dr.sc. Ivan Matić, docent
e-mail: imatic@mathos.hr

Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku,
Trg Ljudevita Gaja 6, HR-31000 Osijek

Izdavač:
Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku

Recenzenti:
dr.sc. Neven Grbac, izvanredni profesor,
Sveučilište u Rijeci - Odjel za matematiku
dr.sc. Marcela Hanzer, izvanredni profesor,
Prirodoslovno-matematički fakultet, Matematički odsjek, Sveučilište u Zagrebu

Lektor:
Doroteja Eškutić

CIP zapis dostupan u računalnom katalogu Gradske i sveučilišne knjižnice Osijek pod brojem 140124026.

ISBN 978–953–6931–80–4

Ovaj udžbenik objavljuje se uz suglasnost Senata Sveučilišta Josipa Jurja Strossmayera u Osijeku pod brojem 6/15.

Tisak:
STUDIO HS Internet d.o.o.
Osijek

UVOD U TEORIJU BROJEVA

Ivan Matić

Osijek, 2015.

Sadržaj

PREDGOVOR

Teorija brojeva je jedna od rijetkih grana matematike u kojoj se problemi od posebnog interesa mogu detaljno pojasniti i osobama oskudnijeg matematičkog predznanja, što je svakako i jedan od razloga njene duge povijesti. No, često je slučaj da problemi jednostavna iskaza imaju izuzetno komplicirano rješenje te se, u potrazi za odgovarajućim metodama i pristupima, teorija brojeva kroz stoljeća razvila do neslućenih razmjera, povlačeći za sobom i mnoge druge grane matematike. Unatoč očekivanjima mnogih velikih matematičara, ova je grana teorijske matematike u novije vrijeme pronašla svoje mjesto i u brojnim primjenama koje su sastavni dio svakodnevnog života.

U ovom udžbeniku, koji pokriva gradivo istoimenog kolegija, prikazani su neki od elementarnih pojmova i elementarnih metoda teorije brojeva te problemi na rješavanje kojih se te metode mogu primijeniti. Priroda obrađenog materijala je takva da ne zahtijeva gotovo nikakvo posebno matematičko predznanje, dok neki od obrađenih pojmova predstavljaju uvod u druge grane matematike, poput algebre i kriptografije, koje su se dijelom iz teorije brojeva i razvile.

Udžbenik je nastao na temelju predavanja iz kolegija Uvod u teoriju brojeva, koja sam nekoliko godina držao studentima druge godine na Odjelu za matematiku Sveučilišta u Osijeku. Osim polaznicima tog kolegija, udžbenik je namijenjem i svima koji žele produbiti ili samo obnoviti svoje znanje teorije brojeva, s posebnim naglaskom na njene primjene i povijesni razvoj. Zahvaljujem se recenzentima i lektoru za korisne sugestije te profesoru Šimi Ungaru na pomoći u izradi završne verzije udžbenika te brojnim vrijednim komentarima.

Osijek, 22. travnja 2015.

Ivan Matić

1

DJELJIVOST

Engleski matematičar Godfrey Harold Hardy u svom je djelu *Isprika jednog matematičara* (*A Mathematician's Apology*), objavljenom 1940., istaknuo kako smatra da je najljepša matematika upravo čista, teorijska matematika koja je oslobođena mogućnosti praktične primjene u čemu, kako je naglasio, prednjači upravo jedno od njegovih polja istraživanja — teorija brojeva (kako ćemo vidjeti kroz nekoliko poglavlja, ubrzo se pokazalo da Hardy nije u pravu). Pritom se Hardy snažno oslanja i na Gaussovu izjavu prema kojoj je „matematika kraljica znanosti, a teorija brojeva kraljica matematike". Iako je prema nekima upravo neprimjenjivost teorije brojeva glavni oslonac Gaussu pri ovoj izjavi, Hardy je jasno istaknuo da se protivi takvom razmišljanju jer pronalazak primjene teorije brojeva zasigurno ne bi rezultirao detroniziranjem statusa ove grane teorijske matematike. Hardy smatra kako se ishodište Gaussova stava, pri čemu se s njim u potpunosti slaže, očituje u činjenici da su temeljni pojmovi i koncepti teorije brojeva mnogo čišći, dublji i elegantniji od istih u drugim granama matematike. Među glavnim osloncima te teze pripada i pojam djeljivosti.

1.1. Osnovni pojmovi

Djeljivost je fundamentalni pojam teorije brojeva. Dakle, neka su a, b cijeli brojevi te neka je $a \neq 0$. Kažemo da a ***dijeli*** b ako postoji cijeli broj d takav da vrijedi $b = a \cdot d$. U tom slučaju pišemo $a \mid b$, broj b nazivamo ***višekratnikom*** broja a, dok broj a nazivamo ***djeliteljem*** broja b.

Ukoliko a ne dijeli b, pišemo $a \nmid b$. Pogledajmo nekoliko primjera.

Primjer 1.1.1. Kako je $4 = 2 \cdot 2$, očito $2 \mid 4$. Također, $2 \mid -6$ jer je $-6 = -3 \cdot 2$. No, $2 \nmid -7$.

Primijetimo kako $a \mid 0$, za svaki $a \in \mathbb{Z} \setminus \{0\}$, jer je $0 = 0 \cdot a$. Slično, $1 \mid b$, za svaki $b \in \mathbb{Z}$. S druge strane, iz $a \mid 1$ slijedi $a \in \{1, -1\}$.

Navedimo nekoliko osnovnih svojstava djeljivosti.

Propozicija 1.1.2. (1) *Ako $a \mid b$ i $b \neq 0$, tada je $|a| \leq |b|$.*
(2) *Ako je a djelitelj broja b, tada je a djelitelj i svakog višekratnika od b.*
(3) *Ako je a djelitelj brojeva b i c, tada je djelitelj i brojeva $b + c$, $b - c$ i $b \cdot c$.*

Dokaz. (1) Neka je $b = a \cdot d$. Odatle slijedi $|b| = |a| \cdot |d|$. Kako je $b \neq 0$, očito je $|d| \geq 1$, iz čega slijedi tvrdnja.
(2) Neka je $b = a \cdot d_1$ te neka je c višekratnik broja b. Prema tome, postoji neki cijeli broj d_2 takav da je $c = b \cdot d_2 = a \cdot d_1 \cdot d_2$. Prema tome, $a \mid c$.
(3) Neka je $b = a \cdot d_1$ te $c = a \cdot d_2$. Redom dobivamo $b \pm c = a \cdot (d_1 \pm d_2)$ i $b \cdot c = a^2 \cdot (d_1 \cdot d_2)$ što povlači tvrdnju. □

Primijetimo da iz tvrdnje (1) prethodne propozicije slijedi da, ukoliko $a \mid b$ i $b \mid a$, tada je $a \in \{b, -b\}$.

Sada ćemo pokazati jedan od osnovnih teorema čitave teorije brojeva, poznat pod nazivom Teorem o djeljenju s ostatkom.

Teorem 1.1.3. *Neka su a, b cijeli brojevi, $a > 0$. Tada postoje jedinstveni cijeli brojevi q i r takvi da je $b = q \cdot a + r$, pri čemu je $0 \leq r < a$.*

Dokaz. Dokažimo najprije da postoje brojevi q i r kao u iskazu teorema. U tu svrhu, promotrimo racionalan broj $\frac{b}{a}$. Neka je q cijeli broj takav da $\frac{b}{a}$ leži u poluotvorenom intervalu $[q, q+1\rangle$. Očito vrijedi $0 \leq \frac{b}{a} - q < 1$.

Stavimo $r = b - a \cdot q = a(\frac{b}{a} - q)$ (primijetimo da je r cijeli broj koji zadovoljava $b = q \cdot a + r$). Iz prethodne nejednakosti slijedi $0 \leq r < a$.

Dokažimo sada i jedinstvenost. Dakle, neka su $b = q_1 \cdot a + r_1$ i $b = q_2 \cdot a + r_2$ dva rastava traženog oblika, tj. $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ te $0 \leq r_1, r_2 < a$.

Oduzimanjem dobivamo $a(q_1 - q_2) = r_2 - r_1$. Ako je $q_1 \neq q_2$, tada a dijeli $r_2 - r_1$. No, $-a + 1 \leq r_2 - r_1 \leq a - 1$ te je $|r_2 - r_1| < a$. Prema prvom dijelu propozicije 1.1.2 slijedi $q_1 = q_2$. No, tada je i $r_1 = r_2$ čime je teorem dokazan. □

U prethodnom se teoremu broj r naziva ostatak pri dijeljenju, dok je q kvocijent cjelobrojnog dijeljenja.

Za realan broj x stavimo $\lfloor x \rfloor$ = najveći cijeli broj koji nije veći od x. Time smo definirali cjelobrojnu funkciju 'pod' (ili funkciju najveće cijelo). Npr. $\lfloor 3.4 \rfloor = 3$, $\lfloor -\pi \rfloor = -4$, $\lfloor n \rfloor = n$ za $n \in \mathbb{Z}$. Tada se kvocijent cjelobrojnog dijeljenja q može zapisati u obliku $q = \lfloor \frac{b}{a} \rfloor$.

Primjer 1.1.4. $100 = 32 \cdot 3 + 4$, $\lfloor \frac{100}{32} \rfloor = 3$. Također, $100 = 3 \cdot 33 + 1$, $\lfloor \frac{100}{3} \rfloor = 33$.

Neka su b i c cijeli brojevi. Cijeli broj a koji dijeli oba broja b i c naziva se zajednički djelitelj brojeva b i c. Ukoliko je barem jedan od brojeva b i c različit od nule, tada taj broj ima konačno mnogo djelitelja. U tom slučaju postoji i konačno mnogo zajedničkih djelitelja brojeva b i c. Najvećeg od njih (a taj je uvijek pozitivan) označavamo s (b, c). Broj (b, c) nazivamo ***najveći zajednički djelitelj brojeva*** b ***i*** c.

Slično se definira i najveći zajednički djelitelj cijelih brojeva $b_1, b_2, \ldots, b_n$ (od kojih je barem jedan različit od nule) koji se označava s $(b_1, b_2, \ldots, b_n)$.

Primijetimo da je (b, c) uvijek prirodan broj.

Primjer 1.1.5. $(100, 17) = 1$, $(24, 16) = 8$, $(a, a \cdot b) = |a|$, za $a \neq 0$.

Za cijele brojeve a i b kažemo da su ***relativno prosti*** ukoliko je $(a, b) = 1$. Brojevi 100 i 17 iz prethodnog primjera su relativno prosti. Slično, za brojeve $b_1, b_2, \ldots, b_n$ kažemo da su relativno prosti ukoliko je $(b_1, b_2, \ldots, b_n) = 1$.

Naravno, postavlja se pitanje kako odrediti najveći zajednički djelitelj danih cijelih brojeva. Ukoliko se radi o većim brojevima (pa već i troznamenkastim), takav zadatak postaje vrlo težak. Efikasan postupak opisati ćemo u idućem poglavlju.

1.2. Euklidov algoritam

Promotrimo najprije sljedeći primjer.

Primjer 1.2.1. Odredite $(70, 32)$.

Prema dijelu (3) propozicije 1.1.2, svaki zajednički djelitelj brojeva 70 i 32 dijeli i njihovu razliku. Prema tome, $(70, 32) \mid 70 - 32 = 38$. Dakle, $(70, 32)$ je i zajednički djelitelj brojeva 32 i 38. No, kako je svaki zajednički djelitelj brojeva 32 i 38 ujedno i djelitelj broja 70, dobivamo jednakost $(70, 32) = (38, 32)$.

Na sličan način možemo vidjeti i $(70, 32) \mid 70 - 2 \cdot 32 = 6$. Time smo problem određivanja broja $(70, 32)$ sveli na problem određivanja broja $(32, 6)$ koji je očito jednak 2; što se može dobiti i sličnim zaključivanjem kao ranije, tj. $(32, 6) \mid 32 - 5 \cdot 6 = 2$, odakle je $(70, 32) = (6, 32) = (6, 2) = 2$.

Općenito, neka su a i b cijeli brojevi te neka smo uzastopnom primjenom teorema 1.1.3 dobili sljedeći niz jednakosti:

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

(postupak završava kada dobijemo ostatak jednak nuli). Kako je $a > r_1 > r_2 > \ldots$ čitav postupak završava nakon konačno mnogo koraka.

Iz prve jednakosti slijedi $(a, b) \mid r_1$ te da je svaki zajednički djelitelj brojeva a i r_1 ujedno i djelitelj broja b. Prema tome, $(a, b) = (a, r_1)$. Na isti način dobivamo i niz jednakosti $(a, b) = (a, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$ jer r_n dijeli r_{n-1}. Prema tome, (a, b) jednak je posljednjem ne-nul ostatku. Opisani postupak određivanja najvećeg zajedničkog djelitelja naziva se ***Euklidov algoritam***. Taj drevni algoritam predstavlja izuzetno efikasan način za određivanje najvećeg zajedničkog djelitelja dvaju cijelih brojeva s brojnim važnim posljedicama. Napomenimo da neki otkriće Euklidova algoritma pripisuju Pitagorejcima, dok ga je Euklid objavio u svojim *Elementima*. Također, poznato je da su isti algoritam koristili još i indijski te kineski matematičari u 5. stoljeću.

Primjer 1.2.2. Odrediti $(172, 50)$.

$$\begin{aligned} 172 &= 3 \cdot 50 + 22 \\ 50 &= 2 \cdot 22 + 6 \\ 22 &= 3 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Odatle je $(172, 50) = 2$.

Primijetimo da iz prve jednakosti Euklidova algoritma možemo zapisati $r_1 = b - q_1 a$. Uvrštavanjem u idući redak dobivamo $r_2 = (1 + q_1 q_2)a - q_2 b$. Nastavljajući na isti način uvrštavanjem u naredne jednakosti, možemo zaključiti da postoje cijeli brojevi x i y za koje vrijedi

$$ax + by = r_n = (a, b).$$

Prethodna se jednakost obično naziva ***Bezoutov identitet***.

U Primjeru 1.2.2 bismo na taj način dobili redom:

$$\begin{aligned} 22 &= 172 - 3 \cdot 50 \\ 6 &= 7 \cdot 50 - 2 \cdot 172 \\ 4 &= 7 \cdot 172 - 24 \cdot 50 \\ (172, 50) = 2 &= 31 \cdot 50 - 9 \cdot 172. \end{aligned}$$

Tim je dan i postupak za nalaženje cjelobrojnih rješenja jednadžbe $ax + by = (a, b)$. Rješivost sličnih jednadžbi prokomentirana je u idućem teoremu.

Teorem 1.2.3. *Neka su a i b cijeli brojevi. Najmanji prirodan broj m za kojeg postoji cjelobrojno rješenje jednadžbe $ax + by = m$ je (a, b). Štoviše, jednadžba $ax + by = m$ ima cjelobrojno rješenje ako i samo ako (a, b) dijeli m.*

Dokaz. Kako $(a, b) \mid a$ i $(a, b) \mid b$, za sve $x, y \in \mathbb{Z}$ mora vrijediti i $(a, b) \mid ax + by$. Prema tome, ako jednadžba $ax + by = m$ ima cjelobrojno rješenje, tada $(a, b) \mid m$. Ukoliko je m prirodan broj manji od (a, b), tada m nije djeljiv s (a, b) pa promatrana jednadžba nema rješenja za takav broj m.

U razmatranjima prije teorema pokazali smo da postoji cjelobrojno rješenje jednadžbe $ax + by = (a, b)$. Neka je $m \in \mathbb{N}$ takav da $(a, b) \mid m$. Tada postoji $d \in \mathbb{N}$ za koji vrijedi $m = (a, b) \cdot d$. Direktno slijedi

$$adx + bdy = d \cdot (a, b) = m$$

pa je dx, dy traženo cjelobrojno rješenje. □

Prethodni teorem pokazuje kako su brojevi a i b relativno prosti ako i samo ako jednadžba $ax + by = 1$ ima cjelobrojno rješenje.

Kod svakog algoritma prirodno je zapitati se koliko je brz, tj. koliko je koraka potrebno da bi se izvršio. Tako postoje situacije u kojima je Euklidov algoritam izrazito efikasan, npr. $a = 51$, $b = 105$:

$$\begin{aligned} 105 &= 2 \cdot 51 + 3 \\ 51 &= 17 \cdot 3, \end{aligned}$$

no i one prilikom čijeg je izvršavanja potrebno znatno više koraka, npr. $a = 89$, $b = 144$:

$$\begin{aligned} 144 &= 1 \cdot 89 + 55 \\ 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Sljedeći rezultat daje ogradu na broj mogućih koraka Euklidova algoritma.

Propozicija 1.2.4. *Neka su a i b prirodni brojevi, pri čemu je $b \geq a$. Za broj koraka Euklidova algoritma vrijedi da je manji ili jednak od $5 \cdot (\lfloor \log a \rfloor + 1)$, gdje smo s $\log a$ označili dekadski logaritam prirodnog broja a.*

Dokaz. Pokažimo najprije kako je broj znamenki broja a jednak upravo $\lfloor \log a \rfloor + 1$. Označimo broj znamenki broja a (u dekadskom zapisu) s n. Tada očito vrijedi

$$10^{n-1} \leq a < 10^n.$$

Logaritmiranjem prethodnog izraza te korištenjem činjenice da je log rastuća funkcija dobivamo

$$n - 1 \leq \log a < n,$$

odakle direktno slijedi $n = \lfloor \log a \rfloor + 1$.

Pretpostavimo da smo primjenom Euklidova algoritma dobili sljedeći niz jednakosti:

$$\begin{aligned} b &= q_{n-1}a + r_{n-1} \\ a &= q_{n-2}r_{n-1} + r_{n-2} \\ &\vdots \\ r_3 &= q_1 r_2 + r_1 \\ r_2 &= q_0 r_1, \end{aligned}$$

dakle imamo n koraka u provedbi algoritma te smo, samo za potrebe ovog dokaza, označili dobivane ostatke redom s $a = r_n > r_{n-1} > \ldots > r_1$.

Kako je $q_i \geq 1$ za sve i, dobivamo $r_{i+1} \geq r_i + r_{i-1}$. Osim toga, $r_1 \geq 1$ i $r_2 \geq 2$. Iz toga dobivamo

$$\begin{aligned} r_3 &\geq r_2 + r_1 \geq 3 \\ r_4 &\geq r_3 + r_2 \geq 5 \\ r_5 &\geq r_4 + r_3 \geq 8. \end{aligned}$$

Možemo zaključiti da je $r_i \geq F_i$, gdje je F_i i-ti Fibonaccijev broj (primijetimo da se Fibonaccijevi brojevi $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144$ pojavljuju i u prethodnom primjeru). Dakle, $a \geq F_n$ i broj znamenki od a veći je ili jednak broju znamenki od F_n.

Da bismo ocijenili broj znamenki Fibonaccijeva broja koristimo Binetovu formulu $F_n = \frac{1}{\sqrt{5}}\big((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}\big)$, jedna od čijih posljedica je i nejednakost $F_n \geq (\frac{1+\sqrt{5}}{2})^{n-1}$. Odatle je $\log F_n \geq (n-1)\log(\frac{1+\sqrt{5}}{2})$. Kako je $\log(\frac{1+\sqrt{5}}{2}) > \frac{1}{5}$, slijedi $\log F_n > \frac{n-1}{5}$ te je broj znamenki od F_n barem $\frac{n}{5}$.

Prema tome, broj koraka algoritma manji je ili jednak od broja znamenki broja a uvećanog 5 puta, odnosno $\lfloor \log a \rfloor + 1 \geq \frac{n}{5}$. □

Napomenimo da se još neke činjenice o mogućnostima korištenja Euklidova algoritma koja svjedoče njegovoj efikasnosti i zapanjujućoj jednostavnosti mogu vidjeti u [11].

1.3. Verižni razlomci

Neka je α realan broj. Najprije stavimo $a_0 = \lfloor \alpha \rfloor$ te definiramo $b_0 = \alpha - a_0$. Ukoliko je $b_0 \neq 0$, stavimo $\alpha_1 = \frac{1}{b_0}$. Primijetimo da je $\alpha_1 > 0$ te $\alpha = a_0 + \frac{1}{\alpha_1}$.

Nastavimo isti postupak s α_1: neka je redom $a_1 = \lfloor \alpha_1 \rfloor$, $b_1 = \alpha_1 - a_1$. Ako je $b_1 \neq 0$, definiramo $\alpha_2 = \frac{1}{b_1}$ te nastavljamo na isti način. Taj postupak staje ukoliko je $b_n = 0$ za neki n, u suprotnom se može nastaviti unedogled.

Pogledajmo taj postupak na primjeru $\alpha = \frac{172}{50}$. Redom je $a_0 = 3$, $b_0 = \frac{22}{50}$, zatim $\alpha_1 = \frac{50}{22}$, $a_1 = 2$, $b_1 = \frac{6}{22}$. Nadalje, $\alpha_2 = \frac{22}{6}$, $a_2 = 3$, $b_2 = \frac{4}{6}$ te $\alpha_3 = \frac{6}{4}$, $a_3 = 1$, $b_3 = \frac{2}{4}$. Naposlijetku, $\alpha_4 = \frac{4}{2} = a_4 = 2$ i $b_4 = 0$.

Time smo dobili sljedeći zapis racionalnog broja $\frac{172}{50}$

$$\frac{172}{50} = 3 + \frac{22}{50} = 3 + \frac{1}{\frac{50}{22}} = 3 + \frac{1}{2 + \frac{6}{22}} = 3 + \frac{1}{2 + \frac{1}{\frac{22}{6}}} = \cdots = 3 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}}$$

koji se naziva ***razvoj racionalnog broja*** $\frac{172}{50}$ ***u jednostavni verižni razlomak***, dok se izrazi koje smo redom dobivali $(3, 3+\frac{1}{2}, 3+\frac{1}{2+\frac{1}{3}}, \ldots)$ nazivaju ***parcijalne konvergente***. Kraće, gornji razvoj u verižni razlomak označavamo s $[3, 2, 3, 1, 2]$ jer je tim nizom potpuno određen.

Primijetimo da se upravo ovaj niz brojeva pojavio u Primjeru 1.2.2. Općenito, neka je $\alpha = \frac{a}{b}$ i neka su primjenom Euklidova algoritma na par (a, b) dobivene jednakosti

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Tada je $a_0 = \lfloor \alpha \rfloor = q_1$, $b_0 = \frac{r_1}{b}$, $\alpha_1 = \frac{b}{r_1}$. Potom $a_1 = \lfloor \alpha_1 \rfloor = q_2$, $b_1 = \frac{r_2}{r_1}$, $\alpha_2 = \frac{r_1}{r_2}$ itd. Odatle dobivamo

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \frac{1}{q_n}}}}$$

te $\frac{a}{b} = [q_1, q_2, \ldots, q_n]$. Primijetimo da je $\alpha_i > 1$ za sve i pa je $q_i \geq 1$ za $i \geq 2$. Osim toga, $q_1 \leq 0$ ako je $\frac{a}{b} \leq 0$.

Još je Euler u 18. stoljeću uočio da se Euklidov algoritam može uklopiti u postupak razvoja racionalnog broja u jednostavni verižni razlomak te je u narednih stotinjak godina upravo to postao omiljeni način opisa Euklidova algoritma. Čak je i Gauss u svom djelu *Disquisitiones* ignorirao sam Euklidov postupak te se referirao isključivo na postupak razvoja racionalnog broja u verižni razlomak. Povratak Euklidova algoritma u osnovnu upotrebu dogodio se oko 1860. godine za što je ponajprije zaslužan Dirichlet koji je ovaj algoritam koristio na otprilike sličan način kako ćemo mi to učiniti u ovom poglavlju.

Opisani postupak razvoja broja α u verižni razlomak staje jedino ukoliko je α racionalan broj. Iracionalni brojevi odgovaraju beskonačnim verižnim razlomcima što ćemo opisati sljedećim primjerom.

Primjer 1.3.1. Odredite razvoj u jednostavni verižni razlomak broja $\sqrt{2}$.

Sada je $\alpha = \sqrt{2}$, $a_0 = 1$ i $b_0 = \sqrt{2} - 1$ te $\alpha_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1$.

U idućem koraku dobivamo $a_1 = 2$, $b_1 = \sqrt{2}-1$, jednako kao i u prethodnom. Naravno, $\alpha_2 = \sqrt{2}+1$ te $a_2 = a_1$. Prema tome, $\alpha_1 = \alpha_2 = \alpha_3 = \cdots = \sqrt{2}+1$ te $a_1 = a_2 = a_3 = \cdots = 2$. Sada $\sqrt{2}$ možemo zapisati u obliku

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$$

ili kraće $\sqrt{2} = [1, \overline{2}\,]$, gdje $\overline{2}$ označava uzastopno ponavljanje broja 2. Gornji razvoj iracionalnog broja $\sqrt{2}$ u verižni razlomak treba promatrati kao aproksimaciju iracionalnog broja parcijalnim konvegentama $[1,2], [1,2,2], [1,2,2,2], \ldots$, koje zaista predstavljaju konvergentan niz racionalnih brojeva čiji je limes jednak $\sqrt{2}$.

Napomenimo kako sam Euklidov algoritam ne igra značajnu ulogu pri razvoju iracionalnih brojeva u verižne razlomke.

1.4. Prosti brojevi

Prirodan broj n, $n > 1$, nazivamo ***prostim*** ukoliko nema niti jednog djelitelja d za koji vrijedi $1 < d < n$. Broj koji nije prost naziva se ***složen***. Primijetimo da su jedini pozitivni djelitelji prostog broja p brojevi 1 i p.

Na primjer, broj 11 je prost, dok je broj $187 = 11 \cdot 17$ složen.

Važnost prostih brojeva očituje se u činjenici da se svaki prirodan broj veći od jedan može prikazati u obliku produkta potencija prostih brojeva, što ćemo u ovom poglavlju i dokazati.

Najprije navedimo jednu važnu tvrdnju, poznatu pod nazivom aksiom dobre uređenosti: Svaki neprazan podskup skupa prirodnih brojeva ima najmanji element.

Označimo skup svih prirodnih brojeva većih od jedan koji se ne mogu prikazati u obliku produkta prostih brojeva sa S te neka je a najmanji element tog skupa. Očito, a nije prost broj jer bi inače na trivijalan način bio prikazan u obliku produkta prostih brojeva. Prema tome, postoje prirodni brojevi b i c, oba veći od 1, takvi da je $a = b \cdot c$. Kako su b i c oba manji od a, ne mogu biti elementi skupa S te se oba mogu napisati kao produkt prostih brojeva. No, tada se i a može napisati u obliku produkta prostih brojeva, što nije moguće. Dakle, skup S je prazan.

Na primjer, $28 = 7 \cdot 4 = 7 \cdot 2 \cdot 2 = 7 \cdot 2^2$.

Jedinstvenost ovakvog rastava prokomentirat ćemo u sljedećem podnaslovu.

Osnovni teorem aritmetike

Pokažimo najprije korisnu lemu.

Lema 1.4.1. *Neka je p prost broj te neka su a i b cijeli brojevi takvi da $p \mid a \cdot b$. Tada $p \mid a$ ili $p \mid b$.*

Dokaz. Neka p ne dijeli jednog od brojeva a, b. Možemo pretpostaviti da $p \nmid a$. Trebamo dokazati da tada p dijeli b. Kako p ne dijeli cijeli broj a, a jedini djelitelji prostog broja p su 1 i p, slijedi da je $(a, p) = 1$. Prema teoremu 1.2.3, postoje cijeli brojevi x, y takvi da je $ax + py = 1$. Množenjem s b dobivamo $abx + pby = b$. Kako p dijeli ab, slijedi da p dijeli b, što je i trebalo dokazati. □

Prethodna se lema može direktno generalizirati na produkt proizvoljno mnogo faktora:

Lema 1.4.2. *Neka je p prost broj te neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi takvi da $p \mid a_1 a_2 \cdots a_n$. Tada $p \mid a_i$ za neki $i \in \{1, 2, \ldots, n\}$.*

Sada smo spremni dokazati ***Osnovni teorem aritmetike***.

Teorem 1.4.3. *Prikaz svakog prirodnog broja većeg od 1 u obliku produkta potencija prostih brojeva je jedinstven do na poredak faktora.*

Dokaz. Dokazat ćemo ovaj izuzetno važan rezultat na dva načina.

Neka je najprije n prirodan broj veći od 1 te neka su $n = p_1 p_2 \cdots p_k$ i $n = q_1 q_2 \cdots q_l$ dva prikaza broja n u obliku produkta prostih brojeva. Tada je $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ pa $p_1 \mid q_1 q_2 \cdots q_l$. Prema lemi 1.4.2, $p_1 \mid q_i$ za neki i. Kako su p_1 i q_i oba prosti, slijedi $p_1 = q_i$. Permutiranjem faktora $q_1, \ldots, q_l$, možemo uzeti da je $i = 1$ te nakon kraćenja dobivamo $p_2 \cdots p_k = q_2 \cdots q_l$.

Sličnim zaključivanjem dobivamo $p_2 = q_2$, $p_3 = q_3, \ldots, p_k = q_k$ te $k = l$. Time je završen prvi dokaz.

U drugom dokazu koristit ćemo metodu poznatu pod nazivom Fermatova metoda beskonačnog spusta. Osnovna ideja te interesantne metode leži u tome da svaki neprazan podskup skupa prirodnih brojeva ima najmanji element. Prema tome, ukoliko želimo pokazati kako ne postoji prirodan broj koji zadovoljava neko svojstvo, dovoljno je dokazati da iz pretpostavke da neki prirodan broj to svojstvo zadovoljava slijedi kako postoji i manji prirodan broj s istim svojstvom, a takvo beskonačno spuštanje ne dozvoljava struktura skupa prirodnih brojeva.

Dakle, neka je T skup svih prirodnih brojeva većih od 1 koji imaju nejedinstven prikaz u obliku produkta prostih brojeva, pri čemu ne uzimamo u obzir

poredak faktora. Primijetimo kako se u skupu T ne pojavljuje niti jedan prost broj jer takvi brojevi imaju trivijalan prikaz u obliku produkta prostih brojeva. Pretpostavimo da je skup T neprazan. Tada postoji minimalan element skupa T, označimo ga s n. Neka su $n = p_1 p_2 \cdots p_k$ i $n = q_1 q_2 \cdots q_l$ dva različita prikaza od n u obliku produkta prostih brojeva, pri čemu je $p_1 \leq p_2 \leq \ldots \leq p_k$ i $q_1 \leq q_2 \leq \ldots \leq q_l$.

Kako p_1 dijeli n, tada p_1 dijeli i produkt $q_1 q_2 \cdots q_l$. Očito možemo uzeti i da je $q_1 = p_1$. No, tada i prirodan broj $\frac{n}{p_1}$ također ima nejedinstven prikaz u obliku produkta prostih brojeva jer bi inače takav prikaz od n bio jedinstven. Kako n nije prost, $\frac{n}{p_1}$ je također element skupa T što nije moguće jer je $\frac{n}{p_1} < n$, a n je najmanji element skupa T. Time je teorem u potpunosti dokazan. □

Tim smo pokazali da svaki prirodan broj $n \geq 2$ možemo (na način jedinstven do na poredak) prikazati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

gdje je $k \in \mathbb{N}$, $p_1, p_2, \ldots, p_k \in \mathbb{N}$ su različiti prosti brojevi te, naravno, $\alpha_i \in \mathbb{N}$. Npr., $96 = 2^5 \cdot 3$.

Prema tome, proste brojeve možemo smatrati temeljnim gradivnim blokovima pomoću kojih se može, na način jedinstven do na poredak, prikazati svaki prirodan broj.

Iako se Osnovni teorem aritmetike ponekad pripisuje Euleru, prvi koji je iznio pravilan i detaljan iskaz i dokaz tog rezultata je Gauss, početkom 19. stoljeća. Iako se u doba antičke Grčke tvrdnja Osnovnog teorema aritmetike smatrala sasvim prirodnom i jasnom, tada još nisu postojale metode za općeniti zapis i formalni dokaz tog teorema.

Najbliže što se sam Euklid približio navedenom rezultatu je Propozicija 14 devete knjige njegovih *Elemenata* koja u slobodnom prijevodu glasi: „Ako je broj izmjeren prostim brojevima, onda ne može biti izmjeren niti jednim prostim brojem izuzev onih kojima je izvorno izmjeren.“ Tu Euklid pod ‘mjeriti’ smatra ‘dijeliti’ jer se u ono doba inzistiralo na promatranju brojeva kao duljina određenih segmenata ili dužina pa npr. 12 može biti izmjeren s 4 jer 3 dužine duljine 4 imaju jednaku duljinu kao dužina duljine 12. Prema nekim mišljenjima, Euklid nije mogao doći do općenitog iskaza Osnovnog teorema aritmetike zbog nemogućnosti prikazivanja produkta u kojem broj faktora nije specificiran. S druge strane, često je i mišljenje kako se tada jednostavno nije moglo doći do rezultata o egzistenciji prikaza prirodnog broja kao produkta prostih brojeva jer Grci nisu mogli pojmiti egzistenciju nečeg što nije kons-

truktibilno metodama elementarne geometrije. U prilog tome ide i tadašnje promatranje dijeljenja kao mjerenja jedne dužine drugom.

Sljedeća propozicija koju navodimo bez dokaza, daje koristan kriterij djeljivosti.

Propozicija 1.4.4. *Neka su* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *i* $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ *prirodni brojevi dani rastavom na proste faktore. Broj* a *djeljiv je brojem* b *ako i samo ako za svaki* q_j, $j \in \{1, 2, \ldots, l\}$, *postoji neki* $i \in \{1, 2, \ldots, k\}$ *tako da je* $q_j = p_i$ *i* $\alpha_i \geq \beta_j$.

Primjer 1.4.5. $18 = 2 \cdot 3^2 \mid 54 = 2 \cdot 3^3$, no $36 = 2^2 \cdot 3^2 \nmid 54$.

Skup prostih brojeva

S $\mathcal{P}$ označavamo skup svih prostih brojeva. Sljedeći rezultat opisuje osnovno svojstvo tog skupa.

Teorem 1.4.6. *Skup* $\mathcal{P}$ *je beskonačan.*

Dokaz. Dokazat ćemo ovaj teorem na dva načina. Ideja prvog dokaz potječe još od Euklida.

Pretpostavimo kako je skup prostih brojeva konačan te neka je $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$. Promotrimo broj $q = p_1 p_2 \cdots p_k + 1$. Očito je $q > p_i$ za sve $i = 1, 2, \ldots, k$, pa $q \notin \mathcal{P}$. Prema tome, broj q nije prost pa mora biti djeljiv nekim prostim brojem. Ako $p_i \mid q$, tada $p_i \mid q - p_1 p_2 \cdots p_k$ te $p_i \mid 1$, što nije moguće. Dakle, skup prostih brojeva je beskonačan.

Drugi dokaz koristi metode matematičke analize.

Podsjetimo se najprije kako je izrazom

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

dan harmonijski red koji je divergentan.

Zapravo se harmonijski red pojavljuje na brojnim mjestima u teoriji brojeva kao poseban slučaj Riemannove zeta funkcije koja je definirana s

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots,$$

gdje je s kompleksan broj. Ta funkcija je produljenje harmonijskog reda koji je dan upravo s $\zeta(1)$.

Pretpostavimo ponovno kako je skup prostih brojeva konačan, te neka su, jednostavnosti radi, $2, 3, 5$ i 7 svi prosti brojevi. Tada se svaki prirodan broj

n može prikazati u obliku $n = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}$. Koristeći taj rastav, harmonijski red $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ možemo zapisati u obliku

$$\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)\left(1+\frac{1}{3}+\frac{1}{3^2}+\cdots\right)\left(1+\frac{1}{5}+\frac{1}{5^2}+\cdots\right)\left(1+\frac{1}{7}+\frac{1}{7^2}+\cdots\right).$$

Svaki od faktora je jednak sumi geometrijskog reda, odakle slijedi da je suma harmonijskog reda jednaka $\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6} = \frac{35}{8}$, što je u suprotnosti s divergencijom harmonijskog reda.

Odatle slijedi da prostih brojeva ima beskonačno mnogo. □

Također, svaki prirodan broj n možemo zapisati u obliku $n = \prod_{p\in\mathcal{P}} p^{\alpha_p}$, gdje je $\alpha_p \in \mathbb{N}\cup\{0\}$ te su svi osim konačno mnogo brojeva α_p jednaki nuli.

Ukoliko su s $a = \prod_{p\in\mathcal{P}} p^{\alpha_p}$, $b = \prod_{p\in\mathcal{P}} p^{\beta_p}$ dani prikazi prirodnih brojeva a i b u obliku produkata potencija prostih brojeva, tada se lako može vidjeti da vrijedi $(a,b) = \prod_{p\in\mathcal{P}} p^{\min(\alpha_p,\beta_p)}$. Možemo zaključiti kako se najveći zajednički djelitelj može lako odrediti ukoliko je poznat rastav danih brojeva na proste faktore, tj. ukoliko je poznata njihova faktorizacija. No, postupak faktorizacije prirodnog broja na proste faktore i ispitivanje prostosti danog broja pripadaju među najteže probleme u teoriji brojeva za čije rješavanje postoje brojni algoritamski postupci koji su prespori u slučaju velikih brojeva.

Ukoliko su a i b cijeli brojevi različiti od nule, možemo definirati i njihov ***najmanji zajednički višekratnik*** kao najmanji prirodan broj koji je djeljiv i s a i s b. Najmanji zajednički višekratnik brojeva a i b označavamo s $[a,b]$. Analogno se može definirati i najmanji zajednički višekratnik cijelih brojeva $a_1, a_2, \ldots, a_n$ (koji su svi različiti od nule) koji se označava s $[a_1, a_2, \ldots, a_n]$.

Lako se može vidjeti da vrijedi $[3,5] = 15$, $[6,4,9] = 36$ te $[a,b] = |a|$ ukoliko b dijeli a. Također, primijetimo da ukoliko $a \mid m$ i $b \mid m$, tada i $[a,b] \mid m$.

Konačno, ukoliko su s $a = \prod_{p\in\mathcal{P}} p^{\alpha_p}$, $b = \prod_{p\in\mathcal{P}} p^{\beta_p}$ dani prikazi prirodnih brojeva a i b u obliku produkata potencija prostih brojeva, tada vrijedi $[a,b] = \prod_{p\in\mathcal{P}} p^{\max(\alpha_p,\beta_p)}$.

Odatle slijedi i $(a,b)\cdot[a,b] = a\cdot b$.

Za prirodan broj n kažemo da je ***potpun kvadrat*** ako postoji cijeli broj m takav da je $n = m^2$. Brojevi $1, 4, 16, 49$ su potpuni kvadrati, dok npr. niti jedan prost broj nije potpun kvadrat.

Može se lako vidjeti da je prirodan broj $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, $n \geq 2$ potpun kvadrat ako i samo ako $2 \mid \alpha_i$ za sve $i = 1, 2, \ldots, k$ (zaista, zapišemo li $\alpha_i = 2\cdot\beta_i$, tada je $n = (p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k})^2$, dok je obrat očigledan).

Za prirodan broj n kažemo da je ***kvadratno slobodan*** ako je 1 najveći potpuni kvadrat koji ga dijeli, tj. ukoliko iz $m^2 \mid n$, $m \in \mathbb{N}$, slijedi $m = 1$. Na

primjer, brojevi 6 i 15 su kvadratno slobodni, dok 12 i 100 nisu. Također, svaki prost broj je kvadratno slobodan. Prirodan broj $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $n \geq 2$, je kvadratno slobodan ako i samo ako je $\alpha_i = 1$, za svaki i.

Broj djelitelja i suma djelitelja prirodnog broja

U ovom potpoglavlju zanimat će nas samo pozitivni djelitelji prirodnih brojeva. Dakle, neka je n prirodan broj veći od 1 te zapišimo n u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (ukoliko je $n = 1$, broj i suma djelitelja su očiti).

Sa $\sigma(n)$ označavamo sumu svih pozitivnih djelitelja broja n, dok s $\tau(n)$ označavamo broj svih pozitivnih djelitelja od n.

Prema propoziciji 1.4.4, svaki djelitelj broja n je oblika $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, gdje je $0 \leq \beta_i \leq \alpha_i$ za sve $i = 1, 2, \ldots, k$. Osim toga, vidimo da svakim ovakvim odabirom eksponenata $\beta_1, \beta_2, \ldots, \beta_k$ dobivamo po jedan djelitelj broja n. Prema tome, kako svaki β_i možemo odabrati na $\alpha_i + 1$ načina, po principu produkta slijedi

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Primjer 1.4.7. Neka je $n = 100$. Kako je $100 = 2^2 \cdot 5^2$, dobivamo $\tau(100) = (2 + 1)(2 + 1) = 9$.

Neka su sada a i b relativno prosti prirodni brojevi, prikažimo ih u obliku $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ i $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$. Kako je $(a, b) = 1$, mora vrijediti $p_i \neq q_j$, za sve i, j. Dakle, $a \cdot b = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l}$ odakle slijedi

$$\tau(ab) = (\alpha_1 + 1) \cdots (\alpha_k + 1) \cdot (\beta_1 + 1) \cdots (\beta_l + 1) = \tau(a)\tau(b).$$

Funkciju $f : \mathbb{N} \to \mathbb{C}$ za koju vrijedi $f(a \cdot b) = f(a) \cdot f(b)$, za relativno proste a i b te $f(1) = 1$ nazivamo ***multiplikativna funkcija***.

Pokazali smo da je funkcija τ multiplikativna.

Pokažimo da i funkcija σ ima to svojstvo. Očito je $\sigma(1) = 1$. Osim toga, $\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}$, za prost broj p.

Promotrimo najprije $\sigma(n)$ u slučaju $n = p^k q^l$, gdje su p i q različiti prosti brojevi. Tada redom imamo:

$$\begin{aligned}
\sigma(p^k q^l) &= 1 + p + p^2 + \cdots + p^k + q + pq + p^2 q + \cdots + p^k q + \cdots + \\
&\quad + q^l + pq^l + p^2 q^l + \cdots + p^k q^l \\
&= (1 + p + p^2 + \cdots + p^k)(1 + q + q^2 + \cdots + q^l) \\
&= \frac{p^{k+1} - 1}{p - 1} \cdot \frac{q^{l+1} - 1}{q - 1} \\
&= \sigma(p^k)\sigma(q^l).
\end{aligned}$$

Generalizacijom prethodnog računa dobivamo da je i funkcija σ multiplikativna te

$$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1} = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\cdots\sigma(p_k^{\alpha_k}).$$

Primjer 1.4.8. $\sigma(100) = \sigma(2^2\cdot 5^2) = \frac{2^3-1}{2-1}\cdot\frac{5^3-1}{5-1} = 217.$

Fermatovi i Mersenneovi brojevi

U ovom kratkom potpoglavlju uvodimo neke specijalne brojeve koji su od posebnog interesa u teoriji brojeva.

Pierre de Fermat bio je francuski pravnik te matematičar iz hobija koji je dao veliki doprinos u analitičkoj geometriji i teoriji vjerojatnosti, a smatra se i jednim od začetnika diferencijalnog računa. Posebno se ipak ističe svojim rezultatima u teoriji brojeva.

Fermatovi brojevi su brojevi oblika $F_n = 2^{2^n}+1$, gdje je n nenegativan cijeli broj. Prvih nekoliko Fermatovih brojeva su:

$$3,\ 5,\ 17,\ 257,\ 65537,\ 4294967297,\ 18446744073709551617,\ \ldots$$

Među Fermatovim brojevima ima i prostih i složenih, a zanimljivo je da su jedini poznati prosti Fermatovi brojevi upravo F_0, F_1, F_2, F_3 i F_4. Sam Pierre de Fermat (kojeg ćemo spominjati i u još nekoliko navrata) je u prvoj polovici 17. stoljeća smatrao da je i F_5 prost, no stotinjak godina nakon Fermata Leonard Euler pronašao je rastav $4294967297 = 641\cdot 6700417$. Drugi složeni Fermatovi brojevi također imaju posebno velike proste djelitelje te ih je iz tog razloga vrlo teško faktorizirati.

Još jedna posebnost Fermatovih brojeva leži u tome što zadovoljavaju nekoliko rekurzivnih relacija koje se mogu dokazati induktivno:

$$\begin{aligned}
F_n &= (F_{n-1}-1)^2+1\\
F_n &= F_{n-1}+2^{2n-1}F_0F_1\cdots F_{n-2}\\
F_n &= F_{n-1}^2-2(F_{n-2}-1)^2\\
F_n &= F_0F_1\cdots F_{n-1}+2
\end{aligned}$$

Posljednju od navedenih relacija iskoristit ćemo u dokazu sljedećeg rezultata.

Propozicija 1.4.9. *Svaka dva različita Fermatova broja su relativno prosta.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti $i > j$. Prema navedenoj relaciji, vrijedi $F_i = F_0 \cdots F_j \cdots F_{i-1} + 2$. Kako (F_i, F_j) dijeli F_i i (F_i, F_j) dijeli $F_0 \cdots F_j \cdots F_{i-1}$, slijedi da (F_i, F_j) dijeli 2. No, svi Fermatovi brojevi su neparni, odakle dobivamo $(F_i, F_j) = 1$. □

Prije nego se dotaknemo Mersenneovih, definirajmo ***savršene brojeve***:

Za prirodan broj n kažemo da je savršen ako vrijedi $\sigma(n) = 2n$, tj. ako je jednak sumi svojih djelitelja manjih od njega.

Primjeri savršenih brojeva su 6 i 28 jer je $6 = 1+2+3$ te $28 = 1+2+4+7+14$.

Sam naziv savršeni brojevi duguju Pitagorejcima koji su brojevima često pridavali mistična svojstva. Također, mnogo stoljeća su se filozofi bavili mističnim i religijskim značajem savršenih brojeva. Tako je sveti Augustin objasnio da je Bog mogao stvoriti svijet odjednom, ali je izabrao to učiniti u šest dana jer je savršenstvo stvaranja svijeta simbolizirano savršenim brojem 6. Rani tumači Starog zavjeta objašnjavali su da je savršenstvo svemira reprezentirano brojem 28, brojem dana koji je potreban da Mjesec obiđe Zemlju.

Problem određivanja parnih savršenih brojeva datira gotovo od matematičkih početaka i još je Euklid oko 300. godine prije Krista pokazao da ako je broj $2^n - 1$ prost onda je broj $2^{n-1}(2^n - 1)$ savršen. Stari su Grci poznavali samo četiri savršena broja: 6, 28, 496 i 8128, koji su navedeni u Nikomahovoj knjizi *Introductio Arithmeticae*. Na osnovi toga nastala je slutnja da n-ti savršen broj ima točno n znamenki te da parni savršeni brojevi završavaju naizmjence znamenkama 6 i 8.

No obje navedene pretpostavke pokazale su se netočnima kada je Cataldi pokazao da su peti, šesti i sedmi savršeni broj jednaki 33550336, 8589869056 i 137438691328. Napomenimo i kako parni savršeni brojevi zaista završavaju znamenkama 6 i 8, ali ne naizmjenično.

Oko 2000 godina poslije Euklida, Euler je dopunio njegov rezultat:

Teorem 1.4.10. *Paran broj n je savršen ako i samo ako se može prikazati u obliku $n = 2^{k-1}(2^k - 1)$, gdje je broj $2^k - 1$ prost.*

Dokaz. Neka je $n = 2^{k-1}(2^k-1)$, gdje je 2^k-1 prost. Direktno slijedi $\sigma(2^{k-1}) = 1 + 2 + 4 + \cdots + 2^{k-1} = \frac{2^{k-1+1}-1}{2-1} = 2^k - 1$ te $\sigma(2^k - 1) = 1 + 2^k - 1 = 2^k$. Kako su 2^{k-1} i $2^k - 1$ relativno prosti, multiplikativnost funkcije σ povlači $\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(2^k - 1) = (2^k - 1) \cdot 2^k = 2n$ pa je broj n savršen.

Obratno, neka je n savršen; zapišimo ga u obliku $n = 2^k \cdot m$, gdje je $k \geq 0$ i m neparan. Kako je $\sigma(n) = 2n$, dobivamo

$$2^{k+1} \cdot m = 2n = \sigma(n) = \sigma(2^k \cdot m) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1)\sigma(m).$$

Iz prethodnih jednakosti zaključujemo da $2^{k+1}-1$ dijeli $2^{k+1}\cdot m$. Kako su 2^{k+1} i $2^{k+1}-1$ relativno prosti, $2^{k+1}-1$ dijeli m. Zapišimo sada m u obliku $m=(2^{k+1}-1)m'$. Dobivamo da je $\sigma(m)=2^{k+1}m'$ te $n=(2^{k+1}-1)2^km'$.

Preostaje još dokazati da je $m'=1$ i da je $2^{k+1}-1$ prost broj.

Ako je $m'\neq 1$, slijedi $\sigma(m)\geq 1+m'+m$. No, vidjeli smo da je $\sigma(m)=2^{k+1}m'=(2^{k+1}-1)m'+m'=m+m'<1+m'+m$. Prema tome, $m'=1$ te $m=2^{k+1}-1$. S druge strane, $\sigma(m)=m+m'=m+1$ pa je m (tj. $2^{k+1}-1$) prost broj. □

Napomenimo da još nije poznato postoji li neki neparan savršen broj.

Prema prethodnom teoremu, važnu ulogu pri određivanju parnih savršenih brojeva imaju prosti brojevi oblika 2^k-1. Upravo su takvi brojevi sadržani među Mersennovim brojevima, koji su brojevi oblika $M_n=2^n-1$, gdje je n prirodan broj. Ti su brojevi nazvani prema francuskom redovniku i matematičaru Marinu Mersenneu koji je živio u drugoj polovici 16. i prvoj polovici 17. stoljeća. Napomenimo da su Mersenne i Fermat često pismima raspravljali o matematičkim problemima, prvenstveno o pitanjima prostosti brojeva oblika 2^n+1 i 2^n-1.

Prvih nekoliko Mersenneovih brojeva su $1,3,7,15,31,63,127,255$, iz čega je vidljivo da su neki Mersenneovi brojevi prosti, a neki složeni. Mersenneovi brojevi koji su prosti nazivaju se ***Mersenneovi prosti brojevi***.

Propozicija 1.4.11. *Ako je Mersenneov broj M_n prost, tada je i n prost broj.*

Dokaz. Ako je broj n složen, možemo ga zapisati u obliku $n=rs$, za neke prirodne brojeve r,s koji su oba veći od 1. Tada je

$$2^{rs}-1=(2^s-1)(2^{s(r-1)}+2^{s(r-2)}+\cdots+2^s+1)$$

te je M_n složen broj jer je djeljiv s 2^s-1. □

U uvodu svoje knjige *Cogitata physico mathematica* 1644. godine Mersenne je iznio posebno zanimljivu tvrdnju o Mersenneovim prostim brojevima. Ustvrdio je da je M_p prost broj za $p=2,3,5,7,13,17,19,31,67,127,257$ te da je M_p složen za sve ostale proste brojeve $p<257$. Mersenneova tvrdnja pobudila je veliko zanimanje iz razloga što su navedeni brojevi toliko veliki da nekoliko stotina godina nitko nije mogao potvrditi ni opovrgnuti njegovu tvrdnju. Tadašnjim je matematičarima bilo jasno da Mersenne nije mogao provjeriti tvrdnju za sve navedene brojeve, ali isto tako nisu mogli ni oni. Euler je 1772. dokazao

da je M_{31} prost, a Lucas 1876. da je i M_{127} prost. Američki matematičar Cole pokazao je 1903.

$$2^{67} - 1 = 193707721 \cdot 761838257287,$$

odakle slijedi da M_{67} nije prost broj. Do 1947. testirani su svi Mersenneovi brojevi M_n za $n \leq 257$ te je pokazano da je Mersenne napravio pet pogrešaka: neispravno je zaključio da su M_{67} i M_{257} prosti te da su M_{61}, M_{89} i M_{107} složeni.

Još nije dokazana slutnja da postoji beskonačno mnogo prostih Mersenneovih brojeva.

Iskažimo na ovom mjestu i kriterij za ispitivanje prostosti Mersenneovih brojeva koji se naziva Lucas-Lehmerov test.

Teorem 1.4.12. *Definirajmo niz prirodnih brojeva* (s_n) *sa* $s_1 = 4$, $s_{n+1} = s_n^2 - 2$. *Neka je* p *neparan prost broj. Mersenneov broj* M_p *je prost ako i samo ako* M_p *dijeli* s_{p-1}.

Dokaz navedenog kriterija koji daleko nadilazi okvire ovog udžbenika može se naći u [13, poglavlje 4.].

2

KONGRUENCIJE

Teorija kongruencija predstavlja još jedno naslijeđe 'Princa matematike', Carl Friedricha Gaussa koji je ovu moćnu tehniku, poznatu i pod nazivom modularna aritmetika, zasnovao u svom djelu *Disquisitiones Arithmeticae* objavljenom 1801. Spomenuta knjiga sastojala se od sedam poglavlja, od kojih je prvih šest bilo posvećeno teoriji brojeva.

Svakodnevni primjer te teorije srećemo pri mjerenju vremena gdje koristimo tzv. aritmetiku modulo 12, dijeleći dan na dva perioda u trajanju od po 12 sati.

2.1. Definicija i osnovna svojstva

Neka je n prirodan broj te neka su a i b cijeli brojevi. Ako n dijeli razliku $a-b$, tada kažemo da je a ***kongruentan*** b ***modulo*** n ili da su a i b ***kongruentni modulo*** n te pišemo $a \equiv b \pmod{n}$.

Primijetimo da je a djeljivo s n ako i samo ako je $a \equiv 0 \pmod{n}$. Također, ako je c prirodan broj i $a \equiv b \pmod{n}$, tada je i $ac \equiv bc \pmod{nc}$.

Primjer 2.1.1. $17 \equiv 5 \pmod{12}$ i $5 \equiv 5 \pmod{12}$. Slično, $24 \equiv 0 \pmod{12}$. Također, $6 \equiv -34 \pmod{40}$.

Napomena 2.1.2. *Budući da $n \mid a-b$ ako i samo ako $-n \mid a-b$, gdje je $n \in \mathbb{Z} \setminus \{0\}$, dovoljno je promatrati samo pozitivne brojeve n.*

Lema 2.1.3. *Neka je n prirodan broj. Biti kongruentan modulo n je relacija ekvivalencije na skupu cijelih brojeva.*

Dokaz. Pokažimo najprije da je a kongruentan b modulo n ako i samo ako a i b daju isti ostatak prije dijeljenju s n.

Pretpostavimo da je a kongruentan b modulo n te korištenjem Teorema o dijeljenju s ostatkom napišimo $a = q_1 \cdot n + r_1$ i $b = q_2 \cdot n + r_2$, pri čemu vrijedi $0 \leq r_1, r_2 \leq n-1$. Sada je $a - b = (q_1 - q_2)n + r_1 - r_2$. Kako n dijeli $a - b$, dobivamo da n dijeli i $r_1 - r_2$ te iz $-n+1 \leq r_1 - r_2 \leq n-1$ slijedi $r_1 - r_2 = 0$, tj. $r_1 = r_2$.

S druge strane, ukoliko a i b daju isti ostatak pri dijeljenju s n, na analogan način slijedi da n dijeli $a - b$, tj. $a \equiv b \pmod{n}$.

Iz dokazanog sada očito slijedi $a \equiv a \pmod{n}$. Također, kako $n \mid a - b$ ako i samo ako $n \mid b - a$, vrijedi i $a \equiv b \pmod{n}$ ako i samo ako je $b \equiv a \pmod{n}$.

Neka su sada a, b, c cijeli brojevi te neka vrijedi $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$. Odatle zaključujemo kako a i b te b i c daju isti ostatak prije dijeljenju s n pa je $a \equiv c \pmod{n}$. □

U sljedećoj propoziciji navodimo osnovna svojstva kongruencija.

Propozicija 2.1.4. (1) *Neka su a, a', b, b' cijeli brojevi te n prirodan broj. Neka je $a \equiv a' \pmod{n}$ i $b \equiv b' \pmod{n}$. Tada vrijedi i $a + b \equiv a' + b' \pmod{n}$, $a - b \equiv a' - b' \pmod{n}$ te $a \cdot b \equiv a' \cdot b' \pmod{n}$.*
(2) *Neka su a, b, c cijeli brojevi i n prirodan broj. Neka su brojevi a i n relativno prosti. Ako je $ab \equiv ac \pmod{n}$, tada vrijedi i $b \equiv c \pmod{n}$.*

Dokaz. (1) Dokažimo treću tvrdnju, prve dvije mogu se dokazati na isti način. Prema uvjetima propozicije, postoje cijeli brojevi m i m' takvi da je $a - a' = mn$ i $b - b' = m'n$. Odatle je $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = am'n + b'm'n$. Prema tome, n dijeli $ab - a'b'$ pa je $ab \equiv a'b' \pmod{n}$.
(2) Kako su a i n relativno prosti, prema teoremu 1.2.3 postoje cijeli brojevi x i y takvi da je $ax + ny = 1$. Iz kongruencije $ab \equiv ac \pmod{n}$ slijedi da postoji cijeli broj k takav da je $a(b - c) = nk$. Množenjem prethodne jednakosti s x, iz $ax = 1 - ny$ dobivamo $(b - c) - ny(b - c) = nkx$. Očito n dijeli $b - c$ pa je $b \equiv c \pmod{n}$. □

Primijetimo da tvrdnja (2) prethodne propozicije ne vrijedi općenito, tj. ukoliko a i n nisu relativno prosti. Npr. $60 \equiv 20 \pmod{5}$, no kongruencija $6 \equiv 2 \pmod{5}$ nije točna. Više informacija o kraćenju u kongruencijama donosi sljedeća propozicija.

Propozicija 2.1.5. *Neka je $ax \equiv ay \pmod{n}$. Tada vrijedi i $x \equiv y \pmod{\frac{n}{d}}$, gdje je $d = (a, n)$.*

Dokaz. Kako je $ax \equiv ay \pmod{n}$, postoji cijeli broj k takav da vrijedi $ax - ay = kn$. Odatle je $\frac{a}{d}(x - y) = \frac{nk}{d}$ pa $\frac{n}{d} \mid \frac{a}{d}(x - y)$. No, kako su $\frac{n}{d}$ i $\frac{a}{d}$ relativno

prosti jer nemaju zajedničkih prostih faktora, dobivamo $\frac{n}{d} \mid x - y$, čime je tvrdnja dokazana. □

Lako se može vidjeti da korištenjem dijela (1) propozicije 2.1.4 vrijedi i obrat prethodne tvrdnje.

Pogledajmo još jednu posljedicu propozicije 2.1.4:

Propozicija 2.1.6. *Neka je n prirodan broj te a i b cijeli brojevi takvi da je $a \equiv b \pmod{n}$. Tada za polinom $p(x)$ s cjelobrojnim koeficijentima vrijedi $p(a) \equiv p(b) \pmod{n}$.*

Dokaz. Neka je $p(x) = \sum_{i=0}^{k} c_i x^i$. Uzastopnom primjenom dijela (1) propozicije 2.1.4 dobivamo $a^i \equiv b^i \pmod{n}$ te $c_i a^i \equiv c_i b^i \pmod{n}$, za sve i. Sumiramo li dobivene kongruencije, dobivamo

$$p(a) = \sum_{i=0}^{k} c_i a^i \equiv \sum_{i=0}^{k} c_i b^i = p(b) \pmod{n}.$$

□

Također, u određenim je slučajevima moguće sustav kongruencija zamijeniti jednom kongruencijom:

Propozicija 2.1.7. *Neka su $n_1, n_2, \ldots, n_k$ prirodni brojevi. Tada su sljedeće tvrdnje ekvivalentne:*

1. $a \equiv b \pmod{n_i}$, *za* $i = 1, 2, \ldots, k$.

2. $a \equiv b \pmod{[n_1, n_2, \ldots, n_k]}$.

Dokaz. Neka je najprije $a \equiv b \pmod{n_i}$, za $i = 1, 2, \ldots, k$. Odatle slijedi da n_i dijeli $a - b$ za sve $i = 1, 2, \ldots, k$ pa je $a - b$ zajednički višekratnik brojeva $n_1, n_2, \ldots, n_k$. No, tada i $[n_1, n_2, \ldots, n_k]$ dijeli $a - b$, tj. $a \equiv b \pmod{[n_1, n_2, \ldots, n_k]}$.

Obratno, neka je $a \equiv b \pmod{[n_1, n_2, \ldots, n_k]}$. Kako $[n_1, n_2, \ldots, n_k]$ dijeli $a - b$ te n_i dijeli $[n_1, n_2, \ldots, n_k]$ za sve $i = 1, 2, \ldots, k$, slijedi da i n_i dijeli $a - b$ za sve $i = 1, 2, \ldots, k$, tj. $a \equiv b \pmod{n_i}$ za $i = 1, 2, \ldots, k$. □

Pogledajmo i jedan primjer rješavanja kongruencije, tj. kongruencijske jednadžbe. Potrebno je odrediti vrijednosti nepoznanica za koje će dana kongruencija biti zadovoljena.

Primjer 2.1.8. Odredimo $x \in \mathbb{Z}$ za koji vrijedi $341x \equiv 1 \pmod{17}$. Kako je 340 djeljivo sa 17, slijedi $340 \equiv 0 \pmod{17}$ te $340x \equiv 0 \pmod{17}$. Prikažemo li $341x$ u obliku $340x + x$, iz prethodne propozicije nalazimo $341x \equiv x \pmod{17}$. Dakle, danu kongruenciju zadovoljava svaki cijeli broj x koji je kongruentan 1 modulo 17, tj. $x \in \{\ldots, -33, -16, 1, 18, 35, \ldots\}$.

O raznolikoj primjeni kongruencija bit će više riječi u sljedećem poglavlju.

Potpuni i reducirani sustavi ostataka

Neka je n prirodan broj veći od 1. Skup $S = \{a_1, a_2, \ldots, a_n\}$ naziva se ***potpuni sustav ostataka modulo*** n ako za svaki cijeli broj b postoji jedinstveni $a_i \in S$ za koji vrijedi $b \equiv a_i \pmod{n}$.

Napomena 2.1.9. *Primijetimo kako svaki potpuni sustav ostataka modulo n ima točno n elemenata. Također, svaki n-člani skup koji se sastoji od cijelih brojeva međusobno nekongruentnih modulo n predstavlja jedan potpuni sustav ostataka modulo n.*

Najčešće korišten potpuni sustav ostataka modulo n je skup $\{0, 1, 2, \ldots, n-1\}$. Navedimo i nekoliko potpunih sustava ostataka modulo 5:

$$\{0, 1, 2, 3, 4\},\ \{-2, -1, 0, 1, 2\},\ \{1, 2, 3, 4, 5\},\ \{-10, -8, -4, 13, 39\}.$$

Očito ih postoji beskonačno mnogo, što pokazuje i sljedeća lema:

Lema 2.1.10. *Neka je $S = \{a_1, a_2, \ldots, a_n\}$ potpuni sustav ostataka modulo n. Tada je i $\{b \cdot a_1, b \cdot a_2, \ldots, b \cdot a_n\}$ potpuni sustav ostataka modulo n, za svaki cijeli broj b za koji vrijedi $(b, n) = 1$.*

Dokaz. Prema napomeni 2.1.9, dovoljno je dokazati da su svaka dva elementa skupa $\{b \cdot a_1, b \cdot a_2, \ldots, b \cdot a_n\}$ međusobno nekongruentna modulo n. Pretpostavimo da je $b \cdot a_i \equiv b \cdot a_j \pmod{n}$, za neke i, j. Kako su b i n relativno prosti, propozicija 2.1.4 (2) povlači $a_i \equiv a_j \pmod{n}$. Iz činjenice da je S potpuni sustav ostataka modulo n, zaključujemo da je $i = j$, čime je tvrdnja dokazana. □

U nastavku ćemo kratko komentirati rješavanje linearnih kongruencija, tj. kongruencija oblika $ax \equiv b \pmod{n}$. Prvotno zanimanje za rješavanje takvih kongruencija dolazi iz diofantskih jednadžbi gdje se često mogu iskoristiti za pronalaženje rješenja ili za dokazivanje neegzistencije rješenja.

Lema 2.1.11. *Neka su a i n prirodni brojevi. Ako su a i n relativno prosti, tada kongruencija $ax \equiv b \pmod{n}$ ima jedinstveno rješenje modulo n, u smislu da ako je $S = \{a_1, a_2, \ldots, a_n\}$ potpuni sustav ostataka modulo n tada postoji jedinstveni $a_i \in S$ takav da je $x \equiv a_i \pmod{n}$ rješenje polazne kongruencije.*

Dokaz. Kako su a i n relativno prosti, postoje cijeli brojevi k, l za koje vrijedi $ak + nl = 1$, odakle je $akb + nkb = b$. Očito, $akb \equiv b \pmod{n}$ pa je $x = kb$ rješenje polazne kongruencije.

Neka su sada x_1 i x_2 dva rješenja polazne kongruencije. Dokažimo da su ta rješenja međusobno kongruentna modulo n.

Kako je $ax_1 \equiv b \pmod{n}$ i $ax_2 \equiv b \pmod{n}$, dobivamo $ax_1 \equiv ax_2 \pmod{n}$. Primjenom propozicije 2.1.4 slijedi $x_1 \equiv x_2 \pmod{n}$, što je i trebalo dokazati. □

Primjer 2.1.12. Kongruencija $3x \equiv 50 \pmod{113}$ ima jedinstveno rješenje, koje je dano s $x \equiv 92 \pmod{113}$.

Jednadžba $5x + 15y = 1$ nema cjelobrojnih rješenja jer kongruencija $5x \equiv 1 \pmod{15}$ nema rješenja.

Teorem 2.1.13. *Neka su a i n prirodni brojevi. Kongruencija $ax \equiv b \pmod{n}$ ima rješenja ako i samo ako $d = (a, n)$ dijeli b. Ako je x_0 rješenje kongruencije $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, tada su sva međusobno nekongruentna rješenja modulo n polazne kongruencije dana s $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$.*

Dokaz. Ako kongruencija $ax \equiv b \pmod{n}$ ima rješenja, tada postoji cijeli broj k takav da je $ax = b + nk$ pa očito $d = (a, n)$ dijeli b.

Kako su brojevi $\frac{a}{d}$ i $\frac{n}{d}$ relativno prosti, prema prethodnoj lemi postoji rješenje kongruencije $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. Označimo to rješenje s x_0. Dakle, postoji cijeli broj k takav da je $\frac{a}{d}x_0 - \frac{b}{d} = k \cdot \frac{n}{d}$, tj. $ax_0 - b = kn$. Prema tome, x_0 je i rješenje kongruencije $ax \equiv b \pmod{n}$.

Stavimo $y = x_0 + t\frac{n}{d}$. Tada je $ay = ax_0 + \frac{a}{d}tn$. Kako d dijeli a, $\frac{a}{d}$ je prirodan broj pa n dijeli $ay - ax_0$. Odatle dobivamo $ay \equiv ax_0 \pmod{n}$ te $ay \equiv b \pmod{n}$. Dakle, y je također rješenje polazne kongruencije.

Pretpostavimo sada da je y rješenje polazne kongruencije. Tada je $ay \equiv ax_0 \pmod{n}$, odakle proizlazi da $\frac{n}{d}$ dijeli $\frac{a}{d}(y - x_0)$. Budući da su $\frac{a}{d}$ i $\frac{n}{d}$ relativno prosti, $\frac{n}{d}$ dijeli $y - x_0$ pa je $y = x_0 + k\frac{n}{d}$, za neki cijeli broj k.

Neka je $0 \leq j \leq d - 1$ takav da je $k \equiv j \pmod{d}$. Tada je $y \equiv x_0 + j\frac{n}{d} \pmod{n}$.

Lako se vidi da ne postoje dva različita broja oblika $x_0 + j\frac{n}{d}$ koja su međusobno kongruentna modulo n za $0 \leq j \leq d - 1$. □

U situaciji kao u iskazu prethodnog teorema, kažemo da kongruencija ima d rješenja modulo n. Općenito, kažemo da kongruencija modulo n ima m rješenja ukoliko ima m međusobno nekongruentnih rješenja modulo n.

Neka je n prirodan broj veći od 1. Skup $S = \{a_1, a_2, \ldots, a_k\}$ naziva se ***reducirani sustav ostataka modulo*** n ako za svaki cijeli broj b koji je relativno prost s n postoji jedinstveni $a_i \in S$ za koji vrijedi $b \equiv a_i \pmod{n}$.

Primjer 2.1.14. Skupovi $\{1, 2, 3, 4\}$ i $\{-2, -6, 6, 7\}$ su reducirani sustavi ostataka modulo 5, dok je npr. $\{1, 5\}$ reducirani sustav ostataka modulo 6.

Primijetimo da postoji beskonačno mnogo reduciranih sustava ostataka modulo n. Također, svaki reducirani sustav ostataka modulo n ima jednako mnogo elemenata.

2.2. Eulerova funkcija

Neka je n prirodan broj. Broj prirodnih brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n označava se s $\varphi(n)$; ovim je definirana funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ koja se naziva ***Eulerova funkcija***.

Primijetimo kako je $\varphi(n)$ upravo broj elemenata reduciranog sustava ostataka modulo n, te u daljnjem reducirani sustav ostataka možemo zapisati u obliku $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$.

Primjer 2.2.1. $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(1) = 1$. Ako je p prost broj, tada je $\varphi(p) = p-1$. Također, ako za neki prirodan broj n vrijedi $\varphi(n) = n-1$, možemo zaključiti kako je n relativno prost sa svakim manjim prirodnim brojem. Prema tome, n nema djelitelja većeg od 1 i manjeg od n pa je prost.

Na isti način kao lema 2.1.10 može se dokazati i

Lema 2.2.2. *Neka je $S = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Tada je i $\{b \cdot a_1, b \cdot a_2, \ldots, b \cdot a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n, za svaki cijeli broj b za koji vrijedi $(b, n) = 1$.*

Teorem 2.2.3 (Eulerov teorem)**.** *Neka je a cijeli broj te n prirodan broj. Ako su brojevi a i n relativno prosti, tada je $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Dokaz. Neka je $S = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Prema prethodnoj lemi tada je i skup $\{a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Prema tome, za svaki a_i, $1 \leq i \leq \varphi(n)$, postoji jedinstveni $a_j \in S$ takav da je $a_i \equiv a \cdot a_j \pmod{n}$.

Primjenom propozicije 2.1.4 (1) dobivamo $a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv aa_1 \cdot aa_2 \cdots aa_{\varphi(n)} \pmod{n}$, tj. $a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 \cdot a_2 \cdots a_{\varphi(n)} \pmod{n}$.

Kako je $(a_i, n) = 1$ za sve $a_i \in S$, uzastopnom primjenom propozicije 2.1.4 (2) dobivamo $1 \equiv a^{\varphi(n)} \pmod{n}$, čime je teorem dokazan. □

Ako je p prost broj i a cijeli broj koji nije djeljiv s p, tada su a i p relativno prosti. Sljedeći je rezultat izravna posljedica Eulerova teorema:

Korolar 2.2.4 (Mali Fermatov teorem)**.** *Neka je p prost broj i a cijeli broj. Tada je $a^p \equiv a \pmod{p}$ te ako p ne dijeli a vrijedi i $a^{p-1} \equiv 1 \pmod{p}$.*

U ostatku potpoglavlja opisat ćemo još neka svojstva Eulerove funkcije.

Lema 2.2.5. *Neka je p prost broj i $k \in \mathbb{N}$. Tada je $\varphi(p^k) = p^k - p^{k-1}$.*

Dokaz. Neka je $1 \leq n \leq p^k$. Ako p ne dijeli n, tada su n i p^k relativno prosti. Prema tome, jedini brojevi u nizu $1, 2, \ldots, p^k$ koji nisu relativno prosti s p^k su $p, 2p, 3p, \ldots, p^k = p^{k-1} \cdot p$, tj. njih p^{k-1}. Odatle slijedi $\varphi(p^k) = p^k - p^{k-1}$. □

Pokazat ćemo i da je Eulerova funkcija multiplikativna. Očito je $\varphi(1) = 1$. U tome će nam koristiti i sljedeći rezultat.

Lema 2.2.6 (Kineski teorem o ostatcima)**.** *Neka su m i n relativno prosti prirodni brojevi. Tada za svaki par cijelih brojeva a, b postoji jedinstveno (modulo mn) rješenje sustava kongruencija $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$.*

Dokaz. Primijetimo da se ovdje radi o sustavu dvije jednadžbe, tj. kongruencije s jednom nepoznanicom. Promatramo preslikavanje

$$i : \{0, 1, \ldots, mn-1\} \to \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\},$$

dano s $i(t) = (t \bmod m, t \bmod n)$.

Primjerice, neka je $m = 2$, $n = 5$ te $a = 1$, $b = 3$. U tom slučaju je npr. $i(0) = (0, 0)$, $i(1) = (1, 1)$, $i(2) = (0, 2)$, $i(7) = (1, 2)$, $i(8) = (1, 3)$, $i(9) = (1, 4)$. Očito je rješenje polaznog sustava kongruencija x za koji vrijedi $i(x) = (1, 3)$ te je dano s $x \equiv 8 \pmod{10}$.

Prema tome, da bismo dokazali tvrdnju leme dovoljno je dokazati da je preslikavanje i bijekcija. Kako skupovi $\{0, 1, \ldots, mn-1\}$ i $\{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$ imaju jednako mnogo elemenata, dovoljno je pokazati da je i injekcija.

Neka su $t_1, t_2 \in \{0, 1, \ldots, mn-1\}$ takvi da je $i(t_1) = i(t_2)$. Tada je $t_1 \equiv t_2 \pmod{m}$ i $t_1 \equiv t_2 \pmod{n}$, tj. $m \mid t_1 - t_2$ i $n \mid t_1 - t_2$. Kako su m i n relativno

prosti, slijedi $mn \mid t_1 - t_2$ te (zbog $-mn+1 \leq t_1 - t_2 \leq mn-1$) $t_1 = t_2$. Prema tome, i je injekcija. □

Punu verziju Kineskog teorema o ostatcima bez dokaza iskazujemo u sljedećem teoremu:

Teorem 2.2.7. *Neka su $n_1, n_2, \ldots, n_k$ u parovima relativno prosti prirodni brojevi te neka su $a_1, a_2, \ldots, a_k$ cijeli brojevi. Tada postoji rješenje sustava kongruencija $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $\ldots$, $x \equiv a_k \pmod{n_k}$. Ako je x_0 jedno rješenje, tada su sva rješenja dana s $x \equiv x_0 \pmod{n_1 n_2 \cdots n_k}$, tj. rješenje je jedinstveno modulo $n_1 n_2 \cdots n_k$.*

Prema predaji, Kinezi su se često u primjenama koristili upravo prethodnim rezultatom. Neki navodi govore da je postupak određivanja rješenja sustava kongruencija prvenstveno korišten u vojne svrhe prilikom prebrojavanja preživjelih vojnika nakon bitke. Naime, umjesto da se nepotrebno troši vrijeme na dugačka prebrojavanja, preživjeli bi se vojnici jednostavno postrojili u redove od $3, 4, 5, 7, 11$ i eventualno 13 vojnika (ukoliko bi se radilo o većem broju preživjelih vojnika), a potom bi se, pomoću broja vojnika preostalih u zadnjem redu dobivao sustav kongruencija. Rješavanje tako dobivenog sustava rezultiralo bi kongruencijom iz koje bi se direktno dobio točan broj preživjelih vojnika. Naravno, broj vojnika u pojedinom redu mogao se i mijenjati, jedino se uvijek moralo paziti da brojevi budu međusobno relativno prosti te njihov produkt dovoljno velik kako bi se iz završne kongruencije mogao očitati točan broj preživjelih vojnika. Sam dokaz prethodnog teorema te njegove primjene i poopćenja mogu se naći u [2].

Teorem 2.2.8. *Eulerova funkcija je multiplikativna.*

Dokaz. Već smo vidjeli da je $\varphi(1) = 1$. Neka su sada m, n relativno prosti cijeli brojevi. Definiramo skupove $S_1 = \{a \in \mathbb{N} : a \leq mn,\ (a, mn) = 1\}$, $S_2 = \{a \in \mathbb{N} : a \leq m,\ (a, m) = 1\}$, $S_3 = \{a \in \mathbb{N} : a \leq n,\ (a, n) = 1\}$. Očito je $|S_1| = \varphi(mn)$, $|S_2| = \varphi(m)$ te $|S_3| = \varphi(n)$.

Za $t \in \{0, 1, \ldots, mn-1\}$ neka je $i(t) = (a, b)$, gdje je i preslikavanje definirano u dokazu leme 2.2.6. Primijetimo da je $(t, mn) = 1$ ako i samo ako je $(a, m) = (b, n) = 1$. Zaista, kako je $t = k_1 m + a = k_2 n + b$, slijedi da je svaki zajednički prost djelitelj brojeva t i m (odnosno, t i n) ujedno i zajednički prost djelitelj brojeva a i m (odnosno, b i n).

Prema tome, restrikcija preslikavanja i na skup S_1 daje bijekciju sa skupa S_1 na skup $S_2 \times S_3$, što povlači $\varphi(mn) = \varphi(m)\varphi(n)$. □

Neka je $n > 1$ prirodan broj. Prikažimo n u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Tada je

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\ &= p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).\end{aligned}$$

Primjer 2.2.9. $\varphi(100) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40.$

2.3. Wilsonov i Lagrangeov teorem

Neka je p prost broj i $a < p$ prirodan broj. Tada postoji prirodan broj b za koji vrijedi $a \cdot b \equiv 1 \pmod{p}$ i takav broj b naziva se multiplikativni inverz od a modulo p.

Zaista, kako su a i p relativno prosti, prema teoremu 1.2.3 postoje cijeli brojevi x, y za koje vrijedi $ax + py = 1$, odakle slijedi $ax \equiv 1 \pmod{p}$ te možemo uzeti $b = x$. Primijetimo kako iz leme 2.1.11 slijedi da su svaka dva multiplikativna inverza od a modulo p međusobno kongruentna modulo p pa postoji jedinstveni multiplikativni inverz od a modulo p koji je prirodan broj manji od p.

Općenito, ako je $a \in \mathbb{N}$ te $p \nmid a$, tada postoji multiplikativni inverz od a modulo p.

Jedna od najistaknutijih primjena multiplikativnih inverza pojavljuje se prilikom evaluacije produkta $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$ modulo p, gdje je p prost broj. Sljedeći teorem pripisuje se engleskom matematičaru iz 18. stoljeća, Johnu Wilsonu, iako ga je vjerojatno otkriven Ibn al-Hayhama u 10. stoljeću, a prvi poznati dokaz je Lagrangeov i datira iz 1770.

Teorem 2.3.1 (Wilsonov teorem)**.** *Ako je p prost broj tada je $(p-1)! \equiv -1 \pmod{p}$.*

Dokaz. Prema diskusiji koja prethodi teoremu, za svaki od brojeva $1, 2, \ldots, p-1$ postoji multiplikativni inverz modulo p. Dakle, svaki od faktora u $(p-1)! = 1 \cdot 2 \cdots (p-1)$ daje 1 modulo p u produktu sa svojim multiplikativnim inverzom, osim faktora koji su sami sebi inverzni. Odredimo takve faktore.

Neka je $x \in \{1, 2, \ldots, p-1\}$ takav da vrijedi $x^2 \equiv 1 \pmod{p}$. Tada p dijeli $x^2 - 1 = (x-1)(x+1)$. Kako je p prost broj i $1 \leq x \leq p-1$, slijedi da je

ili $x-1=0$ ili $x+1=p$. Prema tome, jedini faktori u $(p-1)!$ koji su sami sebi inverzni su 1 i $p-1$. Odatle dobivamo $(p-1)! \equiv 1 \cdot (p-1) \pmod{p}$ te $(p-1)! \equiv -1 \pmod{p}$. □

Prethodni teorem zapravo daje zanimljivu karakterizaciju prostih brojeva jer vrijedi i obrat:

Propozicija 2.3.2. *Ako prirodan broj n zadovoljava kongruenciju $(n-1)! \equiv -1 \pmod{n}$, tada je n prost.*

Dokaz. Iz $(n-1)! \equiv -1 \pmod{n}$ slijedi $(n-1)! \equiv -1 \pmod{m}$, za svaki m koji dijeli n. Ako je $m < n$, tada se m pojavljuje kao faktor od $(n-1)!$ pa je $(n-1)! \equiv 0 \pmod{m}$ te $-1 \equiv 0 \pmod{m}$. Odavde je $m = 1$ te n nema pozitivnih djelitelja različitih od 1 i n pa je n prost. □

Primjer 2.3.3. Iz Wilsonova teorema slijedi $100! \equiv -1 \pmod{101}$, tj. $101 \mid 100! + 1$.

Sada ćemo pokazati kako Wilsonov teorem može biti primijenjen na rješavanje određenih kongruencija, koje ćemo detaljnije obraditi u 4. poglavlju.

Korolar 2.3.4. *Neka je p neparan prost broj. Kongruencija $x^2+1 \equiv 0 \pmod{p}$ ima rješenja ako i samo ako je $p \equiv 1 \pmod{4}$.*

Dokaz. Neka je p neparan prost broj te neka je $k = \frac{p-1}{2}$. Korištenjem kongruencije $p - i \equiv -i \pmod{p}$ u produktu

$$(p-1)! = 1 \cdot 2 \cdots k \cdot (k+1) \cdots (p-2) \cdot (p-1)$$

za $i = 1, 2, \ldots, k$ dobivamo

$$(p-1)! \equiv (-1)^k (k!)^2 \pmod{p}.$$

Wilsonov teorem daje $(p-1)! \equiv -1 \pmod{p}$ te slijedi $(-1)^k (k!)^2 \equiv -1 \pmod{p}$, odakle dobivamo i $(k!)^2 \equiv (-1)^{k+1} \pmod{p}$. Kako je k paran za $p \equiv 1 \pmod{4}$, slijedi $(k!)^2 \equiv -1 \pmod{p}$ te je $x = k!$ rješenje kongruencije $x^2 + 1 \equiv 0 \pmod{p}$.

Neka je sada $p \equiv 3 \pmod{4}$, odakle je $k = \frac{p-1}{2}$ neparan. Ako je x rješenje kongruencije $x^2 + 1 \equiv 0 \pmod{p}$, tada su x i p relativno prosti te je, prema Malom Fermatovom teoremu, $x^{p-1} \equiv 1 \pmod{p}$. Prema tome, $1 \equiv (x^2)^k \equiv (-1)^k \equiv -1 \pmod{p}$, što nije moguće jer je p neparan te u ovom slučaju polazna kongruencija nema rješenja. □

Činjenica da kongruencija $x^2 - 1 \equiv 0 \pmod{p}$ ima najviše dva rješenja (nekongruentna modulo p) ima važnu generalizaciju:

Teorem 2.3.5 (Lagrangeov teorem)**.** *Ako je p prost broj i $P(x)$ polinom stupnja n s cjelobrojnim koeficijentima koji nisu svi djeljivi s p, tada kongruencija $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Dokaz. Dokaz provodimo indukcijom po stupnju polinoma $P(x)$. Ako je stupanj promatranog polinoma jednak 1, tvrdnja teorema slijedi direktno iz leme 2.1.11. Pretpostavimo da tvrdnja vrijedi za polinome stupnja manjeg od n te neka je $P(x)$ polinom stupnja n.

Najprije, ako kongruencija $P(x) \equiv 0 \pmod{p}$ nema rješenja, tada nemamo što dokazivati. Nasuprot tomu, pretpostavimo da je $P(x_0) \equiv 0 \pmod{p}$, za neki cijeli broj x_0 te neka je $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gdje su $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.

Odatle je $P(x) \equiv P(x) - P(x_0) \pmod{p}$, tj. $P(x) \equiv a_n(x^n - x_0^n) + a_{n-1}(x^{n-1} - x_0^{n-1}) + \ldots + a_1(x - x_0) \pmod{p}$.

Kako za $k \in \mathbb{N}$ vrijedi $x^k - x_0^k = (x - x_0)(x^{k-1} + x^{k-2}x_0 + \cdots + x x_0^{k-2} + x_0^{k-1})$, desnu stranu prethodne kongruencije možemo zapisati u obliku $(x - x_0)Q(x)$, gdje je $Q(x)$ polinom stupnja $n - 1$ s cjelobrojnim koeficijentima.

Kako je p prost broj, kongruencija $P(x) \equiv 0 \pmod{p}$ pokazuje da je $x - x_0 \equiv 0 \pmod{p}$ ili $Q(x) \equiv 0 \pmod{p}$. Prema pretpostavci indukcije, kongruencija $Q(x) \equiv 0 \pmod{p}$ ima najviše $n-1$ rješenja pa kongruencija $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja (x_0 i rješenja kongruencije $Q(x) \equiv 0 \pmod{p}$), što je i trebalo dokazati. □

2.4. Pseudoprosti i Carmichaelovi brojevi

Jedno od najčešće postavljanih pitanja u teoriji brojeva je kako na efikasan način provjeriti je li neki broj prost. Postupci koji za rezultat imaju potvrdan ili negativan odgovor na takvo pitanje nazivaju se ***testovi prostosti***. Posebna važnost ispitivanja prostosti danas se može naći u modernoj kriptografiji gdje su šifre bazirane na teškoći ispitivanja prostosti i faktorizacije prirodnih brojeva na proste faktore. O tom će više riječi biti u potpoglavljima 3.5 i 3.6.

Wilsonov teorem dokazan u prethodnom potpoglavlju daje vrlo jednostavnu karakterizaciju prostih brojeva. Nažalost, kompliciranost računanja faktorijela čini ga vrlo neefikasnim testom prostosti čak i za male prirodne brojeve poput dvoznamenkastih.

S druge strane, Mali Fermatov teorem predstavlja jedan način za ispitivanje prostosti: prema tom teoremu, tj. prema njegovu obratu, ako postoji prirodan broj $a < n-1$ takav da $a^{n-1} \not\equiv 1 \pmod{n}$, tada n nije prost broj. Taj test je mnogo jednostavnije primijeniti jer se u modularnoj aritmetici velike potencije mogu izračunati mnogo lakše nego faktorijeli. No, ukoliko za prirodan broj n vrijedi $a^{n-1} \equiv 1 \pmod{n}$, za sve $a \in \{2, 3, \ldots, n-1\}$, ne znači da je n prost jer Malim Fermatovim teoremom nije dana karakterizacija prostih brojeva. Iz tog razloga uvodi se sljedeći pojam:

Definicija 2.4.1. Ako je n neparan složen broj te a cijeli broj za koji vrijedi $(n, a) = 1$ i $a^{n-1} \equiv 1 \pmod{n}$, kažemo da je n ***pseudoprost*** u bazi a.

Još je u staroj Kini smatrano da je prirodan broj n prost ako i samo ako je $2^{n-1} \equiv 1 \pmod{n}$ (primijetimo da je, na primjer, $2^{6-1} = 32 \equiv 2 \pmod{6}$ te 6 nije prost broj), a ta je tvrdnja opovrgnuta tek 1819. sljedećim primjerom:

Primjer 2.4.2. Odredimo čemu je 2^{340} kongruentno modulo 341.

Na tom primjeru ukratko ćemo pokazati i način određivanja potencija modulo prirodan broj. Najprije primijetimo da je $2^{10} = 1024 \equiv 1 \pmod{341}$. Sada dobivamo

$$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{341}.$$

Prema tome, 341 je prošao prethodni test, ali nije prost jer vrijedi $341 = 11 \cdot 31$. Dakle, 341 je složen broj koji posjeduje određena svojstva prostih brojeva. Iz tog razloga kažemo da je 341 pseudoprost u bazi 2.

Prirodni brojevi koji su pseudoprosti u bazi 2 rijetki su, no ima ih mnogo.

Teorem 2.4.3. *Postoji beskonačno mnogo prirodnih brojeva koji su pseudoprosti u bazi* 2.

Dokaz. Neka je n pseudoprost broj u bazi 2. Dokazat ćemo da je tada i $2^n - 1$ pseudoprost u bazi 2. Na taj način, polazeći od 341 dobivamo beskonačno mnogo prirodnih brojeva koji su pseudoprosti u bazi 2.

Kako je n pseudoprost u bazi 2, n je složen neparan broj. Direktno slijedi da je i $2^n - 1$ složen. Kako je $2^{n-1} \equiv 1 \pmod{n}$, dobivamo $2^n \equiv 2 \pmod{n}$ te se 2^n može prikazati u obliku $nk + 2$, za neki prirodan broj k. Iz jednakosti

$$2^{nk} - 1 = (2^n)^k - 1 = (2^n - 1)((2^n)^{k-1} + (2^n)^{k-2} + \cdots + 1)$$

slijedi

$$2^{nk} = 2^{2^n - 2} \equiv 1 \pmod{2^n - 1},$$

što je i trebalo pokazati. □

Slično kao u dokazu teorema 2.4.3 može se pokazati da postoji beskonačno mnogo pseudoprostih brojeva u bazi a za svaki prirodan broj $a \geq 2$. Pogledajmo jedan zanimljiv primjer vezan uz pseudoprostost.

Primjer 2.4.4. Ranije smo vidjeli da je 341 pseudoprost u bazi 2. Iz činjenice da je 341 prošao test s bazom 2 nismo mogli zaključiti niti da je prost niti da je složen. Provedimo isti test s bazom 3. Dakle, treba odrediti čemu je 3^{340} kongruentno modulo 3. Iskoristit ćemo činjenicu da je $341 = 11 \cdot 31$.

Kako je $3^5 = 243 \equiv 1 \pmod{11}$, slijedi $3^{340} = (3^5)^{68} \equiv 1 \pmod{11}$.

Prema Malom Fermatovu teoremu, vrijedi $3^{30} \equiv 1 \pmod{31}$ pa je $3^{340} = 3^{11 \cdot 30+10} \equiv 3^{10} \pmod{31}$. Kako je $3^4 = 81 \equiv 19 \pmod{31}$, dobivamo $3^{10} = 3^4 \cdot 3^4 \cdot 3^2 \equiv -1 \pmod{31}$.

Sada se može lako vidjeti da je $3^{340} \not\equiv 1 \pmod{341}$ pa 341 nije pseudoprost u bazi 3. Primijetimo da dobivena kongruencija pokazuje da 341 nije prost.

Prirodno se nameće sljeeće pitanje: ako je prirodan broj n pseudoprost u bazi a za svaki $2 \leq a \leq n$, $(n, a) = 1$, je li tada n prost? Ili obratno ako je prirodan broj n složen, postoji li nužno a takav da je $(n, a) = 1$ i $a^{n-1} \not\equiv 1 \pmod{n}$? Nažalost, odgovor na ovo pitanje je negativan, što pokazuje da se navedenim testom ne mogu s potpunom sigurnošću određivati prosti brojevi (iako se na taj način mogu određivati s velikom vjerojatnošću).

Definicija 2.4.5. Složen prirodan broj n naziva se ***Carmichaelov broj*** ako za sve prirodne brojeve a koji su relativno prosti s n vrijedi $a^{n-1} \equiv 1 \pmod{n}$.

Primijetimo da je složen broj n Carmichaelov ako i samo ako je pseudoprost u svakoj bazi koja je relativno prosta s n.

Primjer 2.4.6. Najmanji Carmichaelov broj je 561. Lako se vidi da je $561 = 3 \cdot 11 \cdot 17$. Neka je a prirodan broj koji je relativno prost s 561. Tada očito a nije djeljiv niti s 3, niti s 11 niti sa 17 pa je $a^{m-1} \equiv 1 \pmod{m}$, za $m \in \{3, 11, 17\}$. Kako je $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$, dobivamo da je $a^{560} \equiv 1 \pmod{m}$, za $m \in \{3, 11, 17\}$, odakle slijedi $a^{560} \equiv 1 \pmod{561}$

Carmichaelovi brojevi pojavljuju se mnogo rjeđe od prostih brojeva i prilično ih je teško konstruirati. Samu egzistenciju takvih brojeva je utvrdio R. D. Carmichael 1912. te pretpostavio da takvih brojeva postoji beskonačno mnogo, što je dokazano tek 1992.

Lema 2.4.7. *Svaki Carmichaelov broj je neparan.*

Dokaz. Zaista, ako je n paran broj veći od 2, tada je $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \pmod{n}$ pa n nije pseudoprost u bazi $n-1$ (dva uzastopna prirodna broja uvijek su relativno prosti). □

No, postoji i vrlo eksplicitna karakterizacija Carmichaelovih brojeva.

Teorem 2.4.8 (Korseltov kriterij)**.** *Prirodan broj n je Carmichaelov ako i samo ako je n kvadratno slobodan te za svaki prost broj p koji dijeli n vrijedi i da $p-1$ dijeli $n-1$.*

Dokaz. Pokažimo samo dovoljnost. Dokaz drugog smjera zainteresirani čitatelj može naći u [8, poglavlje 6].

Neka je $n = p_1 p_2 \cdots p_k$, gdje su $p_1, p_2, \ldots, p_k$ međusobno različiti prosti brojevi te $p_i - 1 \mid n-1$, za sve $i = 1, 2, \ldots, k$. Neka je a prirodan broj koji je relativno prost s n. Tada je a relativno prost i s p_i te slijedi $a^{p_i-1} \equiv 1 \pmod{p_i}$, za $i = 1, 2, \ldots, k$. Kako $p_i - 1$ dijeli $n-1$, možemo pisati $n-1 = m(p_i-1)$, odakle je $a^{n-1} = (a^{p_i-1})^m \equiv 1 \pmod{p_i}$. Prema tome, $a^{n-1} - 1$ je višekratnik svakog p_i pa je i višekratnik od n (primijetimo da smo ovdje iskoristili činjenicu da je n kvadratno slobodan) te je $a^{n-1} \equiv 1 \pmod{n}$, tj. n je Carmichaelov broj. □

Primjer 2.4.9. 1729 i 2821 su Carmichaelovi brojevi jer je $1729 = 7 \cdot 13 \cdot 19$, $2821 = 7 \cdot 13 \cdot 31$ te je 1728 djeljiv sa $6, 12$ i 18, dok je 2820 djeljiv sa $6, 12$ i 30.

3

PRIMJENA KONGRUENCIJA

Temeljna primjena kongruencija, koja je vjerojatno i inicirala nastanak ove snažne metode, nalazi se u rješavanju diofantskih jednadžbi. Jedan od pristupa pri dokazivanju nerješivosti takvih jednadžbi temelji se na promatranju lijeve i desne strane modulo odabrani prirodan broj te pokazivanju nekongruentnosti, slično kako smo vidjeli u primjeru 2.1.12. Na taj se način može spretno suziti manevarski prostor te promatrati samo ostatke pri dijeljenju s određenim brojem, umjesto traganja za rješenjem na čitavom skupu cijelih brojeva.

No, teorija kongruencija nalazi i mnogo širu primjenu nasuprot Hardyjevu mišljenju navedenom na početku prvog poglavlja. Upravo se na toj teoriji temelji i moderna kriptografija, dok neke ideje koje se mogu vezati uz kongruencije potječu i još iz vremena galskih ratova. Time je teorija brojeva, putem kriptografije, zauzela istaknuto mjesto u omogućavanju svakodnevne zaštite sigurnosti podataka.

3.1. Kriteriji djeljivosti

Pogledajmo najprije neke jednostavne primjene kongruencija u određivanju kriterija djeljivosti:

Propozicija 3.1.1. (1) *Prirodan broj je djeljiv s* 3 *ako i samo ako je suma njegovih znamenki djeljiva s* 3.
(2) *Prirodan broj je djeljiv s* 11 *ako i samo ako je alternirajuća suma njegovih znamenki djeljiva s* 11.

Dokaz. (1) Zapišimo prirodan broj n u obliku $n = \overline{a_k a_{k-1} \dots a_1}$, tj. neka je $n = a_1 + 10 \cdot a_2 + \ldots + 10^{k-2} a_{k-1} + 10^{k-1} a_k$, gdje su $a_1, \dots, a_k$ cijeli brojevi, $1 \leq a_k \leq 9$ i $0 \leq a_j \leq 9$ za $j < k$.

Kako je $10 \equiv 1 \pmod 3$, primjenom propozicije 2.1.4 slijedi $10^j \equiv 1 \pmod 3$, za $j \geq 0$. Odatle je $n = a_1 + 10 \cdot a_2 + \ldots + 10^{k-2}a_{k-1} + 10^{k-1}a_k \equiv a_1 + a_2 + \ldots + a_{k-1} + a_k \pmod 3$, odakle dobivamo tvrdnju propozicije.
(2) Slično kao u dokazu prve tvrdnje, iz $10 \equiv -1 \pmod{11}$ dobivamo $10^j \equiv (-1)^j \pmod{11}$, za $j \geq 0$. Sada je $n \equiv a_1 - a_2 + a_3 - a_4 + \ldots + (-1)^{k+1}a_k \pmod{11}$, čime je propozicija dokazana. □

Propozicija 3.1.2. *Prirodan broj* $n = \overline{a_k a_{k-1} \ldots a_1}$ *je djeljiv sa* $7, 11$ *odnosno* 13 *ako i samo ako je alternirajuća suma* $\overline{a_3 a_2 a_1} - \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} - \cdots$ *blokova koji se sastoje od po tri uzastopne znamenke broja* n *djeljiva sa* $7, 11$ *odnosno* 13.

Dokaz. Pokazat ćemo kriterij djeljivosti sa 7, ostali slijede na potpuno isti način. Najprije pokažimo matematičkom indukcijom da je $10^{3i} \equiv (-1)^i \pmod 7$, za svaki nenegativan cijeli broj i. Tvrdnja se može direktno provjeriti za $i = 0$ te za $i = 1$. Pretpostavimo da tvrdnja vrijedi za i te ju dokažimo za $i + 1$:

$$10^{3(i+1)} = 10^3 \cdot 10^{3i} \equiv (-1)(-1)^i \equiv (-1)^{i+1} \pmod 7.$$

Time je tvrdnja dokazana. Sada imamo

$$\begin{aligned} n = a_1 + 10 \cdot a_2 + \ldots + 10^{k-1}a_k &= \sum_{i=0}^{\lfloor \frac{k}{3} \rfloor - 1} \overline{a_{3i+3}a_{3i+2}a_{3i+1}} \cdot 10^{3i} \\ &\equiv \sum_{i=0}^{\lfloor \frac{k}{3} \rfloor - 1} \overline{a_{3i+3}a_{3i+2}a_{3i+1}} \cdot (-1)^i \pmod 7. \end{aligned}$$

Odatle slijedi da je n djeljiv sa 7 ako i samo ako je izraz iz iskaza propozicije djeljiv sa 7.

□

3.2. Označavanje knjiga

Jedna od najstandarnijih primjena kongruencija nalazi se u označavanju knjiga: svaka je knjiga jednoznačno određena tzv. ISBN brojem (*International Standard Book Number*). Do 2007. je kao ISBN broj korišten niz od 10 znamenki $a_1, a_2, \ldots, a_{10}$, npr. 0–387–95587–9. Znamenke $a_1, \ldots, a_{10}$ podijeljene su u 4 skupine, od kojih prva označava gdje je knjiga izdana, druga izdavača, a treća naslov i redni broj izdanja. Posljednja znamenka, a_{10}, naziva se kontrolna znamenka te se određuje iz prethodnih:

$$a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \pmod{11}.$$

U slučaju da je $a_{10} \equiv 10 \pmod{11}$ na posljednje mjesto upisuje se X. Kontrolna znamenka uvedena je kako bi se na efikasan način mogle ispravljati učestale pogreške koje nastaju pri prepisivanju ISBN brojeva: pogreške nastale zamjenom mjesta dviju znamenki ili greškom u prepisivanju jedne znamenke.

Dakle, pretpostavimo da je niz $b_1, b_2, \ldots, b_{10}$ dobiven prepisivanjem ISBN broja $a_1, a_2, \ldots, a_{10}$, pri čemu je točno jedna znamenka a_j pogrešno prepisana (dakle, $a_j \neq b_j$ te $a_i = b_i$, za $i \neq j$). Pokažimo da tada niz $b_1, b_2, \ldots, b_{10}$ ne predstavlja valjan ISBN broj.

Primijetimo da je kongruencija $a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \pmod{11}$ ekvivalentna s $\sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11}$. Odatle je $\sum_{i=1}^{10} i \cdot b_i \equiv \sum_{i=1}^{10} i \cdot b_i - \sum_{i=1}^{10} i \cdot a_i \pmod{11}$. No, time dobivamo kongruenciju $\sum_{i=1}^{10} i \cdot b_i \equiv j(b_j - a_j) \pmod{11}$. Kako je $b_j \neq a_j$, s desne strane prethodne kongruencije ne možemo dobiti nula pa niz $b_1, b_2, \ldots, b_{10}$ ne predstavlja ISBN broj.

Slično se može provjeriti i situacija u kojoj je niz $b_1, b_2, \ldots, b_{10}$ dobiven zamjenom mjesta dviju znamenki valjanog ISBN broja.

Napomenimo kako se od 01.01.2007. za ISBN broj koristi niz od 13 znamenki $a_1, a_2, \ldots, a_{13}$, koje zadovoljavaju kongruenciju

$$a_1+3a_2+a_3+3a_4+a_5+3a_6+a_7+3a_8+a_9+3a_{10}+a_{11}+3a_{12}+a_{13} \equiv 0 \pmod{10}$$

te ovi ISBN brojevi također posjeduju pokazana svojstva.

3.3. Raspored turnira

Spomenimo sada i jednu učestalu primjenu kongruencija u svijetu sporta.

Pretpostavimo da je potrebno konstruirati raspored susreta u turniru koji se sastoji od n igrača te se održava po principu 'svaki sa svakim'. Takav turnir sastoji se od ukupno $n-1$ kola, svaki se igrač sastaje sa svakim drugim točno jednom te bi svaki igrač trebao nastupiti u svakom kolu. Ukoliko je n neparan, tada se u svakom kolu sastaje $\frac{n-1}{2}$ parova te jedan igrač mora biti slobodan. U tom slučaju dodajemo još jednog, fiktivnog igrača i možemo pretpostaviti da je n paran. Naravno, igrač koji se sastaje s fiktivnim igračem zapravo je slobodan u tom kolu.

Zbog jednostavnosti, označimo igrače s $1, 2, \ldots, n$. U k-tom kolu igrači x i y, $1 \leq x, y \leq n-1$, $x \neq y$, igraju međusobno ukoliko je $x + y \equiv k \pmod{n-1}$. Ukoliko je $x + x \equiv k \pmod{n-1}$, tada igrač x igra s igračem n.

Primijetimo najprije da niti jedan igrač neće igrati više nego jednom u istom kolu jer iz $x + y \equiv x + z \pmod{n-1}$ slijedi $y \equiv z \pmod{n-1}$ te $y = z$ zbog $1 \leq y, z \leq n-1$.

Također, u $n-1$ kolu ne dolazi do ponavljanja susreta jer iz $x+y \equiv k \pmod{n-1}$ i $x+y \equiv k' \pmod{n-1}$ slijedi $k = k'$ zbog $1 \leq k, k' \leq n-1$.

U sljedećoj tablici dan je raspored turnira sa 6 igrača.

Tablica 3.1: Turnir sa 6 igrača.

Kolo	Susreti
1	1-5, 2-4, 3-6
2	1-6, 2-5, 3-4
3	1-2, 4-6, 3-5
4	1-3, 2-6, 4-5
5	1-4, 2-3, 5-6

3.4. Linearne diofantske jednadžbe

Neka su $a_1, a_2, \ldots, a_n, b$ cijeli brojevi. Tada se jednadžba oblika

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

naziva ***linearna diofantska jednadžba***. Tu pretpostavljamo da je n prirodan broj te da su svi brojevi $a_1, a_2, \ldots, a_n$ različiti od nule.

Rješivost linearnih diofantskih jednadžbi (u cijelim brojevima) karakterizirana je sljedećim teoremom:

Teorem 3.4.1. *Linearna diofantska jednadžba $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ ima rješenja ako i samo ako $(a_1, a_2, \ldots, a_n) \mid b$. U tom se slučaju svako rješenje može zapisati pomoću $n-1$ cjelobrojnih parametara.*

Dokaz. Neka je $d = (a_1, a_2, \ldots, a_n)$. Ako d ne dijeli b, tada linearna diofantska jednadžba $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ nema rješenja jer je za bilo koje cijele brojeve $x_1, x_2, \ldots, x_n$ lijeva strana djeljiva s d, dok desna nije.

Pretpostavimo sada da d dijeli b. Dijeljenjem polazne jednadžbe s d dobivamo ekvivalentnu jednadžbu

$$a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n = b', \tag{3.1}$$

gdje je $a_i' = \frac{a_i}{d}$ te $b' = \frac{b}{d}$. Očito vrijedi $(a_1', a_2', \ldots, a_n') = 1$.

Dokazat ćemo da ta jednadžba ima rješenja indukcijom po broju varijabli, tj. indukcijom po n.

Ukoliko je $n = 1$, tada jednadžba ima oblik $x_1 = b'$ ili $-x_1 = b'$ te jedinstveno rješenje ne ovisi ni o kakvom parametru.

Neka je sada $n \geq 2$ te pretpostavimo da jednadžba ima rješenja u slučaju da je broj varijabli $n-1$ te da se svako rješenje može zapisati pomoću $n-2$ cjelobrojna parametra. Dokažimo da tvrdnja vrijedi i za n varijabli.

Neka je $d_1 = (a_1', a_2', \ldots, a_{n-1}')$. Tada svako rješenje jednadžbe $a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n = b'$ zadovoljava i kongruenciju $a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n \equiv b' \pmod{d_1}$ koja je ekvivalentna kongruenciji $a_n'x_n \equiv b' \pmod{d_1}$.

Množenjem s $(a_n')^{\varphi(d_1)-1}$ dobivamo $(a_n')^{\varphi(d_1)}x_n \equiv (a_n')^{\varphi(d_1)-1}b' \pmod{d_1}$. Kako su a_n' i d_1 relativno prosti, Eulerov teorem povlači $x_n \equiv c \pmod{d_1}$, gdje je $c = (a_n')^{\varphi(d_1)-1}b'$.

Prema tome, $x_n = c + d_1t_1$, za neki $t_1 \in \mathbb{Z}$. Uvrštavanjem tog izraza u jednadžbu (3.1) dobivamo jednadžbu u $n-1$ varijabli

$$a_1'x_1 + a_2'x_2 + \cdots + a_{n-1}'x_{n-1} = b' - a_n'c - a_n'd_1t_1. \tag{3.2}$$

Pokažimo da d_1 dijeli $b' - a_n'c - a_n'd_1t_1$. U tu je svrhu dovoljno dokazati da d_1 dijeli $b' - a_n'c$, tj. da je $a_n'c \equiv b' \pmod{d_1}$. No, kako je $a_n'c = (a_n')^{\varphi(d_1)}b'$, prethodna kongruencija vrijedi jer su d_1 i a_n' relativno prosti.

Prema tome, možemo podijeliti jednadžbu (3.2) s d_1, čime dobivamo jednadžbu oblika

$$a_1''x_1 + a_2''x_2 + \cdots + a_{n-1}''x_{n-1} = b'', \tag{3.3}$$

pri čemu je $a_i'' = \frac{a_i'}{d_1}$ te $b'' = \frac{b'-a_n'c}{d_1} - a_n't_1$.

Kako je $(a_1'', a_2'', \ldots, a_{n-1}'') = 1$, po pretpostavci indukcije jednadžba (3.3) ima rješenje te svako rješenje te jednadžbe može biti napisano pomoću $n-2$ cjelobrojna parametra. Pridodamo li tome i $x_n = c + d_1t_1$ dobivamo rješenja polazne jednadžbe $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ zapisana u terminima $n-1$ cjelobrojnih parametara. □

Poseban slučaj linearnih diofantskih jednadžbi dan je idućim korolarom.

Korolar 3.4.2. *Neka su a_1, a_2 relativno prosti cijeli brojevi. Ako je uređen par (x_0, y_0) rješenje jednadžbe $a_1x + a_2y = b$, tada su sva rješenja te jednadžbe dana s $x = x_0 + a_2t$, $y = y_0 - a_1t$.*

Primjer 3.4.3. Riješimo linearnu diofantsku jednadžbu

$$3x + 4y + 7z = 8.$$

Očito mora vrijediti $3x + 4y \equiv 1 \pmod{7}$ pa je $3x + 4y = 1 + 7s$, za neki cijeli broj s. Jedno rješenje te jednadžbe je $x = -1 + 5s$, $y = 1 - 2s$. Prema prethodnom korolaru sva su rješenja dana s $x = -1 + 5s + 4t$, $y = 1 - 2s - 3t$, $t \in \mathbb{Z}$.

Uvrštavanjem u polaznu jednadžbu dobivamo $z = 1 - s$. Dakle, sva rješenja polazne jednadžbe dana su s $(x, y, z) = (-1+5s+4t, 1-2s-3t, 1-s)$, $s, t \in \mathbb{Z}$.

3.5. Kriptosustavi

Znanstvena disciplina koja se bavi analiziranjem i pronalaženjem metoda pomoću kojih je poruku moguće poslati u obliku u kojem ju neće moći pročitati nitko osim onih kojima je namijenjena naziva se ***kriptografija*** (od grčki *krypto*, skrivati te *grafo*, pisati). Ta je disciplina u principu prisutna od samog nastanka pisma i pisanih komunikacija, a prvi napredniji oblici pojavljuju se u antičkoj Grčkoj u 5. stoljeću prije Krista.

U samoj osnovi kriptografije nalaze se dvije osobe, ***pošiljatelj*** i ***primatelj*** poruke, koji žele komunicirati sigurnim putem, tj. žele komunicirati na način da neželjene strane ne mogu odgonetnuti sadržaj poruke koju pošiljatelj šalje primatelju.

Naravno, nije moguće spriječiti da poslana poruka ne dospije u ruke neželjene treće strane. Ono što se može spriječiti, barem na nekoj razini, jest da osoba neupućena u način pisanja poruke ne može razumjeti njezin sadržaj.

Poruka koju pošiljatelj želi poslati naziva se ***otvoreni tekst*** koji pošiljatelj prije slanja transformira koristeći unaprijed dogovoreni postupak šifriranja—time se dobiva šifrirani tekst ili ***šifrat***.

I otvoreni tekst i šifrat sastoje se od elemenata određenih, ne nužno jednakih, alfabeta (općenito, skupova simbola koji su elementi teksta poruke). Najčešće se alfabet otvorenog teksta sastoji od slova abecede i znamenki, ponekad i interpunkcijskih znakova, dok se alfabet šifrata često sastoji samo od znamenki kako bi se dodatno otežalo određivanje teksta izvorne poruke.

Šifrirana poruka zatim se šalje primatelju; presiječe li poruku netko treći, on vidi šifrat, no treba osigurati da ne može doći do sadržaja otvorenog teksta.

S druge strane, primatelj je upućen u postupak šifriranja pa dobivenu poruku može ***dešifrirati*** i tako saznati otvoreni tekst.

Strogo formalno, šifra je uređen par dvije funkcije od kojih prva služi za šifriranje, a druga za dešifriranje. Te funkcije često ovise o nekom unaprijed zadanom parametru (***ključu***), poznatom pošiljatelju i primatelju poruke. Ključ je uglavnom jednak nekom odabranom slovu abecede, broju ili nekoj ključnoj riječi.

Neka je za odabrani parametar t šifra koja odgovara tom parametru označena s (f_t, g_t). Ako je x neki element alfabeta otvorenog teksta (npr. proizvoljno

slovo, broj ili simbol), tada je $f_t(x) = y$ neki element alfabeta šifrata (općenito, moguća je i situacija da se niz elemenata alfabeta otvorenog teksta preslika u jedan element alfabeta šifrata, no ograničimo se na gornju situaciju). Nadalje, mora vrijediti $g_t(f_t(x)) = x$, odakle slijedi da je preslikavanje f_t injekcija, a g_t surjekcija. Također, da bi se tekst šifrata mogao dešifrirati na jednoznačno određen način, preslikavanje g_t također mora biti injekcija.

Dakle, kriptosustav se sastoji od:

- alfabeta otvorenog teksta,
- alfabeta šifrata,
- skupa parametara,
- za svaki parametar t, uređenog para funkcija (f_t, g_t) takvih da je $g_t(f_t(x)) = x$ za svaki element x alfabeta otvorenog teksta.

U daljnjem ćemo pretpostavljati da se alfabet otvorenog teksta sastoji od slova engleske abecede te da se alfabet šifrata sastoji od slova engleske abecede i znamenki $0, 1, 2, \ldots, 9$.

Nasuprot samoj kriptografiji nalazi se znanstvena disciplina pod nazivom ***kriptoanaliza*** čiji je zadatak pronaći način za dešifriranje šifrirane poruke.

Primjer 3.5.1. Pomak abecede ili Cezarova šifra.

Podsjetimo kako pretpostavljamo da se alfabet otvorenog teksta koji koristimo sastoji od 26 slova engleske abecede. Svakom slovu možemo pridružiti njegov odgovarajući redni broj umanjen za 1, tj. slovu A odgovara 0, slovu B odgovara $1, \ldots,$ slovu Z odgovara 25.

Ideja te metode (za koju se pretpostavlja da je korištena još od strane Gaja Julija Cezara) jest da se, jednostavno, svakom slovu korištene abecede (gledano kao cijeli broj između 0 i 25) doda (modulo 26) ključni cijeli broj k.

Ukoliko je, recimo $k = 5$, tada iz poruke (otvorenog teksta) *Ne zaboravite postupak* dobivamo šifrat *SJEFGTWFANYJUTYZUFP*.

Primijetimo kako smo ovdje koristili neke sitne detalje koji ipak donekle otežavaju kriptoanalizu šifrata: zapisali smo otvoreni tekst bez razmaka i interpunkcijskih znakova te koristili isključivo velika slova čime se otežava mogućnost pogađanja otvorenog teksta.

Dakle, alfabet otvorenog teksta i alfabet šifrata u ovom su primjeru jednaki te se sastoje od slova engleske abecede, parametri su cijeli brojevi, dok su funkcije koje služe za šifriranje i dešifriranje zbrajanje i oduzimanje s fiksiranim parametrom modulo 26.

No, predstavljena Cezarova šifra je, nažalost, zbog svoje sigurnosti vrlo nezahvalna. Zaista, iako ključni broj (parametar) k može biti bilo koji cijeli broj zapravo postoji samo 26 različitih parametara. Jer, ukoliko su k_1 i k_2 cijeli brojevi koji su međusobno kongruentni modulo 26, tada se pomaci abecede za k_1 i k_2 podudaraju. Zaključujemo kako su svi predstavnici parametara iskazani upravo potpunim sustavom ostataka modulo 26.

Primjer 3.5.2. Neka je primjenom Cezarove šifre dobiven šifrat *QRSKSTS OYWENE*. Odredimo otvoreni tekst (pretpostavljamo da znamo da je napisan na hrvatskom jeziku) i korišteni parametar k.

Primijetimo kako šifrat počinje trima uzastopnim slovima abecede pa trima uzastopnim slovima mora počinjati i otvoreni tekst.

Pokušavajući redom s $k = 0, 1, 2, 3$ dobivamo za početni dio QRS, PQR, OPQ, NOP. Eventualno bi posljednji dio mogao predstavljati početak nekog teksta na hrvatskom jeziku, no tada bi sljedeće slovo u otvorenom tekstu bilo H.

Uzmemo li da je $k = 4$, dobivamo početni dio MNO te, nastavljajući, i otvoreni tekst $MNOGOPOKUSAJA$. Dakle, poslana poruka glasila je 'Mnogo pokušaja', a korišteni parametar k jednak je 4.

Želimo li konstruirati što sigurniji kriptosustav treba paziti da upravo skup parametara bude što opsežniji jer se u primjerima poput prethodnog kriptoanaliza može provesti direktnim ispitivanjem svih mogućnosti.

Primjer 3.5.3. Jednokratni uzorak.

Sada ćemo predstaviti daleko sigurniji način šifriranja (pod tim, naravno, smatramo da je kriptoanaliza kompliciranija). Neka je $a_1a_2a_3\ldots$ vrlo dug slučajan niz prirodnih brojeva od kojih je svaki manji ili jednak 26. Pod pojmom „vrlo dugi" niz smatramo da broj elemenata u tom nizu prelazi broj znakova korištenih u otvorenom tekstu.

Šifriranje se vrši na sljedeći način: i-to slovo šifrata dobivamo dodajući modulo 26 broj a_i i-tom slovu otvorenog teksta.

Ukoliko je niz $a_1a_2a_3\ldots$ dan s $a_i = (i \bmod 26)+1$, tada iz otvorenog teksta *Ne zaboravite postupak* dobivamo šifrat *OGCEGUYIESEQCCHJLHTE*.

Kada je početni dio niza $a_1a_2\ldots a_n$ iskorišten taj se dio odbacuje, a ostatak $a_{n+1}a_{n+2}\ldots$ koristi za šifriranje sljedećeg otvorenog teksta.

Kako su svi slučajni nizovi $a_1a_2\ldots$ opisanog tipa vrlo slični, slični su i dobiveni šifrati, te je šifriranje korištenjem jednokratnih uzoraka potpuno sigurno. Osim toga, u tom slučaju raspolažemo s golemim brojem parametara koje možemo koristiti.

No, kako korišteni ključni niz mora biti vrlo dugačak i kako svaki njegov dio možemo koristiti najviše jednom, opisani postupak šifriranja u praksi se pokazuje krajnje neprimjenjiv.

Osnovni je cilj kriptografije pronaći način šifriranja koji je kombinacija onih opisanih u prethodnim primjerima: uspješno iskombinirati jednostavnost korištenja Cezarove šifre sa sigurnošću šifriranja korištenjem jednokratnih uzoraka.

Opisani primjeri pripadaju među tzv. ***simetrične šifre*** u kojima su postupak šifriranja i dešifriranja esencijalno jednaki (kakvi zbrajanje i oduzimanje modulo 26 zaista jesu). Također, navedeni postupci pripadaju među kriptosustave s ***tajnim ključem***, jer su parametri korišteni pri šifriranju (ključni broj k i niz $a_1a_2a_3\ldots$) poznati samo pošiljatelju i primatelju poruke.

U praksi se najkorisnijim pokazuju kriptosustavi u kojima se šifriranje može lako provesti, dok je dešifriranje gotovo neizvedivo bez poznavanja nekih dodatnih podataka (dakle, šifre (f_t, g_t) takve su da se $f_t(x)$ može lako izračunati, dok je vrijednost $g_t(y)$ neupućenima gotovo nemoguće izračunati).

Takvi kriptosustavi očito nisu simetrični te pripadaju među ***asimetrične šifre***.

U takvim situacijama neki od podataka (naravno, ne i oni ključni za dešifriranje) mogu biti poznati svima, a ne samo pošiljatelju i primatelju poruke. Tada govorimo o kriptosustavima s ***javnim ključem***.

Osnovni primjer asimetrije možemo vidjeti u činjenici da je dane proste brojeve lako pomnožiti, bez obzira na njihov broj znamenki, no dani složen broj često je vrlo komplicirano prikazati u obliku produkta prostih faktora (bez poznavanja npr. nekog od faktora).

Primjer 3.5.4. Brojevi 11399 i 105929 su prosti. Njihov produkt jednak je 1207484671. No, prilično je težak zadatak prikazati prethodni broj u obliku produkta prostih brojeva, bez poznavanja barem jednog od njih.

Upravo ćemo taj princip iskoristiti u sljedećem potpoglavlju.

3.6. RSA kriptosustav

RSA kriptosustav nastao je 1977. i nazvan je prema inicijalima trojice njegovih tvoraca, matematičarima Ronu Rivestu, Adiu Shamiru i Lenu Adlemanu.

Osnovne sastavnice RSA kriptosustava su multiplikativni inverzi modulo neki prirodan broj koje smo opisali prije Wilsonova teorema te Eulerov teorem.

Alfabet otvorenog teksta ponovno se sastoji od slova engleske abecede, no čitav postupak šifriranja i dešifriranja obavlja se nad cijelim brojevima te možemo smatrati kako se od njih sastoji i polazni alfabet (štoviše, dovoljno je uzeti da je sastavljen od prirodnih brojeva). Opišimo sada postupak šifriranja.

Neka su p_1 i p_2 prosti brojevi, po mogućnosti što veći. Označimo njihov produkt s n.

Prema potpoglavlju 2.2 znamo da je $\varphi(n) = (p_1 - 1) \cdot (p_2 - 1)$.

Nadalje, korisnik odabire i tzv. enkripcijski eksponent e koji može biti bilo koji prirodan broj koji je relativno prost s $\varphi(n)$.

Kako su e i $\varphi(n)$ relativno prosti, slijedi da postoji multiplikativni inverz d od e modulo $\varphi(n)$, tj. $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

Multiplikativni inverz d može se odrediti iz Euklidova algoritma jer ima svojstvo da postoji neki cijeli broj c za koji je $ed + c\varphi(n) = 1$. Broj d naziva se dekripcijski eksponent.

Neka je sada x dio otvorenog teksta koji treba šifrirati, gdje uzimamo da je x strogo manji od n. Tada se odgovarajući dio šifrata dobiva pomoću $f_t(x) = x^e \bmod n$, gdje je t parametar $t = (n, e)$.

Ako je y dio šifrata, dekripcija se obavlja pomoću $g_t(y) = y^d \bmod n$, gdje je ponovo $t = (n, e)$.

Parametar (n, e) smatra se javnim i može biti svima poznat. Također se naziva i javni ključ. Faktorizacija $n = p_1 \cdot p_2$ i podatak d smatraju se tajnim, poznati su samo pošiljatelju i primatelju poruke.

Uvjerimo se najprije da su tako definirane funkcije zaista jedna drugoj inverzne na skupu prirodnih brojeva:

Teorem 3.6.1. *Za $1 \leq x < n$ vrijedi $g_t(f_t(x)) = x$, gdje je $t = (n, e)$, uz uvjet $(e, \varphi(n)) = 1$.*

Dokaz. Očito je $g_t(f_t(x)) = x^{ed} \pmod{n}$.

Kako je d multiplikativni inverz od e modulo $\varphi(n)$, imamo $ed \equiv 1 \pmod{\varphi(n)}$, odakle slijedi da postoji $a \in \mathbb{N}$ takav da je $ed = a \cdot \varphi(n) + 1$. Odatle je $x^{ed} = x \cdot (x^{\varphi(n)})^a$.

Razlikujemo nekoliko mogućnosti:

- $(n, x) = 1$: sada je $x^{\varphi(n)} \equiv 1 \pmod{n}$ pa je $x^{ed} \equiv x \pmod{n}$;
- $(n, x) = p_1$: u ovom slučaju je $x^{ed} \equiv 0 \pmod{p_1}$ i $x^{ed} \equiv x \cdot (x^{p_2 - 1})^{(p_1 - 1)a} \equiv x \pmod{p_2}$ zbog $(x, p_2) = 1$, što slijedi iz činjenica da je $x < n$ i $p_1 \mid x$. Iz dobivenog sustava kongruencija se lako vidi, slično kao u dokazu leme 2.2.6, da je $x^{ed} \equiv x \pmod{n}$;

- $(n, x) = p_2$: na isti način kao u prethodnom slučaju zaključujemo da je $x^{ed} \equiv x \pmod{n}$.

Iz dobivene kongruencije slijedi da je $x = x^{ed} \bmod n$, jer je $x < n$. Dakle, funkcije su međusobno inverzne. □

Primjer 3.6.2. Pokažimo na primjeru da korištenjem RSA kriptosustava možemo šifrirati poruku TB.

Najprije prikažimo otvoreni tekst u obliku niza prirodnih brojeva uzimajući pozicije slova u abecedi. Time dobivamo 202.

Nadalje, odaberimo proste brojeve p_1 i p_2: neka je $p_1 = 7$ i $p_2 = 11$. Sada je $n = 77$ i $\varphi(n) = 60$. Enkripcijski eksponent e mora biti relativno prost sa 60 pa uzmimo da je $e = 13$. Direktno ili primjenom Euklidova algoritma dobivamo da je $d = 37$.

Otvoreni tekst rastavljamo na dva dijela od kojih ćemo svaki šifrirati zasebno, kako bi bili manji od 77. Između opcija 2, 2 i 20, 2 odabiremo drugu.

Prema tome, najprije je $x = 20$, te treba odrediti $20^{13} \bmod 77$. U tu se svrhu koristimo sljedećim nizom kongruencija:

$$\begin{aligned} 20^1 &\equiv 20 \pmod{77} \\ 20^2 &\equiv 15 \pmod{77} \\ 20^4 &\equiv 71 \pmod{77} \\ 20^8 &\equiv 36 \pmod{77}. \end{aligned}$$

Odatle je $20^{13} \equiv 20^8 \cdot 20^4 \cdot 20 \equiv 36 \cdot 71 \cdot 20 \equiv 69 \pmod{77}$.

U sljedećem je koraku $x = 2$ pa imamo $2^{13} \equiv 2^8 \cdot 2^4 \cdot 2 \equiv 256 \cdot 16 \cdot 2 \equiv 30 \pmod{77}$.

Prema tome, šifrat je jednak 69 30.

Naravno, dešifriranjem bimo dobili polazni otvoreni tekst 20 2.

Primijetimo kako je ključan dodatni podatak koji omogućuje dešifriranje uz poznavanje javnog ključa (n, e) upravo faktorizacija $n = p_1 \cdot p_2$, iz koje se lako može odrediti $\varphi(n)$, a zatim i dekripcijski eksponent d. Zapravo, kako je za dešifriranje dovoljno poznavati eksponent d, u postupku dešifriranja ključnu ulogu igra poznavanje parametra $\varphi(n)$.

Prilikom korištenja RSA kriptosustava računski najkompliciraniji koraci su određivanje izraza x^e i y^d modulo n. Kako ovaj kriptosustav često koristi eksponente s više od stotinu znamenki, prethodni izrazi mogu poprimiti vrijednosti koje su krajnje nepogodne za računanje.

No, primijetimo da nama zapravo nisu potrebni prirodni brojevi x^e i i y^d već samo njihovi ostatci pri dijeljenju s n. Računanje ostataka pri dijeljenju koje daju kvadrati je standardno najlakše izvediv zadatak od svih potencija pa se računski koraci obično odvijaju na način prikazan u prethodnom primjeru. Osnovni korak je prikazati eksponent u obliku sume potencija broja 2 te iskoristiti dobivene ostatke u odgovarajućoj kongruenciji.

Primjer 3.6.3. Digitalni potpis

RSA kriptosustav također se koristi prilikom prenošenja digitalnog potpisa kojim se dokazuje kako je korisnik uistinu onaj za kojeg se predstavlja. U tu svrhu, korisnik je dužan pokazati kako posjeduje podatke kojima nitko drugi ne bi trebao raspolagati, poput nekog osobnog koda, zaporke ili dekripcijskog eksponenta d koji dolazi uz javni ključ (n, e).

Jasno, korisnikova ideja ne leži u tome da otkrije eksponent d čime inkriminira sigurnost poslanih šifrata već da, na neki način, samo pokaže poznavanje tog podatka.

U tu svrhu, korisnik uzima neku poznatu poruku x (npr. svoje ime) te šalje $x^d \bmod n$, šifriranu poruku koju je mogao poslati samo poznavatelj eksponenta d. Kako je podatak (n, e) javni, svatko je u mogućnosti odrediti x uzimajući e-tu potenciju od $x^d \bmod n$ jer vrijedi $(x^d)^e = x^{ed} \equiv x (\bmod\ n)$.

Na taj se način svatko može uvjeriti da korisnik posjeduje tajni eksponent d te time i uvjeriti u korisnikov identitet.

4

KVADRATNI OSTATCI

U ovom poglavlju bavimo se općenitim pitanjem posjeduje li cijeli broj a kvadratni korijen modulo n te, ukoliko posjeduje, koliko je takvih te kako ih odrediti. Jedna od osnovnih primjena nalazi se u rješavanju kvadratnih kongruencija, no također se pojavljuje i pri prikazu prirodnih brojeva u obliku $x^2 + dy^2$, gdje je $d \in \mathbb{N}$. Upravo je Fermat započeo istraživanje mogućnosti prikaza prostih brojeva u obliku x^2+y^2, x^2+2y^2 te x^2+3y^2, pri čemu je primijetio važnost tzv. kvadratnog zakona reciprociteta. Taj je rezultat, koji se smatra najdražim Gaussovim teoremom (dokazao ga je na ukupno 8 načina), prvi dokazao Dirichlet, 1837.

4.1. Legendreov simbol

Neka su a i n relativno prosti prirodni brojevi. Ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, tada kažemo da je a ***kvadratni ostatak*** modulo n. U suprotnom, kažemo da je a ***kvadratni neostatak*** modulo n.

Primjer 4.1.1. Prirodni brojevi 1, 2 i 4 su kvadratni ostatci modulo 7, a brojevi 3, 5 i 6 su kvadratni neostatci modulo 7.

Neka je p neparan prost broj i a cijeli broj. ***Legendreov simbol*** $\left(\frac{a}{p}\right)$ definiran je s

$$\left(\frac{a}{p}\right) = \begin{cases} 1\,, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ 0\,, & \text{ako } p \mid a, \\ -1\,, & \text{ako je } a \text{ kvadratni neostatak modulo } p. \end{cases}$$

Kombinirajući prethodni primjer s definicijom Legendreova simbola dobivamo $(\frac{1}{7}) = (\frac{2}{7}) = 1$, $(\frac{3}{7}) = (\frac{6}{7}) = -1$ te $(\frac{14}{7}) = 0$. Primijetimo da vrijedi i $(\frac{1}{p}) = 1$ te $(\frac{a^2}{p}) = 1$, ako p ne dijeli a i $(\frac{a^2}{p}) = 0$, ako p dijeli a.

Podsjetimo se da, u slučaju da su a i p relativno prosti brojevi i p neparan prost, vrijedi $a^{p-1} \equiv 1 \pmod{p}$ (prema korolaru 2.2.4). Euler je iskoristio tu relaciju kako bi dobio sljedeću formulu za određivanje Legendreova simbola:

Teorem 4.1.2 (Eulerov kriterij)**.** *Ako je p neparan prost broj, tada vrijedi $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Prema tome, a je kvadratni ostatak modulo p ako i samo ako je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Dokaz. Očito iz $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$ slijedi $p \mid a^{\frac{p-1}{2}}$. Prema lemi 1.4.2, slijedi da je $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$ ako i samo ako $p \mid a$, tj. ako i samo ako je $(\frac{a}{p}) = 0$. Dakle, u tom je slučaju tvrdnja dokazana. Nadalje, možemo uzeti da su a i p relativno prosti.

Pretpostavimo da je a kvadratni ostatak modulo p. Tada je $a \equiv b^2 \pmod{p}$, za neki b te, $(\frac{a}{p}) = 1$, po definiciji Legendreova simbola. Kako su a i p relativno prosti, slijedi da su i b i p relativno prosti. Time, koristeći Mali Fermatov teorem, dobivamo $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$.

Preostaje još provjeriti formulu iz iskaza teorema u slučaju da je a kvadratni neostatak modulo p. Primijetimo da vrijedi $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$.

No, kako kongruencija $x^2 \equiv 1 \pmod{p}$ ima točno dva rješenja, $x \equiv \pm 1 \pmod{p}$ (prema teoremu 2.3.5 znamo da su ovo jedina rješenja), dovoljno je dokazati da $a^{\frac{p-1}{2}}$ nije kongruentno 1 modulo p kada je a kvadratni neostatak modulo p (jer će iz toga slijediti da mora biti kongruentno -1 modulo p).

Prema istom teoremu, kongruencija $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ima najviše $\frac{p-1}{2}$ rješenja, među kojima se moraju nalaziti $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ jer se, prema već dokazanom, među rješenjima nalaze svi kvadratni ostatci modulo p. Pokažimo da su sva ova rješenja međusobno različita, tj. nekongruentna modulo p.

Ako su x^2, y^2 takvi da je $x^2 \equiv y^2 \pmod{p}$, tada slijedi da ili $p \mid x - y$ ili $p \mid x + y$. Kako je $1 < x + y < p$, dobivamo $x = y$. Dakle, sva rješenja kongruencije $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ dana su navedenim nizom koji uključuje samo kvadratne ostatke modulo p.

Prema tome, ako je a kvadratni neostatak modulo p, tj. $(\frac{a}{p}) = -1$, slijedi $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Direktno iz prethodnog teorema možemo zaključiti da, ukoliko je $a \equiv b \pmod{p}$, vrijedi i $(\frac{a}{p}) = (\frac{b}{p})$. Također vrijedi i tzv. 'pola-pola' svojstvo:

Korolar 4.1.3. *Ako je p neparan prost broj, tada su točno polovica brojeva $1, 2, \ldots, p-1$ kvadratni ostatci modulo p.*

Dokaz. U dokazu prethodnog teorema vidjeli smo kako su $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ kvadratni ostatci modulo p. Pokažimo da je svaki kvadratni ostatak modulo p kongruentan modulo p nekom od brojeva iz prethodnog niza.

Ako je neki $1 \leq a \leq p-1$ kvadratni ostatak modulo p, tada postoji x takav da je $x^2 \equiv a \pmod{p}$. Možemo uzeti da je $1 \leq x \leq p-1$ jer rješenja tražimo u reduciranom sustavu ostataka modulo p.

Ako je $x \leq \frac{p-1}{2}$, tada se x^2 nalazi u prethodnom nizu. Ako je $\frac{p-1}{2} < x$, tada je $x^2 \equiv (p-x)^2 \pmod{p}$ te zbog $p - x < \frac{p-1}{2}$ slijedi da je x^2 kongruentno nekom od brojeva $1^2, 2^2, \ldots, (\frac{p-3}{2})^2$ modulo p.

Time smo dokazali da u nizu $1, 2, \ldots, p-1$ postoji točno $\frac{p-1}{2}$ kvadratnih ostataka modulo p koje čine oni članovi koji su kongruentni s $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ modulo p.

□

Pokažimo još nekoliko svojstava Legendreovih simbola koja su vrlo korisna pri njihovu eksplicitnom određivanju.

Propozicija 4.1.4. *Za svaka dva cijela broja a_1 i a_2 te neparan prost broj p vrijedi $(\frac{a_1 a_2}{p}) = (\frac{a_1}{p})(\frac{a_2}{p})$.*

Dokaz. Korištenjem Eulerova kriterija dobivamo
$(\frac{a_1}{p})(\frac{a_2}{p}) \equiv (a_1)^{\frac{p-1}{2}}(a_2)^{\frac{p-1}{2}} \equiv (a_1 a_2)^{\frac{p-1}{2}} \equiv (\frac{a_1 a_2}{p}) \pmod{p}$ pa, kako je Legendreov simbol jednak $0, 1$ ili -1, slijedi jednakost. □

Osim prethodnog svojstva multiplikativnosti, prilikom računanja često je od velike pomoći znati direktno odrediti neke Legendreove simbole.

Primjer 4.1.5. Odredimo $(\frac{-8}{3})$.

Prema prethodnoj propoziciji je $(\frac{-8}{3}) = (\frac{4}{3})(\frac{2}{3})(\frac{-1}{3}) = (\frac{1}{3})(\frac{2}{3})(\frac{-1}{3}) = (\frac{2}{3})(\frac{-1}{3})$. Ostatak računa možemo provesti direktno preko Eulerova kriterija, no direktniji način za određivanje Legendreovih simbola tog oblika opisat ćemo u ostatku ovog potpoglavlja.

Propozicija 4.1.6. *Za neparan prost broj p vrijedi*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1\,, & \text{ako je } p \equiv 1 \pmod{4}, \\ -1\,, & \text{ako je } p \equiv 3 \pmod{4}. \end{cases}$$

Drugim riječima, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Dokaz. Prema Eulerovu kriteriju je $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.
Ako je $p \equiv 1 \pmod 4$, tada je broj $\frac{p-1}{2}$ paran pa je $(\frac{-1}{p}) = 1$.
Ako je $p \equiv 3 \pmod 4$, tada je broj $\frac{p-1}{2}$ neparan pa je $(\frac{-1}{p}) = -1$. □

Propozicija 4.1.7. *Za neparan prost broj p vrijedi*

$$\left(\frac{2}{p}\right) = \begin{cases} 1\,, & \text{ako je } p \equiv 1 \pmod 8 \text{ ili } p \equiv 7 \pmod 8, \\ -1\,, & \text{ako je } p \equiv 3 \pmod 8 \text{ ili } p \equiv 5 \pmod 8. \end{cases}$$

Dokaz. Opet, prema Eulerovu kriteriju je $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \pmod{p}$, no s izrazom $2^{\frac{p-1}{2}}$ mnogo je teže manipulirati nego s izrazom $(-1)^{\frac{p-1}{2}}$ u prethodnoj propoziciji.

Najprije ćemo dokazati sljedeće kongruencije:

$$2^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{p-1}{4}} \pmod p\,, & \text{ako je } p = 4n+1, \\ (-1)^{\frac{p+1}{4}} \pmod p\,, & \text{ako je } p = 4n+3. \end{cases}$$

Ako je $p = 4n+1$, tj. $p \equiv 1 \pmod 4$, redom imamo

$$\begin{aligned}
(4n)! &\equiv (1 \cdot 3 \cdots (4n-1))(2 \cdot 4 \cdots 4n) \pmod p \\
&\equiv (1 \cdot 3 \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \pmod p \\
&\equiv (1 \cdot 3 \cdots (2n-1))((2n+1)(2n+3) \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \pmod p \\
&\equiv ((-1)(-3) \cdots (-2n+1))(-1)^n((2n+1)(2n+3) \cdots (4n-1)) \cdot \\
&\qquad \cdot (1 \cdot 2 \cdots 2n)2^{2n} \pmod p \\
&\equiv (4n(4n-2) \cdots (2n+2))(-1)^n((2n+1)(2n+3) \cdots (4n-1)) \cdot \\
&\qquad \cdot (1 \cdot 2 \cdots 2n)2^{2n} \pmod p \\
&\equiv (-1)^n 2^{2n}(4n)! \pmod p.
\end{aligned}$$

Kako je $p > 4n$, slijedi $(p, (4n)!) = 1$ te iz prethodnog izraza dobivamo $1 \equiv (-1)^n 2^{2n} \equiv (-1)^{\frac{p-1}{4}} 2^{\frac{p-1}{2}} \pmod p$.

Odatle slijedi $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod p$, za $p \equiv 1 \pmod 4$.

Na potpuno analogan način dobiva se i da je $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod p$, za $p \equiv 3 \pmod 4$.

Sada zasebno razmatramo sve mogućnosti:

- $p \equiv 1 \pmod 8$: u ovom slučaju je $p \equiv 1 \pmod 4$ i $\frac{p-1}{4}$ je paran broj pa je $2^{\frac{p-1}{2}} \equiv 1 \pmod p$,
- $p \equiv 3 \pmod 8$: sada je $p \equiv 3 \pmod 4$ i $\frac{p+1}{4}$ je neparan pa je $2^{\frac{p-1}{2}} \equiv -1 \pmod p$,

- $p \equiv 5 \pmod 8$: sada imamo $p \equiv 1 \pmod 4$ i $\frac{p-1}{4}$ je neparan broj pa je $2^{\frac{p-1}{2}} \equiv -1 \pmod p$,
- $p \equiv 7 \pmod 8$: napokon, $p \equiv 3 \pmod 4$ i $\frac{p+1}{4}$ je paran pa je $2^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Iz promatranih slučajeva direktno slijedi tvrdnja propozicije. □

Prethodnu smo propoziciju mogli iskazati i u ekvivalentnom obliku $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Kako raspolažemo rezultatima iz prethodnih dviju propozicija, uvrštavanjem dobivamo $(\frac{2}{3}) = -1$ i $(\frac{-1}{3}) = -1$. Dakle, $(\frac{-8}{3}) = 1$.

4.2. Kvadratni zakon reciprociteta

Iako smo pokazali nekoliko rezultata pomoću kojih se mogu odrediti Legendreovi simboli, eksplicitno izračunavanje tih simbola i dalje ostaje kompliciran postupak, osobito ako su uključeni veći brojevi. Naprimjer, s kompliciranim postupkom susrećemo se već i prilikom ispitivanja je li 67 kvadratni ostatak modulo 151. Najveći korak prema pojednostavljenju tog postupka je dan upravo kvadratnim zakonom reciprociteta, dubokim rezultatom do kojeg je došao još Gauss. Jednako kao što se Pitagorin teorem može smatrati temeljnim rezultatom u geometriji, kvadratni se zakon reciprociteta danas može smatrati ključnim teoremom u teoriji brojeva koji se pojavljuje kad god se proučavaju kvadratne diofantske jednadžbe. Upravo je iz tog razloga do danas konstruirano mnogo bitno različitih dokaza kvadratnog zakona reciprociteta (do 2000. bilo ih je poznato ukupno 196).

Na ovom mjestu izvest ćemo dokaz kvadratnog zakona reciprociteta koji se temelji na množenju elemenata koji posjeduju multiplikativni inverz modulo produkt dva različita prosta broja. U tome će osnovni korak predstavljati sljedeći tehnički rezultat:

Lema 4.2.1. *Neka su p i q međusobno različiti prosti brojevi. Tada je*

$$\prod_{\substack{1 \le x \le \frac{pq-1}{2} \\ x \text{ invertibilan modulo } pq}} x \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p$$

i

$$\prod_{\substack{1 \le x \le \frac{pq-1}{2} \\ x \text{ invertibilan modulo } pq}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q.$$

Dokaz. Promotrimo invertibilne elemente modulo pq, što su upravo oni elementi koji nisu djeljivi niti s p niti s q. Skup invertibilnih elementa x koji se nalaze u $\{1, 2, \ldots, \frac{pq-1}{2}\}$, promatran modulo p sastoji se od $\frac{q-1}{2}$ nizova $1, 2, \ldots, p-1$ te niza $1, 2, \ldots, \frac{p-1}{2}$, gdje još treba isključiti niz $q, 2q, \ldots, \frac{p-1}{2}q$ koji se sastoji od višekratnika broja q. Na taj način dobivamo

$$\prod_{\substack{1\le x\le \frac{pq-1}{2}\\ x \text{ invertibilan modulo } pq}} x \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \Big/ q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$$

$$\equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p$$

jer se $(\frac{p-1}{2})!$ pokrati, $(p-1)! \equiv -1 \pmod p$, prema Wilsonovu teoremu te $q^{\frac{p-1}{2}} \equiv (\frac{q}{p}) \pmod p$, prema Eulerovu kriteriju.

Na isti način dobivamo i

$$\prod_{\substack{1\le x\le \frac{pq-1}{2}\\ x \text{ invertibilan modulo } pq}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q,$$

čime je lema dokazana. □

Teorem 4.2.2 (Kvadratni zakon reciprociteta)**.** *Neka su p i q različiti neparni prosti brojevi. Tada vrijedi*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Dokaz. Kako bi dokazali taj važan rezultat, produkte

$$\prod_{\substack{1\le x\le \frac{pq-1}{2}\\ x \text{ invertibilan modulo } pq}} x \pmod p \quad \text{i} \quad \prod_{\substack{1\le x\le \frac{pq-1}{2}\\ x \text{ invertibilan modulo } pq}} x \pmod q$$

iz prethodne leme izrazit ćemo isključivo pomoću potencija od -1.

Primijetimo da se za svaki $x \in \{1, 2, \ldots, pq-1\}$ točno jedan element skupa $\{x, -x\} \pmod{pq}$ pojavljuje u nizu $1, 2, \ldots, \frac{pq-1}{2}$. Prema tome, među odgovarajućim uređenim parovima ostataka $(a, b) = (x \bmod p, x \bmod q)$ pojavljuje se točno jedan od parova $(a, b), (-a, -b)$. Točno po jedan od svakog mogućeg para ostataka $(\bmod p, \bmod q)$ dobivamo uzimajući $1 \le a \le p-1$ i $1 \le b \le \frac{q-1}{2}$. Na taj način dobivamo

$$\prod_{\substack{1\le x\le \frac{pq-1}{2}\\ x \text{ invertibilan modulo } pq}} (x, x) \equiv \pm\big((p-1)!^{\frac{q-1}{2}}, ((q-1)/2)!^{p-1}\big) (\bmod p, \bmod q) \quad (4.1)$$

jer se svaki $a \in \{1, 2, \ldots, p-1\}$ pojavljuje u točno $\frac{q-1}{2}$ parova, dok se svaki $b \in \{1, 2, \ldots, \frac{q-1}{2}\}$ pojavljuje u točno $p-1$ parova.

Pomoću Wilsonova teorema prikazat ćemo potencije faktorijela koje se pojavljuju u (4.1) kao potencije od -1. Kako je $(p-1)! \equiv -1 \pmod{p}$, prva komponenta je kongruentna $(-1)^{\frac{q-1}{2}}$ modulo p. Kako bi prikazali i drugu komponentu u obliku potencije od -1, primijetimo da vrijedi

$$\begin{aligned} -1 &\equiv (q-1)! \pmod{q} \\ &\equiv 1 \cdot 2 \cdots (q-1)/2 \cdot (-(q-1)/2) \cdots (-2) \cdot (-1) \pmod{q} \\ &\equiv ((q-1)/2)!^{\,2} (-1)^{\frac{q-1}{2}} \pmod{q}. \end{aligned}$$

Prema tome je

$$((q-1)/2)!^{\,2} \equiv (-1)(-1)^{\frac{q-1}{2}} \pmod{q}.$$

Potenciranjem dobivamo

$$((q-1)/2)!^{\,p-1} \equiv (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \pmod{q}$$

te kongruencija (4.1) prelazi u

$$\prod_{\substack{1 \le x \le \frac{pq-1}{2} \\ x \text{ invertibilan modulo } pq}} (x, x) \equiv \pm\left((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\right) (\text{mod } p, \text{mod } q). \tag{4.2}$$

Izjednačavanjem kongruencije (4.2) i rezultata iz leme 4.2.1 dobivamo da vrijedi jedno od sljedećeg:

- $\left(\frac{q}{p}\right) = 1$ i $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$,
- $\left(\frac{q}{p}\right) = -1$ i $\left(\frac{p}{q}\right) = -(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$,

iz čega slijedi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

Primjer 4.2.3. Odredimo $\left(\frac{67}{151}\right)$.

Primjenom kvadratnog zakona reciprociteta dobivamo

$$\left(\frac{67}{151}\right) = -\left(\frac{151}{67}\right) = -\left(\frac{17}{67}\right) = -\left(\frac{67}{17}\right) = -\left(\frac{16}{17}\right) = -1.$$

Pokažimo i još jednu primjenu kvadratnog zakona reciprociteta. Podsjetimo se kako smo u prvom poglavlju definirali n-ti Fermatov broj F_n s $F_n = 2^{2^n} + 1$. Sljedećim rezultatom dan je efikasan kriterij za ispitivanje prostosti Fermatovih brojeva.

Propozicija 4.2.4. *Fermatov broj F_n je prost ako i samo ako vrijedi*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Dokaz. Pokažimo samo nužnost. Dakle, neka je F_n prost.

Po Eulerovu kriteriju vrijedi $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$.

Prema tome, dovoljno je dokazati da je 3 kvadratni neostatak modulo F_n. Kako je $F_n - 1$ djeljiv s 4, kvadratni zakon reciprociteta povlači $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$.

Nadalje je $F_n \equiv (-1)^{2^n} + 1 \pmod 3$, tj. $F_n \equiv 2 \pmod 3$ pa je $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Dakle, 3 je kvadratni neostatak modulo F_n. □

4.3. Jacobijev simbol

Jacobijev simbol izravna je generalizacija Legendreova simbola. Neka je P neparan prirodan broj te zapišimo P u obliku $P = p_1 p_2 \cdots p_n$, gdje su $p_1, p_2, \ldots, p_n$ prosti brojevi, koji su nužno neparni. Jacobijev simbol $\left(\frac{a}{P}\right)$ definiran je s $\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_n}\right)$, gdje je $\left(\frac{a}{p_i}\right)$ Legendreov simbol.

Ako je P prost, tada se Jacobijev i Legendreov simbol podudaraju. Ako a i P nisu relativno prosti, tada je $\left(\frac{a}{P}\right) = 0$, inače je jednako 1 ili -1.

Nedostatak Jacobijeva simbola nalazi se u tome što $\left(\frac{a}{P}\right) = 1$ ne znači da je a kvadratni ostatak modulo P, što se može vidjeti iz primjera $\left(\frac{2}{15}\right) = 1$, no jednadžba $x^2 \equiv 2 \pmod{15}$ nema rješenja. Štoviše, a je kvadratni ostatak modulo P ako i samo ako je a kvadratni ostatak modulo p_i, za sve $1 \leq i \leq n$.

Izravno se iz dokazanih svojstava Legendreova simbola dobivaju i analogna svojstva Jacobijeva simbola:

Propozicija 4.3.1. *Neka su a i b cijeli brojevi te P_1 i P_2 neparni prirodni brojevi. Tada vrijedi:*
(1) $\left(\frac{a}{P_1P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$,
(2) $\left(\frac{ab}{P_1}\right) = \left(\frac{a}{P_1}\right)\left(\frac{b}{P_1}\right)$,
(3) *ako je* $a \equiv b \pmod{P_1}$, *tada vrijedi* $\left(\frac{a}{P_1}\right) = \left(\frac{b}{P_1}\right)$,
(4) *ako je* $(a, P_1) = 1$, *tada vrijedi* $\left(\frac{a^2}{P_1}\right) = \left(\frac{a}{P_1^2}\right) = 1$,

(5) $\left(\frac{-1}{P_1}\right) = (-1)^{\frac{P_1-1}{2}}$, $\left(\frac{2}{P_1}\right) = (-1)^{\frac{P_1^2-1}{8}}$,
(6) *ako je* $(P_1, P_2) = 1$, *tada vrijedi* $\left(\frac{P_1}{P_2}\right)\left(\frac{P_2}{P_1}\right) = (-1)^{\frac{P_1-1}{2}\cdot\frac{P_2-1}{2}}$.

Dokaz. Prokomentirajmo samo svojstvo (5): očito je $\left(\frac{-1}{P_1}\right) = (-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}}$, gdje je $P_1 = p_1p_2\cdots p_n$, p_i neparan prost za $i = 1, 2, \ldots, n$.

Za neparne brojeve a, b vrijedi $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$ jer je $\frac{ab-1}{2} - \frac{a-1}{2} - \frac{b-1}{2} = \frac{(a-1)(b-1)}{2}$, što je paran broj.

Induktivno slijedi $\sum_{i=1}^{n}\frac{p_i-1}{2} \equiv \frac{p_1p_2\cdots p_n-1}{2} = \frac{P_1-1}{2} \pmod 2$. □

4.4. Primjena kvadratnih ostataka na diofantske jednadžbe

U ovom kratkom potpoglavlju prikazat ćemo neke primjene kvadratnih ostataka na rješavanje nekih specifičnih diofantskih jednadžbi.

Propozicija 4.4.1. *Diofantska jednadžba* $x^2 + 3k + 1 = 0$ *nema rješenja niti za jedan cijeli broj* k.

Dokaz. Pretpostavimo da postoje cijeli brojevi x, k koji zadovoljavaju danu diofantsku jednadžbu. Tada je $x^2 = -3k-1$ pa vrijedi i $x^2 \equiv -3k-1 \pmod p$, za svaki prost broj p.

Posebno, za $p = 3$ dobivamo $x^2 \equiv -1 \pmod 3$, odakle slijedi da je -1 kvadratni ostatak modulo 3. No, Legendreov simbol $\left(\frac{-1}{3}\right)$ je jednak -1 pa polazna jednadžba nema rješenja. □

Teorem 4.4.2. *Neka je* n *prirodan broj. Diofantska jednadžba*

$$x^2 + 3y^2 = n$$

ima rješenja ako i samo ako u rastavu broja n *na proste faktore svaki prost faktor oblika* $3k - 1$ *dolazi s parnom potencijom.*

Dokaz. Pretpostavimo najprije da jednadžba iz iskaza teorema ima rješenje te neka n ima neki prost faktor p oblika $3k - 1$, tj. neka je $p \equiv 2 \pmod 3$.

Kako p dijeli n, dobivamo kongruenciju $x^2 + 3y^2 \equiv 0 \pmod p$ ili, ekvivalentno, $x^2 \equiv -3y^2 \pmod p$.

Iz prethodne kongruencije slijedi da ili p dijeli y ili je $-3y^2$ kvadratni ostatak modulo p. Pretpostavimo najprije da su p i y relativno prosti. Tada je Legendreov simbol $\left(\frac{-3y^2}{p}\right)$ jednak 1. Odatle je i $\left(\frac{-3}{p}\right) = 1$ jer je, po definiciji, $\left(\frac{-3y^2}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{y^2}{p}\right)$ te $\left(\frac{y^2}{p}\right) = 1$.

Nadalje, imamo $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)$, prema propoziciji 4.1.6. Iz $\left(\frac{-3}{p}\right) = 1$ dobivamo $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$. Kvadratni zakon reciprociteta pokazuje

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Odatle je $\left(\frac{p}{3}\right) = 1$, što povlači $p \equiv 1 \pmod 3$, suprotno polaznoj pretpostavci.

Prema tome, p dijeli y, no onda p mora dijeliti i x pa p^2 dijeli i x^2 i y^2 te p^2 dijeli i $x^2 + 3y^2 = n$. Dijeljenjem polazne jednadžbe s p^2 dobivamo novu jednadžbu $\left(\frac{x}{p}\right)^2 + 3\left(\frac{y}{p}\right)^2 = \frac{n}{p^2}$ te indukcijom slijedi da p u rastavu broja n na proste faktore dolazi s parnom potencijom.

Pokažimo sada i dovoljnost. U tu svrhu, primijetimo najprije da se prost broj p može prikazati u obliku $p = x^2 + 3y^2$ ako i samo ako je $p = 3$ ili $p \equiv 1 \pmod 3$. Zaista, $3 = 0^2 + 3 \cdot 1^2$. Nadalje, pretpostavimo $p > 3$ i $p = x^2 + 3y^2$. Očito vrijedi $(p, x) = (p, y) = 1$ jer bismo inače imali $x^2 + 3y^2 > p$, pa postoji multiplikativni inverz y' od y modulo p. Iz kongruencije $x^2 \equiv -3y^2 \pmod p$ slijedi $(xy')^2 \equiv -3 \pmod p$. Sada iz $(xy', 3) = 1$ slijedi $\left(\frac{-3}{p}\right) = 1$ ili, kao prije, $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$. Korištenjem kvadratnog zakona reciprociteta na isti način kao i prije dobivamo $p \equiv 1 \pmod 3$.

Obratno, neka je p prost broj oblika $3k + 1$. Primijetimo da je tada -3 kvadratni ostatak modulo p. Zaista, korištenjem pokazanih svojstava Legendreova simbola i kvadratnog zakona reciprociteta dobivamo $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{3k+1}{3}\right) = \left(\frac{1}{3}\right) = 1$. Prema tome, postoji cijeli broj a za koji vrijedi $a^2 \equiv -3 \pmod p$.

Očito je $(a, p) = 1$ te za $b = \lfloor\sqrt{p}\rfloor$ vrijedi $(b+1)^2 > p$. Postoji $(b+1)^2$ parova $(u, v) \in \{0, 1, \ldots, b\} \times \{0, 1, \ldots, b\}$ i $(b+1)^2$ cijelih brojeva oblika $au + v$, gdje je $u, v \in \{0, 1, \ldots, b\}$. Odatle dobivamo različite parove (u_1, v_1) i (u_2, v_2) za koje vrijedi $au_1 + v_1 \equiv au_2 + v_2 \pmod p$. Pretpostavimo da je $u_1 \geq u_2$ te neka je $x = u_1 - u_2$ i $y = v_1 - v_2$. Dobivamo $0 \leq x, |y| \leq b < \sqrt{p}$ i $ax + y \equiv 0 \pmod p$.

Prema tome, postoje cijeli brojevi x i y takvi da je $0 < x, y < \sqrt{p}$ i $p \mid a^2x^2 - y^2 = (ax - y)(ax + y)$. Sada izravno slijedi

$$p \mid a^2x^2 + 3x^2 - 3x^2 - y^2 = (a^2 + 3)x^2 - (3x^2 + y^2)$$

te zbog $a^2 + 3 \equiv 0 \pmod p$ i $p \mid 3x^2 + y^2$. Odatle je $3x^2 + y^2 = lp$, za neki prirodan broj l. Iz nejednakosti $0 \leq x^2 < p$ i $0 \leq y^2 < p$ slijedi $3x^2 + y^2 < 3p^2 + p^2 = 4p^2$ te $l \in \{0, 1, 2, 3\}$. Također, $l \neq 0$ jer bismo inače imali $3x^2 + y^2 = 0$, odakle slijedi $x = y = 0$, što nije moguće zbog $(u_1, v_1) \neq (u_2, v_2)$.

Promotrimo sada dobivene mogućnosti:

- $l = 1$: dobivamo $p = 3x^2 + y^2$.
- $l = 2$: dobivamo jednakost $2p = 3x^2 + y^2$ koja nije moguća jer iz nje slijedi da su x i y iste parnosti, odakle je $2p$ djeljivo s 4, suprotno pretpostavci.
- $l = 3$: dobivamo jednakost $3p = 3x^2 + y^2$ iz koje slijedi da se y može zapisati u obliku $y = 3y_1$, odakle je $p = x^2 + 3y_1^2$.

Neka je, napokon, n oblika a^2b, gdje je b kvadratno slobodan. Iz pretpostavke teorema slijedi $b = \prod_{i=1}^{m} p_i$, gdje je ili $p_i = 3$ ili $p_i \equiv 1 \pmod 3$ za $i = 1, 2, \ldots, m$. Tada se svaki p_i može zapisati u obliku $p_i = x_i^2 + 3y_i^2$ te iz jednakosti $(x_i^2 + 3y_i^2)(x_j^2 + 3y_j^2) = (x_i x_j + 3y_i y_j)^2 + 3(x_i y_j - x_j y_i)^2$ slijedi $b = x^2 + 3y^2$. Konačno, $n = a^2 b = (ax)^2 + 3(ay)^2$. □

Primijetimo kako prethodni teorem možemo iskazati i na sljedeći način: prirodan broj n se može prikazati u obliku $x^2 + 3y^2$, gdje su x i y cijeli brojevi, ako i samo ako se svaki prost faktor oblika $3k - 1$ u rastavu od n pojavljuje paran broj puta.

5

GAUSSOVI CIJELI BROJEVI

Gaussovi cijeli brojevi predstavljaju proširenje skupa cijelih brojeva koje je Gauss uveo prilikom proučavanja diofantskih jednadžbi oblika $x^2 + y^2 = n$, jer omogućuju faktorizaciju lijeve strane navedene jednadžbe. Kako ćemo i pokazati u ovom poglavlju, skup Gaussovih cijelih brojeva posjeduje i brojna svojstva skupa cijelih brojeva koja omogućuju njegovu primjenu pri rješavanju različitih problema u teoriji brojeva. Upravo je preko Gaussovih cijelih brojeva uveden i pojam norme te pojmovi prostog, invertibilnog i asociranog elementa koji su danas standardni pojmovi u algebri i algebarskoj teoriji brojeva.

5.1. Skup $\mathbb{Z}[i]$

Gaussovi cijeli brojevi su kompleksni brojevi oblika $a + bi$, gdje su a, b cijeli brojevi. Skup Gaussovih cijelih brojeva označava se sa $\mathbb{Z}[i]$, dakle $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$.

Primijetimo kako je svaki cijeli broj ujedno i Gaussov cijeli broj jer je $\mathbb{Z} \subset \mathbb{Z}[i]$. Također, neki cijeli brojevi mogu se zapisati u obliku produkta Gaussovih cijelih brojeva, kao npr. $5 = (2 + i)(2 - i)$ ili $50 = (4 - 3i)(8 + 6i)$.

Posebno, svaki prirodan broj n koji se može prikazati u obliku sume kvadrata dvaju cijelih brojeva x i y (tj. $n = x^2 + y^2$, kratko kažemo da je n suma dvaju kvadrata) može se zapisati u obliku produkta dvaju Gaussovih cijelih brojeva jer vrijedi $x^2 + y^2 = (x + yi)(x - yi)$.

Na skupu Gaussovih cijelih brojeva definiramo normu N: za $\alpha = a + bi \in \mathbb{Z}[i]$ definiramo $N(\alpha) = \alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2$.

Primijetimo kako je $N(\alpha)$ uvijek nenegativan cijeli broj te je $N(\alpha) = 0$ ako i samo ako je $\alpha = 0$.

Osnovno svojstvo norme je njezina multiplikativnost:

Lema 5.1.1. *Za $\alpha, \beta \in \mathbb{Z}[i]$ vrijedi $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.*

Dokaz.

$$N(\alpha \cdot \beta) = (\alpha \cdot \beta)(\overline{\alpha \cdot \beta}) = (\alpha \cdot \beta)(\overline{\alpha} \cdot \overline{\beta}) = (\alpha \cdot \overline{\alpha})(\beta \cdot \overline{\beta}) = N(\alpha)N(\beta). \quad \square$$

Iz te leme izravno slijedi i tzv. Diofantov identitet koji govori kako je produkt suma dvaju kvadrata ponovno suma dvaju kvadrata:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2. \tag{5.1}$$

Primijetimo kako je Diofantov identitet zapravo jednakost $N(a_1 + b_1i)N(a_2 + b_2i) = N((a_1 + b_1i)(a_2 + b_2i))$ koju smo dokazali u lemi 5.1.1.

Primjer 5.1.2. Sljedeći su prikazi brojeva u obliku sume dvaju kvadrata očiti: $13 = 2^2 + 3^2$, $25 = 3^2 + 4^2$, no tada vrijedi i

$$325 = 13 \cdot 25 = (2^2 + 3^2)(3^2 + 4^2) = (2 \cdot 3 - 3 \cdot 4)^2 + (2 \cdot 4 + 3 \cdot 3)^2 = 6^2 + 17^2.$$

Napomenimo da smo normu mogli definirati i općenito za proizvoljan kompleksan broj z pomoću $N(z) = z \cdot \overline{z}$. Također, tada za $z_1, z_2 \in \mathbb{C}$ vrijedi $N(z_1z_2) = N(z_1)N(z_2)$.

Element $\alpha \in \mathbb{Z}[i]$ nazivamo ***invertibilnim*** ukoliko postoji $\beta \in \mathbb{Z}[i]$ takav da je $\alpha \cdot \beta = 1$. Takav element β, ukoliko postoji, obično se označava s α^{-1}.

Propozicija 5.1.3. *Gaussov cijeli broj α je invertibilan ako i samo ako je norme jednake 1. Prema tome, jedini invertibilni Gaussovi cijeli brojevi su $1, -1, i, -i$.*

Dokaz. Neka je najprije $\alpha \in \mathbb{Z}[i]$ invertibilan. Očito je tada $\alpha \neq 0$. Tada postoji $\alpha^{-1} \in \mathbb{Z}[i]$ takav da vrijedi $\alpha \cdot \alpha^{-1} = 1$. Uzimajući normu lijeve i desne strane prethodne jednakosti te koristeći lemu 5.1.1, dobivamo $N(\alpha)N(\alpha^{-1}) = 1$. Kako su $N(\alpha)$ i $N(\alpha^{-1})$ prirodni brojevi, slijedi $N(\alpha) = 1$.

Neka je sada α Gaussov cijeli broj norme 1. Tada je $\alpha \cdot \overline{\alpha} = N(\alpha) = 1$ pa je α invertibilan.

Ako je $\alpha = a + bi$ Gaussov cijeli broj norme 1, tada je $a^2 + b^2 = 1$. Možemo zaključiti $a, b \in \{0, 1, -1\}$, $a \neq b$ i $a \cdot b = 0$. Odatle izravno slijedi posljednja tvrdnja propozicije. $\square$

5.2. Djeljivost i prosti elementi u $\mathbb{Z}[i]$

Kažemo da Gaussov cijeli broj β, različit od nule, dijeli Gaussov cijeli broj α ako postoji Gaussov cijeli broj γ takav da je $\alpha = \beta \cdot \gamma$.

Na primjer, $4 - 3i$ dijeli 25 jer je $25 = (4 - 3i)(4 + 3i)$.

Ako β dijeli α, tada očito i $N(\beta)$ dijeli $N(\alpha)$. Prema tome, npr. $4 + i$ ne može dijeliti $2 - 3i$. Dakle, na određen se način pitanje o djeljivosti u $\mathbb{Z}[i]$ često reducira na pitanje djeljivosti u $\mathbb{Z}$.

Upravo iz toga razloga definiramo da je Gaussov cijeli broj ***prost*** ako se ne može prikazati u obliku produkta Gaussovih cijelih brojeva manje norme.

Primjer 5.2.1. $3+2i$ je prost Gaussov cijeli broj jer je $N(3+2i) = 3^2+2^2 = 13$, koji je prost broj.

2 nije prost Gaussov cijeli broj jer je $2 = (1 + i)(1 - i)$, a $1 + i$, $1 - i$ su oba norme 2, dok je 2 norme 4. Primijetimo da su $1 - i$, $1 + i$ prosti Gaussovi cijeli brojevi pa su oni upravo prosti faktori broja 2 u $\mathbb{Z}[i]$.

Propozicija 5.2.2. *Svaki Gaussov cijeli broj može se prikazati kao produkt prostih Gaussovih cijelih brojeva.*

Dokaz. Dokaz je sličan dokazu analognog svojstva prirodnih brojeva.

Dakle, neka je α Gaussov cijeli broj. Ako je α prost, tada smo gotovi. Ako α nije prost, tada postoje $\beta, \gamma \in \mathbb{Z}[i]$, norme manje od α, takvi da je $\alpha = \beta \cdot \gamma$.

Ako β i γ nisu oba prosti, na isti ih način prikažemo u obliku produkta Gaussovih cijelih brojeva manje norme te nastavimo na isti način. Kako su norme prirodni brojevi i smanjuju se u svakom koraku, taj postupak mora stati nakon konačno mnogo koraka. Time dobivamo traženu faktorizaciju od α. □

Još preostaje prokomentirati jedinstvenost takve faktorizacije. U slučaju prirodnih brojeva, jedinstvenost dokazana u Osnovnom teoremu aritmetike (teorem 1.4.3) oslanjala se na Euklidov algoritam čiji je pak dokaz baziran na Teoremu o dijeljenju s ostatkom (teorem 1.1.3).

Što se faktorizacije u $\mathbb{Z}[i]$ tiče, jedinstvena je do na poredak faktora i množenje faktora invertibilnim elementima. Na primjer, $2 = (1 - i)(1 + i) = (1 + i)(1 - i) = (-1 + i)(-1 - i)$. Iz tog razloga kažemo da su Gaussovi cijeli brojevi α, β ***relativno prosti*** ako su im jedini zajednički djelitelji upravo invertibilni elementi. Npr. $2 + 3i$ i $2 - 3i$ su relativno prosti.

Osim toga, najveći zajednički djelitelj Gaussovih cijelih brojeva α i β je svaki Gaussov cijeli broj γ sa svojstvom da iz $\delta \mid \alpha$ i $\delta \mid \beta$ slijedi $\delta \mid \gamma$. Ekvivalentan

način za definirati najveći zajednički djelitelj Gaussovih cijelih brojeva α i β je reći da je to njihov zajednički djelitelj najveće norme.

Ukoliko je γ najveći zajednički djelitelj Gaussovih cijelih brojeva α i β, izravno iz definicije slijedi da su $-\gamma, i \cdot \gamma$ te $(-i) \cdot \gamma$ također najveći zajednički djelitelji od α i β.

Za dokaz jedinstvenosti faktorizacije najprije nam je potreban analogon Teorema o dijeljenju s ostatkom za Gaussove cijele brojeve:

Teorem 5.2.3. *Za $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, postoje $\gamma, \delta \in \mathbb{Z}[i]$ takvi da je $\alpha = \gamma \cdot \beta + \delta$ te $N(\delta) < N(\beta)$.*

Dokaz. Gaussov cijeli broj γ definiramo kao najbolju aproksimaciju kompleksnog razlomka $\frac{\alpha}{\beta}$ dobivenu zaokruživanjem realnog i imaginarnog dijela na najbliži cijeli broj, posebno 0.5 na 1 i -0.5 na 0.

Nakon toga, definiramo $\delta = \alpha - \beta \cdot \gamma$.

Na primjer, uzmemo li $\alpha = 5 + 7i$ i $\beta = 2 + i$, dobivamo

$$\frac{\alpha}{\beta} = \frac{5+7i}{2+i} = \frac{17}{5} + \frac{9}{5}i$$

te je $\gamma = 3 + 2i$. Dalje je $\delta = 5 + 7i - (2+i)(3+2i) = 1$ te $N(1) = 1 < N(2+i) = 5$.

Provjerimo da $N(\delta) < N(\beta)$ vrijedi i općenito. Primijetimo da je $\frac{\alpha}{\beta} - \gamma = x + yi$, gdje je $|x|, |y| \leq \frac{1}{2}$.

Iz definicije od δ slijedi $N(\delta) = N(\alpha - \beta \cdot \gamma) = N(\frac{\alpha}{\beta} - \gamma)N(\beta)$ pa je $\frac{N(\delta)}{N(\beta)} = N(\frac{\alpha}{\beta} - \gamma) = N(x + yi) = x^2 + y^2 \leq \frac{1}{2}$.

Odatle je $N(\delta) \leq \frac{N(\beta)}{2} < N(\beta)$. □

Korištenjem prethodnog teorema, na isti način kao u prvom poglavlju, dobivamo:

- Euklidov algoritam za Gaussove cijele brojeve,
- prikaz najvećeg zajedničkog djelitelja Gaussovih cijelih brojeva α, β u obliku $\gamma \cdot \alpha + \delta \cdot \beta$, za neke Gaussove cijele brojeve γ, δ,
- činjenicu da ako prost Gaussov cijeli broj β dijeli produkt $\alpha_1 \cdot \alpha_2 \cdots \alpha_n$, tada β dijeli α_i za neki $i \in \{1, 2, \ldots, n\}$,
- jedinstvenost prikaza Gaussovih cijelih brojeva u obliku produkta prostih Gaussovih cijelih brojeva do na poredak i množenje invertibilnim elementima, tj. elementima norme 1.

Pokažimo sada i neke rezultate koji povezuju proste prirodne brojeve i proste Gaussove cijele brojeve.

Propozicija 5.2.4. *Prost prirodan broj p je prost Gaussov cijeli broj ako i samo ako p nije suma dvaju kvadrata.*

Dokaz. Ako je $p = a^2 + b^2$, za neke $a, b \in \mathbb{Z}$, tada je $p = (a - bi)(a + bi)$. Kako je $N(a \pm bi) = p < N(p) = p^2$, p nije prost Gaussov cijeli broj.

Neka je sada p prost prirodan broj koji nije prost u $\mathbb{Z}[i]$. Tada postoji faktorizacija $p = (a + bi)\gamma$, gdje su $a + bi$ i γ Gaussovi cijeli brojevi norme manje od p^2. Konjugiranjem dobivamo $p = (a - bi)\overline{\gamma}$ te množenjem prethodnih izraza $p^2 = (a^2 + b^2)N(\gamma)$.

Kako su $a^2 + b^2$ i $N(\gamma)$ prirodni brojevi veći od 1, a p prost, slijedi $p = a^2 + b^2$. □

Primijetimo da su faktori $a - bi$ i $a + bi$ prostog prirodnog broja p prosti Gaussovi cijeli brojevi jer im je norma jednaka p. U sljedećoj propoziciji dokazat ćemo da se svi prosti Gaussovi cijeli brojevi pojavljuju na taj način.

Propozicija 5.2.5. *Svaki prost Gaussov cijeli broj oblika $a+bi$, gdje je $a \cdot b \neq 0$, djelitelj je prostog prirodnog broja p oblika $a^2 + b^2$.*

Dokaz. Ako je $a + bi$ prost Gaussov cijeli broj, tada je i $a - bi$ prost (inače bi rastav $a - bi = \alpha \cdot \beta$ davao rastav $a + bi = \overline{\alpha} \cdot \overline{\beta}$).

Nadalje, $(a+bi)(a-bi)$ jedinstven je rastav od $p = a^2+b^2 = (a+bi)(a-bi)$ u produkt prostih Gaussovih cijelih brojeva. Ako p nije prost, tada postoji i rastav $p = rs$, $r, s \in \mathbb{N}$, $1 < r, s < p$, što nije moguće jer bismo na taj način dobili još neki rastav u produkt prostih Gaussovih cijelih brojeva što je nemoguće zbog jedinstvenosti rastava na proste Gaussove cijele brojeve. □

5.3. Prikazi prirodnih brojeva u obliku sume dvaju kvadrata

Na samom kraju prethodnog poglavlja izveli smo uvjete pod kojima se prirodan broj može prikazati u obliku $x^2 + 3y^2$. Sada ćemo korištenjem svojstava Gaussovih cijelih brojeva prokomentirati prikaze prirodnih brojeva u obliku $x^2 + y^2$.

Ukoliko je p prost prirodan broj oblika $4k + 3$, korištenjem kongruencija modulo 4 lako se može vidjeti kako se p ne može prikazati u obliku sume dvaju

kvadrata (jer za svaki prirodan broj n vrijedi $n^2 \equiv 0$ ili $1 \pmod 4$). Preostaje vidjeti što se može reći za proste brojeve oblika $4k+1$.

Pokažimo najprije korisnu lemu:

Lema 5.3.1 (Lagrange)**.** *Prost broj $p \in \mathbb{N}$ oblika $4k+1$ dijeli n^2+1 za neki cijeli broj n.*

Dokaz. Primjenom Wilsonova teorema dobivamo:

$$\begin{aligned}
-1 &\equiv (p-1)! \pmod p \\
-1 &\equiv 1 \cdot 2 \cdot 3 \cdots 4k \pmod p \\
&\equiv (1 \cdot 2 \cdots 2k)((2k+1) \cdot (2k+2) \cdots 4k) \pmod p \\
&\equiv (1 \cdot 2 \cdots 2k)((-2k) \cdot (-2k-1) \cdots (-1)) \pmod p \\
&\equiv (1 \cdot 2 \cdots 2k)^2 (-1)^{2k} \pmod p \\
&\equiv (1 \cdot 2 \cdots 2k)^2 \pmod p
\end{aligned}$$

Stavimo li $n = (2k)!$, dobivamo $n^2 \equiv -1 (\mathrm{mod}\ p)$ pa p dijeli n^2+1. □

Teorem 5.3.2 (Fermat)**.** *Svaki prost broj p oblika $4k+1$ može se prikazati u obliku sume kvadrata dvaju cijelih brojeva.*

Dokaz. Neka je $n \in \mathbb{Z}$ takav da p dijeli n^2+1, takav n postoji prema prethodnoj lemi. U $\mathbb{Z}[i]$ vrijedi $n^2+1 = (n-i)(n+i)$.

Iako p dijeli n^2+1, p ne dijeli niti $n-i$ niti $n+i$ jer $\frac{n}{p} - \frac{i}{p}$ i $\frac{n}{p} + \frac{i}{p}$ nisu Gaussovi cijeli brojevi. No, tada p nije prost Gaussov cijeli broj. Sada propozicija 5.2.4 pokazuje da je p oblika $p = a^2 + b^2$, za neke cijele brojeve a i b. □

Teorem 5.3.3. *Prirodan broj n može se prikazati u obliku sume kvadrata dvaju cijelih brojeva ako i samo ako se svaki prost faktor oblika $4k+3$ u rastavu od n pojavljuje s parnom potencijom.*

Dokaz. Neka je najprije $n = x^2 + y^2$ te neka je $p \in \mathbb{N}$ prost faktor broja n oblika $4k+3$. Tada je $x^2 \equiv -y^2 \pmod p$. Nastavljamo slično kao u dokazu teorema 4.4.2: pretpostavimo da p ne dijeli y, tada je Legendreov simbol $(\frac{-y^2}{p})$ jednak 1 te i $(\frac{-1}{p}) = 1$, što nije moguće prema propoziciji 4.1.6.

Prema tome, $p \mid y$ pa $p^2 \mid x^2 + y^2 = n$. Dijeljenjem s p^2 dobivamo novu jednakost $(\frac{x}{p})^2 + (\frac{y}{p})^2 = \frac{n}{p^2}$ te induktivno slijedi da se p pojavljuje u rastavu broja n na proste faktore s parnom potencijom.

Sada pretpostavimo kako se svaki prost broj oblika $4k+3$ u rastavu od n pojavljuje s parnom potencijom. Prema tome, n možemo zapisati u obliku $n = p_1 p_2 \cdots p_l n_1^2$, gdje su $p_1, p_2, \ldots, p_l$ međusobno različiti prosti brojevi od kojih je najviše jedan jednak 2, dok za ostale vrijedi $p_i \equiv 1 (\mathrm{mod}\ 4)$.

Iz teorema 5.3.2 i činjenice da je $2 = 1^2 + 1^2$ slijedi da se svaki od prostih brojeva $p_1, p_2, \ldots, p_l$ može prikazati u obliku sume kvadrata dvaju cijelih brojeva pa iz Diofantova identiteta (5.1) slijedi da se i broj n može prikazati u obliku sume kvadrata dvaju cijelih brojeva. □

5.4. Pitagorine trojke

Uređenu trojku prirodnih brojeva (x, y, z) nazivamo ***Pitagorina trojka*** ako vrijedi

$$x^2 + y^2 = z^2,$$

tj. ako su x i y katete, a z hipotenuza pravokutnog trokuta. Ako su x, y, z relativno prosti, kažemo da je (x, y, z) ***primitivna*** Pitagorina trojka.

Primjer 5.4.1. (3,4,5) je primitivna Pitagorina trojka.

Trojke prirodnih brojeva s navedenim svojstvom bile su intenzivno proučavane u vrijeme antičke Grčke, čemu i duguju svoj današnji naziv, a određivanje takvih trojki može se svrstati među najstarije matematičke probleme. Posebno su zanimljive zbog korelacije koju pružaju između geometrije i teorije brojeva. Još je Euklid izveo izraze kojima su dane sve Pitagorine trojke, dok je analogne trojke racionalnih brojeva proučavao Diofant. Ipak, natpisi na povijesno posebno važnoj kamenoj pločici, danas poznatoj pod nazivom *Plimpton 322*, svjedoče kako su Pitagorine trojke bile poznate i Babiloncima, otprilike 1300 godine prije Pitagore. Više o samoj pločici Plimpton 322 može se saznati u [10]. Napomenimo da su posljednja istraživanja rezultirala činjenicom da su Pitagorine trojke bile sastavni dio nastave matematike u Babilonu ([12]). Drevni su narodi trebali Pitagorine trojke kako bi odredili pravi kut pri gradnji i mjerenju zemljišta: što su brojevi u Pitagorinoj trojci bili veći, pravi se kut mogao preciznije odrediti.

Najprije ćemo promatrati isključivo primitivne Pitagorine trojke, iz kojih se lako dobiju i ostale Pitagorine trojke.

Kako su kvadrati parnih brojeva kongruentni 0 modulo 4, a kvadrati neparnih prirodnih brojeva kongruentni 1 modulo 4, u svakoj je primitivnoj Pitagorinoj trojci točno jedan od brojeva x, y paran, dok je z neparan.

U $\mathbb{Z}[i]$ identitet $x^2+y^2=z^2$ možemo zapisati u obliku $(x-yi)(x+yi)=z^2$. Vezano uz taj identitet, pokažimo sljedeće rezultate.

Lema 5.4.2. *Ako je (x,y,z) primitivna Pitagorina trojka, tada su $x-yi$ i $x+yi$ relativno prosti Gaussovi cijeli brojevi.*

Dokaz. Ako je $\alpha \in \mathbb{Z}[i]$ zajednički djelitelj Gaussovih cijelih brojeva $x-yi$ i $x+yi$, tada je i $\overline{\alpha}$ zajednički djelitelj tih brojeva (primijetimo da iz uvjeta $(x,y)=1$ slijedi da α nije cijeli broj). No, tada je produkt $\alpha\cdot\overline{\alpha}$, koji je prirodan broj, djelitelj od $(x-yi)(x+yi)$.

Kako svaki zajednički djelitelj Gaussovih cijelih brojeva $x-yi$ i $x+yi$ dijeli njihovu sumu $2x$ te njihovu razliku $2yi$, slijedi kako su svi zajednički prosti djelitelji od $x-yi$ i $x+yi$ sadržani među prostim Gaussovim cijelim brojevima $\pm 1 \pm i$ koji dijele 2. No, kako je $(x-yi)(x+yi)=z^2$, gdje je z neparan, slijedi da niti jedan Gaussov cijeli broj oblika $\pm 1 \pm i$ ne dijeli desnu stranu prethodne jednakosti pa su $x-yi$ i $x+yi$ relativno prosti. □

Lema 5.4.3. *Neka su $x-yi$ i $x+yi$ relativno prosti Gaussovi cijeli brojevi takvi da je $(x-yi)(x+yi)=z^2$, za neki $z \in \mathbb{Z}[i]$. Tada postoje $u_1,u_2,\alpha,\beta \in \mathbb{Z}[i]$, u_1,u_2 invertibilni, takvi da je $x-yi=u_1\alpha^2$ te $x+yi=u_2\beta^2$.*

Drugim riječima, relativno prosti faktori kvadrata su kvadrati pomnoženi invertibilnim elementima.

Dokaz. Kako se u rastavu od z^2 svaki prost faktor pojavljuje s parnom potencijom, a $x-yi$ i $x+yi$ nemaju zajedničkih prostih faktora, također se i svaki prost faktor od $x-yi$ i $x+yi$ mora pojaviti s parnom potencijom. Produkt parnih potencija prostih faktora očito je potpun kvadrat. Kako su preostali faktori koji se mogu pojaviti jedino invertibilni elementi, $x-yi$ i $x+yi$ mogu se prikazati u obliku produkata invertibilnih elemenata i potpunih kvadrata. □

Prema prethodnim rezultatima, ako je (x,y,z) primitivna Pitagorina trojka, tada $x-yi$ ima jedan od sljedećih oblika:

$$(s-ti)^2,\ -(s-ti)^2,\ i(s-ti)^2,\ -i(s-ti)^2,$$

gdje su $s,t \in \mathbb{Z}$. Dakle, $x-yi$ je oblika:

$$(s^2-t^2)-2sti,\ (t^2-s^2)+2sti,\ 2st+(s^2-t^2)i,\ -2st+(t^2-s^2)i.$$

Izjednačavanjem realnih i imaginarnih dijelova dobivamo da je jedan od brojeva x, y oblika u^2-v^2, a drugi oblika $2uv$, za neke prirodne brojeve u i v. Očito je $u>v$.

Obično se uzima da je y paran, dakle $y = 2uv$. Kako su x, y relativno prosti (jer se radi o primitivnoj Pitagorinoj trojci), slijedi da su i u i v relativno prosti. Također, u i v su različite parnosti jer bi inače x bio paran.

Iz identiteta $(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$ proizlazi $z = u^2 + v^2$. Time smo dokazali sljedeći teorem.

Teorem 5.4.4. *Ako je (x, y, z) primitivna Pitagorina trojka, tada postoje relativno prosti prirodni brojevi u i v različite parnosti, $u > v$, takvi da je $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$.*

Sve Pitagorine trojke dane su identitetom

$$\big(d(u^2 - v^2)\big)^2 + (2duv)^2 = \big(d(u^2 + v^2)\big)^2,\ d \in \mathbb{N}. \tag{5.2}$$

Primjer 5.4.5. Odredite sve Pitagorine trojke u kojima je jedna stranica jednaka 14.

Iz identiteta (5.2) vidimo da je $d \in \{1, 2, 7, 14\}$. Primijetimo kako dijeljenjem s d dobivamo primitivnu Pitagorinu trojku. Promotrimo moguće slučajeve zasebno:

- $d = 14$: u ovom slučaju dijeljenjem s d dobivamo primitivnu Pitagorinu trojku čiji je jedan član jednak 1. No, kako je $u > v$ te $u^2 - v^2$ neparan, slijedi da je $1 = u^2 - v^2 = (u - v)(u + v)$, odakle slijedi $u - v = u + v = 1$, što nije moguće.

- $d = 7$: sada dobivamo primitivnu Pitagorinu trojku čiji je član $y = 2uv$ jednak 2. Odatle slijedi $u = v = 1$ što ponovno nije moguće jer su u i v različite parnosti.

- $d = 2$: dijeljenje s d vodi na primitivnu Pitagorinu trojku čiji je jedan član jednak 7. Prema teoremu 5.3.3, 7 se ne može prikazati u obliku $u^2 + v^2$. Prema tome, $7 = u^2 - v^2 = (u - v)(u + v)$ pa je $u + v = 7$ i $u - v = 1$. Rješenje ovog sustava je $u = 4$, $v = 3$ te dobivamo Pitagorinu trojku $(14, 48, 50)$.

- $d = 1$: preostaje primitivna Pitagorina trojka s jednim članom jednakim 14. Dakle, $2uv = 14$, tj. $uv = 7$. No, kako su u i v različite parnosti, ovaj slučaj nije moguć.

6

PELLOVE JEDNADŽBE

Pellova jednadžba $x^2 - ny^2 = 1$, gdje je n prirodan broj koji nije potpun kvadrat, pripada među najstarije i najvažnije diofantske jednadžbe drugog reda, a jedini pravi suparnik joj u tome može biti Pitagorina jednadžba $x^2 + y^2 = z^2$ koju smo riješili u prethodnom poglavlju.

Pellova jednadžba ima dugu povijest, a korijeni joj sežu još u doba antičke Grčke. Još je Teon iz Smirne koristio rješenja jednadžbe $x^2 - 2y^2 = 1$ kako bi racionalnim brojem $\frac{x}{y}$ aproksimirao $\sqrt{2}$. Općenito, Arhimed je primijetio da, ako su x i y velika rješenja jednadžbe $x^2 - ny^2 = 1$, tada je $\frac{x}{y}$ dobra aproksimacija iracionalnog broja $\sqrt{n}$. Još je jednu čuvenu Pellovu jednadžbu otkrio Arhimeda. Kako je otkriveno iz povijesnih izvora u 18. stoljeću, nakon što je Apolonij iz Perga kritizirao jedan od Arhimedovih radova, Arhimed u formi epigrama od 44 retka postavlja *problem stoke*. Taj računski izuzetno zahtjevan problem u kojem se traži prebrojavanje bikova različitih boja (i o kojem se više može naći u [5]) temelji se na sustavu sedam jednadžbi s osam nepoznanica koji se svodi na Pellovu jednadžbu $x^2 - 4729494y^2 = 1$. Taj je problem Arhimed poslao Apoloniju, a tek je krajem 19. stoljeća otkriveno da u najmanjem rješenju te jednadžbe y ima čak 41 znamenku.

Zatim se Pellova jednadžba pojavljuje i u indijskoj matematici. Najprije indijski matematičar Baudhayana otkriva da je $x = 577$, $y = 408$ rješenje jednadžbe $x^2 - 2y^2 = 1$ te koristi $\frac{577}{408}$ kako bi aproksimirao $\sqrt{2}$. Zatim, u 7. stoljeću Brahmagupta dolazi do važnog pravila kojim se iz poznatih rješenja Pellove jednadžbe dobivaju i druga rješenja iste jednadžbe te pronalazi i rješenje jednadžbe $x^2 - 92y^2 = 1$, pri čemu naglašava kako se osoba koja ovaj problem riješi za manje od godinu dana može smatrati matematičarem. Konačno, u 12. stoljeću Bhaskara II. pronalazi najmanje rješenje jednadžbe $x^2 - 61y^2 = 1$ u

prirodnim brojevima koje je daleko veće od svih najmanjih rješenja u prirodnim brojevima jednadžbi $x^2 - ny^2 = 1$ za $n \leq 60$.

Navedena jednadžba dobiva današnji naziv nakon što se Euler susreo s Wallisovim djelom *Opera Mathematica* te greškom proglasio kako je prvi koji je ozbiljnije proučavao netrivijalna rješenja jednadžbe $x^2 - ny^2 = 1$ ($x \neq 1$, $y \neq 0$) upravo engleski matematičar John Pell. Ipak, ne postoje dokazi da se Pell ikada bavio jednadžbama tog tipa. Posljednji koji se, prije Eulerova vremena, bavio ovakvim jednadžbama je Fermat koji je još 1657. bez dokaza obznanio tvrdnju da za prirodan broj n koji nije potpun kvadrat jednadžba $x^2 - ny^2 = 1$ ima beskonačno mnogo cjelobrojnih rješenja (tu je tvrdnju dokazao Lagrange, 1770.). Fermat je također izazvao poznate matematičare tog doba, Williama Brounckera i Johna Wallisa da pronađu cjelobrojna rješenja jednadžbi $x^2 - 151y^2 = 1$ i $x^2 - 313y^2 = 1$. Wallis je kratko odgovorio da je $(1728148040, 140634693)$ rješenje prve jednadžbe, dok je Brouncker pronašao uređen par $(126862368, 7170685)$ koji je rješenje druge jednadžbe. Sam je Fermat odbijao otkriti vlastitu metodu za rješavanje Pellove jednadžbe, no poznato je kako je znao da najmanje netrivijalno rješenje jednadžbe $x^2 - 109y^2 = 1$ u prirodnim brojevima glasi $(158070671986249, 1514042455100)$. Nešto kasnije, tijekom 18. stoljeća, metode koje su razvili navedeni matematičari stapaju se u jednostavniju metodu verižnih razlomaka koje se može smatrati modifikacijom Euklidova algoritma za par $(\sqrt{n}, 1)$, a koju ćemo kratko opisati na kraju ovog poglavlja (svi se detalji mogu naći u [6]).

6.1. Osnovni pojmovi i egzistencija rješenja

Pellovom jednadžbom naziva se diofantska jednadžba oblika

$$x^2 - ny^2 = 1,$$

gdje je n prirodan broj koji nije potpun kvadrat. Neka su otkrića u vezi ove jednadžbe greškom od strane Eulera pripisana Johnu Pellu koji nije značajnije pridonio u njezinom rješavanju.

Općenito, jednadžbu oblika $x^2 - ny^2 = k$, gdje je k prirodan broj te n prirodan broj koji nije potpun kvadrat nazivamo ***pellovska jednadžba***.

U antičkoj Grčkoj proučavan je poseban slučaj Pellove jednadžbe za $n = 2$, u kojem rješenja te jednadžbe u prirodnim brojevima pružaju dodatne informacije o prirodi iracionalnog broja $\sqrt{2}$. Postoji i slična veza između rješenja Pellove jednadžbe u prirodnim brojevima s iracionalnim brojem $\sqrt{n}$ (podsje-

timo, za $n \in \mathbb{N}$ vrijedi da je broj $\sqrt{n}$ iracionalan ako i samo ako n nije potpun kvadrat):

Pretpostavimo da postoji niz proizvoljno velikih rješenja $(x_1, y_1), (x_2, y_2), \ldots$ Pellove jednadžbe. Iz jednakosti $x_i^2 - ny_i^2 = 1$ slijedi $\frac{x_i^2}{y_i^2} = n + \frac{1}{y_i^2} \to n$ kada $y_i \to \infty$.

Prema tome, kvocijenti rješenja Pellove jednadžbe predstavljaju racionalne brojeve koji po volji dobro aproksimiraju iracionalan broj $\sqrt{n}$.

Kako ćemo vidjeti, upravo iracionalnost broja $\sqrt{n}$ omogućuje dobivanje jednostavne relacije kojom se sva rješenja Pellove jednadžbe u skupu prirodnih brojeva mogu prikazati u terminima najmanjeg rješenja u prirodnim brojevima. Primijetimo kako Pellova jednadžba ima i trivijalnih cjelobrojnih rješenja $x = \pm 1$, $y = 0$.

Prvi nam je cilj pokazati kako Pellova jednadžba zaista uvijek ima rješenje. Ključni korak u tome dan je sljedećim teoremom:

Teorem 6.1.1 (Dirichletov teorem o aproksimaciji)**.** *Za svaki iracionalni broj oblika $\sqrt{n}$ i prirodan broj B postoje cijeli brojevi a i b, $0 < b < B$, takvi da je*

$$|a - b\sqrt{n}| < \frac{1}{B}.$$

Dokaz. Neka je prirodan broj B proizvoljan, ali fiksiran. Promotrimo $B-1$ brojeva $\sqrt{n}, 2\sqrt{n}, \ldots, (B-1)\sqrt{n}$. Za svaki $k \in \{1, 2, \ldots, B-1\}$ odaberimo cijeli broj A_k takav da je $0 \leq A_k - k\sqrt{n} \leq 1$.

Kako je $\sqrt{n}$ iracionalan, niti jedan od brojeva $A_k - k\sqrt{n}$ ne može biti jednak 0 ili 1. Također, za $k_1 \neq k_2$ vrijedi $A_{k_1} - k_1\sqrt{n} \neq A_{k_2} - k_2\sqrt{n}$ (jer bi u suprotnom vrijedilo $\sqrt{n} = \frac{A_{k_1} - A_{k_2}}{k_2 - k_1}$).

Prema tome, u segmentu $[0, 1]$ imamo $B+1$ različitih brojeva $0, A_1 - \sqrt{n}, A_2 - 2\sqrt{n}, \ldots, A_{B-1} - (B-1)\sqrt{n}, 1$.

Podijelimo li segment $[0, 1]$ na B podintervala duljine $\frac{1}{B}$, prema Dirichletovom principu, barem jedan podinterval sadrži najmanje dva od navedenih brojeva. Neka su to $A_i - i\sqrt{n}$ i $A_j - j\sqrt{n}$, $i \neq j$ (možemo uzeti da je $i < j$).

Tada je $|A_i - i\sqrt{n} - A_j + j\sqrt{n}| < \frac{1}{B}$ te za $a = A_i - A_j$ i $b = j - i$ vrijedi $|a - b\sqrt{n}| < \frac{1}{B}$. Iz $1 \leq i < j \leq B-1$ slijedi $0 < b < B$. □

Navedimo nekoliko direktnih posljedica prethodnog teorema:

- Kako prethodni teorem vrijedi za sve $B > 0$, možemo odabrati proizvoljno mali broj $\frac{1}{B}$ čime dobivamo nove vrijednosti za a i b. Prema tome, postoji beskonačno mnogo parova cijelih brojeva (a, b) takvih da je $|a - b\sqrt{n}| < \frac{1}{B}$. Iz $0 < b < B$ slijedi $|a - b\sqrt{n}| < \frac{1}{b}$.

- Očito je $|a+b\sqrt{n}| \leq |a-b\sqrt{n}| + |2b\sqrt{n}| \leq |3b\sqrt{n}|$ te $|a^2-b^2n| \leq \frac{1}{b}\cdot 3b\sqrt{n} = 3\sqrt{n}$. Prema tome, postoji beskonačno mnogo parova cijelih brojeva (a,b) takvih da je $|a^2-nb^2| \leq 3\sqrt{n}$. Posebno, postoji beskonačno mnogo parova prirodnih brojeva (a_i,b_i) takvih da je $a_i^2 - nb_i^2 = N$, za neki prirodan broj N, $N < 3\sqrt{n}$.

- Postoje različiti parovi prirodnih brojeva (a_1,b_1) i (a_2,b_2) za koje vrijedi $a_1^2 - nb_1^2 = a_2^2 - nb_2^2 = N$, $a_1 \equiv a_2 \pmod N$ te $b_1 \equiv b_2 \pmod N$.

Sada možemo dokazati i egzistenciju rješenja Pellove jednadžbe:

Teorem 6.1.2. *Neka je n prirodan broj koji nije potpun kvadrat. Tada Pellova jednadžba $x^2 - ny^2 = 1$ ima rješenje u prirodnim brojevima $(x,y) \neq (1,0)$.*

Dokaz. Neka je $a - b\sqrt{n}$ kvocijent brojeva $a_1 - b_1\sqrt{n}$ i $a_2 - b_2\sqrt{n}$ dobivenih prije iskaza teorema. Tada je

$$a - b\sqrt{n} = \frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} = \frac{(a_1 - b_1\sqrt{n})(a_2 + b_2\sqrt{n})}{a_2^2 - nb_2^2} = \frac{a_1a_2 - nb_1b_2}{N} + \frac{a_1b_2 - b_1a_2}{N}\sqrt{n}.$$

Očito je $a - b\sqrt{n} \neq \pm 1$.

Kako N dijeli $a_1^2 - nb_1^2$, dobivamo $a_1^2 - nb_1^2 \equiv 0 \pmod N$, odakle iz $a_1 \equiv a_2 \pmod N$ i $b_1 \equiv b_2 \pmod N$ slijedi $a_1a_2 - nb_1b_2 \equiv 0 \pmod N$.

Na isti način je i $a_1b_2 - b_1a_2 \equiv 0 \pmod N$ pa su $\frac{a_1a_2 - nb_1b_2}{N}$ i $\frac{a_1b_2 - b_1a_2}{N}$ cijeli brojevi.

Korištenjem identiteta $a_1^2 - nb_1^2 = a_2^2 - nb_2^2 = N$ jednostavnim računom dobivamo $a^2 - nb^2 = 1$ pa je parom (a,b) dano traženo rješenje. □

6.2. Struktura skupa rješenja Pellove jednadžbe

Rješenje (x_1,y_1) u prirodnim brojevima Pellove jednadžbe $x^2 - ny^2 = 1$ nazivamo najmanjim netrivijalnim rješenjem te jednadžbe ako za svako drugo rješenje (x_2,y_2) u prirodnim brojevima iste jednadžbe vrijedi $x_1 < x_2$ (primijetimo da je tada i $y_1 < y_2$ te $x_1 + \sqrt{n}y_1 < x_2 + \sqrt{n}y_2$). Najmanje netrivijalno rješenje Pellove jednadžbe često nije lako naći. U nekim slučajevima to ipak nije pretežak posao, kao npr. za Pellove jednadžbe $x^2 - 2y^2 = 1$ i $x^2 - 3y^2 = 1$. Naime, najmanja rješenja tih jednadžbi u prirodnim brojevima nisu prevelika te su redom dana s $(x,y) = (3,2)$ te $(x,y) = (2,1)$.

No, napomenimo da je najmanje rješenje jednadžbe $x^2 - 61y^2 = 1$ u prirodnim brojevima jednako $(x,y) = (1766319049, 226153980)$!

Osnovna važnost u poznavanju najmanjeg netrivijalnog rješenja leži u tome što ono odmah daje beskonačno mnogo rješenja:

Propozicija 6.2.1 (Brahmaguptino kompoziciono pravilo)**.** *Ako su* (x_1, y_1) *i* (x_2, y_2) *rješenja Pellove jednadžbe* $x^2 - ny^2 = 1$*, tada je i* $(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + x_2y_1)$ *također rješenje.*

Dokaz. Najprije primijetimo kako vrijedi $(x_1 + \sqrt{n}y_1)(x_2 + \sqrt{n}y_2) = x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)$.

Kako su (x_1, y_1) i (x_2, y_2) rješenja Pellove jednadžbe $x^2 - ny^2 = 1$, očito je $1 = (x_1^2 - ny_1^2)(x_2^2 - ny_2^2)$. Redom dobivamo

$$\begin{aligned}
1 &= (x_1 - \sqrt{n}y_1)(x_1 + \sqrt{n}y_1)(x_2 - \sqrt{n}y_2)(x_2 + \sqrt{n}y_2) \\
&= (x_1 - \sqrt{n}y_1)(x_2 - \sqrt{n}y_2)(x_1 + \sqrt{n}y_1)(x_2 + \sqrt{n}y_2) \\
&= (x_1x_2 + ny_1y_2 - \sqrt{n}(x_1y_2 + x_2y_1))(x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)) \\
&= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + x_2y_1)^2 \\
&= x_3^2 - ny_3^2
\end{aligned}$$

pa je i par (x_3, y_3) rješenje Pellove jednadžbe $x^2 - ny^2 = 1$. □

Primjer 6.2.2. Iz rješenja $(3, 2)$ redom, primjenom prethodnog pravila, dolazimo do rješenja $(17, 12)$, $(99, 70)$ Pellove jednadžbe $x^2 - 2y^2 = 1$.

Vrijedi i mnogo više od prethodno pokazanog, naime, svako rješenje Pellove jednadžbe možemo dobiti na opisani način iz najmanjeg rješenja u prirodnim brojevima:

Teorem 6.2.3. *Neka je s* (x_1, y_1) *označeno najmanje rješenje u prirodnim brojevima Pellove jednadžbe* $x^2 - ny^2 = 1$*. Ako je* (x_2, y_2) *neko rješenje iste Pellove jednadžbe u prirodnim brojevima, tada postoji* $m \in \mathbb{N}$ *takav da je* $x_2 + \sqrt{n}y_2 = (x_1 + \sqrt{n}y_1)^m$*.*

Dokaz. Pretpostavimo da postoji rješenje (x_2, y_2) takvo da $x_2 + \sqrt{n}y_2$ nije oblika $(x_1 + \sqrt{n}y_1)^m$ za neki $m \in \mathbb{N}$. Kako je $x_1 + \sqrt{n}y_1 > 1$ i $x_2 + \sqrt{n}y_2 > 1$, postoji $k \in \mathbb{N}$ za koji vrijedi

$$(x_1 + \sqrt{n}y_1)^k < x_2 + \sqrt{n}y_2 < (x_1 + \sqrt{n}y_1)^{k+1}.$$

Množenjem s $(x_1 - \sqrt{n}y_1)^k$ dobivamo

$$1 < (x_2 + \sqrt{n}y_2)(x_1 - \sqrt{n}y_1)^k < x_1 + \sqrt{n}y_1.$$

Definirajmo cijele brojeve x_3, y_3 s $x_3 + \sqrt{n}y_3 = (x_2 + \sqrt{n}y_2)(x_1 - \sqrt{n}y_1)^k$. Odatle slijedi i $x_3^2 - ny_3^2 = (x_2^2 - ny_2^2)(x_1^2 - ny_1^2)^k = 1$.

Iz $1 < x_3 + \sqrt{n}y_3$ slijedi i $0 < x_3 - \sqrt{n}y_3 < 1$ pa je $2x_3 > 1$ i $2\sqrt{n}y_3 > 0$. Prema tome, (x_3, y_3) rješenje je Pellove jednadžbe $x^2 - ny^2 = 1$ u prirodnim brojevima koje je manje od rješenja (x_1, y_1) jer vrijedi $x_3 + \sqrt{n}y_3 < x_1 + \sqrt{n}y_1$, što nije moguće. □

6.3. Određivanje rješenja Pellove jednadžbe

Netrivijalna rješenja Pellove jednadžbe $x^2 - ny^2 = 1$ najlakše se mogu odrediti korištenjem razvoja iracionalnog broja $\sqrt{n}$ u jednostavni verižni razlomak. Iracionalnost broja $\sqrt{n}$ implicira kako ovaj razvoj nije konačan, ali vidjet ćemo da ima vrlo poseban oblik.

Za beskonačan verižni razlomak $[a_1, a_2, \ldots]$ kažemo da je ***periodski*** ako postoje prirodni brojevi k i m takvi da je $a_{m+n} = a_n$, za sve $n \geq k$. Najmanji takav broj m nazivamo ***periodom*** verižnog razlomka $[a_1, a_2, \ldots]$ te pišemo

$$[a_1, a_2, \ldots] = [a_1, a_2, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}].$$

Prema Primjeru 1.3.1, možemo pisati $\sqrt{2} = [1, \overline{2}]$.
Iskažimo postupak za određivanje razvoja u jednostavni verižni razlomak broja $\sqrt{n}$:

- Najprije stavimo $a_1 = \lfloor \sqrt{n} \rfloor$, te neka je zatim $s_1 = a_1$ i $t_1 = n - s_1^2$.
- U sljedećem koraku stavimo $\alpha_1 = \frac{s_1 + \sqrt{n}}{t_1}$.
- U svakom od narednih koraka uzimamo $a_i = \lfloor \alpha_{i-1} \rfloor$, $s_i = a_i t_{i-1} - s_{i-1}$ te $t_i = \frac{n - s_i^2}{t_{i-1}}$.
- Nakon toga, neka je $\alpha_i = \frac{s_i + \sqrt{n}}{t_i}$.

Iz relacija $s_i = a_i t_{i-1} - s_{i-1}$ i $t_i = \frac{n - s_i^2}{t_{i-1}} = \frac{n - s_{i-1}^2}{t_{i-1}} + 2a_i s_{i-1} - a_i^2 t_i$ induktivno slijedi da su s_i, t_i nenegativni cijeli brojevi te da je $t_i \neq 0$.

U svakom koraku vrijedi

$$\alpha_{i-1} - a_i = \frac{s_{i-1} + \sqrt{n} - a_i t_{i-1}}{t_{i-1}} = \frac{\sqrt{n} - s_i}{t_{i-1}} = \frac{n - s_i^2}{t_{i-1}(\sqrt{n} + s_i)} = \frac{t_i}{\sqrt{n} + s_i} = \frac{1}{\alpha_i}.$$

Dakle, s $[a_1, a_2, \ldots]$ dan je razvoj broja $\sqrt{n}$ u jednostavni verižni razlomak.

Primijetimo da je razvoj periodski ako postoje prirodni brojevi i, j, $i \neq j$, takvi da je $(s_i, t_i) = (s_j, t_j)$. Može se pokazati da vrijedi nejednakost $t_i < s_i + \sqrt{n} < 2\sqrt{n}$, iz koje slijedi kako brojevi s_i i t_i mogu poprimiti samo konačno mnogo vrijednosti, čime dobivamo sljedeći rezultat:

Propozicija 6.3.1. *Ako je n prirodan broj koji nije potpun kvadrat, tada je razvoj broja $\sqrt{n}$ u jednostavni verižni razlomak periodski.*

Primjer 6.3.2. Korištenjem prethodno opisanog postupka može se dobiti $\sqrt{28} = [5, \overline{3, 2, 3, 10}]$.

Situacija pokazana prethodnim primjerom nije slučajna. Naime, ako je n prirodan broj koji nije potpun kvadrat, tada iracionalni broj $\sqrt{n}$ ima razvoj u jednostavni verižni razlomak oblika $[a_1, \overline{a_2, a_3, \ldots, a_{m-1}, 2a_1}]$, gdje vrijedi $a_2 = a_{m-1}$, $a_3 = a_{m-2}$ itd.

Sada je prirodno postaviti pitanje kojeg su oblika iracionalni brojevi koji imaju periodski razvoj u jednostavni verižni razlomak. To ćemo pitanje riješiti narednom definicijom i rezultatom:

Definicija 6.3.3. Iracionalan broj α zovemo ***kvadratna iracionalnost*** ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.

Primijetimo da je kvadratna iracionalnost α oblika $\frac{a \pm \sqrt{b}}{c}$ za $c \neq 0$ i $b > 0$ koji nije potpun kvadrat.

Teorem 6.3.4 (Euler, Lagrange)**.** *Iracionalan broj α ima periodski razvoj u jednostavni verižni razlomak ako i samo ako je α kvadratna iracionalnost.*

Dokaz. Periodičnost zapisa slijedi na isti način kao i u opisanom slučaju razvoja drugog korijena iz prirodnog broja koji nije potpun kvadrat. Pojasnimo sada i vezu periodskih zapisa s kvadratnim iracionalnostima.

Neka je $\alpha = [a_1, a_2, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m-1}}]$ razvoj iracionalnog broja α u periodski verižni razlomak. Pokažimo da je α kvadratna iracionalnost. Neka je najprije $\beta = [\overline{a_{k+1}, \ldots, a_{k+m-1}}]$. Tada vrijedi

$$\beta = a_{k+1} + \cfrac{1}{\ddots + \cfrac{1}{a_{k+m-1} + \frac{1}{\beta}}},$$

odakle dobivamo da postoje cijeli brojevi a, b, a', b' takvi da je

$$\beta = \frac{a\beta + b}{a'\beta + b'},$$

što daje i kvadratnu jednadžbu za β. Prema tome, β je kvadratna iracionalnost te je oblika $\beta = \frac{c + \sqrt{d}}{e}$. Kako je $\alpha = [a_1, a_2, \ldots, a_k, \beta]$, direktno slijedi da je i α također kvadratna iracionalnost, tj. da je α također oblika $\frac{c' + \sqrt{d'}}{e'}$ za prirodan broj d' koji nije potpun kvadrat. □

Sljedećim su teoremom potpuno određena rješenja Pellove jednadžbe:

Teorem 6.3.5. *Sva rješenja u prirodnim brojevima jednadžbe* $x^2 - ny^2 = 1$ *nalaze se među* $x = p_i$, $y = q_i$, *gdje su* $\frac{p_i}{q_i}$ *parcijalne konvergente u razvoju broja* $\sqrt{n}$ *u jednostavni verižni razlomak. Prirodan broj* $\lfloor \sqrt{n} \rfloor$ *smatra se nultom konvergentnom te se, shodno tome, uzima* $p_0 = \lfloor \sqrt{n} \rfloor$ *i* $q_0 = 1$. *Neka je* m *duljina perioda u razvoju od* $\sqrt{n}$. *Ako je* m *paran, tada su rješenja dana s* $x = p_{mk-1}$, $y = q_{mk-1}$, *za* $k \in \mathbb{N}$. *Ako je* m *neparan, tada su rješenja dana s* $x = p_{mk-1}$, $y = q_{mk-1}$, *za paran* $k \in \mathbb{N}$.

Primjer 6.3.6. Najmanje rješenje u prirodnim brojevima Pellove jednadžbe $x^2 - 28y^2 = 1$ dano je s $x = p_3 = 127$, $y = q_3 = 24$ jer je

$$\frac{p_3}{q_3} = 5 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3}}} = 5 + \frac{1}{3 + \frac{3}{7}} = 5 + \frac{7}{24} = \frac{127}{24}.$$

Literatura

[1] T. Andreescu, D. Andrica: *An Introduction to Diophantine Equations*; Gil Publishing House, 2002

[2] S. Bingulac, I. Matić: *Kineski teorem o ostatcima za polinome*; Osječki matematički list, 14(2012), 34–55

[3] D. M. Burton: *The History of Mathematics: An Introduction*; McGraw-Hill Primis, 2006

[4] L. N. Childs: *A Concrete Introduction to Higher Algebra*; Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1995

[5] B. Dakić: *Arhimedov problem stoke*; Matematika i Škola, 51(2009), 34–37

[6] A. Dujella: *Uvod u teoriju brojeva*; skripta, PMF - Matematički odsjek, Sveučilište u Zagrebu, 2003

[7] H. M. Edwards: *Fermat's Last Theorem*; Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1977

[8] G. A. Jones, J. M. Jones: *Elementary Number Theory*; Undergraduate Texts in Mathematics, Springer-Verlag, London, 2003

[9] N. Koblitz: *A Course in Number Theory and Cryptography*; Graduate Texts in Mathematics, Springer-Verlag, New York, 1994

[10] M. Libl, I. Matić: *Plimpton* 322; Matematika i škola, 73(2014), 114–118

[11] I. Matić, D. Ševerdija: *Grčko-kineski stil u teoriji brojeva*; Osječki matematički list, 10(2010), 43–58

[12] E. Robson: *Words and pictures: New light on Plimpton* 322, American Mathematical Monthly, 109, 2(2002), 105–120

[13] G. Savin: *Numbers, Groups and Cryptography*; skripta, Department of Mathematics, University of Utah, 2009

[14] J. Stillwell: *Elements of Number Theory*; Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003

[15] J. Stillwell: *Mathematics and Its History*; Springer-Verlag, New York, 2002

Indeks