рефлексивна. Из $m \mid 0$ слиједи $m \mid a - a$, па је $a \equiv a \pmod{m}$ за свако $a \in \mathbb{Z}$.

Релација је симетрична. Нека су $a, b \in \mathbb{Z}$. Ако је $a \equiv b \pmod{m}$, онда је $m \mid a - b$, што значи да је и $m \mid b - a$, одакле је $b \equiv a \pmod{m}$.

Релација је транзитивна. Нека су $a, b, c \in \mathbb{Z}$.Ако је $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, онда је

$$m \mid a - b \text{ и } m \mid b - c,$$

одакле је $a - b = mk_1$, $b - c = mk_2$ за неке цијеле бројеве k_1 и k_2. Сабирањем лијевих и десни страна последње двије једнакости, добијамо $a - c = m(k_1 + k_2)$ што значи да је $a \equiv c \pmod{m}$.

■

Дакле, према дефиницији конгруенције и претходној леми, закључујемо да су цијели бројеви a и b у истој класи еквиваленције по модулу m ако и само ако је $a \equiv b \pmod{m}$, односно ако ова два броја дају исти остатак приликом дијељења са m.

Могући остаци приликом дијељења цијелог броја са m, сходно Теореми 4.1 су

$$0, 1, \ldots, m - 1.$$

То су заправо представници класа еквиваленције у односу на успостављену релацију. На примјер у класи еквиваленције остатка r, $0 \leq r < m$ коју означавамо са $[r]$ се налазе сви цијели бројеви који дају остатак r приликом дијељења са m, што је

$$[r] = \{r + km \mid k \in \mathbb{Z}\}.$$

Означимо се $\mathbb{Z}_m$ скуп класа еквиваленције, односно $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$. Из практичних разлога, врло често, умјесто ознаке класа, користимо само представнике класа, па пишемо $\mathbb{Z}_m = \{0, \ldots, m-1\}$.

Лема 6.2 *Нека су a, b, c, d цијели бројеви.*

1. *Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, онда је*

$$a + c \equiv b + d \pmod{m},\ a - c \equiv b - d \pmod{m},\ ac \equiv bd \pmod{m}.$$

2. *Ако је $a \equiv b \pmod{m}$ и $d \mid m$, онда је $a \equiv b \pmod{d}$.*

3. *Ако је $a \equiv b \pmod{m}$, онда је $ac \equiv bc \pmod{mc}$ за сваки $c \neq 0$.*

Претходна лема је кључна у *рачуну остатака*. У следећем примјеру се истичу неке од њених употребних вриједности.

Примјер 6.1 *Рачунамо $3^{188} \pmod{13}$. Наивни, али практично немогућ приступ би се састојао од тражења вриједности 3^{188} коју би потом дијелили са 13 да би се нашао тражени остатак. Међутим, Лема 6.2 нам сугерише другачији пут. Наиме*

$$3^2 = 9 \equiv -4 \pmod{13},\ 3^4 = (3^2)^2 \equiv (-4)^2 = 16 \equiv 3 \pmod{13},$$

па је

$$3^8 = (3^4)^2 \equiv 3^2 = 9 \pmod{13},\ 3^{12} = 3^8 3^4 \equiv 9 \cdot 3 \equiv 1 \pmod{13}.$$

Чињеница да је $3^{12} \equiv 1 \pmod{13}$ је од кључне вриједности, јер онда из $188 = 12 \cdot 15 + 8$, схватамо да је

$$3^{188} = \left(3^{12}\right)^1 5 \cdot 3^8 \equiv 1 \cdot 9 \pmod{13}.$$

Примјер 6.2 *Докажимо да је $a(a+1)(2a+1)$ дјељиво са 6 за сваки цијели број a. Директном провјером, на примјер ако је $a \equiv 2 \pmod{6}$ онда је*

$$a(a+1)(2a+1) \equiv 2 \cdot 3 \cdot 5 \equiv 0 \pmod{6},$$

што значи да је производ дјељив са 6. Слично можемо провјерити и за остале остатке $\{0, 1, 3, 4, 5\}$ по модулу 6 и утврдити да ће у сваком од тих случајева производ $a(a+1)(2a+1)$ бити дјељив са 6.

Примјер 6.3 *Наћи последњу цифру броја*

$$1997^{1998^{1999}}.$$

Рјешење. Нека је $N = 1997^{1998^{1999}}$. Задатак се заправо своди на одређивање $N \pmod{10}$. Како је $1997 \equiv 7 \pmod{10}$, онда је

$$N \pmod{10} \equiv 7^{1998^{1999}}.$$

Са друге стране, из низа $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$, $7^5 \equiv 7 \pmod{10}, \ldots$, видимо да је

$$7^a \equiv \begin{cases} 1 \pmod{10} & \text{ако је } a \equiv 0 \pmod 4 \\ 7 \pmod{10} & \text{ако је } a \equiv 1 \pmod 4 \\ 9 \pmod{10} & \text{ако је } a \equiv 2 \pmod 4 \\ 3 \pmod{10} & \text{ако је } a \equiv 3 \pmod 4 \end{cases}$$

Из $1998 \equiv 2 \pmod 4$, слиједи $1998^{1999} \equiv 2^{1999} \equiv 4 \cdot 2^{1997} \equiv 0 \pmod 4$, одакле закључујемо да је

$$N \equiv 1 \pmod{10}.$$

■

Примјер 6.4 *Доказати да је* $11 \cdot 14^n + 1$ *сложен број за* $n \in \mathbb{N}$.

Рјешење. Ако је $N = 11 \cdot 14^n + 1$, покажимо да $p \mid N$ за неки прост број p, такав да је $N > p$.

Ако је $n = 2k$, онда је $14 \equiv -1 \pmod 3$, одакле је $14^n \equiv 1 \pmod 3$. Закључујемо да

$$N \equiv 2 \cdot 1 + 1 \equiv 0 \pmod 3,$$

што значи да је дјељив са 3.

У случају да је $n = 2k+1$, онда је $14 \equiv -1 \pmod 5$, па је $14^n \equiv -1 \pmod 5$. Дакле,

$$N \equiv 1 \cdot (-1) + 1 \equiv 0 \pmod 5,$$

чиме је показано да је дјељив са 5.

Значи, у оба случаја закључујемо да је N дјељив са простим бројем који је строго мањи од њега, што значи да је сложен. ■

Лема 6.3 *Нека је f полином са цјелобројним коефицијентима. Ако је $a \equiv b \pmod m$, онда је $f(a) \equiv f(b) \pmod m$.*

Лема 6.4 *Нека су a, x, y цијели бројеви, при чему $a \neq 0$. Вриједи*

$$ax \equiv ay \pmod{m} \quad \text{ако и само ако} \quad x \equiv y \pmod{\frac{m}{\textbf{нзд}(a,m)}}.$$

Доказ. Нека је $ax \equiv ay \pmod{m}$, а $\textbf{нзд}(a,m) = d$. Пошто је $a(x-y) = mk$, онда је

$$\frac{a}{d}(x-y) = \frac{m}{d}k.$$

Како је $\textbf{нзд}(\frac{a}{d}, \frac{m}{d}) = 1$, онда слиједи да

$$\frac{m}{d} \mid (x-y).$$

Обратно, из $x - y = \frac{m}{d}k$, слиједи да

$$a(x-y) = m\frac{a}{d}k.$$

Како је $\frac{a}{d}$ цијели број, онда слиједи тврђење. ■

Лема 6.5 *Нека су a, b, x, y цијели бројеви, $a \neq 0$, $b \neq 0$. Онда је*

$$x \equiv y \pmod{a} \text{ и } x \equiv y \pmod{b} \iff x \equiv y \pmod{\textbf{нзс}(a,b)}.$$

Доказ. Ако је $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$, онда је $x - y = \alpha a$, $x - y = \alpha b$, што значи да је $x - y$ заједнички садржалац бројева a и b, па је према томе и $x \equiv y \pmod{\textbf{нзс}(a,b)}$. Ово слиједи из тврђења да је сваки садржалац бројева a и b дјељив са $\textbf{нзс}(a,b)$, а што је доказано у Леми 4.10.

Обратно слиједи директно из Леме 6.2, тврђење 2. ■

Дефиниција 6.2 *Скуп $\{x_1, x_2, \ldots, x_m\}$ се зове потпун систем остатака модуло m ако и само ако за сваки $y \in \mathbb{Z}$ постоји тачно један x_j такав да је $y \equiv x_j \pmod{m}$ Другим ријечима, потпуни систем остатака добијамо тако што из сваке класе еквиваленције узмемо по једног представника.*

Примјер 6.5 *Да ли је скуп $\{1^2, 2^2, \ldots, m^2\}$ комплетан систем остатака по модулу m?*

Рјешење. Како је

$$1^2 \equiv (m-1)^2 \pmod{m},$$

онда је јасно да дати скуп није потпун систем остатака. ■

Теорема 6.1 *Нека је $\{x_1, x_2, \ldots, x_m\}$ потпуни систем остатака модуло m, те нека је $(a, m) = 1$. Тада је $\{ax_1, ax_2, \ldots, ax_m\}$ такође потпуни систем остатака модуло m.*

Доказ. Ако је

$$ax_i \equiv ax_j \pmod{m}, \text{ за } i \neq j,$$

онда је

$$x_i \equiv x_j \pmod{m}, \text{ за } i \neq j,$$

на основу Леме 6.4. Пошто је, по претпоставци, $\{x_1, x_2, \ldots, x_m\}$ потпуни систем остатака модуло m, онда имамо контрадикцију. ■

Теорема 6.2 *Нека су $a, m \in \mathbb{N}$, а $b \in \mathbb{Z}$. Конгруенција*

$$ax \equiv b \pmod{m}$$

има рјешења ако и само ако $d = (a, m)$ дијели b. Ако је x_0 било које рјешење задате конгруенције, онда су сва друга рјешења дата са

$$x = x_0 + \frac{mt}{d}, \; t \in \mathbb{Z}.$$

Посебно, ова рјешења формирају тачно d класа конгруенције по модулу m, а чији су представници

$$x = x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

Доказ. Дата конгруенција је еквивалентна Диофантовој једначини

$$ax + my = b,$$

па користећи Теорему 5.1 слиједи потребан и довољан услов постојања њеног рјешења, као и облик тог рјешења

$$x = x_0 + \frac{mt}{d}, \; t \in \mathbb{Z},$$

гдје је x_0 било које рјешење дате конгруенције.

С обзиром на то да се ради о конгруенцији по модулу m, јасно је да су њена рјешења неке од класа конгруенције по датом модулу, па их може имати највише m. Примјећујемо да

$$x_0 + \frac{mt}{d} \equiv x_0 + \frac{mt'}{d} \pmod{m}$$

ако и само ако $m \mid \dfrac{m(t-t')}{d}$ што значи да $d \mid t - t'$, односно да различита рјешења конгруенције по модулу m добијамо тако што t прође комплетан скуп остатака по модулу d, као што је $\{0, 1, \ldots, d-1\}$.

■

Посљедица 6.1 *За $a, m \in \mathbb{N}$ једначина*

$$ax \equiv 1 \pmod{m}$$

има рјешење ако и само ако **нзд**$(a, m) = 1$, *односно ако су a, m узајамно прости.*

Примјер 6.6 *Ријешимо конгруенцију* $555x \equiv 15 \pmod{5005}$.

Ако скратимо са 5 цијелу конгруенцију, добијамо $111x \equiv 3 \pmod{1001}$.

Најприје, рјешавамо конгруенцију

$$111x \equiv 1 \pmod{1001}.$$

Користимо Бланкишип методу

$$\begin{bmatrix} 111 & 1 & 0 \\ 1001 & 0 & 1 \end{bmatrix}$$

Ако помножимо прву врсту са 9 и то одузмемо од друге врсте, добијамо

$$\begin{bmatrix} 111 & 1 & 0 \\ 2 & -9 & 1 \end{bmatrix}$$

Одузимање од прве врсте друге, претходно помножене са 55

$$\begin{bmatrix} 1 & 496 & -55 \\ 2 & -5 & 1 \end{bmatrix}$$

На крају, одузимањем прве врсте од друге, претходно помножене са 2, имамо

$$\begin{bmatrix} 1 & 496 & -55 \\ 0 & x & y \end{bmatrix}$$

Дакле, имамо да је $111 \cdot 496 \equiv 1 \pmod{1001}$.

Дакле, једно рјешење почетне конгруенције је $3 \cdot 49 \equiv 487 \pmod{1001}$.

На основу Теореме 6.2 имамо 5 неконгруентних рјешења почетне једначине

$$x \equiv 487,\ 1488,\ 2489,\ 3490,\ 4491 \pmod{5005}.$$

Примјер 6.7 *Доказати да полином $f(x) = x^5 - x^2 + x - 3$ нема цјелобројних корије́на.*

Рјешење. Ако овај полином има цјелобројну нулу a, то значи да је $f(a) = 0$, па је и

$$f(a) \equiv 0 \pmod{n}$$

за произвољан природан број n. То значи да ако пронађемо неко m тако да

$$f(x) \not\equiv 0 \pmod{m} \text{ за свако } x \in \mathbb{Z}_m,$$

онда ће то значити да дати полином нема цјелобројних рјешења.

У конкретном случају, директном порвјером, уочавамо да је

$$f(x) \not\equiv 0 \pmod 4 \text{ за } x \in \mathbb{Z}_4.$$

■

6.1. Остаци квадрата

Последња цифра квадрата цијелих бројева може бити из скупа:

$$\{0, 1, 4, 5, 6, 9\},$$

што се може записати и на следећи начин: Конгруенција

$$x^2 \equiv a \pmod{10}$$

има рјешења по x ако и само ако $a \in \{0, 1, 4, 5, 6, 9\}$.

Примјер 6.8 *Могући остаци квадрата природних бројева су*

по модулу 3: 0,1

по модулу 4: 0,1

по модулу 5: 0,1,4

по модулу 6: 0,1,3,4

по модулу 7: 0,1,2,4

по модулу 8: 0,1,4

по модулу 9: 0,1,4,7

Примјер 6.9 *Доказати да постоји бесконачно много цијелих бројева који се не могу представити у облику збира кубова три цијела броја.*

Рјешење. Одредимо могуће остатке цијелих бројева по модулу 9:

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8

Дакле, ти остаци су 0, 1 и 8. Збир три таква броја модуло 9 може бити само: 0, 1, 2, 3, 6, 7 и 8. Дакле, бројеви облика $9k + 4$ и $9k + 5$ се не могу представити у облику збира три куба. ■

6.2. Кинеска теорема о остацима

Кинеска теорема о остацима се заправо бави проблемом рјешавања система линеарних конгруенција.

Теорема 6.3 *(Кинеска теорема о остацима) Нека су $m_1, m_2, \ldots, m_r$ у паровима релативно прости природни бројеви, те нека су $a_1, a_2, \ldots, a_r$ цијели бројеви. Тада систем конгруенција*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots \quad , x \equiv a_r \pmod{m_r}$$

има рјешења. Ако је x_0 једно рјешење, онда су сва рјешења система дата са

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}.$$

Посебно, постоји јединствено рјешење датог система по модулу M, гдје је $M = m_1 \cdots m_r$.

Доказ. Нека је $n_j = \frac{M}{m_j}$, за $j = 1, 2, \ldots, r$. Јасно је да је **нзд**$(m_j, n_j) = 1$, па на основу Леме 6.2 постоји цијели број x_j такав да

$$n_j x_j \equiv a_j \pmod{m_j}.$$

Посматрајмо број

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Очигледно, за овај број вриједи да је

$$x_0 \equiv 0 + \cdots + n_j x_j + \cdots + 0 \equiv a_j \pmod{m_j}.$$

Дакле, x_0 јесте рјешење датог система конгруенција.

Ако су x, y два рјешења датог система, онда је

$$x \equiv y \pmod{m_j} \text{ за } j = 1, \ldots, r.$$

Због чињенице да су m_j у паровима релативно прости, слиједи да је $x \equiv y \pmod{M}$, што значи да је рјешење јединствено по модулу M. ■

Примјер 6.10 *Ријешити систем конгруенција*

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Рјешење. Уз ознаке Теореме 6.3 имамо да је

$$x_0 = 77x_1 + 55x_2 + 35x_3,$$

гдје x_1, x_2, x_3 задовољавају

$$77x_1 \equiv 2 \pmod{5}, \quad 55x_2 \equiv 3 \pmod{7}, \quad 35x_3 \equiv 4 \pmod{11},$$

односно

$$2x_1 \equiv 2 \pmod 5, \quad 6x_2 \equiv 3 \pmod 7, \quad 2x_3 \equiv 4 \pmod{11}.$$

Рјешавањем појединачних конгруенција, добијамо

$$x_1 = 1,\ x_2 = 4,\ x_3 = 2,$$

што даје $x_0 = 367$. Према томе, сва рјешења система су дата са

$$x \equiv 367 \pmod{385}.$$

■

Примјер 6.11 *Ријешити систем конгруенција*

$$x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}, \quad x \equiv 5 \pmod{84}.$$

Umjesto ovog uzeti Garet primjer 3.15 strana 55

6.3. Примјене конгруенција

Конгруенције имају бројне, веома занимљиве примјене, а посебно Кинеска теорема о остацима.

Претпоставимо да морамо да рачунамо вриједност K која укључује збирове, разлике, производе неких великих бројева $a_1, a_2, \ldots a_m$. Одаберимо низ од r простих бројева, $p_1, p_2, \ldots, p_r$, такве да је сигурно да је $K < p_1 p_2 \cdots p_r$. Поступак добијања K можемо "паралелизовати" на r процесора, при чему ће сваки од њих вршити рачунања у mod p_i аритметици. На крају, сви резултати добијени на појединачним процесорима се удружују путем Кинеске теореме о остацима у коначан резултат.

(This result has applications in many areas, including astronomy: if k events occur regularly, with periods nl, ... ,nk, and with the i-th event happening at timesx = ai,ai+ni,ai+2ni,...

Garret strana 53

7 Увод у алгебарске структуре

Иако су читаоци већ, могуће и у оквиру средњошколског образовања стекли одређене појмове о алгебарским структурама, у овом поглављу полазимо од основних појмова.

Током основне и средње школе смо се сусрели са различитим скуповима бројева као што су: скуп природних бројева $\mathbb{N}$, скуп цијелих бројева $\mathbb{Z}$, скуп рационалних бројева $\mathbb{Q}$, скуп реалних бројева $\mathbb{R}$, скуп комплексних бројева $\mathbb{C}$. Над овим скуповима смо дефинисали сабирање, одузимање, множење, дијељење, степеновање...

Подсјетимо се неких основних законитости.

1) *Збир два природна броја је природан број.*

$$\text{Ако } x, y \in \mathbb{N} \text{ онда } x + y \in \mathbb{N}.$$

2) *Збир два цијела броја је цио број.*

$$\text{Ако } x, y \in \mathbb{Z} \text{ онда } x + y \in \mathbb{Z}.$$

3) *Производ два природна броја је природан број.*

$$\text{Ако } x, y \in \mathbb{N} \text{ онда } x \cdot y \in \mathbb{N}.$$

4) *Производ два цијела броја је цио број.*

$$\text{Ако } x, y \in \mathbb{Z} \text{ онда } x \cdot y \in \mathbb{Z}.$$

5) *Разлика два природна броја није увијек природан број.*

$$\text{Постоје } x, y \in \mathbb{N} \text{ тако да } x - y \notin \mathbb{N}.$$

6) *Разлика два цијела броја је цијели број.*

$$\text{Ако } x, y \in \mathbb{Z} \text{ онда } x - y \in \mathbb{Z}.$$

7) *Количник два природна броја није увијек природан број.*

$$\text{Постоје } x, y \in \mathbb{N} \text{ тако да } x/y \notin \mathbb{N}.$$

8) *Количник два цијела броја није увијек цио број.*

$$\text{Постоје } x, y \in \mathbb{Z} \text{ тако да } x/y \notin \mathbb{Z}.$$

Ако би сабирање, одузимање, множење или дијељење означили симболом $\star$, а скуп цијелих или природних бројева са S, онда би горње исказе могли да замијенимо *математичким реченицима*:

А. За свака два елемента x и y из S, вриједи да $x \star y$ припада S.

Б. Постоје елементи x и y из S, тако да $x \star y$ не припада S.

Видимо да у случају кад је, на примјер, S скуп природних бројева $\mathbb{N}$ а $\star$ сабирање $+$, онда вриједи исказ **А**. У том случају, ако вриједи исказ А, онда кажемо да је скуп S ***затворен*** у односу на операцију $\star$. Такође, видимо да је скуп $\mathbb{Z}$ затворен у односу на множење, али није у односу на дијељење. Заправо, ако је скуп S затворен у односу на $\star$, то зачи да

$$a \star b \in S,$$

за свако a и b из тог скупа S. Тиме долазимо и до следеће дефиниције.

Дефиниција 7.1 *Пресликавање $\star$*

$$\begin{aligned} \star : S \times S &\to S \\ (a, b) &\to \star(a, b) \end{aligned}$$

*на непразном скупу S назовамо **бинарна операција**. Вриједност $\star(a, b)$ из скупа S уобичајено означавамо са $a \star b$.*

Дакле, ако кажемо да је $\star$ бинарна операција на непразном скупу S, то онда подразумијева затвореност. То се у одређеном смислу разиликује од уобичајене употребе појма *операција*, као што су сабирање, одузимање, множење, дијељење. Наиме, видјели смо да, на примјер, одузимање није операција на скупу $\mathbb{N}$ иако ми неке природне бројеве можемо да одузимамо.

Дефиниција 7.2 *За уређени пар $(S, \star)$, гдје је $\star$ бинарна операција на непразном скупу S кажемо да је **групоид**.*

Примјер 7.1 *Нека је $S = \{-1, 1\}$ а $+, -, \cdot, /$ уобичајене операције сабирања, одузимања, множења и дијељења. С обзиром да*

$$1 + 1 \notin S, \; 1 - 1 \notin S$$

онда је јасно да $(S, +)$ и $(S, -)$ нису групоиди. Међутим, $(S, \cdot)$ и $(S, /)$ јесу.

Из претходног, видимо да су $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}, \cdot)$ групоиди, док на примјер $(\mathbb{N}, -)$ и $(\mathbb{Z}, /)$ то нису. Премда смо навикли да операције углавном везујемо за оне са којима имамо највише искуства у школовању и свакодневици, оне могу бити апстрактне и без неке одређене "употребне" вриједности.

Примјер 7.2 *Нека је $S = \{1, 2, 3, 4\}$. Дефинишимо операцију $\circ$ на следећи начин*

$$i \circ j = j$$

за свако $i, j \in S$.

Очигледно, овако дефинисана операција је затворена у S, па је S групоид.

На основу дефиниције бинарне, лако се долази до појма $n-$арне операције.

Дефиниција 7.3 *Пресликавање*

$$\begin{aligned} \star : S \times S \cdots \times S &\rightarrow S \\ (a_1, \ldots, a_n) &\rightarrow \star(a_1, \ldots, a_n) \end{aligned}$$

*на непразном скупу S називамо $n-$**арна операција**.*

Примјер 7.3 *Као што смо већ уочили, на истом скупу је често могуће дефинисати више разиличитих операција. На примјер, на скупу $\mathbb{Z}$, можемо увести бинарне операције попут*

$$x * y = \textbf{нзд}(x, y)$$

$$x \circ y = \textbf{нзс}(x, y) + 1$$

$$x \bullet y = x + y^2 - 1$$

У алгебарском смислу, ради се о различитим структурама $(\mathbb{Z}, *)$, $(\mathbb{Z}, \circ)$ и $(\mathbb{Z}, \bullet)$

*Могуће је дефинисати и операције веће "арности", попут **тернарних**, кад је $n = 3$, на примјер*

$$*(x, y, z) = x^2 + y + z - 1$$

*за цијеле бројеве x, y, z. Очигледно, ова операција је само илустрација, која нема неки очигледно практични значај. Примјер тернарне операције која има пуни математички смисао би био примјер **мјешовитог векторског производа** у векторском простору.*

Примјер 7.4 *Иако смо досад скоро по правилу упућени на скупове бројева, попут* $\mathbb{Z}$ *и* $\mathbb{N}$*, могуће је направити и "нетипичан" скуп. На примјер, ако посматрамо скуп свих подскупова* $\mathcal{P}(S)$ *неког непразног скупа* S*, онда можемо увести скуповне операције попут*

$$G \diamond H = G \cap H$$

$$G \odot H = G \cup H$$

$$G * H = A \setminus (G \setminus H)$$

Дакле, у свим наведеним случајевима се ради о групоидима.

◉ *Ако је* S *скуп свих пресликавања непразног скупа* A *у себе, док је композиција* $\circ$ *операција на* S*, да ли је* $(S, \circ)$ *групоид?*

◉ *Да ли је скуп матрица димензија* $n \times n$ *са елементима из скупа цијелих бројева* $\mathcal{M}_n(\mathbb{Z})$ *у односу на операцију множења матрица групоид?*

7.1. Својства операција

У примјерима које смо наводили, све операције су *бинарне*, такве да су у интеракцији два елемента скупа, а то резултира трећим елементом.

Дакле, видимо да на имплицитан начин појам бинарне операције подразумијева, односно укључује затвореност на скупу.

Међутим, уколико би своја интересовања задржали искључиво на скуп и бинарну операцију на њему, то би било прилично сувопарно. Поред саме дефиниције бинарне релације, оно што је занимљиво су њене особине, наравно у квалитативној вези са скупом на ком су дефинисане. Кад кажемо *особине операција*, то можемо илустровати у нама блиским, односно познатим примјерима.

Примјер 7.5 *На скупу цијелих бројева $\mathbb{Z}$, за операције сабирања и множења вриједи особина* ***асоцијативности***

$$a + (b + c) = (a + b) + c, \;\; a * (b * c) = (a * b) * c,$$

за свако a, b, c из скупа цијелих бројева.

За исте операције вриједи и својство ***комутативности****, односно*

$$a + b = b + a, \;\; a \cdot b = b \cdot a$$

за свако a, b из скупа цијелих бројева.

Примјетићемо да асоцијативност и комутативност операција сабирања и одузимања вриједи и на скуповима $\mathbb{N}$, $\mathbb{Q}$ и $\mathbb{R}$.

Међутим, асоцијативност не вриједи за операцију одузимања, односно, јасно је да не вриједи у општем случају

$$a - (b - c) = (a - b) - c$$

ни у једном од наведених скупова.

Такође, не вриједи комутативност за операцију одузимања.

У складу са претходним примјером, уводимо дефиницију

Дефиниција 7.4 *Бинарна операција $\star$ на скупу S је асоцијативна ако вриједи*

$$a \star (b \star c) = (a \star b) \star c \;\; \text{за свако } a, b, c \in S.$$

Бинарна операција $\star$ на скупу S је комутативна ако вриједи

$$a \star b = b \star a \;\; \text{за свако } a, b \in S.$$

Примјер 7.6 *Као у Примјеру 7.4, на скупу подскупова непразног скупа X, партитивном скупу $\mathcal{P}(X)$ посматрамо операције пресјека и уније. Елементарна је чињеница да*

$$A \cap (B \cap C) = (A \cap B) \cap C, \;\; A \cap B = B \cap A,$$

као и

$$A \cup (B \cup C) = (A \cup B) \cup C, \;\; A \cup B = B \cup A.$$

Дакле, обје операције су и асоцијативне и комутативне на скупу $\mathcal{P}(X)$. С тим у вези, $(\mathcal{P}(X), \cap)$ и $(\mathcal{P}(X), \cap)$ су асоцијативни групоиди.

Примјер 7.7 *На скупу природних бројева $\mathbb{N}$, посматрамо операцију степеновања, односно*

$$a \circ b := a^b.$$

Очигледно, ова операција није ни асоцијативна ни комутативна, односно не важи

$$(a \circ b) \circ c = a \circ (b \circ c) \text{ ни } a \circ b = b \circ a$$

за свако a, b, c из скупа природних бројева.

На примјер,

$$\left(2^3\right)^2 \neq 2^{3^2} \text{ као и } 2^3 \neq 3^2.$$

Примјер 7.8 *Операција на скупу $S = \{x \mid x \in \mathbb{R} \text{ и } x \geq 0\}$ дефинисана са*

$$x \star y = \sqrt{x + y}$$

је очигледно комутативна. Међутим, није асоцијативна, јер

$$\sqrt{x + \sqrt{y + z}} \neq \sqrt{\sqrt{x + y} + z}$$

у општем случају. Дакле, можемо рећи да је $(S, \star)$ неасоцијативни, комутативни групоид.

Дефиниција 7.5 *Групоид $(S, \star)$ у ком је операције $\star$ асоцијативна се назива* ***полугрупа****.*

Примјер 7.9 *Количник два ненулта рационална броја опет ненулти рационални број, па је скуп свих ненултих, рационалних бројева, $\mathbb{Q}^*$, групоид. Међутим,*

$$\frac{1}{2} \div \frac{1}{4} = 2 \neq \frac{1}{2} = \frac{1}{4} \div \frac{1}{2},$$

$$\frac{1}{2} \div \left(\frac{1}{4} \div \frac{1}{3}\right) = \frac{2}{3} \neq 6 = \left(\frac{1}{2} \div \frac{1}{4}\right) \div \frac{1}{3},$$

па операција на овом скупу није ни комутативна, а ни асоцијативна.

Како је у полугрупи $(S, \star)$ операција асоцијативна, онда има смисла дефинисати

$$a^n := \underbrace{a \star a \star \cdots \star a}_{n}.$$

Примјер 7.10 *Нека је $M_n(\mathbb{Z})$ скуп свих матрица димензије $n \times n$, са елементима из скупа цијелих бројева. Из елементарне линеране алгебре нам је познато да вриједи*

$$A + (B + C) = (A + B) + C, \ A \star (B \star C) = (A \star B) \star C.$$

гдје знак $+$ означава уобичајено матрично сабирање, $\star$ матрично множење, а A, B, C су матрице из скупа $M_n(\mathbb{Z})$.

Значи, $(M_n(\mathbb{Z}), +)$ и $(M_n(\mathbb{Z}), \star)$ су полугрупе. С обзиром да је

$$A + B = B + A$$

за A, B из $M_n(\mathbb{Z})$, онда је $(M_n(\mathbb{Z}), +)$ комутативна полугрупа, за разлику од $(M_n(\mathbb{Z}), \star)$ с обзиром на то да матрично множење није комутативно.

Наравно, све претходно важи и за матрице над неким другим скупом бројева, као на примјер над скупом реалних бројева, $M_n(\mathbb{R})$.

Поред посматрања особина операција, можемо се осврнути и на неке специфичне елементе скупа на ком је дефинисана операција, односно његове особине. На примјер, знамо да вриједи

$$a + 0 = 0 + a$$

за сваки цијели број a. Дакле, нула има врло специфичну особину у односу на сабирање цијелих бројева. Слично је и са јединицом у односу на множење цијелих бројева

$$a \cdot 1 = 1 \cdot a.$$

Примјећујемо да су нула и једница, у односу на сабирање односно множење, у одређеном смислу неутралне, односно да не утичу на резултат.

Дефиниција 7.6 *Елемент e у групоиду $(S, \star)$ је* ***лијево неутралан*** *у односу на операцију $\star$ уколико вриједи*

$$e \star a = a$$

за сваки елемент a у скупу S. Аналогно, ако је

$$a \star e' = a,$$

за свако a у скупу S онда је e' ***десни неутрални.*** *Ако је e лијеви и десни неутрални, онда кажемо да је* ***неутрални*** *у односу на дату операцију.*

Примјер 7.11 *Нека је дата операција $a \circ b = a(a^2 - 1) + b$ на скупу цијелих бројева $\mathbb{Z}$. Очигледно, $(\mathbb{Z}, \circ)$ је групоид. Примјетимо да су 0, -1 и 1 лијеви неутрални елементи у групоиду $(\mathbb{Z}, \circ)$, док не постоји десни неутрални.*

Примјер 7.12 *Посматрамо операцију степеновања на скупу* $\mathbb{N}$

$$a \circ b = a^b.$$

Видимо да је 1 десни неутрални елемент у групоиду $(\mathbb{N}, \circ)$*, док не постоји лијеви.*

Примјер 7.13 *Посматрајмо операцију* $\star$ *на скупу* $\mathbb{Z}$ *дефинисану са*

$$a \star b := 2a + 3b.$$

Лако се уочава да је $(\mathbb{Z}, \star)$ *групоид у ком не постоји ни лијеви ни десни неутрални елемент.*

Лема 7.1 *Нека је* e *лијево неутрални, а* e' *десно неутрални елемент у групоиду* $(S, \star)$*. Онда је* $e = e'$*.*

Доказ. Пошто је e лијеви неутрални, онда је

$$e \cdot e' = e'.$$

Са друге стране,

$$e \cdot e' = e,$$

јер је e' десни неутрални. Из ове двије једнакости слиједи да је $e = e'$. ■

На основу претходне леме закључујемо да у групоиду може постојати највише један неутрални елемент.

Посљедица 7.1 *Групоид* $(S, \star)$ *има највише један неутрални елемент.*

Доказ. Као што смо видјели у Примјеру 7.13, групоид $(S, \star)$ не мора да има неутрални елемент. Претпоставимо да постоје два неутрална елемента e и $'$. Пошто је e уједно и лијеви неутрални, а $'$ десни неутрални, онда је на основу Леме 7.1, јасно да је $e = e'$. ■

Дефиниција 7.7 *Полугрупа* $(S, \star)$ *која има неутрални елемент* e *се назива* ***моноид****.*

Примјер 7.14 *Скуп природних бројева у односу на операцију множења* $(\mathbb{N}, \cdot)$ *и елемент 1 чини моноид. Слично, скуп цијелих бројева у односу на операцију сабирања* $(\mathbb{Z}, +)$ *и 0 као неутрални елемент такође чини моноид.*

Јасно је да једначине

$$a + x = b \text{ или } cx = d$$

гдје су a, b, c, d природни бројеви није увијек могуће ријешити у скупу природних бројева. Међутим, уочавамо да је прву једначину увијек могуће ријешити у скупу цијелих бројева. Уколико је $c \neq 0$, онда је другу једначину увијек могуће ријешити у скупу рационалних бројева. У нешто апстрактнијем обику, претходно питање можемо поставити на следећи начин.

◉ *Да ли је у моноиду* $(S, \star)$ *могуће ријешити једначину*

$$a \star x = b \text{ или } x \star a = b,$$

за неке $a, b \in S$.

Претходно питање је везано за комплекснију алгебарску структуру, а тијесно је везано за појам инверзног елемента, објашњеног у следећој дефиницији.

Дефиниција 7.8 *За елемент* a' *моноида* $(S, \star)$ *са неутралним елементом* e*, кажемо да је* ***лијеви инверз*** *елемента* a *из* S *ако да вриједи*

$$a' \star a = e.$$

Аналогно, за a'' *кажемо да је* ***десни инверз*** *елемента* a *из* S *ако*

$$a \star a'' = e.$$

Ако је a' *уједно и лијеви и десни инверзни елемента* a *кажемо да је* ***инверзни елемент*** *или* ***инверз*** *од* a.

Вратимо се још једном питању да ли је у моноиду $(S, \star)$ могуће ријешити једначину

$$a \star x = b$$

за неке конкретне $a, b \in S$. Уколико је a' лијеви инверз елемента $a \in S$, онда је

$$\begin{aligned} a' \star (a \star x) &= a' \star b, \\ (a' \star a) \star x &= a' \star b, \\ e \star x &= a' \star b \\ x &= a' \star b. \end{aligned}$$

Слично би се рјешавала и једначина $x \star a = b$ под условом да постоји десни инверз елемента a. Наравно, у случају да је операција $\star$ комутативна, онда појмови лијеви или десни инверз губе смисао.

Примјер 7.15 *Нека је дат моноид* $(\mathbb{N}, \cdot)$*, скуп природних бројева са операцијом множења. Јасно, у питању је комутативни моноид. Очигледно, ниједан елемент сем неутралног елемента 1 нема свој инверз.*

Примјер 7.16 *Нека је дат непразан скуп* A*. Посматрајмо* $\mathcal{M}(A)$ *који се састоји од свих пресликавања из* A *у* A*. Лако се показује да је овај скуп заправо моноид, чији је неутрални елемент* I_A *које је дефинисано као* $I_A(x) = x$*,* $x \in A$*. Међутим, нема свако пресликавање инверзни елемент.*

Посматрајмо, на примјер скуп $A = \mathbb{Z}$ *и пресликавања* $f, g \in A$*, дефинисана као*

$$f(x) = 2x, \quad g(x) = \begin{cases} \frac{x}{2} & \text{ако је } x \text{ паран,} \\ 4 & \text{ако је } x \text{ непаран.} \end{cases}$$

Очигледно, не постоји десни инверз за пресликавање f*, односно не постоји* $h \in A$ *вриједи* $f \circ h = I_{\mathbb{Z}}$*. С друге стране, постоји лијеви инверз за* f *и то је управо пресликавање* g*, јер је* $g \circ f = I_{\mathbb{Z}}$*.*

Умјесто броја 4, у дефиницији пресликавања g *за непарне аргументе, може бити било који други број што неће промијенити* $g \circ f = I_{\mathbb{Z}}$*. С обзиром на то да функција* f *предаје функцији* g *само парне бројеве, онда је неважно, у смислу лијевог инверза за* f*, како ће* g *бити дефинисано на скупу непарних бројева.*

Из претходних примјера видимо да у моноиду $(S, \star)$ не мора постојати инверз за дати елемент, потом да може постојати само лијеви инверз или само десни. Међутим, уколико елемент има и лијеви и десни инверз у моноиду S, онда се ради о истом елементу. То је и тврђење наредне леме.

Лема 7.2 *Нека је дат моноид* $(S, \star)$ *са неутралним елементом* e*, док је* w *елемент* S *чији је* w' *лијеви инверз, а* w'' *десни инверз. Онда је*

$$w' = w''.$$

Доказ. Нека је $y = w \star w'$. Онда је

$$y = y \star e = (w \star w') \star (w \star w'') = w \star (w' \star w) \star w'' = (w \star e) \star w'' = w \star w'' = e.$$

Дакле,

$$w \star w' = e,$$

што значи да је u' заправо десни инверз по дефиницији, па је $w' = w''$. ■

Посљедица 7.2 *За елемент* w *моноида* $(S, \star)$ *постоји највише један инверзни елемент.*

Доказ. Као што смо видјели у Примјеру 7.16, не мора да постоји инверз за сваки елемент моноида. Међутим, ако постоји, онда је јединствен. Наиме, претпоставимо да су w' и w'' инверзни елементи елемента w. Онда су они истовремено и лијеви и десни инверзи, па закључак да је $w' = w''$ директно слиједи из Леме 7.2. ■

Дакле, елемент u моноида S не мора имати обавезно инверзни елемент, али ако га има, он је јединствен. Из претходног се природно намеће идеја о моноиду $(S, \star)$ у ком сваки елемент има свој инверз. Управо такви моноиду су предмет наше пажње у наредној секцији.

7.2. Групе

Сусрели смо се са идејом моноида $(S, \star)$ у којем је могуће рјешавати једначине

$$a \star x = b \text{ или } x \star a = b,$$

за произвољно a, b из S. Као што смо већ истакли, ове једначине је могуће рјешавати кад год елемент $a \in S$ има инверз у S.

Примјер 7.17 *Подсјетимо се* $\mathbb{Z}_m$*, гдје је* $m \in \mathbb{N}$*, скупа класа еквиваленције у односу на релацију конгруенције по модулу* m

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}.$$

Уводимо операцију $\boxplus_m$ *на класама еквиваленције. Ако су* $[s]$ *и* $[t]$ *двије класе еквиваленције из скупа* $\mathbb{Z}_m$*, дефинишемо сабирање класа као*

$$[s] \boxplus_m [t] = [s+t].$$

Најприје, потребно је доказати да је овако уведена операција добро дефинисана. То значи да резултат сабирања класа не смије зависити од избора представника тих класа. Дакле, ако је $[s_1] = [s_2]$, $[t_1] = [t_2]$*, онда је* $s_1 + t_1 \equiv s_2 + t_2 \pmod{m}$*, односно* $[s_1 + t_1] = [s_2 + t_2]$*, а што значи да је*

$$[s_1] \boxplus_m [t_1] = [s_2] \boxplus_m [t_2].$$

Дакле, операција сабирања на класама је добро дефинисана. Неутрални елемент у односу на операцију $\boxplus_m$ *је класа којој припада нула, односно* $[0]$*. Операција* $\boxplus_m$ *је комутативна*

$$[s] \boxplus_m [t] = [s+t] = [t+s] = [t] \boxplus_m [s].$$

Слично доказујемо асоцијативност $\boxplus_m$ *.*

$$\begin{aligned}
([s] \boxplus_m [t]) \boxplus_m [v] &= [s+t] \boxplus_m [v] \\
&= [(s+t)+v] \\
&= [s+(t+v)] \\
&= [s] \boxplus_m [t+v] \\
&= [s] \boxplus_m ([t] \boxplus_m [v])
\end{aligned}$$

За произвољну класу $[a]$ *из* $\mathbb{Z}_m$ *вриједи*

$$[a] \boxplus_m [m-a] = [0],$$

што значи да сваки елемент има свој инверз. Такође, очигледно је да је $\boxplus_m$ *комутативна операција, па је* $(\mathbb{Z}_m, \boxplus_m)$ *Абелова група.*

Ако уведемо операцију множења над калсама, слично као што смо увели сабирање, коју алгебарску структуру ћемо добити?

Примјер 7.18 *Дефинишимо операцију* $\ast_m$ *на скупу* $\mathbb{Z}_m$

$$[s] \ast_m [t] = [st].$$

Као и у претходном примјеру, доказујемо да је операција добро дефинисана. Наиме, из $[s_1] = [s_2]$ *и* $[t_1] = [t_2]$*, односно* $s_1 \equiv t_1 \pmod m$ *и* $s_2 \equiv t_2 \pmod m$ *слиједи*

$$s_1 t_1 \equiv s_2 t_2 \pmod m.$$

Одавде је $[s_1 t_1] = [s_2 t_2]$.

Операција је асоцијативна.

$$\begin{aligned}([s] \ast_m [t]) \ast_m [v] &= [st] \ast_m [v] \\ &= [(st)v] \\ &= [s(tv)] \\ &= [s] \ast_m [tv] \\ &= [s] \ast_m ([t] \ast_m [v])\end{aligned}$$

Такође, из $[s] \ast_m [t] = [st] = [ts] = [t] \ast_m [s]$*, слиједи да је операција комутативна. Очигледно,* $[1]$ *је неутрални елемент. Дакле,* $(\mathbb{Z}_m, \ast_m)$ *је комутативни моноид.*

Међутим, $(\mathbb{Z}_m, \ast_m)$ *није група. Очигледно,* $[0]$ *нема инверзни елемент. На основу Леме 6.1, класа* $[a] \in \mathbb{Z}_m$ *има инверзни елемент ако и само ако су* a *и* m *узајамно прости.*

На основу претходних примјера закључујемо да скуп $\mathbb{Z}_m$, остатака по модулу m, зависно од посматране операције, $+_m$ или $\ast_m$ представља одређене алгебарске структуре, што се наводи у следећој леми.

Лема 7.3 *За природан број* m*, скуп остатака* $\mathbb{Z}_m$ *у односу на операцију* $+_m$ *је Абелова група, а у односу на* $\ast_m$ *комутативни моноид.*

У Примјеру 7.18 наведено је да елмент $a \in \mathbb{Z}_m$ има инверзни елемент ако и само ако је **нзд**$(a, m) = 1$. Шта се дешава ако за дато $m \in \mathbb{N}$ посматрамо скуп свих елемената из $\mathbb{Z}_m$ са тим својством? Тиме се бави следећи примјер.

Примјер 7.19 *Посматрајмо скуп* $G = \{[1], [2], [4], [5], [7], [8]\} \subseteq \mathbb{Z}_9$, *оних елемената из скупа остатака који су релативно прости са 9, у односу на операцију множења по модулу 9.*

У следећој табели су садржани резултати операције $\circledast_9$ *на посматраном скупу* G. *На примјер,* $[5] \circledast_9 [7] = [8]$, *док је* $[7]^{-1} = [4]$. *Провјеравајући све особине из дефиниције, није тешко утврдити да је* $(G, \circledast_9)$ *Абелова група.*

$\bullet$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Као што знамо, операција множења по модулу 9 је комутативна, па је $(G, \cdot)$ *комутативни моноид.*

Дефиниција 7.9 *Моноид* $(G, \star)$ *у ком сваки елемент има свој инверз се назива* ***група****. Уколико је операција* $\star$ *у групи комутативна, онда се* $(G, \star)$ *назива* ***Абелова група****.*

Примјер 7.20 *а. Скуп $G = \{1, 2, 4, 5, 7, 8\}$ у односу на операцију множења по модулу 9 је Абелова група.*

б. Скуп свих цијелих бројева, у односу на сабирање је Абелова група. Означавамо је $(\mathbb{Z}, +)$.

в. Скуп свих реалних бројева изузев нуле, у односу на множење је Абелова група. Ову групу означавамо $(\mathbb{R}^*, \cdot)$.

*г. Скуп свих **реалних матрица** (матрица чији су елементи реални бројеви) реда 3×3 чија је детерминанта различита од нуле, у односу на множење матрица је некомутативна група. Њу означавамо са $(GL_3(\mathbb{R}), \cdot)$. На примјер, за матрице*

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

вриједи $AB \neq BA$, што значи да је ова група некомутативна.

Наравно, ово можемо уопштити за $(GL_n(\mathbb{R}), \cdot)$, групу матрица димензије n, за произвољан природан број.

Примјер 7.21 *У примјеру 7.16 смо видјели да је скуп $\mathcal{M}(A)$ свих пресликавања из A у A моноид, ако је A непразан скуп. Међутим, ако посматрамо подскуп $S(A)$ од $\mathcal{M}(A)$, свих бијективних пресликавања из A у A, онда лако уочавамо да је у питању **група у односу на композицију пресликавања**. Наиме, чињеница да се ради о бијективним пресликавањима обезбјеђује постојање инверзног елемента за сваки елемент из $S(A)$. Дакле, $(S(A), \circ)$ је група. Ову групу називамо **групом пермутација** а њима ћемо се посебно бавити у наредној секцији.*

Лема 7.4 *Нека је $(G, \star)$ група. Онда*

а. Постоји јединствени неутрални елемент у G.

б. За сваки $u \in G$ постоји јединствени инверзни елемент $u' \in G$.

Доказ. Тврђење **а.** слиједи директно из Последице 7.1, док тврђење **б.** слиједи из Последице 7.2. ■

Као што смо већ констатовали, скуп свих реалних бројева изузев нуле, $(\mathbb{R}^*, \cdot)$, у односу на множење је Абелова група. Међутим, није тешко утврдити и да скуп рационалних бројева без нуле, $\mathbb{Q}^*$, а што је подскуп од $\mathbb{R}^*$, у односу на операцију множења такође чини групу. То нас доводи до наредне дефиниције.

Дефиниција 7.10 *Нека је $(G, \cdot)$ група, а H подскуп скупа G. Уколико је $(H, \cdot)$ група, онда за H кажемо да је* ***подгрупа*** *групе G и означавамо са $H \leq G$.*

Примјер 7.22 *Скуп* ***реалних матрица****, $(GL_3(\mathbb{R}), \cdot)$, реда 3×3 чија је детерминанта различита од нуле, као што смо већ констатовали у Примјеру 7.20, у односу на множење матрица је некомутативна група. Посматрајмо подскуп скупа GL_3, оних матрица чија је детерминанта једнака јединици, односно*

$$SL_3 = \{A \in GL_3 \mid \det(A) = 1\}.$$

У односу на множење матрице, скуп SL_3 чини групу, што се тривијално провјерава. Дакле, $(SL_3(\mathbb{R}), \cdot)$ је подгрупа групе $(GL_3(\mathbb{R}), \cdot)$.

Лема 7.5 *Нека је H непразан подскуп групе $(G, \cdot)$. Онда је $(H, \cdot)$ подгрупа ако и само ако вриједи*

$$xy^{-1} \in H$$

за свако x и y из H.

С обзиром на то да је из контекста јасно на коју се операцију мисли за поједину групу, онда се ознака за ту операцију најчешће изоставља. Тако се, умјесто $(G, \cdot)$, пише само G, при чему се каже да је G са мултипликативном операцијом. Слично, ако користимо ознаку $+$, онда кажемо да је G адитивна. Сходно претходном, у случају мултипликативне групе, уобичајена ознака за јединични елемент је 1, а 0 у случају адитивне групе. Уколико је тип операције у групи небитан, онда се пише само - група G.

Дефиниција 7.11 *Ред групе G, који се означава са $|G|$, је број елемената у скупу G. За групу чији је ред коначан кажемо да је* ***коначна****. Ако ред није коначан, тада је група* ***бесконачна****, што се означава са $|G| = \infty$.*

Примјер 7.23 *Група $GL_3(\mathbb{R})$, из Примјера 7.20 је бесконачна, јер јој припадају, на примјер, све матрице облика*

$$A = \begin{bmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

за произвољно $a \in \mathbb{R}$, $a \neq 0$.

За разлику од претходне, група у Примјеру 7.19 је коначна и њен ред је 6.

7.2.1. Групе пермутација

Примјер 7.24 *Нека је дат скуп $A = \{1, 2, 3, 4\}$. Посматрајмо скуп свих бијекција овог скупа, односно*

$$S_4 = \{\pi \mid \pi : A \to A,\ \pi \text{ бијекција}\}.$$

Пресликавања из S_4 можемо представити на природан начин, табелама попут

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Видимо да је, на примјер, $\pi_1(2) = 1$, а $\pi_1(4) = 4$. Посматрамо операцију композиције пресликавања. На примјер, ако је

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

онда је

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Наиме, композиција два пресликавања из S_4 је пресликавање из S_4. Композиција је асоцијативна, а идентичко пресликавање је

$$id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

неутрални елемент у односу на композицију. Такође, ако је $\pi \in S_4$ и $\pi(i) = j$, онда је $\pi^{-1}(j) = i$, чиме се лако дефинише инверзно пресликавање датом пресликавању. Дакле, скуп S_4 у односу на композицију пресликавања $(S_4, \circ)$ је група.

Свакако, претходни примјер можемо уопштити на произвољно $n \in \mathbb{N}$ односно свих бијекција скупа $A = \{1, 2, \ldots, n\}$. Ако је $\tau \in S_n$, онда се и ово пресликавање може представити

$$\tau = \begin{pmatrix} 1 & \cdots & n \\ \tau(1) & \cdots & \tau(n) \end{pmatrix}$$

Лема 7.6 *Скуп свих бијекција скупа $A = \{1, 2, \ldots, n\}$ чини групу S_n у односу на композицију пресликавања. Ову групу називамо* ***симетрична група****. Њен ред је $n!$*

Доказ. Јасно је да је композиција двије бијекције скупа опет бијекција тог скупа. Такође, композиција пресликавања је асоцијативна операција. Неутрални елемент у односу на композицију је идентичко пресликавање

$$id(i) = i,\ i = 1, \ldots, n.$$

За дату бијекцију f постоји бијективно пресликавање f^{-1} тако да

$$f \circ f^{-1} = f^{-1} \circ f = id,$$

што значи да је S_n група.

Број бијекција $n-$точланог скупа је заправо број пермутација скупа од n елемената, а то је $n!$. ■

Лема 7.7 *Симетричне групе S_1 и S_2 су комутативне, док S_3 није.*

Доказ. Симетрична група S_1 се састоји од идентичког пресликавања id које слика 1 у 1.

Симетрична група S_2 се састоји од два пресликавања id и π

$$id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Очигледно, S_2 је комутативна. Да би показали да S_3 није комутативна, довољно је да покажемо да постоје двије пермутације из S_3 које не комутирају. У том смислу, посматрајмо пермутације $\pi_1,\ \pi_2$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Видимо да

$$1 = \pi_1(\pi_2(1)) \neq \pi_2(\pi_1(1)) = 3,$$

што значи да π_1 и π_2 не комутирају. Дакле, група S_3 није комутативна. ■

Посљедица 7.3 *Симетрична група S_k није комутативна за $k \geq 3$.*

Доказ. Како је случај $k = 3$ већ обрађен у претходној леми, онда за $k > 3$, користећи сличан приступ, посматрамо пермутације $\pi_1,\ \pi_2$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & k \\ 2 & 1 & 3 & 4 & \cdots & k \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & k \\ 2 & 3 & 1 & 4 & \cdots & k \end{pmatrix}.$$

Пошто су сви елементи за $k \geq 4$ фиксирани, а као и прије вриједи

$$1 = \pi_1(\pi_2(1)) \neq \pi_2(\pi_1(1)) = 3,$$

јасно је да π_1 и π_2 не комутирају. Дакле, група S_k, за $k \geq 4$ није комутативна. ■

7.2.2. Групе изометрија

Присјетимо се Еуклидске удаљености између двије тачке равни $P_1 = (a_1, b_1)$, $P_2 = (a_2, b_2)$ равни $\mathbb{R}^2$

$$d(P_1, P_2) = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}.$$

Разматрамо пресликавања у равни која *чувају удаљеност* између тачака. На примјер, такво пресликавање је транслација за неки фиксни вектор (v_1, v_2)

$$f((x, y)) = (x, y) + (v_1, v_2) = (x + v_1, y + v_2).$$

Јасно је да у овом случају вриједи

$$d(P_1, P_2) = d(f(P_1), f(P_2)),$$

за било које двије тачке P_1, P_2 равни $\mathbb{R}^2$.

Дефиниција 7.12 *Изометрија равни је бијективно пресликавање $f : \mathbb{R}^2 \to \mathbb{R}^2$ које чува удаљеност, односно*

$$d(P_1, P_2) = d(f(P_1), f(P_2)),$$

за сваке двије тачке P_1, P_2 из равни $\mathbb{R}^2$. Са $\mathcal{I}(\mathbb{R}^2)$ означавамо скуп свих изометрија равни.

Иако смо се у претходном разматрању ограничили на раван, јасно је да се све одреднице могу пренијети и на праву $\mathbb{R}$, као и на простор $\mathbb{R}^3$. Међутим, одабрали смо раван $\mathbb{R}^2$ због познатих илустративних примјера изометрија. С тим у вези, наводимо, поред транслација, још неке основне примјере изометрија равни.

. Најједноставнији примјер изометрије равни је **идентичко пресликавање** које се назива и **коинциденција**.

$$(x, y) \to (x, y).$$

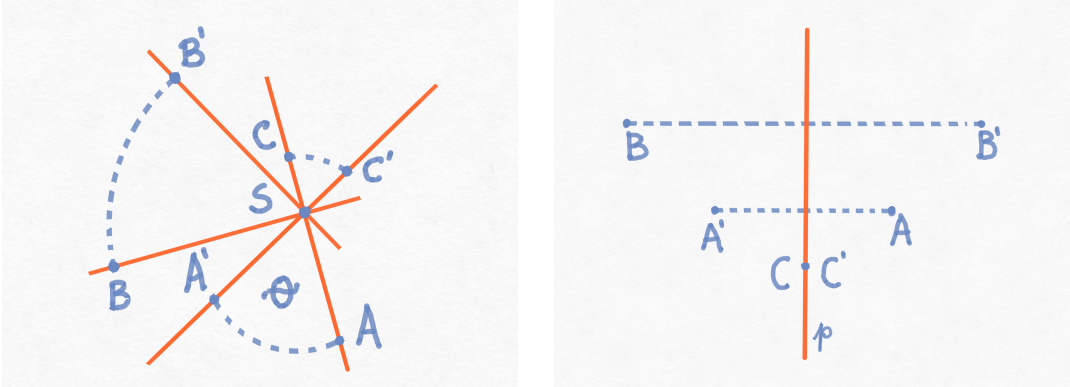
.. **Ротација** за угао θ у односу на фискну тачку S, $\rho_{\theta,S}$.

$$(x, y) \to (x\cos(\theta) - y\sin(\theta), x\sin(\theta) + y\cos(\theta)).$$

Примјетимо да за ротацију за угао од 180 степени добијамо нешто што је познато као **централна симетрија у односу на фиксну тачку**.

... **Осна симетрија** σ_p у односу на неку праву (осу) $p \equiv ax + by + c = 0$. Координате тачке (s', t') осносиметричне тачки (s, t) у односу на дату праву p су

$$s' = \frac{s(a^2 - b^2) - 2b(at + c)}{a^2 + b^2}, \quad t' = \frac{t(b^2 - a^2) - 2a(bs + c)}{a^2 + b^2}.$$



(a) ротација (b) осна симетрија

Слика 7.1: Примјери изометрија

Ако су f, g двије изометрије равни, онда је

$$d((f \circ g)(P_1), (f \circ g)(P_2)) = d(f(g(P_1)), f(g(P_2))) = d(g(P_1), g(P_2)) = d(P_1, P_2)$$

за сваке двије тачке P_1 и P_2 равни. Такође, копозиција $f \circ g$ двије бијекције је бијекција. Дакле, за $f, g \in \mathcal{I}(\mathbb{R}^2)$, слиједи да је $f \circ g \in \mathcal{I}(\mathbb{R}^2)$.

Пошто је f изометрија, па тиме и бијекција, онда постоји f^{-1} пресликавање равни $\mathbb{R}^2$), за које вриједи

$$d(f^{-1}(P_1), f^{-1}(P_2)) = d(f(f^{-1}(P_1)), f(f^{-1}(P_2))) = d(P_1, P_2)$$

за сваке двије тачке P_1, P_2 равни, па је тиме и $f^{-1} \in \mathcal{I}(\mathbb{R}^2)$. Примјећујемо да за ротацију $\rho_{\theta,S}$ и осну симетрију σ_p вриједи

$$\rho_{\theta,S}^{-1} = \rho_{2\pi-\theta,S} \text{ и } \sigma_p^{-1} = \sigma_p.$$

Из претходног слиједи важно тврђење.

Лема 7.8 *Скуп свих изометрија, $\mathcal{I}(\mathbb{R})$ равни $\mathbb{R}^2$ чини групу у односу на композицију пресликавања.*

Као што је већ наглашено, претходна лема се може односити и на $\mathbb{R}$ и на $\mathbb{R}^3$. Из саме дефиниције изометрије се види да се сваки скуп F тачака равни изометријом пресликава у њему подударан скуп тачака. Међутим, од посебног значаја су оне симетрије које дати скуп F пресликавају на самог себе. С тим у вези је следећа дефиниција.

Дефиниција 7.13 *За изометрију $f \in \mathcal{I}(\mathbb{R}^2)$ кажемо да* ***чува*** *скуп $F \subseteq \mathbb{R}^2$, уколико важи да је $f(F) = F$, гдје је $f(F)$ скуп слика тачака из F, односно*

$$f(F) = \{f(P) \mid P \in F\}.$$

Тада кажемо и да је f ***симетрија*** *скупа F. Скуп свих симетрија скупа F означавамо са $\mathcal{I}(F)$. Дакле,*

$$\mathcal{I}(F) = \{f \in \mathcal{I}(\mathbb{R}) \mid f(F) = F\}.$$

За произвољан подскуп F равни $\mathbb{R}^2$, увијек постоји бар једна изометрија која га чува. Наравно, у питању је идентичко пресликавање односно коинциденција. Величина $\mathcal{I}(F)$ зависи од самог скупа F, односно његове "симетричности".

Примјер 7.25 *Нека је $F = k(O, r)$ кружница у равни са центром у тачки O и полупречником r. Свака осна симетрија у односу на произвољну праву која пролази кроз центар кружнице O је уједно и симетрија саме кружнице. Дакле, због "бесконачне" симетричности кружнице, $\mathcal{I}(F)$ је бесконачна група.*

Поред осних симетрија, изометрије које чувају кружницу су и ротације око центра кружнице за произвољан угао.

Примјер 7.26 *Одређујемо $\mathcal{I}(F)$ за скуп $F = \{(-1, 0), (1, 0)\}$. Означимо $A = (-1, 0)$, $A' = (1, 0)$.*

Постоје само двије опције, два могућа пресликавања у $\mathcal{I}(F)$. Нека су то f и g. Онда

1. $$f(A) = A,\ f(A') = A',$$

2. $$g(A) = A',\ g(A') = A.$$

Пресликавању f би могла да одговара коинциденција на $\mathbb{R}^2$, док би пресликавању g одговарала осна симетрија у односу на симетралу дужи AA'.

На истовјетан начин како је показано да је $(\mathcal{I}(R^2), \circ)$ група, показује се да је то и $(\mathcal{I}(F), \circ)$ за било који подсуп $F \subseteq \mathbb{R}^2$.

Лема 7.9 *Нека је F подскуп равни $\mathbb{R}^2$. Онда је $\mathcal{I}(F)$ група у односу на композицију пресликавања.*

Од свих подскупова равни $\mathbb{R}^2$, многоуглови, односно групе њихових симетрија су посебно интересантне. Ове групе су имале снажан утицај на развој теорије група.

Лема 7.10 *Нека је f изометрија равни, A и B двије тачке у равни, а $A' = f(A)$ и $B' = f(B)$ њихове слике. Онда се дуж AB слика у дуж $A'B'$. Посебно, ако је тачка C дужи AB, онда је $C' = f(C)$ тачка дужи $A'B'$.*

Доказ. Нека је C тачка на дужи AB. Како је $|AC| + |CB| = |AB|$, онда мора бити и $|f(A)f(C)| + |f(C)f(B)| = |f(A)f(B)|$. Због неједнакости троугла, ово је могуће само уколико је тачка $f(C)$ на дужи $f(A)f(B)$. ■

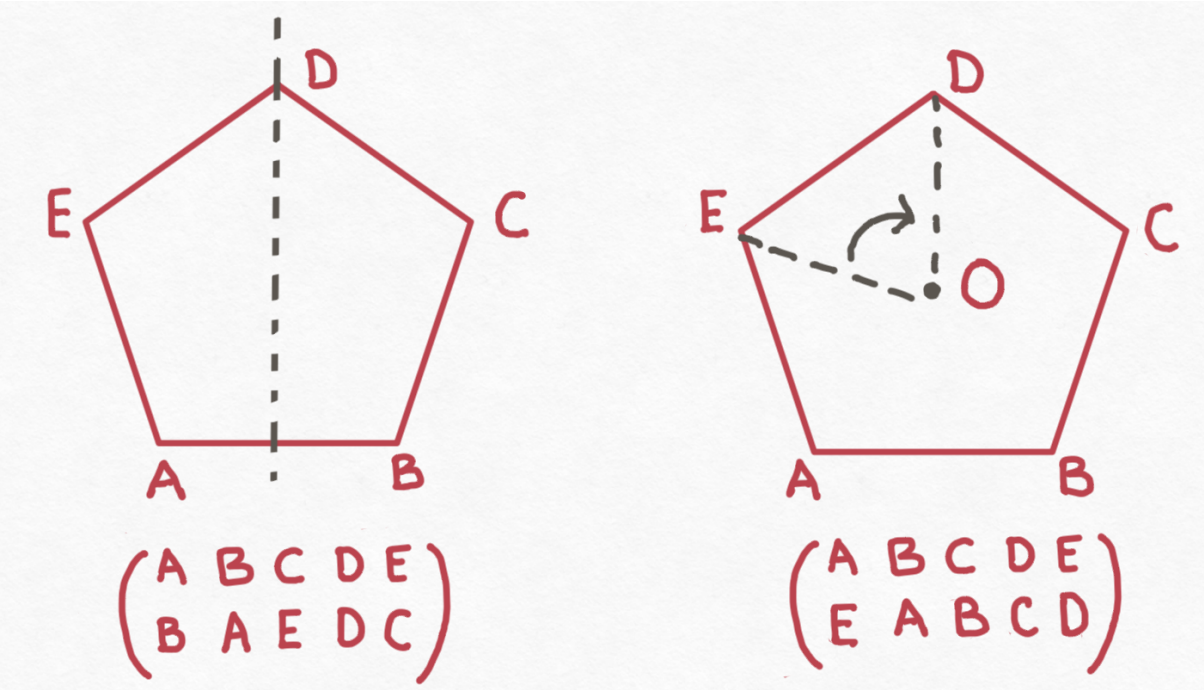
Из претходне леме, слиједи веома важна чињеница.

Посљедица 7.4 *Нека је P_n многоугао у равни. Онда свака симетрија P_n пермутује његова тјемена $A_1, A_2, \ldots, A_n$.*

Доказ. Нека је A_1A_2 страница многугла P_n. Према Леми 7.10, свака страница многоугла се слика у страницу многоугла $A'_iA'_{i+1}$, при чему је $A'_i = f(A_1)$ и $A'_{i+1} = f(A_i)$. У случају да је $i = n$, онда подразумијевамо да је $A_{n+1} = A_1$.

У сваком случају, тјемена се сликају у тјемена. Како је f бијекција, онда је јасно да f заправо пермутује тјемена многоугла. ■

У суштини, свака симетрија $n-$тоугла је на јединствен начин одређена пермутацијом његових тјемена. Посебно је интересантан и важан случај правилног $n-$тоугла.



Слика 7.2: Примјери симетрија петоугла

На слици 7.2 видимо примјер двије симетрије петоугла. То су осна симетрија која пролази кроз тјеме B и средину супротне странице, као и централна ротација за угао од α од 72 степена. Руководећи се истим принципом, видимо да постоје још осне симетрије кроз тјемена A, E, D, C, као и централне ротације за углове 2α, 3α, 4α. Уз идентичко пресликавање, а које одговара и ротацији од 0, односно 360 степени, постоје 5 изометрија петоугла које одговарају централним ротацијама.

Са друге стране, постоје 5 изометрија које одговарају осним симетријама које пролазе кроз тјемена A, B, C, D, E и средине наспрамних страница. Дакле, постоје најмање 10 изометрија које чувају петоугао? Да ли их има више?

◉ *Нека је R_n правилни $n-$тоугао. Колики је ред групе $\mathcal{I}(R_n)$?*

Нека је O центар правилног многоугла R_n, односно тачка описаног и уписаног круга за R_n. Примјетимо ротације $\rho_{\alpha_k,O}$ око тачке , рецимо у смјеру супротном кретању казаљке на сату, гдје је $\alpha_k = 2k\pi/n$, за $k = 1, 2, \ldots, n$. Таквих ротација, видимо, има n. Ако је $\rho = \rho_{\alpha_1,O}$ ротација за основни угао $2\pi/n$, очигледно је да је

$$\rho_{\alpha_k,O} = \rho^k, \;\; k = 1, 2, \ldots, n,$$

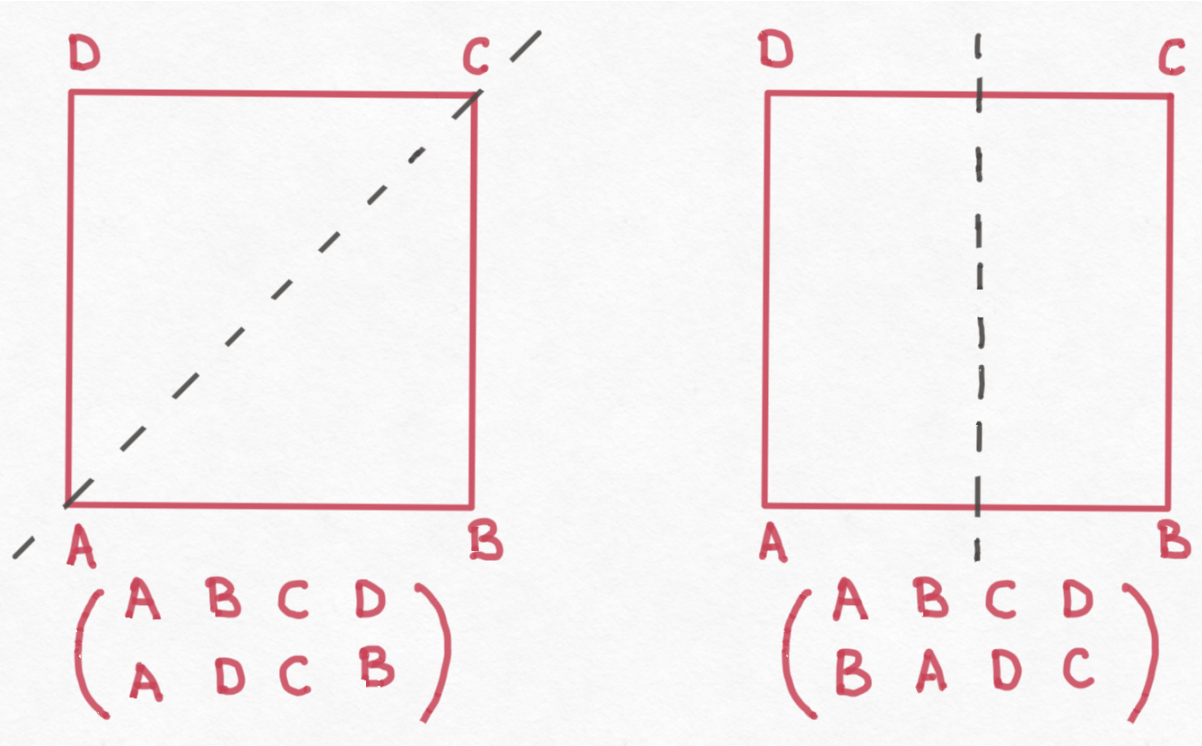
Матрична репрезентације пермутације која одговара ротацији $\rho_{\alpha_k,O}$ је

$$\rho_{\alpha_k,O} = \begin{pmatrix} A_1 & A_2 & \ldots & A_{n-k+1} & A_{n-k+2} & \ldots & A_n \\ A_k & A_{k+1} & \ldots & A_n & A_1 & \ldots & A_{k-1} \end{pmatrix},$$

за $k \in \{1, \ldots, n\}$. Поред описаних ротација имамо и осне симетрије правилног $n-$тоугла. Оне се дјелимично разликују у слаучају кад је n непарно и кад је n парно.

Наиме, уколико је n непарно, онда имамо, као у случају петоугла на Слици 7.2 тачно n изометрија које одговарају осним симетријама које пролазе кроз neko од n тјемена и средину супротне странице.

У случају да је $n = 2k$ парно, на примјер у случају квадрата као на Слици 7.3, онда имамо k изометрија које одговарају осним симетријама у односу на праве које пролазе кроз пар супротних тјемена $n-$тоугла. Такође, имамо и k изометрија које одговарају осним симетријама у односу на праве које пролазе кроз средине наспрамних страница $n-$тоугла.



Слика 7.3: Примјери осних симетрија квадрата

Дакле, за произвољни, правилни $n-$тоугао имамо:

- n ротација око центра за n различитих углова $2k\pi/n$, за $k = 0, 1, \ldots, n-1$.

- n осних симетрија у односу на праве које пролазе кроз два тјемена (кад је n парно) или једно тјеме и средину наспрамне странице (кад је n непарно).

То значи да за правилни постоји $n-$тоугао имамо најмање $2n$ изометрија које га чувају. Испоставиће се да их и нема више.

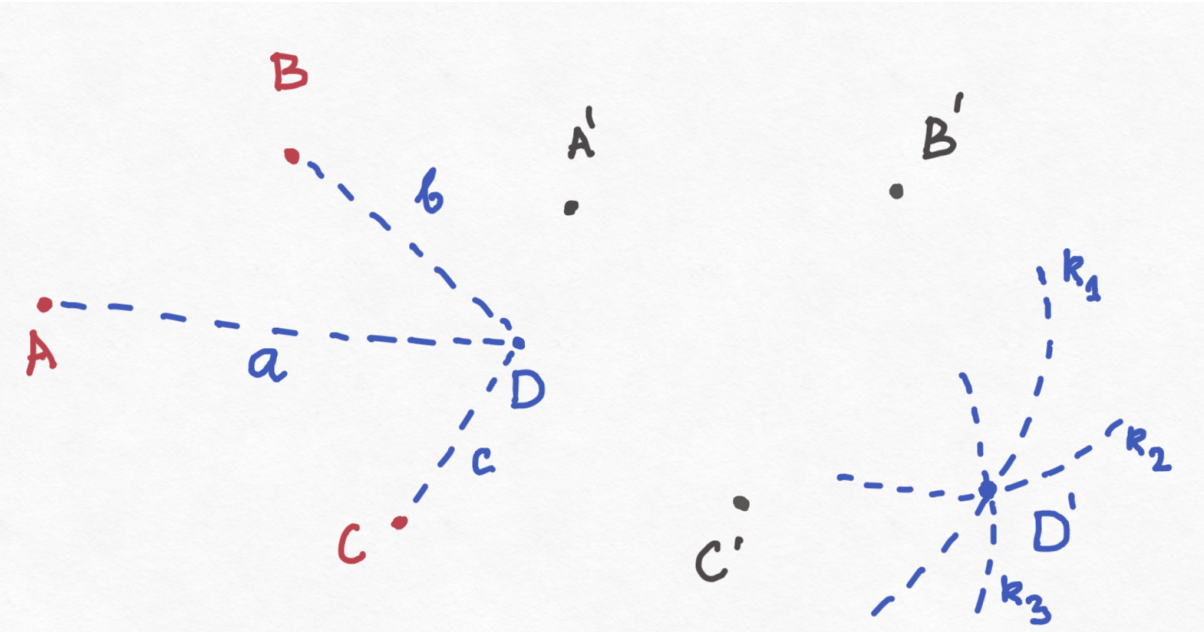
Следећа лема је важна у пребројавању укупног броја изометрија дате фигуре у равни.

Лема 7.11 *Свака изометрија је једнозначно одређена сликом три неколинеарне тачке.*

Доказ. Нека су A, B, C три неколинеарне тачке, а f изометрија равни. Претпоставимо

$$f(A) = A',\ f(B) = B',\ f(C) = C'.$$

Пошто су тачке A, B, C неколинеране, онда су то и A', B', C'. Нека је D произвољна тачка равни различита од A, B, C. Показујемо да је $f(D) = D'$ једнозаначно одређена.



Слика 7.4: Свака изометрија је једнозначно одређена са три тачке

Ако је $d(A, D) = a$, $d(B, D) = b$, $d(C, D) = c$, онда мора бити

$$d(A', D') = a,\ d(B', D') = b,\ d(C', D') = c.$$

То значи да ће се D' наћи у пресјеку кружница $k_1(A', a)$, $k_1(B', b)$ и $k_3(C', c)$. Међутим, пресјек три кружнице може бити скуп од двије тачке само у случају када су им центри колинеарни. Пошто се у овом случају ради о три неколинеарним тачкама у којима су смјештени центри кружница, онда је пресјек тачно једна тачка. Тиме је и $f(D) = D'$ једнозначно одређено. ■

Већ показали да је $\mathcal{I}(R_n) \geq 2n$, за правилни $n-$тоугао R_n. Следећа лема утврђује $\mathcal{I}(R_n) \leq 2n$ чиме је утврђен тачан број изометрија правилног $n-$тоугла.

Лема 7.12 *Нека је R_n правилни $n-$тоугао. Онда је број симетрија правилног $n-$тоугла једнак $2n$. Дакле, ред групе $\mathcal{I}(R_n)$ је $2n$.*

Доказ. Нека је $f \in \mathcal{I}(R_n)$. Како f пермутује тјемена $n-$тоугла, онда је, без умањења општости $f(A_1) = A_k$, за неко $k \in \{1, \ldots, n\}$. Дефинишимо лијевог, $\ell(A_k)$, и десног, $r(A_k)$, сусједа тјемена A_k.

$$\ell(A_k) = \begin{cases} A_n & \text{ако је } k = 1 \\ A_{k-1} & \text{ако је } k > 1 \end{cases} \quad r(A_k) = \begin{cases} A_1 & \text{ако је } k = n \\ A_{k+1} & \text{ако је } k < n. \end{cases}$$

Дакле, укупан број могућности за $f(A_1)$ је n. Које су онда могућности за њему сусједно тјеме, A_2? Због чувања растојања, очигледно је да за A_2 постоје двије могућности, $\ell(A_k)$ или $r(A_k)$. Међутим, избором једне од те двије могућности, једнозначно је утврђена и слика за A_3, односно $f(A_3)$. Дакле, ако је $f(A_1) = A_k$, онда

$$f(A_3) = \begin{cases} \ell(\ell(A_k)) & \text{ако је } f(A_2) = \ell(A_k) \\ r(r(A_k)) & \text{ако је } f(A_2) = r(A_k) \end{cases}$$

Како је, према Леми 7.11, сликама тачака A_1, A_2, A_3 у потпуности одређена изометрија, онда је укупан број могућности симетрија правилног $n-$тоугла број могућности на које можемо изабрати $f(A_1)$ помножен са бројем могућности избора за $f(A_2)$, што је $2n$. Примјетимо да избор $f(A_2)$ на лијеву или десну страну од A_k, утврђује и смјер којим се циклично сликају и сва остала тјемена, у смјеру казаљке на сату или супротно томе. Како је раније показано да је $\mathcal{I}(R_n) \geq 2n$, онда је $\mathcal{I}(R_n) = 2n$. ■

С обзиром да свакој симетрији правилног $n-$тоугла одговара једна пермутација из S_n, онда је група $\mathcal{I}(R_n)$ заправо подгрупа групе пермутација S_n. За групу изометрија правилног $n-$тоугла користимо посебан назив - *диједарска група* и обично је означавамо са D_{2n}.

Лема 7.13 *Нека је ρ ротација око центра правилног $n-$тоугла R_n за угао од $2\pi/n$ у смјеру супротном од кретања казаљке на сату, а σ осна симетрија у односу на неку праву која пролази кроз произвољно тјеме $n-$тоугла. Група D_{2n} се састоји од n ротација $id, \rho, \ldots, \rho^{n-1}$ и n осних симетрија $\sigma, \rho\sigma, \ldots, \rho^{n-1}\sigma$, односно*

$$D_{2n} = \{d, \rho, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \ldots, \rho^{n-1}\sigma\}.$$

Посебно, вриједи

$$\sigma\rho\sigma^{-1} = \sigma\rho\sigma = \rho^{-1}.$$

Доказ. Већ смо констатовали, у Леми 7.12, да је број симетрија правилног $n-$тоугла R_n једнак $2n$. С тим у вези, знамо да су ротације $id, \rho, \ldots, \rho^{n-1}$ половина тог броја.

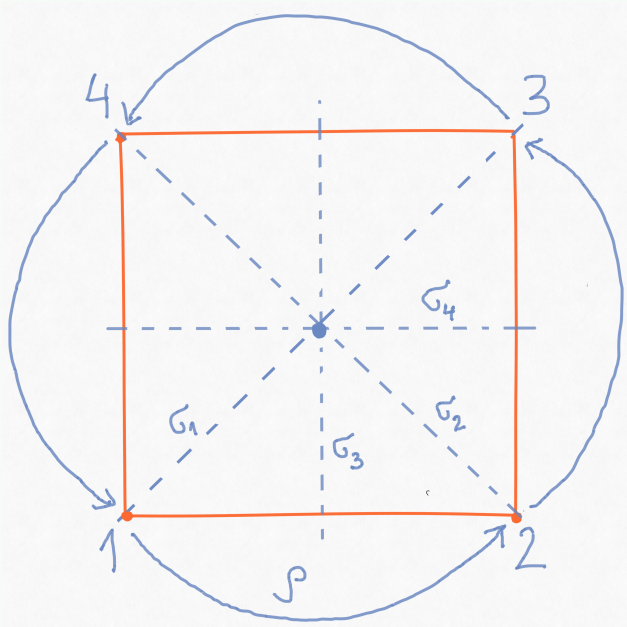
Са друге стране, посматрајмо пресликавања $\rho^k\sigma \in D_{2n}$ за $k = 0, \ldots, n-1$. Примјетимо да ова пресликавања нису ротације. Наиме, ако би $\rho^k\sigma = \rho^\ell$, слиједи да $\sigma = \rho^{\ell-k}$, али σ није ротација. Дакле, у питању су осне симетрије. Како за сваку осну симетрију важи да је сама себи инверзна, онда је и $(\rho\sigma)^2 = id$, што значи $\rho\sigma\rho\sigma = id$, односно

$$\sigma\rho\sigma^{-1} = \sigma\rho\sigma = \rho^{-1}.$$

■

У следећем примјеру разматрамо групу симетрија квадрата, односно групу D_8.

Примјер 7.27 *Нека су тјемена квадрата означена симболима* $1, 2, 3, 4$, *као на слици.*



Симетрије квадрата, представљене у облику пермутација, су

$$id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Пошто су σ_i *осне симетрије онда је* $\sigma_i^2 = id$ *за* $i = 1, 2, 3, 4$. *Такође, уочавамо да је* $H = \{id, \rho, \rho^2, \rho^3\}$ *циклична подгрупа групе симетрија квадрата* D_8 *генерисана ротацијом* ρ. *Директним рачунањем долазимо до мултипликативне табеле групе* D_8.

$\circ$	id	ρ	ρ^2	ρ^3	σ_1	σ_2	σ_3	σ_4
id	id	ρ	ρ^2	ρ^3	σ_1	σ_2	σ_3	σ_4
ρ	ρ	ρ^2	ρ^3	id	σ_4	σ_3	σ_1	σ_2
ρ^2	ρ^2	ρ^3	id	ρ	σ_2	σ_1	σ_4	σ_3
ρ^3	ρ^3	id	ρ	ρ^2	σ_3	σ_4	σ_2	σ_1
σ_1	σ_1	σ_3	σ_2	σ_4	id	ρ^2	ρ	ρ^3
σ_2	σ_2	σ_4	σ_1	σ_3	ρ^2	id	ρ^3	ρ
σ_3	σ_3	σ_2	σ_4	σ_1	ρ^3	ρ	id	ρ^2
σ_4	σ_4	σ_1	σ_3	σ_2	ρ	ρ^3	ρ^2	id

7.3. Коначне групе

У контексту повезивања алгебре са аритметиком, посебно су значајне групе са коначним бројем елемената - *коначне групе.*

Дефиниција 7.14 *Број елемената коначне групе $(G, \star)$ називамо* ***ред групе*** *и означавамо са* $\mathrm{ord}(G)$ *или са* $|G|$. *За елемент $a \in G$ кажемо да има коначни ред n, ако је n најмањеи природни број такав да је $a^n = e$, гдје је e јединични елемент групе G. Ред лемента a у групи G означавамо са* $\mathrm{ord}(a)$ *или* $|a|$.

Примјер 7.28

Уколико није назначено другачије, у наставку ћемо подразумијевати мутипликативну операцију на посматраној групи G,

Дефиниција 7.15 *Ако је G група таква да је*

$$G = \{a^n \mid n \in \mathbb{Z}\}$$

онда се G назива ***цикличка група*** *генерисана елементом a из дгрупе G. У том случају користимо ознаку $G = [a]$.*

Елемент a се назива ***генератор*** *групе G.*

Примјер 7.29 *Посматрајмо групу симетрија квадрата. Као што смо већ уочили, група има 8 елемената. Нека је ρ ротација за 90 степени. Онда је*

$$H = \{\rho, \rho^2, \rho^3, \rho^4 = id\}$$

подгрупа групе симетрија квадрата. Јасно, H је циклична група генерисана елементом ρ.

Нека је H подгрупа мултипликативне групе G, а t елемент групе G. Онда скуп

$$tH = \{th \mid h \in H\}$$

називамо **лијеви сускуп** или **лијеви косет** подгрупе H. Аналогно дефинишемо и **десни сускуп** Ht. С обзиром на то да је јединични елемент у подгрупи H, онда је $t \in tH$. Елемент t је **представник** сускупа tH. У случају адитивне групе G, лијеви косет подгрупе H је

$$t + H = \{t + h \mid h \in H.\}$$

Лема 7.14 *Нека је H подгрупа мултипликативне групе G, а t_1, t_2 произвољни елементи групе G. Онда*

$$t_1H = t_2H \text{ или } t_1H \cap t_2H = \emptyset.$$

Такође,

$$|t_1H| = |t_2H| = |H|.$$

Доказ. Претпоставимо да

$$t_1H \cap t_2H \neq \emptyset,$$

односно да $a \in t_1H \cap t_2H$. То значи да је $a = t_1h_1 = t_2h_2$, $h_1, h_2 \in H$. Одавде слиједи да $t_1 = t_2h_2h_1^{-1}$, односно $t_1 = t_2h'$, гдје је $h' = h_2h_1^{-1}$, што значи $h' \in H$. Дакле,

$$t_1H \subseteq t_2H.$$

Аналогно, слиједи да је

$$t_2H \subseteq t_1H,$$

па коначно закључујемо да је $t_1H = t_2H$.

За други дио тврђења, довољно је да докажемо да је $|t_1H| = |H|$. Како је

$$t_1h = t_1h'$$

за h, h' из H, могуће искључиво ако је $h = h'$, онда је јасно да је број елемената у t_1H једнак броју елемената у H. Тиме је тврђење доказано. ■

Лема 7.15 *Нека је H подгрупа мултипликативне групе G. Онда постоји подскуп $A \subseteq H$ тако да је G дисјунктна унија сусукупова чији су представници из скупа A, односно*

$$G = \dot{\bigcup_{g \in A}} gH.$$

Доказ. Нека је дата подгрупа H мултипликативне групе G. Посматрајмо релацију $\equiv_H$ коју дефинишемо као

$$a \equiv_H b \iff a^{-1}b \in H \iff aH = bH.$$

Очигледно, ова релација је релација еквиваленције, па се скуп G може представити као дисјунктна унија класа еквиваленције, а чији је скуп представника заправо подскуп A скупа G.

■

Теорема 7.1 *(Лагранж) Нека је H подгрупа коначне групе G. Онда је ред групе H дјелитељ реда групе G, односно*

$$|G| = n|H|$$

за неко $n \in \mathbb{N}$. За број n кажемо да је ***индекс*** *подгрупе H у групи G.*

Доказ. Ако је $H = \{e\}$ или $H = G$ онда је тврђење тривијално тачно.

Претпоставимо да $1 < |H| < |G|$. Нека је $t_1 \in G \setminus H$. Онда је, на основу Леме 7.14, $|t_1H| = |H|$ и $t_1H \cap H = \emptyset$. Уколико је

$$H \cup t_1H = G$$

онда је доказ завршен. У супротном, нека је $t_2 \in G \setminus (H \cup t_1H)$. Слично, као у претходном кораку, имамо $|t_2H| = |H|$ и

$$t_2H \cap H = t_2H \cap t_1H = \emptyset.$$

Опет, ако је

$$H \cup t_1H \cup t_2H = G,$$

доказ је завршен, а ако није, онда бирамо $t_3 \in G \setminus (H \cup t_1H \cup t_2H)$. Због коначности групе G, јасно је да се овај поступак мора завршити у коначном броју корака, па

$$H \cup t_1H \cup \cdots \cup t_{n-1}H = G.$$

С обзиорм на то да је

$$|H| = |t_1H| = \cdots |t_{n-1}H|,$$

изводимо закључак да је

$$|G| = |H| + |t_1H| + \cdots + |t_{n-1}H| = n|H|,$$

чиме је тврдња доказана. ■

Примјер 7.30 *Посматрајмо групу цијелих бројева $(\mathbb{Z}, +)$ и њену подгрупу парних цијелих бројева*

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$$

у односу на стандардно сабирање. Није тешко закључити да постоје само два косета у односу на дату подгрупу, односно да је

$$\mathbb{Z} = 2\mathbb{Z} \cup (1 + 2\mathbb{Z}).$$

Лема 7.16 *Нека је G коначна група, а t произвољан елемент различит од јединичног. Онда је $\mathrm{ord}(t)$ коначан и*

$$[t] = \{1, t, \ldots, t^{n-1}\}$$

гдје је $\mathrm{ord}(t) = n$. То значи да је $\mathrm{ord}(t) = |[t]|$.

Доказ. С обзиром на то да је ред групе G коначан, а елементи

$$1, t, t^2, \ldots$$

из групе G, онда је јасно да постоје природни бројеви k и ℓ тако да

$$t^k = t^\ell.$$

Уз претпоставку да је $k > \ell$, а која не умањује општост, онда је

$$t^{k-\ell} = 1,$$

из чега слиједи да је ред елемента t коначан. Нека је $\mathrm{ord}(t) = n$.

Нека је m произвољан цио број. Онда је $m = nq + r$, при чему је $0 \leq r < n$. Зато је

$$t^m = t^{nq+r} = (t^n)^q t^r = t^r.$$

Дакле,

$$[t] = \{1, t, \ldots, t^{n-1}\}.$$

■

Посљедица 7.5 *Нека је G коначна група, а t произвољан елемент различит од јединичног. Онда је $\mathrm{ord}(t)$ коначан и дијели ред групе G.*

Доказ. Како је $\mathrm{ord}(t)$ једнак реду цикличне подгрупе $[t]$, онда на основу Лагранжове теореме 7.1 $\mathrm{ord}(t)$ дијели ред групе G. ■

7.4. Мултипликативна група $\mathcal{I}_n$

Већ смо констатовали да је $\mathbb{Z}_n$, скуп свих остатака по модулу n, Абелова група у односу на операцију модуларног сабирања. Међутим, $\mathbb{Z}_n$ није група у односу на операцију модуларног множења. Наиме, лако се провјерава да у општем случају не постоји инверз за сваки дати елемент.

На примјер, за $n = 10$, не постоји инверз за 4, односно није могуће наћи елемент a из $\mathbb{Z}_{10}$ такав да је

$$4a \equiv 1 \pmod{10}.$$

Међутим, ако посматрамо само оне елементе који су узајамно прости у односу на неки број n, онда се добија та недостајућа "компонента" која нам је фалила у претходном примјеру. Тај скуп се уобичајено у лиетартури означава са $\mathbb{Z}_n^*$, али ћемо ми користити ознаку $\mathcal{I}_n$. Дакле,

$$\mathcal{I}_n = \{[a] \in \mathbb{Z}_n \mid \textbf{нзд}(a, n) = 1\}.$$

Лема 7.17 *Скуп $\mathcal{I}_n$ у односу на операцију множења по модулу n је Абелова група.*

Доказ. Нека су $[a]$ и $[b]$ елементи $\mathcal{I}_n$. Пошто је $\textbf{нзд}(a,n) = \textbf{нзд}(b,n) = 1$, онда је према Леми 4.6 $\textbf{нзд}(ab,n) = 1$. Дакле, $[ab] \in \mathcal{I}_n$, односно $[a] \ast_n [b] \in \mathcal{I}_n$. Како је модуларно множење асоцијативна и комутативна операција, онда је $(\mathcal{I}_n, \ast_n)$ полугрупа.

Нека је $[a] \in \mathcal{I}_n$ произвољан елемент. Како је $\textbf{нзд}(a,n) = 1$, онда према Теореми 4.2 постоје a' и n' такви да је

$$aa' + nn' = 1.$$

То заправо значи да је $aa' \equiv 1 \pmod{n}$. Примјетимо да је $[a'] \in \mathcal{I}_n$. Дакле, $[a']$ је мултипликативни инверз елемента $[a]$ у $\mathcal{I}_n$, односно

$$[a] \ast_n [a'] = [1].$$

Закључујемо да је $\mathcal{I}_n$ Абелова група. ■

Примјер 7.31 *Посматрамо*

$$\mathcal{I}_{20} = \{[1],[3],[7],[9],[11],[13],[17],[19]\}.$$

Ред ове групе је 8. Рачунамо ред појединих елемената. Пошто је $3^4 \equiv 1 \pmod{20}$, *онда је и* $[3]^4 = 1$ *у групи* $\mathcal{I}_{20}$. *Дакле,* $\mathrm{ord}([3]) = 4$.

На основу дефиниције скупа $\mathcal{I}_n$ имамо

$$\mathcal{I}_p = \{[1],\ldots,[p-1]\},$$

док на основу Леме 7.17 слиједи да је $(\mathcal{I}_p, \ast_p)$ Абелова група.

Посљедица 7.6 *Ако је p прост број, онда је $\mathcal{I}_p = \{[1],\ldots,[p-1]\}$, па је по претходној леми $(\mathcal{I}_p, \ast_p)$ Абелова група.*

7.5. Прстени и поља

Видјели смо да је скуп цијелих бројева $\mathbb{Z}$ у односу на сабирање Абелова група, док је у односу на множење полугрупа. Сем тога, знамо да је операција множења *дистрибутивна* у односу на сабирање, односно вриједи

$$(a+b)c = ac + bc, \;\; a(b+c) = ab + ac \tag{7.1}$$

за свако a, b, c из $\mathbb{Z}$. Слично, можемо да посматрамо и скуп рационалних, реалних или комплексних бројева.

Дефиниција 7.16 *Нека је R непразан скуп, а $+$ и $\cdot$ операције на њему. Ако је*

1. *$(R,+)$ Абелова група*
2. *$(R,\cdot)$ је полугрупа*
3. *Операција $\cdot$ је дистрибутивна у односу на $+$, односно вриједи 7.1 за свако a, b, c из R,*

*онда се уређена тројка $(R,+,\cdot)$ назива **прстен**. Уколико је операција $\cdot$ комутативна, онда кажемо да је прстен $(R,+,\cdot)$ **комутативан**. Ако је $(R,\cdot)$ моноид, односно ако постоји јединични елемент у односу на операцију $\cdot$, онда кажемо да је то јединични елемент прстена или да је $(R,+,\cdot)$ **прстен са јединицом**.*

Примјер 7.32 *Уређена тројка $(\mathbb{Z}_m, \boldsymbol{+}_m, \boldsymbol{*}_m)$ је прстен. Наиме, позивајући се на Лему 7.3, знамо да је $(\mathbb{Z}_m, \boldsymbol{+}_m)$ Абелова група, док је $(\mathbb{Z}_m, \boldsymbol{*}_m)$ комутативни моноид. Пошто је*

$$a(b+c) \equiv ab+ac \pmod{m}, \ (a+b)c \equiv ac+bc \pmod{m}$$

за свако a, b, c из $\mathbb{Z}$, то је онда

$$[a] \boldsymbol{*}_m ([b] \boldsymbol{+}_m [c]) = [a] \boldsymbol{*}_m [b] \boldsymbol{+}_m [a] \boldsymbol{*}_m [c],$$

$$([a] \boldsymbol{+}_m [b]) \boldsymbol{*}_m [c] = [a] \boldsymbol{*}_m [c] \boldsymbol{+}_m [b] \boldsymbol{*}_m [c].$$

Заправо, ово је комутативни прстен са јединицом.

Дефиниција 7.17 *Нека је$(R,+,\cdot)$ прстен и 0 неутрални елемент у односу на операцију сабирања. Уколико је $(R\setminus\{0\},\cdot)$ Абелова група, онда уређену тројку $(R,+,\cdot)$ називамо **поље**.*

Лема 7.18 *Нека је p прост број. Онда је $(\mathbb{Z}_p, \boldsymbol{+}_p, \boldsymbol{*}_p)$ поље.*

Доказ. На основу Примјера 7.32, имамо да је $(\mathbb{Z}_p, \boldsymbol{+}_p, \boldsymbol{*}_p)$ прстен. Како је према Леми 7.17 скуп $\mathcal{I}_p = \{1,\ldots,p-1\}$ у односу на операцију модуларног множења $\boldsymbol{*}_p$ Абелова група, онда је јасно да је $(\mathbb{Z}_p, \boldsymbol{+}_p, \boldsymbol{*}_p)$ поље. ■

8 Прости бројеви

Вјероватно не постоји у историји математике појам који је привлачио више пажње како лаичке, тако и стручне математичке јавности од простих бројева.

Дефиниција 8.1 *Природан број $p > 1$ је* ***прост*** *ако нема других дјелитеља сем 1 и себе. Ако природан број $m > 1$ није прост, онда је* ***сложен****.*

Примјер 8.1 *Одредити прост број p ако се зна да су $p+10$ и $p+14$ прости бројеви.*

Рјешење. За $p = 3$ су $p+10$ и $p+14$ прости бројеви. Ако је $p \geq 3$ прост број, онда је он или облика $3k+1$ или облика $3k+2$, за неко $k \in \mathbb{N}$. У првом случају је $p+14 = 3(k+5)$, а у другом је $p + 10 = 3(k + 4)$ сложен број. Дакле, једини такав p је број 3. ■

Лема 8.1 *Најмањи дјелилац већи од јединице, произвољног цијелог броја је прост број.*

Доказ. Нека је n цио број и нека је q његов најмањи дјелилац који је већи од 1. Ако би q био сложен, онда би постојао неки дјелилац p за који важи $1 < p < q$. Но, тада би p дјелилац и броја n, па q не би био најмањи међу дјелиоцима броја n који су већи од 1. ■

Теорема 8.1 *(**Еуклид**) Постоји бесконачно много простих бројева. Другим ријечима, од сваког простог броја постоји већи прост број.*

Доказ. Претпоставимо да тврђење није истинито, односно да постоји коначан скуп простих бројева $p_1, p_2, \ldots, p_k$, а да су сви остали природни бројеви већи од 1 сложени. Број

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

је према томе сложен. На основу претходне леме, слиједи да је најмањи дјелилац, већи од 1, неки прост број. Међутим, то није могуће, јер N приликом дијељења са било којим простим бројем из листе $p_1, p_2, \ldots, p_k$ даје остатак 1. То значи да скуп простих бројева мора бити бесконачан. ■

Примјер 8.2 *Користећи идеју из Еуклидове теореме, показати да ако су $q_1, q_2, \ldots, q_n$ прости бројеви, онда постоји прост број $q \notin \{q_1, \ldots, q_n\}$. Наравно, узевши у обзир саму тврдњу Еуклидове теореме, доказ ове чињенице је тривијалан.*

Користећи идеју у доказу наведене теореме, нека је $N = q_1 \cdots q_n + 1$. На основу Леме 8.1, постоји прост број q такав да $q \mid N$. Сад се једноставно показује да $q \notin \{q_1, \ldots, q_n\}$.

Теорема 8.2 *Сваки природан број $n > 1$ може се приказати (представити) као производ простих бројева. Овај приказ је јединствен, односно два представљања се могу разликовати само у поретку чинилаца.*

Примјетимо да претходна теорема обезбјеђује да се сваки природан број n може приказати у облику

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

гдје су $p_1, \ldots, p_r$ различити бројеви, а $\alpha_1, \ldots, \alpha_r$ природни бројеви. Овај приказ називамо **канонским растављањем** или **канонском факторизацијом** природног броја на просте чиниоце.

Лема 8.2 *Ако је p_n прост број који је $n-$ти по реду у низу простих бројева, онда је $p_n \leq 2^{2^{n-1}}$ за свако $n \geq 1$.*

Доказ. Доказ изводимо индукцијом по n. Резултат очигледно слиједи за $p_1 = 2^{2^0}$.

Претпоставимо да тврђење вриједи за $n = 1, 2, \ldots, k$. Као и у доказу Теореме 8.1, број $p_1 p_2 \cdots p_k + 1$ мора бити дјељив са неким простим бројем p, при чему тај прости број не може бити неки од $p_1, p_2, \ldots, p_k$, јер би онда тај прости број дијелио 1, што је немогуће. Дакле, тај прости број p мора бити већи или једнак од p_{k+1}, па

$$p_{k+1} \leq p \leq p_1 p_2 \cdots p_k + 1 \leq 2^{2^0} 2^{2^1} \cdots 2^{2^{k-1}} + 1 = 2^{2^k - 1} + 1.$$

На другој страни,

$$2^{2^k - 1} + 1 = \frac{1}{2} 2^{2^k} + 1 \leq 2^{2^k}.$$

Овдје смо користили индуктивну претпоставку да је $p_i \leq 2^{2^i}$ за $i \leq k$, као и формулу за суму k чланова геометријске прогресије. ■

Напоменимо да је ова процјена, иако тачна, веома слаба у смислу прецизности. На примјер, $p_4 = 7$, а $2^{2^3} = 256$.

Лема 8.3 *Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$. Општије, ако $p \mid a_1 a_2 \cdots a_n$, онда p дијели бар један чинилац a_i.*

Доказ. Претпоставимо да p не дијели a. Онда су p и a узајамно прости бројеви. У том случају, на основу Леме 4.7, слиједи да $p \mid b$. Општији случај се по истом принципу доказује индукцијом. ■

Примјер 8.3 *Доказати да ако је n непаран број, онда је n^2-1 дјељив са 8, а ако је n прост број већи од 3, онда је n^2-1 дјељив са 24.*

Рјешење. Пошто је $n^2-1=(n-1)(n+1)$ производ два узастопна парна броја, онда је бар један од њих дјељив са 4, па је производ дјељив са 8. Уколико је n прост број већи од 3, онда n није дјељив са 3, али зато неки од његових сусједа, $n-1$ или $n+1$ мора бити. Стога је производ дјељив са 8 и 3, односно са 24. ■

Примјер 8.4 *Доказати да*

$$M=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

не може бити цијели број.

Рјешење. Нека је k највећи цио број за који је $2^k\leq n$ и P производ свих непарних бројева који нису већи од n. Претпоставимо, супротно тврђењу, да је број M цио. Онда је и $2^{k-1}PM$ цијели број. Међутим, тада имамо да су у изразу

$$2^{k-1}PM=2^{k-1}P(\frac{1}{2}+\frac{1}{3}+\ldots\frac{1}{2^k}+\ldots+\frac{1}{n})$$

сви сабирци цијели бројеви изузев $2^{k-1}P\dfrac{1}{2^k}=\dfrac{P}{2}$. Контрадикција. ■

Теорема 8.3 *Ако је производ два релативно проста природна броја квадрат цијелог броја*

$$ab=c^2,\ \textbf{нзд}(a,b)=1,$$

онда су a и b такође квадрати неких цијелих бројева.

Доказ. Да би број био квадрат неопходно је и довољно да су му сви експоненти у факторизацији парни. Како су бројеви a и b узајамно прости, сваки прост дјелилац броја c^2 се јавља или у факторизацији броја a или b, али не у оба. Из тог разлога, експоненти простих бројева који у учествују у факторизацији бројева a и b морају бити парни. ■

Примјер 8.5 *Одредити све просте бројеве p и q за које је*

$$p^2-2q^2=1.$$

Рјешење. Дата једначина се може написати у облику

$$(p-1)(p+1)=2q^2.$$

Очигледно, за $p=2$ она нема рјешења. Ако је p прост и $p>2$, онда $(p-1)(p+1)$ мора бити дјељиво са 8, па је q^2 дјељиво са 4, па q није прост, изузев ако је $q=2$. Но, у том

случају, $p = 3$. Дакле, једино рјешење је $p = 3$ и $q = 2$. ■

Интересантно је, коришћењем факторизације цијелих бројева на просте факторе, опет размотрити највећи заједнички дјелилац и најмањи садржалац. Наиме, лако се закључује да

$$\textbf{нзд}(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))},$$
$$\textbf{нзс}(a, b) = \prod_p p^{\max(\alpha(p),\beta(p))}.$$

Овај облик представљања и чињеница да за произвољне природне бројеве α и β вриједи

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta,$$

доказује на још један начин Теорему 4.4, односно да је

$$\textbf{нзд}(a, b)\,\textbf{нзс}(a, b) = |ab|,$$

за ненулте цијеле бројеве a и b.

Примјер 8.6 *Доказати да сваки сложен број n има прост чинилац $p \leq \sqrt{n}$.*

Доказ. Нека је p најмањи прост број који дијели n. Слиједи да је

$$n = pm, \text{ при чему је } p \leq m.$$

Дакле, $n \geq p^2$, што значи да $p \leq \sqrt{n}$. ■

Примјер 8.7 *Нека су $p_1 = 2, p_2 = 3, p_3 = 5, \ldots,$ а у општем случају, p_i представља i-ти прост број. Доказати или оповргнути да је*

$$p_1 p_2 \cdots p_n + 1$$

прост за све $n \geq 1$.

[Упуство: Ако је $n = 1$ онда је $2+1 = 3$ прост. Ако је $n = 2$ слиједи да је $2 \cdot 3 + 1 = 7$ прост. Ако је $n = 3$, такође је $2 \cdot 3 \cdot 5 + 1 = 31$ прост. Пробати још неке вриједности за n. Користити Примјер 8.6.]

Примјер 8.8 *Доказати да простих бројева облика $4k + 3$ има бесконачно много.*

Рјешење. Сви непарни прости бројеви су облика $4r + 1$ или $4k + 3$. Лако се уочава да се множењем два броја облика $4r + 1$ добија број истог облика.

Претпоставимо да су $\{p_1, p_2, \ldots, p_n\}$ сви прости бројеви облика $4k+3$. Посматрајмо број

$$4p_1 p_2 \cdots p_n - 1.$$

Овај број није облика $4r+1$, што значи да има бар један прост фактор облика $4k+3$. Наиме, ако би сви његови чиниоци били облика $4k+1$, онда би и производ био тог облика.

Дакле, један његов прост фактор облика $4k+3$ мора бити из скупа $\{p_1, p_2, \ldots, p_n\}$, а одатле слиједи да тај прост број дијели 1, што је немогуће. Закључујемо да је претпоставка да имамо коначно много простих бројева облика $4k+3$ је погрешна. ■

Примјер 8.9 *Доказати да за сваки природан број n постоји n узастопних сложених бројева.*

Рјешење. Посматрајмо бројеве

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n,\ (n+1)!+n+1.$$

Сваки од датих бројева облика $(n+1)!+j$, гдје је $2 \leq j \leq n+1$ је сложен, јер се фактор j може извући као уаједнички за два сабирка. ■

Примјер 8.10 *Доказати да не постоји полином $f(x)$ са цјелобројним коефицијентима степена $m \geq 1$, такав да је $f(n)$ прост за све $n \in \mathbb{N}$.*

Рјешење. Нека је $f(1) = p$. Тада је p прост број. Како увијек $x - y$ дијели $x^m - y^m$, онда је $f(1+kp) - f(1)$ дјељиво са $(1+kp) - 1 = kp$. Одавдје слиједи да $p \mid f(1+kp)$ за сваки $k \in \mathbb{N}$. Међутим, $f(1+kp)$ је прост, па мора бити $f(1+kp) = p$ за свако $k \in \mathbb{N}$. Значи, полином $f(x) - p$ има бесконачно много нула, одакле закључујемо да је $f(x) = p$, а што је у супротности са претпоставком да је степен полинома $f(x)$ већи од један. ■

Примјер 8.11 *Нека је број 2^n+1 прост. Доказати да је тада $n = 0$ или $n = 2^k$ за неки $k \geq 0$.*

Рјешење. Претпоставимо супротно, да је $n = 2^k m$, гдје је m непаран број већи од 1. Тада је

$$2^n + 1 = \left(2^{2^k}\right)^m + 1,$$

па $2^{2^k}+1 \mid 2^n+1$, јер $x+y \mid x^m+y^m$ за непарно m. Дакле, ако је $m > 1$, број 2^n+1 има нетривијални фактор, па није прост. Из тога слиједи тврђење. ■

Бројеви облика $2^{2^n}+1$ називају се **Фермаови бројеви**. Иако је Ферма сматрао да су сви бројеви тог облика прости, постоје и сложени Фермаови бројеви. На примјер, број $2^{32}+1$ је сложен.

Примјер 8.12 *Нека је број $2^m - 1$ прост. Доказати да је тада m прост број.*

Рјешење. Ако би било $n = n_1 n_2$, $1 < n_1, n_2 < n$, број $2^n - 1 = (2^{n_1})^{n_2} - 1$ би био дјељив са $2^{n_1} - 1$. ■

Бројеви облика $M_p = 2^p - 1$, за прост број p, називају се **Мерсенови бројеви**. Неки Мерсенови бројеви су прости као на примјер $M_7 = 127$, а неки сложени, као на примјер $M_{11} = 2047 = 23 \cdot 89$. Хипотеза је да има бесконачно много простих Мерсенових бројева.

Лема 8.4 *Нека су $a_1, a_2, \ldots, a_r$ у паровима релативно прости природни бројеви, а производ $a_1 a_2 \cdots a_r = b^m$ за неке природне бројеве b и m. Онда је сваки a_i, за $i = 1, 2, \ldots, r$ такође $m-$ти степен неког природног броја.*

Доказ. Претпоставимо да је

$$b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Онда је

$$b^m = p_1^{me_1} p_2^{me_2} \cdots p_k^{me_k}.$$

Пошто су сви бројеви a_i који учествују у факторизацији b^m узајамно прости, то значи да се у факторизацији неког a_i или појављује степен простог броја у "пуном" обиму, на примјер $p_j^{me_j}$ или се уопште не појављује. Другим ријечима, не може се десити да дио $p_j^{me_j}$ учествује у факторизацији једног, а дио у факторизацији неког другог a_i, јер би то нарушило претпоставку да су они у паровима узајамно прости. Дакле, сви степени простих бројева у факторизацији произвољног a_i су дјељиви са m, па су и сами $m-$ти степени неког природног броја. ■

Посљедица 8.1 *Ако је m природан број који није потпун квадрат, онда је $\sqrt{m}$ ирационалан.*

Доказ. Претпоставимо да је $\sqrt{m}$ рационалан, односно $\sqrt{m} = \dfrac{a}{b}$, гдје су a и b природни бројеви. Слиједи да је

$$m = \frac{a^2}{b^2}.$$

Нека су дате факторизације бројева

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ и } b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Примјетимо да су $e_i - f_i \geq 0$ за свако i, те да је

$$m = \left(p_1^{e_1 - f_1} p_2^{e_2 - f_2} \cdots p_k^{e_k - f_k}\right)^2,$$

што значи да је m потпун квадрат. ■

8.1. Теорема о дистрибуцији простих бројева

Једно важно питање које се тиче простих бројева је процјена колико их има у неком интервалу, односно колико има простих бројева који су мањи од неког задатог природног броја n?

Дефинишимо функцију $\pi(n)$ као број простих бројева који су мањи или једнаки n

$$\pi(n) = |\{p \in \mathbf{P} \mid p \leq n\}|.$$

У следећој табели су дате неколико првих вриједности функције $\pi(n)$. Примјетимо да је функција монотоно растућа

n	2	3	4	5	6	7	8	9	10	11	...
$\pi(n)$	1	2	2	3	3	4	4	4	4	5	...

У криптографији, врло често се користе веома велики прости бројеви. Иако је показано да простих бројева има бесконачно много, један од проблема је и како наћи довољно велики прости број. Овај проблем је везан за питање дистрибуције простих бројева. На примјер, колико је вјероватно да дати интервал садржи прост број? Следећа теорема, коју дајемо без доказа, даје одговор на претходно питање. Наиме, каже да је могуће наћи прост број задате величине, а и да то, с обзиром на густину простих бројева $\mathbf{P}$ унутар скупа природних бројева, није тешко.

Теорема 8.4

$$\lim_{n\to\infty} \frac{\pi(n)\ln(n)}{n} = 1$$

Дакле, претходна теорема даје прилично тачну апроксимацију о броју простих бројва мањих или једнаких n

$$\pi(n) \approx \frac{n}{\ln(n)},$$

што значи да је број простих бројева у интервалу (n_1, n_2) приближно $\pi(n_2) - \pi(n_1)$, односно

$$\frac{n_2}{\ln(n_2)} - \frac{n_1}{\ln(n_1)}.$$

Многи велики проблеми у историји математике су везани за просте бројеве. Још увијек постоји много отворених проблема из ове области, а ми ћемо навести неке. На примјер, претпоставља се да постоји бесконачно много *простих близанаца*, односно парова простих бројева p и $p+2$. Такође, чувена *Голдбахова хипотеза* каже да је сваки паран број могуће представити као збор два проста броја.

Примјер 8.13 *Доказати да је изложилац са којим дати прост број p фигурише у канонској факторизацији броја $n!$ једнак*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Рјешење. Ако је $p > n$, онда је наведена сума једнака нули, што се поклапа са чињеницом да у том случају p не учествује у факторизацији броја n.

За $p \leq n$ видимо да имамо

$$\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor$$

бројева који су мањи или једнаки од n, а дјељиви су са p, дочим нису са p^2. Слично, закључујемо да је

$$\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor$$

бројева који су мањи или једнаки од n, дјељивих са p^2, али не са p^3.

На тај начин, долазимо до закључка да је изложилац простог фактора p у факторизацији $n!$ једнак

$$\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor + 2\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + 3\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) \cdots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

■

Примјер 8.14 *Доказати да је $n^4 + 4$ сложен ако је $n \in \mathbb{N}$, $n > 1$. (Овај задатак је познат као задатак Софије Жермен)*

Рјешење. Пошто је

$$n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$$

и оба фактора на десној страни су већа од 1 за $n > 1$, тиме је тврђење доказано. ■

Примјер 8.15 *Ако су p и $8p^2 + 1$ прости бројеви, доказати да је и $8p^2 + 2p + 1$ прост број.*

Рјешење. Очигледно, тврђење вриједи за $p = 3$. Сви остали прости бројеви, већи од 3, су облика $3k - 1$, односно $3k + 1$. У случају да је p облика $3k - 1$ или $3k + 1$ видимо да је $8p^2 + 1$ дјељив са 3. Тиме је показано да је за $p > 3$, број $8p^2 + 1 > 3$ и дјељив са 3, што значи да није прост. Дакле, једина могућност је $p = 3$. ■

Примјер 8.16 *Ако је p прост број већи од 2, доказати да је бројилац сведеног разломка једнаког збиру*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

дјељив са p.

Рјешење. Бројилац датог збира је

$$\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\frac{(p-1)!}{3}+\cdots+\frac{(p-1)!}{p-2}+\frac{(p-1)!}{p-1}.$$

У претходном збиру имамо паран број сабирака, па можемо сабирати у паровима: први и последњи, други и претпоследњи... На овај начин добијамо збирове облика

$$\frac{(p-1)!}{k}+\frac{(p-1)!}{p-k}=\frac{p(p-1)!}{k(p-k)},\ \text{за } k<p.$$

Јасно је да је на десној страни претходне једнакости цијели број, представљен у облику разломка у чијем бројиоцу је и фактор p. Пошто су k и $p-k$ строго мањи од простог броја p, то значи да се прости број p не може скратити ни са чим из имениоца $k(p-k)$. То значи да је

$$\frac{p(p-1)!}{k(p-k)},\ \text{за } k<p,$$

цијели број дјељив са p. Тиме је доказано да је и посматрани збир дјељив са p. ■

Примјер 8.17 *Нека је n природан број и p прост број такав да $n \mid (p-1)$ и $p \mid (n^6-1)$. Доказати да је бар један од бројева $p-n$ и $p+n$ потпун квадрат.*

Рјешење. Како је $n \mid (p-1)$, слиједи да је $p=1+an$ за неки природан број a. Из услова

$$p \mid (n^6-1)=(n^3-1)(n^3+1)=(n-1)(n^2+n+1)(n+1)(n^2-n+1)$$

слиједи да $p \mid (n-1)$, $p \mid (n+1)$, $p \mid (n^2+n+1)$ или $p \mid (n^2-n+1)$.

Разматрамо сваки до ових услова посебно.

Ако $p \mid (n-1)$, онда је $n-1 \geq p=1+na \geq n+1$, а ово је немогуће.

Ако $p \mid (n+1)$, онда је $n+1 \geq p=1+na$, па онда слиједи да је $a=1$, одакле слиједи да је $p-n=1$ потпун квадрат.

Ако $p \mid (n^2+n+1)$ имамо да је $n^2+n+1=pb$ за неки природан број b. Замјеном $p=1+na$ добијамо $n^2+n+1=nab+b$, односно $n(n-ab+1)=b-1$. Одавде слиједи да је $n \mid b-1$ и $b=1+nc$ за неки ненегативан цио број c. Вратимо се још једном на израз $n^2+n+1=nab+b$ и уврстимо добијене изразе

$$n^2+n+1=na(nc+1)+(nc+1)=n^2ac+n(a+c)+1,$$

одакле даље слиједи

$$n+1=acn+a+c.$$

Ако је $ac \geq 1$ тада је $a+c \geq 2$ и последња једнакост није могућа. Дакле, $ac=0$, одакле

из услова да је a природан број, слиједи да је $c = 0$, па је $a = n + 1$. Стога је

$$p + n = (1 + na) + n = 1 + n(n + 1) + n = n^2 + 2n + 1 = (n + 1)^2.$$

Следећи случај тече скоро идентично као претходни.

Ако $p \mid (n^2 - n + 1)$ имамо да је $n^2 - n + 1 = pb$ за неки природан број b. Замјеном $p = 1 + na$ добијамо $n^2 - n + 1 = nab + b$, односно $n(n - ab - 1) = b - 1$. Одавде слиједи да је $n \mid b - 1$ и $b = 1 + nc$ за неки ненегативан цио број c. Вратимо се још једном на израз $n^2 - n + 1 = nab + b$ и уврстимо добијене изразе

$$n^2 + n + 1 = na(nc + 1) + (nc + 1) = n^2ac + n(a + c) + 1,$$

одакле даље слиједи

$$n - 1 = acn + a + c.$$

Ако је $ac \geq 1$ тада је $a + c \geq 2$ и последња једнакост није могућа. Дакле, $ac = 0$, одакле из услова да је a природан број, слиједи да је $c = 0$, па је $a = n - 1$. Стога је

$$p - n = (1 + na) - n = 1 + n(n - 1) - n = n^2 - 2n + 1 = (n - 1)^2,$$

чиме је тврђење у потпуности доказано. ■

1. Доказати да бројеви $2^n - 1$ и $2^n + 1$, за $n > 2$, не могу бити истовремено прости.
2. Одредити све природне бројеве $n > 1$ за које је број $\dfrac{n(n+1)}{2} - 1$ прост.
3. Ако је p прост број, онда из $p \mid a^k$ слиједи $p \mid a$, а одатле $p^k \mid a^k$. Да ли вриједи исти закључак уколико је p сложен број?
4. Ако је $n^4 + 4^n$ прост број за $n \in \mathbb{N}$, онда је $n = 1$.
5. Ако је p прост број, а a, b природни бројеви, испитати који је од следећих исказа тачан.
   а. Ако је **нзд**$(a, p^2) = p$ онда **нзд**$(a^2, p^2) = p^2$.
   б. Ако је **нзд**$(a, p^2) = p$ и **нзд**$(b, p^2) = p^2$ онда **нзд**$(ab, p^4) = p^3$.
   в. Ако је **нзд**$(a, p^2) = p$ и **нзд**$(b, p^2) = p$ онда **нзд**$(ab, p^4) = p^2$.
   г. Ако је **нзд**$(a, p^2) = p$ онда **нзд**$(a + p, p^2) = p$.

   За сваки од исказа дати доказ или контрапримјер.
6. Наћи све просте бројеве p за које вриједи да је $p + 2$ такође прост.
7. Нека су n и q природни бројеви. Доказати да је број умножака броја q у скупу $1, 2, \ldots, n$ једнак $\lfloor n/q \rfloor$. На основу овог показати да вриједи да ако је p прост број и e највећи природан број такав да $p^e \mid n!$, онда је

$$e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots .$$

8. Доказати да је за цијеле бројеве a, b и природан број n

$$\textbf{нзд}(a^n, b^n) = \textbf{нзд}(a, b)^n \text{ за } n \geq 1.$$

9. Нека је n природан број већи од 2. Доказати да постоји прост број p за који важи $n < p < n!$.
10. Претпоставимо да су p и $p+2$ прости бројеви и $p > 3$. Доказати да је њихов збир $2p+2$ дјељив са 12.

9 Прстен остатака модуло n

9.1. Ојлерова функција. Фермаова и Ојлерова теорема

Дефиниција 9.1 *Редуковани скуп остатака модуло m је скуп*

$$R_m = \{a \in \mathbb{Z}_m | \ \textbf{нзд}(a, m) = 1\}.$$

Функција $\phi : \mathbb{N} \to \mathbb{N}$ дефинисана као

$$\phi(m) = \begin{cases} 1 & \text{ако је } m = 1 \\ |R_m| & \text{ако је } m > 1 \end{cases}$$

се зове ***Ојлерова функција***.

Примјер 9.1 *За модуло* 12*, редуковани скуп остатака је* $\{1, 5, 7, 11\}$.

Посматрајмо R_m, скуп редукованих остатака модуло m, у односу на операцију множења по модулу m. Уочавамо неколико карактеристика

- Производ два елемента из R_m је елемент из R_m.
- Множење по модулу m је асоцијативно.
- У R_m се обавезно налази *јединица*, односно елемент a, такав да $a \equiv 1 \pmod{m}$ и тиме $ar \equiv r \pmod{m}$ за свако $r \in R_m$.
- Како једначина $ax \equiv 1 \pmod{m}$ има јединствено рјешење за свако $a \in R_m$, а које се такође налази у R_m, закључујемо да сваки елемент из R_m има *инверзни* елемент у R_m.

Очигледно, претходна четири својства нам говоре да је R_m у односу на операцију множења по модулу m група.

Лема 9.1 *Редуковани скуп остатака R_m, у односу на операцију модуларног множења по модулу m је Абелова група.*

Ово запажање ће нам помоћи приликом разумијевања наведених резултата, који се могу посматрати из два угла: Теорије бројева и Алгебре. У наведеним доказима ћемо се углавном ослањати на Теорију бројева, мада се лако и природно изводе докази алгебарским методама.

Примјер 9.2 *Нека је m природан број. Подсјетимо се једног корисног тврђења:*

Ако је G коначна мултипликативна група чији је ред n, онда за свако $a \in G$ вриједи

$$a^n = 1.$$

У конкретном случају, групе R_m, са множењем по модулу m вриједи

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

Чињеница из претходног примјера, позната под називом Ојлерова теорема, може се доказати без помоћи теорије група.

Теорема 9.1 *(Ојлерова теорема) Ако је $(a, m) = 1$, онда је*

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

Доказ. Нека је

$$\{r_1, r_2, \ldots, r_{\phi(m)}\}$$

један редуковани скуп остатака по модулу m. Из Теореме 6.1 слиједи да је и

$$\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$$

такође редуковани скуп остатака по модулу m. Зато, имамо

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m},$$

односно

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} (r_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

Како је **нзд**$(r_i, m) \equiv 1 \pmod{m}$ за свако i, онда је и

$$\prod_{i=1}^{\phi(m)} r_i \pmod{m} \equiv 1 \pmod{m}.$$

Зато, према Теореми 6.4 имамо да је

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

■

Примјетимо да је претходна теорема само парафраза познатог тврђења из теорије група:

Ако је G коначна група реда n, онда ред сваког елемента из G дијели ред групе, односно

$$a^n = 1,\ a \in G.$$

Посљедица 9.1 *(Мала Фермаова теорема) Нека је p прост број. Ако $p \nmid a$ онда је $a^{p-1} \equiv 1 \pmod{p}$. За сваки цијели број a вриједи*

$$a^p \equiv a \pmod{p}.$$

Доказ. Како је $\phi(p) = p - 1$, онда према Теореми 9.1 директно слиједи тврђење. ■

Примјер 9.3 *Показаћемо да је $a^{25} - a$ дјељив са 30 за сваки цијели број a. То ћемо показати тако што ћемо потврдити дјељивост датог израза са 5, 3 и 2. Најприје, имамо на основу Теореме 9.1 да је $a^5 \equiv a \pmod{5}$, па је*

$$a^{25} \equiv (a^5)^5 \equiv a^5 \equiv a \pmod{5},$$

одакле је $5 \mid a^{25} - a$. Слично, из $a^3 \equiv a \pmod{3}$ имамо

$$a^{25} \equiv (a^3)^8 a \equiv a^8 a \equiv a^9 \equiv (a^3)^3 \equiv a^3 \equiv a \pmod{3}.$$

Закључујемо да је $3 \mid a^{25} - a$. На крају, из $a^2 \equiv a \pmod{2}$, слиједи

$$a^{25} \equiv (a^2)^{12} a \equiv a^{12} a \equiv \ldots \equiv a^3 a \equiv (a^2)^2 \equiv a^2 \equiv a \pmod{2},$$

што повлачи $2 \mid a^{25} - a$. Како је израз $a^{25} - a$ дјељив са 2, 3 и 5, онда је дјељив са 30 за сваки цијели број a.

Примјер 9.4 *Одредити двије последње цифре у децималном запису броја 3^{400}.*

Будући да је $\phi(25) = 20$, онда је $3^{20} \equiv 1 \pmod{25}$, што значи да је $3^{400} \equiv 1 \pmod{25}$.

Слично, имамо да је $3^2 \equiv 1 \pmod{4}$, па је $3^{400} \equiv 1 \pmod{4}$. Како су бројеви 25 и 4 узајамно прости, онда слиједи да је $3^{400} \equiv 1 \pmod{100}$, а исти закључак слиједи из Кинеске теореме о остацима. Дакле, последње двије цифре су 01.

Дефиниција 9.2 *Функцију* $\psi : \mathbb{N} \to \mathbb{C}$ *за коју вриједи*

1. $\psi(1) = 1$,

2. $\psi(mn) = \psi(m)\psi(n)$ *за све* m, n *такве да је* $(m, n) = 1$,

зовемо мултипликативна функција.

Теорема 9.2 *Ојлерова функција* ϕ *је мултипликативна.*

Доказ. Нека су m и n релативно прости бројеви, а R_m и R_n редуковани скупови остатака по модулу m и n, респективно. Посматрајмо скуп

$$nR_m + mR_n = \{na + mb \mid a \in R_m, b \in R_n\},$$

при чему су операције сабирања и множења по модулу mn. Доказујемо да је

$$|nR_m + mR_n| = \phi(m)\phi(n),$$

те да вриједи

$$nR_m + mR_n = R_{mn}.$$

Из претходног ће слиједити да је

$$\phi(mn) = \phi(m)\phi(n).$$

На почетку, уочимо да је свако $na + mb \in nR_m + mR_n$ релативно просто са m и са n, за $a \in R_m$ и $b \in R_n$. Стога, $na + mb$ је релативно просто и са mn.

Нека је c цијели број такав да **нзд**$(c, mn) = 1$. Доказујемо да је

$$c \equiv na + mb \pmod{mn}, \text{ за неке } a, b.$$

Како је **нзд**$(m, n) = 1$, онда постоје цијели бројеви x, y такви да

$$mx + ny = 1, \text{ а одавде је } m(cx) + n(cy) = c.$$

Пошто је **нзд**$(x, n) =$ **нзд**$(y, m) = 1$, онда је и

$$\textbf{нзд}(cx, n) = \textbf{нзд}(cy, m) = 1.$$

Закључујемо да за бројеве

$$a \equiv cy \pmod{m} \text{ и } b \equiv cx \pmod{n}$$

вриједи $c \equiv na + mb \pmod{mn}$, а **нзд**$(a, m) = 1$ и **нзд**$(b, n) = 1$.

Овим је доказано да

$$R_{mn} = nR_m + mR_n,$$

што повлачи да је

$$|R_{mn}| = \phi(mn) = |nR_m + mR_n|.$$

Покажимо да је $|nR_m + mR_n| = \phi(m)\phi(n)$.

Свака два елемента из $nR_m + mR_n$ су међусобно неконгруентна по модулу mn. Заиста, из

$$na + mb \equiv na' + mb' \pmod{mn}$$

слиједи да је

$$(a - a')n \equiv (b - b')m \pmod{mn}.$$

Из претходног је јасно да

$$m \mid a - a', \text{ као и } n \mid b - b',$$

па је $a \equiv a' \pmod{m}$ и $b \equiv b' \pmod{n}$, што значи да је

$$|nR_m + mR_n| = \phi(m)\phi(n), \text{ па је } \phi(mn) = \phi(m)\phi(n).$$

■

Лема 9.2 *За сваки природан број $n > 1$ вриједи*

$$\phi(n) = n\prod_{p|n}(1 - \frac{1}{p}).$$

Доказ. Посматрајмо најприје бројеве облика p^k, гдје је p прост, а k природан број. Једини природни бројеви мањи од p^k који нису релативно прости са њим су

$$p, 2p, \ldots, p^{k-1}p,$$

што значи да је $\phi(p^k) = p^k - p^{k-1}$. Нека је сада n произвољан природан број. Према теореми о јединственој факторизацији на просте чиниоце, имамо да

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Због мултипликативности Ојлерове функције, слиједи

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}),$$

односно

$$\phi(n) = \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)\prod_{i=1}^{k}(1 - \frac{1}{p_i}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}) = n\prod_{p|n}(1 - \frac{1}{p}).$$

■

Претходно дата посљедица крије у себи и вјероватносну интерпретацију. Наиме, ако је a цијели број изабран на случајан начин, онда је вјероватноћа да је узајамно прост са неким простим бројем p једнака

$$\frac{p-1}{p} = 1 - \frac{1}{p}.$$

Да би a био узајамно прост са неким датим бројем n, потребно је и довољно да буде узајамно прост са сваким простим дјелиоцем тог броја. Пошто догађаји који се односе на дјељивост у односу на различите просте бројеве независни, онда је вјероватноћа да би a био узајамно прост са n

$$\prod_{p|n}(1 - \frac{1}{p}).$$

Са друге стране, ова вјероватноћа, изражена у терминима Ојлерове функције је једнака $\frac{\phi(n)}{n}$, из чега слиједи да је

$$\frac{\phi(n)}{n} = \prod_{p|n}(1 - \frac{1}{p}).$$

Уколико је $n > 1$, онда је $0 < \phi(n)/n < 1$. Следећи примјер показује да је могуће изабрати n тако да је дата вјероватноћа произвољно близу 1.

Примјер 9.5 *За произвољно $\epsilon > 0$ постоји природан број n тако да*

$$\frac{\phi(n)}{n} > 1 - \epsilon.$$

Пошто је скуп простих бројева бесконачан, онда за свако $\epsilon > 0$ постоји прост број p тако да $p > 1/\epsilon$. За $n = p^e$, гдје је $e \in \mathbb{N}$, имамо да

$$\frac{\phi(n)}{n} = 1 - \frac{1}{p} > 1 - \epsilon.$$

Примјер 9.6 *За које вриједности n је $\phi(n)$ непаран број? Доказати да постоје природни бројеви за које је $\phi(n) = 2, 4, 6, 8, 10$ и 12, али не 14.*

Рјешење. Лако се уочава да је $\phi(n)$ непарно ако и само ако $n \leq 2$. Наиме, ако је $n > 2$ онда је дјељив са непарним простим бројем или са 4, па зато $2 \mid \phi(n)$. Очиглчедно $\phi(1) = \phi(2) = 1$.

За $\phi(n) = 2, 4, 6, 8, 10, 12$, имамо одговарајуће бројеве $n = 3, 5, 7, 15, 11, 13$. За $\phi(n) = 14$, имамо да $7 \mid \phi(n)$. Како је

$$\phi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1),$$

онда $7^2 \mid n$ или постоји прост број p_i тако да $7 \mid p_i - 1$. У првом случају закључујемо да је $6 \mid \phi(n)$, док у другом случају $p_i - 1 > 14$, што значи да $\phi(n) > 14$. Дакле, не

постоји природан број n тако да $\phi(n) = 14$. ■

Примјер 9.7 *Одредимо све природне бројеве n за које вриједи $\phi(n) = 12$.*

Нека је дата факторизација $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Слиједи

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

Пошто фактори облика $p_i - 1$ дијеле $\phi(n)$, онда слиједи да $(p_i - 1) \mid 12$. Закључујемо да $p_i \in \{2, 3, 5, 7, 13\}$, те да $5, 7, 13$ могу у факторизацији броја n могу имати највише степен 1, док 2 може имати највише до трећег, а 3 до највише другог степена. Дакле,

$$n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} 7^{\alpha_4} 13^{\alpha_5},$$

$\alpha_1 \leq 3, \alpha_2 \leq 2$, док $\alpha_3, \alpha_4, \alpha_5 \leq 1$. Такође, лако се уочава да највише један од експонената $\alpha_3, \alpha_4, \alpha_5$ може бити јединица. Значи, имамо укупно четири могућности $n = 2^{\alpha_1} 3^{\alpha_2}$, $n = 5 \cdot 2^{\alpha_1} 3^{\alpha_2}$, $n = 7 \cdot 2^{\alpha_1} 3^{\alpha_2}$, $n = 13 \cdot 2^{\alpha_1} 3^{\alpha_2}$.

Рецимо да је $n = 7 \cdot 2^{\alpha_1} 3^{\alpha_2}$. Онда је $\phi(n) = 6 \cdot \phi(k)$, гдје је $k = 2^{\alpha_1} 3^{\alpha_2}$. Слиједи да је $\phi(k) = 2$, одакле је $k \in \{3, 4, 6\}$, па је у овом случају $n \in \{21, 28, 42\}$.

Директном провјером за сваку од наведених могућности, добијамо $n \in \{13, 21, 26, 28, 36, 42\}$.

Примјер 9.8 *Наћи најмањи $n \in \mathbb{N}$ за који вриједи $\phi(n)/n < 1/4$.*

Рјешење. Најприје, уочимо да је

$$(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = \frac{4}{15} > \frac{1}{4}.$$

Како је

$$\frac{\phi(n)}{n} = \prod_{p \mid n} (1 - \frac{1}{p}),$$

онда је јасно да за сваки природни број n са највише 3 проста фактора вриједи

$$\frac{\phi(n)}{n} \geq (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = \frac{4}{15} > \frac{1}{4}.$$

Најмањи природни број који има више од 3 проста фактора је $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, а за њега вриједи

$$\frac{\phi(n)}{n} = \frac{8}{35} < \frac{1}{4}.$$

■

За дату мултипликативну функцију f често везујемо

$$g(n) = \sum_{d \mid n} f(d)$$

која је такође мултипликативна. Претпоставимо да је $(m,n)=1$. Тада је

$$g(mn)=\sum_{d|m}\sum_{d'|n}f(dd')=\sum_{d|m}\sum_{d'|n}f(d)f(d')=\left(\sum_{d|m}f(d)\right)\left(\sum_{d'|n}f(d')\right)$$

$=g(m)g(n)$.

Теорема 9.3

$$\sum_{d|n}\phi(d)=n.$$

Доказ. Примјетимо да је

$$\begin{aligned} g(p^\alpha) &= \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^\alpha)\\ &= 1+(p-1)+(p^2-p)+\cdots+(p^\alpha-p^{\alpha-1})\\ &= p^\alpha. \end{aligned}$$

Са друге стране, функција

$$g(n)=\sum_{d|n}\phi(d)$$

је мултипликативна, па имамо

$$\begin{aligned} g(n) &= g(p_1^{\alpha_1}\cdots p_k^{\alpha_k})\\ &= g(p_1^{\alpha_1})\cdots g(p_k^{\alpha_k})\\ &= p_1^{\alpha_1}\cdots p_k^{\alpha_k}=n. \end{aligned}$$

■

Примјер 9.9 *Нека су дати природни бројеви, d и n, тако да $d\mid n$. Ако је*

$$S_d=\{a\in\mathbb{Z}_n \mid \textbf{нзд}(a,n)=\frac{n}{d}\},$$

доказати да је $|S_d|=\phi(d)$.

Рјешење. Нека је $a\in S_d$. Онда је $a=\frac{n}{d}a'$. Уочимо да је $1\le a'\le d$ и $\textbf{нзд}(a',d)=1$. Наиме, лако се уочава да ако $\textbf{нзд}(a',d)>1$, онда $\textbf{нзд}(a,n)>\frac{n}{d}$.

Такође, за свако $a'\in U_d$, слиједи да $\textbf{нзд}(a'\frac{n}{d},n)=\frac{n}{d}$. Закључујемо да је

$$S_d=\frac{n}{d}U_d,$$

одакле слиједи тврђење. ■

Примјер 9.10 *Користећи тврђење претходног задатка доказати Теорему 9.3.*

Рјешење. Користећи претходно уведене ознаке, уочимо да је

$$\mathbb{Z}_n = \bigcup_{d|n} S_d$$

дисјунктна унија. Како је $|S_d| = \phi(d)$, закључујемо

$$n = \sum_{d|n} \phi(d).$$

■

Теорема 9.4 *(Вилсон) Ако је p прост број, онда је*

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказ. За $p = 2$ или $p = 3$, тврдња је очигледно тачна. Нека је p прост број већи од 3, а скуп

$$S = \{2, 3, \ldots, p-2\}.$$

Ако посматрамо конгруенције

$$ax \equiv 1 \pmod{p}, \text{ за } a \in S,$$

јасно је, на основу Теореме 6.2, да постоји рјешење, да је јединствено и да се налази у скупу S. Такође, рјешење претходне конгруенције је различито од a јер би у супротном било

$$a^2 \equiv 1 \pmod{p}, \text{ односно } p|(a-1)(a+1),$$

а што није могуће јер $a \leq p-2$. Зато, у скупу S имамо парове $i, j \in S$ такве да је $i \cdot j \equiv 1 \pmod{p}$, што значи да је

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

На основу овог, слиједи

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

■

Примјетимо да тврђење Вилсонове теореме вриједи у обрнутом смјеру, односно да ако је

$$(p-1)! \equiv -1 \pmod{p}$$

за неки природан број p, онда тај број мора бити прост. Наиме, ако p има дјелитељ d, $1 < d < p$, онда d дијели $(p-1)!$, а то значи да d дијели и -1, што је контрадикција.

Теорема 9.5 *(Лагранж) Нека је $f(x)$ полином с цјелобројним коефицијентима степена n. Претпоставимо да је p прост број, те да водећи коефицијент од f није дјељив с p. Тада конгруенција $f(x) \equiv 0 \pmod{p}$ има највише n рјешења модуло p.*

Доказ. За $n = 1$ тврдња је тачна на основу Теореме 6.2. Претпоставимо да је тврђење тачно за све полиноме степена $n-1$, те нека је f полином степена n. За сваки $a \in \mathbb{Z}$ имамо

$$f(x) - f(a) = (x-a)g(x),$$

гдје је полином $g(x)$ степена $n-1$ и са истим водећим коефицијентом као f. Зато, ако конгруенција

$$f(x) \equiv 0 \pmod{p} \text{ има рјешење } x = a,$$

онда сва рјешења ове конгруенције задовољавају

$$(x-a)g(x) \equiv 0 \pmod{p}.$$

По индуктивној претпоставци, конгруенција $g(x) \equiv 0 \pmod{p}$ има највише $n-1$ рјешења, па тиме и конгруенција $f(x) \equiv 0 \pmod{p}$ има највише n рјешења. ■

10 Примитивни коријени

Примјер 10.1 *Посматрајмо степене бројева из скупа остатака по модулу* 14.
$2^1 \equiv 2 \pmod{14}$, $2^2 \equiv 4 \pmod{14}$, $2^3 \equiv 8 \pmod{14}$, $2^4 \equiv 2 \pmod{14}$, $\ldots$ *Дакле, једини остаци по модулу 14 степена броја 2 су 2, 4 и 8. Ако узмемо степене броја 3, онда добијамо*
$3^1 \equiv 3 \pmod{14}$, $3^2 \equiv 9 \pmod{14}$, $3^3 \equiv 13 \pmod{14}$, $3^4 \equiv 11 \pmod{14}$, $3^5 \equiv 5 \pmod{14}$, $3^6 \equiv 1 \pmod{14}, \ldots$

Као што се види из претходног примјера, за одређене бројеве $a \in \mathbb{Z}_n$ постоји степен k тако да је

$$a^k \equiv 1 \pmod{n},$$

па у том случају кажемо a има *ред по модулу* n. Следећа лема даје одговор на питање када ред постоји.

Лема 10.1 *Ред броја a по модулу n постоји ако и само ако су бројеви a и n узајамно прости.*

Доказ. Ако је $a^k \equiv 1 \pmod{n}$ за неко k, онда је

$$a \cdot a^{k-1} - nt = 1,$$

одакле слиједи да су a и n узајамно прости.

Обратно, ако су a и n узајамно прости, онда из Ојлерове теореме слиједи $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Дефиниција 10.1 *Нека су a и n узајамно прости природни бројеви. Најмањи природан број d такав да је $a^d \equiv 1 \pmod{n}$ зове се ред од a модуло n. У том случају, број d означавамо са $r_n(a)$.*

Лема 10.2 *За природан број k вриједи $a^k \equiv 1 \pmod{n}$ ако и само ако $r_n(a) \mid k$. Посебно $r_n(a) \mid \phi(n)$.*

Доказ. Нека је $a^k \equiv 1 \pmod{n}$, а $k = r_n(a)q + r$, при чему је $0 \leq r \leq r_n(a)$. Јасно је да $a^r \equiv 1 \pmod{n}$, па сходно дефиницији броја $r_n(a)$, слиједи да је $r = 0$. Одатле слиједи да $r_n(a) \mid k$. ■

Претходна лема значајно помаже приликом одређивања реда елемента a по датом модулу n. Умјесто да првјеравамо редом, испитујемо само дјелитеље $\phi(n)$. На примјер, за $a = 2$ и $n = 13$ имамо да је $\phi(13) = 12$, па су могућности за ред од a дјелиоци броја 12, дакле 1, 2, 3, 4, 6 или 12. Пошто је

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^6 \equiv 12,\ 2^{12} \equiv 1 \pmod{13},$$

слиједи да 2 има ред 12 по модулу 13.

Међутим, за произвољни дјелилац d од $\phi(n)$, не постоји увијек елемент a који има ред d. Примјер је $n = 12$. Дакле, $\phi(12) = 4$, али не постоји ни један елемент по модулу 12 такав да му је ред 4. Заиста,

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12},$$

па су једини редови елемената 1 или 2.

Дефиниција 10.2 *Ако је ред од a модуло n једнак $\phi(n)$, онда се a зове примитивни коријен модуло n.*

Примјер 10.2 *Посматрајмо редуковани скуп остатака $R_7 = \{1, 2, 3, 4, 5, 6\}$. Дати елементи из овог скупа имају ред: 1, 3, 6, 3, 6, 2 респективно. Дакле, уочавамо да су 3 и 5 примитивни коријени по модулу 7.*

Ако посматрамо $R_8 = \{1, 3, 5, 7\}$, уочавамо да су њихови редови: 1 и 2. То значи да ниједан од њих није примитивни коријен.

При крају овог поглавља, доказаћемо да једино за $2, 4, p^\alpha, 2p^\alpha$, гдје је p непаран прост број постоје примитивни коријени.

Теорема 10.1 *Ако је g примитивни коријен по модулу n, онда је*

$$R_n = \{g^i \mid i = 0, 1, \ldots, \phi(n) - 1\}.$$

Доказ. Јасно је да је сваки број облика g^i, $i \in \mathbb{N}$ узајамно прост са m. Такође, ако

$$g^k \equiv g^\ell \pmod{n}, 0 \leq \ell < k < \phi(n),$$

онда би било

$$g^{k-\ell} \equiv 1 \pmod{n},\ 0 < k - \ell < \phi(n),$$

што је у супротности са претпоставком да је g примитивни коријен. ■

Задатак 10.1 *Нека је $p \geq 3$ прост број и n природан број. Доказати да је*

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} -1 \pmod{p}, & \text{ако } p-1 \mid n, \\ 0 \pmod{p}, & \text{иначе.} \end{cases}$$

Теорема 10.2 *Ако је p прост број, онда постоји тачно $\phi(p-1)$ примитивних коријена модуло p.*

Доказ. Алгебарским рјечником речено, ова теорема каже да је R_p циклична група. За сваки број d који дијели $p-1$, односно ред групе R_p, дефинишемо

$$\Omega_d = \{a \in R_p \mid a \text{ има ред } d\} \text{ и } \omega_d = |\Omega_d|.$$

Наш циљ је да покажемо да је $\omega_d = \phi(d)$, за свако d који дијели $p-1$. Један од основних резултата у теорији група је да ред сваког елемента дијели ред групе, па тиме и ред сваког елемента из R_p дијели $p-1$.

То значи да скупови Ω_d чине једну партицију скупа R_p, а одатле слиједи да

$$\sum_{d \mid p-1} \omega_d = p-1.$$

Са друге стране, на основу Теореме 9.3 имамо

$$\sum_{d \mid p-1} \phi(d) = p-1,$$

одакле слиједи

$$\sum_{d \mid p-1} (\phi(d) - \omega_d) = 0.$$

Уколико покажемо да за свако $d \mid p-1$ вриједи $\omega_d \leq \phi(d)$, онда из претходног идентитета, да би укупна сума ненегативних сабирака била једнака нули мора слиједити да су сви једнаки нули, односно $\omega_d = \phi(d)$.

Тражена неједнакост је очигледна уколико је за дато d скуп Ω_d празан, односно $\omega_d = 0$. Уколико то није случај, то значи да постоји бар један елемент a из скупа Ω_d, односно елемент реда d. Сада показујемо да су сви елементи реда d на следећој листи

$$a, a^2, \ldots, a^{d-1}, 1.$$

Најприје, врло лако се уочава да су сви претходни елементи заправо коријени полинома $f(x) = x^d - 1$ унутар $\mathbb{Z}_p$, а како дати полином и не може имати више од d нула, онда то значи да су то заправо све његове нуле. Са друге стране, сви елементи реда d су уједно и нуле полинома $f(x)$, чиме је показано да се сви елементи реда d налазе у наведеној листи.

Да би комплетирали доказ, потребно је показати да је

$$\Omega_d = \{a^i \mid \textbf{нзд}(i, d) = 1\}.$$

Ако је b неки елемент реда d, онда је $b = a^i$ за неко i из скупа $1 \leq i \leq d-1$. Претпоставимо да је **нзд**$(i, d) = s$. Из следећег низа једнакости

$$b^{\frac{d}{s}} = a^{\frac{di}{s}} = a^{d\frac{i}{s}} = (a^d)^{\frac{i}{s}} = 1.$$

Дакле, уколико је ред елемента b једнак d, онда s мора бити једнак 1. Такође, сваки елемент реда d мора бити облика $b = a^i$ за **нзд**$(i, d) = s$, а како таквих i бројева има $\phi(d)$, онда то значи да је $\omega_d \leq \phi(d)$ односно $\omega_d = \phi(d)$. ■

Примјер 10.3 *Наћи најмањи примитивни коријен*
а) модуло 5, б) модуло 11, ц) модуло 23.
а) Како је $2^2 \not\equiv 1 \pmod 5$ *слиједи да је 2 примитивни коријен модуло 5.*
б) Пошто је $2^2 \not\equiv 1 \pmod{11}$ *и* $2^5 \not\equiv 1 \pmod{11}$ *имамо да је 2 примитивни коријен модуло 11.*
в) Лако се утврђује да је $2^{11} \equiv 1 \pmod{23}$, $3^{11} \equiv 1 \pmod{23}$, *као и* $4^{11} \equiv 1 \pmod{23}$. *Међутим,* $5^{11} \not\equiv 1 \pmod{23}$, *па је 5 примитивни коријен модуло 23.*

Дефиниција 10.3 *Ако је број g примитивни коријен по модулу n, то значи да је $R_n = \{g, g^2, \ldots, g^{\phi(n)}\}$. Дакле, за сваки такав да је* **нзд**$(a, n) = 1$ *постоји јединствени ℓ такав да $g^\ell \equiv a \pmod n$. Тај број ℓ зовемо дискретни логаритам a у односу на примитивни коријен g. Означавамо га са* **длог**$_g(a)$ *или само са* **длог**(a) *уколико је из контекста јасно на који се примитивни коријен мисли.*

Као што видимо, дискретни логаритам неког броја у односу на дати примитивни коријен подсјећа на логаритам неког броја по датој основи. Следећа теорема указује да постоји веза између особина дискретног логаритма и логаритма.

Теорема 10.3 *Нека је g примитивни коријен по модулу n. Онда је*

(а) **длог**$(a) +$ **длог**$(b) \equiv$ **длог**$(ab) \pmod{\phi(n)}$

(б) **длог** $1 = 0$ *и* **длог**$(g) = 1$

(в) **длог**$(a^m) \equiv m$ **длог**$(a) \pmod{\phi(n)}$, *за* $m \in \mathbb{N}$

(г) **длог**$(-1) = \frac{1}{2}\phi(n)$ *за* $n \geq 3$

11 Упуства и рјешења

ПОГЛАВЉЕ 2

Задаци 2.5

6

Ово се може записати као

$$a(r^{n+1}-1) = (r-1)(a + ar + ar^2 + \cdots + ar^n).$$

Важан специјалан случајан претходног је

$$(r^{n+1}-1) = (r-1)(1 + r + r^2 + \cdots + r^n).$$

8

Пробати најприје са случајевима $n = 12$, 13, 14, и 15 посебно. Онда искористити индукцију за $n \geq 16$.

ПОГЛАВЉЕ 4

Задаци 4.5

1. Наравно, ово је у општем случају нетачно. На примјер

$$2 \mid (3+7) \text{ док } 2 \nmid 3 \text{ и } 2 \nmid 7.$$

2. Ако је a дјељив са 3, онда је закључак јасан. Уколико a даје остатак 1 при дјељењу са 3, онда је $a+2$ дјељиво са 3, а уколико даје остатак 2, онда је $a+4$ дјељиво са 3.
3. Нека је $d = \textbf{нзд}(a, a+n)$. Онда $d \mid (a+n) - a$, односно $d \mid n$.

ПОГЛАВЉЕ 4

Задаци 4.7

1.

$$\begin{aligned} 93 &= 81 \cdot 1 + 12 \\ 81 &= 12 \cdot 6 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 3 &= 3 \cdot 3 + 0. \end{aligned}$$

Дакле, **нзд**$(93, 81) = 3$. Из проширеног Еуклидовог алгоритма, може се добити цјелобројна линеарна комбинација

$$93 \cdot 7 + 81 \cdot (-8) = 3.$$

Претходни поступак се могао добити и коришћењем Бланкишип методе.

2. Како је

$$(n+1) - n = 1,$$

то значи да постоји линеарна комбинација ова два броја која даје јединицу. С обзиром да је највећи заједнички дјелилац бројева a и b уједно и најмањи природан број који се може добити цјелобројном линеарном комбинацијом, то значи да 1 мора бити највећи заједнички дјелилац.

3. Слично, као и у претходном задатку, правимо линеарну комбинацију

$$(n+1)(n!+1) - ((n+1)!+1) = n,$$

из чега слиједи да $d =$ **нзд**$(n!+1, (n+1)!+1) \mid n$. Како $d \mid n!+1$, онда $d \mid$ **нзд**$(n, n!+1)$. Међутим, **нзд**$(n, n!+1) = 1$, из чега слиједи да $d = 1$.

4. Пошто су a и b узастопни цијели бројеви, то значи да је један од њих паран, а други непаран. Без умањења општости, можемо претпоставити да је a непаран, а b паран. Разликујемо два случаја:

   i. Ако је n паран, онда је $bn + a$ непаран, па мора и d бити такав.

   ii. Ако је n непаран, онда је $an + b$ непаран, па мора и d бити такав.

5. Нека је $d =$ **нзд**$(a+b, a-b)$. Из $d \mid a+b$ и $d \mid a-b$, слиједи да $d \mid 2a$, $d \mid 2b$. Слиједи да

$$d \mid \textbf{нзд}(2a, 2b) = 2 \cdot \textbf{нзд}(a, b) = 2.$$

Дакле, $d = 1$ или $d = 2$.

6. Уочавамо да је

$$mn(m^4 - n^4) = mn(m+n)(m-n)(m^2+n^2).$$

Доказујемо да је дати број дјељив са 2, 3 и 5.

Дјељивост са 2.
Ако је бар један до бројева m, n паран, онда је mn паран. Ако су оба непарна, онда је $m+n$ паран.

Дјељивост са 3.
Ако је бар један до бројева m, n дјељив са 3, онда је mn дјељив са 3. Ако оба дају исти остатак при дијељењу са 3, онда је $m-n$ дјељив са 3, а ако дају различит ненулти остатак, онда је $m+n$ дјељив са 3.

Дјељивост са 5.
Ако је бар један до бројева m, n дјељив са 5, онда је mn дјељив са 5. За све остале могућности, лако се провјерава да је m^4-n^4 дјељив са 5.

Дакле, број је дјељив са 30.

7. Ако је **нзд**$(a,b)=1$, онда постоје $x,y\in\mathbb{Z}$ тако да $ax+by=1$. Одавде је $(a+b)x+b(y-x)=1$. Како је $a+b=c\cdot k$, онда је
$$ckx+b(y-x)=1,$$
што значи да су c и b узајамно прости.

8. Како је **нзд**$(a,b)=1$, онда постоје $x,y\in\mathbb{Z}$ тако да $ax+by=1$. Са друге стране, $a=m\cdot k$, па
$$mkx+by=,$$
што значи да је **нзд**$(m,b)=1$.

9. Нека је $d=$ **нзд**(m,n) и $m=s\cdot d$, $n=t\dot{d}$. Онда је
$$a^d-1\mid a^m-1,\ a^d-1\mid a^n-1.$$
Пошто је $d=$ **нзд**(m,n), онда постоје $x,y\in\mathbb{Z}$, тако да
$$mx+ny=d.$$
Јасно је да x и y морају бити различитог знака, јер ако би оба била негативна, онда би и d било негативно, а ако би оба била позитивна, онда би $d\geq m+n$, што је такође немогуће. Нека је, без умањења општости, $x>0$, $y\leq 0$, а
$$t=\textbf{нзд}(a^m-1,a^n-1).$$
Како је
$$t\mid a^{mx}-1,\ t\mid a^{-ny}-1,$$
онда
$$t\mid\Big((a^{mx}-1)-a^d(a^{-ny}-1)\Big),$$
односно
$$t\mid(a^d-1),$$
чиме је тврђење доказано.

Библиографија

[1] David Burton Eelementary number theory

[2] Edwin Clark Elementary Number Theory

[3] Dujela Teorija brojeva sa kriptografijom

[4] Теорија бројева за мат. гимназију