UNIVERZA V LJUBLJANI
PEDAGOŠKA FAKULTETA

TILEN MIKLAVEC

GRUPA OBRNLJIVIH ELEMENTOV KOLOBARJA $\mathbb{Z}_n$

MAGISTRSKO DELO

LJUBLJANA, 2019

UNIVERZA V LJUBLJANI

PEDAGOŠKA FAKULTETA

POUČEVANJE, PREDMETNO POUČEVANJE

TILEN MIKLAVEC

Mentor: izr. prof. dr. Primož Šparl

GRUPA OBRNLJIVIH ELEMENTOV KOLOBARJA $\mathbb{Z}_n$

Magistrsko delo

LJUBLJANA, 2019

Zahvala

Za strokovno vodenje in pomoč pri izdelavi magistrskega dela se iskreno zahvaljujem svojemu mentorju, izr. prof. dr. Primožu Šparlu.

Iskrena hvala moji družini in dekletu za razumevanje, spodbudo in zaupanje, ki sem ga bil deležen v času študija.

Tilen Miklavec

Povzetek

V magistrskem delu proučujemo kolobarje in njihove grupe obrnljivih elementov. Obrnljivi elementi poljubnega kolobarja z enico namreč tvorijo grupo za pripadajočo multiplikativno operacijo. V posebnem primeru kolobarja $\mathbb{Z}_n$ gre za *grupo obrnljivih elementov* U_n, ki ji rečemo tudi *grupa enot*. Glavni namen magistrskega dela je predstaviti kolobar $\mathbb{Z}_n$ in ugotoviti, kateri znani grupi je izomorfna grupa obrnljivih elementov U_n. Zanima nas tudi, kdaj je ta grupa ciklična. V ta namen natančno opišemo strukturo grupe obrnljivih elementov U_n in jo zapišemo kot direktni produkt samih cikličnih grup. V magistrskem delu pokažemo tudi, kako si lahko z rezultati o strukturi grupe U_n pomagamo pri reševanju nekaterih kongruenčnih enačb.

Klasifikacija MSC (2010): 16U60, 13A05, 11A07

Ključne besede: kolobar $\mathbb{Z}_n$, grupa obrnljivih elementov, ciklična grupa, primitivni koren

Title: The group of units of the ring $\mathbb{Z}_n$

Abstract

In the master's thesis we study finite rings and their groups of units. The invertible elements of an arbitrary ring with a multiplicative identity form a group for the corresponding multiplicative operation. In the special case of the ring $\mathbb{Z}_n$, this is a group denoted by U_n, also called the group of units. The main purpose of the thesis is to introduce the ring $\mathbb{Z}_n$ and to determine, for each integer n, the well known group that the group of units U_n is isomorphic to. We also determine the necessary and sufficient condition on n for the group U_n to be cyclic. To this end, we investigate the structure of the group of units U_n and show that we can write it as a direct product of certain cyclic groups. We also indicate how our results can be used for solving some congruence equations.

MSC(2010) classification: 16U60, 13A05, 11A07

Keywords: ring $\mathbb{Z}_n$, group of units, cyclic group, primitive root

Kazalo

Poglavje 1

Uvod

Vsebina magistrskega dela sodi predvsem na področje teorije števil, saj v prvi vrsti raziskujemo nekatere značilnosti celih števil. Ob tem pa precej posega tudi na področje algebre, saj se pri naši obravnavi osredotočimo na nekatere pripadajoče algebrske strukture, kot so kolobarji in grupe. Večino pojmov, ki jih srečamo v okviru tega magistrskega dela, študentje Pedagoške fakultete Univerze v Ljubljani spoznajo pri predmetu algebrske strukture, zato vseh osnovnih pojmov ne bomo navajali. Algebrske strukture, ki imajo vrsto zanimivih lastnosti in bodo predstavljale osrednjo temo magistrskega dela, so grupe in kolobarji. Kolobar je algebrska struktura z dvema operacijama, ki vsaka zase zadoščata ustreznim lastnostim in sta obenem še medsebojno usklajeni (velja distributivnost). Eno od dveh operacij označimo s $+$ in ji rečemo vsota, drugo pa označimo s $\cdot$ in ji rečemo produkt ali množenje v kolobarju. Primeri kolobarjev so $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ in $(\mathbb{C}, +, \cdot)$, kjer gre za običajna seštevanja in množenja celih, racionalnih, realnih in kompleksnih števil. V primeru, da ima kolobar nevtralni element za množenje, lahko obravnavamo množico vseh multiplikativno obrnljivih elementov. Izkaže se, da je ta množica za operacijo množenja grupa. Grupa obrnljivih elementov je lahko bistveno različna za kolobarje, ki so si na prvi pogled precej podobni. Kolobar celih števil $\mathbb{Z}$ ima tako na primer le dva obrnljiva elementa, 1 in -1, in zato je pripadajoča grupa enot izomorfna grupi $\mathbb{Z}_2$. Kolobar racionalnih števil, ki je prav tako neskončen in celo vsebuje kolobar celih števil $\mathbb{Z}$ kot podkolobar, pa ima neskončno grupo enot, saj so obrnljivi vsi njegovi neničelni elementi. Zanimivo se je torej vprašati, kaj nam grupa obrnljivih elementov pove o samem kolobarju.

V magistrskem delu se zato osredotočimo na grupo obrnljivih elementov oziroma grupo enot končnega kolobarja $\mathbb{Z}_n$. Pri opisovanju in raziskovanju strukture grupe obrnljivih elementov kolobarja $\mathbb{Z}_n$ v celoti operiramo s celimi števili in proučujemo njihove lastnosti predvsem v povezavi s pojmom deljivosti in kongruence po danem modulu, zato moramo poznati določene pojme s področja teorije števil. Osnovne rezultate z omenjenega področja, kot sta na primer Eulerjev izrek in Mali Fermatov izrek, smo študentje Pedagoške fakultete Univerze v Ljubljani spoznali pri predmetu abstraktna algebra, vseeno pa velja omeniti eno pomembnejših funkcij na področju teorije števil, ki v magistrskem delu igra pomembno vlogo. To je Eulerjeva φ funkcija, ki nam za poljubno naravno število n vrne število vseh naravnih števil, ki so tuja n in ga ne presegajo. Izkaže se, da Eulerjeva funkcija podaja ravno red grupe obrnljivih elementov kolobarja $\mathbb{Z}_n$. Pomaga nam tudi pri določitvi tistih naravnih števil n, za katera je grupa obrnljivih elementov kolobarja $\mathbb{Z}_n$ ciklična. Potem ko natančno proučimo strukturo grupe obrnljivih elementov kolobarja $\mathbb{Z}_n$, zapišemo izrek, ki pove, kateri znani grupi je izomorfna ta grupa.

Magistrsko delo je sestavljeno takole. V drugem poglavju ponovimo nekatere osnovne pojme algebre in teorije števil, ki so bistveni za razumevanje magistrskega dela. V tretjem poglavju vpeljemo pojem relacije kongruence po modulu n na množici celih števil in nato konstruiramo kolobar celih števil $\mathbb{Z}_n$, ki je temelj nadaljnjemu preučevanju njegovih elementov. Množica vseh njegovih multiplikativno obrnljivih elementov skupaj z operacijo množenja tvori grupo obrnljivih elementov ali grupo enot kolobarja $\mathbb{Z}_n$. V četrtem poglavju obravnavamo vprašanje, kako je cikličnost grupe obrnljivih elementov kolobarja $\mathbb{Z}_n$ odvisna od naravnega števila n. Na koncu tega poglavja določimo vsa naravna števila n, za katera je grupa obrnljivih elementov ciklična. Peto poglavje zaključimo z izrekom, ki nam pove, kateri znani grupi je za dani n izomorfna grupa obrnljivih elementov kolobarja $\mathbb{Z}_n$. Na koncu magistrskega dela s pomočjo dobljenih rezultatov in kitajskega izreka o ostankih prikažemo postopek za reševanje nekaterih kongruenčnih enačb.

Poglavje 2

Teoretična izhodišča

Teoretična izhodišča magistrskega dela so večinoma zajeta v študijski literaturi predmetov logika in množice, algebrske strukture in abstraktna algebra, ki jih med dodiplomskim študijem poslušajo študentje študijskega programa Dvopredmetni učitelj matematike na Pedagoški fakulteti v Ljubljani. Od bralca se pričakuje, da pozna osnovne pojme in nekatere splošno znane izreke teorije grup in teorije števil, a bomo v tem poglavju nekatere izmed njih kljub vsemu navedli, saj so ključnega pomena za razumevanje magistrskega dela.

2.1 Osnovni pojmi

V magistrskem delu obravnavamo grupe obrnljivih elementov kolobarjev z enico in njihove elemente, zato v ta namen najprej definiramo osnovne pojme teorije grup, ki so ključnega pomena za nadaljnje raziskovanje in preučevanje strukture grupe obrnljivih elementov kolobarjev z enico. Pri tem dokaze nekaterih trditev in izrekov izpuščamo, zato bralca vabim, da jih bodisi skuša dokazati sam ali pa si več o njih prebere v navedeni literaturi. V magistrskem delu obravnavamo predvsem končne ciklične grupe, za katere se izkaže, da imajo veliko zanimivih lastnosti, ki se jih da utemeljiti z relativno preprostimi premisleki, zato te grupe najprej definiramo, nato pa spoznamo nekaj njihovih osnovnih lastnosti. Pri preučevanju grup se je naravno vprašati, kdaj sta dve na videz različni grupi strukturno pravzaprav enaki, zato definiramo pojma homomorfizma in izomorfizma grup. Sledi pregled osnovnih pojmov, povezanih s kolobarji in njihovimi elementi. Razdelek

zaključimo še s konceptom izomorfizma kolobarjev. Razdelek je povzet po [3] in [7].

2.1.1 Grupe

Spomnimo se, da je grupa abstraktna matematična struktura, ki smo jo spoznali pri Abstraktni algebri. Definirali smo jo tako, da smo izhajali iz množice in operacije na tej množici.

Definicija. Binarna operacija $*$ na množici S je vsaka preslikava iz kartezičnega produkta $S \times S$ v S, ki vsakemu urejenemu paru (a, b) priredi natanko določen element iz množice S. Običajno jo označujemo z $*$, to je

$$* : S \times S \to S.$$

V nadaljevanju bomo za $a, b, c \in S$ namesto $c = *(a, b)$ pisali $c = a * b$.

Definicija. Urejeni par $(G, *)$, kjer je G neprazna množica in $*$ binarna operacija na G, je *grupa*, če zadošča naslednjim aksiomom:

(i) asociativnost: binarna operacija $*$ je asociativna, to je, za vse $a, b, c \in G$ velja $(a * b) * c = a * (b * c)$.

(ii) identiteta: obstaja element e iz množice G, da velja $e * a = a * e = a$ za vsak $a \in G$. Elementu e pravimo *nevtralni element* grupe G.

(iii) inverz: za vsak $a \in G$ obstaja $a' \in G$, da velja $a' * a = a * a' = e$. Element a' je *inverz* elementa a glede na operacijo $*$ in ga običajno označujemo z a^{-1}.

Ko govorimo o grupi $(G, *)$, znak za binarno operacijo pogosto spuščamo. Tako govorimo o grupi G, na kateri je definirana binarna operacija $*$, za katero je G grupa.

Definicija. Grupa G je *abelska* ali *komutativna*, če je njena binarna operacija $*$ komutativna, torej če velja $a * b = b * a$ za vse $a, b \in G$.

Trditev 2.1.1 *V grupi G z dano operacijo $*$ obstaja le en nevtralni element $e \in G$, da velja $e*a = a*e = a$ za vse $a \in G$. Podobno za vsak $a \in G$ obstaja le en njegov inverz a^{-1}, da velja $a * a^{-1} = a^{-1} * a = e$.*

Dogovorimo se, da za vsak $a \in G$ in nenegativno celo število n namesto $\underbrace{a * a * \ldots * a}_{n}$ pišemo a^n in namesto $\underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{n}$ pišemo a^{-n}. Grupa G je *končna*, če je pripadajoča množica G končna, sicer je grupa *neskončna*. V nadaljevanju govorimo le o končnih grupah.

Definicija. *Red grupe* G, ki ga označujemo z $|G|$, je število vseh elementov pripadajoče množice G.

Definicija. Naj bo G grupa in e njen nevtralni element. *Red elementa* $a \in G$ je najmanjše naravno število n, da je $a^n = e$. Tedaj red elementa a označujemo z $|a|$. Če obstaja najmanjše naravno število m, da je $a^m = e$ za vsak $a \in G$, potem temu številu pravimo *eksponent* grupe G in ga označujemo s $e(G)$.

Opomba. Naj bo G grupa. Za vsak $a \in G$ velja $|a| = |a^{-1}|$.

Definicija. Naj bo G grupa in H neprazna podmnožica množice G. Če množica H s podedovano operacijo tvori grupo, potem pravimo, da je H *podgrupa* grupe G, kar označimo s $H \leq G$.

Izrek 2.1.2 *(Lagrangev izrek). Naj bo G končna grupa in H njena podgrupa. Potem red podgrupe H deli red grupe G.*

Posledica 2.1.3 *V končni grupi red vsakega elementa grupe deli red grupe.*

Definicija. Če je G grupa in $a \in G$, potem je množica

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

podgrupa grupe G, ki jo imenujemo *(ciklična) podgrupa grupe G, generirana z a.* Grupa G je *ciklična grupa*, če velja $G = \langle a \rangle$ za nek $a \in G$. V tem primeru je a *generator* grupe G.

Posledica 2.1.4 *Če je G končna grupa in $a \in G$, potem $a^{|G|} = e$.*

Definicija. Naj bosta $(G, \circ)$ in $(H, \star)$ grupi. Preslikavi $\varphi : G \to H$, za katero za vse $a, b \in G$ velja

$$\varphi(a \circ b) = \varphi(a) \star \varphi(b),$$

rečemo *homomorfizem* grup.

Kot smo se že dogovorili, bomo znak za operacijo določene grupe v splošnem spuščali. Torej zgornjo enakost zapišemo $\varphi(ab) = \varphi(a)\varphi(b)$.
Preslikava φ je *izomorfizem* grup, če velja:

(i) φ je homomorfizem grup, torej velja $\varphi(ab) = \varphi(a)\varphi(b)$, za vse $a, b \in G$, ter

(ii) φ je bijekcija.

Če obstaja izomorfizem grup $\varphi : G \to H$, rečemo, da sta grupi G in H *izomorfni*, kar označimo s $G \cong H$.

Do sedaj smo si ogledali nekatere lastnosti grup, se seznanili s končnimi cikličnimi grupami ter spoznali, kdaj sta dve grupi izomorfni. Sledi definicija direktnega produkta grup.

Definicija. Naj bosta $(G, *)$ in $(H, \star)$ grupi. *Direktni produkt* $(G, *)$ in $(H, \star)$ je množica urejenih parov

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

skupaj z operacijo

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$$

za $g_1, g_2 \in G, h_1, h_2 \in H$.

Izkaže se, da je ta operacija dobro definirana in da je direktni produkt grup z dano operacijo grupa.

Izrek 2.1.5 *Naj bosta G in H grupi in naj bosta $a \in G$ ter $b \in H$. Tedaj je red elementa $(a, b) \in G \times H$ enak najmanjšemu skupnemu večkratniku $v(|a|, |b|)$ redov $|a|$ in $|b|$.*

Izkaže se, da za vsako naravno število n obstaja do izomorfizma natančno natanko ena ciklična grupa reda n in je izomorfna grupi $\mathbb{Z}_n$ za seštevanje, ki jo bomo spoznali v tretjem poglavju.

2.1.2 Kolobarji

V tem razdelku sledi pregled pojmov, povezanih s kolobarji in njihovimi elementi, ki predstavljajo temelj nadaljnjemu preučevanju strukture grupe obrnljivih elementov končnih kolobarjev.

Definicija. *Kolobar* je algebrska struktura $(K, +, \cdot)$ z dvema binarnima operacijama $+$ in $\cdot$. Prvi rečemo vsota in jo označujemo s $+$, drugi pa rečemo množenje ali produkt v kolobarju in jo označujemo s $\cdot$. Ti dve operaciji morata zadoščati naslednjim pogojem:

(i) $(K, +)$ je abelska grupa in ima nevtralni element, ki ga označimo z 0,

(ii) operacija množenja je asociativna, torej velja $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ za vse $a, b, c \in K$, ter

(iii) obe operaciji povezuje distributivnostni zakon, to je, za vse $a, b, c \in K$ velja $a \cdot (b + c) = a \cdot b + a \cdot c$ in $(a + b) \cdot c = a \cdot c + b \cdot c$.

Primeri neskončnih kolobarjev so $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ in $(\mathbb{Q}, +, \cdot)$ za običajno seštevanje in množenje. Na tem mestu le omenimo primer končnega kolobarja, ki ga bomo podrobneje spoznali v naslednjem poglavju, to je kolobar $(\mathbb{Z}_n, +, \cdot)$.

Definicija. Kolobar, v katerem je množenje komutativno, je *komutativen kolobar*. Če v kolobarju K obstaja nevtralni element 1 za operacijo množenja, tako da velja $a \cdot 1 = 1 \cdot a = 1$ za vse $a \in K$, potem takšen kolobar imenujemo *kolobar z enico*.

Trditev 2.1.6 *Naj bo K kolobar z enico* 1. *Tedaj je* 1 *edini nevtralni element za operacijo množenja.*

Dokaz. Denimo, da ima kolobar K dva nevtralna elementa za operacijo množenja, 1 in $1'$. Ker je 1 nevtralni element za operacijo množenja, velja $1 \cdot 1' = 1'$. Ker je $1'$ prav tako nevtralni element, velja $1 \cdot 1' = 1$. Od tod sledi, da je $1 = 1'$, torej imamo zgolj en nevtralni element za operacijo množenja.

□

Definicija. Direktni produkt $K_1 \times K_2 \times \ldots \times K_n$ kolobarjev $K_1, K_2, \ldots, K_n$ definiramo podobno kot direktni produkt grup. Njegovi elementi so n-terke $(k_1, \ldots, k_n)$, pri čemer je $k_i \in K_i$ za vsa naravna števila i, z operacijama seštevanja in množenja po komponentah.

Opomba. Ni se težko prepričati, da na ta način $K_1 \times K_2 \times \ldots \times K_n$ postane kolobar.

Definicija. Naj bosta K in K' poljubna kolobarja. Funkcija $\varphi : K \to K'$ je homomorfizem kolobarjev, če velja $\varphi(r + s) = \varphi(r) + \varphi(s)$ in $\varphi(rs) = \varphi(r)\varphi(s)$ za vse $r, s \in K$. Če je φ bijektivna, ji rečemo *izomorfizem kolobarjev*. Če obstaja izomorfizem med K in K', potem sta kolobarja *izomorfna*, kar označimo s $K \cong K'$.

Poglavje 3

Ekvivalenčne relacije in kolobar $\mathbb{Z}_n$

Glavni namen tega poglavja je, da s pomočjo že znanih rezultatov iz teorije števil in teorije grup konstruiramo kolobar $\mathbb{Z}_n$. V ta namen se najprej spomnimo pojma deljivosti celih števil in zapišemo osnovni izrek o deljenju ter ga tudi dokažemo. Sledi definicija kongruence po modulu n in dokaz nekaterih pomembnih lastnosti te relacije. Kljub temu da smo relacije na množicah spoznali že na začetku študija, vseeno obnovimo osnovne pojme, povezane z njimi, največ pozornosti pa nato namenimo ekvivalenčnim relacijam, ki določajo razbitje množice na ekvivalenčne razrede. Poglavje zaključimo z dokazom, da je $(\mathbb{Z}_n, +, \cdot)$ kolobar. Končni kolobar celih števil $(\mathbb{Z}_n, +, \cdot)$ bo namreč temelj nadaljnjemu delu v okviru tega magistrskega dela.

3.1 Relacije na množici $\mathbb{Z}$

V tem razdelku najprej obnovimo pojem deljivosti celih števil, nato zapišemo ter dokažemo osnovni izrek o deljenju. Spomnimo se pojma kongruence v kolobarju $\mathbb{Z}$, ter kaj so relacije na množicah. Navsezadnje definiramo ekvivalenčne relacije, ekvivalenčne razrede in pripadajočo kvocientno množico ter pokažemo, da sta operaciji seštevanja in množenja po modulu n na tej kvocientni množici dobro definirani. Razdelek je povzet po [3], [6] in [7].

Definicija. (Deljivost celih števil).
Naj bosta a in b celi števili. Rečemo, da celo število b *deli* celo število a, če obstaja tako celo število k, da velja $a = k \cdot b$, kar označimo s $b \mid a$.

Opomba. Naj bodo a, b in c cela števila. Če $a \mid b$ ter $b \mid c$, potem $a \mid c$. Poleg tega velja tudi, da je število 0 deljivo z vsakim neničelnim celim številom b, saj je $0 = 0 \cdot b$.

Naslednji izrek in njegov dokaz je povzet iz [7].

Izrek 3.1.1 *(Osnovni izrek o deljenju). Za poljubni celi števili a in b, pri čemer je $b \neq 0$, obstajata enolično določeni celi števili q in r, pri čemer je $0 \leq r < |b|$, da velja $a = qb + r$.*

Dokaz. Dokažimo izrek za primer, ko sta a in b nenegativni števili, ostale primere pa prepuščam bralcu. Oglejmo si množico $S = \{k \in \mathbb{N} \cup \{0\} \mid a - kb \geq 0\}$. Najprej opazimo, da je množica S neprazna. Ker je $a \geq 0$, namreč množica S vsebuje vsaj število 0. Ker je $b > 0$, je b naravno število. Zaradi neomejenosti naravnih števil obstaja nenegativno celo število k, da je $kb > a$. Množica S ima tako največji element, zato je navzgor omejena. Označimo največji element S s q in definirajmo $r = a - qb$. Ker je $q \in S$, je $r \geq 0$. Če je $r \geq b$, je $a - (q+1)b = r - b \geq 0$, torej je $q + 1 \in S$, kar pa je nemogoče, saj smo q definirali kot največji element množice S. Velja torej $0 \leq r < b$ in $a = qb + r$, s čimer smo zagotovili obstoj števil q in r iz izreka. V samem zaključku dokaza dokažimo še enoličnost celih števil q in r. Naj za $0 \leq r, r' < b$ in $q, q' \in \mathbb{Z}$ velja $qb + r = a = q'b + r'$. Privzemimo, da je $r \geq r'$. Tedaj je $r - r' = (q' - q)b \geq 0$. Če velja $r' \neq r$, je zaradi $r - r' > 0$ tudi $q' \neq q$ in je zato zaradi $b > 0$ potem $r - r' = (q' - q)b \geq b$. A ker velja $0 \leq r, r' < b$, je to nemogoče. Potemtakem je $r = r'$, in ker je $b > 0$, posledično še $q = q'$. □

Opomba. Celemu številu q iz zgornjega izreka rečemo *kvocient*, številu r pa *ostanek* pri deljenju a z b.

Definicija. Naj bosta a in b poljubni celi števili ter naj bo n naravno število. Tedaj rečemo, da je število a *kongruentno* številu b *po modulu* n, kar zapišemo z

$a \equiv b \pmod{n}$, če in samo če n deli razliko $b - a$, to je

$$a \equiv b \pmod{n} \iff n \mid (b - a).$$

Trditev 3.1.2 *Naj bosta a in b poljubni celi števili in naj bo n naravno število. Tedaj velja $a \equiv b \pmod{n}$ natanko tedaj, ko imata a in b enak ostanek pri deljenju z n.*

Dokaz. ($\Longrightarrow$) Naj bosta števili a in b kongruentni po modulu n. Po izreku 3.1.1 obstajajo cela števila q_1, q_2, r_1 in r_2, da je $0 \leq r_1, r_2 < n$ in da velja $a = q_1 n + r_1$ in $b = q_2 n + r_2$. Zapišemo $b - a = (q_1 n + r_1) - (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2)$. Ker sta a in b kongruentni po modulu n, n deli $b - a$. Člen $(q_1 - q_2)n$ je po definiciji deljivosti celih števil deljiv z n. Drugi člen, $r_1 - r_2$, je po absolutni vrednosti manjši od n in je zato z njim deljiv le, če je enak 0, torej mora res veljati $r_1 = r_2$.
($\Longleftarrow$) Naj bo r ostanek, ki ga dobimo pri deljenju celih števil a in b z naravnim številom n. Po izreku 3.1.1 obstajata celi števili q_1 in q_2, da velja $a = q_1 n + r$ in $b = q_2 n + r$. Velja torej $a - q_1 n = b - q_2 n$. Če to enakost nekoliko preuredimo, dobimo $b - a = (q_2 - q_1)n$. Po definiciji deljivosti celih števil naravno število n deli razliko $b - a$, zato sta a in b kongruentni po modulu n, oziroma $a \equiv b \pmod{n}$.
□

Definicija. Naj bosta A in B množici. *Relacija* iz A v B je vsaka množica urejenih parov (a, b), pri čemer je $a \in A$ ter $b \in B$. To je torej podmnožica kartezičnega produkta $A \times B$. O *relaciji na množici* A govorimo, ko je $B = A$.

Opomba. Relacije običajno označujemo s črkami R, S, T. Če je $(x, y) \in R$, rečemo, da je x v relaciji R z y, kar zapišemo z xRy.

Definicija. Naj bo R relacija na množici A. Pravimo, da je relacija R

(i) *refleksivna*, če za vsak $x \in A$ velja xRx,

(ii) *simetrična*, če za poljubna $x, y \in A$ velja $xRy \Rightarrow yRx$,

(iii) *tranzitivna*, če za poljubne $x, y, z \in A$ velja $xRy \wedge yRz \Rightarrow xRz$.

Če je relacija R refleksivna, simetrična in tranzitivna, potem rečemo, da je R *ekvivalenčna relacija*.

Opomba. Ekvivalenčne relacije običajno označujemo z $\sim$.

Trditev 3.1.3 *Naj bo n naravno število. Relacija kongruence po modulu n je ekvivalenčna relacija na $\mathbb{Z}$.*

Dokaz. Pokazati moramo, da je relacija kongruence po modulu n refleksivna, simetrična in tranzitivna. Naj bodo a, b in c cela števila. Ker velja $a-a = 0 = n\cdot 0$, je ta relacija refleksivna. Naj bo $a \equiv b \pmod{n}$. Tedaj za nek $q \in \mathbb{Z}$ velja $b-a = nq$, torej je $a-b = n(-q)$, in zato je $b \equiv a \pmod{n}$. Relacija kongruence po modulu n je torej simetrična. Navsezadnje denimo, da je $a \equiv b \pmod{n}$ in $b \equiv c \pmod{n}$. Tedaj obstajata števili q in k, da velja $b-a = qn$ ter $c-b = kn$. Tedaj je $c-b+b-a = c-a = n(q+k)$. Ker je $q+k \in \mathbb{Z}$, od tod sledi $a \equiv c \pmod{n}$, s čimer smo pokazali, da je relacija kongruence po modulu n tudi tranzitivna relacija in s tem ekvivalenčna relacija. □

Opomba. Ekvivalenčno relacijo kongruence po modulu n na neki množici A bomo včasih označevali z $\sim_n$.

Definicija. Naj bo $\sim$ ekvivalenčna relacija na neprazni množici A. Za nek element $a \in A$ množico $[a]_\sim = \{b \in A : a \sim b\}$ imenujemo *ekvivalenčni razred* elementa a pri relaciji $\sim$. V nadaljevanju bomo namesto $[a]_\sim$ pisali $[a]$, saj bomo vedno govorili le o ekvivalenčni relaciji kongruence po modulu n. Množico vseh ekvivalenčnih razredov relacije $\sim$ na množici A označimo z $A/_\sim$ in ji rečemo *kvocientna množica* množice A glede na relacijo $\sim$.

V kolikor govorimo o ekvivalenčni relaciji $\sim_n$ na množici vseh celih števil, pripadajoče ekvivalenčne razrede imenujemo *kongruenčni razredi*.

Opomba. Naj bosta a in n naravni števili. Tedaj je kongruenčni razred števila a glede na relacijo $\sim_n$ enak

$$[a] = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Vsak ekvivalenčni razred ustreza enemu izmed ostankov $r = 0, 1, 2, \ldots, n-1$, ki jih dobimo pri deljenju z n, zato imamo n različnih ekvivalenčnih razredov. To so

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\},$$
$$[1] = \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n\},$$
$$\vdots$$
$$[n-1] = \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}.$$

To so ravno vsi paroma različni kongruenčni razredi, saj je $[n] = \{\ldots, -n, 0, n, 2n, \ldots\} = [0]$, $[n+1] = [1]$, itd.

Oglejmo si naslednji izrek, ki je le konkretna oblika bolj splošnega izreka iz [6]. Pove nam, kdaj sta dva kongruenčna razreda enaka.

Izrek 3.1.4 *Naj bo $\sim_n$ ekvivalenčna relacija kongruence po modulu n na množici $\mathbb{Z}$, kjer je n naravno število. Tedaj za $a, b \in \mathbb{Z}$ velja $a \sim_n b \iff [a] = [b]$. Potemtakem za vsaka a, $b \in \mathbb{Z}$ velja, da v kolikor je $[a] \cap [b] \neq \emptyset$, velja $[a] = [b]$.*

Dokaz. Najprej dokažimo prvi del izreka.
($\Longrightarrow$) Denimo, da velja $a \sim_n b$, ter pokažimo, da v tem primeru velja $[a] = [b]$. Naj bo $k \in [a]$ poljuben, kar pomeni, da je $a \sim_n k$. Ker je $a \sim_n b$ in je $\sim_n$ ekvivalenčna relacija, zaradi simetričnosti in tranzitivnosti te relacije velja $b \sim_n k$, torej je $k \in [b]$. Od tod sledi $[a] \subseteq [b]$. Zaradi simetričnosti relacije velja $b \sim_n a$ in po enakem premisleku kot prej je tudi $[b] \subseteq [a]$. Od tod sledi, da je $[a] = [b]$.
($\Longleftarrow$) Denimo sedaj, da je $[a] = [b]$. Zaradi refleksivnosti je $b \in [b]$ in zato tudi $b \in [a]$ in od tod sledi $a \sim_n b$.
Sedaj dokažimo še drugi del izreka. Če je $k \in [a] \cap [b]$, potem velja $k \sim_n a$ ter $k \sim_n b$. Tedaj je po prvem delu izreka $[a] = [k]$ in $[b] = [k]$, od koder sledi, da je $[a] = [b]$. □

Vsaka ekvivalenčna relacija na neki neprazni množici A nam poda *razbitje* te množice na paroma disjunktne podmnožice. Razbitje množice A je taka množica njenih nepraznih podmnožic, da vsak njen element nastopa v natanko eni izmed množic razbitja. Vseh razbitij množice A je ravno toliko, kolikor je možnih ekvivalenčnih relacij na tej množici. Več o tem pove naslednji izrek, ki ga ne bomo dokazovali. Bralca zato vabim, da si o njem več prebere samostojno.

Izrek 3.1.5 *Naj bo $\sim$ ekvivalenčna relacija na neprazni množici A. Tedaj je $\{[x]_\sim : x \in A\}$ razbitje množice A. Obratno, če je $\{A_i : i \in I\}$ razbitje množice A, je relacija $\sim$ na A, podana s predpisom $x \sim y \iff \exists i \in I : x, y \in A_i$, ekvivalenčna relacija, katere ekvivalenčni razredi sovpadajo z elementi družine $\{A_i : i \in I\}$.*

Posledica 3.1.6 *Ekvivalenčno relacijo na A lahko predpišemo tako, da kar določimo njene ekvivalenčne razrede.*

Na tej točki definiramo množico, ki nam bo omogočila konstrukcijo kolobarja $\mathbb{Z}_n$, kar je v bistvu cilj tega poglavja in hkrati temelj za nadaljnje preučevanje strukture grupe njegovih obrnljivih elementov.

Definicija. Kvocientno množico množice $\mathbb{Z}$ glede na relacijo $\sim_n$ imenujemo *množica kongruenčnih razredov po modulu n* in jo označimo z $\mathbb{Z}_n$.

Čeprav smo to množico že spoznali med študijem, si oglejmo na primer množico $\mathbb{Z}_8$ in njene elemente. To množico sestavlja 8 kongruenčnih razredov, pri čemer vsak kongruenčni razred ustreza enemu izmed ostankov $r = 0, 1, \ldots, 7$, ki jih dobimo pri deljenju celih števil z 8. Torej $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$. Bralca opozarjam, da torej po naši definiciji $\mathbb{Z}_8$ ni množica osmih števil, ampak je množica osmih množic. V izogib pisanju oglatih oklepajev v nadaljevanju občasno elemente $\mathbb{Z}_n$ pišemo kar kot najmanjše nenegativne predstavnike pripadajočih ekvivalenčnih razredov, pri čemer se zavedamo, da so elementi množice $\mathbb{Z}_n$ v bistvu množice. Včasih na njih torej gledamo kot na množice, včasih pa kot na predstavnike ekvivalenčnih razredov, torej kot na cela števila.
Da bi lahko na množici $\mathbb{Z}_n$ vpeljali strukturo kolobarja, moramo definirati ustrezno seštevanje in množenje ekvivalenčnih razredov. Naslednja trditev pokaže, da lahko to storimo na povsem naraven način.

Trditev 3.1.7 *Naj bo n naravno število in naj bodo a, a', b in b' cela števila, pri čemer velja $a \equiv a' \pmod{n}$ in $b \equiv b' \pmod{n}$. Tedaj velja $a + b \equiv a' + b' \pmod{n}$ in $ab \equiv a'b' \pmod{n}$.*

Dokaz. Ker je $a \equiv a' \pmod{n}$, n deli $a' - a$, in ker je $b \equiv b' \pmod{n}$, n deli tudi $b' - b$. Po definiciji deljivosti celih števil obstajata celi števili q in k, da velja $a'-a = qn$ ter $b'-b = kn$. Tedaj zapišemo $a'-a+b'-b = (a'+b')-(a+b) = n(q+k)$. Ker sta q in k celi števili, je njuna vsota celoštevilska. Od tod sledi, da n deli $(a' + b') - (a + b)$, zato velja $a + b \equiv a' + b' \pmod{n}$.
Posvetimo se še množenju. Podobno kot prej obstajata celi števili q in k, da velja $a' - a = qn$ ter $b' - b = kn$. Tedaj je $a'b' = (qn + a)(kn + b) = (qkn^2 + bqn + akn + ab) = ab + n(qkn + bq + ak)$. Od tod sledi, da n deli $a'b' - ab$, zato velja $ab \equiv a'b' \pmod{n}$. □

Sedaj lahko končno vpeljemo operaciji seštevanja in množenja na množici $\mathbb{Z}_n$.

Definicija. Naj bo n naravno število. Tedaj za poljubna $[a], [b] \in \mathbb{Z}_n$ seštevanje in množenje kongruenčnih razredov $[a]$ in $[b]$ definiramo kot:

$$\begin{aligned} [a] + [b] &= [a + b], \\ [a] \cdot [b] &= [a \cdot b]. \end{aligned} \tag{3.1}$$

Posledica 3.1.8 *Seštevanje in množenje kongruenčnih razredov $[a], [b] \in \mathbb{Z}_n$ iz (3.1) je dobro definirano.*

Dokaz. Da sta operaciji iz (3.1) dobro definirani, sledi neposredno iz trditve 3.1.7, saj le-ta pokaže, da ekvivalenčni razred $[a + b]$ (oziroma $[a \cdot b]$) ni odvisen od konkretnih predstavnikov razredov $[a]$ in $[b]$.

Za konec tega razdelka zapišimo naslednjo trditev in njeno posledico, ki jo potrebujemo v nadaljevanju magistrskega dela.

Trditev 3.1.9 *Naj bodo n, r in s naravna števila. Če je $n = r \cdot s$, kjer je $D(r, s) = 1$, za poljubni celi števili a in b velja*

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{r} \quad in \quad a \equiv b \pmod{s}.$$

Dokaz. ($\Longrightarrow$) Če n deli $b - a$, potem, ker r deli n, tudi r deli $b - a$, in ker s deli n, potem tudi s deli $b - a$.
($\Longleftarrow$) Če r deli $b - a$ in s deli $b - a$, ker sta r in s tuji, tudi njun produkt deli $b - a$. □

Z indukcijo na število različnih praštevil v faktorizaciji števila n dobimo naslednjo posledico.

Posledica 3.1.10 *Naj bo n naravno število in naj bo $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ faktorizacija števila n, pri čemer so $p_1, p_2, \ldots, p_k$ paroma različna praštevila. Tedaj za vsaki celi števili a in b velja $a \equiv b \pmod{n}$, če in samo če je $a \equiv b \pmod{p_i^{e_i}}$ za vsak $i = 1, \ldots, k$.*

3.2 Kolobar $\mathbb{Z}_n$

Do sedaj smo definirali relacijo kongruence po modulu n in dokazali, da je ekvivalenčna relacija. Definirali smo pripadajoče kongruenčne razrede in množico $\mathbb{Z}_n$ ter pokazali, da sta operaciji seštevanja in množenja iz (3.1) v tej množici dobro definirani. Navsezadnje lahko izpeljemo to, kar smo si prizadevali skozi celotno poglavje, to je, da množica $\mathbb{Z}_n$ skupaj s tema operacijama seštevanja in množenja po modulu n postane kolobar. Najprej dokažimo, da je $(\mathbb{Z}_n, +)$ z operacijo seštevanja kot v (3.1) res grupa. Razdelek je povzet po [7].

Trditev 3.2.1 *Naj bo n naravno število. Tedaj je $(\mathbb{Z}_n, +)$ z operacijo seštevanja kot v (3.1) grupa.*

Dokaz. Po posledici 3.1.8 za poljubne $a, b, c \in \mathbb{Z}$ velja $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c]$, torej je $+$ asociativna operacija na $\mathbb{Z}_n$. Nevtralni element je očitno $[0]$, saj velja $[a]+[0] = [a+0] = [0+a] = [0]+[a] = [a]$. Očitno je, da za vsak element $a \in \mathbb{Z}_n$ obstaja aditivni inverz za $[a]$, saj velja $[a]+[-a] = [a+(-a)] = [0] = [(-a)+a] = [-a]+[a]$. Torej je $(\mathbb{Z}_n, +)$ res grupa.

□

Trditev 3.2.2 *Naj bo n naravno število. Tedaj je $(\mathbb{Z}_n, +, \cdot)$, kjer sta operaciji seštevanja in množenja kot v (3.1), komutativen kolobar.*

Dokaz. Naj bosta $[a], [b] \in \mathbb{Z}_n$. Grupa $(\mathbb{Z}_n, +)$ je abelova, saj $[a]+[b] = [a+b] = [b+a] = [b]+[a]$. Pri množenju kongruenčnih razredov asociativnost spet sledi iz asociativnosti množenja celih števil, to je, $([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c])$. Obe operaciji pa povezuje distributivnostni zakon, ki sledi

iz distributivnosti na celih številih, torej $[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c]$ in $([a]+[b])[c] = [a+b][c] = [(a+b)c] = [ac+bc] = [ac]+[bc] = [a][c]+[b][c]$. Pri množenju kongruenčnih razredov komutativnost sledi iz komutativnosti množenja celih števil, to je, $[a][b] = [ab] = [ba] = [b][a]$. Torej je $(\mathbb{Z}_n, +, \cdot)$ res komutativen kolobar.

□

Opomba. Ko v nadaljevanju govorimo o elementih kolobarja $\mathbb{Z}_n$, v skladu z našim dogovorom pravzaprav govorimo o najmanjših predstavnikih posameznih kongruenčnih razredov. Zato moramo seveda najmanjše predstavnike pripadajočih kongruenčnih razredov seštevati in množiti po modulu n, to je, za dobljeno vsoto oziroma produkt moramo izračunati ostanek pri deljenju z n.

Preden nadaljujemo z naslednjim poglavjem, zapišimo izreka iz [7], ki sta ključnega pomena za razumevanje magistrskega dela.

Izrek 3.2.3 *(Klasifikacija končnih komutativnih grup). Naj bo n naravno število in naj bo G komutativna grupa reda n. Tedaj obstajajo (ne nujno paroma različna) praštevila $p_1, p_2, \ldots, p_k$ in naravna števila $i_1, i_2, \ldots, i_k$, da velja $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ in je*

$$G \cong \mathbb{Z}_{p_1^{i_1}} \times \mathbb{Z}_{p_2^{i_2}} \times \cdots \times \mathbb{Z}_{p_k^{i_k}}.$$

Izrek 3.2.4 *Naj bosta n in m naravni števili. Grupa $\mathbb{Z}_n \times \mathbb{Z}_m$ je ciklična natanko tedaj, ko velja $D(n,m) = 1$.*

Dokaz. ($\Longrightarrow$) V primeru, ko je vsaj eno od števil m in n enako 1, ni kaj dokazati, saj je $\mathbb{Z}_n \cong \mathbb{Z}_n \times \mathbb{Z}_1 \cong \mathbb{Z}_1 \times \mathbb{Z}_n$. Privzemimo, da je $n, m \geq 2$. Po izreku 2.1.5 je red elementa $(1,1)$ v $\mathbb{Z}_n \times \mathbb{Z}_m$ enak $v(n,m)$. Po izreku iz teorije števile, o katerem si bralec lahko več prebere v [2], velja $v(n,m) = \frac{nm}{D(n,m)}$. V primeru, ko je $D(n,m) = 1$, je torej $(1,1)$ generator grupe $\mathbb{Z}_n \times \mathbb{Z}_m$, ki je zato ciklična.
($\Longleftarrow$) Po posledici 2.1.3 za vsak $a \in \mathbb{Z}_n$ ter $b \in \mathbb{Z}_m$ velja, da $|a|$ deli n in $|b|$ deli m. Tedaj je red elementa (a,b) po izreku 2.1.5 delitelj najmanjšega skupnega večkratnika $v(n,m)$, ki pa je v primeru, ko je $D(n,m) > 1$, zagotovo manjši od mn. Če je torej $D(n,m) > 1$, v grupi $\mathbb{Z}_n \times \mathbb{Z}_m$ ni elementa reda mn, zato ta grupa ni ciklična. □

Opomba. Rezultat, ki nam ga podaja izrek 3.2.4, lahko posplošimo na več faktorjev.

Poglavje 4

Kdaj je grupa enot U_n ciklična?

Kolobar $\mathbb{Z}_n$ ima nekaj zanimivih lastnosti, ki jih v nadaljevanju raziščemo. V tem poglavju si pobliže ogledamo elemente tega kolobarja. Najprej navedemo dokaz dobro znanega dejstva, da v vsakem kolobarju z enico obrnljivi elementi kolobarja skupaj z operacijo množenja tvorijo grupo. To grupo imenujemo grupa enot ali grupa obrnljivih elementov. V tem poglavju zapišemo glavne lastnosti te grupe za primer kolobarja $\mathbb{Z}_n$, in jih dokažemo s pomočjo že znanih rezultatov iz teorije grup in teorije števil. Kolobar $\mathbb{Z}_n$ ima očitno enico, namreč ekvivalenčni razred števila 1. V tem poglavju največ pozornosti posvetimo vprašanju: kdaj je grupa enot kolobarja $\mathbb{Z}_n$ ciklična? Bolj natančno, skušamo ugotoviti, kako je cikličnost grupe enot kolobarja $\mathbb{Z}_n$ odvisna od naravnega števila n. Izkaže se, da ima glavno vlogo pri tem, ali je grupa enot ciklična, praštevilska faktorizacija števila n. V nadaljevanju poglavja preučujemo grupe enot kolobarja $\mathbb{Z}_n$ pri različnih oblikah praštevilske faktorizacije naravnega števila n. V zaključku tega poglavja zapišemo izrek, ki nam pove, za katera naravna števila n je grupa enot U_n ciklična. Poglavje je povzeto po [1],[2],[3],[6] in [7].

4.1 Grupa enot U_n

V tem razdelku najprej ponovimo definicijo obrnljivega elementa v kolobarju z enico in pripadajoče grupe enot. Dokaze nekaterih izrekov izpustimo, zato vabim bralca, da si več o njih prebere samostojno v [2]. Glavno matematično orodje v tem delu magistrskega dela je Eulerjeva funkcija, s pomočjo katere bomo v tem

razdelku preučevali strukturo grupe enot kolobarja $\mathbb{Z}_n$. Definiramo tudi pojem primitivnega korena, ki nam bo v pomoč pri ugotavljanju, ali je dana grupa ciklična ali ne. Nato si ogledamo cikličnost grupe enot kolobarja $\mathbb{Z}_n$ za različna naravna števila n. V samem zaključku razdelka zapišemo, pri katerih naravnih številih n je grupa enot kolobarja $\mathbb{Z}_n$ ciklična in pri katerih ne. Ta razdelek je povzet po [8] in [9].

Definicija. Naj bo K kolobar z enico. *Multiplikativni inverz neničelnega elementa* a kolobarja K je element $a^{-1} \in K$, tako da velja $aa^{-1} = a^{-1}a = 1$ (če seveda sploh obstaja). Element $a \in K$ je *enota* ali *obrnljiv element* natanko tedaj, ko ima multiplikativni inverz. Množico vseh obrnljivih elementov kolobarja K označimo s K^*.

Trditev 4.1.1 *Naj bo K kolobar z enico. V kolikor obstaja multiplikativni inverz elementa $a \in K$, je ta en sam.*

Dokaz. Dokaz dostopen v [3].

Trditev 4.1.2 *Naj bo K kolobar z enico. Tedaj je množica obrnljivih elementov K^* skupaj z operacijo množenja grupa.*

Dokaz. Očitno je, da je podedovana operacija množenja iz kolobarja K v K^* asociativna. Element $1 \in K$ je obrnljiv, saj $1 \cdot 1 = 1$, torej je $1^{-1} = 1$. Vsak $a \in K^*$ ima po definiciji inverz v K, torej obstaja $a^{-1} \in K$, da je $aa^{-1} = a^{-1}a = 1$, od koder pa takoj sledi, da je tudi $a^{-1} \in K^*$. Za vsak $a, b \in K^*$ velja $aa^{-1} = a^{-1}a = 1$, ter $bb^{-1} = b^{-1}b = 1$. Od tod sledi, da je $(aa^{-1})(bb^{-1}) = (a^{-1}a)(b^{-1}b) = (a^{-1}b^{-1})(ab) = (ab)(ab)^{-1} = 1$. Tedaj je $ab \in K^*$, zato je podedovana operacija množenja iz kolobarja K v K^* notranja.

□

V nadaljevanju se posvetimo le končnim kolobarjem oblike $(\mathbb{Z}_n, +, \cdot)$, pri čemer je naravno število $n \geq 2$. Dogovorimo se, da od tu dalje z $\mathbb{Z}_n$ označujemo kolobar $(\mathbb{Z}_n, +, \cdot)$, njegovo grupo obrnljivih elementov za to množenje imenujemo tudi *grupa enot*, označujemo pa jo z U_n.

Po trditvi 4.1.2 dobimo naslednjo posledico.

Posledica 4.1.3 *Naj bo n naravno število in naj bo $\mathbb{Z}_n$ kolobar. Tedaj je U_n komutativna grupa.*

Dokaz. Da je $(U_n, \cdot)$ grupa, sledi iz trditve 4.1.2, da je komutativna, pa iz trditve 3.2.2. □

Na tem mestu najprej zapišemo izrek, s pomočjo katerega dokažemo trditev, ki sledi.

Izrek 4.1.4 *(Bezoutova identiteta). Naj bosta a in b celi števili, pri čemer je vsaj eno od njiju različno od 0. Tedaj obstajata celi števili u in v, da velja $D(a,b) = au + bv$, kjer je $D(a,b)$ največji skupni delitelj števil a in b.*

Trditev 4.1.5 *Naj bo n naravno število in $a \in \mathbb{Z}_n$. Tedaj je a enota ali obrnljiv element kolobarja $\mathbb{Z}_n$, če in samo če je $D(a,n) = 1$.*

Dokaz. ($\Longrightarrow$) Naj bo a enota kolobarja $\mathbb{Z}_n$. Tedaj obstaja $b \in \mathbb{Z}_n$, da v $\mathbb{Z}_n$ velja $ab = 1$, to pa pomeni, da obstajata celi števili b in q, da velja $ab = 1 + qn$. Torej mora veljati $D(a,n) = 1$, saj bi sicer skupni delitelj a in n delil 1.
($\Longleftarrow$) Naj bo $D(a,n) = 1$. Potem po izreku 4.1.4 za določeni celi števili u in v velja $1 = au + nv$. Ker je nv večkratnik števila n, velja $nv \equiv 0 \pmod{n}$, torej je u multiplikativni inverz a v $\mathbb{Z}_n$ in zato je a enota kolobarja $\mathbb{Z}_n$.

□

Zgled. Poskusimo zapisati elemente grupe U_{10} in ugotoviti, kateri znani grupi je izomorfna. Kolobar $\mathbb{Z}_{10}$ ima po trditvi 4.1.5 štiri obrnljive elemente, namreč $1, 3, 7$ in 9. Vsi našteti obrnljivi elementi tvorijo grupo $U_{10} = \{1, 3, 7, 9\}$. Red te grupe je 4. Po izreku 3.2.3 sta edini komutativni grupi reda 4 grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$ in $\mathbb{Z}_4$, zato je U_{10} izomorfna natanko eni izmed njiju. U_{10} ima element reda 4, to je na primer element 3, $\mathbb{Z}_2 \times \mathbb{Z}_2$ pa takšnega elementa nima, zato je $U_{10} \cong \mathbb{Z}_4$. Od tod sledi, da je grupa U_{10} ciklična.

Zgled. Kolobar $\mathbb{Z}_6$ ima dva obrnljiva elementa, to sta 1 in 5. Ta dva elementa tvorita grupo $U_6 = \{1, 5\}$, ki je reda 2. Po izreku 3.2.3 velja $U_6 \cong \mathbb{Z}_2$ in zato je grupa U_6 ciklična.

Če želimo dve grupi med seboj primerjati, moramo v prvi vrsti poznati njuna reda. Red poljubne grupe enot lahko načeloma določimo tako, da zapišemo vse njene

elemente in jih preštejemo. To se mogoče izide za majhne vrednosti števila n, a je za večje vrednosti n ta način iskanja reda grupe enot zelo zamuden, zato zapišimo naslednjo definicijo in izrek.

Definicija. *Eulerjeva φ - funkcija* je funkcija $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, ki vsakemu naravnemu številu n priredi število vseh naravnih števil, ki so tuja n in ne presegajo števila n.

Dobro znano je (osnovni izrek aritmetike), da lahko vsako naravno število, ki je večje od 1, do vrstnega reda faktorjev natančno enolično faktoriziramo na produkt samih praštevil. Takšni faktorizaciji naravnega števila n bomo rekli *prafaktorizacija* števila n

Izrek 4.1.6 *Naj bo n naravno število. Če je prafaktorizacija števila n oblike $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, pri čemer so $p_1, \ldots, p_k$ paroma različna praštevila, $e_1, \ldots, e_k \in \mathbb{N}$, ter $k \in \mathbb{N}$, velja*

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Če sta torej naravni števili a in b tuji, velja $\varphi(ab) = \varphi(a)\varphi(b)$. Če je p praštevilo, potem velja $\varphi(p) = p - 1$ in $\varphi(p^e) = p^{e-1}(p - 1)$ za vse $e \geq 1$.

Dokaz. Dokaz lahko izpeljemo s pomočjo načela vključitev in izključitev. Bralec si ga lahko ogleda v [4].

Zgled. Določimo število vseh števil, ki so manjša od 190 in so tuja 190, to je, izračunajmo $\varphi(190)$. Če faktoriziramo število 190, dobimo $190 = 2 \cdot 5 \cdot 19$. Po izreku 4.1.6 izračunamo $\varphi(190)$ kot

$$\varphi(190) = 190 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{19}) = 190 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{18}{19} = 72.$$

Trditev 4.1.7 *Naj bo n poljubno naravno število. Tedaj za grupo U_n kolobarja $\mathbb{Z}_n$ velja $|U_n| = \varphi(n)$.*

Dokaz. Naj bo $a \in \mathbb{Z}_n$. Po trditvi 4.1.5 je a enota $\mathbb{Z}_n$ natanko tedaj, ko je a tuje številu n. Tedaj ima grupa enot U_n kolobarja $\mathbb{Z}_n$ toliko elementov, kolikor je tujih naravnih števil številu n, ki ne presegajo n, teh pa je po definiciji ravno $\varphi(n)$.

□

Posledica 4.1.8 *(Mali Fermatov izrek). Za vsako praštevilo p in za vsako celo število a, ki ni deljivo s p, velja $a^{p-1} \equiv 1 \pmod{p}$.*

Dokaz. Po trditvi 4.1.5 so vsi neničelni elementi kolobarja $\mathbb{Z}_p$ obrnljivi, po posledici 4.1.3 pa vsi ti elementi tvorijo multiplikativno grupo U_p. Po trditvi 4.1.7 je red grupe U_p enak $\varphi(p) = p - 1$. Tedaj po posledici 2.1.4 za vsak $a \in U_p$ velja $a^{p-1} \equiv 1 \pmod{p}$.

□

Leonhard Euler je Fermatov izrek posplošil s praštevil na poljubno naravno število.

Izrek 4.1.9 *(Eulerjev izrek). Naj bo n naravno število in naj bo a tako celo število, da je $D(a, n) = 1$. Tedaj je $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Dokaz. Po trditvi 4.1.5 vemo, da je $a \in \mathbb{Z}_n$ obrnljiv v $\mathbb{Z}_n$ natanko tedaj, ko je a tuj številu n. Tako je grupa U_n reda $\varphi(n)$. Ker je $D(a, n) = 1$, element $a \in \mathbb{Z}_n$ pripada grupi U_n. Po posledici 2.1.4 v grupi U_n velja $a^{\varphi(n)} \equiv 1 \pmod{n}$.

□

Zgled. Izračunajmo red grupe U_{15}. Po trditvi 4.1.7 velja $|U_{15}| = \varphi(15)$. V faktorizaciji števila 15 nastopata praštevili 3 in 5, ki sta si tuji, zato po izreku 4.1.6 velja $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$. Torej je red grupe U_{15} enak 8. Bralca vabimo, da se prepriča, ali je ta grupa ciklična ali ne.

Zgled. Izračunajmo še red grupe U_{48}. Po trditvi 4.1.7 velja $|U_{48}| = \varphi(48)$. Zapišemo $48 = 2^4 \cdot 3$. Po izreku 4.1.6 velja $\varphi(48) = 16$. Torej je $|U_{48}| = 16$. Tudi tokrat naj bralec preveri, ali je grupa ciklična ali ne.

Za preučevanje grupe U_n moramo spoznati in dokazati še nekatere lastnosti njenih elementov, zato sledijo naslednje trditve.

Trditev 4.1.10 *Naj bo n naravno število, naj bo $a \in U_n$ reda k in naj bo m naravno število. Tedaj je $a^m \equiv 1 \pmod{n}$ natanko tedaj, ko $k \mid m$.*

Dokaz. Čeprav je to neposredna posledica izreka 2.1.2 in dejstva, da je U_n grupa, vseeno zapišimo neposreden dokaz.
($\Longrightarrow$) Naj bo $a^m \equiv 1 \pmod{n}$. Po izreku 3.1.1 obstajata celi števili q in r, da velja $m = qk + r$, pri čemer je $0 \leq r < k$. Tedaj je $1 \equiv a^m \equiv a^{qk+r} \equiv a^{qk}a^r \equiv$

$(a^k)^q a^r \equiv 1a^r \equiv a^r \pmod{n}$. Ker je a reda k, mora veljati $r = 0$. Od tod sledi, da $k \mid m$.
($\Longleftarrow$) Naj k deli m. Po definiciji deljivosti obstaja celo število q, da velja $m = qk$. Tedaj je $a^m \equiv a^{qk} \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}$.

□

Po posledici 2.1.3 dobimo naslednji rezultat.

Posledica 4.1.11 *Naj bo k naravno število in naj bo $a \in U_n$ reda k. Tedaj k deli $\varphi(n)$.*

Trditev 4.1.12 *Naj bo $a \in U_n$ reda k in naj bo d tako naravno število, da velja $d \mid k$. Tedaj je red a^d enak $\frac{k}{d}$.*

Dokaz. Označimo red a^d z m. Tedaj velja $(a^d)^m \equiv a^{dm} \equiv 1 \pmod{n}$. Ker je a reda k, sledi, da je $k \leq dm$. Od tod sledi, da je $m \geq \frac{k}{d}$.
Opazimo, da je $(a^d)^{\frac{k}{d}} \equiv a^k \equiv 1 \pmod{n}$, ampak ker je a^d reda m, je $m \leq \frac{k}{d}$. Od tod sledi, da je $m = \frac{k}{d}$.

□

Trditev 4.1.13 *Naj bo $a \in U_n$ reda k in naj bo i poljubno naravno število. Tedaj velja $|a^i| = \frac{k}{D(i,k)}$.*

Dokaz. Naj bo t takšno naravno število, da velja $(a^i)^t \equiv 1 \pmod{n}$. Tedaj je $a^{it} \equiv 1 \pmod{n}$, torej je po trditvi 4.1.10 it večkratnik števila k in zato tudi skupni večkratnik števil i in k. Izrek iz teorije števil, o katerem si bralec lahko več prebere v [2], pravi, da je vsak skupni večkratnik i in k večkratnik $v(i,k) = \frac{ik}{D(i,k)}$. Ker je število it večkratnik števila ik, slednji pa je večkratnik števila $\frac{ik}{D(i,k)}$, je it večkratnik $\frac{ik}{D(i,k)}$. Od tod sledi, da je t večkratnik $\frac{k}{D(i,k)}$.
Sedaj pokažimo, da je red a^i enak $\frac{k}{D(i,k)}$. Zapišimo $(a^i)^{\frac{k}{D(i,k)}} \equiv (a^k)^{\frac{i}{D(i,k)}} \equiv 1^{\frac{k}{D(i,k)}} \equiv 1 \pmod{n}$.

□

Posledica 4.1.14 *Naj bo $a \in U_n$ reda k in naj za neko naravno število i velja $D(i,k) = 1$. Tedaj velja $|a^i| = k$.*

Trditev 4.1.15 *Naj bo n naravno število in naj ima $a \in U_n$ red k_1 in naj ima $b \in U_n$ red k_2. Če je $D(k_1, k_2) = 1$, potem ima $a \cdot b \in U_n$ red $k_1 \cdot k_2$.*

Dokaz. Naj bo i tako naravno število, da je $(ab)^i \equiv 1 \pmod{n}$. Tedaj je $a^i b^i \equiv 1 \pmod{n}$. Od tod sledi, da je b^i inverz a^i, posledično pa sta a^i in b^i istega reda. Po trditvi 4.1.13 red a^i deli red a ter red b^i deli red b. Če je $D(k_1, k_2) = 1$, sta torej tudi reda a^i in b^i tuja, a ker je po zgornjem njun red enak, velja $a^i \equiv b^i \equiv 1 \pmod{n}$. Tedaj je i večkratnik števila k_1 in večkratnik števila k_2, in ker sta k_1 in k_2 tuji števili, je i večkratnik $k_1 \cdot k_2$. Sledi, da je $i \geq k_1 \cdot k_2$. Vzemimo najmanjši tak i, to je $i = k_1 \cdot k_2$ in pokažimo, da je red $a \cdot b$ enak $k_1 \cdot k_2$. Zapišimo $(a \cdot b)^{k_1 \cdot k_2} \equiv (a^{k_1})^{k_2} \cdot (b^{k_2})^{k_1} \equiv 1^{k_2} \cdot 1^{k_1} \equiv 1 \pmod{n}$. Od tod sledi, da je $|ab| = k_1 \cdot k_2$.

□

Trditev 4.1.16 *Naj bodo $a_1, a_2, \ldots, a_r \in U_n$ reda $n_1, n_2, \ldots, n_r$ v tem zaporedju. Če so števila $n_1, n_2, \ldots, n_r$ paroma tuja, je red $a_1 a_2 \cdots a_r$ enak $n_1 n_2 \cdots n_r$.*

Dokaz. Dokaz sledi po trditvi 4.1.15 z indukcijo na r. Podrobnosti prepuščam bralcu.

□

4.1.1 Primitivni koren grupe U_n

V nadaljevanju želimo opisati strukturo grupe U_n za vsa naravna števila n. V kolikor želimo to storiti, nam poznavanje reda grupe U_n ne zadostuje, kajti na primer grupi U_5 in U_8 sta enakega reda, saj je $\varphi(5) = \varphi(8) = 4$. Kljub temu pa ti dve grupi nista izomorfni, saj U_5 vsebuje elemente reda 4, na primer 3, medtem ko ga U_8 ne vsebuje, saj so vsi njeni netrivialni elementi reda 2 in zato je $U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. V tem razdelku zato spoznamo primitivne korene, s pomočjo katerih v nadaljevanju poglavja določimo tiste vrednosti n, za katere je grupa U_n ciklična, kar je navsezadnje cilj tega poglavja.

Definicija. Naj bo n tako naravno število, da je grupa U_n ciklična. Tedaj vsak generator a grupe U_n imenujemo *primitivni koren po modulu n.*

Opomba. Ker je primitivni koren po modulu n generator ciklične grupe U_n, ki je reda $\varphi(n)$, je torej ta primitivni koren reda $\varphi(n)$.

Trditev 4.1.17 *Naj bo n naravno število in naj bo $a \in U_n$. Element a je primitivni koren po modulu n natanko tedaj, ko za vsako praštevilo q, ki deli red grupe U_n, velja $a^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$.*

Dokaz. ($\Longrightarrow$) Denimo torej, da je $a \in U_n$ primitivni koren po modulu n, kar med drugim pomeni, da je U_n ciklična grupa. Po definiciji in trditvi 4.1.7 velja $|a| = \varphi(n) = |U_n|$, zato je po trditvi 4.1.10 $a^i \not\equiv 1 \pmod{n}$ za vsa naravna števila $i < \varphi(n)$. Tedaj velja $a^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$ za vsako praštevilo q, ki deli red grupe U_n.
($\Longleftarrow$) Če za vsako praštevilo q, ki deli red grupe U_n, velja $a^{\frac{\varphi(n)}{q}} \not\equiv 1 \pmod{n}$, potem je red a enak $\varphi(n)$, saj po posledici 2.1.4 in trditvi 4.1.7 velja $a^{\varphi(n)} \equiv 1 \pmod{n}$. Torej je a primitivni koren po modulu n.

□

Zgled. Oglejmo si grupi U_{17} in U_8. Poiščimo najprej primitivne korene U_{17}, če obstajajo. Po trditvi 4.1.7 velja $\mid U_{17} \mid = \varphi(17) = 17 - 1 = 16$. Ker je $16 = 2^4$, je po trditvi 4.1.17 $a \in U_{17}$ primitivni koren po modulu 17 natanko tedaj, ko velja $a^{\frac{16}{2}} \not\equiv 1 \pmod{17}$. Na primer, po trditvi 4.1.5 grupa U_{17} vsebuje element 2, saj velja $D(2, 17) = 1$, vendar ta element ni primitivni koren po modulu 17, ker je $2^8 = 256 \equiv 1 \pmod{17}$, zato poglejmo, ali je mogoče 3 primitivni koren po modulu 17. Velja $3^8 = (3^4)^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$, od koder sledi, da je 3 primitivni koren grupe U_{17}. Bralca vabim, da poišče preostale primitivne korene te grupe.
Že na začetku tega razdelka smo videli, da je $U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, torej grupa U_8 ni ciklična in zato ne obstaja primitivni koren po modulu 8.

Opazimo, da nekatere grupe enot imajo generatorje in so torej ciklične, nekatere pa jih nimajo. V kolikor grupa enot ima primitivne korene, nas v določenih primerih zanima, koliko je vseh, zato ta razdelek zaključimo z naslednjo trditvijo.

Trditev 4.1.18 *Naj bo n tako naravno število, da ima grupa enot U_n vsaj en primitivni koren po modulu n. Tedaj ima U_n natanko $\varphi(\varphi(n))$ takšnih primitivnih korenov.*

Dokaz. Naj bo $a \in U_n$ primitivni koren po modulu n. Red grupe U_n označimo z m. Po trditvi 4.1.7 velja $m = \varphi(n)$. Primitivni koren a po modulu n generira grupo U_n in zato je njegov red enak m. Po trditvi 4.1.13 je za poljubno naravno število i element a^i reda m (in je zato tudi primitivni koren po modulu n) natanko tedaj, ko velja $D(i, m) = 1$. Takšnih naravnih števil i, ki obenem ne presegajo reda m grupe U_n, je toliko, kolikor je tujih števil številu m, ki ga ne presegajo, to je $\varphi(m) = \varphi(\varphi(n))$.

□

4.2 Grupa U_p

Grupa enot U_n kolobarja $\mathbb{Z}_n$ je torej ciklična natanko tedaj, ko vsebuje vsaj en primitivni koren po modulu n. Vprašanje, kdaj le-ta obstaja, pa v splošnem ni povsem enostavno, zato se bomo analize lotili sistematično glede na praštevilsko faktorizacijo števila n. V tem razdelku začnemo z najbolj enostavno situacijo, ko je n praštevilo. Oglejmo si torej grupo enot kolobarja $\mathbb{Z}_p$, kjer je p poljubno praštevilo. Preden pokažemo, da je v tem primeru grupa U_p ciklična, zapišimo in dokažimo nekatere trditve. Prva sledi neposredno iz posledice 4.1.11.

Trditev 4.2.1 *Naj bo $p > 2$ praštevilo in naj bo $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ prafaktorizacija $p-1$. Tedaj je red poljubnega elementa $a \in U_p$ oblike $q_1^{c_1} \cdots q_r^{c_r}$, pri čemer je $c_i \leq e_i$ za vsak i.*

Trditev 4.2.2 *Naj bo $p > 2$ praštevilo in naj bo $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ prafaktorizacija $p-1$. Tedaj za vsak i, kjer je $1 \leq i \leq r$, obstaja element $a_i \in U_p$, katerega red je večkratnik števila $q_i^{e_i}$.*

Dokaz. Dokaz opravimo le za $i = 1$. Za ostale vrednosti števila i je dokaz povsem podoben. Denimo, da trditev ne drži za $i = 1$. Tedaj red vsakega elementa iz U_p deli $\frac{(p-1)}{q_1} = q_1^{e_1-1} \cdot q_2^{e_2} \cdots q_r^{e_r}$. Naj bo $d = \frac{(p-1)}{q_1}$. Torej po posledici 2.1.3 za vsak $a \in U_p$ velja $a^d \equiv 1 \pmod{p}$, to je $a^d - 1 \equiv 0 \pmod{p}$. Torej je vsak element grupe U_p ničla polinoma $x^d - 1$, kjer na ta polinom gledamo kot na polinom s koeficienti iz $\mathbb{Z}_p$. Ta polinom pa ima lahko v polju $\mathbb{Z}_p$ največ d različnih ničel, kar nas privede v protislovje, saj je po trditvi 4.1.7 vseh elementov grupe U_p natanko $p - 1 > d$.

□

Opomba. V tem dokazu smo se sklicevali na rezultat iz [7], ki pove, da ima lahko polinom stopnje n nad poljem največ n različnih ničel, ampak na tem mestu bi preveč skrenili z začrtane poti, če bi želeli razviti in zapisati vso potrebno teorijo polinomov in njihovih ničel nad polji, da bi lahko izpeljali pripadajoči dokaz. Bralec si lahko več o tem prebere v [7].

Trditev 4.2.3 *Naj bo p praštevilo, pri čemer je $p > 2$, in naj bo $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ prafaktorizacija $p-1$. Tedaj za vsak i, kjer je $1 \leq i \leq r$, obstaja $a_i \in U_p$, ki je reda $q_i^{e_i}$.*

Dokaz. Po trditvi 4.2.2 obstaja $b_i \in U_p$ reda $kq_i^{e_i}$ za neko naravno število k, ki po posledici 2.1.3 seveda deli $\frac{p-1}{q_i^{e_i}}$. Naj bo $a_i \equiv b_i^k \pmod{p}$. Po trditvi 4.1.12 je red a_i enak $q_i^{e_1}$.

□

Izrek 4.2.4 *Naj bo p poljubno praštevilo. Tedaj grupa U_p vsebuje element reda $\varphi(p) = p-1$ in je zato ciklična.*

Dokaz. Jasno je, da je grupa U_2 ciklična, zato privzemimo, da je $p > 2$. Naj bo $p-1 = q_1^{e_1} \cdots q_r^{e_r}$ prafaktorizacija $p-1$. Po trditvi 4.2.3 za vsak i, kjer je $1 \leq i \leq r$ obstaja $a_i \in U_p$, ki je reda $q_i^{e_i}$. Po trditvi 4.1.16 je red elementa $a_1 a_2 \cdots a_r \in U_p$ enak $p-1$.

□

4.3 Grupa U_{p^e}

Do sedaj smo pokazali, da je grupa U_{p^e} ciklična za vsa liha praštevila p in $e = 1$, zato bomo v tem razdelku preučevali grupe enot U_{p^e}, pri čemer je p liho praštevilo in $e \geq 2$.

Preden se spomnimo dobro znanega binomskega izreka, ponovimo definicijo binomskih simbolov. Za poljubno naravno število n in celo število r, kjer je $0 \leq r \leq n$, zapisu $\binom{n}{r}$ pravimo *binomski koeficient* in velja $\binom{n}{r} = \frac{n!}{(n-r)!r!}$.

Izrek 4.3.1 *(Binomski izrek). Naj bodo a, b in n naravna števila. Tedaj velja enakost*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.$$

Izrek 4.3.2 *Naj bo p liho praštevilo. Tedaj je grupa U_{p^e} ciklična za vse $e \geq 1$.*

Dokaz. Po izreku 4.2.4 lahko predpostavimo, da je $e \geq 2$. Strategija iskanja primitivnega korena po modulu p^e je naslednja. Najprej izberemo nek primitivni koren g po modulu p, nato izpeljemo dokaz v dveh korakih:

(i) Pokažemo, da je vsaj eden od g in $g+p$ primitivni koren po modulu p^2.

(ii) Pokažemo, da v kolikor je h poljuben primitivni koren po modulu p^2, je tudi primitivni koren po modulu p^e za vse $e \geq 2$.

Naj bo torej p liho praštevilo. Tedaj je po izreku 4.2.4 grupa U_p ciklična, zato obstaja primitivni koren g po modulu p. Zanj torej velja $g^{p-1} \equiv 1 \pmod{p}$ in $g^i \not\equiv 1 \pmod{p}$ za $1 \leq i < p-1$, pri čemer je i naravno število.
Ker je $g \in U_p$, sta g in p tuji si števili in zato sta si tuji tudi g in p^2. Posledično je $g \in U_{p^2}$. Označimo red elementa g v U_{p^2} z d. Tedaj velja $g^d \equiv 1 (\mathrm{mod}\ p^2)$ in zato seveda velja tudi $g^d \equiv 1 (\mathrm{mod}\ p)$. Po posledici 2.1.3 število d deli red grupe U_{p^2}, ki je po trditvi 4.1.7 enak $\varphi(p^2) = p(p-1)$. Red $g \in U_p$ je $p-1$, zato zaradi $g^d \equiv 1 \pmod{p}$ po trditvi 4.1.10 velja $p-1 \mid d$. Ker je p praštevilo, velja $d = p(p-1)$ ali $d = p-1$. Če je $d = p(p-1)$, potem je g primitivni koren po modulu p^2, kot smo tudi želeli pokazati. Denimo torej, da je $d = p-1$ in naj bo $h = g+p$. Tedaj je h primitivni koren po modulu p, saj je $h \equiv g \pmod{p}$. Po podobnem razmisleku kot prej je red $h \in U_{p^2}$ enak $p(p-1)$ ali $p-1$. Ker je $d = p - 1\mathrm{m}$ velja $g^{p-1} \equiv 1 \pmod{p^2}$, zato po izreku 4.3.1 sledi

$$h^{p-1} = (g+p)^{p-1} = \binom{p-1}{0}g^{p-1} + \binom{p-1}{1}g^{p-2}p +$$

$$+\binom{p-1}{2}g^{p-3}p^2 + \ldots + \binom{p-1}{p-2}gp^{p-2} + \binom{p-1}{p-1}p^{p-1} \equiv 1 - pg^{p-2} \pmod{p^2}.$$

Števili g in p sta tuji, zato velja $pg^{p-2} \not\equiv 0 \pmod{p^2}$ in zato je $h^{p-1} \not\equiv 1 \pmod{p^2}$. Torej red $h \in U_{p^2}$ ni enak $p-1$, od koder po zgornjem sledi, da je h v U_{p^2} reda $p(p-1)$ in zato je primitivni koren po modulu p^2.

Utemeljimo sedaj še drugega od zgoraj napovedanih korakov. Naj bo h poljuben primitivni koren po modulu p^2. Z indukcijo na e pokažemo, da je h primitivni koren po modulu p^e za vse $e \geq 2$. Predpostavimo torej, da je h primitivni koren po modulu p^e za nek $e \geq 2$. Pokazati želimo, da je h primitivni koren tudi po modulu p^{e+1}. Red elementa h v grupi $U_{p^{e+1}}$ označimo z d. Podobno kot v prvem delu dokaza velja, da je $h^d \equiv 1 \pmod{p^{e+1}}$ in zato tudi $h^d \equiv 1 \pmod{p^e}$. Po posledici 2.1.3 torej d deli $\varphi(p^{e+1}) = p^e(p-1)$, hkrati pa je deljiv s $\varphi(p^e) = p^{e-1}(p-1)$. Po enakem razmisleku kot prej velja, da je $d = p^e(p-1)$ ali pa je $d = p^{e-1}(p-1)$. V kolikor je $d = p^e(p-1)$, je h primitivni koren po modulu p^{e+1}, zato denimo nasprotno, da je $d = p^{e-1}(p-1)$.
Red primitivnega korena h po modulu p^e je $\varphi(p^e) = p^{e-1}(p-1)$, zato velja $h^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$. Ker je h tuj številu p^e, je tuj tudi številu p^{e-1}, zato $h \in U_{p^{e-1}}$. Po trditvi 4.1.7 je red grupe $U_{p^{e-1}}$ enak $\varphi(p^{e-1}) = p^{e-2}(p-1)$. Tedaj po izreku 4.1.9 velja $h^{p^{e-2}(p-1)} \equiv 1 \pmod{p^{e-1}}$. Od tod sledi, da je $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$, pri čemer je k neko naravno število, ki je tuje številu p. Sledi enakost

$$h^{p^{e-1}(p-1)} = (h^{p^{e-2}(p-1)})^p = (1+kp^{e-1})^p = 1 + \binom{p}{1}kp^{e-1} + \binom{p}{2}(kp^{e-1})^2 +$$
$$+\binom{p}{3}(kp^{e-1})^3 + \ldots + \binom{p}{p-1}(kp^{e-1})^{p-1} + \binom{p}{p}(kp^{e-1})^p = 1 + kp^e +$$
$$+k^2(p^{e-1})^2\frac{p(p-1)}{2} + k^3(p^{e-1})^3\frac{p(p-1)(p-2)}{6} + \ldots + pk^{p-1}(p^{e-1})^{p-1} + k^p(p^{e-1})^p.$$

Vsi členi od vključno četrtega dalje so deljivi s $(p^{e-1})^3$ in zato tudi s p^{e+1}, saj je $3(e-1) = 3e-3 = e+1+2(e-2) \geq e+1$ za $e \geq 2$. Sledi

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e + k^2p^{2e-2}\frac{p(p-1)}{2} \pmod{p^{e+1}}. \tag{4.1}$$

Ker je p liho praštevilo, je število $p-1$ sodo in s tem deljivo z 2, posledično pa p^{e+1} deli $k^2p^{2e-2}\frac{p(p-1)}{2}$, saj je $2e-2 = e+e-2 \geq e$. Torej je

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \pmod{p^{e+1}}.$$

Ker je k tuje p, velja

$$h^{p^{e-1}(p-1)} \not\equiv 1 \pmod{p^{e+1}},$$

kar je v protislovju s predpostavko, da je $d = p^{e-1}(p-1)$.

□

Opomba. Denimo, da je $p = 2$. Potemtakem število $k^2 p^{2e-2} \frac{p(p-1)}{2} = k^2 2^{2e-2}$ iz (4.1) za $e = 2$ ni deljivo z $2^{e+1} = 2^3$. Zato dokaz izreka 4.3.2 deluje le za liha praštevila p.

Zgled. Vzemimo grupo enot U_5. Število 2 je primitivni koren po modulu 5, saj je njegov red v U_5 enak redu grupe U_5, to je $\varphi(5) = 4$. Po dokazu izreka 4.3.2 je 2 bodisi primitivni koren po modulu 25, bodisi je red 2 v U_{25} enak 4. Ker je $2^4 = 16 \neq 1$ v U_{25}, je torej 2 primitivni koren po modulu 25, torej je po trditvi 4.1.17 njegov red v U_{25} enak $\varphi(25) = 20$.
Sedaj vzemimo število 7. Ker je $7 \equiv 2 \pmod 5$, število 2 pa generira grupo U_5, je tudi 7 primitivni koren po modulu 5. Red elementa $7 \in U_{25}$ je 4, saj je $7^4 = (7^2)^2 \equiv (-1)^2 \equiv 1 \pmod{25}$, zato 7 ni primitivni koren po modulu 25. Dokaz izreka 4.3.2 zagotavlja, da je $7 + 5 \equiv 12 \pmod{25}$ primitivni koren po modulu 25. Bralec se lahko prepriča, da je 12 res reda 20 v U_{25}.

Zgled. Pokažimo, da je 3 primitivni koren po modulu 7^e za vse $e \geq 1$. Pokazati moramo le, da je 3 primitivni koren po modulu 7 in po modulu 49. V kolikor je to res, potem po dokazu izreka 4.3.2 sledi, da je 3 primitivni koren po modulu 7^e za vse $e \geq 1$. Ker je $3^6 = (3^2)^3 \equiv 2^3 \equiv 1 \pmod 7$ in $3^3 \equiv -1 \pmod 7$, je 3 primitivni koren po modulu 7. Bralec se lahko prepriča, da red elementa 3 v U_{49} ni 6, od koder po dokazu izreka 4.3.2 sledi, da element 3 res generira celo grupo U_{49}, zato je ta element primitivni koren po modulu 49. Ker je 3 primitivni koren po modulu 7 in po modulu 49, po dokazu izreka 4.3.2 sledi, da je 3 primitivni koren po modulu 7^e za vse $e \geq 1$.

4.4 Grupa U_{2^e}

V prejšnjem razdelku smo pokazali, da je grupa U_{p^e} ciklična za vsa naravna števila e in za vsa liha praštevila p, nismo pa obravnavali cikličnosti te grupe, ko je p edino sodo praštevilo. Zato v tem razdelku proučujemo cikličnost grupe U_{2^e}, pri čemer je $e \geq 1$. Ta grupa je zanimiva, a ne zato, ker je ciklična le za nekatere vrednosti e, ampak zato, ker je število 5 "skoraj" primitivni koren po modulu 2^e za $e \geq 3$ in zato je ta grupa "skoraj" ciklična. Slednjemu dejstvu se posvetimo v zaključku razdelka.

Izrek 4.4.1 *Grupa U_{2^e} je ciklična le za naravni števili $e = 1$ in $e = 2$.*

Dokaz. Najprej si oglejmo cikličnost grupe enot U_{2^e} za naravni števili $e = 1$ in $e = 2$. Jasno je, da je trivialna grupa $U_2 = \{1\}$ ciklična. Prav tako pa je tudi $U_4 = \{1, 3\}$ ciklična, saj je 3 primitivni koren po modulu 4. Da dokončamo dokaz izreka, moramo torej pokazati, da grupa U_{2^e} ni ciklična za naravna števila $e \geq 3$. To storimo tako, da pokažemo, da za $e \geq 3$ ne obstaja primitivni koren po modulu 2^e. Dokazujemo torej, da v primeru, ko je $e \geq 3$, grupa U_{2^e} ne vsebuje elementa reda $\varphi(2^e) = 2^{e-1}$. Z indukcijo na e pokažimo, da za vsa naravna števila $e \geq 3$ in za vsa liha števila a velja

$$a^{2^{e-2}} \equiv 1 \pmod{2^e}. \tag{4.2}$$

Naj bo $e = 3$ in naj bo $a = 2b + 1$, pri čemer je b poljubno naravno število. Tedaj velja $a^{2^{e-2}} = a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1 \equiv 1 \pmod{8}$, saj je eno od števil b in $b+1$ sodo. Torej enakost (4.2) velja za $e = 3$ in za vsa liha števila a. Predpostavimo, da enakost (4.2) velja za nek $e \geq 3$. Tedaj za vsako liho število a velja

$$a^{2^{e-2}} = 1 + k \cdot 2^e,$$

pri čemer je k ustrezno celo število. Tedaj velja

$$a^{2^{(e+1)-2}} = (a^{2^{e-2}})^2 = (1 + 2^e k)^2 =$$

$$= 1 + 2^{e+1}k + 2^{2e}k^2 = 1 + 2^{e+1}(k + 2^{e-1}k^2) \equiv 1 \pmod{2^{e+1}}.$$

Potemtakem enakost (4.2) velja za vse $e \geq 3$ in vsa liha števila a. Torej U_{2^e} ne vsebuje primitivnega korena po modulu 2^e in zato U_{2^e} ni ciklična za $e \geq 3$.

□

Na tej točki najprej vpeljemo nov pojem in nato zapišemo trditev, s pomočjo katere dokažemo, da je grupa enot U_{2^e} "skoraj" ciklična, obenem pa nas to dejstvo pripelje do posledice, ki ima pomembno vlogo v zaključnem izreku magistrskega dela.

Definicija. Če je p praštevilo in n naravno število, potem zapis $p^e \parallel n$, kjer je e neko naravno število, pomeni, da je n deljiv s p^e, ni pa deljiv s p^{e+1}.

Trditev 4.4.2 *Za vsako celo število $n \geq 0$ velja $2^{n+2} \parallel 5^{2^n} - 1$.*

Dokaz. Dokaz opravimo z indukcijo na n. Trditev velja za $n = 0$, saj $2^2 \parallel 4$. Prepostavimo torej, da velja $2^{n+2} \parallel 5^{2^n} - 1$ za nek $n \geq 0$. Zapišemo

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1).$$

Ker je $5^{2^n} \equiv 1^{2^n} \equiv 1 \pmod 4$, velja $2 \parallel 5^{2^n} + 1$, po indukcijski predpostavki pa velja $2^{n+2} \parallel 5^{2^n} - 1$. Od tod sledi, da $2^{n+3} \parallel 5^{2^{n+1}} - 1$.

□

Trditev 4.4.3 *Naj bo e naravno število, pri čemer je $e \geq 3$. Tedaj je $U_{2^e} = \{\pm 5^i \mid 0 \leq i < 2^{e-2}\}$.*

Dokaz. Red elementa $5 \in U_{2^e}$ označimo z m. Po trditvi 4.1.7 je red grupe U_{2^e} enak $\varphi(2^e) = 2^{e-1}$. Po posledici 2.1.3 m deli $\varphi(2^e) = 2^{e-1}$, torej je $m = 2^k$ za nek $k \leq e-1$. Po izreku 4.4.1 grupa U_{2^e} ni ciklična, zato je $k \leq e-2$. Po trditvi 4.4.2 (za $n = e-3$) velja $2^{e-1} \parallel 5^{2^{e-3}} - 1$. Tedaj $5^{2^{e-3}} \not\equiv 1 \pmod{2^e}$ in zato $k > e-3$. Sledi, da je $k = e-2$, torej je $m = 2^{e-2}$. Grupo U_{2^e} tvorijo vsa liha števila, ki so manjša ali enaka $2^e - 1$. Element $5 \in U_{2^e}$ generira polovico vseh elementov te grupe, to je 2^{e-2} elementov, kjer so vsi oblike 5^i za $0 \leq i < 2^{e-2}$. Ker pa je $5 \equiv 1 \pmod 4$, je ta polovica elementov kongruentna 1 po modulu 4. Preostala polovica elementov je kongruentna -1 po modulu 4, torej so ti elementi oblike -5^i za $0 \leq i < 2^{e-2}$. Od tod sledi, da lahko vsak element grupe U_{2^e} zapišemo kot 5^i ali kot -5^i za nek $i \in \{0, 1, 2, \ldots, 2^{e-2} - 1\}$.

□

Dokaz trditve 4.4.3 pove, da je grupa U_{2^e} generirana z elementoma -1 in 5. Element $-1 \in U_{2^e}$ generira ciklično podgrupo reda 2, ki je izomorfna grupi $\mathbb{Z}_2$, medtem ko $5 \in U_{2^e}$ generira ciklično podgrupo reda 2^{e-2}, ki je izomorfna grupi $\mathbb{Z}_{2^{e-2}}$.

Trditev 4.4.4 *Naj bo $e \geq 3$. Vsak element $a \in U_{2^e}$ lahko enolično zapišemo kot $a = (-1)^j 5^i$, pri čemer je $0 \leq i < 2^{e-2}$ in $j \in \{0, 1\}$.*

Dokaz. Pokazati moramo, da, če velja $(-1)^j 5^i = (-1)^{j'} 5^{i'}$ za $j \in \{0, 1\}$ in $0 \leq i, i' < 2^{e-2}$, potem je $j = j'$ in $i = i'$. Iz enakosti $(-1)^j 5^i = (-1)^{j'} 5^{i'}$ sledi enakost $(-1)^{j-j'} = 5^{i'-i'}$. Tedaj obstajata dve možnosti. Najprej, če je $j - j' = 1$, potem je $(-1)^{j-j'} = -1$, česar pa ne moremo zapisati kot $5^{i'-i}$, pri čemer je $0 \leq i, i' < 2^{e-2}$, saj smo že v dokazu trditve 4.4.3 omenili, da je $-1 \equiv 3 \pmod 4$ in $5 \equiv 1 \pmod 4$. Če pa je $j - j' = 0$, potem je $(-1)^{j-j'} = 1$, kar pa lahko zapišemo kot $5^{i'-i}$, če je $i' - i = 0$. Od tod sledi, da je $j = j'$ in $i = i'$.

□

Posledica 4.4.5 *Naj bo $e \geq 3$. Tedaj je $U_{2^e} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$.*

Zgled. Vzemimo grupo U_{32}. To grupo tvorijo vsi najmanjši lihi predstavniki ekvivalenčnih razredov kolobarja $\mathbb{Z}_{32}$, ki so manjši od 31. Vsak njen element lahko po trditvi 4.4.4 enolično zapišemo kot $(-1)^j 5^i$ za $j \in \{0, 1\}$ ter $i \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Torej je $5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 \equiv 25$, $5^3 = 125 \equiv 29$, $5^4 = 25^2 = 625 \equiv 17$, $5^5 = 5^4 \cdot 5 \equiv 17 \cdot 5 \equiv 21$, $5^6 = 5^5 \cdot 5 \equiv 21 \cdot 5 \equiv 9$, $5^7 = 5^6 \cdot 5 \equiv 9 \cdot 5 \equiv 13$ in $-5^0 = -1 \equiv 31$, $-5^1 \equiv 27$, $-5^2 = -25 \equiv 7$, $-5^3 = -125 \equiv 3$, $-5^4 = -625 \equiv 15$, $-5^5 \equiv 11$, $-5^6 \equiv 23$ in $-5^7 \equiv 19$ vse po (mod 32).

Trditev 4.4.6 *Naj bo e naravno število, pri čemer je $e \geq 3$. Tedaj je $U_{2^e} = \{\pm 3^i \mid 0 \leq i < 2^{e-2}\}$.*

Dokaz. Dokaz opravimo v dveh korakih. Najprej z indukcijo pokažimo, da je

$$2^{n+2} \parallel 3^{2^n} - 1 \tag{4.3}$$

za vse $n \geq 1$, nato pa pokažimo, da je element $3 \in U_{2^e}$ reda 2^{e-2} za vse $e \geq 3$.
Za $n = 1$ velja $2^3 \parallel 8$. Predpostavimo torej, da velja $2^{n+2} \parallel 3^{2^n} - 1$ za nek $n \geq 1$. Zapišemo

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

Ker je $3^{2^n} \equiv (-1)^{2^n} \equiv 1 \pmod 4$, velja $2 \parallel 3^{2^n} + 1$, po indukcijski predpostavki pa velja $2^{n+2} \parallel 3^{2^n} - 1$. Od tod sledi, da $2^{n+3} \parallel 3^{2^{n+1}} - 1$.

Nadaljujemo z drugim korakom dokaza. Red elementa 3 v U_{2^e} označimo z m. Po trditvi 4.1.7 je red grupe U_{2^e} enak $\varphi(2^e) = 2^{e-1}$. Na podoben način, kot smo to storili v dokazu izreka 4.4.3, tudi tukaj ugotovimo, da je $m = 2^{e-2}$. Element $3 \in U_{2^e}$ generira polovico elementov te grupe, to je 2^{e-2} elementov, kjer so vsi oblike 3^i za $0 \leq i < 2^{e-2}$. Ta polovica elementov je kongruentna 1 ali 3 $\pmod 8$, preostala polovica elementov pa je oblike -3^i in je zato ta polovica elementov kongruentna -1 ali $-3 \pmod 8$. Od tod sledi, da lahko vsak element grupe U_{2^e} zapišemo kot 3^i ali -3^i za nek $i \in \{0, 1, 2, \ldots, 2^{e-2} - 1\}$.

□

4.5 Grupa U_{2p^e}

V prejšnjem razdelku smo spoznali, da je grupa U_{2^e} ciklična le za naravni števili $e = 1$ in $e = 2$. V tem razdelku pokažemo, da je U_{2p^e} ciklična za vsa liha praštevila p in za vsa naravna števila e.

Trditev 4.5.1 *Naj bo p liho praštevilo. Tedaj je U_{2p^e} ciklična za vsa naravna števila e.*

Dokaz. Po trditvi 4.1.7 je red U_{2p^e} enak $\varphi(2p^e)$. Po izreku 4.1.6 velja $\varphi(2p^e) = \varphi(2) \cdot \varphi(p^e) = \varphi(p^e)$. Po izreku 4.3.2 obstaja primitivni koren g po modulu p^e. Seveda je tudi $g+p^e$ primitivni koren po modulu p^e in eden od teh dveh primitivnih korenov po modulu p^e je lih. Ta lih primitivni koren po modulu p^e označimo s h. Pokažimo, da je h primitivni koren po modulu $2p^e$. Ker je število h primitivni koren po modulu p^e in je liho število, je tuje številoma 2 in p^e in zato je tuje tudi $2p^e$. Tedaj je $h \in U_{2p^e}$. Naj bo i takšno naravno število, da velja $h^i \equiv 1 \pmod{2p^e}$. Potemtakem velja tudi $h^i \equiv 1 \pmod{p^e}$. Ker je h primitivni koren po modulu p^e, red grupe U_{p^e}, to je $\varphi(p^e)$, deli i. Ker je $\varphi(2p^e) = \varphi(p^e)$, tudi $\varphi(2p^e)$ deli i, zato je h reda $\varphi(2p^e)$ v U_{2p^e}. Torej je h primitivni koren po modulu $2p^e$.

□

4.6 Cikličnost U_n

Najprej smo ugotovili, da je grupa enot U_p ciklična, pri čemer je p poljubno praštevilo. Nato smo pokazali, da je tudi grupa U_{p^e} ciklična za vsa liha praštevila p in za vsa naravna števila e. Navsezadnje smo pokazali, da je grupa U_{2^e} ciklična le za prvi dve naravni števili e in da je grupa U_{2p^e} ciklična za vsa liha praštevila p in za vsa naravna števila e. V tem razdelku zberemo vsa do sedaj spoznana dejstva o cikličnosti U_n in pokažemo, da so to pravzaprav edine vrednosti števila n, za katere je grupa U_n ciklična. Da bi to dokazali, moramo najprej zapisati še naslednjo pomožno trditev in njen dokaz.

Trditev 4.6.1 *Število $\varphi(n)$ je liho le za naravni števili $n = 1$ in $n = 2$.*

Dokaz. Za $n = 1$ in $n = 2$ je število $\varphi(n)$ liho, saj je $\varphi(2) = \varphi(1) = 1$. Sedaj pokažimo še, da je število $\varphi(n)$ za vse $n \geq 3$ sodo. Če je $n \geq 3$, potem je n deljiv z lihim praštevilom p ali s številom 4 (lahko velja tudi oboje). Prafaktorizacija števila n je enaka $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, kjer so p_i paroma različna praštevila in k je naravno število. Po izreku 4.1.6 velja enakost $\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$. Torej velja $(p-1) \mid \varphi(n)$ ali $2 \mid \varphi(n)$. V vsakem primeru je $\varphi(n)$ sodo število.

□

Trditev 4.6.2 *Naj bo n takšno naravno število, da za naravni števili $r, s > 2$, kjer je $D(r, s) = 1$, velja $n = rs$. Potem grupa U_n ni ciklična.*

Dokaz. Po izreku 4.1.6 velja $\varphi(n) = \varphi(r)\varphi(s)$. Po trditvi 4.6.1 sta $\varphi(r)$ in $\varphi(s)$ sodi števili, zato je število $\varphi(n)$ deljivo s 4 in zato je naravno število $k = \frac{\varphi(n)}{2}$ deljivo s $\varphi(r)$ in $\varphi(s)$. Naj bo $a \in U_n$. Ker je a tuje n, je tuje tudi r in s, zato velja $a \in U_r$ ter $a \in U_s$. Po posledici 2.1.4 velja $a^{\varphi(r)} \equiv 1 \pmod{r}$ in $a^{\varphi(s)} \equiv 1 \pmod{s}$. Ker $\varphi(r)$ in $\varphi(s)$ delita k, po trditvi 4.1.10 sledi $a^k \equiv 1 \pmod{r}$ in $a^k \equiv 1 \pmod{s}$. Ker sta si r in s tuji števili, potem po trditvi 3.1.9 sledi, da je $a^k \equiv 1 \pmod{rs}$, torej $a^k \equiv 1 \pmod{n}$. Tedaj ne obstaja primitivni koren po modulu n, saj je $k < \varphi(n)$.

□

Izrek 4.6.3 *Naj bo $n \geq 2$ naravno število. Tedaj je grupa U_n ciklična natanko tedaj, ko je $n \in \{2, 4\}$, ali pa je n oblike p^e ali $2p^e$, kjer je p liho praštevilo in e naravno število.*

Dokaz. Že v prejšnjih razdelkih smo pokazali, da je grupa U_n ciklična za vse $n \in \{2, 4\}$ in n oblike p^e ali $2p^e$, kjer je p liho praštevilo in e naravno število. Zato moramo pokazati le še, da grupa U_n ni ciklična za vsa preostala naravna števila n.

Če $n \notin \{2, 4\}$, ali pa ni oblike p^e ali $2p^e$, kjer je p liho praštevilo in e naravno število, potem velja;

(i) $n = 2^e$, pri čemer je $e \geq 3$, ali

(ii) $n = 2^e p^f$, pri čemer sta $e \geq 2$ in $f \geq 1$, ter je p liho praštevilo, ali

(iii) n je deljiv s produktom vsaj dveh različnih lihih praštevil.

V primeru (i) po izreku 4.4.1 grupa U_n ni ciklična. V primeru (ii) gre za produkt dveh tujih števil, torej $r = 2^e$ in $s = p^f$, ki sta obe večji od 2. Tedaj po trditvi 4.6.2 grupa U_n ni ciklična. V primeru (iii) je n deljiv s produktom vsaj dveh različnih praštevil, ki sta večji od 2, na primer p in q. Naj bo t takšno naravno število, da $p^t \parallel n$. Potem je število $\frac{n}{p^t}$ še vedno deljivo s q in je torej večje od 2. Tedaj lahko število n zapišemo kot produkt dveh tujih si števil, torej $n = p^t \cdot \frac{n}{p^t}$, pri čemer sta obe števili večji od 2. Po trditvi 4.6.2 sledi, da grupa U_n v tem primeru ni ciklična. □

4.7 Kitajski izrek o ostankih

Preden nadaljujemo z naslednjim poglavjem, kjer dokončno opišemo strukturo grupe enot kolobarja $\mathbb{Z}_n$, zapišimo kitajski izrek o ostankih, s pomočjo katerega v poglavju, ki sledi, pokažemo, kateri grupi je izomorfna grupa enot U_n kolobarja $\mathbb{Z}_n$, ko ni ciklična. Kitajski izrek o ostankih ima namreč pomembno vlogo tudi pri reševanju kongruenčnih enačb v zadnjem poglavju. Zato je bralec v tem razdelku seznanjen z linearnimi kongruencami in njihovimi rešitvami ter z omenjenim kitajskim izrekom o ostankih in njegovim dokazom.

Dokaz naslednjega izreka lahko bralec najde v [7].

Izrek 4.7.1 *Naj bodo a, b in n naravna števila in naj bo $d = D(a, n)$. Tedaj ima linearna kongruenčna enačba $ax \equiv b \pmod{n}$ rešitev v celih številih natanko*

tedaj, ko d deli b. Če je x_0 poljubna rešitev te enačbe, potem je vsaka rešitev te enačbe oblike

$$x = x_0 + \frac{nt}{d},$$

kjer je $t \in \mathbb{Z}$. Rešitve te enačbe v tem primeru tvorijo natanko d kongruenčnih razredov (mod n) *s predstavniki*

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

Posledica 4.7.2 *Naj bodo a, b in n naravna števila. Če je $D(a, n) = 1$, rešitve linearne kongruenčne enačbe $ax \equiv b \pmod{n}$ tvorijo en sam kongruenčni razred po modulu n.*

Izrek 4.7.3 *(Kitajski izrek o ostankih). Naj bodo $n_1, n_2, \ldots, n_k$ paroma tuja si naravna števila. Naj bodo $a_1, a_2, \ldots, a_k$ taka cela števila, da za vsak $i \in \{1, 2, \ldots, k\}$ velja $0 \leq a_i < n_i$. Tedaj obstaja celo število x, ki zadošča sistemu linearnih kongruenc*

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

Vsaki dve števili, ki zadoščata zgornjemu sistemu, sta si kongruentni po modulu $n_1 n_2 \cdots n_k$.

Dokaz. Najprej bomo dokazali, da je v primeru, ko rešitev obstaja, le-ta enolična do modula $n_1 n_2 \cdots n_k$ natančno, nato pa bomo dokazali obstoj rešitve.
Naj bosta $x, y \in \mathbb{Z}$ rešitvi sistema. Tedaj velja

$$\begin{aligned} x - y &\equiv 0 \pmod{n_1} \\ x - y &\equiv 0 \pmod{n_2} \\ &\vdots \\ x - y &\equiv 0 \pmod{n_k}. \end{aligned}$$

Torej števila $n_1, n_2, \ldots, n_k$ vsa delijo $x - y$. Ker so števila $n_1, n_2, \ldots, n_k$ paroma tuja, tudi njihov produkt $n_1 n_2 \ldots n_k$ deli $x - y$. Torej je

$$x \equiv y \pmod{n_1 n_2 \cdots n_k}.$$

Naj bo $N = n_1 n_2 \cdots n_k$ in $C_i = \frac{N}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$ za $i = 1, \ldots, k$. Velja $D(C_i, n_i) = 1$ za vse i, saj so vsa števila $n_1, n_2, \ldots, n_k$ paroma tuja. Od tod po izreku 4.7.1 sledi, da je vsaka od kongruenc

$$C_i x \equiv 1 \pmod{n_i}$$

rešljiva. Za vsak i, $1 \leq i \leq k$, z x_i označimo neko rešitev kongruence $C_i x_i \equiv 1 \pmod{n_i}$. Trdimo, da je

$$x = C_1 x_1 a_1 + C_2 x_2 a_2 + \ldots + C_k x_k a_k$$

rešitev našega sistema. Za poljuben $i = 1, 2, \ldots, k$ je $C_i x_i \equiv 1 \pmod{n_i}$ oziroma $C_i x_i a_i \equiv a_i \pmod{n_i}$, za vse j, ki so različni od i, pa velja $C_j x_j a_j \equiv 0 x_j a_j \equiv 0 \pmod{n_i}$, saj $n_i \mid C_j$, zato je

$$x \equiv a_i \pmod{n_i},$$

za vse $i = 1, \ldots, k$. S tem smo utemeljili obstoj rešitve našega sistema linearnih kongruenc.

□

Zgled. Poiščimo rešitev sistema linearnih kongruenčnih enačb

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

Izrek 4.7.3 nam zagotavlja, da obstaja rešitev x po modulu $7 \cdot 5 \cdot 3 = 105$. Običajno najprej poiščemo rešitev x linearne kongruenčne enačbe z največjim modulom, v našem primeru je to kongruenčna enačba $x \equiv 2 \pmod{7}$. Najbolj očitna rešitev te linearne kongruenčne enačbe je 2. Ostale rešitve te enačbe dobimo s prištevanjem in odštevanjem večkratnikov števila 7, zato je poljubna rešitev oblike $x = 2 + 7t$, kjer je t poljubno celo število. Sedaj med vsemi takimi števili $x = 2 + 7t$ poiščemo tiste, ki so hkrati rešitve linearne kongruenčne enačbe

$x \equiv 3 \pmod 5$. To storimo tako, da rešitev kongruenčne enačbe z največjim modulom, $x = 2 + 7t$, vstavimo v kongruenčno enačbo $x \equiv 3 \pmod 5$. Tedaj iščemo rešitve t kongruenčne enačbe $2 + 7t \equiv 3 \pmod 5$. Od tod sledi, da je $2t \equiv 1 \pmod 5$. Če desno in levo stran te kongruenčne enačbe pomnožimo s 3, dobimo kongruenčno enačbo oblike $t \equiv 3 \pmod 5$. Poljubna rešitev te kongruenčne enačbe je oblike $t = 3 + 5l$, pri čemer je l poljubno celo število. Tedaj je poljubna rešitev kongruenčnih enačb $x \equiv 2 \pmod 7$ in $x \equiv 3 \pmod 5$ oblike $x = 2 + 7 \cdot (3 + 5l) = 23 + 35l$. Navsezadnje med vsemi takimi števili poiščemo tiste, ki so hkrati rešitve še zadnje kongruenčne enačbe $x \equiv 2 \pmod 3$. Rešitev $x = 23 + 35l$ prejšnjih dveh kongruenčnih enačb vstavimo v kongruenčno enačbo $x \equiv 2 \pmod 3$. Tedaj išemo rešitve l kongruenčne enačbe $23 + 35l \equiv 2 \pmod 3$. To kongruenčno enačbo nekoliko preuredimo in dobimo $l \equiv 0 \pmod 3$. Poljubna rešitev te kongruenčne enačbe je oblike $l = 0 + 3m$, kjer je m poljubno celo število. Rešitev zgornjega sistema linearnih kongruenčnih enačb je tako $x = 23 + 35 \cdot (0 + 3m) = 23 + 105m$. Drugače zapisano, rešitev zgornjega sistema linearnih kongruenčnih enačb je kongruenčni razred [23] po modulu 105.

Poglavje 5

Algebraična struktura U_n

V tem poglavju dokončno opišemo strukturo grupe enot kolobarja $\mathbb{Z}_n$. Proti koncu prejšnjega poglavja smo pokazali, da je za določena naravna števila n grupa enot U_n ciklična. Tedaj je grupa enot U_n izomorfna kar ciklični grupi $\mathbb{Z}_{\varphi(n)}$. Za preostale vrednosti števila n grupa U_n ni ciklična, zato je po izreku 3.2.3 izomorfna direktnemu produktu vsaj dveh cikličnih grup. V tem poglavju torej pokažemo, kateri grupi je izomorfna grupa enot U_n kolobarja $\mathbb{Z}_n$, ko ni ciklična. Poglavje je povzeto po [2], [3] in [5].

5.1 Direktni produkt kolobarjev

V tem razdelku pokažemo, da lahko končni kolobar $\mathbb{Z}_n$ zapišemo kot direktni produkt manjših kolobarjev te oblike in njegovo grupo enot U_n zapišemo kot direktni produkt cikličnih grup glede na prafaktorizacijo naravnega števila n. Preučevanje strukture grupe U_n kolobarja $\mathbb{Z}_n$ se zato omeji na vrednosti prafaktorizacije števila n, kar smo že obravnavali v prejšnjih poglavjih. V tem razdelku si najprej ogledamo, v kakšnem odnosu sta kolobarja $\mathbb{Z}_n$ in $\mathbb{Z}_l$, ko l deli n. Nato si ogledamo, v kakšnem odnosu so kolobarji $\mathbb{Z}_n, \mathbb{Z}_l$ in $\mathbb{Z}_m$, ko je $n = lm$, pri čemer sta l in m tuji števili.

Definicija. Naj bosta $\mathbb{Z}_l$ in $\mathbb{Z}_n$ kolobarja in naj bo $a \in \mathbb{Z}$. Ekvivalenčni razred a v kolobarju $\mathbb{Z}_l$ označimo z $[a]_l$, ekvivalenčni razred a v kolobarju $\mathbb{Z}_n$ pa označimo z $[a]_n$.

Trditev 5.1.1 *Naj bosta l in n naravni števili in naj bosta $a, a' \in \mathbb{Z}$. Če $l \mid n$ in velja $a \equiv a' \pmod{n}$, potem je tudi $a \equiv a' \pmod{l}$. Velja torej $[a]_n \subseteq [a]_l$.*

Dokaz. Denimo torej, da velja $l \mid n$ in $a \equiv a' \pmod{n}$. Po definiciji n deli $a' - a$. Ker l deli n, potem l deli tudi $a' - a$, zato velja $a \equiv a' \pmod{l}$.

□

Trditev 5.1.2 *Naj bosta l in n naravni števili in naj velja $l \mid n$. Naj bo ϕ preslikava $\phi : \mathbb{Z}_n \to \mathbb{Z}_l$, ki vsak ekvivalenčni razred iz $\mathbb{Z}_n$ preslika v tisti ekvivalenčni razred iz $\mathbb{Z}_l$, ki ga vsebuje, to je $\phi([a]_n) = [a]_l$. Tedaj je ϕ homomorfizem kolobarjev.*

Dokaz. Ker za $[a]_n, [b]_n \in \mathbb{Z}_n$ velja $[a]_n + [b]_n = [a + b]_n$, je $\phi([a]_n + [b]_n) = \phi([a + b]_n) = [a + b]_l$, prav tako pa je $\phi([a]_n) + \phi([b]_n) = [a]_l + [b]_l = [a + b]_l$. Za $[a]_n, [b]_n \in \mathbb{Z}_n$ velja $[a]_n \cdot [b]_n = [a \cdot b]_n$, zato je $\phi([a]_n \cdot [b]_n) = \phi([a \cdot b]_n) = [a \cdot b]_l$, prav tako pa je $\phi([a]_n) \cdot \phi([b]_n) = [a]_l \cdot [b]_l = [a \cdot b]_l$. Tedaj je ϕ res homomorfizem kolobarjev $\mathbb{Z}_n$ in $\mathbb{Z}_l$.

□

Opomba. Če sta l in n naravni števili, pri čemer $l \mid n$, potem obstaja naravno število m, da velja $n = lm$. Podobno kot smo v trditvi 5.1.2 definirali preslikavo ϕ za l, sedaj definiramo preslikavo $\phi' : \mathbb{Z}_n \to \mathbb{Z}_m$ s predpisom $\phi'([a]_n) = [a]_m$. Trditev 5.1.2 pove, da je tudi ϕ' homomorfizem kolobarjev $\mathbb{Z}_n$ in $\mathbb{Z}_m$.

Opomba. V tem primeru homomorfizmoma ϕ in ϕ' rečemo *naravna homomorfizma.*

Posledica 5.1.3 *Naj bodo n, m in l taka naravna števila, da velja $n = lm$. Tedaj za preslikavo ϕ iz trditve 5.1.2 velja $\phi(U_n) \subseteq U_l$, pripadajoča skrčitev $\phi^* : U_n \to U_l$ pa je homomorfizem grup.*

Dokaz. Če je celo število a tuje številu n, je a enota kolobarja $\mathbb{Z}_n$. Tedaj je a tuje tudi številu l, zato je tudi enota kolobarja $\mathbb{Z}_l$, torej velja $\phi(U_n) \subseteq U_l$. Od tod po trditvi 5.1.2 sledi, da je $\phi^* : U_n \to U_l$ homomorfizem grup.

□

Opomba. Po podobnem razmisleku je tudi skrčitev homomorfizma ϕ' na $\phi'^* : U_n \to U_m$ homomorfizem grup.

Trditev 5.1.4 *Za poljubni naravni števili l in m in za pripadajoča kolobarja $\mathbb{Z}_l$ in $\mathbb{Z}_m$ velja $(\mathbb{Z}_l \times \mathbb{Z}_m)^* = U_l \times U_m$.*

Dokaz. Elementi množice $(\mathbb{Z}_l \times \mathbb{Z}_m)^*$ so urejeni pari $([a]_l, [b]_m) \in \mathbb{Z}_l \times \mathbb{Z}_m$, ki imajo inverz, torej za katere obstaja $([a']_l, [b']_m) \in \mathbb{Z}_l \times \mathbb{Z}_m$, da velja $([a]_l, [b]_m) \cdot ([a']_l, [b']_m) = ([1]_l, [1]_m)$. To pa pomeni, da mora veljati $[a]_l \cdot [a']_l = [1]_l$ ter $[b]_m \cdot [b']_m = [1]_m$. Od tod pa sledi, da je $[a]_l \in U_l$ ter $[b]_m \in U_m$. Torej vsak element iz $(\mathbb{Z}_l \times \mathbb{Z}_m)^*$ je hkrati tudi element $U_l \times U_m$.
Vzemimo element $([a]_l, [b]_m) \in U_l \times U_m$. Ker je $[a]_l \in U_l$, ima inverz oblike $[a^{-1}]_l \in U_l$, in ker je $[b]_m \in U_m$, ima inverz oblike $[b^{-1}]_m \in U_m$. Ker je $([a]_l, [b]_m) \cdot ([a^{-1}]_l, [b^{-1}]_m) = ([1]_l, [1]_m)$, je $([a]_l, [b]_m) \in (\mathbb{Z}_l \times \mathbb{Z}_m)^*$.

□

Naslednja trditev je neposredna posledica trditve 5.1.2 in posledice 5.1.3.

Trditev 5.1.5 *Naj bodo n, l in m takšna naravna števila, da velja $n = lm$. Naj bosta $\phi : \mathbb{Z}_n \to \mathbb{Z}_l$ in $\phi' : \mathbb{Z}_n \to \mathbb{Z}_m$ naravna homomorfizma. Tedaj je preslikava $\theta : \mathbb{Z}_n \to \mathbb{Z}_l \times \mathbb{Z}_m$, podana s predpisom $\theta([a]_n) = ([a]_l, [a]_m)$, homomorfizem kolobarjev, skrčitev $\theta^* : U_n \to U_l \times U_m$ pa homomorfizem grup.*

Trditev 5.1.6 *Naj bodo n, l in m takšna naravna števila, da je $n = lm$ in $D(l, m) = 1$. Naj bosta $\phi : \mathbb{Z}_n \to \mathbb{Z}_l$ in $\phi' : \mathbb{Z}_n \to \mathbb{Z}_m$ naravna homomorfizma. Tedaj je homomorfizem $\theta : \mathbb{Z}_n \to \mathbb{Z}_l \times \mathbb{Z}_m$ iz trditve 5.1.5 izomorfizem kolobarjev, njegova skrčitev $\theta^* : U_n \to U_l \times U_m$ pa izomorfizem grup.*

Dokaz. Pokažimo, da je θ bijektivna preslikava. Ker je $D(l, m) = 1$, po izreku 4.7.3 za vsak par $([a]_l, [b]_m) \in \mathbb{Z}_l \times \mathbb{Z}_m$ obstaja natanko en kongruenčni razred $x \pmod{n}$, ki je rešitev sistema kongruenčnih enačb $x \equiv a \pmod{l}$ in $x \equiv b \pmod{m}$. Tedaj obstaja natanko en ekvivalenčni razred $[x]_n \in \mathbb{Z}_n$, da velja $\theta([x]_n) = ([a]_l, [b]_m)$. Od tod sledi, da je θ bijektivna preslikava, s tem pa po trditvi 5.1.5 izomorfizem kolobarjev $\mathbb{Z}_n$ in $\mathbb{Z}_l \times \mathbb{Z}_m$. Po trditvi 5.1.4 potem takoj sledi, da je $U_n \cong U_l \times U_m$, očitno pa je eden od pripadajočih izomorfizmov ravno θ^*.

□

5.2 Čemu je izomorfna grupa U_n?

V prejšnjem razdelku smo pokazali, da je kolobar $\mathbb{Z}_{lm}$ izomorfen direktnemu produktu $\mathbb{Z}_l \times \mathbb{Z}_m$, če sta l in m tuji števili. V tem razdelku zapišemo izrek, ki povzame

celotno poglavje.

Izrek 5.2.1 *Naj bo n naravno število in naj bo $n = n_1 \cdots n_k$, pri čemer je k naravno število, $n_1, \ldots, n_k$ pa so paroma tuja naravna števila, večja od 1. Tedaj je preslikava $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, dana s predpisom $\theta([a]_n) = ([a]_{n_1}, \ldots, [a]_{n_k})$, izomorfizem kolobarjev, skrčitev $\theta^* : U_n \to U_{n_1} \times \ldots U_{n_k}$ pa je izomorfizem grup. Če je $n = p_1^{e_1} \cdots p_k^{e_k}$, pri čemer so $p_1, \ldots, p_k$ paroma različna praštevila in so $e_1, \ldots, e_k$ naravna števila, potem velja*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}} \quad in \quad U_n \cong U_{p_1^{e_1}} \times \ldots \times U_{p_k^{e_k}}.$$

Dokaz. Z indukcijo na k in uporabo trditve 5.1.6.

□

Grupa enot U_n kolobarja $\mathbb{Z}_n$ je po izreku 4.6.3 ciklična natanko tedaj, ko je $n \in \{2, 4\}$, ali pa je oblike p^e ali $2p^e$, pri čemer je p liho praštevilo in e naravno število. V tem primeru je U_n izomorfna ciklični grupi $\mathbb{Z}_{\varphi(n)}$. V primeru, da grupa U_n ni ciklična, je izomorfna direktnemu produktu nekih cikličnih grup. Tedaj lahko s pomočjo dosedanjih rezultatov o grupi enot in njeni strukturi natančno določimo, kateri grupi je izomorfna grupa U_n. V ta namen vsa dosedanja spoznanja o grupi enot zapišemo v izreku, a najprej vpeljimo naslednjo oznako.

Definicija. Naj bo k naravno število in naj bodo $p_1, p_2, \ldots, p_k$ praštevila in $e_1, e_2, \ldots, e_k$ naravna števila. Tedaj direktni produkt grup $\mathbb{Z}_{p_1^{e_1}}, \mathbb{Z}_{p_2^{e_2}}, \ldots, \mathbb{Z}_{p_k^{e_k}}$, torej $\mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}}$, označimo z $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$.

Izrek 5.2.2 *Naj bo $n \geq 2$ poljubno naravno število in naj bo $n = 2^f \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ njegova prafaktorizacija, pri čemer je k nenegativno celo število, $p_1, \ldots, p_k$ so paroma različna liha praštevila, $e_1, \ldots, e_k$ so naravna števila in f je nenegativno celo število. Tedaj velja*

$$U_n \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{f-2}} \times \prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i-1}(p_i-1)} & \text{če } f \geq 2, \text{ in} \\ \prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i-1}(p_i-1)} & \text{če } f \leq 1. \end{cases} \tag{5.1}$$

Dokaz. Po izreku 5.2.1 velja $U_n \cong U_{2^f} \times U_{p_1^{e_1}} \times \ldots \times U_{p_k^{e_k}}$. Tedaj je red vsake posamezne grupe $U_{p_k{}^{e_k}}$, pri čemer je k nenegativno celo število, enak $\varphi(p_k^{e_k}) = p_k^{e_k-1}(p_k - 1)$. Po izreku 4.3.2 je $U_{p_k{}^{e_k}}$ ciklična za vsak $k \geq 1$, zato velja $U_{p_k^{e_k}} \cong \mathbb{Z}_{p_k^{e_k-1}(p_k-1)}$, pri čemer se razume, da, če je $f = 0$, potem grupo U_{2^f} izpustimo, če pa je $k = 0$, potem je $U_n \cong U_{2^f}$. Če je $f = 1$, potem je grupa U_{2^f} izomorfna trivialni grupi, če pa je $f \geq 2$, potem po posledici 4.4.5 vemo, da je $U_{2^f} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{f-2}}$.

□

Zgled. Vzemimo kolobar $\mathbb{Z}_{400}$ in določimo strukturo grupe enot U_{400}. Ker je $400 = 2^4 \cdot 5^2$, je v tem primeru $f = 4$, torej po izreku 5.2.2 velja $U_{400} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{20}$.

Zgled. Vzemimo sedaj kolobar $\mathbb{Z}_{242}$ in si oglejmo njegovo grupo enot U_{242}. S pomočjo faktorizacije dobimo $242 = 2 \cdot 11^2$. Tedaj je $f = 1$, zato je po izreku 5.2.2 grupa U_{242} ciklična, saj je $U_{242} \cong \mathbb{Z}_{110}$.

Zgled. Vzemimo sedaj še kolobar $\mathbb{Z}_{4725}$ in pripadajočo grupo enot U_{4725}. Ugotovimo, da je $4725 = 3^3 \cdot 5^2 \cdot 7$. Ker je $f = 0$, po izreku 5.2.2 velja, da je $U_{4725} \cong \mathbb{Z}_{18} \times \mathbb{Z}_{20} \times \mathbb{Z}_6$.

Poglavje 6

Reševanje kongruenčnih enačb

V tem poglavju magistrskega dela si oglejmo reševanje nekaterih kongruenčnih enačb, ki jih rešujemo s pomočjo dosedanjih spoznanj o grupi enot in njenih lastnostih. V tem poglavju torej podamo splošne rešitve kongruenčnih enačb oblike $x^m \equiv c \pmod{n}$, kjer so naravna števila m, c in n podana, vrednost celega števila x pa želimo izračunati. Izkaže se, da nam dosedanja spoznanja o grupi enot zelo olajšajo reševanje tovrstnih kongruenčnih enačb. Poglavje je povzeto po [2].

6.1 Kongruenčne enačbe

V tem razdelku si najprej oglejmo tri konkretne primere reševanja kongruenčnih enačb oblike $x^m \equiv c \pmod{n}$, pri čemer so m, c in n naravna števila, medtem pa opravimo splošno analizo in zapišemo postopek za iskanje splošne rešitve tovrstnih kongruenčnih enačb. V prvem zgledu rešimo kongruenčno enačbo oblike $x^m \equiv c \pmod{n}$, pri čemer je n poljubno praštevilo, v drugem zgledu pa iščemo rešitve tovrstne oblike kongruenčne enačbe, ko je n poljubna potenca edinega sodega praštevila. V zadnjem zgledu si ogledamo še reševanje omenjenih kongruenčnih enačb, ko v prafaktorizaciji števila n nastopata vsaj dve lihi praštevili.

Zgled. Dano imamo kongruenčno enačbo $x^6 \equiv 4 \pmod{23}$. Najprej opazimo, da mora biti vsaka rešitev x element grupe U_{23}. Po izreku 4.6.3 je ta grupa ciklična in zato obstaja primitivni koren g po modulu 23. Ker je $\varphi(23) = 22 = 2 \cdot 11$, ker velja $5^2 = 25 \equiv 2 \pmod{23}$ in $5^{11} = (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 \equiv 22 \pmod{23}$, je po trditvi 4.1.17 element 5 generator grupe U_{23}. Torej je rešitev kongruenčne enačbe

$x^6 \equiv 4 \pmod{23}$ oblike $x = 5^i$ za nek $0 \leq i \leq 22$. Ker je $5^4 \equiv (5^2)^2 \equiv 4 \pmod{23}$, torej rešujemo kongruenčno enačbo $5^{6i} \equiv 5^4 \pmod{23}$. Red primitivnega korena 5 po modulu 23 je $\varphi(23) = 22$, zato je $5^{6i} = 5^4$ natanko tedaj, ko je $6i \equiv 4 \pmod{22}$. Rešitvi linearne kongruenčne enačbe $3i \equiv 2 \pmod{11}$ sta $i = 8$ in $i = 19 \pmod{22}$, zato sta rešitvi začetne kongruenčne enačbe ravno $x = 5^8 = (5^4)^2 \equiv 4^2 \equiv 16 \pmod{23}$ ter $x = 5^{19} = (5^4)^4 \cdot 5^2 \cdot 5 \equiv 3 \cdot 2 \cdot 5 \equiv 7 \pmod{23}$. Rešitvi začetne kongruenčne enačbe $x^6 \equiv 4 \pmod{23}$ sta torej $\pm 7 \pmod{23}$.

Opomba. To je primer reševanja kongruenčnih enačb, ko obstaja nek primitivni koren g po modulu n, v zgornjem zgledu je na primer $g = 5$ in $n = 23$. Reševanje kongruenčne enačbe $x^m \equiv c \pmod{n}$ s pomočjo zapisa $x = g^i$ ter $c = g^b$, pri čemer so i, c, m, b naravna števila, na ta način pretvorimo v reševanje linearne kongruenčne enačbe $mi \equiv b \pmod{\varphi(n)}$. Rešitve te linearne kongruenčne enačbe nam določajo rešitve začetne nelinearne kongruenčne enačbe. Edino težavo pri tem predstavljata iskanje primitivnega korena g po modulu n in izražanje števila c, ki ga dobimo s potenciranjem primitivnega korena g po modulu n.

V naslednjem primeru si oglejmo primer kongruenčne enačbe oblike $x^m \equiv c \pmod{2^e}$, ko sta m in c naravni števili in $e \geq 3$.

Zgled. Dano imamo kongruenčno enačbo $x^{11} \equiv 7 \pmod{32}$. Po izreku 4.4.1 grupa U_{32} ni ciklična, zato ne obstaja primitivni koren po modulu 32. Po trditvi 4.4.4 lahko vsak element grupe U_{32} enolično zapišemo kot $\pm 5^i$, za nek $0 \leq i \leq 7$. Naj bo $x = \pm 5^i$ rešitev naše kongruenčne enačbe. Ugotovimo, da $-5^2 \equiv 7 \pmod{32}$, zato kongruenčno enačbo $x^{11} \equiv 7 \pmod{32}$ zapišemo kot $(\pm 5^{11i}) \equiv -5^2 \pmod{32}$. Denimo, da je $x = +5^i$. Tedaj velja $5^{11i} = -5^2$ v U_{32}, kar pa je nemogoče, saj je $5 \equiv 1 \pmod{4}$, torej so tudi vse potence števila 5 kongruentne $1 \pmod{4}$, medtem ko je $-5 \equiv 3 \pmod{4}$. Denimo, da je tokrat $x = -5^i$. Tedaj velja $5^{11i} \equiv 5^2 \pmod{32}$, kar pa velja natanko tedaj, ko $11i \equiv 2 \pmod{8}$, saj je red elementa $5 \in U_{32}$ enak 8. Rešitev te linearne kongruenčne enačbe je 6, zato je $x \equiv -5^6 \equiv -(5^3)^2 \equiv -(-3)^2 \equiv -9 \equiv 23 \pmod{32}$.

Opomba. Pri reševanju kongruenčnih enačb oblike $x^m \equiv c \pmod{2^e}$, pri čemer sta m in c naravni števili in $e \geq 3$, uporabimo rezultat izreka 4.4.1, ki pravi, da za $e \geq 3$ grupa U_{2^e} ni ciklična, po trditvi 4.4.4 pa lahko vsak element te grupe enolično

zapišemo kot $\pm 5^i$ za nek $0 \leq i \leq 2^{e-2} - 1$. Torej je rešitev naše kongruenčne enačbe oblike $x = \pm 5^i$. Tedaj rešujemo kongruenčno enačbo oblike $(\pm 5^i)^m \equiv \pm 5^k \pmod{2^e}$, pri čemer je $\pm 5^k \equiv c \pmod{2^e}$ za neko celo število k. Red elementa $5 \in U_{2^e}$ oziroma $-5 \in U_{2^e}$ je 2^{e-2}. Reševanje začetne kongruenčne enačbe nas tako vodi v iskanje rešitve i linearne kongruenčne enačbe $mi \equiv k \pmod{2^{e-2}}$, s pomočjo katere dobimo rešitev x začetne kongruenčne enačbe.

Preostane nam le še reševanje kongruenčne enačbe oblike $x^m \equiv c \pmod{n}$, ko ne obstaja primitivni koren po modulu n. V tem zadnjem zgledu si oglejmo, kako se lotimo reševanja takšnih kongruenčnih enačb.

Zgled. Dano imamo kongruenčno enačbo $x^4 \equiv 4 \pmod{99}$. Ker je prafaktorizacija 99 enaka $3^2 \cdot 11$, po izreku 4.6.3 ne obstaja primitivni koren po modulu 99, zato rešitve te kongruenčne enačbe ne moremo poiskati po enakem postopku kot prej. Kongruenčna enačba $x^4 \equiv 4 \pmod{99}$ je po posledici 3.1.10 ekvivalentna paru kongruenčnih enačb $x^4 \equiv 4 \pmod{11}$ in $x^4 \equiv 4 \pmod{9}$. Poiščimo sedaj rešitve obeh kongruenčnih enačb. Po izreku 4.6.3 je grupa U_9 ciklična, zato obstaja primitivni koren po modulu 9. S pomočjo trditve 4.1.17 se zlahka prepričamo, da je 2 primitivni koren po modulu 9. Naj bo i tako naravno število, da je $x = 2^i$ rešitev naše kongruenčne enačbe $x^4 \equiv 4 \pmod{9}$. Tedaj je $2^{4i} \equiv 4 \pmod{9}$, kar se zgodi natanko tedaj, ko je $4i \equiv 2 \pmod{6}$, saj je red elementa $2 \in U_9$ enak $\varphi(9) = 6$. Rešitvi te linearne kongruenčne enačbe sta 2 in 5 $\pmod{6}$. Sledi, da je $x \equiv 2^2 \equiv 4 \pmod{9}$ in $x \equiv 2^5 \equiv 5 \pmod{9}$. Torej sta rešitvi kongruenčne enačbe $x^4 \equiv 4 \pmod{9}$ ravno $\pm 4 \pmod{9}$.
Po izreku 4.6.3 je U_{11} ciklična grupa, zato obstaja primitivni koren po modulu 11. S pomočjo trditve 4.1.17 se lahko prepričamo, da je element 2 primitivni koren po modulu 11. Naj bo tedaj i tako naravno število, da je $x = 2^i$ rešitev kongruenčne enačbe $x^4 \equiv 4 \pmod{11}$. Tedaj je $2^{4i} \equiv 4 \pmod{11}$, kar pa je ekvivalentno kongruenci $4i \equiv 2 \pmod{10}$, saj je red elementa $2 \in U_{11}$ enak $\varphi(11) = 10$. Rešitvi te linearne kongruenčne enačbe sta $i = 3$ in $i = 8 \pmod{10}$. Sledi, da je $x \equiv 2^3 \equiv 8 \pmod{11}$ in $x \equiv 2^8 \equiv (2^3)^2 \cdot 2^2 \equiv 9 \cdot 4 \equiv 3 \pmod{11}$. Torej sta rešitvi kongruenčne enačbe $x^4 \equiv 4 \pmod{11}$ enaki $\pm 3 \pmod{11}$.
Rešitev prve kongruenčne enačbe $x^4 \equiv 4 \pmod{9}$ predstavljata dva kongruenčna razreda po modulu 9 in rešitev kongruenčne enačbe $x^4 \equiv 4 \pmod{11}$ predsta-

vljata prav tako dva kongruenčna razreda po modulu 11. Ker sta modula tuji si števili, nam po izreku 4.7.3 vsak od štirih parov rešitev poda končno rešitev kongruenčne enačbe $x^4 \equiv 4 \pmod{99}$. Rešitev $x \equiv 4 \pmod{9}$ prve kongruenčne enačbe $x^4 \equiv 4 \pmod{9}$ in rešitev $x \equiv 3 \pmod{11}$ druge kongruenčne enačbe $x^4 \equiv 4 \pmod{11}$ tvorita sistem dveh linearnih kongruenčnih enačb. Splošna rešitev kongruenčne enačbe $x \equiv 4 \pmod{9}$ je $x = 4 + 9t$, kjer je t poljubno celo število. Sedaj med vsemi takimi števili $x = 4 + 9t$ poiščemo tiste, ki so hkrati rešitve linearne kongruenčne enačbe $x \equiv 3 \pmod{11}$. V to kongruenčno enačbo vstavimo $x = 4 + 9t$ in iščemo rešitve kongruenčne enačbe $4 + 9t \equiv 3 \pmod{11}$. Od tod sledi, da je $t \equiv 6 \pmod{11}$. Poljubna rešitev te kongruenčne enačbe je $t = 6 + 11l$, pri čemer je l poljubno celo število. Rešitev obravnavanega sistema dveh linearnih kongruenčnih enačb je tedaj $x = 4 + 9 \cdot (6 + 11l) = 58 + 99l$. Ostale tri rešitve dobimo tako, da na podoben način rešimo preostale tri sisteme linearnih kongruenčnih enačb. Slednje prepuščam bralcu.

Opomba. Reševanja kongruenčnih enačb oblike $x^m \equiv c \pmod{n}$, ko ne obstaja primitivni koren po modulu n, pri čemer sta m, c poljubni naravni števili in n poljubno liho naravno število, se lotimo torej lahko tako, da število n najprej prafaktoriziramo, torej $n = p_1^{e_1} \cdots p_k^{e_k}$, nato pa poiščemo rešitve kongruenčnih enačb $x^m \equiv c \pmod{p_i^{e_i}}$, pri čemer je $i = 1, 2, \ldots, k$. Nato rešimo sisteme kongruenčnih enačb in s pomočjo izreka 4.7.3 poiščemo rešitev začetne kongruenčne enačbe tako, kot smo to storili v zgornjem zgledu.

Poglavje 7

Zaključek

V magistrskem delu smo preučevali grupo obrnljivih elementov kolobarja $\mathbb{Z}_n$. Osredotočili smo se na vprašanje, kako je cikličnost te grupe odvisna od naravnega števila n. Določili smo potreben in zadosten pogoj za naravno število n, da je grupa obrnljivih elementov kolobarja $\mathbb{Z}_n$ ciklična. Za vsako naravno število n smo določili, kateri znani grupi je izomorfna grupa obrnljivih elementov kolobarja $\mathbb{Z}_n$. Nazadnje smo pokazali, kako si lahko s pridobljenimi rezultati pomagamo pri reševanju določenih kongruenčnih enačb.

Pri omenjenih kongruenčnih enačbah smo se osredotočili na kongruenčne enačbe oblike $x^m \equiv c \pmod{n}$, kjer iščemo rešitev $x \in \mathbb{Z}_n$, pri čemer sta m in c celi števili, n pa je naravno število. Reševanje takšnih enačb pa lahko umestimo v malce širši kontekst. Izkaže se, da imajo tovrstne kongruenčne enačbe velik pomen na področju kriptografije. Če sta a in c elementa grupe U_n, pri čemer je n naravno število, potem rešitev k kongruenčne enačbe $a^k \equiv c \pmod{n}$ imenujemo *diskretni logaritem z osnovo a od c* v grupi U_n. Za izračun diskretnega logaritma za zdaj ne poznamo nobenega učinkovitega algoritma, zato je iskanje diskretnega logaritma za velika naravna števila n izjemno zahtevno. Težavnost tega problema tako omogoča konstrukcijo različnih kriptografskih sistemov. Kot možnost nadaljnjega študija tako bralcu priporočamo, da si v ustrezni literaturi prebere več o tovrstnih kriptografskih sistemih (ki so jih prvi razvili Diffie, Hellman in Merkle), ali pa se posveti vprašanju, ali je mogoče rezultate tega magistrskega dela uporabiti tudi za reševanje kakšnih drugačnih kongruenčnih enačb.

Literatura

[1] Fraleigh, J.B. (1989). *A first course in abstract algebra*. Boston: Addison-Wesley Publishing Company, Inc.

[2] Jones, G.A. in Jones, M.J. (2005). *Elementary number theory*. London: Springer-Verlag London Limited.

[3] Malnič, A. (2015). *Algebrske strukture*. Zapiski predavanj.

[4] Medved, I. (2013). *Načelo vključitev in izključitev ter njegova uporaba* (Diplomsko delo). Univerza v Ljubljani, Pedagoška fakulteta, Ljubljana.

[5] Roman, S. (1995). *Field theory*. New york: Springer-Verlag New York, Inc.

[6] Šparl, P. (2017). *Logika in množice*. Zapiski predavanj.

[7] Šparl, P. (2018). *Abstraktna algebra*. Zapiski predavanj.

Spletna literatura

[8] Aitken, W. (2005). *Cyclic unit groups*. Pridobljeno 13. 5. 2019 s $https://public.csusm.edu/aitken_html/m372/cyclic.pdf$

[9] Aitken, W. (2009). *Cyclic unit groups*. Pridobljeno 13. 5. 2019 s $https://public.csusm.edu/aitken_html/m422/Handout9.pdf$.

Izjava o avtorstvu

Spodaj podpisani Tilen Miklavec, z vpisno številko 01170624, izjavljam, da je magistrsko delo z naslovom

GRUPA OBRNLJIVIH ELEMENTOV KOLOBARJA $\mathbb{Z}_n$,

ki sem ga napisal pod mentorstvom izr. prof. Primoža Šparla, avtorsko delo in da so uporabljeni viri ter literatura korektno navedeni.

Podpis študenta:

Ljubljana, avgust 2019