# Kodiranje pri MaRSovskih igrah

Nino Cajnkar, Rok Jurinčič, Sarah Ramadani
Mentorica: Jana Vidrih


Matematično raziskovalno srečanje
20. avgust 2016

**Povzetek**

Skupina MaRSovcev, ki se je rešila izpod vladavine zlobnega LaTeX-ističnega vladarja priča, kako so s kodiranjem polj na šahovnici zakodirali Magično polje, si izborili svobodo in kako so razkrinkali Čaro-MaRSnikov trik s kartami s pomočjo teorije grup in permutacij.

## 1 Magična šahovnica

Na MaRSu je vladal zloben vladar, ki je MaRSovski posadki onemogočil vrnitev na Zemljo. Posadka je bila zaprta v zaporu, kjer ni bilo nobenih drugih zapornikov. Pred ječo, v katero so bili zaprti, je bil jarek v katerem so plavali morski psi, zato je bil pobeg nemogoč. Nekega dne, je vladar posadki ponudil možnost za rešitev iz ječe. Bili so srečni in njegovo ponudbo takoj sprejeli. Vladar je povabil dva predstavnika na igro s šahovnico in kovanci za življenje celotne posadke. Če bosta uspela zmagati, se bodo lahko vrnili na Zemljo, če ne pa bodo morali za vedno ostati zaprti v ječi na MaRSu.

### 1.1 Navodila igre

Posadka izbere dva predstavnika (Zelenouha in Rdečepeta), ki bosta sodelovala pri nalogi, preostala posadka pa medtem čaka v celici. Vladar odpelje Zelenouha v sobo, kjer ga na mizi čaka šahovnica velikosti

8×8 in skodelica s 64 kovanci. Vladar in Zelenouh sta v sobi sama. Vladar bo iz skodelice vzel nekaj kovancev in jih položil na poljubna polja. Na vsako polje lahko položi največ en kovanec. Koliko kovancev bo vzel iz skodelice in kam jih bo položil, ve samo vladar. Če se Zelenouh na kakršenkoli način vmeša v postavljanje kovancev, je posadka obsojena na smrt. Ko bo vladar postavil kovance tako kot želi, se bo obrnil k Zelenouhu in pokazal na eno polje. To polje je Magično polje in je ključ do vrnitve posadke na Zemljo.

Vladar bo Zelenouhu nato dovolil eno spremembo: lahko vzame poljubni kovanec iz šahovnice ali položi novi kovanec na katerokoli polje, ki še nima kovanca. Po tem ga bo vladar pospremil iz sobe. Če bo za sabo pustil kakršnokoli drugo sporočilo ali namig za Rdečepeta, bo njegova skupina obsojena na smrt.

Vladar bo nato v sobo pripeljal Rdečepeta. Njegova naloga je, da ugotovi katero polje je Magično polje. Dobil bo samo eno priložnost za ugibanje. Če ugane, je celotna posadka rešena, v nasprotnem primeru pa se vam slabo piše in boste za večno ostali na MaRSu pod vladavino zlobnega vladarja.

Vladar pravila naloge predstavi obema, Zelenouhu in Rdečepetu, na začetku, preden Zelenouha pospremi v sobo s šahovnico. Pred igro jima pusti tudi dovolj časa, da se dogovorita za strategijo.

## 1.2 Potek reševanja

### 1.2.1 Dvojiški sistem

Obstaja veliko številskih sistemov. Ljudje večinoma pišemo števila v desetiškem sistemu, medtem ko računalnik podatke zapisuje v dvojiškem. Dvojiški ali binarni številski sistem je številski sistem z osnovo 2. Edini števki uporabljeni v tem sistemu sta 0 in 1.

**Primer 1.** *Imejmo 19 zapisano v desetiškem sistemu. V binarni zapis ga pretvorimo takole*

$$19 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 10011.$$

### 1.2.2 Številčenje šahovnice

Eden izmed načinov, da se bosta Zelenouh in Rdečepet lahko sporazumela glede polj na šahovnici je, da jih oštevilčita. Številčenje začneta v zgornjem levem kotu s številom 0 in končata v spodnjem desnem kotu s številom 63. Števila pišeta po vrsti od 0 do 63 in sicer po vrsticah. Nato jih pretvorita iz desetiškega v dvojiški zapis. Oštevilčena polja lahko vidimo na sliki 1.

Vsako polje je tako predstavljeno z urejeno šesterico ničel in enic oziroma s šestimi biti. Vprašanje je, ali lahko Zelenouh in Rdečepet uporabita položaje kovancev na šahovnici za zakodiranje teh šestih bitov.

### 1.2.3 Razdelitev polj na množice

Definirajmo šest množic $A_i$, $i = 1, \ldots, 6$, ki so podmnožice množice vseh polj šahovnice. Množici $A_i$ pripadajo tista polja, ki imajo $i$-ti bit enak 1. Za lažjo predstavo množice vidimo na slikah 1 do 6.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

Slika 1: V množici $A_1$ so polja s števili, ki imajo na prvem bitu 1. Obarvana so s svetlo modro barvo.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

Slika 2: V množici $A_2$ so polja s števili, ki imajo na drugem bitu 1. Obarvana so s svetlo modro barvo.

Vsako polje je enolično določeno z vsebovanostjo v teh šestih množicah. Na primer polje s številom 001001 je vsebovano v množici $A_3$ in v množici $A_6$ in ni vsebovano v preostalih množicah $A_1, A_2, A_4$ in $A_5$.

Edino polje, ki je vsebovano v množicah $A_1, A_2$ in $A_4$ pa je polje s številko 110100.

### 1.2.4 Kateri kovanec je potrebno obrniti?

Najprej za vsako množico $A_i$, $i = 1, \ldots, 6$ posebej preštejemo število polj v množici, ki so pokrita s kovanci. Množice $A_i$ po vrsti od 1 do 6 predstavljajo zaporedne bite. Če je število kovancev v množici liho, je

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

Slika 3: V množici $A_3$ so polja s števili, ki imajo na tretjem bitu 1. Obarvana so s svetlo modro barvo.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

Slika 4: V množici $A_4$ so polja s števili, ki imajo na četrtem bitu 1. Obarvana so s svetlo modro barvo.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

Slika 5: V množici $A_5$ so polja s števili, ki imajo na petem bitu 1. Obarvana so s svetlo modro barvo..

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000001 | 000010 | 000011 | 000100 | 000101 | 000110 | 000111 |
| 001000 | 001001 | 001010 | 001011 | 001100 | 001101 | 001110 | 001111 |
| 010000 | 010001 | 010010 | 010011 | 010100 | 010101 | 010110 | 010111 |
| 011000 | 011001 | 011010 | 011011 | 011100 | 011101 | 011110 | 011111 |
| 100000 | 100001 | 100010 | 100011 | 100100 | 100101 | 100110 | 100111 |
| 101000 | 101001 | 101010 | 101011 | 101100 | 101101 | 101110 | 101111 |
| 110000 | 110001 | 110010 | 110011 | 110100 | 110101 | 110110 | 110111 |
| 111000 | 111001 | 111010 | 111011 | 111100 | 111101 | 111110 | 111111 |

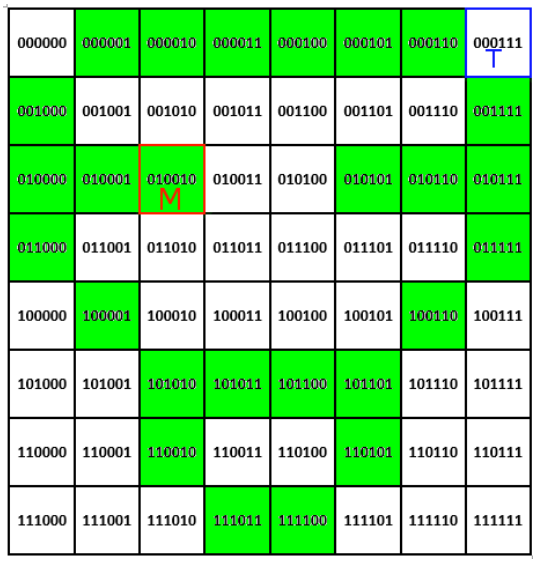
Slika 6: V množici $A_6$ so polja s števili, ki imajo na šestem bitu 1. Obarvana so s svetlo modro barvo.

bit, ki ga množica predstavlja, enak 1, če je število sodo, pa je bit enak 0. Tako dobimo binarni zapis nekega števila, ki kaže na eno izmed 64 polj.

Vsak položaj kovancev torej preko števila kovancev v množicah določa eno polje. Vprašanje je, ali na šahovnici obstaja takšno polje,

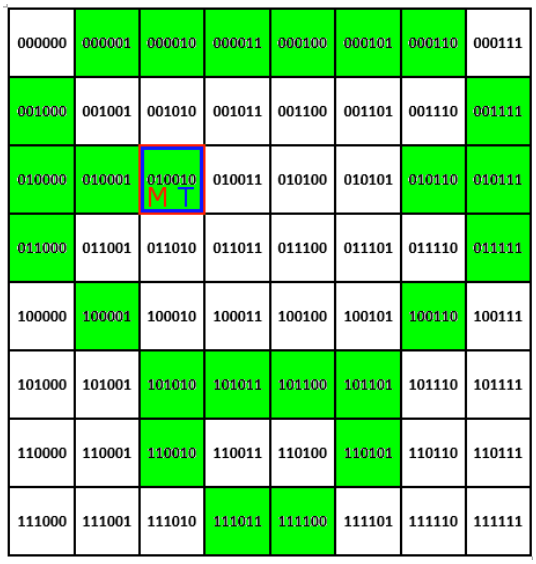
na katerega bi lahko ali položili kovanec ali ga iz njega odstranili tako, da bo nova postavitev kovancev kazala na magično polje.

**Primer 2.** *Poglejmo si primer, na katerega sta tistega dneva naletela Zelenouh in Rdečepet. Vladar je kovance postavil na polja, ki so na sliki 7 pobarvana z zeleno barvo. Za Magično polje je izbral polje s številko* 010010. *Na sliki je Magično polje obrobljeno z rdečo barvo in vsebuje velik* $M$.




Slika 7: Z zeleno so obarvana polja na katerih so kovanci. Določiti želimo polje na katero kaže ta postavitev kovancev. Preštevamo kovance v množicah $A_i$, $i = 1, \ldots, 6$. V množici $A_1$ je 10 pobarvanih polj. Ker je 10 sodo število, je prvi bit števila na katero kaže postavitev kovancev enak 0. V drugi množici je 12 kovancev. Ker je 12 sodo število, je tudi drugi bit 0. V tretji množici je spet sodo število kovancev in tako je tudi tretji bit enak 0. V množici $A_4$ je 13 zelenih polj. Četrti bit je zato enak 1. Podobno preštejemo kovance še v preostalih dveh množicah $A_5$ in $A_6$. Dobimo število 000111. Polje, ki ga število 000111 predstavlja, je na sliki obrobljeno z modro in vsebuje velik tiskani $T$.

*Zelenouh je dober matematik in tako je ugotovil, da če želi, da bo razporeditev kovancev kazala na Magično polje* 010010, *odstraniti kovanec, ki je vsebovan v množicah* $A_2, A_4, A_6$ *in ni vsebovan v* $A_1, A_3, A_5$. *To polje je polje s številko* 010101. *Če primerjamo sliki 7 in 8 vidimo, da polje* 010101 *na sliki 8 več ni pobarvano. Zelenouh je iz tega polja odstranil kovanec. Sedaj je na vrsti Rdečepet, da ugotovi katero je Magično polje.*




Slika 8: Magično polje je zakodirano s številko 010010. Poiščemo polje na katero kažejo kovanci. Spomnimo, kovanci se nahajajo na zelenih poljih. Rdečepet prešteje število zelenih polj v posamezni množici. V množici $A_1$ se nahaja 10 kovancev, torej je prvi bit 0. V množici $A_2$ je 11 zelenih polj in zato je drugi bit enak 1. Preštejemo še zelena polja po preostalih množicah $A_i$, $i = 3, \ldots, 6$. in dobimo število 010010. To število predstavlja Magično polje.

*Tako je razmišljal tudi Rdečepet. Po preštevanju kovancev po množicah $A_i$, $i = 1, \ldots, 6$ je pravilno ugotovil Magično polje in posadka je bila rešena.*

*Zelenouh in Rdečepet sta si izbrala pravo strategijo in zmagala. Vladar je od jeze doživel srčno kap in prevzela sta MaRSovsko oblast. Vse neprijazne sta zaprla v ječo, z ostalimi pa cele noči igrala družabne igre. Vrnitev na Zemljo tako prestavili za nekaj let. Vendar pa je vladar imel zlobnega sina, ki je iz zapora rešil vse zlobneže in posadko ponovno zaprl v ječo. Do konca življenja bodo za pisanje dokumentov lahko uporabljali samo še LaTeX.*

### 1.2.5 Ekskluzivni ali

Za lažje računanje magičnega polja sta Zelenouh in Rdečepet uporabila logično operacijo ekskluzivni ali.

Operacijo ekskluzivni ali najlažje podamo s pravilnostno tabelo 1. Lahko jo razširimo tudi na zaporedje ničel in enic dolžine $n$.

**Primer 3.** *Operacijo izvedemo na dveh zaporedjih ničel in enic*

Tabela 1: Pravilnostna tabela za ekskluzivni ali.

| A | B | A $\oplus$ B |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

.

$$\begin{array}{rr} & 10001010 \\ \oplus & 00100100 \\ \hline & 10101110. \end{array}$$

V našem primeru imamo števila zapisana z zaporedjem 6 števk. Operacijo izvajamo na isto ležečih števkah v zaporedju, kjer upoštevamo za vsak par zgornjo pravilnostno tabelo 1.

Sedaj izvedemo operacijo ekskluzivni ali na številih, ki predstavljata Magično polje in polje na katerega kaže trenutna postavitev kovancev. Dobljena številka predstavlja polje na katerem moramo narediti spremembo (odvzamemo ali dodamo kovanec).

Ko je Rdečepet prišel na vrsto, da ugane Magično polje, je moral tako le ponovno prešteti število kovancev po posameznih množicah. Za liho število kovancev v množici $A_i$ je zapisal bit 1 na $i$-to mesto, za soda števila pa 0. Število, ki ga je dobil, predstavlja Magično polje.

# 2 Trik ali črna LaTeXija?

Na MaRSu se je pojavil ČaroMaRSnik, ki je trdil da lahko z uporabo magije ugotavlja tudi to, kar mu je prikrito. Da bi to dokazal, je MaRSovcem pokazal urok govorečih kart.

ČaroMaRSnik je kupček kart za poker podal MaRSovcem, ti pa so izbrali pet poljubnih kart in jih podali ČaroMaRSnikovemu asistentu. Ta je karte prerazporedil, eno pokazal MaRSovcem in jo spravil v žep tako, da ČaroMaRSnik karte ni videl. Preostale štiri karte je nato predal ČaroMaRSniku. Ta je nad njimi izvedel urok, ki je karte pripravil do tega, da mu povedo s katero karto so se družile v asistentovih rokah. ČaroMaRSnik je pravilno povedal katero karto je asistent pospravil.

Večina MaRSovcev je bila šokirana. Nekateri so ploskali in se čudili, drugi so hoteli ČaroMaRSnika zgrabiti in ga obsoditi na zažigi z raketnim motorjem, saj so bili prepričani da ČaroMaRSnik uporablja črno LaTeXijo. Manjši skupini MaRSovcev pa se je asistentovo prerazporejanje kart zdelo nekoliko sumljivo. Prepričani, da ČaroMaRSnik sploh nima ČaroMaRSniških moči so se odločili, da bodo primer vzeli

pod drobnogled. Po zaslugi tega, da so v raziskavo vložili veliko truda in znanja (ki je že kar mejilo na čaroMaRSijo) so ČaroMaRSnika razkrinkali in MaRSovcem razložili, da je njegova čaroMaRSija v resnici le trik.

## 2.1 Razkrivanje

Skupina bistroumnih MaRSovcev je po dolgi in zapleteni preiskavi razkrinkala kar je bilo MaRSovcem prikrito.

1. ČaroMaRSnik je publiki podal standardni kupček kart, ki vsebuje karte štirih barv (pik, kara, srce, križ), s števili od dva do deset in figurami fant, dama, kralj in As v vsaki od barv.
2. Publike je izbrala pet poljubnih kart in jih podala ČaroMaRSnikovemu asistentu.
3. Asistent je izbral tisto izmed štirih barv, ki je v izbranih petih kartah zastopana vsaj dvakrat (taka je vsaj ena barva, saj publika poda asistentu pet kart, različne barve pa so le štiri).
4. Figuram priredimo števila (fant predstavlja število enajst, dama dvanajst, kralj trinajst in As ena) in jih ciklično razporedimo. To pomeni, da je As za ena večji od kralja in da je število dve za dva večja od kralja. Velja tudi, da je kralj za trinajst večji od Asa in dvanajst od karte dve.
5. Izmed dveh kart enake barve asistent ugotovi katera je za šest ali manj manjša od druge. Manjšo karto obdrži večjo pa vtakne v žep. Manjšo karto da na prvo mesto med preostalimi štirimi kartami in predstavlja barvo skrite karte.
6. S preostalimi tremi kartami asistent tvori eno izmed šestih možnih permutacij.
7. Permutacije tvori tako, da vsaki od treh preostalih kart priredi eno od treh velikosti (velika, srednja, majhna). Karte razporedi po velikosti od dvojke do Asa, kjer za karte istih števil in različnih barv upošteva še v naprej dogovorjeni vrstni red barv (npr.♠ > ♡ > ♢ > ♣). Karti z največjim številom določi velikost V (velika), srednji S (srednja) in najmanjši M (majhna).

   ČaroMaRSnik in njegov asistent sta se dogovorila za spodnji primer vrstnega reda permutacij. Vsaka permutacija treh kart predstavlja eno število od 1 do 6.

   I . M S V ..... 1
   II . M V S ..... 2
   III . S M V ..... 3

IV . S V M ..... 4

V . V M S ..... 5

VI . V S M ..... 6

8. Ker je različnih vrednosti na kartah samo 13 in se vsaka številka pojavi samo enkrat, asistent lahko vedno med dvema kartama enake barve izbere karto, ki je 6 ali manj manjša od druge.
9. ... in tako ČaroMaRSnik iz štirih kart, ki mu jih poda asistent dekodira karto, ki jo je asistent skril.

## 2.2 Primer trika

Publika izbere srčevo 4, karino 6, pikovega kralja, pikovega Asa in križevo damo.

Asistent pogleda karte. Ker sta med kartami dva pika, bo skril enega izmed njih. Kralj in As se razlikujeta za 1 in kralj je manjši. Prva karta v kupčku, ki ga bo asistent dal ČaroMaRSniku bo tako pikov kralj, Asa pa bo skril v žep.

Ker se kralj in As razlikujeta za 1, želi asistent s preostalimi tremi kartami zakodirati število 1. Zato ostale 3 karte postavi v prvo permutacijo, to je M S V. Zato bodo naslednje tri karte v kupčku po vrsti srce 4, kara 6 in križ dama.

ČaroMaRSnik nato pogleda karte, prva je pikov kralj, torej ve, da je barva skrite karte pik. Ostale 3 so v prvi permutaciji zato kralju prišteje 1. Tako ve, da je asistent skril pikovega Asa.

# 3 Permutacije in grupe

## 3.1 Permutacije

**Definicija 1.** *Permutacija je bijektivna preslikava množice z n elementi samo vase.*

Permutacije lahko predstavimo na dva načina, z dvovrstičnim ali s cikličnim zapisom.

**Primer 4.** *1. Primer dvovrstičnega zapisa:*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$$

*Ta zapis pomeni, da se število 1 preslika v število 2, število 2 v število 4, 3 v 1 in podobno do 6 se preslika v 3. Zapišimo isto permuntacijo še s cikličnim zapisom.*

*2. Primer cikličnega zapisa:*

$$\pi = (124563)$$

**Definicija 2.** *Množico prvih n naravnih števil označimo z* $[n]$,

$$[n] = \{1, 2, 3, \ldots, n\}.$$

*Pri cikličnem zapisu je zelo pomemben vrstni red števil v oklepaju. Z vrstnim redom so določene preslikave. Zapis pomeni, da se 1 preslika v 2, 2 se preslika v 4, saj število 4 stoji neposredno za številom 2. Število 4 se preslika v 5, saj je desno od 4 v ciklu 5, 5 se preslika v 6, 6 pa v 3. Ko pridemo do zadnje številke v oklepaju, skočimo nazaj na začetek. Tako velja, da se 3 preslika v 1.*

*Permutacija se ne spremeni, če cikel zamaknemo za kakšno mesto. Na primer*

$$\pi = (124563) = (456312) = (312456).$$

Permutacije lahko med seboj tudi množimo. To ustreza dvema zaporednima zamenjavama vrstnega reda števil od 1 do $n$. Kako množimo v splošnem, si lahko pogledate v viru [1], mi pa se bomo množenja naučili kar ob primeru.

**Primer 5.** *Naj bosta* $\pi_1$ *in* $\pi_2$*, podani z*

$$\pi_1 = (135)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$\pi_2 = (1234)(5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

*Ko ju zmnožimo dobimo permutacijo* $\pi_1 * \pi_2$*. Če je permutacija podana z dvovstičnim zapisom, množimo na naslednji način.*

*Najprej v prvi dve vrstici prepišemo permutacijo* $\pi_1$*,*

$$\pi_1 * \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \\ x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix}.$$

*Pri permutaciji* $\pi_2$ *premešamo stolpce. S tem se permutacija ne spremeni, spremeni se le zapis*

$$\pi_2 = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}.$$

*Opazimo, da je druga vrstica permutacije $\pi_1 * \pi_2$ enaka prvi vrstici permutacije $\pi_2$, ki smo ji premešali stolpce. Sedaj samo še v tretjo vrstico permutacije $\pi_1 * \pi_2$ namesto neznanih vrednosti $x_1, \ldots, x_5$ prepišemo drugo vrstico permutacije $\pi_2$ s premešanimi stolpci*

$$\pi_1 * \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}.$$

*Drugo vrstico izbrišemo in dobimo permutacije $\pi_1 * \pi_2$ z dvovrstičnim zapisom*

$$\pi_1 * \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}.$$

*Prepišimo dvovrstični zapis $\pi_1 * \pi_2$ še v cikličnega. Število 1 gre v število 4, zato zapišemo 1 in 4 kot prvi dve števili nove permutacije $\pi_1 * \pi_2$, nato gre število 4 v število 3, ki je na tretjem mestu cikličnega zapisa permutacije $\pi_1 * \pi_2$. Število 3 gre v število 5, ki je tako na četrtem mestu, število 5 pa gre v število 2 na peto mesto cikličnega zapisa. Tukaj se zapis konča, saj gre število 2 v število 1, ki pa je že na začetku. Končen zapis permutacije $\pi_1 * \pi_2$ je torej*

$$\pi_1 * \pi_2 = (14532).$$

## 3.2 Grupe

Ugotovili smo, da ima množica vseh permutacij z operacijo množenja permutacij veliko pomembnih lastnosti. V ta namen bomo definirali pojem grupe.

**Definicija 3.** *Naj bo $G$ neprazna množica z binarno operacijo $*$, $* : G \times G \to G$, ki ima lastnosti*

1. Zaprtost*: $a, b \in G \Rightarrow a * b \in G$,*
2. Asociativnost $a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$,
3. Enota*: $\exists e \in G \, \forall a \in G : \; a * e = e * a = a$,*
4. Inverz*: $\forall a \in G \, \exists b \in G : \; a * b = b * a = e$.*

*Potem je $(G, *)$ grupa.*

*Če je operacija $*$ komutativna, rečemo, da je $(G, *)$ abelova grupa.*

Nekaj primerov grup: $(\mathbb{Z}, *)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C}, +)$.

**Primer 6.** *Sedaj bomo pogledali ali je množica celih števil z operacijo seštevanja grupa. Da bi to bila grupa, mora imeti operacija vse štiri zgoraj naštete lastnosti. Pogledali bomo vsako lastnost posebej.*

1. Zaprtost*: Če dve seli števili seštejemo, dobimo spet celo število, torej je množica celih števil zaprta za operacijo množenja.*
2. Asociativnost*: Že iz osnovne šole vemo da je operacija seštevanja asociativna v množici celih števil.*
3. Enota*: Enota za seštevanje je* 0*. Množica* $(\mathbb{Z}, +)$ *ima torej enoto in s tem je zadoščena tretja potrebna lastnost operacije* $+$*.*
4. Inverz*: Vemo, da ima vsako celo število sebi nasprotno število. Če seštejemo dve nasprotni števili, dobimo* 0*, ki je enota za* $+$*. Torej je tudi zadoščeno pogoju* $a*b = b*a = e$*, v našem primeru:*

$$a + (-a) = (-a) + a = 0$$

.

*Ker ima množica celih števil za seštevanje vse lastnosti grupe, zaključimo, da je množica* $(\mathbb{Z}, +)$ *grupa.*
*Operacija seštevanja je v celih številih tudi komutativna in zato je* $(\mathbb{Z}, +)$ *abelova grupa.*

Tudi množica vseh permutacij z operacijo množenja je grupa in imenujemo jo *simetrična grupa.* Več o tej temi lahko preberete v knjigi [1].

# Literatura


[1] I. Vidav: *Algebra,* Matematika-Fizika 4, DMFA Slovenije, Ljubljana, 1972.

[2] *Imposible escape?* [ogled: 16. 8. 2016], dostopno na: `datagenetics.com/blog/december12014/index.html`