

UVOD U TEORIJU BROJEVA

Ivan Matić

Predavanja održana na Odjelu za matematiku
Sveučilišta Josipa Jurja Strossmajera u Osijeku
u ljetnom semestru akademske godine 2010./2011.

Osijek, 2011.

Sadržaj

1	DJELJIVOST	4
1.1	Osnovni pojmovi	4
1.2	Euklidov algoritam	5
1.3	Verižni razlomci	8
1.4	Prosti brojevi	10
1.4.1	Osnovni teorem aritmetike	10
1.4.2	Skup prostih brojeva	11
1.4.3	Broj djelitelja i suma djelitelja prirodnog broja	12
1.4.4	Fermatovi i Mersennovi brojevi	13
2	KONGRUENCIJE	16
2.1	Definicija i osnovna svojstva	16
2.1.1	Potpuni i reducirani sustavi ostataka	18
2.2	Eulerova funkcija	20
2.3	Wilsonov i Lagrangeov teorem	22
3	PRIMJENA KONGRUENCIJA	24
3.1	Linearne diofantske jednadžbe	24
3.2	Kriptosustavi	25
3.3	RSA kriptosustav	29
4	KVADRATNI OSTATCI	32
4.1	Legendreov simbol	32
4.2	Kvadratni zakon reciprociteta	35
4.3	Jacobijev simbol	36
4.4	Primjena kvadratnih ostataka na diofantske jednadžbe	37
5	GAUSSOVI CIJELI BROJEVI	39
5.1	Skup $\mathbb{Z}[i]$	39
5.2	Djeljivost i prosti elementi u $\mathbb{Z}[i]$	40
5.3	Prikazi prirodnih brojeva u obliku sume dvaju kvadrata	42
5.4	Pitagorine trojke	43

6	PELLOVE JEDNADŽBE	47
6.1	Osnovni pojmovi i egzistencija rješenja	47
6.2	Struktura skupa rješenja Pellove jednadžbe	49
6.3	Određivanje rješenja Pellove jednadžbe	50

Poglavlje 1

DJELJIVOST

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.

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

Navedimo nekoliko osnovnih svojstava djeljivosti:

Propozicija 1.1.1. (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. \square

Primijetimo kako 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 1.1.2. 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 $[q, q + 1)$. 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 1.1.1 slijedi $q_1 = q_2$. No, tada je i $r_1 = r_2$ čime je teorem dokazan. \square

U prethodnom teoremu se 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 cjelobrojni 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 2. $100 = 32 \cdot 3 + 4$, $\lfloor \frac{100}{32} \rfloor = 3$. 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 se naziva 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 označavamo s (b, c) . Izraz (b, c) nazivamo *najveći zajednički djelitelj brojeva b i c* .

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

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

Primjer 3. $(100, 17) = 1$, $(24, 16) = 8$, $(a, a \cdot b) = a$.

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, \dots, b_n kažemo da su relativno prosti ukoliko je $(b_1, b_2, \dots, b_n) = 1$.

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 ćemo opisati u idućem poglavlju.

1.2 Euklidov algoritam

Promotrimo najprije idući primjer.

Primjer 4. *Odredite $(70, 32)$.*

Prema dijelu (3) Propozicije 1.1.1, 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 samo uzastopnom primjenom Teorema 1.1.2 dobili slijedeći 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 $a > r_1 > r_2 > \dots$ 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 $(a, b) = (a, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n$, jer r_n dijeli r_{n-1} . Prema tome, (a, b) jednak je posljednjem nenul ostatku. Opisani postupak određivanja najvećeg zajedničkog djelitelja se naziva *Euklidov algoritam*.

Primjer 5. *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

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

U prethodnom primjeru bi na taj način dobili redom:

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

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

Teorem 1.2.1. *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 $(a, b) \mid b$, 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 smo pokazali kako 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 je prirodno zapitati se koliko je brz, tj. koliko je koraka potrebno da bi se izvršio. Tako postoje situacije u kojima je Euklidov algoritam izrazito efikasan, kao npr. $a = 51, b = 105$:

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

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

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

Slijedeći rezultat daje ogradu na broj mogućih koraka Euklidova algoritma.

Propozicija 1.2.2. *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 $5 \cdot (\lceil \log a \rceil + 1)$.*

Dokaz. Podsjetimo kako je broj znamenki broja a jednak upravo $\lfloor \log a \rfloor + 1$.

Pretpostavimo kako smo primjenom Euklidova algoritma dobili slijedeći niz jednakosti

$$\begin{aligned} b &= q_{n-1}a + r_{n-1} \\ a &= q_{n-2}r_{n-1} + r_{n-2} \\ &\vdots \\ r_3 &= q_1r_2 + r_1 \\ r_2 &= q_0r_1, \end{aligned}$$

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

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 kako je $r_i \geq F_i$, gdje je F_i i -ti Fibonaccijev broj (primijetimo kako 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 je veći ili jednak broju znamenki od F_n .

Kako bi ocijenili broj znamenki Fibonaccijeva broja, koristimo Binetovu formulu $F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$. Za velike n je izraz $\left(\frac{1-\sqrt{5}}{2} \right)^{n+1}$ mali (blizu nuli) te možemo koristiti ocjenu $F_n \approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1}$. Iz ove ocjene slijedi

$$\log F_n \approx (n+1) \log \left(\frac{1+\sqrt{5}}{2} \right) - \log \sqrt{5} \approx \frac{n}{5},$$

jer je $\log \left(\frac{1+\sqrt{5}}{2} \right) \approx \frac{1}{5}$. Prema tome, broj znamenki broja a nije veći od broja koraka algoritma podijeljenog s 5, tj. broj koraka algoritma je manji ili jednak od broja znamenki broja a uvećanog 5 puta, odnosno $\lfloor \log a \rfloor + 1 \geq \frac{n}{5}$. \square

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. Ovaj postupak staje ukoliko je $b_n = 0$ za neki n , u suprotnom se može nastaviti u nedogled.

Pogledajmo ovaj 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 $\alpha_3 = \frac{6}{4}$, $a_3 = 1$, $b_3 = \frac{2}{4}$. Naposljetku, $\alpha_4 = \frac{4}{2} = a_4 = 2$ i $b_4 = 0$.

Ovim smo dobili idući zapis racionalnog broja $\frac{172}{50}$:

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

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

Primijetimo kako se upravo ovaj niz brojeva pojavio u Primjeru 5. 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 $a_0 = [\alpha] = q_1$, $b_0 = \frac{r_1}{b}$, $\alpha_1 = \frac{b}{r_1}$. Potom $a_1 = [\alpha_1] = q_2$, $b_1 = \frac{r_2}{r_1}$, $\alpha_2 = \frac{r_1}{r_2}$ itd. Odatle dobivamo

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

te $\frac{a}{b} = [q_1, q_2, \dots, q_n]$. 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 $\frac{a}{b} \leq 0$.

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

Primjer 6. *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, $\alpha_1 = \alpha_2 = \alpha_3 = \dots = \sqrt{2} + 1$ te $a_1 = a_2 = a_3 = \dots = 2$. Sada $\sqrt{2}$ možemo zapisati u obliku

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}},$$

ili kraće $\sqrt{2} = [1, \bar{2}]$, gdje $\bar{2}$ označava uzastopno ponavljanje broja 2. Gornji razvoj iracionalnog broja $\sqrt{2}$ u verižni razlomak treba promatrati kao aproksimaciju iracionalnog broja parcijalnim konvergentama $[1, 2], [1, 2, 2], [1, 2, 2, 2], \dots$, koje zaista predstavljaju konvergentan niz racionalnih brojeva čiji limes je 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 se naziva složen. Primijetimo kako 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 se očituje 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 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 ćemo prokomentirati u slijedećem podnaslovu.

1.4.1 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 1.2.1, 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. \square

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

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

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. Neka je 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, \dots, 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 $p_2 = q_2, p_3 = q_3, \dots, p_k = q_k$ te $k = l$. Time je teorem u potpunosti dokazan. \square

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

Iduća 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 je djeljiv brojem b ako i samo ako za svaki q_j , $j \in \{1, 2, \dots, l\}$ postoji neki $i \in \{1, 2, \dots, k\}$ tako da je $q_j = p_i$ i $\alpha_i \geq \beta_j$.*

Primjer 7. $18 = 2 \cdot 3^2 \mid 54 = 2 \cdot 3^3$, no $36 = 2^2 \cdot 3^2 \nmid 54$.

1.4.2 Skup prostih brojeva

S \mathcal{P} označavamo skup svih prostih brojeva. Idući rezultat opisuje osnovno svojstvo ovog skupa:

Teorem 1.4.5. *Skup \mathcal{P} je beskonačan.*

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

Pretpostavimo kako je skup prostih brojeva konačan, te stavimo $\mathcal{P} = \{p_1, p_2, \dots, p_k\}$. Promotrimo broj $q = p_1 p_2 \cdots p_k + 1$. Očito je $q > p_i$ za sve $i = 1, 2, \dots, k$ 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.

Riemannova zeta funkcija je definirana s

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

gdje je s kompleksan broj. Primijetimo da je $\zeta(1)$ upravo harmonijski red, koji je divergentan.

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 ovaj rastav, harmonijski red $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ možemo zapisati u obliku konačnog produkta

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

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 kako prostih brojeva ima beskonačno mnogo. \square

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 proste 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.

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 $i = 1, 2, \dots, k$ (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 $\alpha_i \geq 2$ za neki i .

1.4.3 Broj djelitelja i suma djelitelja prirodnog broja

U ovom potpoglavlju će nas interesirati 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 $i = 1, 2, \dots, k$. Osim toga, vidimo da svakim ovakvim odabirom eksponenata $\beta_1, \beta_2, \dots, \beta_k$ 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 8. 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 $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}$. 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 $f : \mathbb{N} \rightarrow \mathbb{C}$ 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 9. $\sigma(100) = \sigma(2^2 \cdot 5^2) = \frac{2^3-1}{2-1} \cdot \frac{5^3-1}{5-1} = 217$.

1.4.4 Fermatovi i Mersennovi brojevi

U ovom kratkom potpoglavlju uvodimo neke specijalne brojeve, koji su od posebnog interesa u teoriji brojeva. Više svojstava tih brojeva ćemo dokazati u narednim poglavljima.

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

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

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 u još nekoliko navrata) je smatrao da je i F_5 prost, no 100-tinjak godina nakon Fermata je Leonard Euler pronašao 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:

$$\begin{aligned} F_n &= (F_{n-1} - 1)^2 + 1 \\ F_n &= F_{n-1} + 2^{2^{n-1}} F_0 F_1 \cdots F_{n-2} \\ F_n &= F_{n-1}^2 - 2(F_{n-2} - 1)^2 \\ F_n &= F_0 F_1 \cdots F_{n-1} + 2 \end{aligned}$$

Posljednju od navedenih relacija ćemo iskoristiti u dokazu idućeg rezultata:

Propozicija 1.4.6. *Neka su i, j nenegativni cijeli brojevi. Ako je $i \neq j$, tada je $(F_i, F_j) = 1$.*

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 $(F_i, F_j) \mid F_i$ i $(F_i, F_j) \mid F_0 \cdots F_j \cdots F_{i-1}$, slijedi da $(F_i, F_j) \mid 2$. No, svi Fermatovi brojevi su neparni, odakle dobivamo $(F_i, F_j) = 1$. \square

Prije nego se dotaknemo Mersennovih, 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 $28 = 1 + 2 + 4 + 7 + 14$.

Idući teorem potječe od L. Eulera:

Teorem 1.4.7. *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 $n = (2^{k+1} - 1)2^k m'$.

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. \square

Napomenimo kako 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 takvi brojevi su sadržani među Mersennovim brojevima.

Mersennovi brojevi su brojevi oblika $M_n = 2^n - 1$, gdje je n prirodan broj. Može se vidjeti da ako je Mersennov broj M_n prost, tada i n mora biti prost. Još nije dokazana slutnja da postoji beskonačno mnogo prostih Mersennovih brojeva.

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

Teorem 1.4.8. *Definirajmo niz prirodnih brojeva (s_n) sa $s_1 = 4$, $s_{n+1} = s_n^2 - 2$. Neka je p neparan prost broj. Mersennov broj M_p je prost ako i samo ako M_p dijeli s_{p-1} .*

Poglavlje 2

KONGRUENCIJE

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 $ac \equiv bc \pmod{nc}$.

Primjer 10. $17 \equiv 5 \pmod{12}$ i $5 \equiv 5 \pmod{12}$. Slično, $24 \equiv 0 \pmod{12}$. Također, $6 \equiv -34 \pmod{40}$.

Napomena 2.1.1. *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 2.1.2. *Neka je n prirodan broj. Biti kongruentan modulo n je relacija ekvivalencije na skupu cijelih brojeva.*

Dokaz. Kako $n \mid 0 = a - a$, očito je $a \equiv a \pmod{n}$. 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 $b \equiv c \pmod{n}$. Iz $n \mid a - b$ i $n \mid b - c$ dobivamo $n \mid a - b + b - c = a - c$ te $a \equiv c \pmod{n}$. \square

U idućoj propoziciji navodimo osnovna svojstva kongruencija:

Propozicija 2.1.3. (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 se mogu 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 1.2.1 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 $b \equiv c \pmod{n}$. \square

Primijetimo kako 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 iduća propozicija:

Propozicija 2.1.4. *Neka je $ax \equiv ay \pmod{n}$. Tada vrijedi $x \equiv y \pmod{\frac{n}{d}}$, 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. \square

Lako se može vidjeti, korištenjem dijela (1) Propozicije 2.1.3, kako vrijedi i obrat prethodne tvrdnje.

Primjer 11. *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. $x \in \{\dots, -33, -16, 1, 18, 35, \dots\}$.*

Pogledajmo neke jednostavne primjene kongruencija:

Propozicija 2.1.5. (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 $n = a_1 + 10 \cdot a_2 + \dots + 10^{k-2} a_{k-1} + 10^{k-1} a_k$, 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 2.1.3 slijedi $10^j \equiv 1 \pmod{3}$, za $j \geq 0$. Odatle je $n = a_1 + 10 \cdot a_2 + \dots + 10^{k-2} a_{k-1} + 10^{k-1} a_k \equiv a_1 + a_2 + \dots + a_{k-1} + a_k \pmod{3}$, 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 $n \equiv a_1 - a_2 + a_3 - a_4 + \dots + (-1)^{k+1} a_k \pmod{11}$, čime je propozicija dokazana. \square

Jedna od najstandarnijih primjena kongruencija se nalazi u označavanju knjiga - svaka knjiga je jednoznačno određena tzv. ISBN brojem (*International Standard Book Number*). ISBN broj je niz od 10 znamenki a_1, a_2, \dots, a_{10} , npr. 0 - 387 - 95587 - 9. Znamenke a_1, \dots, a_{10} su podijeljene u 4 skupine, od kojih prva označava gdje je knjiga

izdana, druga izdavača, a treća naslov i redni broj izdanja. Posljednja znamenka, a_{10} , se naziva 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 se upisuje X . Kontrolna znamenka je uvedena kako bi se na efikasan način mogle korigirati učestale pogreške koje nastaju pri prepisivanju ISDN brojeva - pogreške nastale zamjenom mjesta dvaju znamenki ili greškom u prepisivanju jedne znamenka.

Dakle, pretpostavimo kako je niz b_1, b_2, \dots, b_{10} dobiven prepisivanjem ISBN broja a_1, a_2, \dots, 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 kako tada niz b_1, b_2, \dots, b_{10} ne predstavlja valjan ISBN broj.

Primijetimo kako 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, \dots, b_{10} ne predstavlja ISBN broj.

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

2.1.1 Potpuni i reducirani sustavi ostataka

Neka je n prirodan broj veći od 1. Skup $S = \{a_1, a_2, \dots, a_n\}$ se naziva *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 2.1.6. *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 potpun sustav ostataka modulo n je skup $\{0, 1, 2, \dots, n-1\}$. 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 iduća lema:

Lema 2.1.7. *Neka je $S = \{a_1, a_2, \dots, a_n\}$ potpuni sustav ostataka modulo n . Tada je i $\{b \cdot a_1, b \cdot a_2, \dots, b \cdot a_n\}$ potpuni sustav ostataka modulo n , za svaki cijeli broj b za koji vrijedi $(b, n) = 1$.*

Dokaz. Prema Napomeni 2.1.6, dovoljno je dokazati da su svaka dva elementa skupa $\{b \cdot a_1, b \cdot a_2, \dots, b \cdot a_n\}$ 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 2.1.3 (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. \square

U nastavku ćemo kratko komentirati rješavanje linearnih kongruencija, tj. kongruencija oblika $ax \equiv b \pmod{n}$. Prvotni interes za rješavanje ovakvih kongruencija dolazi iz diofantskih jednačbi, gdje se često mogu iskoristiti za pronalaženje rješenja.

Lema 2.1.8. *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 , tj. ako je $S = \{a_1, a_2, \dots, a_n\}$ 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, postoji 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 ova 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 2.1.3 slijedi $x_1 \equiv x_2 \pmod{n}$ što je i trebalo dokazati. \square

Primjer 12. *Kongruencija $3x \equiv 50 \pmod{113}$ ima jedinstveno rješenje, koje je dano $s \equiv 92 \pmod{113}$.*

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

Teorem 2.1.9. *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 $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$.*

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 $\frac{a}{d}(y - x_0)$. Pošto 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 nikoja dva različita broja oblika $x_0 + j\frac{n}{d}$ nisu međusobno kongruentni modulo n za $0 \leq j \leq d - 1$. \square

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 $S = \{a_1, a_2, \dots, a_k\}$ se naziva *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 13. 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 $1, 2, \dots, n$ koji su relativno prosti s n se označava s $\varphi(n)$; ovim je definirana funkcija $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ 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 $\{a_1, a_2, \dots, a_{\varphi(n)}\}$.

Primjer 14. $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(1) = 1$. 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 2.1.7 se može dokazati i

Lema 2.2.1. Neka je $S = \{a_1, a_2, \dots, a_{\varphi(n)}\}$ potpuni sustav ostataka modulo n . Tada je i $\{b \cdot a_1, b \cdot a_2, \dots, b \cdot a_{\varphi(n)}\}$ potpuni sustav ostataka modulo n , za svaki cijeli broj b za koji vrijedi $(b, n) = 1$.

Teorem 2.2.2 (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 $S = \{a_1, a_2, \dots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n . Prema prethodnoj lemi je tada i skup $\{a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(n)}\}$ 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 2.1.3 (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 2.1.3 (2) dobivamo $1 \equiv a^{\varphi(n)} \pmod{n}$, čime je teorem dokazan. \square

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

Korolar 2.2.3 (Mali Fermatov teorem). Neka je p prost broj i a cijeli broj. Ako p ne dijeli a , tada je $a^{p-1} \equiv 1 \pmod{p}$.

U ostatku ovog potpoglavlja ćemo opisati još neka svojstva Eulerove funkcije.

Lema 2.2.4. *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 $1, 2, \dots, p^k$ koji nisu relativno prosti s p^k su $p, 2p, 3p, \dots, p^k = p^{k-1} \cdot p$, tj. njih p^{k-1} . Odatle slijedi $\varphi(p^k) = p^k - p^{k-1}$. \square

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

Lema 2.2.5 (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 kako se ovdje radi o sustavu dvije jednačbe, tj. kongruencije, s jednom nepoznanicom. Promatramo preslikavanje

$$i : \{0, 1, \dots, mn - 1\} \rightarrow \{0, 1, \dots, m - 1\} \times \{0, 1, \dots, n - 1\},$$

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

Primjera radi, 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, rješenje polaznog sustava kongruencija je x za koji vrijedi $i(x) = (1, 3)$ te je dano s $x \equiv 8 \pmod{10}$.

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

Neka su $t_1, t_2 \in \{0, 1, \dots, mn - 1\}$ 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. \square

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

Teorem 2.2.6. *Neka su n_1, n_2, \dots, n_k u parovima relativno prosti prirodni brojevi te neka su a_1, a_2, \dots, a_k cijeli brojevi. Tada postoji rješenje sustava kongruencija $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, \dots , $x \equiv a_k \pmod{n_k}$. Ako je x_0 jedno rješenje, tada su sva rješenja dana s $x \equiv x_0 \pmod{n_1 n_2 \cdots n_k}$.*

Teorem 2.2.7. *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 $t \in \{0, 1, \dots, mn\}$, neka je $i(t) = (a, b)$, gdje je i preslikavanje definirano u dokazu Leme 2.2.5. Primijetimo da je $(t, mn) = 1$ ako i samo ako je $(a, m) = (b, n) = 1$.

Zaista, kako je $t = k_1m + a = k_2n + b$, 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 $\varphi(mn) = \varphi(m)\varphi(n)$. \square

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

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

Primjer 15. $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$.

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 se naziva multiplikativni inverz od a modulo p .

Zaista, kako su a i p relativno prosti, prema Teoremu 1.2.1 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 2.1.8 slijedi da su svaka dva multiplikativna inverza od a modulo p međusobno kongruentni 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 .

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 $1, 2, \dots, p-1$ 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 $x \in \{1, 2, \dots, p-1\}$ takav da vrijedi $x^2 \equiv 1 \pmod{p}$. Tada $p \mid x^2 - 1 = (x-1)(x+1)$. Kako je p prost broj i $1 \leq x \leq p-1$, slijedi da je ili $x-1 = p$ 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 $(p-1)! \equiv -1 \pmod{p}$. \square

Primjer 16. *Iz Wilsonova teorema slijedi da je $100! \equiv -1 \pmod{101}$, tj. $101 \mid 100! + 1$.*

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

Teorem 2.3.2 (Lagrangeov teorem). *Ako je p prost broj i $P(x)$ polinom stupnja n s cjelobrojnim koeficijentima, 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 2.1.8. Pretpostavimo kako 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, pretpostavimo kako je $P(x_0) \equiv 0 \pmod{p}$, za neki cijeli broj x_0 te neka je $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, gdje su $a_0, a_1, \dots, a_n \in \mathbb{Z}$.

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

Kako za $k \in \mathbb{N}$ vrijedi $x^k - x_0^k = (x - x_0)(x^{k-1} + x^{k-2}x_0 + \dots + x x_0^{k-2} + x_0^{k-1})$, 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 $P(x_0) \equiv 0 \pmod{p}$ pokazuje kako je ili $x - x_0 \equiv 0 \pmod{p}$ ili $Q(x) \equiv 0 \pmod{p}$. Prema pretpostavci indukcije, kongruencija $Q(x) \equiv 0 \pmod{p}$ ima najviše $n - 1$ rješenja pa kongruencije $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja (x_0 i rješenja kongruencije $Q(x) \equiv 0 \pmod{p}$), što je i trebalo dokazati. \square

Poglavlje 3

PRIMJENA KONGRUENCIJA

3.1 Linearne diofantske jednačbe

Neka su a_1, a_2, \dots, a_n, b cijeli brojevi. Tada se jednačba oblika

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

naziva *linearna diofantska jednačba*. Ovdje pretpostavljamo da je n prirodan broj te da su svi brojevi a_1, a_2, \dots, a_n različiti od nule.

Rješivost linearnih diofantskih jednačbi (u cijelim brojevima) je karakterizirana idućim teoremom:

Teorem 3.1.1. *Linearna diofantska jednačba $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$ ima rješenja ako i samo ako $(a_1, a_2, \dots, a_n) \mid b$. U tom slučaju, svako rješenje se može zapisati pomoću $n - 1$ cjelobrojnih parametara.*

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

Pretpostavimo sada da d dijeli b . Dijeljenjem polazne jednačbe s d dobivamo ekvivalentnu jednačbu

$$a'_1x_1 + a'_2x_2 + \dots + a'_nx_n = b', \quad (3.1)$$

gdje je $a'_i = \frac{a_i}{d}$ te $b' = \frac{b}{d}$. Očito vrijedi $(a'_1, a'_2, \dots, a'_n) = 1$.

Dokazat ćemo da ova jednačba ima rješenja indukcijom po broju varijabli, tj. indukcijom po n .

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

Neka je sada $n \geq 2$ te pretpostavimo da jednačba ima rješenja u slučaju da je broj varijabli manji od n . Dokažimo da tvrdnja vrijedi i za n varijabli.

Neka je $d_1 = (a'_1, a'_2, \dots, a'_{n-1})$. Tada svako rješenje jednačbe $a'_1x_1 + a'_2x_2 + \dots + a'_nx_n = b'$ zadovoljava i kongruenciju $a'_1x_1 + a'_2x_2 + \dots + a'_nx_n \equiv b' \pmod{d_1}$, koja je ekvivalentna kongruenciji $a'_nx_n \equiv b' \pmod{d_1}$.

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 ovog izraza u jednadžbu (3.1) dobivamo jednadžbu u $n - 1$ varijabli

$$a'_1x_1 + a'_2x_2 + \cdots + a'_{n-1}x_{n-1} = b' - a'_nc - a'_{n-1}d_1t_1. \quad (3.2)$$

Pokažimo da d_1 dijeli $b' - a'_nc - a'_{n-1}d_1t_1$. U tu svrhu je dovoljno dokazati da d_1 dijeli $b' - a'_nc$, tj. da je $a'_nc \equiv b' \pmod{d_1}$. No, kako je $a'_nc = (a'_n)^{\varphi(d_1)}b'$, 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

$$a''_1x_1 + a''_2x_2 + \cdots + a''_{n-1}x_{n-1} = b'', \quad (3.3)$$

pri čemu je $a''_i = \frac{a'_i}{d_1}$ te $b'' = \frac{b' - a'_nc}{d_1} - a'_{n-1}t_1$.

Kako je $(a''_1, a''_2, \dots, a''_{n-1}) = 1$, po pretpostavci indukcije jednadžba (3.3) ima rješenja te svako rješenje ove 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. \square

Poseban slučaj linearnih diofantskih jednadžbi je dan idućim korolarom.

Korolar 3.1.2. *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 ove jednadžbe dana s $x = x_0 + a_2t$, $y = y_0 - a_1t$.*

Primjer 17. *Rješimo 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 ove jednadžbe je $x = -1 + 5s$, $y = 1 - 2s$. Prema prethodnom korolaru su sva 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 su dana s $(x, y, z) = (-1 + 5s + 4t, 1 - 2s - 3t, 1 - s)$, $s, t \in \mathbb{Z}$.

3.2 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 se naziva *kriptografija* (od grčki krypto - skrivati te grafo - pisati). Ova disciplina je u principu prisutna od samog nastanka pisma i pisanih komunikacija, a prvi napredniji oblici se pojavljuju u antičkoj Grčkoj u petom stoljeću prije Krista.

U samoj osnovi kriptografije se nalaze dvije osobe, *pošiljaoc* i *primaoc* poruke, koje žele komunicirati sigurnim putem, tj. žele komunicirati na način da neželjene strane ne mogu odgonetnuti sadržaj poruke koju pošiljaoc šalje primaocu.

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

Poruka koju pošiljaoc želi poslati se naziva *otvoreni tekst*, kojeg pošiljaoc prije slanja transformira koristeći unaprijed dogovoreni postupak šifriranja - time se dobiva šifrirani tekst ili *šifrat*.

I otvoreni tekst i šifrat se sastoje 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 se zatim šalje primaocu; presječe li poruku netko treći, on vidi šifrat, no treba osigurati da ne može doći do sadržaja otvorenog teksta.

S druge strane, primaoc je upućen u postupak šifriranja po 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. Ove funkcije često ovise o nekom unaprijed zadanom parametru (*ključu*), poznatom pošiljaocu i primaocu 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 su preslikavanja f_t i g_t injekcije.

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 $0, 1, 2, \dots, 9$.

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

Primjer 18. *Pomak alfabeta 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, ..., slovu Z odgovara 25.

Ideja ove 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 kriptanalizu 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 su u ovom 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 fiksnim parametrom modulo 26.

No, predstavljena Cezarova šifra je nažalost vrlo nezahvalna radi njene sigurnosti. 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 alfabeta za k_1 i k_2 podudaraju. Zaključujemo kako su svi predstavnici parametara iskazani upravo potpunim sustavom ostataka modulo 26.

Primjer 19. *Neka je primjenom Cezarove šifre dobiven šifrat QRSKSTSOYWENE. Odredimo otvoreni tekst (pretpostavljamo da znamo da je napisan na hrvatskom jeziku) i korišteni parametar k .*

Primijetimo kako šifrat počinje s tri uzastopna slova abecede, pa s tri uzastopna slova 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 naredno 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 je glasila 'Mnogo pokušaja', a korišteni parametar k je jednak 4.

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

Primjer 20. *Jednokratni uzorak.*

Sada ćemo predstaviti daleko sigurniji način šifriranja (po tim, naravno, smatramo da je kriptanaliza kompliciranija). Neka je $a_1a_2a_3 \dots$ vrlo dug slučajan niz prirodnih

brojeva, od kojih je svaki manji ili jednak 26. Pod pojmom vrlo dugi niz smatramo da broj elemenata u ovom nizu prelazi broj znakova korištenih u otvorenom tekstu.

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

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

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

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

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

Osnovni cilj kriptografije je 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 takozvane *simetrične šifre*, kod kojih 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 $a_1a_2a_3\dots$) poznati samo pošiljaocu i primaocu 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) su takve 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 pošiljaocu i primaocu 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 je često vrlo komplicirano prikazati u obliku produkta prostih faktora (bez poznavanja npr. nekog od faktora).

Primjer 21. Brojevi 11399 i 105929 su prosti. Njihov produkt je jednak 1207484671. No, prikazati prethodni broj u obliku produkta prostih brojeva, bez poznavanja barem jednog od njih, je prilično težak zadatak.

Upravo ovaj princip ćemo iskoristiti u idućem potpoglavlju.

3.3 RSA kriptosustav

RSA kriptosustav je nastao 1977. i nazvan je prema inicijalima trojice njegovih tvoraca, matematičara Rona Rivesta, Adia Shamira i Lena Adlemana.

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

Alfabet otvorenog teksta se ponovno sastoji od slova engleske abecede, no čitav postupak šifriranja i dešifriranja se obavlja 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 takozvani enkripcijski eksponent e , koji može biti bilo koji cijeli 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 se može odrediti iz Euklidova algoritma, jer ima svojstvo da postoji neki cijeli broj c za koji je $ed + c\varphi(n) = 1$. Broj d se naziva 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 $f_t(x) = x^e \pmod n$, gdje je t parametar $t = (n, e)$.

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

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

Uvjerimo se najprije da su ovako definirane funkcije zaista jedna drugoj inverzne:

Teorem 3.3.1. *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 2.2.5 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 $x = x^{ed} \pmod{n}$, jer je $x < n$. Dakle, funkcije su međusobno inverzne. \square

Primjer 22. Pokažimo na primjeru kako 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 s 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 $20^{13} \pmod{77}$. U tu svrhu se koristimo idućim 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 idućem koraku je $x = 2$ 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 bi 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 su računski najkompliciraniji koraci 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 nepoгодne za računanje.

No, primijetimo kako nama u stvari nisu potrebni prirodni brojevi x^e i y^d , već samo njihovi ostaci 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 23. *Digitalni potpis*

RSA kriptosustav se također koristi prilikom prenošenja digitalnog potpisa kojim se dokazuje kako je korisnik uistinu onaj za koga se predstavlja. U tu svrhu, korisnik je dužan pokazati kako posjeduje podatke kojima nitko drugi ne bi trebao raspolagati, poput nekog osobnog koda, lozinke ili poput dekrpcijskog 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 $x^d \pmod n$, 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 $x^d \pmod n$, jer vrijedi $(x^d)^e = x^{ed} \equiv x \pmod n$.

Na taj način se svatko može uvjeriti da je korisnik u posjedu tajnog eksponenta d te time i u njegov identitet.

Poglavlje 4

KVADRATNI OSTATCI

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 24. 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 $\left(\frac{a}{p}\right)$ je definiran s

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

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

Podsjetimo se kako, u slučaju da su a i p relativno prosti brojevi i p neparan prost, vrijedi $a^{p-1} \equiv 1 \pmod{p}$ (prema Korolaru 2.2.3). Euler je iskoristio ovu relaciju kako bi dobio iduću formulu za određivanje Legendreova simbola:

Teorem 4.1.1 (Eulerov kriterij). *Ako je p neparan prost broj, tada vrijedi $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Prema tome, a je kvadratni ostatak modulo p ako i samo ako je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Dokaz. Očito je $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$ ako i samo ako $p \mid a$, tj. ako i samo ako je $\left(\frac{a}{p}\right) = 0$. Dakle, u tom slučaju je 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, $\left(\frac{a}{p}\right) = 1$ po definiciji Legendreova simbola. Kako su a i p relativno prosti, slijedi da su i b i p relativno prosti. Time dobivamo $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$.

Preostaje još provjeriti formulu iz iskaza teorema u slučaju da a nije kvadratni ostatak modulo p . Primijetimo kako 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 2.3.2 znamo da su ovo jedina rješenja), dovoljno je dokazati da $a^{\frac{p-1}{2}}$ nije kongruentno 1 modulo p kada a nije kvadratni ostatak 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 su moraju nalaziti $1^2, 2^2, \dots, (\frac{p-1}{2})^2$, 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 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ su dana navedenim nizom koji uključuje samo kvadratne ostatke modulo p .

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

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

Dokaz. U dokazu prethodnog teorema smo vidjeli kako su $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ 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 $1^2, 2^2, \dots, (\frac{p-3}{2})^2$ modulo p .

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

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

Propozicija 4.1.3. *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

$$(\frac{a_1}{p})(\frac{a_2}{p}) \equiv (a_1)^{\frac{p-1}{2}} (a_2)^{\frac{p-1}{2}} \equiv (a_1 a_2)^{\frac{p-1}{2}} \equiv (\frac{a_1 a_2}{p}) \pmod{p}. \quad \square$$

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

Primjer 25. Odredimo $\left(\frac{-8}{3}\right)$.

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

Propozicija 4.1.4. 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 rječima, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Dokaz. Prema Eulerovu kriteriju je $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.

Ako je $p \equiv 1 \pmod{4}$, tada je broj $\frac{p-1}{2}$ paran pa je $\left(\frac{-1}{p}\right) = 1$.

Ako je $p \equiv 3 \pmod{4}$, tada je broj $\frac{p-1}{2}$ neparan pa je $\left(\frac{-1}{p}\right) = -1$. □

Propozicija 4.1.5. 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 $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}$, no s izrazom $2^{\frac{p-1}{2}}$ je mnogo teže manipulirati nego s izrazom $(-1)^{\frac{p-1}{2}}$ u prethodnoj propoziciji.

Najprije ćemo dokazati iduće kongruencije:

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

Redom imamo

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

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 se dobiva 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. \square

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

Kako raspolažemo rezultatima iz prethodne dvije propozicije, uvrštavanjem dobivamo $\left(\frac{2}{3}\right) = -1$ i $\left(\frac{-1}{3}\right) = 1$. Dakle, $\left(\frac{-8}{3}\right) = -1$.

4.2 Kvadratni zakon reciprociteta

Iako smo pokazali nekoliko rezultata pomoću kojih se mogu odrediti Legendreovi simboli, eksplicitno izračunavanje ovih simbola i dalje ostaje kompliciran postupak, osobito ako su uključeni veći brojevi. Npr. s kompliciranim postupkom se susrećemo 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.

Za dokaz tog rezultata ćemo trebati iduću lemu, koju dajemo bez dokaza:

Lema 4.2.1. *Ako je p neparan prost broj te a neparan cijeli broj koji nije djeljiv s p . Tada je*

$$\left(\frac{a}{p}\right) = (-1)^k$$

gdje je $k = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{ia}{p} \rfloor$.

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. Podijelimo skup $T = \{(x, y) : x, y \in \mathbb{N}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$, koji se sastoji od $\frac{p-1}{2} \cdot \frac{q-1}{2}$ elemenata na dva disjunktna podskupa A i B na način da se u skupu A nalaze parovi (x, y) u kojima je $qx > py$, a u skupu B oni parovi koji zadovoljavaju $qx < py$.

Kako su p i q prosti te $x < p$, $y < q$, očito je $qx \neq py$ pa je $A \cup B = T$.

Skup A se sastoji od parova (x, y) za koje vrijedi $1 \leq x \leq \frac{p-1}{2}$ te $1 \leq y < \frac{qx}{p}$ pa slijedi da A ima $\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor$ elemenata.

Slično se dobiva da skup B ima $\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{py}{q} \rfloor$ elemenata.

Iz prethodne leme dobivamo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{\frac{q-1}{2}} \lfloor \frac{xp}{q} \rfloor} \cdot (-1)^{\sum_{y=1}^{\frac{p-1}{2}} \lfloor \frac{yq}{p} \rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

Primjer 26. 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 $F_n = 2^{2^n} + 1$. Idućim rezultatom je dan efikasan kriterij za ispitivanje prostosti Fermatovih brojeva.

Propozicija 4.2.3. 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 Eulerovom kriteriju vrijedi $3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$.

Prema tome, dovoljno je dokazati da 3 nije kvadratni ostatak 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 $\left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Prema tome, 3 nije kvadratni ostatak modulo F_n . □

4.3 Jacobijev simbol

Jacobijev simbole je direktna 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, \dots, p_n prosti brojevi.

Jacobijev simbol $\left(\frac{a}{P}\right)$ je definiran 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 se nalazi 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 $1 \leq i \leq n$.

Direktno iz dokazanih svojstava Legendreova simbola se 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:

$$(1) \left(\frac{a}{P_1 P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right),$$

- (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 $\left(\frac{a^2}{P_1}\right) = \left(\frac{a}{P_1}\right)^2 = 1$,
(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 $P_1 = p_1 p_2 \cdots p_n$, p_i neparan prost za $i = 1, 2, \dots, n$.

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 $\sum_{i=1}^n \frac{p_i-1}{2} \equiv \frac{p_1 p_2 \cdots p_n - 1}{2} \equiv \frac{P_1 - 1}{2} \pmod{2}$. \square

4.4 Primjena kvadratnih ostataka na diofantske jednadžbe

U ovom kratkom potpoglavlju ćemo prikazati 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. \square

Teorem 4.4.2. *Neka je n prirodan broj. Ako diofantska jednadžba*

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

ima rješenja tada u rastavu broja n na proste faktora svaki prost faktor oblika $3k - 1$ dolazi s parnom potencijom.

Dokaz. Pretpostavimo da jednadžba iz iskaza teorema ima rješenja te neka je 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 $\left(\frac{-3}{p}\right) = 1$.

Nadalje, imamo $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)$. 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 p^2 dijeli i x^2 i y^2 pa p^2 dijeli i $x^2 + 3y^2 = n$. Dijeljenjem polazne jednačbe s p^2 dobivamo novu jednačbu $\left(\frac{x}{p}\right)^2 + 3\left(\frac{y}{p}\right)^2 = \frac{n}{p^2}$, te indukcijom slijedi da p u rastavu broja n na proste faktore dolazi s parnom potencijom. \square

Napomenimo kako vrijedi i obrat prethodnog teorema.

Poglavlje 5

GAUSSOVI CIJELI BROJEVI

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 se označava 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 se mogu 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) se može 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 $N(\alpha)$, za $\alpha = a + bi \in \mathbb{Z}[i]$ s $N(\alpha) = \alpha \cdot \bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2$.

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.

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

□

Iz ove leme direktno slijedi i tzv. Diofantov identitet, koji govori kako je produkt suma dvaju kvadrata ponovno suma dvaju kvadrata:

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

Primijetimo kako je Diofantov identitet ustvari 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 27. *Idući prikazi brojeva u obliku sume dvaju kvadrata su 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 $N(z) = z \cdot \bar{z}$. Također, tada za $z_1, z_2 \in \mathbb{C}$ vrijedi $N(z_1 z_2) = N(z_1)N(z_2)$.

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, se obično označava s α^{-1} .

Propozicija 5.1.2. *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 $\alpha \cdot \bar{\alpha} = N(\alpha) = 1$ 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 direktno 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 način se 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 28. $3 + 2i$ 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 5.2.1. *Svaki Gaussov cijeli broj se može 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 način ih 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, ovaj postupak mora stati nakon konačno mnogo koraka. Time dobivamo traženu faktorizaciju od α . □

Još preostaje prokomentirati jedinstvenost ovakve faktorizacije. U slučaju prirodnih brojeva, jedinstvenost dokazanu u Osnovnom teoremu aritmetike (Teorem 1.4.3) se oslanjala na Euklidov algoritam, ključno svojstvo za čiji dokaz je bilo dano Teoremom o dijeljenju s ostatkom (Teorem 1.1.2).

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 $\delta \mid \gamma$.

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

Teorem 5.2.2. *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, uzmimo $\alpha = 5 + 7i$ te $\beta = 2 + i$. Tada je

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

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 ,
- ako prost Gaussov cijeli broj β dijeli produkt $\alpha_1 \cdot \alpha_2 \cdots \alpha_n$, tada β dijeli α_i za neki $i \in \{1, 2, \dots, n\}$,

- 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 5.2.3. *Prost prirodan broj p je prost Gaussov cijeli broj ako i samo ako p nije suma dva 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 $a + bi, \gamma$ Gaussovi cijeli brojevi norme manje od p^2 . Konjugiranjem dobivamo $p = (a - bi)\bar{\gamma}$, 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 $p = a^2 + b^2$. \square

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

Propozicija 5.2.4. *Prosti Gaussovi cijeli brojevi $a + bi$, gdje je $a \cdot b \neq 0$, su faktori prostih prirodnih brojeva 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 $a + bi = \bar{\alpha} \cdot \bar{\beta}$).

Nadalje, $(a + bi)(a - bi)$ je jedinstven 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 bi na taj način dobili još neki rastav u produkt prostih Gaussovih cijelih brojeva. \square

5.3 Prikazi prirodnih brojeva u obliku sume dvaju kvadrata

Ukoliko je p prost prirodan broj oblika $4k + 3$, korištenjem kongruencija modulo 4 se lako 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:

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

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

Teorem 5.3.2 (Fermat). *Svaki prost broj p oblika $4k + 1$ se može 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 5.2.3 pokazuje da je p oblika $p = a^2 + b^2$ za neke cijele brojeve a, b . \square

Teorem 5.3.3. *Prirodan broj n se može 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 4.1.4.

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, \dots, p_l međusobno različiti prosti brojevi za koje vrijedi $p_i \equiv 1 \pmod{4}$, $1 \leq i \leq l$.

Prema Teoremu 5.3.2, svaki od prostih brojeva p_1, p_2, \dots, p_l se može prikazati u obliku sume kvadrata dvaju cijelih brojeva pa iz Diofantova identita (5.1) slijedi da se i broj n može prikazati u obliku sume kvadrata dvaju cijelih brojeva. \square

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 29. $(3,4,5)$ je primitivna Pitagorina trojka.

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 primitivnoj Pitagorinoj trojci je 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 ovaj identitet, pokažimo iduće rezultate:

Lema 5.4.1. *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 $\bar{\alpha}$ zajednički djelitelj tih brojeva (primijetimo da iz uvjeta $(x, y) = 1$ slijedi da α nije cijeli broj). No, tada je i produkt $\alpha \cdot \bar{\alpha}$ zajednički djelitelj od $x - yi, x + yi$, koji je prirodan broj veći od 1.

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 prosti Gaussovimi 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. \square

Lema 5.4.2. *Neka su $x - yi, x + yi$ relativno prosti Gaussovi cijeli brojevi takvi da je $(x - yi)(x + yi) = z^2$, za neki $z \in \mathbb{Z}[x]$, tada postoje $u_1, u_2, \alpha, \beta \in \mathbb{Z}[x]$, 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 $x - yi, x + yi$ nemaju zajedničkih prostih faktora, također se i svaki prost faktor od $x - yi, x + yi$ mora pojaviti s parnom potencijom. Produkt parnih potencija prostih faktora je očito potpun kvadrat. Kako su preostali faktori koji se mogu pojaviti jedino invertibilni elementi, $x - yi, x + yi$ se mogu prikazati u obliku produkata invertibilnih elemenata i potpunih kvadrata. \square

Prema prethodnim rezultatima, ako je (x, y, z) primitivna Pitagorina trojka, tada $x - yi$ ima jedan od slijedećih 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, 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, 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 $z = u^2 + v^2$.

Teorem 5.4.3. *Ako je (x, y, z) primitivna Pitagorina trojka, tada postoje relativno prosti prirodni brojevi u, v različite parnosti, $u > v$, takvi da je $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$.*

Sve Pitagorine trojke su dane identitetom

$$[d(u^2 - v^2)]^2 + (2d uv)^2 = [d(u^2 + v^2)]^2, d \in \mathbb{N}. \quad (5.2)$$

Primjer 30. *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 $u > v$, 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, 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.

Zaključimo ovo poglavlje posebnim slučajem Velikog Fermatova teorema. Započnimo idućom lemom, čiji dokaz koristi vrlo interesantnu metodu poznatu pod nazivom 'Fermatova metoda beskonačnog spusta'.

Lema 5.4.4. *Jednadžba $x^4 + y^4 = z^2$ nema rješenja u prirodnim brojevima.*

Dokaz. Pretpostavimo da postoji rješenje jednadžbe $x^4 + y^4 = z^2$ u prirodnim brojevima te neka je (x, y, z) trojka prirodna brojeva koja je rješenje s najmanjim z . Tada je (x^2, y^2, z) primitivna Pitagorina trojka, inače bi dijeljenjem s najvećim zajedničkim djeliteljem dobili rješenje s manjim z .

Dakle, postoje prirodni brojevi u, v takvi da je $x^2 = u^2 - v^2, y^2 = 2uv, z = u^2 + v^2$. Time dobivamo i novu primitivnu Pitagorinu trojku $x^2 + v^2 = u^2$, pa su y i v parni te možemo staviti $y = 2m$ i $v = 2n$. Uvrštavanjem u jednakost $y^2 = 2uv$ dobivamo $m^2 = un$. Kako su u i v relativno prosti, moraju i u i n biti relativno prosti pa su i potpuni kvadrati. Zapišimo ih u obliku $u = u_1^2, n = n_1^2$.

Iz primitivne Pitagorine trojke (x, v, u) slijedi da postoje i relativno prosti prirodni brojevi a, b takvi da je $x = a^2 - b^2$, $v = 2ab$, $u = a^2 + b^2$.

No, sada je, zbog $v = 2n = 2n_1^2$, $2ab = 2n_1^2$ pa je $ab = n_1^2$. Zbog $(a, b) = 1$, a i b su također potpuni kvadrati pa ih možemo zapisati u obliku $a = a_1^2$ i $b = b_1^2$. Uvrštavanjem u jednakost $u = a^2 + b^2$ dobivamo $a_1^4 + b_1^4 = u_1^2$. Kako je $u_1 < z$, dobivamo kontradikciju s minimalnošću od z . Dakle, polazna jednačba nema rješenja u prirodnim brojevima. \square

Direktna posljedica prethodne leme je

Teorem 5.4.5. *Jednačba $x^4 + y^4 = z^4$ nema rješenja u prirodnim brojevima.*

Poglavlje 6

PELLOVE JEDNADŽBE

6.1 Osnovni pojmovi i egzistencija rješenja

Pellovom jednadžbom se naziva diofantska jednadžba oblika

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

gdje je n prirodan broj koji nije potpun kvadrat. Neka otkrića u vezi ove jednadžbe su greškom od strane Eulera proglašena Pellovim, koji nije značajnije priodnio u njenom rješavanju.

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

U antičkoj Grčkoj je proučavan specijalan slučaj Pellove jednadžbe za $n = 2$, u kojem rješenja ove jednadžbe u prirodnim brojevima pružaju dodatne informacije o prirodni iracionalnog broja $\sqrt{2}$. Postoji i slična veza između rješenja Pellove jednadžbe u prirodnim brojevima s iracionalnim brojem \sqrt{n} (podsjetimo, 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 $(x_1, y_1), (x_2, y_2), \dots$ Pellove jednadžbe. Iz jednakosti $x_i^2 - ny_i^2 = 1$ slijedi $\frac{x_i^2}{y_i^2} = n + \frac{1}{y_i^2} \rightarrow n$ kada $y_i \rightarrow \infty$.

Prema tome, kvocijenti rješenja Pellove jednadžbe predstavljaju prirodne 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 prirodnim 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 cilj nam je pokazati kako Pellova jednadžba zaista uvijek ima rješenja. Ključni korak u tome je dan idućim 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 $\sqrt{n}, 2\sqrt{n}, \dots, (B-1)\sqrt{n}$. Za svaki $k \in \{1, 2, \dots, B-1\}$ odaberimo cijeli broj A_k takav da je $0 < A_k - k\sqrt{n} < 1$.

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 $0, A_1 - \sqrt{n}, A_2 - 2\sqrt{n}, \dots, A_{B-1} - (B-1)\sqrt{n}, 1$.

Podijelimo li segment $[0, 1]$ na B podintervala duljine $\frac{1}{B}$, prema Dirichletovom principu barem jedan podinterval sadrži barem 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 rješenja u prirodnim brojevima $(a, b) \neq (1, 0)$.*

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 ($a, b \in \mathbb{Z}$). 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 $N \mid a_1^2 - nb_1^2$, dobivamo $a_1^2 - nb_1^2 \equiv 0 \pmod{N}$, te iz $a_1 \equiv a_2 \pmod{N}$ te $b_1 \equiv b_2 \pmod{N}$ 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

Najmanje netrivialno 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 ovih jednadžbi u prirodnim brojevima nisu prevelika, te su redom dana s $(x, y) = (3, 2)$ te $(x, y) = (2, 1)$.

No, napomenimo kako je najmanje rješenje jednadžbe $x^2 - 61y^2 = 1$ jednako $(x, y) = (1766319049, 226153980)$! (Ovaj primjer je još u 12. stoljeću pronašao indijski matematičar Bhaskara II.)

Osnovna važnost u poznavanju najmanjeg netrivialnog rješenja leži u tome što ono daje 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 $(x_1 + \sqrt{ny_1})(x_2 + \sqrt{ny_2}) = x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)$.

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

$$\begin{aligned} 1 &= (x_1 - \sqrt{ny_1})(x_1 + \sqrt{ny_1})(x_2 - \sqrt{ny_2})(x_2 + \sqrt{ny_2}) \\ &= (x_1 - \sqrt{ny_1})(x_2 - \sqrt{ny_2})(x_1 + \sqrt{ny_1})(x_2 + \sqrt{ny_2}) \\ &= (x_1x_2 + ny_1y_2 - \sqrt{n}(x_1y_2 + x_2y_1))(x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)) \\ &= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + x_2y_1)^2 \\ &= x_3^2 - ny_3^2 \end{aligned}$$

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

Primjer 31. *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 6.2.2. *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 $x_2 + \sqrt{ny_2} = (x_1 + \sqrt{ny_1})^m$.*

Dokaz. Pretpostavimo da postoji rješenje (x_2, y_2) koje nije oblika $(x_1 + \sqrt{ny_1})^m$, za $m \in \mathbb{N}$. Kako je $x_1 + \sqrt{ny_1} > 1$ i $x_2 + \sqrt{ny_2} > 1$, postoji $k \in \mathbb{N}$ za koji vrijedi

$$(x_1 + \sqrt{ny_1})^k < x_2 + \sqrt{ny_2} < (x_1 + \sqrt{ny_1})^{k+1}.$$

Množenjem s $(x_1 - \sqrt{ny_1})^k$ dobivamo

$$1 < (x_2 + \sqrt{ny_2})(x_1 - \sqrt{ny_1})^k < x_1 + \sqrt{ny_1}.$$

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) je rješenje Pellove jednadžbe $x^2 - ny^2 = 1$ u prirodnim brojevima, koje je manje od rješenja (x_1, y_1) što nije moguće. \square

6.3 Određivanje rješenja Pellove jednadžbe

Netrivijalna rješenja Pellove jednadžbe $x^2 - ny^2 = 1$ se najlakše 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 beskonačni verižni razlomak $[a_1, a_2, \dots]$ 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 $[a_1, a_2, \dots]$ te pišemo

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

Prema Primjeru 6, 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 idućem 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 $[a_1, a_2, \dots]$ je dan razvoj broja \sqrt{n} u jednostavni verižni razlomak.

Primijetimo da je razvoj periodičan ako postoje prirodni brojevi i, j , $i \neq j$, takvi da je $(s_i, t_i) = (s_j, t_j)$. Može se pokazati kako vrijedi nejednakost $t_i < s_i + \sqrt{n} < 2\sqrt{n}$, iz koje slijedi kako brojevi s_i, t_i mogu poprimiti samo konačno mnogo vrijednosti, čime dobivamo idući 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 32. *Korištenjem prethodno opisanog postupka dobivamo $\sqrt{28} = [5, \overline{3, 2, 3, 10}]$.*

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 $[a_1, \overline{a_2, a_3, \dots, a_{m-1}, 2a_1}]$, gdje vrijedi $a_2 = a_{m-1}$, $a_3 = a_{m-2}$ itd.

Idućim teoremom su potpuno određena rješenja Pellove jednadžbe:

Teorem 6.3.2. *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 $\lfloor \sqrt{n} \rfloor$ se smatra 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 33. *Najmanje rješenje u prirodnim brojevima Pellove jednadžbe $x^2 - 28y^2 = 1$ je dano s $x = p_3 = 127$, $y = q_3 = 24$, jer je*

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

Bibliografija

- [1] T. Andreescu, D. Andrica: *An Introduction to Diophantine equations*; Gil Publishing House, 2002
- [2] A. Dujella: *Uvod u teoriju brojeva*; skripta, PMF - Matematički odsjek, Sveučilište u Zagrebu, 2003
- [3] H. M. Edwards: *Fermat's Last Theorem*; Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1977
- [4] G. A. Jones, J. M. Jones: *Elementary Number Theory*; Undergraduate Texts in Mathematics, Springer-Verlag, London, 2003
- [5] N. Koblitz: *A course in number theory and cryptography*; Graduate Texts in Mathematics, Springer-Verlag, New York, 1994
- [6] G. Savin: *Numbers, Groups and Cryptography*; skripta, Department of Mathematics, University of Utah, 2009
- [7] J. Stillwell: *Elements of Number Theory*; Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003