Izbrana poglavja iz matematike
5. sklop nalog

Teorija števil

(1) Pokaži, da za vsak $n \in \mathbb{N}$ velja:

(a) $5 \,|\, (2^{6n} + 3^{2n-2})$,
(b) $133 \,|\, (11^{n+1} + 12^{2n-1})$,
(c) $7 \,|\, (1 + 2^{3n+1} + 2^{6n+2})$.

Rešitev: Računajmo:

(a) $2^{6n} + 3^{2n-2} \equiv \left(2^6\right)^n + \left(3^2\right)^{n-1} \equiv (-1)^n + (-1)^{n-1} \equiv 0 \,(\mathrm{mod}\ 5)$,

(b) $11^{n+1} + 12^{2n-1} \equiv 11^{n+1} + 12 \cdot \left(12^2\right)^{n-1} \equiv (11^2 + 12) \cdot 11^{n-1} \equiv 133 \cdot 11^{n-1} \equiv 0 \,(\mathrm{mod}\ 133)$,

(c) $1 + 2^{3n+1} + 2^{6n+2} \equiv 1 + 2 \cdot \left(2^3\right)^n + 4 \cdot \left(2^6\right)^n \equiv 1 + 2 \cdot 1^n + 4 \cdot 1^n \equiv 0 \,(\mathrm{mod}\ 7)$.

□

(2) Dokaži naslednja kriterija deljivosti:

(a) $17 \,|\, (10^n a_n + \cdots + 10a_1 + a_0) \iff 17 \,|\, \left((10^{n-1}a_n + \cdots + 10a_2 + a_1) - 5a_0\right)$,
(b) $33 \,|\, (10^n a_n + \cdots + 10a_1 + a_0) \iff 33 \,|\, ((a_0 + 10a_1) + (a_2 + 10a_3) + (a_4 + 10a_5) + \cdots)$.

Rešitev: (a) Najprej velja

$$\begin{aligned} 10^n a_n + \cdots + 10a_1 + a_0 &\equiv 10(10^{n-1}a_n + \cdots + 10a_2 + a_1) + a_0, \\ &\equiv 10(10^{n-1}a_n + \cdots + 10a_2 + a_1 - 5a_0) + 51a_0, \\ &\equiv 10((10^{n-1}a_n + \cdots + 10a_2 + a_1) - 5a_0) \,(\mathrm{mod}\ 17). \end{aligned}$$

Ker sta si števili 10 in 17 tuji, od tod sledi

$$10^n a_n + \cdots + 10a_1 + a_0 \equiv 0 \,(\mathrm{mod}\ 17) \iff (10^{n-1}a_n + \cdots + 10a_2 + a_1) - 5a_0 \equiv 0 \,(\mathrm{mod}\ 17).$$

(b) Ta kriterij sledi iz kongruence $10^2 \equiv 1 \,(\mathrm{mod}\ 33)$, saj je

$$10^n a_n + \cdots + 10a_1 + a_0 \equiv (a_0 + 10a_1) + (a_2 + 10a_3) + (a_4 + 10a_5) + \cdots \,(\mathrm{mod}\ 33).$$

□

(3) Naj bo a naravno število, zapisano v šestnajstiškem sistemu. Pokaži, da je število a deljivo s 15 natanko takrat, ko je vsota njegovih števk deljiva s 15.

Rešitev: Naj bo

$$a = 16^n a_n + 16^{n-1} a_{n-1} + \cdots + 16a_1 + a_0,$$

kjer so $a_i \in \{0, 1, 2, \ldots, 8, 9, A, B, C, D, E, F\}$. Iz enakosti $16^n \equiv 1 \pmod{15}$ od tod sledi

$$16^n a_n + \cdots + 16a_1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{15}.$$

□

(4) Določi obrnljive elemente v kolobarju $\mathbb{Z}_{25}$ in nato poišči njihove inverze.

Rešitev: Element $a \in \mathbb{Z}_n$ je obrnljiv natanko takrat, ko je a tuj proti n. Od tod sledi, da so v $\mathbb{Z}_{25}$ obrnljivi vsi elementi razen $\{0, 5, 10, 15, 20\}$.

Inverz obrnljivega elementa $x \in \mathbb{Z}_n$ je element $x^{-1} \in \mathbb{Z}_n$, za katerega velja

$$xx^{-1} \equiv x^{-1}x \equiv 1 \pmod{n}.$$

V $\mathbb{Z}_{25}$ imamo naslednje pare inverznih elementov (nekateri elementi so inverzni sami sebi)

$$1 \leftrightarrow 1, 2 \leftrightarrow 13, 3 \leftrightarrow 17, 4 \leftrightarrow 19, 6 \leftrightarrow 21, 7 \leftrightarrow 18, 8 \leftrightarrow 22, 9 \leftrightarrow 14, 11 \leftrightarrow 16, 12 \leftrightarrow 23, 24 \leftrightarrow 24.$$

□

(5) Izračunaj število obrnljivih elementov v naslednjih kolobarjih:

(a) $\mathbb{Z}_{20}$,
(b) $\mathbb{Z}_{131}$,
(c) $\mathbb{Z}_{391}$.

Rešitev: Za poljubno naravno število n označimo s $\phi(n)$ število naravnih števil med 1 in $n-1$, ki so tuja proti n. Tako dobljena funkcija $\phi : \mathbb{N} \to \mathbb{N}$ se imenuje *Eulerjeva funkcija*. Če je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ razcep števila n na prafaktorje, je

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Ker so števila v $\{1, 2 \ldots, n-1\}$, ki so tuja proti n, ravno obrnljivi elementi v $\mathbb{Z}_n$, je število obrnljivih elementov v $\mathbb{Z}_n$ enako $\phi(n)$.

(a) Velja $20 = 2^2 \cdot 5$. Od tod dobimo

$$\phi(20) = 20 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 8.$$

Preverimo lahko, da velja $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

(b) Število 131 je praštevilo, zato je

$$\phi(131) = 131 \left(1 - \frac{1}{131}\right) = 130.$$

V $\mathbb{Z}_{131}$ so torej obrnljivi vsi elementi razen ničelnega. V splošnem za praštevilo p velja

$$\phi(p) = p - 1.$$

(c) Sedaj imamo razcep $391 = 17 \cdot 23$, od koder sledi

$$\phi(391) = 391 \left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{23}\right) = 16 \cdot 22 = 352.$$

V $\mathbb{Z}_{391}$ so obrnljivi vsi elementi razen večkratnikov števil 17 in 23. Teh pa je ravno $23 + 17 - 1 = 39$. Velja si zapomniti, da za števila oblike $n = pq$, kjer sta p in q praštevili, velja

$$\phi(n) = (p-1)(q-1).$$

□

(6) Izračunaj inverza naslednjih elementov:

(a) $16 \in \mathbb{Z}_{75}$,
(b) $73 \in \mathbb{Z}_{81}$.

Rešitev: Inverz obrnljivega elementa $a \in \mathbb{Z}_n$ lahko poiščemo z reševanjem Diofantske enačbe $nx + ay = 1$. Eno izmed rešitev te enačbe lahko poiščemo s pomočjo razširjenega Evklidovega algoritma.

(a) Rešujemo enačbo $75x + 16y = 1$. S pomočjo Evklidovega algoritma dobimo

i	r_i	x_i	y_i	k_i
0	75	1	0	
1	16	0	1	
2	11	1	-4	4
3	5	-1	5	1
4	1	3	-14	2

Od tod preberemo, da velja $75 \cdot 3 - 16 \cdot 14 = 1$ oziroma

$$16^{-1} \equiv -14 \equiv 61 \,(\text{mod } 75).$$

(b) Sedaj rešujemo enačbo $81x + 73y = 1$. Z Evklidovim algoritmom dobimo

i	r_i	x_i	y_i	k_i
0	81	1	0	
1	73	0	1	
2	8	1	-1	1
3	1	-9	10	9

od koder sledi

$$73^{-1} \equiv 10 \,(\text{mod } 81).$$

□

(7) Reši diofantske enačbe:

(a) $113x + 51y = 1$,
(b) $480x + 131y = 2$,
(c) $5x - 2y - 4z = 1$.

Rešitev: Linearna diofantska enačba $ax + by = c$ je rešljiva natanko takrat, ko $\gcd(a, b)|c$. Splošno rešitev enačbe lahko v tem primeru zapišemo v obliki

$$x = x_0 - k\frac{b}{\gcd(a, b)},$$
$$y = y_0 + k\frac{a}{\gcd(a, b)},$$

kjer je k poljubno celo število, (x_0, y_0) pa neka rešitev enačbe, ki jo lahko poiščemo z Evklidovim algoritmom, včasih pa tudi kar uganemo.

(a) Rešujemo enačbo $113x + 51y = 1$. Evklidov algoritem izvedemo s pomočjo tabele

i	r_i	x_i	y_i	k_i
0	113	1	0	
1	51	0	1	
2	11	1	-2	2
3	7	-4	9	4
4	4	5	-11	1
5	3	-9	20	1
6	1	14	-31	1

Od tod preberemo, da je $(x_0, y_0) = (14, -31)$ ena izmed rešitev enačbe $113x + 51y = 1$. Splošna rešitev pa je

$$x = 14 - 51k,$$
$$y = -31 + 113k.$$

(b) V primeru enačbe $480x + 131y = 2$ imamo

i	r_i	x_i	y_i	k_i
0	480	1	0	
1	131	0	1	
2	87	1	-3	3
3	44	-1	4	1
4	43	2	-7	1
5	1	-3	11	1

Od tod dobimo, da je $(-3, 11)$ rešitev enačbe $480x+131y = 1$. Da bi dobili rešitev enačbe $480x + 131y = 2$, moramo to rešitev pomnožiti z 2. Tako dobimo, da je splošna rešitev dane enačbe oblike

$$x = -6 - 131k,$$
$$y = 22 + 480k.$$

(c) Linearno diofantsko enačbo treh spremenljivk $5x - 2y - 4z = 1$ bomo rešili s pomočjo Eulerjeve metode. Najprej poiščemo tistega izmed koeficientov enačbe, ki je najmanjši po absolutni vrednosti in izrazimo ustrezno spremenljivko z ostalimi. Tako dobimo

$$y = \frac{1 - 5x + 4z}{-2} = 2x - 2z + \frac{1 - x}{-2}.$$

Ker hočemo, da je y celo število, mora biti $\frac{1-x}{-2} = k$ za nek $k \in \mathbb{Z}$. Od tod dobimo, da je $x = 1 + 2k$, če to vstavimo v zgornjo enačbo, pa še $y = 2 + 5k - 2z$. Vrednost spremenljivke z je poljubna, zato lahko vzamemo $z = l$, kjer je $l \in \mathbb{Z}$. Splošno rešitev enačbe $5x - 2y - 4z = 1$ lahko tako zapišemo v obliki

$$\begin{aligned} x &= 1 + 2k, \\ y &= 2 + 5k - 2l, \\ z &= l, \end{aligned}$$

kjer sta k in l poljubni celi števili. □

(8) Imamo sod z volumnom 100 litrov in pa vedri z volumnoma 51 litrov oziroma 30 litrov. V vsakem koraku lahko v sod vlijemo ali pa iz njega odvzamemo vedro tekočine. Edini pogoj je, da morajo biti pri tem vedra vedno polna in da se ne sme tekočina nikoli preliti čez rob soda.

(a) Poišči zaporedje korakov, po katerem bo v sodu natanko 15 litrov tekočine. Kolikšno je najmanjše število korakov, ki je za to potrebnih?

(b) Ali lahko po zgornjem postopku sod napolnimo natanko do polovice?

Rešitev: (a) V matematičnem jeziku lahko dano nalogo zastavimo na naslednji način. Iščemo zaporedje števil $a_1, a_2, \ldots, a_N$, tako da za vsak $1 \leq i \leq N$ velja

$$a_i \in \{30, 51, -30, -51\},$$

$$0 \leq a_1 + a_2 + \cdots a_i \leq 100,$$

$$a_1 + a_2 + \cdots a_N = 15.$$

Če iščemo minimalen N, za katerega obstaja takšno zaporedje, se lahko omejimo na zaporedja, katerih členi so ali v $\{30, -51\}$ ali pa v $\{51, -30\}$ (sicer bi s krajšanjem dveh nasprotnih števil in s preureditvijo vrstnega reda dobili krajše zaporedje, ki ustreza pogojem). Če sedaj zberemo iste člene skupaj, pridemo do linearne diofantske enačbe

$$51x + 30y = 15,$$

kjer je $N = |x| + |y|$. Obratno pa lahko iz vsake rešitve te diofantske enačbe konstruiramo zaporedje števil, ki ustreza pogojem naloge. Rešimo sedaj dano diofantsko enačbo s pomočjo razširjenega Evklidovega algoritma:

i	r_i	x_i	y_i	k_i
0	51	1	0	
1	30	0	1	
2	21	1	-1	1
3	9	-1	2	1
4	3	3	-5	2

Od tod dobimo splošno rešitev

$$x = 15 - 10k,$$
$$y = -25 + 17k.$$

Za vsak $k \in \mathbb{Z}$ nam zgornja rešitev pomaga konstruirati zaporedje števil, ki ustreza pogojem naloge. Za rešitev z najmanjšim N pa moramo poiskati minimum funkcije

$$|x| + |y| = \begin{cases} 40 - 27k & ; \ k < 2, \\ 27k - 40 & ; \ k \geq 2. \end{cases}$$

Hitro se lahko prepričamo, da bo minimum dosežen pri $k = 1$ oziroma $x = 5$ in $y = -8$. To pomeni, da bomo morali v sod 5-krat vliti polno 51-litrsko vedro, iz njega pa bomo morali 8-krat odvzeti po 30 litrov tekočine. Eno takšno zaporedje (delnih vsot) je npr.

$$\overset{+}{51},\ \overset{-}{21},\ \overset{+}{72},\ \overset{-}{42},\ \overset{-}{12},\ \overset{+}{63},\ \overset{-}{33},\ \overset{-}{3},\ \overset{+}{54},\ \overset{-}{24},\ \overset{+}{75},\ \overset{-}{45},\ \overset{-}{15}.$$

(b) Na vsakem koraku je število litrov tekočine v sodu deljivo s 3. Ker število 50 ni deljivo s 3, soda ne moremo napolniti natanko do polovice. □

(9) Reši naslednje sisteme kongruenc:

(a) $x \equiv 1 \pmod 5$,
$x \equiv 2 \pmod 6$,
$x \equiv 3 \pmod 7$,

(b) $x \equiv 1 \pmod 2$,
$x \equiv 1 \pmod 3$,
$x \equiv 1 \pmod 4$,
$x \equiv 1 \pmod 5$,
$x \equiv 1 \pmod 6$,
$x \equiv 0 \pmod 7$,

(c) $x \equiv 3 \pmod{45}$,
$x \equiv 7 \pmod{756}$.

Rešitev: Sisteme kongruenc rešujemo s pomočjo naslednjega izreka.

Kitajski izrek o ostankih: Naj bodo $n_1, n_2, \ldots, n_k$ paroma tuja naravna števila. Potem je sistem kongruenc

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k}, \end{aligned}$$

rešljiv. Rešitev je enolična po modulu $N = n_1 n_2 \cdots n_k$.

Da najdemo rešitev, lahko uporabimo naslednji algoritem:

(1) definirajmo $N_i = \dfrac{N}{n_i}$,
(2) poiščemo inverze $x_i = N_i^{-1} \pmod{n_i}$,
(3) izračunajmo $x = a_1 x_1 N_1 + a_2 x_2 N_2 + \cdots + a_k x_k N_k$.

(a) Rešujemo sistem kongruenc

$$\begin{aligned} x &\equiv 1 \pmod 5, \\ x &\equiv 2 \pmod 6, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Ker so moduli paroma tuji, lahko direktno uporabimo Kitajski izrek o ostankih. Velja $N = 210$, $N_1 = 42$, $N_2 = 35$ in $N_3 = 30$. Inverze teh elementov v ustreznih kolobarjih lahko izračunamo kar na pamet:

$$\begin{aligned} x_1 &\equiv 42^{-1} \equiv 2^{-1} \equiv 3 \pmod 5, \\ x_2 &\equiv 35^{-1} \equiv 5^{-1} \equiv 5 \pmod 6, \\ x_3 &\equiv 30^{-1} \equiv 2^{-1} \equiv 4 \pmod 7. \end{aligned}$$

Od tod dobimo $x = 1 \cdot 3 \cdot 42 + 2 \cdot (-1) \cdot 35 + 3 \cdot 4 \cdot 30 = 416$, kar pomeni, da je rešitev sistema

$$x \equiv 206 \pmod{210}.$$

(b) Sedaj imamo sistem kongruenc

$$\begin{aligned} x &\equiv 1 \pmod 2, \\ x &\equiv 1 \pmod 3, \\ x &\equiv 1 \pmod 4, \\ x &\equiv 1 \pmod 5, \\ x &\equiv 1 \pmod 6, \\ x &\equiv 0 \pmod 7. \end{aligned}$$

Moduli tokrat niso paroma tuji, zato Kitajskega izreka o ostankih ne moremo direktno uporabiti. V takih primerih vsak modul n najprej razstavimo na obliko $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$ in kongruenco $x \equiv a \pmod n$ nadomestimo s sistemom kongruenc

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^{\alpha_1}}, \\ x &\equiv a_2 \pmod{p_2^{\alpha_2}}, \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_l \pmod{p_l^{\alpha_l}}, \end{aligned}$$

kjer je $a_i \equiv a \pmod{p_i^{\alpha_i}}$. Na ta način dobimo malce večji sistem kongruenc od prvotnega. Sedaj nastopita dve možnosti. Če kongruence, ki nastopajo pri nekem praštevilu, med sabo niso konsistentne, sistem kongruenc ni rešljiv. Če pa so vse kongruence pri vseh

praštevilih, ki nastopajo v sistemu, konsistentne, obdržimo samo kongruenco z najvišjo potenco vsakega praštevila. Ko to izvedemo za vsa dobljena praštevila, dobimo sistem, ki ga rešimo s pomočjo Kitajskega izreka o ostankih. V praksi modulov ni potrebno faktorizirati popolnoma. Važno je le, da odcepimo praštevila, ki se pojavijo v večih kongruencah.

Splošna verzija Kitajskega izreka o ostankih pravi, da je sistem kongruenc

$$\begin{aligned} x &\equiv a_1 \,(\mathrm{mod}\ n_1), \\ x &\equiv a_2 \,(\mathrm{mod}\ n_2), \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \,(\mathrm{mod}\ a_k), \end{aligned}$$

rešljiv natanko takrat, ko $\gcd(n_i, n_j)|(a_i - a_j)$ za vsak par indeksov $1 \leq i, j \leq k$. V tem primeru je rešitev enolična po modulu $\mathrm{lcm}(n_1, n_2, \ldots, n_k)$.

V našem primeru lahko kongruenco $x \equiv 1 \,(\mathrm{mod}\ 6)$ nadomestimo s parom kongruenc

$$\begin{aligned} x &\equiv 1 \,(\mathrm{mod}\ 2), \\ x &\equiv 1 \,(\mathrm{mod}\ 3), \end{aligned}$$

ki pa sta že od prej prisotni v sistemu. Kongruenci $x \equiv 1 \,(\mathrm{mod}\ 2)$ in $x \equiv 1 \,(\mathrm{mod}\ 4)$ pri praštevilu $p = 2$ sta konsistentni, zato lahko kongruenco $x \equiv 1 \,(\mathrm{mod}\ 2)$ izpustimo. Tako nam ostane sistem kongruenc

$$\begin{aligned} x &\equiv 1 \,(\mathrm{mod}\ 3), \\ x &\equiv 1 \,(\mathrm{mod}\ 4), \\ x &\equiv 1 \,(\mathrm{mod}\ 5), \\ x &\equiv 0 \,(\mathrm{mod}\ 7), \end{aligned}$$

s paroma tujimi moduli. Takoj lahko uganemo, da prve tri enačbe reši $x \equiv 1 \,(\mathrm{mod}\ 60)$, zato moramo rešiti sistem

$$\begin{aligned} x &\equiv 1 \,(\mathrm{mod}\ 60), \\ x &\equiv 0 \,(\mathrm{mod}\ 7). \end{aligned}$$

Ta sistem lahko rešimo s pomočjo algoritma iz Kitajskega izreka o ostankih, lahko pa sklepamo tudi takole. Vemo, da bo rešitev sistema neko število med 0 in 419. Iz prve enačbe sledi, da so možne rešitve $1, 61, 121, 181, 241, 301$ in 361. Izmed teh je le število 301 deljivo s 7, kar pomeni, da je rešitev sistema kongruenc

$$x \equiv 301 \,(\mathrm{mod}\ 420).$$

(c) Sistem kongruenc

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\ 45), \\ x &\equiv 7 \,(\mathrm{mod}\ 756), \end{aligned}$$

najprej razširimo do sistema

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\ 5),\\ x &\equiv 3 \,(\mathrm{mod}\ 9),\\ x &\equiv 3 \,(\mathrm{mod}\ 4),\\ x &\equiv 0 \,(\mathrm{mod}\ 7),\\ x &\equiv 7 \,(\mathrm{mod}\ 27). \end{aligned}$$

Kongruenci $x \equiv 3 \,(\mathrm{mod}\ 9)$ in $x \equiv 7 \,(\mathrm{mod}\ 27)$ nista konsistentni, zato sistem kongruenc v tem primeru ni rešljiv. □

(10) Izračunaj:

(a) $11^{11} \,(\mathrm{mod}\ 110)$,

(b) $27^{26} \,(\mathrm{mod}\ 20)$,

(c) $43^{2011} \,(\mathrm{mod}\ 31)$.

Rešitev: Pri tej nalogi si bomo pogledali potenciranje v kolobarjih ostankov. Za izračun visoke potence nekega števila bi z rekurzivnim množenjem potrebovali precej operacij, računanje pa si lahko olajšamo s triki, ki jih bomo spoznali v nadaljevanju.

(a) Računamo $11^{11} \,(\mathrm{mod}\ 110)$. Za izračun produkta n števil v splošnem potrebujemo $n-1$ operacij, če pa so vsa števila med sabo enaka, pa lahko število operacij zmanjšamo na približno $2 \log_2 n$. Najprej potenco zapišemo v 'dvojiškem zapisu':

$$11^{11} = 11^{1+2+8} = 11 \cdot 11^2 \cdot 11^8.$$

Sedaj induktivno s kvadriranjem izračunamo potence, pri katerih je eksponent potenca števila 2:

$$\begin{aligned} 11^2 &\equiv 121 \equiv 11 \,(\mathrm{mod}\ 110),\\ 11^4 &\equiv (11^2)^2 \equiv 11^2 \equiv 11 \,(\mathrm{mod}\ 110),\\ 11^8 &\equiv (11^4)^2 \equiv 11^2 \equiv 11 \,(\mathrm{mod}\ 110). \end{aligned}$$

Od tod dobimo

$$11^{11} \equiv 11 \cdot 11^2 \cdot 11^8 \equiv 11 \cdot 11 \cdot 11 \equiv 11 \cdot 11 \equiv 11 \,(\mathrm{mod}\ 110).$$

(b) V tem primeru iščemo $27^{26} \,(\mathrm{mod}\ 20)$. Če znamo eksponent razstaviti v obliki $e = pq$, si lahko včasih računanje olajšamo s pravilom $x^{pq} = (x^p)^q$. Računajmo

$$27^{26} \equiv 7^{26} \equiv (7^2)^{13} \equiv 9^{13} \equiv 9 \cdot (9^2)^6 \equiv 9 \cdot 1^6 \equiv 9 \,(\mathrm{mod}\ 20).$$

(c) V primeru $43^{2011} \,(\mathrm{mod}\ 31)$ si bomo pomagali z Eulerjevim izrekom. Za poljubno število a, ki je tuje proti n, velja namreč

$$a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\ n).$$

Ker je 31 praštevilo, od tod sledi, da je $a^{30} \equiv 1 \,(\mathrm{mod}\ 31)$ za poljubno število a, ki ni večkratnik števila 31. Sledi

$$43^{2011} \equiv 12^{2011} \equiv 12^{30 \cdot 67 + 1} \equiv (12^{30})^{67} \cdot 12 \equiv 1^{67} \cdot 12 \equiv 12 \,(\mathrm{mod}\ 31).$$

□

(11) Oseba A za prejemanje sporočil uporablja RSA-šifro z javnim ključem $n = 133$, $e = 31$.

(a) Osebi A želiš poslati šifrirano sporočilo. Kateri niz ji moraš poslati, če tvoje originalno sporočilo ustreza nizu 2 11 132?

(b) Oseba B je osebi A poslala šifrirano sporočilo 108 73 21. Poišči vsebino sporočila, če črke ustrezajo številom od 1 do 25.

Rešitev: (a) Za šifriranje sporočila z RSA-šifro moramo najprej izbrati število $n = pq$, ki je produkt dveh (velikih) praštevil in pa število e, ki je tuje proti $\phi(n)$. Paru (n, e) rečemo javni ključ. Dano sporočilo lahko nato zašifriramo v naslednjih dveh korakih:

(1) Pretvorimo sporočilo v zaporedje števil med 1 in n.

(2) Potenciramo vsako število na e-to potenco v kolobarju $\mathbb{Z}_n$.

V praksi torej šifriranje z RSA-šifro ustreza potenciranju v kolobarjih ostankov. V našem primeru imamo

$$\begin{aligned} 2^{31} &\equiv (2^7)^4 \cdot 2^3 \equiv (-5)^4 \cdot 8 \equiv 125 \cdot 5 \cdot 8 \equiv -8 \cdot 40 \equiv -320 \equiv 79 \,(\mathrm{mod}\ 133), \\ 11^{31} &\equiv (11^3)^{10} \cdot 11 \equiv 1^{10} \cdot 11 \equiv 11 \,(\mathrm{mod}\ 133), \\ 132^{31} &\equiv (-1)^{31} \equiv -1 \equiv 132 \,(\mathrm{mod}\ 133). \end{aligned}$$

Z RSA-šifro z javnim ključem $n = 133$ in $e = 31$ se sporočilo 2 11 132 torej zašifrira v

$$79 \quad 11 \quad 132.$$

(b) Da bi lahko zašifrirano sporočilo odšifrirali, moramo najprej izračunati privatni ključ d, ki je enak inverzu števila e v kolobarju $\mathbb{Z}_{\phi(n)}$. Ker je $n = 133 = 7 \cdot 19$, je $\phi(n) = 6 \cdot 18 = 108$. Privatni ključ lahko sedaj izračunamo s pomočjo posplošenega Evklidovega algoritma.

i	r_i	x_i	y_i	k_i
0	108	1	0	
1	31	0	1	
2	15	1	-3	3
3	1	-2	7	2

Od tod preberemo, da je

$$31^{-1} \equiv 7 \,(\mathrm{mod}\ 108).$$

Sporočila lahko odšifriramo po istem postopku, kot jih šifriramo, le da potenciranje na e-to potenco nadomestimo s potenciranjem na d-to potenco. Dobimo

$$\begin{aligned} 108^7 &\equiv (-25)^7 \equiv -25 \cdot 25^2 \cdot 25^4 \equiv -25 \cdot 93 \cdot 4 \equiv 10 \,(\mathrm{mod}\ 133), \\ 73^7 &\equiv 73 \cdot 73^2 \cdot 73^4 \equiv 73 \cdot 9 \cdot 81 \equiv 17 \,(\mathrm{mod}\ 133), \\ 21^7 &\equiv 21 \cdot 21^2 \cdot 21^4 \equiv 21 \cdot 42 \cdot 35 \equiv 14 \,(\mathrm{mod}\ 133). \end{aligned}$$

Če sedaj upoštevamo, da števila od 1 do 25 ustrezajo črkam abecede, dobimo

$$\mathrm{IPM}.$$

□

Izbrana poglavja iz matematike
6. sklop nalog

Polgrupe in grupe

(1) Razišči strukturo naslednjih grupoidov:

(a) $S = \mathbb{R}$ za operacijo $x \circ y = x + y + xy$,

(b) $S = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \,\middle|\, x \in \mathbb{R} \right\}$ za operacijo množenje matrik,

(c) $S = \mathbb{R}^3$ za operacijo vektorski produkt,

(d) $S = \mathbb{R}$ za operaciji $a *_L b = a$ in $a *_R b = b$,

(e) $S = \{1, 2, 3, 4, 5\}$ za operacijo, ki je podana s tabelo

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

.

Rešitev: Pri tej nalogi bomo študirali različne lastnosti binarnih operacij. Najprej začnimo z nekaj terminologije:

- *Grupoid* S je množica z binarno operacijo $\circ : S \times S \to S$.
- *Polgrupa* je grupoid z asociativno operacijo. To pomeni, da velja

$$(a \circ b) \circ c = a \circ (b \circ c)$$

za vsako trojico $a, b, c \in S$.

- *Enota* grupoida S je tak element $e \in S$, da velja

$$e \circ a = a \circ e = a$$

za vsak $a \in S$. Če velja samo $e \circ a = a$ ali pa samo $a \circ e = a$ za vsak $a \in S$, rečemo, da je e leva oziroma desna enota. Če ima grupoid vsaj eno levo in vsaj eno desno enoto, sta enaki in sta avtomatično enota grupoida.

- *Monoid* je polgrupa z enoto.
- Če ima grupoid S enoto e, je *inverz* elementa $a \in S$ tak element $x \in S$, da velja

$$x \circ a = a \circ x = e.$$

Inverz elementa a označimo z a^{-1}. Če velja samo $x \circ a = e$ ali pa $a \circ x = e$, rečemo elementu x levi oziroma desni inverz elementa a. Če ima element a iz neke polgrupe levi in desni inverz, sta ta inverza enaka. V grupoidu to ni nujno res.

· *Grupa* je monoid, v katerem ima vsak element inverz.

· Grupoid S je *komutativen*, če velja

$$a \circ b = b \circ a$$

za vsak par $a, b \in S$.

(a) $S = \mathbb{R}$ za operacijo $x \circ y = x + y + xy$:

- Najprej pokažimo, da je operacija asociativna. To sledi iz enakosti

$$(x \circ y) \circ z = (x + y + xy) \circ z = x + y + xy + z + xz + yz + xyz,$$
$$x \circ (y \circ z) = y \circ (y + z + yz) = x + y + z + yz + xy + xz + xyz.$$

- Število 0 je enota za operacijo $\circ$.
- Operacija je komutativna.
- Inverz x^{-1} elementa $x \in \mathbb{R}$ mora zadoščati pogoju

$$x^{-1} \circ x = x^{-1} + x + x^{-1}x = 0.$$

Od tod lahko izpeljemo, da je

$$x^{-1} = -\frac{x}{1+x},$$

kar pomeni, da so obrnljivi vsi elementi razen $x = -1$.

- Iz vsega navedenega sledi, da je $(S, \circ)$ komutativen monoid. Imamo izomorfizem

$$f : (S, \circ) \to (\mathbb{R}, \cdot),$$
$$x \mapsto x + 1.$$

(b) $S = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \,\middle|\, x \in \mathbb{R} \right\}$ za operacijo množenje matrik:

- Najprej bomo preverili, da je množica S zaprta za množenje. To sledi iz enakosti

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}.$$

- Asociativnost operacije sledi iz asociativnosti matričnega množenja.
- Enota za dano operacijo je matrika $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Inverz poljubnega elementa je enak

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}.$$

- Dokazali smo, da je $(S, \cdot)$ grupa. Izomorfna je grupi realnih števil za seštevanje. Ekspliciten izomorfizem je podan s predpisom

$$f : (S, \cdot) \to (\mathbb{R}, +),$$
$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mapsto x.$$

(c) $S = \mathbb{R}^3$ za operacijo vektorski produkt:

- Vektorski produkt dveh vektorjev iz $\mathbb{R}^3$ je spet vektor iz $\mathbb{R}^3$, zato je operacija dobro definirana.
- Pri preverjanju asociativnosti vektorskega produkta bomo uporabili formuli za dvojni vektorski produkt:

$$\vec{a} \times (\vec{b} \times \vec{c}) = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{c}(\vec{a} \cdot \vec{b}),$$
$$(\vec{a} \times \vec{b}) \times \vec{c} = \vec{b}(\vec{a} \cdot \vec{c}) - \vec{a}(\vec{b} \cdot \vec{c}).$$

  Ti dve enakosti nam dasta slutiti, da vektorski produkt ni asociativna operacija. Konkretno lahko to vidimo na primeru:

$$\vec{i} \times (\vec{i} \times \vec{j}) = \vec{i} \times \vec{k} = -\vec{j},$$
$$(\vec{i} \times \vec{i}) \times \vec{j} = 0 \times \vec{j} = 0.$$

- Ker je vektorski produkt dveh vektorjev pravokoten na oba vektorja, ta operacija nima enote.
- Glede na našo definicijo je torej $(\mathbb{R}^3, \times)$ le grupoid. Je pa kljub temu vektorski produkt primer zelo razširjene algebraične strukture, ki se ji reče Liejeva algebra.

(d) $S = \mathbb{R}$ za operaciji $a *_L b = a$ in $a *_R b = b$:

- Vzemimo najprej operacijo $*_L$. Asociativnost te operacije sledi iz enakosti

$$a *_L (b *_L c) = a *_L b = a,$$
$$(a *_L b) *_L c = a *_L c = a.$$

  Analogno lahko pokažemo, da je tudi operacija $*_R$ asociativna.
- Operacija $*_L$ nima niti enote niti nobene leve enote. Je pa vsak element $x \in \mathbb{R}$ desna enota. Podobno operacija $*_R$ nima nobene desne enote, je pa vsak element leva enota.
- Množica $\mathbb{R}$ je za obe operaciji polgrupa.

(e) $S = \{1, 2, 3, 4, 5\}$ za operacijo, ki je podana s tabelo:

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	5	3
3	3	5	4	2	1
4	4	1	5	3	2
5	5	3	2	1	4

.

- Preverjanje asociativnosti operacije, ki je podana s tabelo je včasih časovno zelo zahtevno. Lažje pa je dokazati, da operacija ni asociativna, če najdemo protiprimer. V našem primeru je

$$2 \circ (2 \circ 3) = 2 \circ 1 = 2,$$
$$(2 \circ 2) \circ 3 = 4 \circ 3 = 5,$$

  kar pomeni, da dana operacija ni asociativna.

- Operacija $\circ$ ima enoto 1.
- Vsak element S ima tako levi kot desni inverz, ki pa nista vedno enaka, kot kaže primer $4 \circ 2 = 2 \circ 3 = 1$.
- Grupoidu z enoto, v katerem ima vsak element levi in desni inverz, rečemo zanka. Če je operacija asociativna, sta oba inverza avtomatično enaka, ta primer pa kaže, da pri neasociativni operaciji to ni več nujno res.

□

(2) Dokaži, da sta naslednji množici z danima operacijama grupi:

(a) $S = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \,\middle|\, x, y \in \mathbb{R},\ x \neq 0 \right\}$ za operacijo množenje matrik,

(b) $S = \left\{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q},\ (a, b) \neq (0, 0) \right\}$ za množenje števil.

Rešitev: (a) $S = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \,\middle|\, x, y \in \mathbb{R},\ x \neq 0 \right\}$ za operacijo množenje matrik:

- Najprej preverimo, da je množica S zaprta za množenje. Velja

$$\begin{bmatrix} x_1 & y_1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_2 & y_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x_1 x_2 & x_1 y_2 + y_1 \\ 0 & 1 \end{bmatrix}.$$

  Ker sta x_1 in x_2 neničelna, je tudi $x_1 x_2$ neničelno število, zato je produkt danih matrik tudi matrika iz S.
- Asociativnost operacije sledi iz asociativnosti matričnega množenja.
- Enota za dano operacijo je matrika $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Inverz poljubnega elementa lahko izračunamo po formuli

$$\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{bmatrix}.$$

(b) $S = \left\{ a + b\sqrt{2} \,|\, a, b \in \mathbb{Q},\ (a, b) \neq (0, 0) \right\}$ za množenje števil:

- Produkt dveh števil iz S je enak

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1 a_2 + 2 b_1 b_2 + (a_2 b_1 + a_1 b_2)\sqrt{2},$$

  kar pomeni, da je množica S zaprta za množenje.
- Asociativnost operacije sledi iz asociativnosti množenja realnih števil.
- Enota za dano operacijo je število 1.
- Inverz števila $a + b\sqrt{2}$ je enak

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

□

(3) Izračunaj rede vseh elementov v grupah $\mathbb{Z}_{20}$, S_3 in S_5.

Rešitev: Red elementa a iz grupe G je najmanjše naravno število n, za katero velja ena izmed enakosti

$$na = 0,$$
$$a^n = e,$$

odvisno od tega, ali pišemo grupno operacijo aditivno ali pa multiplikativno. Če takšen n ne obstaja, rečemo, da ima a neskončen red. Red elementa a označimo z $\mathrm{red}(a)$.

$\underline{\mathbb{Z}_{20}}$:

Elementi ciklične grupe $\mathbb{Z}_{20}$, ki so tuji proti 20 imajo maksimalen možni red 20. Če nek tak element množimo z 2, dobimo element reda 10. Če ga množimo s 4, dobimo element reda 5. Podobno velja tudi za ostale delitelje števila 20. Tako dobimo:

- elementi $1, 3, 7, 9, 11, 13, 17, 19$ imajo red 20,
- elementi $2, 6, 14, 18$ imajo red 10,
- elementi $4, 8, 12, 16$ imajo red 5,
- elementa 5 in 10 imata red 4,
- element 10 ima red 2,
- enota 0 ima red 1.

Bolj splošno imajo redi elementov ciklične grupe $\mathbb{Z}_n$ naslednje lastnosti:

- elementi, ki so tuji proti n, imajo red n. Takih elementov je $\phi(n)$, njihovi večkratniki pa tvorijo celo grupo $\mathbb{Z}_n$. Rečemo jim generatorji grupe $\mathbb{Z}_n$.
- enota 0 ima red 1,
- ostali elementi imajo red, ki zadošča pogoju $1 < \mathrm{red}(a) < n$ in ki deli število n.

$\underline{S_3}$:

Permutacijska grupa S_3 ima šest elementov. Njihovi redi so:

- elementi $(1\,2), (1\,3), (2\,3)$ imajo red 2,
- elementa $(1\,2\,3)$ in $(1\,3\,2)$ imata red 3,
- enota $(1)(2)(3)$ ima red 1.

$\underline{S_5}$:

Permutacijska grupa S_5 ima 120 elementov. Njihovi redi so odvisni samo od ciklične strukture, zato si bomo pogledali vse možne ciklične oblike elementov iz S_5.

- $(1\,2\,3\,4\,5)\ldots$ 5-cikli imajo red 5. Takih elementov je 24.
- $(1\,2\,3\,4)(5)\ldots$ $4+1$-cikli imajo red 4. Takih elementov je 30.
- $(1\,2\,3)(4\,5)\ldots$ $3+2$-cikli imajo red 6. Takih elementov je 20.
- $(1\,2\,3)(4)(5)\ldots$ $3+1+1$-cikli imajo red 3. Takih elementov je 20.
- $(1\,2)(3\,4)(5)\ldots$ $2+2+1$-cikli imajo red 2. Takih elementov je 15.
- $(1\,2)(3)(4)(5)\ldots$ $2+1+1+1$-cikli imajo red 2. Takih elementov je 10.

· $(1)(2)(3)(4)(5)\ldots$ enota ima red 1.

V splošnem je red permutacije enak najmanjšemu skupnemu večkratniku dolžin ciklov, ki nastopajo v dekompoziciji dane permutacije. □

(4) Dana je permutacija $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 5 & 6 & 4 & 8 & 1 \end{pmatrix} \in S_8$. Izračunaj a^{-1}, a^2 in a^{1000}.

Rešitev: Najprej zapišimo permutacijo a kot produkt disjunktnih ciklov

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 5 & 6 & 4 & 8 & 1 \end{pmatrix} = (1\,3\,7\,8)(4\,5\,6).$$

Pri računanju potenc permutacije nam pride prav dejstvo, da disjunktni cikli med sabo komutirajo, zato je dovolj potencirati vsak cikel posebej. Tako dobimo:

$$\begin{aligned} a^{-1} &= (1\,8\,7\,3)(4\,6\,5), \\ a^2 &= (1\,7)(3\,8)(4\,6\,5), \\ a^{1000} &= (4\,5\,6). \end{aligned}$$

□

(5) Poišči vse homomorfizme grup:

(a) $\mathbb{Z} \to \mathbb{Q}$,
(b) $\mathbb{Q} \to \mathbb{Z}$,
(c) $\mathbb{Z}_n \to \mathbb{Z}$,
(d) $\mathbb{Z}_n \to U(1)$.

Rešitev: Naj bosta G in H grupi. Homomorfizem grup $\phi : G \to H$ je preslikava, ki zadošča pogoju

$$\phi(xy) = \phi(x)\phi(y)$$

za vsaka $x, y \in G$. Pri tem moramo na levi vzeti operacijo v G na desni pa operacijo v H. Iz definicije sledi, da homomorfizem grup slika enoto v enoto in inverze v inverze. Če sta grupi G in H komutativni, ponavadi operacijo pišemo aditivno. V tem primeru je homomorfizem grup kar aditivna preslikava, ki po definiciji zadošča pogoju

$$\phi(x + y) = \phi(x) + \phi(y).$$

(a) Homomorfizmi $\mathbb{Z} \to \mathbb{Q}$:

Grupa $\mathbb{Z}$ je ciklična grupa z generatorjem 1, kar pomeni, da je vsak element $\mathbb{Z}$ večkratnik elementa 1. To preprosto dejstvo ima zanimivo posledico. Vsak homomorfizem iz grupe $\mathbb{Z}$ v neko grupo je namreč natanko določen s sliko elementa 1.

Vzemimo torej poljuben homomorfizem $\phi : \mathbb{Z} \to \mathbb{Q}$ in označimo $\phi(1) = q$. Po predpostavki je q racionalno število, pogoj aditivnosti pa nam potem pove, da za poljuben $n \in \mathbb{N}$ velja

$$\phi(n) = \phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n} = nq.$$

Ker homomorfizem slika inverze v inverze, od tod sledi, da velja

$$\phi(m) = mq$$

za poljuben $m \in \mathbb{Z}$. Vidimo, da je homomorfizmov iz $\mathbb{Z}$ v $\mathbb{Q}$ ravno toliko kot je racionalnih števil oziroma

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) \cong \mathbb{Q}.$$

Podobno velja, če grupo $\mathbb{Q}$ zamenjamo s poljubno grupo H, saj je zmeraj

$$\mathrm{Hom}(\mathbb{Z}, H) \cong H.$$

(b) Homomorfizmi $\mathbb{Q} \to \mathbb{Z}$:

Sedaj iščemo aditivne preslikave iz grupe racionalnih števil v grupo celih števil. Grupa $\mathbb{Q}$ ni generirana z elementom 1, zato ne moremo uporabiti podobnega argumenta kot pri prejšnji nalogi. Videli bomo, da obstaja samo en homomorfizem iz $\mathbb{Q}$ v $\mathbb{Z}$.

Vzemimo poljuben homomorfizem $\phi : \mathbb{Q} \to \mathbb{Z}$ in naj bo $\phi(1) = m$. Poglejmo, kaj nam pogoj aditivnosti pove o vrednosti $\phi\left(\frac{1}{n}\right)$ za nek $n \in \mathbb{N}$. Velja

$$m = \phi(1) = \phi\Big(\underbrace{\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}}_{n}\Big) = n\phi\left(\frac{1}{n}\right).$$

Od tod sledi, da je število m večkratnik vsakega naravnega števila n. To je mogoče le, če je $m = 0$. Od tod pa potem sledi

$$\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}) \cong \{0\}.$$

(c) Homomorfizmi $\mathbb{Z}_n \to \mathbb{Z}$:

Grupa $\mathbb{Z}_n$ je ciklična z generatorjem 1, zato je vsak homomorfizem iz $\mathbb{Z}_n$ v $\mathbb{Z}$ natanko določen s sliko elementa 1.

Naj bo $\phi : \mathbb{Z}_n \to \mathbb{Z}$ poljuben homomorfizem in naj velja $\phi(1) = m$. Ker je v grupi $\mathbb{Z}_n$

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

mora torej veljati

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \phi(0) = 0.$$

Po drugi strani pa iz aditivnosti sledi

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n} = nm.$$

Ker je po predpostavki n naravno število, mora biti $m = 0$. Torej je spet

$$\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}) \cong \{0\}.$$

(d) Homomorfizmi $\mathbb{Z}_n \to U(1)$:

Grupa $U(1)$ je grupa enotskih kompleksnih števil za množenje

$$U(1) = \{z \in \mathbb{C} \,|\, |z| = 1\}.$$

Enota grupe $U(1)$ je število 1. Pri študiju homomorfizmov iz $\mathbb{Z}_n$ v $U(1)$ bomo zopet uporabili dejstvo, da je 1 generator grupe $\mathbb{Z}_n$.

Izberimo poljuben homomorfizem $\phi : \mathbb{Z}_n \to U(1)$ in označimo $\phi(1) = w$. Po predpostavki je $|w| = 1$. Iz pogoja

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

tokrat sledi

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = 1.$$

Pogoj aditivnosti pa nam tokrat pove, da je

$$\phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \phi(1)^n = w^n.$$

Oboje skupaj nam da pogoj

$$w^n = 1.$$

Homomorfizmov iz $\mathbb{Z}_n$ v $U(1)$ je torej toliko, kot je n-tih korenov enote. Teh pa je ravno n in so enaki

$$w_k = e^{\frac{i2\pi k}{n}}$$

za $k = 0, 1, \ldots, n-1$. Predpis za homomorfizem, ki pripada korenu w_k, je

$$\phi_k(m) = e^{\frac{i2\pi km}{n}}$$

za $m \in \mathbb{Z}_n$. Velja torej

$$\mathrm{Hom}(\mathbb{Z}_n, U(1)) \cong \mathbb{Z}_n.$$

Opomba: Homomorfizmom iz grupe G v grupo $U(1)$ rečemo karakterji. Karakterji igrajo osrednjo vlogo v teorijah Fourierovih vrst, Fourierove transformacije in diskretne Fourierove transformacije. Pri posplošitvi Fourierove teorije na nekomutativne grupe karakterje nadomestimo s homomorfizmi dane grupe v matrične grupe, ki jih imenujemo tudi reprezentacije oziroma upodobitve. □

(6) Poišči vse avtomorfizme grup $\mathbb{Z}, \mathbb{Z}_5$ in $\mathbb{Z}_{10}$.

Rešitev: Avtomorfizem grupe G je bijektivni homomorfizem $\phi : G \to G$.

Avtomorfizmi grupe $\mathbb{Z}$:

Vsak homomorfizem $\phi : \mathbb{Z} \to \mathbb{Z}$ je določen s sliko generatorja 1 grupe $\mathbb{Z}$. Če označimo $\phi(1) = n$, je potem

$$\phi(m) = nm$$

za poljuben $m \in \mathbb{Z}$. V sliki preslikave ϕ so vsa števila, ki so deljiva z n. Če torej hočemo, da bo ϕ bijektivna, mora biti $n = \pm 1$. To pa pomeni, da je

$$\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}, -\mathrm{Id}\}.$$

Avtomorfizmi grupe $\mathbb{Z}_5$:

Grupa $\mathbb{Z}_5$ je ciklična, zato je vsak homomorfizem $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ določen s sliko generatorja. Če označimo $\phi(1) = n$, bo ϕ bijektivna preslikava natanko takrat, ko bo

$$n \in \{1, 2, 3, 4\}.$$

Torej je

$$\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_5^*.$$

Avtomorfizmi grupe $\mathbb{Z}_{10}$:

Tudi grupa $\mathbb{Z}_{10}$ je ciklična, zato velja podoben sklep kot zgoraj. Če označimo $\phi(1) = n$, bo tokrat ϕ bijektivna preslikava za

$$n \in \{1, 3, 7, 9\},$$

kar pomeni, da je

$$\mathrm{Aut}(\mathbb{Z}_{10}) \cong \mathbb{Z}_{10}^*.$$

Opomba: V splošnem so avtomorfizmi grupe $\mathbb{Z}_n$ v bijektivni korespondenci z elementi $\mathbb{Z}_n^*$. Elementu $m \in \mathbb{Z}_n^*$ pripada preslikava množenja z m po modulu n. □

(7) Ugotovi, ali sta dani grupi izomorfni in poišči eksplicitni izomorfizem, če sta:

(a) $\mathbb{Z}_6$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$,

(b) $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$,

(c) $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Rešitev: (a) Imamo Abelovi grupi reda 6:

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Grupa $\mathbb{Z}_6$ je ciklična z generatorjem 1, medtem ko pri grupi $\mathbb{Z}_2 \times \mathbb{Z}_3$ ni na prvi pogled jasno, ali je generirana z enim elementom. Hitro pa lahko preverimo, da jo generira element $(1, 1)$, kar pomeni, da lahko definiramo izomorfizem $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ s predpisi:

$$\phi(1) = (1, 1),$$
$$\phi(2) = (0, 2),$$
$$\phi(3) = (1, 0),$$
$$\phi(4) = (0, 1),$$
$$\phi(5) = (1, 2),$$
$$\phi(0) = (0, 0).$$

(b) Sedaj imamo dve Abelovi grupi reda 4:

$$\mathbb{Z}_4 = \{0, 1, 2, 3\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Grupa $\mathbb{Z}_4$ je spet ciklična z generatorjem 1, medtem ko grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ tokrat ni ciklična. Če bi namreč bila, bi obstajal element reda 4. Preverimo pa lahko, da so vsi elementi, razen enote, reda 2, kar pomeni, da grupi $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ nista izomorfni.

(c) Grupi $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ sta reda 30. Ker so $2, 3$ in 5 paroma tuja števila, ima element $(1, 1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ red 30, zato lahko definiramo izomorfizem $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ s predpisom:

$$\phi(k) = (k \mod (2), k \mod (3), k \mod (5)).$$

Opomba: Grupi $\mathbb{Z}_{mn}$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ sta izomorfni natanko takrat, ko sta števili m in n tuji. V tem primeru je izomorfizem $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ dan s predpisom

$$\phi(k) = (k \mod (m), k \mod (n)).$$

Od tod med drugim sledi, da za vsako končno Abelovo grupo G obstaja izomorfizem

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}},$$

kjer so p_i praštevila, ki delijo red grupe G. Isto praštevilo se lahko ponovi večkrat, kot smo videli v primeru $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. □

(8) Poišči vse Abelove grupe reda 80.

Rešitev: Razcep števila 80 se glasi

$$80 = 5 \cdot 2^4.$$

Če je G Abelova grupa reda 80, je torej produkt faktorjev oblike $\mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8$ in $\mathbb{Z}_{16}$. Različne možnosti so:

$$\begin{aligned}
&G \cong \mathbb{Z}_5 \times \mathbb{Z}_{16},\\
&G \cong \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_2,\\
&G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_4,\\
&G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\\
&G \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

□

(9) Zapiši grupno tabelo za operacijo v grupi $\mathbb{Z}_{10}^*$. Kateri grupi je izomorfna grupa $\mathbb{Z}_{10}^*$?

Rešitev: Z oznako $\mathbb{Z}_n^*$ označimo grupo (za množenje) obrnljivih elementov v kolobarju $\mathbb{Z}_n$. Ta grupa ima $\phi(n)$ elementov, njena enota pa je element 1.

V našem primeru je

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\},$$

grupna tabela pa se glasi

$\circ$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Iz tabele lahko preberemo, da ima element 3 red 4, kar pomeni, da je

$$\mathbb{Z}_{10}^* \cong \mathbb{Z}_4.$$

□

(10) Dana je grupa G z grupno tabelo

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Kateri znani grupi je izomorfna grupa G?

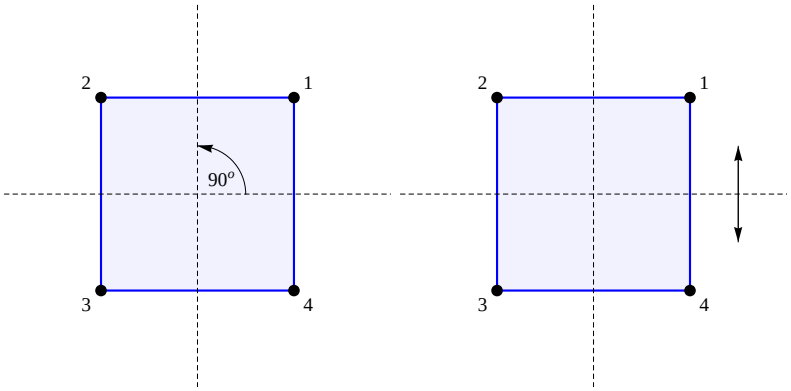
Rešitev: Iz tabele je razvidno, da je e enota grupe G in da je G komutativna. Torej je G izomorfna bodisi grupi $\mathbb{Z}_4$ bodisi grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. Če bi bila G ciklična grupa, bi moral obstajati element reda 4, kar pa vidimo, da ni res. Od tod sledi

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

(11) Opiši grupo izometrij kvadrata.

Rešitev: Obstaja osem izometrij kvadrata. Identiteta, tri rotacije in štiri zracaljenja.



Izkaže se, da lahko vsako izmed teh izometrij izrazimo z eno rotacijo in z enim zrcaljenjem. Izberemo lahko na primer:

- $a = (1\,2\,3\,4)\ldots$ rotacija za $90°$ v pozitivni smeri,
- $b = (1\,4)(2\,3)\ldots$ zrcaljenje preko vodoravnice.

Preostale netrivialne izometrije so potem:

- $a^2 = (1\,3)(2\,4)\ldots$ rotacija za $180°$,
- $a^3 = (1\,4\,3\,2)\ldots$ rotacija za $270°$,
- $ab = (1\,3)(2)(4)\ldots$ zrcaljenje preko simetrale sodih kvadrantov,

- $a^2b = (1\,2)(3\,4)\ldots$ zrcaljenje preko navpičnice,
- $a^3b = (2\,4)(1)(3)\ldots$ zrcaljenje preko simetrale lihih kvadrantov.

Grupi izometrij kvadrata rečemo diedrska grupa reda 8 in jo označimo z D_8. Dejstvo, da lahko vsako izometrijo izrazimo z a in b, pomeni, da je grupa D_8 generirana z elementoma a in b, ki pa še zadoščata nekim pogojem. Reda elementov a in b nam dasta pogoja $a^4 = 1$ in $b^2 = 1$. Poleg teh dveh pa velja še zveza $bab = a^3$. Kompaktno lahko te pogoje strnemo v naslednjem zapisu

$$D_8 = \{a, b \,|\, a^4 = 1,\, b^2 = 1,\, bab = a^3\}.$$

Opomba: V splošnem ima grupa izometrij pravilnega n-kotnika $2n$ elementov. Poleg identične preslikave ima še $n-1$ rotacij in pa n zrcaljenj. Označimo jo z D_{2n} in ji rečemo diedrska grupa reda $2n$. V primeru $n = 3$ je grupa D_6 izomorfna grupi S_3. □

(12) Poišči vse podgrupe grup $\mathbb{Z}, \mathbb{Z}_{10}$ in Q.

Rešitev: Podmnožica H grupe G je *podgrupa* grupe G, če je zaprta za množenje in za invertiranje. Pri tem uporabljamo oznako $H \leq G$.

Podgrupe grupe $\mathbb{Z}$:

Množica, ki vsebuje samo enoto $\{0\}$ je zmeraj podgrupa v vsaki grupi. Tej podgrupi rečemo trivialna podgrupa.

Naj bo sedaj H netrivialna podgrupa grupe $\mathbb{Z}$. Potem je za vsak $x \in H$ tudi $-x \in H$, zato obstaja neko naravno število, ki leži v H. Označimo z n najmanjše naravno število, ki leži v H. Ker je H zaprta za seštevanje, so potem vsi večkratniki števila n tudi v H, pokazali pa bomo, da so to natanko vsi elementi H.

Če bi namreč obstajal $m \in H$, ki ni večkratnik n, bi bil največji skupni delitelj d števil m in n manjši od n. Iz teorije diofantskih enačb potem sledi, da bi morala obstajati $a, b \in \mathbb{Z}$, da bi veljalo

$$an + bm = d,$$

od koder pa bi sledilo $d \in H$. To pa je v nasprotju z minimalnostjo števila n.

Vsaka podgrupa grupe $\mathbb{Z}$ je torej oblike

$$H_n = n\mathbb{Z},$$

za nek $n \geq 0$. Pri $n = 0$ dobimo trivialno podgrupo, pri $n = 1$ pa kar celo grupo.

Podgrupe grupe $\mathbb{Z}_{10}$:

Grupa $\mathbb{Z}_{10}$ ima štiri podgrupe. Te so:

$$\begin{aligned} H_1 &= \{0\}, \\ H_2 &= \mathbb{Z}_{10}, \\ H_3 &= \{0, 5\} \cong \mathbb{Z}_2, \\ H_4 &= \{0, 2, 4, 6, 8\} \cong \mathbb{Z}_5. \end{aligned}$$

Podgrupe kvaternionske grupe Q:

Kvaternionska grupa Q ima 8 elementov

$$Q = \{1, -1, i, -i, j, -j, k, -k\}.$$

Elementi $\pm i, \pm j, \pm k$ se množijo analogno, kot se vektorsko množijo vektorji $\pm\vec{i}, \pm\vec{j}, \pm\vec{k}$, poleg tega pa veljajo še enakosti

$$(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1.$$

Podgrupe kvaternionske grupe so:

$$\begin{aligned}
H_1 &= \{0\}, \\
H_2 &= Q, \\
H_3 &= \{1, -1\} \cong \mathbb{Z}_2, \\
H_4 &= \{1, i, -1, -i\} \cong \mathbb{Z}_4, \\
H_5 &= \{1, j, -1, -j\} \cong \mathbb{Z}_4, \\
H_6 &= \{1, k, -1, -k\} \cong \mathbb{Z}_4.
\end{aligned}$$

□

(13) Dokaži, da je vsaka grupa praštevilskega reda ciklična.

Rešitev: Denimo, da ima grupa G red p, kjer je p praštevilo in naj bo $a \in G$ nek element, ki ni enota grupe. Ker red poljubnega elementa deli red grupe, mora imeti element a red p. To pa pomeni, da velja

$$G = \{e, a, a^2, a^3, \ldots, a^{p-1}\}$$

oziroma, da je G ciklična grupa z generatorjem a.

Z dosedaj zbranim znanjem lahko zapišemo seznam vseh grup do reda 10.

red	grupe
1	$\{0\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_8, Q
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_{10}

□

(14) V grupi $\mathbb{Z}_{11}^*$ izračunaj diskretna logaritma $\log_2 5$ in $\log_6 2$.

Rešitev: Grupa $\mathbb{Z}_{11}^*$ je ciklična grupa reda 10. Če je a poljuben generator grupe $\mathbb{Z}_{11}^*$, mora veljati

$$\mathbb{Z}_{11}^* = \{1, a, a^2, \ldots, a^9\}.$$

Za vsak generator a grupe $\mathbb{Z}_{11}^*$ in poljuben $k \in \mathbb{Z}_{11}^*$ lahko definiramo diskretni logaritem $\log_a k$ kot število, ki je implicitno določeno s pogojem

$$a^{\log_a k} = k.$$

Najprej poglejmo potence števila 2 v grupi $\mathbb{Z}_{11}^*$:

$$2,\ 4,\ 8,\ 5,\ 10,\ 9,\ 7,\ 3,\ 6,\ 1.$$

Od tod sledi, da je

$$\log_2 5 = 4.$$

Sedaj poglejmo še potence števila 6 v grupi $\mathbb{Z}_{11}^*$:

$$6,\ 3,\ 7,\ 9,\ 10,\ 5,\ 8,\ 4,\ 2,\ 1.$$

Torej je

$$\log_6 2 = 9.$$

□

(15) Določi jezika, ki ju sprejmeta naslednja avtomata:

(a) $(\{p, q\}, \{a, b\}, \delta, p, \{q\})$, kjer je prehodna funkcija δ definirana s predpisom:

	a	b
p	q	p
q	p	q

(b) $(\{p, q, r\}, \{a, b\}, \delta, p, \{r\})$, kjer je prehodna funkcija δ definirana s predpisom:

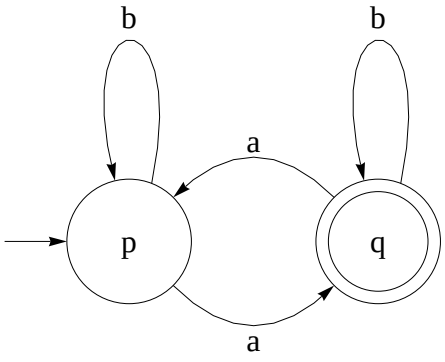
	a	b
p	q	p
q	q	r
r	q	p

Rešitev: Deterministični končni avtomat lahko podamo s peterico $(Q, \Sigma, \delta, q_0, F)$, kjer je:

- Q končna množica stanj,
- Σ abeceda,
- δ prehodna funkcija,
- q_0 začetno stanje,
- F množica sprejemnih stanj.

Avtomat kot vhodni podatek sprejme neko besedo iz črk abecede in se glede na prehodno funkcijo premika med različnimi stanji. Če konča v stanju iz množice sprejemnih stanj, rečemo, da besedo sprejme, sicer pa jo zavrne.

(a) Dani avtomat si lahko grafično predstavljamo z naslednjim diagramom



Puščice diagrama nam povedo, kako se premikamo med stanji, ko preberemo dano črko. Da je začetno stanje avtomata p poudarimo tako, da narišemo puščico brez začetka, ki kaže v stanje p. Poglejmo si na primeru besede *abbabaa*, kako deluje avtomat:

$$p \xrightarrow{a} q \xrightarrow{b} q \xrightarrow{b} q \xrightarrow{a} p \xrightarrow{b} p \xrightarrow{a} q \xrightarrow{a} p.$$

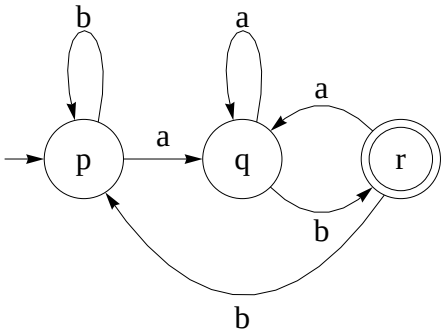
Ker stanje p ne leži v množici sprejemnih stanj, avtomat besedo *abbabaa* zavrne. Če bi vzeli na primer besedo *abaa*, pa bi dobili

$$p \xrightarrow{a} q \xrightarrow{b} q \xrightarrow{a} p \xrightarrow{a} q,$$

kar pomeni, da avtomat to besedo sprejme.

Če dobro pogledamo, kako avtomat deluje, vidimo, da črka b ne spreminja stanja, črka a pa stanji zamenja. Avtomat torej sprejme besede, ki vsebujejo liho mnogo a-jev.

(b) Ta avtomat lahko predstavimo z diagramom



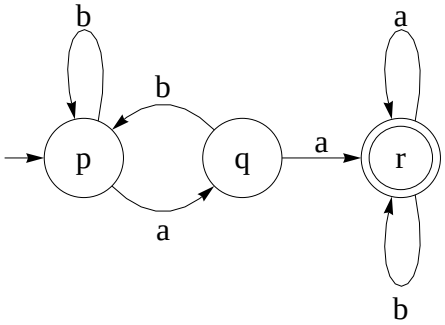
Če avtomat neko besedo sprejme, mora biti zadnja črka nujno b, predzadnja pa posledično a. Preverimo lahko, da avtomat sprejme vse besede, ki se končajo na ab. □

(16) Poišči avtomata, ki sprejmeta besede iz naslednjih jezikov nad abecedo $\Sigma = \{a, b\}$:

(a) Jezik vseh besed, ki vsebujejo dva a-ja zapored.

(b) Jezik vseh besed, ki se začnejo z a.

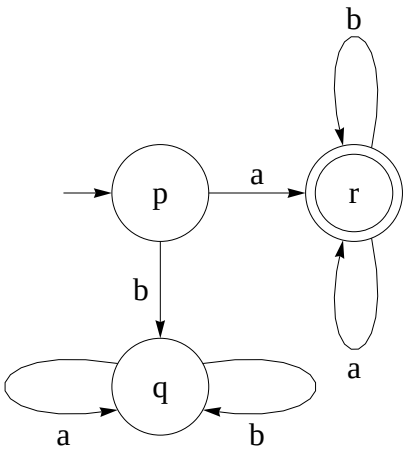
Rešitev: (a) Takšen avtomat je recimo



Njegovo prehodno funkcijo lahko predstavimo s tabelo

	a	b
p	q	p
q	r	p
r	r	r

(b) Sedaj lahko vzamemo avtomat



s prehodno funkcijo

	a	b
p	r	q
q	q	q
r	r	r

□

(17) Opiši orbite naslednjih delovanj grupe $(\mathbb{R}, +)$ na $\mathbb{R}^2$:

(a) Delovanja $\mu : \mathbb{R}^2 \times \mathbb{R} \to \mathbb{R}^2$, ki je dano s predpisom $\mu((x, y), t) = (e^t x, e^t y)$.

(b) Delovanja $\mu : \mathbb{R}^2 \times \mathbb{R} \to \mathbb{R}^2$, ki je dano s predpisom $\mu((x, y), t) = (e^t x, e^{-t} y)$.

Rešitev: Pri tej nalogi je prostor stanj neskončen, delovanje pa si lahko predstavljamo kot dinamični sistem. Če si izberemo nek $(x, y) \in \mathbb{R}^2$, lahko preslikavo

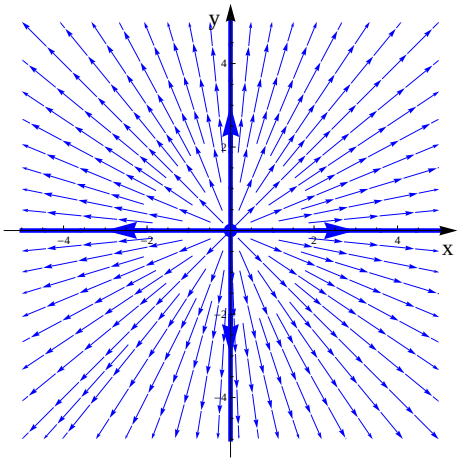
$$t \mapsto \mu((x, y), t)$$

interpretiramo kot gibanje točke (x, y). Ob času $t = 0$ je v začetnem položaju (x, y), ko t preteče vsa realna števila, pa opiše neko krivuljo v ravnini, ki ji rečemo orbita delovanja. Kadar točka (x, y) ves čas miruje, ji rečemo fiksna točka. V tem primeru je njena orbita kar točka sama.

(a) V primeru delovanja $\mu((x, y), t) = (e^t x, e^t y)$ imamo naslednje orbite:

- Točka $(0, 0)$ je fiksna točka delovanja.
- Če je $(x, y) \neq (0, 0)$, je orbita skozi točko (x, y) odprt polneskončen poltrak z začetkom v izhodišču, ki gre skozi točko (x, y).

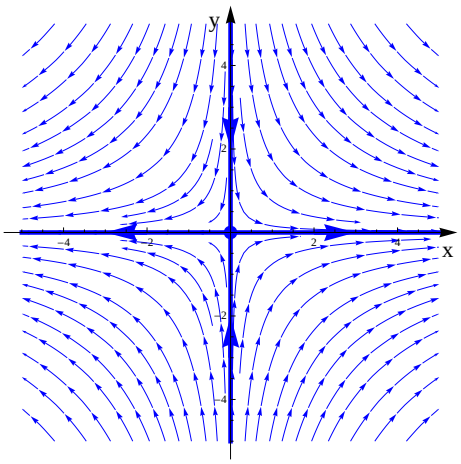
Grafično si lahko orbite predstavljamo kot tokovnice vektorskega polja $\vec{v}(x, y) = (x, y)$.



(b) V primeru delovanja $\mu((x,y),t) = (e^t x, e^{-t} y)$ pa so orbite naslednje množice:

- Točka $(0,0)$ je fiksna točka delovanja.
- Če je $(x,y) \neq (0,0)$ in če točka (x,y) leži na eni izmed koordinatnih osi, je orbita skozi točko (x,y) odprt polneskončen poltrak z začetkom v izhodišču, ki gre skozi točko (x,y).
- Če točka leži v notranjosti enega izmed kvadrantov, je ustrezna orbita veja hiperbole $xy = C$, ki gre skozi dano točko.

Orbite si tokrat lahko predstavljamo kot tokovnice vektorskega polja $\vec{v}(x,y) = (x,-y)$.



□

Izbrana poglavja iz matematike
7. sklop nalog

Kolobarji in obsegi

(1) Poišči vse obrnljive elemente in vse delitelje niča v kolobarjih $\mathbb{Z}$, $\mathbb{Z}_{10}$ in $M_2(\mathbb{R})$.

Rešitev: Kolobar je algebraična struktura, ki jo tvori množica K skupaj z operacijama seštevanja in množenja, ki zadoščata pogojem:

- za seštevanje je K Abelova grupa z enoto 0,
- za množenje je K je monoid z enoto 1,
- operaciji seštevanja in množenja sta povezani z distributivnostnima zakonoma:

$$a(b+c) = ab + ac,$$
$$(a+b)c = ac + bc,$$

ki morata veljati za vse $a, b, c \in K$.

V splošnem ne zahtevamo komutativnosti množenja. Če je tudi množenje komutativno, rečemo, da je kolobar *komutativen*. Element $x \in K$ je *obrnljiv*, če obstaja tak element $x^{-1} \in K$, da velja

$$xx^{-1} = x^{-1}x = 1.$$

Element $x \in K$ je *delitelj niča*, če obstaja neničeln element $y \in K$, da je $xy = 0$ ali $yx = 0$.

Kolobar $\mathbb{Z}$:

V kolobarju celih števil $\mathbb{Z}$ ni netrivialnih deliteljev niča, obrnljiva pa sta samo elementa 1 in -1.

Kolobar $\mathbb{Z}_{10}$:

V kolobarju ostankov $\mathbb{Z}_{10}$ so obrnljivi elementi $\{1, 3, 7, 9\}$. Vsi ostali elementi pa so delitelji niča, kar sledi iz naslednjih kongruenc:

$$2 \cdot 5 \equiv 0 \mod 10,$$
$$4 \cdot 5 \equiv 0 \mod 10,$$
$$6 \cdot 5 \equiv 0 \mod 10,$$
$$8 \cdot 5 \equiv 0 \mod 10.$$

Kolobar $M_2(\mathbb{R})$:

V kolobarju 2×2 realnih matrik so obrnljive natanko matrike z neničelno determinanto. Matrike, ki imajo determinanto enako nič, pa so obenem delitelji niča. Vsaka taka matrika A ima namreč vzporedni vrstici in je zato oblike

$$\begin{bmatrix} a & b \\ ca & cb \end{bmatrix}$$

za neka realna števila a, b in c. Potem lahko preverimo, da velja

$$\begin{bmatrix} a & b \\ ca & cb \end{bmatrix} \cdot \begin{bmatrix} b & b \\ -a & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Opomba: Kolobarju, v katerem so vsi neničelni elementi obrnljivi, rečemo *obseg*. Znani so obsegi racionalnih, realnih in kompleksnih števil in pa obsegi ostankov po praštevilskem modulu. Ti obsegi so vsi komutativni. Poleg teh se pogosto uporabljajo še Galoisovi obsegi (ti so končni in komutativni) ter obseg kvaternionov (ta obseg je nekomutativen).

Če kolobar nima deliteljev niča, mu rečemo *cel kolobar*. Celi kolobarji so posplošitve celih števil, tipični predstavniki pa so kolobarji polinomov s koeficienti v nekem obsegu. □

(2) Naj bo $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ kolobar Gaussovih celih števil.

(a) Poišči vse obrnljive elemente $\mathbb{Z}[i]$.

(b) Katera naravna števila so nerazcepna v $\mathbb{Z}[i]$?

Rešitev: (a) Vzemimo poljubno neničelno Gaussovo celo število $a + bi$ in ga za trenutek smatrajmo kot kompleksno število. Njegova obratna vrednost je potem

$$(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Če hočemo, da bo število $a + bi$ obrnljivo v kolobarju $\mathbb{Z}[i]$, morata biti $\frac{a}{a^2+b^2}$ in $\frac{b}{a^2+b^2}$ celi števili. Hitro se lahko prepričamo, da tem pogojem ustrezajo samo štiri števila

$$1, -1, i, -i.$$

(b) Za Gaussovo celo število $x \neq 1$ rečemo, da je nerazcepno, če iz razcepa $x = yz$ sledi, da je ali y ali pa z obrnljiv element. Nerazcepni elementi so posplošitev praštevil.

Ker so naravna števila hkrati tudi Gaussova cela števila, nas bo zanimalo, katera naravna števila lahko razcepimo v kolobarju $\mathbb{Z}[i]$. Če lahko neko naravno število razcepimo v celih številih, je ta razcep dober tudi v kolobarju Gaussovih celih števil, zato so potencialni nerazcepni elementi samo praštevila. Števili 2 in 5 lahko razcepimo v obliki

$$2 = (1 + i)(1 - i),$$
$$5 = (1 + 2i)(1 - 2i),$$

kar pomeni, da vsa praštevila niso nerazcepna. Ločili bomo dva primera. Vsako liho praštevilo zadošča eni izmed naslednjih kongruenc:

$$p \equiv 1 \mod 4,$$
$$p \equiv 3 \mod 4.$$

Če je praštevilo p oblike $p = 4k+1$, ga lahko zapišemo v obliki vsote kvadratov $p = a^2+b^2$, od koder dobimo razcep

$$p = (a + bi)(a - bi).$$

Denimo sedaj, da je praštevilo p oblike $p = 4k + 3$ in da obstaja razcep

$$p = (a + bi)(c + di).$$

Kvadrata absolutnih vrednosti zgornjih števil potem zadoščata enakosti

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Ker zahtevamo, da elementa $a + bi$ in $c + di$ nista obrnljiva, je $a^2 + b^2 > 1$ in $c^2 + d^2 > 1$ in posledično

$$a^2 + b^2 = c^2 + d^2 = p.$$

V tem primeru bi torej število p lahko zapisali kot vsoto kvadratov dveh števil. Vsota kvadratov pa ne more dati ostanka tri po modulu štiri, kar pomeni, da dani razcep ni možen.

V kolobarju Gaussovih celih števil so torej nerazcepna natanko praštevila oblike $4k+3$. □

(3) Poišči največji skupni delitelj Gaussovih celih števil 30 in $-2 + 6i$ in ju nato zapiši kot produkt nerazcepnih elementov.

Rešitev: Na kolobarju Gaussovih celih števil $\mathbb{Z}[i]$ lahko definiramo normo s predpisom

$$N(a + bi) = a^2 + b^2$$

za poljuben $a+bi \in \mathbb{Z}[i]$. Z uporabo norme lahko definiramo *največji skupni delitelj* števil $a, b \in \mathbb{Z}[i]$ kot število $D(a, b) \in \mathbb{Z}[i]$, ki deli a in b in ima največjo normo izmed vseh skupnih deliteljev. Največji skupni delitelj je določen do obrnljivega elementa natančno.

Za izračun največjega skupnega delitelja uporabljamo prirejen Evklidov algoritem, ki temelji na dejstvu, da lahko za vsak par Gaussovih celih števil a in b zapišemo

$$a = kb + r.$$

Pri tem mora veljati $N(a) > N(b)$, število r pa lahko izberemo tako, da je $N(r) < N(b)$. Po končnem številu takšnih korakov pridemo do največjega skupnega delitelja danih števil.

V našem primeru je $D(30) = 900$ in $D(-2 + 6i) = 40$, zato bomo izbrali $a = 30$ in $b = -2 + 6i$. Sledi

$$\frac{30}{-2 + 6i} = \frac{30(-2 - 6i)}{40} = -\frac{3}{2} - \frac{9}{2}i.$$

Kvocient ni Gaussovo celo število, kar pomeni, da a ni deljiv z b. Kot količnik v takem primeru vzamemo Gaussovo celo število, ki je najbližje številu a/b. Če jih je več, lahko izberemo katerokoli izmed njih. Izberimo na primer $k = -2 - 5i$. Potem je

$$r = a - kb = 30 - (-2 - 5i)(-2 + 6i) = 30 - 4 + 12i - 10i - 30 = -4 + 2i.$$

V naslednjem koraku sedaj postopek ponovimo za par števil b in r. Velja

$$\frac{-2 + 6i}{-4 + 2i} = \frac{(-2 + 6i)(-4 - 2i)}{20} = \frac{8 - 24i + 4i + 12}{20} = 1 - i.$$

Kvocient je sedaj Gaussovo celo število, kar pomeni, da je

$$-2 + 6i = (-4 + 2i)(1 - i) + 0,$$

zato lahko postopek končamo. Največji skupni delitelj danih števil je torej

$$D(30, -2 + 6i) = -4 + 2i.$$

Razcep števil a in b kot produkt nerazcepnih faktorjev pa je enak

$$30 = 2 \cdot 3 \cdot 5 = (1+i)(1-i)3(-2+i)(-2-i),$$
$$-2+6i = 2(-1+3i) = (1+i)(1-i)(1-i)(-2+i).$$

□

(4) Poišči vse nerazcepne polinome stopnje največ 3 v kolobarju polinomov $\mathbb{Z}_2[x]$.

Rešitev: Najprej naštejmo vse nekonstantne polinome stopnje največ 3 s koeficienti v $\mathbb{Z}_2$:

stopnja 1 : $x, x+1$,
stopnja 2 : $x^2, x^2+x, x^2+1, x^2+x+1$,
stopnja 3 : $x^3, x^3+x^2, x^3+x, x^3+1, x^3+x^2+x, x^3+x^2+1, x^3+x+1, x^3+x^2+x+1$.

Polinom stopnje največ 3 je nerazcepen natanko takrat, ko nima ničel. Z uporabo tega dejstva lahko preverimo, da so v kolobarju $\mathbb{Z}_2[x]$ nerazcepni naslednji polinomi:

stopnja 1 : $x, x+1$,
stopnja 2 : x^2+x+1,
stopnja 3 : x^3+x^2+1, x^3+x+1.

Nerazcepne polinome dane stopnje je težko najti, obstaja pa vsaj eden nerazcepen polinom poljubne stopnje $n \geq 1$. □

(5) Zapiši tabeli za seštevanje in množenje v Galoisovem obsegu $GF(2^2)$, ki je definiran z nerazcepnim polinomom $p(x) = x^2 + x + 1$.

Rešitev: Poleg obsegov ostankov $\mathbb{Z}_p$ poznamo še en tip končnih obsegov, ki jim rečemo Galoisovi obsegi. Izkaže se, da za vsako praštevilo p in vsako naravno število n obstaja natanko en obseg, ki ga označimo z $GF(p^n)$. Konstruiramo ga lahko s pomočjo polinomov na naslednji način:

- Izberemo nerazcepen polinom stopnje n v kolobarju $\mathbb{Z}_p[x]$.
- Elementi $GF(p^n)$ so polinomi stopnje največ $n-1$ v $\mathbb{Z}_p[x]$, ki jih lahko interpretiramo tudi kot ostanke pri deljenju s polinomom $p(x)$.
- Seštevanje je definirano kot seštevanje polinomov.
- Produkt dveh polinomov dobimo tako, da najprej izračunamo njun produkt v $\mathbb{Z}_p[x]$, nato pa vzamemo ostanek pri deljenju s polinomom $p(x)$.

V našem primeru je

$$GF(2^2) = \{0, 1, x, 1+x\}$$

operaciji seštevanja in množenja pa lahko predstavimo s tabelama:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

.

Množica vseh elementov obsega zmeraj tvori grupo za seštevanje, ki je v našem primeru izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. Grupa obrnljivih elementov Galoisovega obsega $GF(2^2)$ pa je izomorfna grupi $\mathbb{Z}_3$. Bolj splošno velja, da je grupa obrnljivih elementov končnega obsega vedno izomorfna ciklični grupi. □

(6) Obseg $GF(2^8)$ definiramo z nerazcepnim polinomom $p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_8[x]$.

(a) Izračunaj vsoto polinomov $s(x) = x^6 + x^4 + x + 1$ in $t(x) = x^7 + x^6 + x^2 + 1$ v $GF(2^8)$.

(b) Izračunaj produkt polinomov $s(x) = x^6 + x^2 + 1$ in $t(x) = x^5 + x^3 + x$ v $GF(2^8)$.

(c) Izračunaj inverz polinoma $q(x) = x^5 + x + 1$ v $GF(2^8)$.

Rešitev: (a) Vsota danih polinomov je

$$s(x) + t(x) = x^7 + x^4 + x^2 + x.$$

(b) Najprej izračunajmo produkt polinomov s in t v kolobarju $\mathbb{Z}_8[x]$

$$s(x)t(x) = (x^6 + x^2 + 1)(x^5 + x^3 + x) = x^{11} + x^9 + x.$$

Pri deljenju polinoma $x^{11} + x^9 + x$ s polinomom $p(x)$ dobimo kvocient $x^3 + x$ in ostanek $x^7 + x^6 + x^5 + x^3 + x^2$. V obsegu $GF(2^8)$ torej velja

$$s(x) \cdot t(x) = x^7 + x^6 + x^5 + x^3 + x^2.$$

(c) Inverz polinomov v Galoisovih obsegih iščemo s pomočjo posplošenega Evklidovega algoritma.

r_i	x_i	y_i	k_i
$x^8 + x^4 + x^3 + x + 1$	1	0	
$x^5 + x + 1$	0	1	
$x + 1$	1	x^3	x^3
1	$x^4 + x^3 + x^2 + x$	$x^7 + x^6 + x^5 + x^4 + 1$	$x^4 + x^3 + x^2 + x$

Ta tabela temelji na izračunih:

$$x^8 + x^4 + x^3 + x + 1 = x^3 \cdot (x^5 + x + 1) + x + 1,$$
$$x^5 + x + 1 = (x^4 + x^3 + x^2 + x) \cdot (x + 1) + 1,$$

iz nje pa lahko preberemo, da velja

$$q(x)^{-1} = x^7 + x^6 + x^5 + x^4 + 1.$$

□

(7) Z uporabo kvaternionov zavrti vektor $\vec{r} = (x, y, z)$ za kot $\phi = 90°$ okoli osi $\vec{e} = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0\right)$.

Rešitev: Kvaternioni so števila oblike

$$q = \alpha + xi + yj + zk = \alpha + \vec{r},$$

kjer so α, x, y, z realna števila, i, j in k pa imaginarne enote. Vektorje v $\mathbb{R}^3$ lahko pri tem zapisu identificiramo s kvaternioni, ki imajo skalarni del enak nič. Podobno kot pri kompleksnih številih imamo tudi pri kvaternionih konjugiranje

$$q^* = \alpha - \vec{r},$$

množenje kvaternionov pa je definirano z enakostmi

$$i^2 = j^2 = k^2 = -1$$

in

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

Za rotiranje vektorjev s pomočjo kvaternionov lahko uporabimo formulo

$$R(\vec{e}, \phi) \cdot \vec{r} = q\,\vec{r}\,q^*,$$

kjer je $q = \cos\frac{\phi}{2} + \sin\frac{\phi}{2}\vec{e}$.

V našem primeru je $\phi = 90°$ in $\vec{e} = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0\right)$, kar nam da

$$q = \frac{1}{2}\left(\sqrt{2} + i + j\right),$$
$$q^* = \frac{1}{2}\left(\sqrt{2} - i - j\right).$$

Sedaj bomo izračunali, kako se zavrtijo bazni vektorji:

$$\begin{aligned}
R(\vec{e}, \phi) \cdot \vec{i} &= \frac{1}{2}\left(\sqrt{2} + i + j\right) \cdot i \cdot \frac{1}{2}\left(\sqrt{2} - i - j\right) = \frac{1}{4}\left(\sqrt{2}i - 1 - k\right)\left(\sqrt{2} - i - j\right), \\
&= \frac{i}{2} + \frac{j}{2} - \frac{\sqrt{2}}{2}k, \\
R(\vec{e}, \phi) \cdot \vec{j} &= \frac{1}{2}\left(\sqrt{2} + i + j\right) \cdot j \cdot \frac{1}{2}\left(\sqrt{2} - i - j\right) = \frac{1}{4}\left(\sqrt{2}j + k - 1\right)\left(\sqrt{2} - i - j\right), \\
&= \frac{i}{2} + \frac{j}{2} + \frac{\sqrt{2}}{2}k, \\
R(\vec{e}, \phi) \cdot \vec{k} &= \frac{1}{2}\left(\sqrt{2} + i + j\right) \cdot k \cdot \frac{1}{2}\left(\sqrt{2} - i - j\right) = \frac{1}{4}\left(\sqrt{2}k - j + i\right)\left(\sqrt{2} - i - j\right), \\
&= \frac{\sqrt{2}}{2}i - \frac{\sqrt{2}}{2}j.
\end{aligned}$$

Od tod sledi, da rotaciji $R(\vec{e}, \phi)$ ustreza rotacijska matrika

$$Q = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{\sqrt{2}}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \end{bmatrix}$$

□

2. sklop dodatnih vaj iz Izbranih poglavij iz matematike

(1) Reši diofantske enačbe:

(a) $31x + 41y = 3$,
(b) $67x + 23y = 1$,
(c) $288x + 30y = 6$.

Rešitev:

(a) $x = 12 - 41k$, $y = -9 + 31k$, $k \in \mathbb{Z}$,
(b) $x = 11 - 23k$, $y = -32 + 67k$, $k \in \mathbb{Z}$,
(c) $x = 2 - 5k$, $y = -19 + 48k$, $k \in \mathbb{Z}$.

(2) Reši sistema kongruenc:

(a) $x \equiv 1 \pmod 2$,
$x \equiv 3 \pmod 4$,
$x \equiv 1 \pmod 5$,
$x \equiv 4 \pmod 7$,
$x \equiv 7 \pmod 8$,
(b) $x \equiv 14 \pmod{35}$,
$x \equiv 39 \pmod{75}$.

Rešitev:

(a) $x \equiv 151 \pmod{280}$,
(b) $x \equiv 189 \pmod{525}$.

(3) Oseba A za prejemanje sporočil uporablja RSA-šifro z javnim ključem $n = 391$, $e = 235$.

(a) Poišči privatni ključ.
(b) Oseba B je osebi A poslala šifrirano sporočilo 188 365 1. Poišči vsebino sporočila, če črke ustrezajo številom od 1 do 25.

Rešitev:

(a) $d = 3$,
(b) RSA.

(4) Bijekciji $f, g : \mathbb{Z}_{17} \to \mathbb{Z}_{17}$ sta dani s predpisoma:

$$f(x) = 2x,$$
$$g(x) = x^3.$$

Poišči reda bijekcij f in g, če ju smatramo kot elementa simetrične grupe S_{17}.

Rešitev: Bijekcija f ima red 8, bijekcija g pa red 4.

(5) Kolikšen je maksimalen red, ki ga lahko ima element grupe S_{12}?

Rešitev: Maksimalen možni red je 60. Takšen red ima na primer permutacija

$$(1\,2\,3\,4\,5)(6\,7\,8\,9)(10\,11\,12).$$

(6) Poišči vse homomorfizme grup:

(a) $\mathbb{Z}_8 \to S_3$,
(b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$,
(c) $\mathbb{Z}_4 \to \mathbb{Z}_3$.

Rešitev:

(a) Vsak homomorfizem $\phi : \mathbb{Z}_8 \to S_3$ je določen z vrednostjo $\phi(1)$. Ker mora red elementa $\phi(1)$ deliti 8, dobimo štiri možnosti:

$$\phi(1) = (1)(2)(3),$$
$$\phi(1) = (1\,2)(3),$$
$$\phi(1) = (1\,3)(2),$$
$$\phi(1) = (1)(2\,3).$$

(b) Homomorfizem $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ je določen s slikama elementov $(1, 0)$ in $(0, 1)$, ki morata imeti red 1 ali 2. Tako dobimo naslednje možnosti:

$$\phi(1,0) = 0,\ \phi(0,1) = 0,$$
$$\phi(1,0) = 2,\ \phi(0,1) = 0,$$
$$\phi(1,0) = 0,\ \phi(0,1) = 2,$$
$$\phi(1,0) = 2,\ \phi(0,1) = 2.$$

(c) Edini možni homomorfizem $\phi : \mathbb{Z}_4 \to \mathbb{Z}_3$ je ničelni homomorfizem.

(7) Poišči vse Abelove grupe reda 36.

Rešitev: Do izomorfizma natanko so to grupe:

$$G \cong \mathbb{Z}_{36},$$
$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3,$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9,$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

(8) Poišči vse podgrupe grup $\mathbb{Z}_2 \times \mathbb{Z}_4$ in S_3.

Rešitev:

Podgrupe grupe $\mathbb{Z}_2 \times \mathbb{Z}_4$ so:

$$\begin{aligned}
H_1 &= \{(0,0)\},\\
H_2 &= \mathbb{Z}_2 \times \mathbb{Z}_4,\\
H_3 &= \{(0,0),(1,0)\} \cong \mathbb{Z}_2,\\
H_4 &= \{(0,0),(0,1),(0,2),(0,3)\} \cong \mathbb{Z}_4,\\
H_5 &= \{(0,0),(0,2)\} \cong \mathbb{Z}_2,\\
H_6 &= \{(0,0),(1,2)\} \cong \mathbb{Z}_2,\\
H_7 &= \{(0,0),(1,1),(0,2),(1,3)\} \cong \mathbb{Z}_4,\\
H_8 &= \{(0,0),(1,2),(1,0),(0,2)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

Podgrupe grupe S_3 so:

$$\begin{aligned}
H_1 &= \{(1)(2)(3)\},\\
H_2 &= S_3,\\
H_3 &= \{(1)(2)(3),(1\,2)(3)\} \cong \mathbb{Z}_2,\\
H_4 &= \{(1)(2)(3),(1\,3)(2)\} \cong \mathbb{Z}_2,\\
H_5 &= \{(1)(2)(3),(1)(2\,3)\} \cong \mathbb{Z}_2,\\
H_6 &= \{(1)(2)(3),(1\,2\,3),(1\,3\,2)\} \cong \mathbb{Z}_3.
\end{aligned}$$

(9) Grupa G je podana s tabelo

$\circ$	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	e	c	g	b	f	1	d
b	b	c	f	1	e	g	d	a
c	c	g	1	a	f	d	b	e
d	d	b	e	f	a	c	g	1
e	e	f	g	d	c	1	a	b
f	f	1	d	b	g	a	e	c
g	g	d	a	e	1	b	c	f

.

(a) Poišči rede vseh elementov grupe G.

(b) Ugotovi, kateri znani grupi je izomorfna grupa G in poišči eksplicitni izomorfizem.

Rešitev:

(a) Redi elementov grupe G so: $\mathrm{red}(1) = 1$, $\mathrm{red}(a) = 4$, $\mathrm{red}(b) = 8$, $\mathrm{red}(c) = 8$, $\mathrm{red}(d) = 8$, $\mathrm{red}(e) = 2$, $\mathrm{red}(f) = 4$ in $\mathrm{red}(g) = 8$.

(b) Grupa G je izomorfna grupi $\mathbb{Z}_8$. Eksplicitni izomorfizem $\phi : G \to \mathbb{Z}_8$ je podan s predpisom:

$$\begin{aligned}\phi(1) &= 0,\\ \phi(a) &= 2,\\ \phi(b) &= 7,\\ \phi(c) &= 1,\\ \phi(d) &= 5,\\ \phi(e) &= 4,\\ \phi(f) &= 6,\\ \phi(g) &= 3.\end{aligned}$$

(10) Poišči največja skupna delitelja naslednjih Gaussovih celih števil:

(a) $a = 11 + 3i$ in $b = 1 + 8i$,
(b) $a = 32 + 9i$ in $b = 4 + 11i$.

Rešitev:

(a) $D(a, b) = -1 + 2i$,
(b) $D(a, b) = 1$.

(11) Na kolobarju $K = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ definirajmo normo s predpisom

$$N(a + b\sqrt{5}i) = a^2 + 5b^2.$$

(a) Pokaži, da za normo velja enakost $N(ab) = N(a)N(b)$ za poljubna $a, b \in K$ in nato poišči vse obrnljive elemente K.
(b) Ali v kolobarju K velja izrek o enolični faktorizaciji?

Rešitev:

(a) Obrnljiva sta elementa 1 in -1.
(b) Ne. Protiprimer je $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$.

(12) (a) Pokaži, da je polinom $p(x) = x^4 + x^3 + 1$ nerazcepen v kolobarju $\mathbb{Z}_2[x]$.
(b) Poišči vse nerazcepne kvadratne polinome v kolobarju $\mathbb{Z}_3[x]$.

Rešitev: Če se omejimo na polinome z vodilnim koeficientom 1, so v kolobarju $\mathbb{Z}_3[x]$ nerazcepni naslednji kvadratni polinomi:

$$\begin{aligned}p_1(x) &= x^2 + 1,\\ p_2(x) &= x^2 + x + 2,\\ p_3(x) &= x^2 + 2x + 2.\end{aligned}$$

(13) Naj bo Galoisov obseg $GF(3^2)$ definiran s polinomom $p(x) = x^2+x+2 \in \mathbb{Z}_3[x]$.

(a) Kateri grupi je izomorfna grupa $(GF(3^2), +)$?

(b) Kateri grupi je izomorfna grupa obrnljivih elementov obsega $GF(3^2)$?

Rešitev:

(a) Grupa $(GF(3^2), +)$ je izomorfna grupi $\mathbb{Z}_3 \times \mathbb{Z}_3$. Ekspliciten izomorfizem $\phi : (GF(3^2), +) \to \mathbb{Z}_3 \times \mathbb{Z}_3$ je:

$$\phi(ax + b) = (a, b).$$

(b) Grupa obrnljivih elementov obsega $GF(3^2)$ je izomorfna ciklični grupi $\mathbb{Z}_8$. Eden izmed generatorjev je polinom x, njegove potence pa so

$$x,\ 2x + 1,\ 2x + 2,\ 2,\ 2x,\ x + 2,\ x + 1,\ 1.$$

(14) Naj bo obseg $GF(2^8)$ definiran s polinomom $p(x) = x^8+x^6+x^5+x+1 \in \mathbb{Z}_8[x]$.

(a) Izračunaj produkt polinomov $s(x) = x^6 + x^3$ in $t(x) = x^7 + x^5 + x^2 + 1$ v $GF(2^8)$.

(b) Izračunaj inverz polinoma $q(x) = x^3 + x^2 + 1$ v $GF(2^8)$.

Rešitev:

(a) $s(x) \cdot t(x) = x^3$.

(b) $q(x)^{-1} = x^6 + x^4 + x^2$.

(15) Z uporabo kvaternionov zavrti vektor (x, y, z) za kot $\phi = 60^\circ$ okoli premice s smernim vektorjem $\vec{s} = (1, 1, 1)$.

Rešitev:

$$R(x, y, z) = \begin{bmatrix} \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{2}{3} \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$