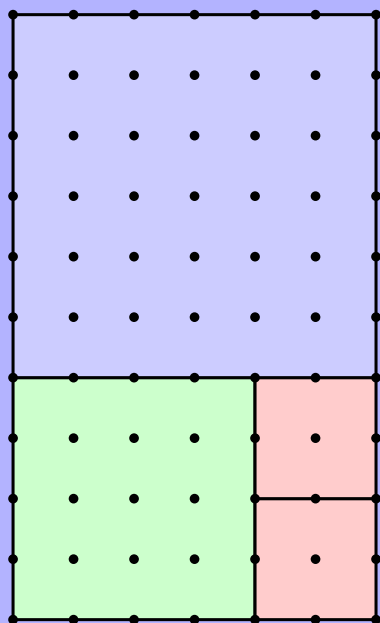
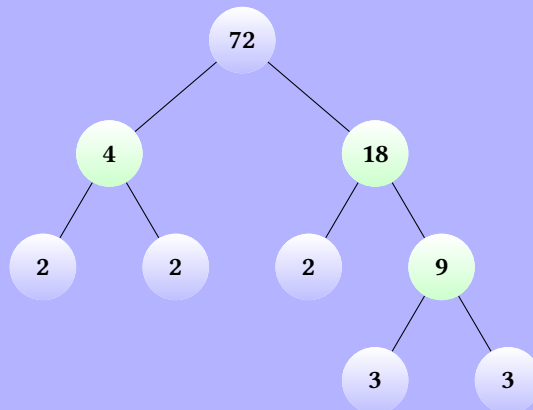




Mirela Jukić Bokun
Ivan Soldo



Zbirka zadataka iz teorije brojeva



Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Mirela Jukić Bokun, Ivan Soldo

ZBIRKA ZADATAKA IZ TEORIJE BROJEVA



Osijek, 2023.

Izdavač:

Sveučilište Josipa Jurja Strossmayera u Osijeku - Fakultet primijenjene matematike i informatike, Trg Ljudevita Gaja 6, HR-31 000 Osijek, Hrvatska

Odgovorna osoba izdavača:

Prof. dr. sc. Kristian Sabo

Recenzenti:

izv. prof. dr. sc. Zrinka Franušić, PMF - Matematički odsjek, Sveučilište u Zagrebu,

izv. prof. dr. sc. Ana Jursić, Fakultet za matematiku, Sveučilište u Rijeci

Lektor:

Marina Tomić, mag. educ. philol. croat.

Tehnička obrada:

izv. prof. dr. sc. Mirela Jukić Bokun, izv. prof. dr. sc. Ivan Soldo

Mjesec i godina objavljivanja publikacije:

rujan, 2023.

CIP zapis dostupan je u računalnom katalogu Gradske i sveučilišne knjižnice Osijek pod brojem 150822077.

ISBN 978-953-8154-22-5

Sveučilište Josipa Jurja Strossmayera u Osijeku



Suglasnost za izdavanje ovog sveučilišnog priručnika donio je Senat Sveučilišta Josipa Jurja Strossmayera u Osijeku na 11. sjednici u akademskoj godini 2022./2023. održanoj 27. rujna 2023. godine pod brojem 17/23.

Priručnik se tiska uz novčanu potporu Ministarstva znanosti i obrazovanja.

Tisak:

Studio HS Internet d.o.o., Osijek

*Matematika je kraljica znanosti, a teorija
brojeva kraljica je matematike.*

Carl Friedrich Gauss

Sadržaj

Predgovor	iii
1 Djeljivost	1
1. Definicija i osnovna svojstva djeljivosti	1
2. Euklidov algoritam	9
3. Prosti brojevi	15
4. Broj i zbroj svih pozitivnih djelitelja prirodnog broja	22
5. Zadatci za vježbu	27
Upute za rješavanje zadataka	29
2 Kongruencije	33
1. Definicija i osnovna svojstva kongruencija	33
2. Linearne kongruencije	37
3. Eulerova funkcija i Eulerov teorem	43
4. Primitivni korijeni i indeksi	48
5. Wilsonov i Lagrangeov teorem	52
6. Primjena kongruencija u kriptografiji	55
6.1. Pomak alfabeta ili Cezarova šifra	55
6.2. RSA kriptosustav	57
7. Zadatci za vježbu	58
Upute za rješavanje zadataka	62
3 Kvadratni ostatci	65
1. Legendreov simbol	65
2. Gaussov kvadratni zakon reciprociteta	69
3. Jacobijev simbol	72
4. Zadatci za vježbu	74
Upute za rješavanje zadataka	77

4	Diofantske jednažbe	81
1.	Linearne diofantske jednažbe	81
2.	Pitagorine trojke	84
3.	Pellove jednažbe	88
4.	Zadatci za vježbu	94
	Upute za rješavanje zadataka	97
	Literatura	101
	Kazalo	102

PREDGOVOR

Ova zbirka zadataka temelji se na nastavi - vježbama koje smo posljednjih godina vodili na drugoj godini *Prijediplomskog studija Matematika* na *Odjelu za matematiku* u sastavu *Sveučilišta Josipa Jurja Strossmayera u Osijeku* iz kolegija *Teorija brojeva*. Sastoji se od četiri poglavlja: *Djeljivost, Kongruencije, Kvadratni ostatci* i *Diofantske jednadžbe*. Gradivo se izlaže na primjeren i pristupačan način. Pritom su u tekstu dana kratka, ali temeljita teorijska objašnjenja koja se sastoje od rezultata potrebnih za uspješno praćenje gradiva. Potkrepljuju ih pomno odabrani i potpuno riješeni raznovrsni primjeri i zadaci. Sve te primjere i zadatke preporuča se pažljivo i temeljito proučiti. Gradivo se može temeljito svladati samo onda ako se riješi što veći broj raznovrsnih zadataka. Stoga nakon riješenih zadataka često slijedi odgovarajući zadatak za vježbu, a na kraju svakog poglavlja, nakon seta riješenih primjera i zadataka, slijede zadatci za samostalno rješavanje. Za zadatke koji nisu riješeni navedena su i njihova rješenja, a za neke postoje i upute za uspješno rješavanje. Sve to može pridonijeti boljem razumijevanju i usvajanju gradiva.

Literatura usko povezana sa sadržajem ovog priručnika navedena je na kraju zbirke zadataka i u njoj se može naći neophodan pregled najvažnijih pojmova i rezultata. Osim toga, može poslužiti i za nastavak samostalnog rada u području teorije brojeva. Na kraju priručnika nalazi se i indeks osnovnih pojmova.

Vjerujemo da će ovaj priručnik biti koristan nastavnicima i studentima i drugih fakulteta tijekom pripremanja nastave iz kolegija slične tematske strukture. Zahvaljujemo se recenzentima izv. prof. dr. sc. Zrinki Franušić i izv. prof. dr. sc. Ani Jursić te lektorici Marini Tomić, koji su svojim primjedbama i prijedlozima značajno pomogli da ovaj tekst bude bolji. Također, hvala svim studentima Fakulteta primijenjene matematike i informatike koji su na bilo koji način sudjelovali u pripremi završne verzije ove zbirke zadataka.

U Osijeku, 1. rujna 2023.

Mirela Jukić Bokun

Ivan Soldo

Djeljivost

1. Definicija i osnovna svojstva djeljivosti

Na početku ovoga odjeljka navest ćemo definiciju djeljivosti u skupu cijelih brojeva.

Definicija 1.1. *Neka su $a, b \in \mathbb{Z}, a \neq 0$. Ako postoji $d \in \mathbb{Z}$ takav da je $b = ad$ kažemo da a dijeli b i pišemo $a \mid b$. U tom slučaju kažemo da je a djelitelj od b te da je b višekratnik od a .*

Ako a ne dijeli b , pišemo $a \nmid b$.

Primjer 1.1. *Ako je $n \in \mathbb{Z}$ oblika $n = 5(k^2 + 1), k \in \mathbb{Z}$, onda $5 \mid n$.*

Zadatak 1.1. *Neka je $n \in \mathbb{Z}$. Ako $3 \mid n - 1$, dokažite da $3 \mid n + 2$.*

Rješenje. Ako $3 \mid n - 1$, onda postoji $d \in \mathbb{Z}$ takav da je $n - 1 = 3d$. Dodamo li i lijevoj i desnoj strani prethodne jednakosti broj 3, dobivamo $n + 2 = 3(d + 1)$. Zaključujemo da $3 \mid n + 2$. \diamond

Oznakom $\overline{a_{k-1}a_{k-2}\dots a_1a_0}$ označavamo prirodni broj n oblika

$$n = a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \dots + a_110 + a_0,$$
$$a_i \in \{0, 1, \dots, 9\}, i = 0, 1, \dots, k-1, a_{k-1} \neq 0.$$

Uočimo da tako zapisan prirodni broj n ima k znamenki.

Zadatak 1.2. *Ako je $a = \overline{xy}, b = \overline{yx}$, dokažite da $9 \mid a - b$.*

Rješenje. Iz $a = \overline{xy}, b = \overline{yx}$ slijedi

$$a = 10x + y,$$
$$b = 10y + x.$$

Odavde slijedi da je $a - b = 9(x - y)$, tj. $9 \mid a - b$. \diamond

Zadatak 1.3. Dokažite da je zbroj svake tri uzastopne potencije broja 3 djeljiv s 39.

Zadatak 1.4. Neka je $m \in \mathbb{N}$ pravi djelitelj prirodnog broja n , tj. $m \mid n$ i $m \neq n$. Dokažite da je $m \leq \frac{n}{2}$.

Rješenje. Budući da je m pravi djelitelj od n , postoji $d \in \mathbb{N}$, $d \neq 1$ takav da je $n = md$. Ako pretpostavimo da je $m > \frac{n}{2}$, dobivamo $2m > n = md$. Kako je $m > 0$, dijeljenjem prethodne nejednakosti s m dobivamo $d < 2$, tj. $d = 1$. Dolazimo, dakle, do kontradikcije s $d \neq 1$ pa zaključujemo da ne može vrijediti $m > \frac{n}{2}$. Stoga slijedi tvrdnja zadatka. \diamond

Zadatak 1.5. Neka su $a, b \in \mathbb{N}$, $ab = n$. Dokažite da je $a \leq \sqrt{n}$ ili $b \leq \sqrt{n}$.

Iz definicije djeljivosti lako se može zaključiti (dokažite to za vježbu) da vrijede svojstva navedena u sljedećoj propoziciji.

Propozicija 1.1. Neka su $a, b, c \in \mathbb{Z}$. Tada vrijedi:

- (1) ako $a \mid b$ i $b \mid c$, onda $a \mid c$,
- (2) ako $a \mid b$, $b \neq 0$, onda je $|a| \leq |b|$,
- (3) ako $a \mid b$ i $a \mid c$, onda $a \mid b + c$, $a \mid b - c$, $a \mid bc$,
- (4) ako $a \mid b$ i $b \mid a$, onda je $|a| = |b|$.

Zadatak 1.6. Neka je $n \in \mathbb{Z}$ takav da $5 \mid n + 2$. Koji je od sljedećih izraza djeljiv s 5:

- (a) $n^2 - 4$,
- (b) $n^2 + 4n$,
- (c) $n^2 + 8n + 17$,
- (d) $n^4 - 1$?

Rješenje. Iz $5 \mid n + 2$ slijedi da postoji $d \in \mathbb{Z}$ takav da vrijedi $n + 2 = 5d$.

- (a) Kako je $n^2 - 4 = (n - 2)(n + 2) = 5d(n - 2)$, slijedi da je $n^2 - 4$ djeljiv s 5.
- (b) Uočimo da vrijedi $n^2 + 4n = (n + 2)^2 - 4 = 25d^2 - 4 = 5k - 4$, $k = 5d^2$. Ako $5 \mid n^2 + 4n$, iz prethodnog izraza slijedi $5 \mid 5k - 4$, tj. $5 \mid -4$ pa dobivamo kontradikciju. Zaključujemo da izraz $n^2 + 4n$ nije djeljiv s 5.

(c) Iz

$$\begin{aligned} n^2 + 8n + 17 &= (n + 2)^2 + 4n + 13 \\ &= (n + 2)^2 + 4(n + 2) + 5 \\ &= 25d^2 + 20d + 5 \\ &= 5(5d^2 + 4d + 1) \end{aligned}$$

slijedi $5 \mid n^2 + 8n + 17$.

(d) Izraz $n^4 - 1$ dovodimo u vezu s $n + 2$ na sljedeći način:

$$\begin{aligned} n^4 - 1 &= n^4 - 16 + 15 \\ &= (n^2 - 4)(n^2 + 4) + 15 \\ &= (n - 2)(n + 2)(n^2 + 4) + 15. \end{aligned}$$

Kako je $n + 2 = 5d$, odavde, kao i ranije, zaključujemo da $5 \mid n^4 - 1$.

◇

Zadatak 1.7. *Odredite sve $n \in \mathbb{Z}$ sa svojstvom $n + 1 \mid n^2 + 1$.*

Rješenje. Odmah vidimo $n \neq -1$.

1. način: Uočimo da vrijedi

$$n^2 + 1 = n^2 - 1 + 2 = (n - 1)(n + 1) + 2.$$

Ako $n + 1 \mid n^2 + 1$, iz prethodne jednakosti zaključujemo $n + 1 \mid 2$. Cjelobrojni djelitelji broja 2 su $-1, 1, -2, 2$ pa je $n + 1 \in \{-2, -1, 1, 2\}$. Odavde slijedi $n \in \{-3, -2, 0, 1\}$.

2. način: Podijelimo li polinom $n^2 + 1$ polinomom $n + 1$, dobivamo

$$\frac{n^2 + 1}{n + 1} = n - 1 + \frac{2}{n + 1}.$$

Pretpostavka $n + 1 \mid n^2 + 1$ povlači da je $\frac{n^2 + 1}{n + 1} \in \mathbb{Z}$ pa zbog prethodne jednakosti vrijedi $\frac{2}{n + 1} \in \mathbb{Z}$. Odavde zaključujemo da $2 \mid n + 1$ pa nastavak ide kao u prvom načinu rješavanja. ◇

Zadatak 1.8. *Odredite sve $n, k \in \mathbb{Z}$ za koje je $k(n - 3) = 3n$.*

Zadatak 1.9. *Dokažite da postoji beskonačno mnogo različitih prirodnih brojeva a, b, c takvih da je zbroj svaka dva od njih djeljiv s trećim.*

Rješenje. Bez smanjenja općenitosti neka su $a, b, c \in \mathbb{N}$ takvi da je $a < b < c$ i pretpostavimo $a \mid b + c, b \mid a + c, c \mid a + b$. Tada postoje $d_1, d_2, d_3 \in \mathbb{N}$ takvi da vrijedi

$$b + c = ad_1, \quad (1.1)$$

$$a + c = bd_2, \quad (1.2)$$

$$a + b = cd_3. \quad (1.3)$$

Kako je $a < b < c$, iz (1.3) slijedi $a + b = cd_3 < 2c$. Odavde je $d_3 < 2$ pa je $d_3 = 1$ (jer je $d_3 \in \mathbb{N}$). Vrijedi, dakle,

$$a + b = c. \quad (1.4)$$

Uvrstimo li tu jednakost u (1.2), dobivamo $2a + b = bd_2$, odnosno $2a = b(d_2 - 1) < 2b$. Odavde je $0 < d_2 - 1 < 2$ pa je $d_2 = 2$, odnosno $b = 2a$. Jednakost (1.4) povlači $c = 3a$. No onda je $b + c = 5a$ pa zaključujemo da vrijedi (1.1) (uz $d_1 = 5$). Stoga brojevi oblika $a, 2a, 3a, a \in \mathbb{N}$ zadovoljavaju tražene uvjete i ima ih beskonačno mnogo. \diamond

Sljedeći rezultat sadrži važno svojstvo djeljivosti, ima široku primjenu i često će biti korišten u daljnjem tekstu.

Teorem 1.1. (Teorem o dijeljenju s ostatkom, [3]) *Za $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da vrijedi*

$$b = aq + r, \quad 0 \leq r < a.$$

Primjer 1.2. *Podijelimo li broj -21 s 5 , prema Teoremu o dijeljenju s ostatkom dobivamo $-21 = 5(-5) + 4$.*

Napomena 1.1. *Iz Teorema o dijeljenju s ostatkom zaključujemo da se, za $n \in \mathbb{N}$, proizvoljan $z \in \mathbb{Z}$ može zapisati u točno jednom od sljedećih oblika:*

$$nk, nk + 1, \dots, nk + n - 1,$$

za neki $k \in \mathbb{Z}$.

Primjer 1.3. *Cijeli broj n može biti paran ili neparan, tj. može se prikazati u obliku $2k$ ili $2k + 1$.*

Cijeli broj n može se prikazati u jednom od sljedećih oblika: $3k, 3k + 1, 3k + 2$.

Zadatak 1.10. *Dokažite da za svaki $n \in \mathbb{Z}$ vrijedi:*

- (a) $2 \mid n(n+1)$,
- (b) $3 \mid n^3 - n$.

Rješenje.

- (a) Ako je n paran, tj. postoji $k \in \mathbb{Z}$ takav da je $n = 2k$, onda $2 \mid n$ pa $2 \mid n(n+1)$. Ako je n neparan, tj. postoji $k \in \mathbb{Z}$ takav da je $n = 2k+1$, onda je $n+1 = 2(k+1)$ pa $2 \mid n+1$, odnosno $2 \mid n(n+1)$.

Zadatak smo mogli riješiti i tako da uočimo da je $n(n+1)$ umnožak dvaju uzastopnih cijelih brojeva pa je jedan od njih djeljiv s 2.

- (b) Kako je $n^3 - n = (n-1)n(n+1)$ umnožak triju uzastopnih cijelih brojeva, jedan od njih mora biti djeljiv s 3.

◇

Definicija 1.2. *Kažemo da je $n \in \mathbb{N}$ (potpun) kvadrat ako postoji $m \in \mathbb{N}$ takav da je $n = m^2$. Pišemo i $n = \square$.*

Zadatak 1.11. *Dokažite:*

- (a) *Ako je $n \in \mathbb{N}$ potpun kvadrat, onda je oblika $4k$ ili $4k+1$, za neki $k \in \mathbb{Z}$.*
- (b) *Ni jedan cijeli broj oblika $4k+3$ ne može se prikazati kao zbroj dvaju kvadrata.*
- (c) *Zbroj kvadrata dvaju neparnih cijelih brojeva ne može biti potpun kvadrat.*

Rješenje.

- (a) Kako se svaki cijeli broj može prikazati u obliku $2k$ ili $2k+1$, zaključujemo da su potpuni kvadrati sljedećeg oblika:

$$\begin{aligned}(2k)^2 &= 4k^2 = 4K, \\ (2k+1)^2 &= 4k^2 + 4k + 1 = 4(k^2 + k) + 1 = 4K + 1.\end{aligned}$$

Time je tvrdnja dokazana.

- (b) Provjerimo kojeg oblika može biti zbroj dvaju kvadrata, tj. zbroj oblika $x^2 + y^2$, $x, y \in \mathbb{Z}$. Prema prethodnoj tvrdnji, x^2, y^2 mogu biti oblika $4k$ ili $4k+1$. Promatranjem svih mogućih kombinacija dobivamo sljedeće:

x^2	y^2	$x^2 + y^2$
$4k$	$4l$	$4m$
$4k$	$4l + 1$	$4m + 1$
$4k + 1$	$4l + 1$	$4m + 2$
$4k + 1$	$4l$	$4m + 1$

Uočimo da je posljednji redak gornje tablice analogan drugom retku (jedan od kvadrata djeljiv je s 4, a drugi daje ostatak 1 pri dijeljenju s 4) i nije ga potrebno posebno razmatrati. Iz tablice zaključujemo da zbroj dvaju kvadrata ne može biti oblika $4m + 3$.

- (c) Iz tablice u prethodnom dijelu zadatka zaključujemo da je zbroj kvadrata dvaju neparnih cijelih brojeva oblika $4m + 2$, a prema prvom dijelu zadatka slijedi da broj oblika $4m + 2$ ne može biti potpun kvadrat.

◇

Zadatak 1.12. *Dokažite:*

- (a) *Kvadrat bilo kojeg cijelog broja je oblika $3k$ ili $3k + 1$, za neki $k \in \mathbb{Z}$.*
 (b) *Ako $3 \mid a^2 + b^2$, onda $3 \mid a$ i $3 \mid b$.*
 (c) *$\sqrt{3}$ iracionalan je broj.*
 (d) *Za sve $a, b \in \mathbb{Z}$ vrijedi $3 \mid ab(b^2 - a^2)$.*

Rješenje.

- (a) Kako se svaki cijeli broj može prikazati u obliku $3k$, $3k + 1$ ili $3k + 2$, analogno, kao u prethodnom zadatku, slijedi tvrdnja.
 (b) Neka $3 \mid a^2 + b^2$. Pretpostavimo $3 \nmid a$ ili $3 \nmid b$. To znači da 3 ne dijeli oba broja ili 3 jedan broj dijeli, a drugi ne dijeli. Prema prvom dijelu zadatka dobivamo:

a^2	b^2	$a^2 + b^2$
$3k + 1$	$3l$	$3m + 1$
$3k + 1$	$3l + 1$	$3m + 2$

Zaključujemo da $3 \nmid a^2 + b^2$ pa smo dobili kontradikciju.

- (c) Pretpostavimo da je $\sqrt{3} = \frac{p}{q}$ te da su p i q maksimalno skraćeni. Tada je $3 = \frac{p^2}{q^2}$, odnosno $p^2 = 3q^2$. Odavde zaključujemo da $3 \mid p^2$, a onda i $3 \mid p$ pa je $p = 3p_1$, za neki $p_1 \in \mathbb{Z}$. Uvrstimo li tu relaciju u $p^2 = 3q^2$, dobivamo $q^2 = 3p_1^2$. Odavde zaključujemo da $3 \mid q^2$, odnosno $3 \mid q$. Zaključili smo da su i p i q djeljivi s 3 pa nisu maksimalno skraćeni i time smo došli do kontradikcije.
- (d) Ako $3 \mid a$ ili $3 \mid b$, onda $3 \mid ab(b^2 - a^2)$. U suprotnom $3 \nmid a$ i $3 \nmid b$ pa je prema prvom dijelu zadatka $a^2 = 3k + 1$, a $b^2 = 3l + 1$. No onda je $a^2 - b^2 = 3(k - l)$ pa $3 \mid a^2 - b^2$, odnosno $3 \mid ab(b^2 - a^2)$. Time je tvrdnja dokazana.

◇

Zadatak 1.13. *Dokažite:*

- (a) Četvrta potencija bilo kojeg cijelog broja je oblika $5k$ ili $5k + 1$.
- (b) Za sve $a, b \in \mathbb{Z}$ vrijedi $5 \mid ab(a^4 - b^4)$.

Uočimo da su u prvim tvrdnjama prethodnih triju zadataka dani mogući oblici nekih potencija cijelih brojeva i mogu se koristiti pri rješavanju zadataka vezanih uz djeljivost.

Zadatak 1.14. *Dokažite da razlika dvaju susjednih potpunih kubova nije djeljiva s 2.*

Zadatak 1.15. *Pokažite da je svaki cijeli broj oblika $6k + 5$ uvijek i oblika $3m + 2$, ali obrat ne vrijedi.*

Rješenje. Kako je

$$6k + 5 = 3(2k + 1) + 2 = 3m + 2,$$

tvrdnja je zadovoljena. Kako bismo pokazali da obrat tvrdnje ne vrijedi, trebamo naći kontraprimjer. Jasno je da vrijedi $8 = 3 \cdot 2 + 2$. Međutim, $8 = 6k + 5$ povlači $k = \frac{1}{2}$, što je nemoguće. ◇

Zadatak 1.16. *Dokažite da je kub bilo kojeg cijelog broja oblika $9k$, $9k + 1$ ili $9k - 1$.*

Definicija 1.3. *Neka su $a, b \in \mathbb{Z}$. Ako $d \mid a$ i $d \mid b$, onda je d zajednički djelitelj brojeva a i b . Ako je barem jedan od brojeva a i b različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja brojeva a i b . Najveći takav djelitelj naziva se najveći zajednički djelitelj brojeva a i b i označava se s $s(a, b)$.*

Analogno, (a_1, \dots, a_n) najveći je zajednički djelitelj brojeva a_1, \dots, a_n koji nisu svi jednaki 0.

Iz definicije je jasno da vrijedi $(a, b) \in \mathbb{N}$ i $(a, b) = (b, a) = (-a, b)$.

Definicija 1.4. *Ako je $(a, b) = 1$, kažemo da su a i b relativno prosti brojevi. Analogno, ako je $(a_1, \dots, a_n) = 1$, kažemo da su a_1, \dots, a_n relativno prosti brojevi.*

Ako je $(a_i, a_j) = 1, i \neq j, i, j \in \{1, 2, \dots, n\}$, kažemo da su a_1, \dots, a_n u parovima relativno prosti brojevi.

Zadatak 1.17. *Ako su a_1, \dots, a_n u parovima relativno prosti, onda su i relativno prosti. Obrat te tvrdnje ne vrijedi. Dokažite.*

Rješenje. Neka su a_1, \dots, a_n u parovima relativno prosti i neka je $d = (a_1, \dots, a_n)$. Kako $d \mid a_1$ i $d \mid a_2$ slijedi da je d zajednički djelitelj brojeva a_1 i a_2 . Kako su a_1 i a_2 relativno prosti i $d \in \mathbb{N}$, slijedi $d = 1$.

Da bismo pokazali da relativno prosti brojevi ne moraju biti u parovima relativno prosti, promotrimo sljedeći primjer: $(2, 3, 6) = 1$, ali $(2, 6) = 2$. \diamond

Zadatak 1.18. *Dokažite:*

(a) *Ne postoje $a, b \in \mathbb{Z}$ takvi da je $(a, b) = 3$ i $a + b = 65$.*

(b) *Postoje $a, b \in \mathbb{Z}$ takvi da je $(a, b) = 5$ i $a + b = 65$.*

Rješenje.

(a) *Pretpostavimo da postoje $a, b \in \mathbb{Z}$ sa svojstvom $(a, b) = 3$ i $a + b = 65$. Kako $3 \mid a$ i $3 \mid b$, iz $a + b = 65$ dobili bismo $3 \mid 65$ pa bismo imali kontradikciju.*

(b) *Neka su $a, b \in \mathbb{Z}$ takvi da je $(a, b) = 5$ i $a + b = 65$. Tada je $a = 5x, b = 5y$, za neke $x, y \in \mathbb{Z}$ te je*

$$65 = a + b = 5(x + y).$$

Oдавде je $x + y = 13$ pa postoji beskonačno mnogo takvih cijelih brojeva i određeni su s $y = 13 - x, x \in \mathbb{Z}$.

\diamond

2. Euklidov algoritam

Pojam najvećeg zajedničkog djelitelja dvaju cijelih brojeva a i b susreli smo već u osnovnoj i srednjoj školi. Sada ćemo opisati Euklidov algoritam, vrlo učinkovitu metodu za pronalaženje najvećeg zajedničkog djelitelja dvaju cijelih brojeva. Euklidov algoritam jedan je od najstarijih algoritama. Spominje se u djelu *Elementi* koje je napisao Euklid (4.-3. st. pr. Kr.) te je tako i dobio ime.

Neka je $a \in \mathbb{N}$, $b \in \mathbb{Z}$. Pretpostavimo da smo uzastopnom primjenom Teorema o dijeljenju s ostatkom dobili sljedeći niz jednakosti:

$$\begin{aligned}
 b &= aq_1 + r_1, & 0 < r_1 < a, \\
 a &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2, \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2.1}$$

Tada je $r_n = (a, b)$ (vidi [3]).

Lako se vidi da je r_1 , a onda i r_2 pa i svaki r_i , $i \in \{1, 2, \dots, n\}$ cjelobrojna linearna kombinacija brojeva a i b . Stoga postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$ax_0 + by_0 = (a, b).$$

Prethodna jednakost naziva se Bézoutov identitet. Odavde slijedi da jednačba $ax + by = (a, b)$ ima rješenje. To je primjer linearne diofantske jednačbe s dvjema nepoznicama. Diofantske jednačbe su jednačbe kod kojih tražimo rješenja u skupu cijelih brojeva. Više o ovoj temi bit će navedeno u četvrtom poglavlju ove zbirke zadataka.

Napomena 2.1.

- (1) Množenjem svake jednakosti u Euklidovom algoritmu s $d > 0$ dobiva se $(da, db) = d(a, b)$.
- (2) Iz Bézoutovog identiteta odmah slijedi da ako $d \mid a$ i $d \mid b$, onda $d \mid (a, b)$.

Primjer 2.1. *Euklidovim algoritmom odredimo $(819, 165)$. Vrijedi*

$$\begin{aligned} 819 &= 165 \cdot 4 + 159, \\ 165 &= 159 \cdot 1 + 6, \\ 159 &= 6 \cdot 26 + 3, \\ 6 &= 3 \cdot 2. \end{aligned}$$

Zaključujemo da je $(819, 165) = 3$. Iz prethodnog niza jednakosti slijedi

$$\begin{aligned} 3 &= 159 - 6 \cdot 26 \\ &= 159 - (165 - 159)26 \\ &= 27 \cdot 159 - 26 \cdot 165 \\ &= 27(819 - 4 \cdot 165) - 26 \cdot 165 \\ &= 27 \cdot 819 - 134 \cdot 165. \end{aligned}$$

Stoga je $(x, y) = (27, -134)$ jedno rješenje diofantske jednadžbe

$$819x + 165y = (819, 165).$$

Teorem 2.1. ([3]) *Neka su $a, b \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{Z}$. Jednadžba $ax + by = m$ ima cjelobrojnih rješenja ako i samo ako $(a, b) \mid m$.*

Lako se vidi da iz prethodnog teorema slijedi sljedeći korolar.

Korolar 2.1. *Vrijedi: $(a, b) = 1$ ako i samo ako jednadžba $ax + by = 1$ ima cjelobrojnih rješenja.*

Primjer 2.2. *Uočimo da za svaki $k \in \mathbb{Z}$ vrijedi jednakost*

$$6(7k + 6) + (-7)(6k + 5) = 1.$$

Prethodni korolar povlači da je $(7k + 6, 6k + 5) = 1$, za svaki $k \in \mathbb{Z}$.

Zadatak 2.1. *Neka je $n \in \mathbb{N}$. Odredite $d = (n! + 1, (n + 1)! + 1)$.*

Rješenje. Kako je

$$n = (n + 1)(n! + 1) - 1 \cdot [(n + 1)! + 1],$$

slijedi da $d \mid n$. No kako $d \mid n! + 1$, odavde slijedi da $d \mid 1$. Zaključujemo da je $d = 1$. \diamond

Zadatak 2.2. *Ako je $(a, b) = 1$, odredite sve moguće vrijednosti parametra $d = (2a + b, a + 2b)$.*

Rješenje. Uočimo da d dijeli svaku linearnu kombinaciju brojeva $2a + b$ i $a + 2b$, tj. $d \mid (2a + b)x + (a + 2b)y$, za sve $x, y \in \mathbb{Z}$. Za $x = 2, y = -1$ dobivamo da $d \mid 3a$, a za $x = -1, y = 2$ dobivamo da $d \mid 3b$. Iz $d \mid 3a$ i $d \mid 3b$ slijedi $d \mid (3a, 3b) = 3(a, b) = 3$ (primijeni se svojstvo (1) iz Napomene 2.1.). Zaključujemo da je $d = 1$ ili $d = 3$. Pokažimo još da se obje vrijednosti dostižu: za $a = b = 1$ dobiva se $d = 3$, a za $a = 1, b = 2$ dobiva se $d = 1$. \diamond

Slijedeći zadatak sadrži neka korisna svojstva najvećeg zajedničkog djelitelja dvaju cijelih brojeva i može se koristiti u rješavanju idućih zadataka.

Zadatak 2.3. *Koristeći Bézoutov identitet dokažite da vrijedi:*

- (a) *Ako $a \mid c, b \mid c$ i $(a, b) = 1$, onda $ab \mid c$.*
- (b) *Ako je $(a, b) = d, a = xd, b = yd$, onda je $(x, y) = 1$.*
- (c) *Ako $a \mid bc$ i $(a, b) = 1$, onda $a \mid c$.*
- (d) *Ako je $(a, b) = 1, (a, c) = 1$, onda je $(a, bc) = 1$.*

Rješenje. Pokazat ćemo samo tvrdnju (a), a ostale se mogu dokazati za vježbu. Iz $a \mid c$ i $b \mid c$ slijedi $c = ax$ i $c = by$, za neke $x, y \in \mathbb{Z}$, dok iz $(a, b) = 1$ slijedi kako postoje $u, v \in \mathbb{Z}$ sa svojstvom $au + bv = 1$. Množenjem te jednakosti s c dobiva se $acu + bcv = c$. Uvrštavanjem jednakosti $c = by$ umjesto broja c u prvom izrazu s lijeve strane te uvrštavanjem $c = ax$ umjesto broja c u drugom izrazu s lijeve strane dobivamo

$$ab(uy + xv) = c.$$

Slijedi $ab \mid c$. \diamond

Napomena 2.2.

- (1) *Uočite da iz $a \mid c$ i $b \mid c$ ne mora slijediti da $ab \mid c$ (tj. uvjet $(a, b) = 1$ u prethodnom zadatku je nužan). Primjerice, $2 \mid 12$ i $4 \mid 12$, ali $8 \nmid 12$.*
- (2) *Metodom matematičke indukcije može se pokazati da vrijedi sljedeće poopćenje tvrdnje iz prethodnog zadatka: Ako $m_i \mid c, i = 1, \dots, n$ i m_1, \dots, m_n su u parovima relativno prosti brojevi, onda $m_1 \cdots m_n \mid c$.*

Zadatak 2.4. *Dokažite da $6 \mid n(n + 1)(2n + 1)$, za sve $n \in \mathbb{Z}$.*

Rješenje. Ranije smo se već podsjetili da $2 \mid n(n+1)$ pa odmah slijedi $2 \mid n(n+1)(2n+1)$.

Promotrimo sada djeljivost s 3. Ako $3 \mid n$ ili $3 \mid n+1$, slijedi $3 \mid n(n+1)(2n+1)$. Ako $3 \nmid n$ i $3 \nmid n+1$, onda $3 \mid n+2$ pa postoji $k \in \mathbb{Z}$ takav da je $n+2 = 3k$, tj. $n = 3k-2$. No onda je $2n+1 = 3(2k-1)$ pa zaključujemo da $3 \mid 2n+1$, odnosno $3 \mid n(n+1)(2n+1)$.

Kako $2 \mid n(n+1)(2n+1)$, $3 \mid n(n+1)(2n+1)$ i $(2, 3) = 1$, zaključujemo da vrijedi tvrdnja. \diamond

Zadatak 2.5. *Dokažite da je za svaki $n \in \mathbb{Z}$ broj $n^5 - n$ djeljiv s 30, a ako je n neparan, onda je djeljiv i s 240.*

Zadatak 2.6. *Neka su $a, b, c \in \mathbb{Z}$ takvi da $6 \mid a + b + c$. Dokažite da $6 \mid a^3 + b^3 + c^3$.*

Rješenje. Znamo da postoji $k \in \mathbb{Z}$ takav da je $a + b + c = 6k$. Uočimo da vrijedi

$$\begin{aligned} a^3 + b^3 + c^3 &= a^3 + b^3 + c^3 - a - b - c + a + b + c \\ &= a^3 - a + b^3 - b + c^3 - c + 6k. \end{aligned} \quad (2.2)$$

Ranije smo već pokazali (Zadatak 1.10.) da $3 \mid n^3 - n$, za sve $n \in \mathbb{Z}$. Analogno se zaključi da $2 \mid n^3 - n$. Kako je $(2, 3) = 1$, zaključujemo da $6 \mid n^3 - n$, za sve $n \in \mathbb{Z}$. Odavde slijedi da $6 \mid (a^3 - a) + (b^3 - b) + (c^3 - c)$. Iz (2.2) onda dobivamo da $6 \mid a^3 + b^3 + c^3$. \diamond

Zadatak 2.7. *Neka su $n, n_1, n_2 \in \mathbb{N}$ takvi da $n \mid n_1 n_2$ i ni jedan od brojeva n_1 i n_2 nije djeljiv s n . Dokažite da je broj*

$$d = \frac{n_1}{\left(n_1, \frac{n_1 n_2}{n}\right)} \quad (2.3)$$

djelitelj broja n i $1 < d < n$.

Rješenje. Iz (2.3) slijedi

$$\left(n_1, \frac{n_1 n_2}{n}\right) = \frac{n_1}{d}. \quad (2.4)$$

Iz Bézoutovog identiteta zaključujemo da postoje $x, y \in \mathbb{Z}$ takvi da vrijedi

$$n_1 x + \frac{n_1 n_2}{n} y = \frac{n_1}{d}.$$

Množenjem prethodne jednakosti s $\frac{d}{n_1}$ dobivamo

$$dx + \frac{n_2 dy}{n} = 1. \quad (2.5)$$

Odavde zaključujemo da je $\frac{n_2 dy}{n} \in \mathbb{Z}$ pa postoji $k \in \mathbb{Z}$ takav da je $n_2 dy = nk$. Uvrštavanjem te jednakosti u (2.5) dobivamo $dx + k = 1$. Prema Korolaru 2.1. je $(d, k) = 1$, a zatim $n_2 dy = nk$ povlači da $d \mid n$, što je i trebalo pokazati.

Uočimo da je d zadan s (2.4) prirodni broj. Kako je, uz to, i djelitelj broja n , zaključujemo da je $1 \leq d \leq n$. Dokažimo da je $d \neq 1$ i $d \neq n$. Uočimo da vrijedi:

- Ako je $d = 1$, onda bi prema (2.4) zaključili $n_1 \mid \frac{n_1 n_2}{n}$. No onda bi postojao t takav da je $\frac{n_1 n_2}{n} = tn_1$, odnosno $n_2 = tn$, tj. $n \mid n_2$. Time smo došli do kontradikcije.
- Ako je $d = n$, onda iz (2.4) slijedi $(n_1, \frac{n_1 n_2}{n}) = \frac{n_1}{n}$, odnosno $n \mid n_1$ što je opet kontradikcija.

Time je pokazano da je $1 < d < n$. ◇

Napomena 2.3. *Ako su q_i i r_i kao u Euklidovom algoritmu (2.1), onda se jedno rješenje jednadžbe $bx + ay = (a, b)$ može dobiti na sljedeći način:*

$$\begin{aligned} x_{-1} &= 1, & x_0 &= 0, & x_i &= x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, & y_0 &= 1, & y_i &= y_{i-2} - q_i y_{i-1}; \end{aligned} \quad i = 1, 2, \dots, n,$$

$$bx_n + ay_n = (a, b).$$

Ova tvrdnja dokazuje se matematičkom indukcijom.

Algoritam koji se temelji na Euklidovom algoritmu, a kojim se, osim najvećeg zajedničkog djelitelja dvaju brojeva, određuje i rješenje polazne linearne diofantske jednadžbe naziva se prošireni Euklidov algoritam.

Zadatak 2.8. *Dokažite da, uz oznake kao u prethodnoj napomeni, za $i = 0, \dots, n + 1$ vrijedi*

$$x_{i-1} y_i - x_i y_{i-1} = (-1)^i$$

te $(x_i, y_i) = 1$.

Primjer 2.3. *Odredimo $x, y \in \mathbb{Z}$ takve da vrijedi:*

$$237x + 173y = (237, 173).$$

Primijenimo li Euklidov algoritam na brojeve $a = 237, b = 173$, dobivamo sljedeći niz jednakosti:

$$\begin{aligned}
 237 &= 173 \cdot 1 + 64, \\
 173 &= 64 \cdot 2 + 45, \\
 64 &= 45 \cdot 1 + 19, \\
 45 &= 19 \cdot 2 + 7, \\
 19 &= 7 \cdot 2 + 5, \\
 7 &= 5 \cdot 1 + 2, \\
 5 &= 2 \cdot 2 + 1, \\
 2 &= 2 \cdot 1.
 \end{aligned}$$

Dakle, uočavamo da je $(237, 173) = 1$. Korištenjem rekurzivnih formula iz Napomene 2.3. vrlo brzo i efikasno možemo dobiti rješenje (x, y) polazne jednadžbe. Račun pišemo u sljedećem tabličnom obliku:

i	-1	0	1	2	3	4	5	6	7
q_i			1	2	1	2	2	1	2
x_i	1	0	1	-2	3	-8	19	-27	73
y_i	0	1	-1	3	-4	11	-26	37	-100

Dakle, $(x, y) = (x_7, y_7) = (73, -100)$.

Zadatak 2.9. Odredite $x, y \in \mathbb{Z}$ takve da vrijedi

$$50x + 71y = 1.$$

Rješenje. Primjenom Euklidova algoritma dobivamo:

$$\begin{aligned}
 50 &= 71 \cdot 0 + 50, \\
 71 &= 50 \cdot 1 + 21, \\
 50 &= 21 \cdot 2 + 8, \\
 21 &= 8 \cdot 2 + 5, \\
 8 &= 5 \cdot 1 + 3, \\
 5 &= 3 \cdot 1 + 2, \\
 3 &= 2 \cdot 1 + 1, \\
 2 &= 1 \cdot 2.
 \end{aligned}$$

Uočimo da je $50 > 71$ pa je prvi kvocijent jednak 0 i u sljedećoj tablici imamo jednu iteraciju više no što je uobičajeno, tj.:

i	-1	0	1	2	3	4	5	6	7
q_i			0	1	2	2	1	1	1
x_i	1	0	1	-1	3	-7	10	-17	27
y_i	0	1	0	1	-2	5	-7	12	-19

Rješenje polazne jednadžbe je $(x, y) = (x_7, y_7) = (27, -19)$.

Napomenimo kako zadatak možemo riješiti i uvođenjem supstitucije $x = Y, y = X$ pa potpuno analogno promatramo jednadžbu $71X + 50Y = 1$. Tako bismo u prethodnoj tablici izbjegli dodatnu iteraciju i prvi bi nam kvocijent bio različit od nule. \diamond

Zadatak 2.10. *Odredite $x, y \in \mathbb{Z}$ takve da vrijedi*

$$435x - 303y = (435, 303).$$

3. Prosti brojevi

Proučavanje prostih brojeva oduvijek je bio vrlo važan dio teorije brojeva. Njima su se bavili i starogrčki matematičari već u četvrtom stoljeću prije Krista. U ovom ćemo odjeljku istaknuti osnovna svojstva prostih brojeva i njihovu ulogu u faktorizaciji prirodnih brojeva te ćemo pokazati primjenu navedenih svojstava u rješavanju zadataka.

Definicija 3.1. *Neka je $n \in \mathbb{N}, n > 1$. Ako su 1 i n jedini pozitivni djelitelji broja n , kažemo da je n prosti broj. U suprotnom je n složen broj.*

Primjer 3.1. *Ako je p prosti broj i $p = ab, a, b \in \mathbb{N}$, onda mora biti $a = 1$ ($i b = p$) ili $b = 1$ ($i a = p$).*

Zadatak 3.1. *Odredite sve $n \in \mathbb{N}$ za koje je $n^2 - 1$ prosti broj.*

Rješenje. Kako je $n^2 - 1 = (n-1)(n+1)$, n je prirodni broj i $n-1 < n+1$, zaključujemo da mora biti $n-1 = 1$, tj. $n = 2$. Jer je $2^2 - 1 = 3$ prosti broj, zaključujemo da je $n = 2$ jedini mogući prirodni broj s tim svojstvom. \diamond

Napomena 3.1. Pogledajmo moguće oblike cijelih brojeva i odgovarajuće oblike prostih brojeva:

$z \in \mathbb{Z}$	p prost
$2k, 2k + 1$	$2, 2k + 1$
$3k, 3k + 1, 3k + 2$	$3, 3k + 1, 3k + 2$
$4k, 4k + 1, 4k + 2, 4k + 3$	$2, 4k + 1, 4k + 3$
$6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$	$2, 3, 6k + 1, 6k + 5$

Teorem 3.1. (Osnovni teorem aritmetike, [3]) Svaki prirodni broj veći od 1 može se prikazati u obliku umnoška prostih brojeva. Ta faktorizacija jedinstvena je do na poredak prostih faktora.

Prema Osnovnom teoremu aritmetike zaključujemo da za svaki $n \in \mathbb{N}, n \geq 2$ postoje $\alpha_i \in \mathbb{N}$ i p_i prosti brojevi za $i \in \{1, 2, \dots, k\}$ takvi da vrijedi

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Prethodni rastav naziva se kanonski rastav broja n na proste faktore.

Teorem 3.2. ([3]) Prostih brojeva ima beskonačno mnogo.

Kanonski rastav prirodnog broja n na proste faktore može se zapisati i na ovaj način:

$$n = \prod_{p \text{ prost}} p^{\alpha_p}, \quad \alpha_p \in \mathbb{N}_0,$$

pri čemu je $\alpha_p = 0$ ako $p \nmid n$. Stoga u gornjem rastavu samo za konačno mnogo prostih brojeva p vrijedi $\alpha_p \neq 0$. Napomenimo da ćemo u takvom zapisu u nastavku podrazumijevati da umnožak ide po prostim brojevima p te ćemo ispuštati opis "prost".

Zadatak 3.2. Dokažite da prostih brojeva oblika $4k + 3$ ima beskonačno mnogo.

Rješenje. Pretpostavimo suprotno, tj. da prostih brojeva oblika $4k + 3$ ima konačno mnogo. Neka su to brojevi p_1, \dots, p_n . Promotrimo broj

$$M = 4p_1 \cdots p_n - 1.$$

Uočimo da je M neparan pa nije djeljiv s 2 i mogući prosti faktori od M oblika su $4k + 1$ ili $4k + 3$. Nadalje, M ne može imati proste faktore oblika $4k + 3$ jer nije djeljiv ni s jednim $p_i, i = 1, \dots, n$. Stoga su svi prosti djelitelji

broja M oblika $4k + 1$. Lako se vidi da je umnožak konačno mnogo brojeva oblika $4k + 1$ opet broj oblika $4k + 1$ pa zaključujemo da je M oblika $4k + 1$. Kako je

$$M = 4p_1 \cdots p_n - 1 = 4p_1 \cdots p_n - 4 + 3 = 4m + 3, \quad m = p_1 \cdots p_n - 1,$$

polazna pretpostavka dovela nas je do kontradikcije pa prostih brojeva oblika $4k + 3$ ima beskonačno mnogo. \diamond

Definicija 3.2. *Neka su $a, b \in \mathbb{Z} \setminus \{0\}$. Najmanji prirodni broj koji je djeljiv i sa a i sa b naziva se najmanji zajednički višekratnik brojeva a i b , a označava se s $[a, b]$.*

Analogno se definira najmanji zajednički višekratnik brojeva $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ i označava s $[a_1, \dots, a_n]$.

Primjer 3.2. *Najmanji zajednički višekratnik brojeva 36 i 24 je 72, tj. $[36, 24] = 72$.*

Prisjetimo se: najmanji zajednički višekratnik u školskoj matematici pojavljuje se prilikom određivanja najmanjeg zajedničkog nazivnika dvaju razlomaka.

Napomena 3.2. *Ako je $a = \prod_p p^{\alpha_p}, b = \prod_p p^{\beta_p}$, onda vrijedi*

$$(1) \quad a \mid b \text{ povlači da je } \alpha_p \leq \beta_p,$$

$$(2) \quad (a, b) = \prod_p p^{\min\{\alpha_p, \beta_p\}},$$

$$(3) \quad [a, b] = \prod_p p^{\max\{\alpha_p, \beta_p\}},$$

$$(4) \quad (a, b)[a, b] = ab.$$

Zadatak 3.3. *Odredite sve $a, b \in \mathbb{N}$ za koje vrijedi $a \geq b, (a, b) = 10$ i $[a, b] = 100$.*

Rješenje. Uočimo da je $(a, b) = 2 \cdot 5, [a, b] = 2^2 \cdot 5^2$ i mora biti $ab = 2^3 \cdot 5^3$. Stoga je $a = 2^{\alpha_2} 5^{\alpha_5}, b = 2^{\beta_2} 5^{\beta_5}$. Iz uvjeta zadatka slijedi da je $\min\{\alpha_2, \beta_2\} = 1, \max\{\alpha_2, \beta_2\} = 2$ pa je $(\alpha_2, \beta_2) \in \{(1, 2), (2, 1)\}$. Analogno je $\min\{\alpha_5, \beta_5\} = 1, \max\{\alpha_5, \beta_5\} = 2$ pa je $(\alpha_5, \beta_5) \in \{(1, 2), (2, 1)\}$. Uvjet $a \geq b$ daje sljedeće moguće slučajeve:

- $\alpha_2 = 2, \alpha_5 = 2, \beta_2 = 1, \beta_5 = 1$, tj. tj. $a = 100, b = 10$,

- $\alpha_2 = 2, \alpha_5 = 1, \beta_2 = 1, \beta_5 = 2$, tj. $a = 50, b = 20$.

◇

Zadatak 3.4. *Ako je $n \in \mathbb{N}$ složen broj, dokažite da on ima prosti faktor $p \leq \sqrt{n}$.*

Rješenje. Neka je $n \in \mathbb{N}$ složen broj i pretpostavimo da je p najmanji prosti faktor od n . Tada postoji $m \geq p$ takav da $n = pm$. Iz $p \leq m$ slijedi $n = pm \geq p^2$, tj. $p \leq \sqrt{n}$. ◇

Napomena 3.3. *Iz prethodnog zadatka slijedi da ako prirodni broj n nema prosti faktor $p \leq \sqrt{n}$, onda je on prosti broj. Ta tvrdnja može se iskoristiti za generiranje tablice prostih brojeva tzv. Eratostenovim sitom.*

Primjerice, ako je m prirodni broj i ako želimo napisati sve proste brojeve koji se pojavljuju u nizu $2, 3, 4, \dots, m$, dovoljno je iz toga niza za svaki prosti broj $p \leq \sqrt{m}$ obrisati sve njegove višekratnike $kp, k > 1$. Tako je za $m = 300$ dovoljno obrisati sve prave višekratnike prostih brojeva do uključivo 17 (jer je već $19 > \sqrt{300}$). Svi su neobrisani brojevi prosti.

Zadatak 3.5. *Nadite $n \in \mathbb{N}$ sa svojstvom da je $\frac{n}{2}$ potpun kvadrat, $\frac{n}{3}$ potpun kub i $\frac{n}{5}$ peta potencija nekog prirodnog broja.*

Rješenje. Ako pretpostavimo da je $\frac{n}{2}$ potpun kvadrat, $\frac{n}{3}$ potpun kub i $\frac{n}{5}$ peta potencija nekog prirodnog broja, onda postoje $a, b, c \in \mathbb{N}$ takvi da je

$$\frac{n}{2} = a^2, \quad \frac{n}{3} = b^3, \quad \frac{n}{5} = c^5. \quad (3.1)$$

Iz pretpostavki slijedi da $2, 3, 5 \mid n$ pa zaključujemo da postoje $K, L, M, l \in \mathbb{N}$ takvi da je $n = 2^K 3^L 5^M l$. Odredimo najmanji n koji ima tražena svojstva. On je oblika $n = 2^K 3^L 5^M$. Iz (3.1) slijedi:

- $\frac{n}{2} = a^2 = 2^{K-1} 3^L 5^M$, tj. $K - 1 = 2k_1, L = 2l_1, M = 2m_1, k_1, l_1, m_1 \in \mathbb{N}$,
- $\frac{n}{3} = b^3 = 2^K 3^{L-1} 5^M$, tj. $K = 3k_2, L - 1 = 3l_2, M = 3m_2, k_2, l_2, m_2 \in \mathbb{N}$,
- $\frac{n}{5} = c^5 = 2^K 3^L 5^{M-1}$, tj. $K = 5k_3, L = 5l_3, M - 1 = 5m_3, k_3, l_3, m_3 \in \mathbb{N}$.

Odavde je

$$K = 2k_1 + 1, \quad K = 3k_2, \quad K = 5k_3$$

pa je K neparni broj i $15 \mid K$. Najmanji takav K je upravo $K = 15$. Analogno dobivamo $L = 10$ i $M = 6$. Odavde je $n = 2^5 3^{10} 5^6 = 30\,233\,088\,000\,000$.

◇

Napomena 3.4. Za $n \in \mathbb{N}$ vrijede sljedeće jednakosti:

$$a^{2n+1} \pm b^{2n+1} = (a \pm b)(a^{2n} \mp a^{2n-1}b + \dots + b^{2n}), \quad (3.2)$$

$$a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n). \quad (3.3)$$

Odavde slijedi da za sve $m \in \mathbb{N}$ vrijedi $a - b \mid a^m - b^m$.

Zadatak 3.6. Neka je $k \in \mathbb{N}$ takav da je $2^k + 1$ prosti broj. Dokažite da je $k = 0$ ili $k = 2^n$, za neki $n \in \mathbb{N}$.

Rješenje. Uočimo da za $k = 0$ dobivamo $2^k + 1 = 2$ i to je prosti broj. Pretpostavimo da je $k \neq 0$ i k ima neparni prosti faktor p . Tada postoji $m \in \mathbb{N}$ takav da je $k = mp$, $m \geq 1$. Prema Napomeni 3.4. vrijedi

$$2^k + 1 = (2^m)^p + 1 = (2^m + 1)((2^m)^{p-1} - (2^m)^{p-2} + \dots + 1).$$

Zaključujemo da $2^m + 1 \mid 2^k + 1$. Kako je $m \neq k$, odavde slijedi da $2^k + 1$ nije prosti broj pa smo došli do kontradikcije. Zaključujemo da k ne može imati neparni prosti faktor pa je $k = 2^n$, $n \in \mathbb{N}$. ◇

Definicija 3.3. Brojevi oblika $F_n = 2^{2^n} + 1$, $n \geq 0$ nazivaju se Fermatovi brojevi.

Fermat je smatrao da su svi Fermatovi brojevi prosti. Međutim, Euler je uočio da je $F_5 = 2^{32} + 1$ složen broj i može se faktorizirati na način

$$2^{32} + 1 = 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4).$$

Hipoteza je da postoji samo konačno mnogo Fermatovih prostih brojeva. Napomenimo da je najveći Fermatov broj za koji se trenutno zna da je složen jednak $F_{18233954}$.¹

¹Aktualni rezultati vezani uz faktorizaciju Fermatovih brojeva mogu se naći na stranici: <http://www.prothsearch.com/fermat.html#Summary>

Zadatak 3.7.

- (i) Dokažite da za sve $n \in \mathbb{N}$ vrijedi $F_0 F_1 \cdots F_{n-1} = F_n - 2$.
- (ii) Dokažite da za $m \neq n$ vrijedi $(F_m, F_n) = 1$.
- (iii) Pokažite da tvrdnja (ii) povlači da prostih brojeva ima beskonačno mnogo.

Rješenje.

- (i) Ta tvrdnja dokazuje se metodom matematičke indukcije te ju ostavljamo za vježbu.
- (ii) Bez smanjenja općenitosti, pretpostavimo da je $m < n$ i $(F_m, F_n) = d$. Prema tvrdnji (i) slijedi da je $F_0 \cdots F_m \cdots F_{n-1} = F_n - 2$. Kako $d \mid F_n$ i $d \mid F_m$, zaključujemo da $d \mid 2$. S obzirom da su F_n neparni brojevi, moguće je samo $d = 1$.
- (iii) Prema Osnovnom teoremu aritmetike svaki F_n ima barem jedan prosti djelitelj p_n . Prema prethodnoj tvrdnji vrijedi $(F_m, F_n) = 1$ pa zaključujemo da je $p_m \neq p_n$, za sve $m, n \in \mathbb{N}$. Kako Fermatovih brojeva ima beskonačno mnogo, zaključujemo da prostih brojeva ima beskonačno mnogo.

◇

Zadatak 3.8. Neka je $n \in \mathbb{N}$ takav da je $2^n - 1$ prosti broj. Dokažite da je tada i n prosti broj.

Rješenje. Pretpostavimo da je $2^n - 1$ prosti broj. Ako bi n bio složen broj, onda bi postojali $a, b \in \mathbb{N}$, $1 < a, b < n$, $n = ab$. No onda je

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1.$$

Prema Napomeni 3.4. slijedi da $2^a - 1 \mid 2^n - 1$ pa je $2^n - 1$ složen broj i došli smo do kontradikcije. Zaključujemo da n mora biti prosti broj. ◇

Definicija 3.4. Brojevi oblika $M_n = 2^n - 1$, $n \in \mathbb{N}$ nazivaju se Mersenneovi brojevi. Ako je M_p prosti broj, onda je M_p Mersenneov prosti broj.

Neki Mersenneovi brojevi su prosti (npr. $M_7 = 127$), a neki su složeni (npr. $M_{11} = 2047 = 23 \cdot 89$). Hipoteza je da Mersenneovih prostih brojeva ima beskonačno mnogo. Najveći do sada otkriveni Mersenneov prosti broj je $M_{82589933}$ i ima 24 862 048 znamenaka. Osim toga, najveći poznati prosti brojevi su Mersenneovi prosti brojevi (vidi [2]).

Zadatak 3.9. *Odredite sve prirodne brojeve n za koje su $2^n - 1$ i $2^n + 1$ prosti brojevi.*

Rješenje. Brojevi oblika $2^n - 1, 2^n, 2^n + 1$ uzastopni su prirodni brojevi pa je jedan od njih djeljiv s 3. Kako $3 \nmid 2^n$, slijedi da $3 \mid 2^n - 1$ ili $3 \mid 2^n + 1$. Budući da je 3 prosti broj, $2^n - 1$ i $2^n + 1$ prosti su brojevi i $2^n - 1 < 2^n + 1$, zaključujemo da je $2^n - 1 = 3$. Odavde je $n = 2$. Za $n = 2$ slijedi $2^n + 1 = 5$, a to je prosti broj. Time smo pokazali da je jedini prirodni broj s tim svojstvom $n = 2$. \diamond

Zadatak 3.10. *Dokažite da za svaki $n \in \mathbb{N}$ postoji n uzastopnih složenih brojeva.*

Rješenje. Uočimo da za sljedeći niz brojeva

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n, (n+1)! + n + 1$$

vrijedi $j \mid (n+1)! + j, j = 2, 3, \dots, n+1$. Time je tvrdnja dokazana. \diamond

Zadatak 3.11. *U skupu prostih brojeva riješite jednadžbu $x^y + 1 = z$.*

Rješenje. Neka su x, y, z prosti brojevi koji zadovoljavaju danu jednadžbu. Kako su $x, y \geq 2$, slijedi $z = x^y + 1 \geq 5$. Zaključujemo da je z neparni prosti broj. No onda je $z - 1 = x^y$ paran broj pa je x parni prosti broj, odnosno $x = 2$. Pretpostavimo da je y neparni, tj. $y = 2k + 1, k \in \mathbb{N}$. Tada je (primjenjujemo jednakosti iz Napomene 3.4.)

$$z = 2^y + 1 = 2^{2k+1} + 1 = (2+1)(2^{2k} - 2^{2k-1} + \dots + 1).$$

Odavde slijedi da $3 \mid z$. Kako je z prosti broj i $z \geq 5$, dolazimo do kontradikcije. Stoga je y paran i prost pa je $y = 2$. Za $x = y = 2$, dobivamo $z = 2^2 + 1 = 5$. Time smo odredili jedinstveno rješenje $(x, y, z) = (2, 2, 5)$ dane jednadžbe u skupu prostih brojeva. \diamond

Zadatak 3.12. *Neka je $k \in \mathbb{N}, k > 2$. Dokažite da je broj $4^k - 1$ umnožak barem triju prirodnih brojeva različitih od 1.*

Zadatak 3.13. *Ako su $p, p > 3$ i $2p+1$ prosti brojevi, dokažite da je $4p+1$ složen broj.*

Rješenje. Ako je $p, p > 3$ prosti broj, onda je on oblika $3k+1$ ili $3k+2$, za neki $k \in \mathbb{N}$. Pretpostavimo li da je $p = 3k+1$, onda je $2p+1 = 3(2k+1)$ pa broj $2p+1$ neće biti prost (jer $3 \mid 2p+1$ i $2p+1 > 3$). Stoga p mora biti oblika $3k+2$. U tom je slučaju $4p+1 = 3(4k+3)$, odakle slijedi da je $4p+1$ složen broj. \diamond

Zadatak 3.14. Neka $n \in \mathbb{N}, n \geq 3$ i neka su p, q prosti brojevi sa svojstvom $p \mid n!$ i $q \mid n! - 1$. Dokažite da je $p < q$.

Rješenje. Pretpostavimo da je $n \in \mathbb{N}, n \geq 3$ i p, q prosti su brojevi sa svojstvom $p \mid n!$ i $q \mid n! - 1$. Neka je $p \geq q$. Iz $p \mid n!$ slijedi da je $p \leq n$ pa zaključujemo da je $q \leq p \leq n$. No onda $q \mid n!$. Budući da $q \mid n! - 1$, sada slijedi da $q \mid 1$. Tako smo došli do kontradikcije i zaključujemo da je $p < q$.
◇

Zadatak 3.15. Odredite sve $n \in \mathbb{N}$ za koje je $n^4 + 4$ prost broj.

Rješenje. Uočimo da vrijedi

$$\begin{aligned} n^4 + 4 &= n^4 + 4n^2 + 4 - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 + 2 + 2n)(n^2 + 2 - 2n). \end{aligned}$$

Osim toga, $n^2 + 2 + 2n, n^2 + 2 - 2n \in \mathbb{N}$ i $n^2 + 2 - 2n < n^2 + 2 + 2n$. Kako je $n^4 + 4$ prost broj, mora biti $n^2 + 2 - 2n = 1$ (i $n^2 + 2 + 2n$ prosti je broj). Iz $n^2 + 2 - 2n = 1$ slijedi da je $n = 1$. Za tako određen n lako se vidi da je broj $n^4 + 4 = 5$ (i $n^2 + 2 + 2n = 5$) prost. Time je dokazana polazna tvrdnja.
◇

Zadatak 3.16. Odredite sve $n \in \mathbb{Z}$ za koje je $n^2 + 6n - 16$ prost broj.

4. Broj i zbroj svih pozitivnih djelitelja prirodnog broja

Koristeći faktorizaciju prirodnih brojeva možemo odrediti broj i zbroj svih njegovih pozitivnih djelitelja. Takve probleme proučavat ćemo u ovom odjeljku.

Definicija 4.1. Neka je $n \in \mathbb{N}$. Definirajmo funkcije $\sigma, \tau : \mathbb{N} \rightarrow \mathbb{N}$ na sljedeći način:

$$\sigma(n) - \text{zbroj svih pozitivnih djelitelja broja } n \quad (\sigma(n) = \sum_{d \mid n} d),$$

$$\tau(n) - \text{broj svih pozitivnih djelitelja broja } n \quad (\tau(n) = \sum_{d \mid n} 1).$$

Primjer 4.1.

- (1) Ako je p prosti broj, jedini su mu pozitivni djelitelji 1 i p pa je $\sigma(p) = p + 1$, $\tau(p) = 2$.
- (2) Ako je p prosti broj i $k \in \mathbb{N}$, tada se (korištenjem formule za parcijalnu sumu geometrijskog reda) dobiva

$$\sigma(p^k) = 1 + p + \dots + p^k = \frac{1 - p^{k+1}}{1 - p}$$

$$\text{i } \tau(p) = k + 1.$$

Primjer 4.2. Ako $d \mid n$, onda postoji jedinstveni d_1 takav da je $dd_1 = n$. Stoga je

$$\sum_{d \mid n} d = \sum_{d_1 \mid n} \frac{n}{d_1} = \sum_{d \mid n} \frac{n}{d}.$$

Kako je $\tau(n)$ broj svih pozitivnih djelitelja broja n , niz pozitivnih djelitelja broja n možemo zapisati u obliku $d_1, d_2, \dots, d_{\tau(n)}$ (ili $\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_{\tau(n)}}$).

Definicija 4.2. Funkcija $f : \mathbb{N} \rightarrow \mathbb{N}$ multiplikativna je funkcija ako vrijedi:

- (i) $f(1) = 1$,
- (ii) $f(mn) = f(m)f(n)$, za sve $(n, m) = 1$.

Teorem 4.1. ([8]) Funkcije σ i τ su multiplikativne.

Korolar 4.1. Neka je $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ kanonski rastav broja n na proste faktore. Tada je

$$\sigma(n) = \prod_{j=1}^k \frac{1 - p_j^{\alpha_j+1}}{1 - p_j}, \quad \tau(n) = \prod_{j=1}^k (\alpha_j + 1).$$

Važna će nam biti tvrdnja sljedećeg zadatka i ona se može koristiti kod rješavanja drugih zadataka.

Zadatak 4.1. Neka je $n \in \mathbb{N}$. Dokazite: n je potpuni kvadrat ako i samo ako je $\tau(n)$ neparan.

Rješenje. Ako je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ potpun kvadrat to je ekvivalentno tome da su svi α_i parni brojevi. No to je ekvivalentno tome da su svi $\alpha_i + 1$ neparni brojevi, tj. $\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$ je neparan. \diamond

Uočite kako, prema prethodnom zadatku, slijedi da prirodni broj n nije potpun kvadrat ako i samo ako je $\tau(n)$ paran.

Zadatak 4.2. *Dokažite da je za neparni prirodni broj n broj $\sigma(n)$ neparan ako i samo ako je n potpun kvadrat.*

Zadatak 4.3. *Neka je $n \in \mathbb{N}$.*

(i) *Dokažite: $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.*

(ii) *Odredite oblik prirodnog broja n za koji vrijedi:*

$$\prod_{d|n} d = n^2.$$

Rješenje.

(i) Spomenuli smo u Primjeru 4.2. da sve pozitivne djelitelje prirodnog broja n možemo zapisati u obliku $d_1, d_2, \dots, d_{\tau(n)}$ ili $\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_{\tau(n)}}$. Uočimo da je $d_i \frac{n}{d_i} = n$, za sve $i = 1, \dots, \tau(n)$. No onda je

$$\left(d_1 \frac{n}{d_1}\right) \cdots \left(d_{\tau(n)} \frac{n}{d_{\tau(n)}}\right) = \left(\prod_{d|n} d\right)^2.$$

Oдавде slijedi tvrdnja.

(ii) Ako je $\prod_{d|n} d = n^2$, onda prema prvoj tvrdnji ovog zadatka slijedi $\tau(n) = 4$. Za $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ je $\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$ i $\alpha_i + 1 \geq 2, i = 1, \dots, k$. Zaljučujemo da postoje samo dvije mogućnosti:

- Ako je $\tau(n) = 4 = \alpha_1 + 1$, onda je $\alpha_1 = 3$ pa je $n = p^3$, gdje je p prosti broj,
- Ako je $\tau(n) = 2 \cdot 2 = (\alpha_1 + 1)(\alpha_2 + 1)$, onda je $\alpha_1 + 1 = 2, \alpha_2 + 1 = 2$, tj. $\alpha_1 = \alpha_2 = 1$. Stoga je $n = pq$, gdje su p, q različiti prosti brojevi.

\diamond

Zadatak 4.4. Neka je $n \in \mathbb{N}$. Odredite sve $n \in \mathbb{N}$ koji su djeljivi s 12 i imaju točno 16 djelitelja.

Rješenje. Neka je $n \in \mathbb{N}$ djeljiv s 12 i ima točno 16 djelitelja. Kako $12 \mid n$ slijedi da je $n = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$ i $\alpha_1 \geq 2, \alpha_2 \geq 1, \alpha_3, \dots, \alpha_k \in \mathbb{N}_0$. S obzirom da n ima 16 djelitelja, mora vrijediti

$$16 = \tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Kako n ima barem dva, a najviše 3 prosta faktora, znamo da je $\alpha_1 + 1 \geq 3, \alpha_2 + 1 \geq 2$ pa ima smisla promatrati samo sljedeće umnoške $2 \cdot 8 = 4 \cdot 4 = 2 \cdot 2 \cdot 4$ koji daju broj 16. Odavde dobivamo da je $n = 2^7 3, n = 2^3 3^3$ ili $n = 2^3 3p, p > 3$ prosti broj. \diamond

Zadatak 4.5. Neka je $n \in \mathbb{N}$ takav da $16 \mid n+1$. Dokažite da je $\tau(n)$ paran.

Rješenje. Neka je $n \in \mathbb{N}, 16 \mid n+1$. Tada postoji $k \in \mathbb{Z}$ takav da je $n+1 = 16k$. Nadalje je

$$n = 16k - 1 = 4(4k - 1) + 3 = 4m + 3, \quad m = 4k - 1.$$

U Zadatku 1.11. zaključili smo da je potpun kvadrat oblika $4l$ ili $4l+1$ pa slijedi da n nije potpun kvadrat. No onda prema Zadatku 4.1. slijedi da je $\tau(n)$ paran. \diamond

Zadatak 4.6. Ako za $n \in \mathbb{N}$ vrijedi $\tau(5n) = 2\tau(n)$, dokažite da je $(5, n) = 1$.

Rješenje. Neka je $n \in \mathbb{N}$ i neka je $n = 5^\alpha m, m \in \mathbb{N}, \alpha \in \mathbb{N}_0, (5, m) = 1$. Tada je (primjenjujemo multiplikativnost funkcije τ)

$$\tau(5n) = \tau(5^{\alpha+1} m) = \tau(5^{\alpha+1})\tau(m) = (\alpha + 2)\tau(m).$$

Kako je $\tau(n) = (\alpha + 1)\tau(m)$, iz uvjeta $\tau(5n) = 2\tau(n)$ dobivamo

$$(\alpha + 2)\tau(m) = 2(\alpha + 1)\tau(m).$$

Odavde slijedi $\alpha = 0$ i time je tvrdnja dokazana. \diamond

Definicija 4.3. Za $n \in \mathbb{N}$ kažemo da je savršen broj ako je $\sigma(n) = 2n$.

Za različite prirodne brojeve m i n kažemo da su prijateljski ako je $\sigma(n) = m + n = \sigma(m)$.

Poznato je da svi parni savršeni brojevi završavaju znamenkom 6 ili 8. Jedan od neriješenih problema teorije brojeva odnosi se na neparne savršene brojeve. Naime, nije poznato postoji li uopće neparni savršen broj (vidjeti npr. [5]).

Primjer 4.3. *Najmanji savršeni broj je broj 6, a brojevi 220 i 284 prijateljski su brojevi.*

Primjer 4.4. *Ako je n savršen broj, onda prema Primjeru 4.2. slijedi*

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d} = 2n.$$

Zaključujemo da je n savršen ako i samo ako je $\sum_{d|n} d^{-1} = 2$.

Dokažite za vježbu da za prijateljske brojeve m i n vrijedi

$$\frac{1}{\sum_{d|n} \frac{1}{d}} + \frac{1}{\sum_{d|m} \frac{1}{d}} = 1.$$

Zadatak 4.7. *Dokažite da je parni broj n savršen ako i samo ako se može prikazati u obliku $n = 2^k(2^{k+1} - 1)$, $k \in \mathbb{N}$, gdje je $2^{k+1} - 1$ prosti broj.*

Rješenje. Dokažimo najprije da je parni broj oblika $n = 2^k(2^{k+1} - 1)$, $k \in \mathbb{N}$, gdje je $2^{k+1} - 1$ prosti broj, savršen broj. Vrijedi:

$$\begin{aligned} \sigma(n) &= \sigma(2^k(2^{k+1} - 1)) \\ &= \sigma(2^k)\sigma(2^{k+1} - 1) \quad [\text{jer } (2^k, 2^{k+1} - 1) = 1] \\ &= \frac{2^{k+1} - 1}{2 - 1} 2^{k+1} \quad [\text{jer je } 2^{k+1} - 1 \text{ prosti broj}] \\ &= 2(2^k(2^{k+1} - 1)) = 2n. \end{aligned}$$

Neka je n parni savršen broj. Tada je $\sigma(n) = 2n$ i $n = 2^k m$, $k, m \in \mathbb{N}$, $(m, 2) = 1$. Iz $\sigma(n) = 2n$ slijedi

$$2^{k+1}m = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m). \quad (4.1)$$

Oдавде zaključujemo da $2^{k+1} - 1 \mid 2^{k+1}m$ pa postoji m' takav da je $m = (2^{k+1} - 1)m'$. Pretpostavimo li da je $m' \neq 1$, slijedi $\sigma(m) \geq 1 + m' + m$. S druge strane, iz $m = (2^{k+1} - 1)m'$ slijedi $m + m' = 2^{k+1}m'$ pa dobivamo $\sigma(m) \geq 1 + 2^{k+1}m'$. Uvrštavanjem $m = (2^{k+1} - 1)m'$ u jednakost (4.1) slijedi da je $\sigma(m) = 2^{k+1}m'$. No onda dobivamo $\sigma(m) \geq 1 + \sigma(m)$, a to nije moguće. Stoga je $m' = 1$ i $\sigma(m) = m + 1$, tj. $m = 2^{k+1} - 1$ prosti je broj. \diamond

Zadatak 4.8. *Dokažite da je $2 \cdot 3^\alpha$, $\alpha \in \mathbb{N}$ savršen broj ako i samo ako je $\alpha = 1$.*

5. Zadatci za vježbu

Zadatak 5.1. Neka su $m, n \in \mathbb{N}$. Ako $10 \mid 3^n + m$, dokažite da $10 \mid 3^{n+4} + m$.

Zadatak 5.2. Dokažite da se ni jedan prirodni broj oblika $8k + 7, k \in \mathbb{N}$ ne može prikazati kao zbroj triju kvadrata.

Zadatak 5.3. Dokažite da $24 \mid (n^2 + n - 1)^2 - 1$, za sve $n \in \mathbb{Z} \setminus \{0\}$.

Zadatak 5.4. Dokažite da je razlika kvadrata dvaju cijelih brojeva koji nisu djeljivi ni s 2 ni s 3 djeljiva s 24.

Zadatak 5.5. Odredite najmanji $n \in \mathbb{N}, n > 2023$ takav da je izraz

$$M = \frac{x_1^4 + x_2^4 + \dots + x_n^4}{5}$$

prirodni broj za svaki x_i sa svojstvom da $5 \nmid x_i, i = 1, \dots, n$.

Zadatak 5.6. Ako je $r \in \mathbb{Z}$ ostatak pri dijeljenju broja $a \in \mathbb{Z}$ brojem $b \in \mathbb{Z} \setminus \{0\}$, dokažite da je $(a, b) = (b, r)$.

Zadatak 5.7. Ako je poznato da je r ostatak pri dijeljenju brojeva 2014 i 2121 brojem $n \in \mathbb{N} \setminus \{1\}$, odredite $n - r$.

Zadatak 5.8. Neka su $a, b \in \mathbb{Z}, (a, b) = 1$. Dokažite da je tada $(a + b, a - b) = 1$ ili 2.

Zadatak 5.9. Neka su m, n prirodni brojevi i $(m, n) = 1$. Odredite $(m + n, m^2 - mn + n^2)$.

Zadatak 5.10. Odredite sve prirodne brojeve $d = (5n + 6, 8n + 7), n \in \mathbb{N}$.

Zadatak 5.11. Neka je $(a, b) = 10$. Odredite sve vrijednosti za (a^3, b^4) .

Zadatak 5.12. Neka je n višekratnik broja 3. Dokažite da se razlomak $\frac{n-2}{2n-1}$ ne može skratiti.

Zadatak 5.13. Dokažite da za sve prirodne brojeve a, b vrijedi $(a, b) \leq (a + b, a - b)$.

Zadatak 5.14. *Neka je $n \in \mathbb{N}$. Dokažite da su elementi skupa*

$$S = \{n! \cdot i + 1 : i \in \{1, 2, \dots, n\}\}$$

u parovima relativno prosti.

Zadatak 5.15. *Odredite jedno cjelobrojno rješenje (x, y) jednadžbe $41x - 74y = -1$.*

Zadatak 5.16. *Ispitajte ima li jednadžba $616x + 63y = 33$ cjelobrojnih rješenja.*

Zadatak 5.17. *Dokažite da prostih brojeva ima beskonačno mnogo.*

Zadatak 5.18. *Odredite sve prirodne brojeve a, b takve da je $a^4 + 4b^4$ prosti broj.*

Zadatak 5.19. *Odredite sve prirodne brojeve n za koje su sva tri broja n , $n + 4$ i $4n - 1$ prosti.*

Zadatak 5.20. *Odredite sve proste brojeve p takve da je $19p + 8$ kub cijelog broja x .*

Zadatak 5.21. *Neka je $p > 3$ prosti broj. Dokažite da je tada barem jedan od brojeva $p + 2$ i $p + 4$ složen broj.*

Zadatak 5.22. *Ako je p prosti broj sa svojstvom da je $4p^2 + 1$ također prosti broj, dokažite da je $p^2 + 11$ složen broj.*

Zadatak 5.23. *Dokažite da se svaki neparni prosti broj može zapisati kao razlika dvaju kvadrata.*

Zadatak 5.24. *Odredite sve proste brojeve p za koje postoje $m, n \in \mathbb{N}$ takvi da je $p^{2n+1} = 2^m + 1$.*

Zadatak 5.25. *Odredite sve prirodne brojeve n koji imaju dva prosta djelitelja i vrijedi $\tau(n) = 6$ i $\sigma(n) = 28$.*

Zadatak 5.26. *Odredite sve $n \in \mathbb{N}$ sa svojstvom da je $\tau(9n) = 10$.*

Zadatak 5.27. *Dokažite da je broj djelitelja broja $\underbrace{1111 \dots 1}_{2023}$ parni broj.*

Zadatak 5.28. *Dokažite da broj oblika $n = 12m + 9$, $(3, m) = 1$, ne može biti savršen.*

Zadatak 5.29. *Neka je n prirodni broj. Odredite prirodni broj m sa svojom da je $m = 2p$, p je prosti broj i vrijedi $\sigma(2m) = 2^{n+2}(2^{n+2} - 1)$.*

Zadatak 5.30. *Ako je $2^m - 1$, $m \in \mathbb{N}$ složen broj, dokažite da broj oblika $n = 2^{m-1}(2^m - 1)$ nije savršen broj.*

Upute za rješavanje zadataka

Zadatak 1.3. Zapišite sumu triju uzastopnih potencija broja 3, a zatim pokažite da je dobiveni izraz djeljiv s 39.

Zadatak 1.5. Promotrite što bi dala pretpostavka da je $a > \sqrt{n}$, $b > \sqrt{n}$.

Zadatak 1.8. Rješenja zadane jednadžbe su $(n, k) \in \{(-6, 2), (0, 0), (2, -6), (4, 12), (6, 6), (12, 4)\}$. Izrazite k pomoću n .

Zadatak 1.13. Proizvoljan cijeli broj jednog je od oblika: $5k, 5k+1, \dots, 5k+4$, za neki cijeli broj k . To upotrijebite u podzadacima.

Zadatak 1.14. Iskoristite činjenicu da je za proizvoljan cijeli broj n broj $n(n+1)$ paran.

Zadatak 1.16. Promotrite oblik proizvoljnog cijelog broja n s obzirom na djeljivost s 3.

Zadatak 2.5. Faktorizirajte izraz $n^5 - n$. Iskoristite svojstva djeljivosti s 2 i 3 te oblik bilo koje četvrte potencije cijelog broja k .

Zadatak 2.8. Primjenom rekurzivnih formula iz Napomene 2.3. pokažite da vrijedi jednakost $y_i x_{i-1} - x_i y_{i-1} = -(y_{i-1} x_{i-2} - x_{i-1} y_{i-2})$, a zatim ju uzastopno primijenite.

Zadatak 2.10. Rješenje jednadžbe je $(x, y) = (-39, -56)$.

Zadatak 3.12. Koristite suprotnu pretpostavku i faktorizaciju izraza $4^k - 1$.

Zadatak 3.16. Faktorizacijom danog izraza dobiva se $n \in \{-3, 9\}$.

Zadatak 4.2. Upotrijebite kanonski rastav neparnog prirodnog broja n na proste faktore i iskoristite svojstva funkcije σ .

Zadatak 5.1. Upotrijebite pretpostavku $3^n + m = 10k$, $k \in \mathbb{N}$.

Zadatak 5.2. Za $k \in \mathbb{N}$, prirodni broj n jednog je od oblika $8k, 8k + 1, \dots, 8k + 7$. Upotrijebite to!

Zadatak 5.3. Rastavite izraz $(n^2 + n - 1)^2 - 1$ na faktore.

Zadatak 5.4. Za $n = 12$ iskoristite Teorem o dijeljenju s ostatkom.

Zadatak 5.5. Rješenje je $n = 2025$. Promotrite oblike četvrtih potencija pri dijeljenju s 5.

Zadatak 5.6. Iskoristite Teorem o dijeljenju s ostatkom i svojstva najvećeg zajedničkog djelitelja dvaju cijelih brojeva.

Zadatak 5.7. Dobiva se $n = 107, r = 88$. Primijenite Teorem o dijeljenju s ostatkom.

Zadatak 5.8. Napišite $d = (a + b, a - b)$ kao odgovarajuću linearnu kombinaciju cijelih brojeva.

Zadatak 5.9. Napišite $d = (m + n, m^2 - mn + n^2)$ kao odgovarajuću linearnu kombinaciju cijelih brojeva te iskoristite svojstva najvećeg zajedničkog djelitelja dvaju cijelih brojeva.

Zadatak 5.10. Napišite d kao odgovarajuću linearnu kombinaciju cijelih brojeva i zaključite da je $d = 1, 13$.

Zadatak 5.11. Upotrijebite svojstva najvećeg zajedničkog djelitelja dvaju cijelih brojeva.

Zadatak 5.12. Stavite $d = (n - 2, 2n - 1)$ i pokažite da je $d = 1$.

Zadatak 5.13. Upotrijebite svojstva najvećeg zajedničkog djelitelja dvaju cijelih brojeva.

Zadatak 5.14. Stavite $d = (n! \cdot i + 1, n! \cdot j + 1)$, $i, j \in \{1, \dots, n\}$, a zatim napišite d kao odgovarajuću linearnu kombinaciju cijelih brojeva i zaključite da je $d = 1$.

Zadatak 5.15. Jedno rješenje dane jednadžbe je $(x, y) = (9, 5)$.

Zadatak 5.16. Odredite $d = (616, 63)$ i zaključite kako ne postoji cjelobrojno rješenje navedene jednadžbe.

Zadatak 5.17. Pretpostavite da su p_1, \dots, p_k svi prosti brojevi i promotrite broj $q = p_1 \cdots p_k + 1$.

Zadatak 5.18. Faktorizirajte izraz $a^4 + 4b^4$.

Zadatak 5.19. Rješenje je $n = 3$. Iskoristite zapis broja n s obzirom na djeljivost s 3.

Zadatak 5.20. Rješenje je $p = 487$. Koristite faktorizaciju razlike kubova dvaju cijelih brojeva.

Zadatak 5.21. Promotrite prikaz broja p s obzirom na dijeljenje s 3.

Zadatak 5.22. Koristite prikaz brojeva p i p^2 s obzirom na dijeljenje s 5.

Zadatak 5.23. Faktorizirajte razliku kvadrata dvaju cijelih brojeva i iskoristite definiciju prostog broja.

Zadatak 5.24. Promotrite faktorizaciju broja $p^{2n+1} - 1$.

Zadatak 5.25. Rješenje je $n = 12$. Za različite proste brojeve p i q te prirodne brojeve u i v promotrite broj $n = p^u q^v$.

Zadatak 5.26. Dobiva se $n = 3^7$ i $n = 9p$, gdje je $p \neq 3$ prost broj. Stavite $n = 3^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $p_i \neq 3$, $i = 1, \dots, k$ i primijenite svojstvo multiplikativnosti funkcije τ .

Zadatak 5.27. Iskoristite tvrdnju dokazanu u Zadatku 4.1.: n je potpun kvadrat ako i samo ako je $\tau(n)$ neparan.

Zadatak 5.28. Promotrite što bi se zaključilo ako bi n bio savršen broj.

Zadatak 5.29. Dobiva se $m = 2(2^{n+2} - 1)$; zasebno promotrite slučajeve $p = 2$ i $p \neq 2$.

Zadatak 5.30. Pretpostavite suprotno i iskoristite mutiplikativnost funkcije σ .

Kongruencije

1. Definicija i osnovna svojstva kongruencija

Pojam kongruencije uveo je Carl Friedrich Gauss u svome poznatom djelu *Disquisitiones Arithmeticae* iz 1801. godine. Jedan je to od osnovnih pojmova moderne teorije brojeva, a temelji se na djeljivosti u skupu cijelih brojeva.

Definicija 1.1. *Neka je $n \in \mathbb{N}, a, b \in \mathbb{Z}$. Ako $n \mid a - b$, kažemo da je a kongruentan b modulo n i pišemo*

$$a \equiv b \pmod{n}.$$

U suprotnom kažemo da a nije kongruentan b modulo n i pišemo $a \not\equiv b \pmod{n}$.

Primjer 1.1. *Direktno iz definicije može se zaključiti da npr. vrijedi $8 \equiv 2 \pmod{3}$, $8 \equiv -1 \pmod{3}$, $8 \not\equiv 3 \pmod{3}$. Također, ako za $a, b \in \mathbb{Z}$ vrijedi $a = b$, onda je $a \equiv b \pmod{n}$, za sve $n \in \mathbb{N}$.*

Napomena 1.1. *Ako je r ostatak pri dijeljenju broja $a \in \mathbb{Z}$ s $n \in \mathbb{N}$, onda ga, prema Teoremu o dijeljenju s ostatkom, možemo zapisati u obliku $a = nq + r$, $q, r \in \mathbb{Z}, 0 \leq r < n$. Stoga je $a \equiv r \pmod{n}$. Za ostatak r koristi se i oznaka $a \bmod n$.*

Primjer 1.2. *Znamo da je potpun kvadrat oblika $4k$ ili $4k+1$ (Zadatak 1.11.). U terminima kongruencija možemo pisati $\square \equiv 0, 1 \pmod{4}$.*

Lako se može pokazati da vrijede osnovna svojstva kongruencija navedena u sljedećoj napomeni.

Napomena 1.2. *Neka je $n \in \mathbb{N}$.*

- (1) Za svaki $k \in \mathbb{Z}$ vrijedi $kn \equiv 0 \pmod{n}$.
- (2) Za $c \in \mathbb{N}, a, b \in \mathbb{Z}$ vrijedi:
- (i) $a \equiv b \pmod{n} \iff ca \equiv cb \pmod{cn}$,
- (ii) $a \equiv b \pmod{cn} \implies a \equiv b \pmod{n}$. Obrat te tvrdnje ne vrijedi.
Primjerice, $2 \equiv 0 \pmod{2}$, ali $2 \not\equiv 0 \pmod{4}$.
- (3) Relacija "biti kongruentan modulo n " relacija je ekvivalencije na skupu \mathbb{Z} .
- (4) Neka su $a, a', b, b' \in \mathbb{Z}$. Ako je $a \equiv a' \pmod{n}$ i $b \equiv b' \pmod{n}$, onda je $a \pm b \equiv a' \pm b' \pmod{n}$ i $ab \equiv a'b' \pmod{n}$.
- (5) Neka su $a, b \in \mathbb{Z}, a \equiv b \pmod{n}$. Tada za polinom $f(x)$ s cjelobrojnim koeficijentima vrijedi

$$f(a) \equiv f(b) \pmod{n}.$$

Primjer 1.3.

- (a) Pretpostavimo da je $p \equiv 3 \pmod{4}$. Kako je $9 \equiv 1 \pmod{4}$, to je $9p \equiv 3 \pmod{4}$.
- (b) Iz $6 \equiv 1 \pmod{5}$ slijedi $6^{1000} \equiv 1 \pmod{5}$ pa je ostatak pri dijeljenju broja 6^{1000} s 5 jednak 1.

Navedimo sada još jedno važno svojstvo kongruencija:

Propozicija 1.1. ([3]) Neka je $n \in \mathbb{N}, a, x, y \in \mathbb{Z}, a \neq 0$ i $d = (a, n)$. Vrijedi

$$ax \equiv ay \pmod{n} \iff x \equiv y \pmod{\frac{n}{d}}.$$

Primjer 1.4. Ako za $a, b \in \mathbb{Z}$ vrijedi $10a \equiv 20b \pmod{15}$, onda je to ekvivalentno s $a \equiv 2b \pmod{\frac{15}{(15,10)}}$, tj. $a \equiv 2b \pmod{3}$.

Definicija 1.2. Neka je $n \in \mathbb{N}$. Skup $S = \{a_1, a_2, \dots, a_n\} \subseteq \mathbb{Z}$ naziva se potpun sustav ostataka modulo n ako za svaki $y \in \mathbb{Z}$ postoji jedinstveni $a_j \in S$ takav da vrijedi $y \equiv a_j \pmod{n}$.

Uočimo da potpun sustav ostataka modulo n sadrži točno jednog predstavnika svake moguće klase ekvivalencije modulo n .

Primjer 1.5. *Sljedeći su skupovi potpuni sustavi ostataka modulo 5:*

$$\begin{aligned} S_1 &= \{0, 1, 2, 3, 4\}, \\ S_2 &= \{1, 2, 3, 4, 5\}, \\ S_3 &= \{-5, -4, -3, -2, -1\}, \\ S_4 &= \{-2, -1, 0, 1, 2\}, \\ S_5 &= \{-10, -9, 7, 18, 49\}. \end{aligned}$$

Npr. S_5 je potpun sustav ostataka modulo 5 jer je

$$\begin{aligned} -10 &\equiv 0 \pmod{5}, \\ -9 &\equiv 1 \pmod{5}, \\ 7 &\equiv 2 \pmod{5}, \\ 18 &\equiv 3 \pmod{5}, \\ 49 &\equiv 4 \pmod{5} \end{aligned}$$

pa u skupu S_5 imamo predstavnike svih mogućih klasa ekvivalencije modulo 5.

Skup

$$S_6 = \{-4, 0, 1, 2, 3\}$$

nije potpun sustav ostataka modulo 5 jer primjerice za broj 6 vrijedi $6 \equiv 1 \equiv -4 \pmod{5}$, tj. 1 i -4 predstavnici su iste klase (nije zadovoljen uvjet postojanja jedinstvenog predstavnika svake klase). Kako u S_6 nema predstavnika klase u kojoj se nalazi broj 4, također smo mogli zaključiti da S_6 nije potpun sustav ostataka modulo 5 jer ne postoji $a_i \in S_6$ takav da vrijedi $4 \equiv a_i \pmod{5}$.

Zadatak 1.1. *Može li skup $S = \{-70, -48, -29, -4, 9, 40, 74\}$ biti potpun sustav ostataka modulo n , za neki $n \in \mathbb{N}$? Tvrdnju obrazložite.*

Primjer 1.6. *Apsolutno najmanji potpuni sustavi ostataka modulo n dani su sa:*

- *n neparan:* $\left\{-\frac{n-1}{2}, -\frac{n-3}{2}, \dots, -1, 0, 1, \dots, \frac{n-3}{2}, \frac{n-1}{2}\right\}$,
- *n paran:* $\left\{-\frac{n-2}{2}, -\frac{n-4}{2}, \dots, -1, 0, 1, \dots, \frac{n-2}{2}, \frac{n}{2}\right\}$.

Zadatak 1.2. *Dokažite: $7 \mid 1941^{1963} + 1963^{1991}$.*

Rješenje. Iz $1941 \equiv 2 \pmod{7}$ slijedi $1941^3 \equiv 1 \pmod{7}$. Kako je $1963 = 3 \cdot 654 + 1$, dobivamo

$$1941^{1963} \equiv (1941^3)^{654} 1941 \equiv 2 \pmod{7}. \quad (1.1)$$

Analogno, iz $1963 \equiv 3 \pmod{7}$ slijedi $1963^2 \equiv 2 \pmod{7}$, odnosno $1963^6 \equiv 1 \pmod{7}$. Iz $1991 = 6 \cdot 331 + 5$ dobivamo

$$1963^{1991} \equiv 3^5 \equiv 5 \pmod{7}. \quad (1.2)$$

Iz (1.1) i (1.2) slijedi da je $n \equiv 0 \pmod{7}$, čime je tvrdnja dokazana. \diamond

Zadatak 1.3. *Dokažite: $39 \mid 53^{103} + 103^{53}$.*

Zadatak 1.4. *Odredite posljednje dvije znamenke broja 9^{9^9} .*

Rješenje. Uočimo da će nam u tu svrhu biti korisno odrediti ostatak pri dijeljenju broja 9^{9^9} sa 100. Kako je $9^9 = 387420489$ i $9^{10} \equiv 1 \pmod{100}$, slijedi

$$9^{9^9} = 9^{387420489} = 9^{38742048 \cdot 10 + 9} \equiv (9^{10})^{38742048} 9^9 \equiv 89 \pmod{100}.$$

Stoga su posljednje dvije znamenke broja 9^{9^9} jednake 89. \diamond

Zadatak 1.5. *Odredite ostatak pri dijeljenju broja $1! + 2! + \dots + 100!$ s 15.*

Rješenje. Kako je za $n \geq 5$ broj $n!$ djeljiv s 5, slijedi

$$1! + 2! + \dots + 100! \equiv 1 + 2! + 3! + 4! \equiv 33 \equiv 3 \pmod{15}.$$

\diamond

Zadatak 1.6. *Dokažite: $13 \mid 1 + 3^a + 9^a$, za sve brojeve a oblika $3n+1$, $n \in \mathbb{N}$.*

Zadatak 1.7. *Dokažite da diofantska jednadžba*

$$37z^2 = 81x^2y^2 - 9x^2 - T$$

nema rješenja za

$$(i) T = 4, \quad (ii) T = 3.$$

Rješenje.

- (i) Neka je $T = 4$. Promatrajući zadanu jednadžbu modulo 3 dobivamo kongruenciju $z^2 \equiv 2 \pmod{3}$. Ako bi polazna jednadžba imala rješenja, onda bi i pripadna kongruencija imala rješenja. Prema Zadatku 1.12. u poglavlju Djeljivost znamo da vrijedi $\square \equiv 0, 1 \pmod{3}$ pa zaključujemo da jednadžba ne može imati rješenja.
- (ii) Analogno, ako je $T = 3$, promatrajući zadanu jednadžbu modulo 3 dobivamo kongruenciju $z^2 \equiv 0 \pmod{3}$. Odavde slijedi da $3 \mid z$, odnosno $z^2 \equiv 0 \pmod{9}$. Reduciramo li polaznu jednadžbu modulo 9, dobivamo $z^2 \equiv 6 \pmod{9}$. Time dolazimo do kontradikcije pa zaključujemo da jednadžba nema rješenja.

◇

Zadatak 1.8. *Dokažite da diofantska jednadžba*

$$x^2 + y^2 = 4n - 1$$

nema rješenja.

2. Linearne kongruencije

Proučavat ćemo rješavanje linearnih kongruencija $ax \equiv b \pmod{n}$, gdje su a, b i n odgovarajući cijeli brojevi. Navedimo sada preciznu definiciju:

Definicija 2.1. *Neka je $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $n \nmid a$. Kongruencija oblika*

$$ax \equiv b \pmod{n} \tag{2.1}$$

naziva se linearna kongruencija.

Ako linearna kongruencija (2.1) ima rješenje x_0 , lako se vidi da je i $x_0 + kn$ također rješenje te kongruencije, za sve $k \in \mathbb{Z}$. Uočimo da su rješenja x_0 i $x_0 + kn$ međusobno kongruentna modulo n . Pod brojem rješenja kongruencije modulo n podrazumijevat ćemo broj međusobno nekongruentnih rješenja modulo n .

Poznato nam je da linearna jednadžba $ax = b, a \neq 0$ uvijek ima jedinstveno realno rješenje. Međutim, linearna kongruencija $ax \equiv b \pmod{n}$ ne mora imati rješenja, a ako ih ima, ima ih beskonačno mnogo. Sljedeći rezultat govori nam o postojanju rješenja linearne kongruencije (2.1).

Teorem 2.1. ([3]) *Neka su $a, n \in \mathbb{N}, b \in \mathbb{Z}$ i neka je $d = (a, n)$.*

- (a) *Kongruencija (2.1) ima rješenja ako i samo ako $d \mid b$.*
 (b) *Ako $d \mid b$ i x_0 je rješenje kongruencije*

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}, \quad (2.2)$$

onda su sva međusobno nekongruentna rješenja modulo n kongruencije (2.1) dana sa

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

Napomena 2.1. *Neka su $a, n \in \mathbb{N}, b \in \mathbb{Z}$ i neka je $d = (a, n)$ i $d \mid b$.
 Postupak rješavanja kongruencije*

$$ax \equiv b \pmod{n} \quad i \quad d = (a, n):$$

- (1) *Nađe se rješenje x_0 kongruencije*

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \quad (2.3)$$

na sljedeći način:

- (a) *Korištenjem Euklidovog algoritma nađe se u iz Bézoutovog identiteta*

$$\frac{a}{d}u + \frac{n}{d}v = 1.$$

- (b) *Za tako određen u vrijedi*

$$\frac{a}{d}u \equiv 1 \pmod{\frac{n}{d}}. \quad (2.4)$$

- (c) *Množenjem obiju strana kongruencije (2.3) s u dobiva se*

$$\frac{a}{d}ux \equiv \frac{b}{d}u \pmod{\frac{n}{d}}$$

pa je zbog (2.4)

$$x_0 \equiv \frac{b}{d}u \pmod{\frac{n}{d}}$$

rješenje kongruencije (2.3) i rješenje početne kongruencije.

- (2) *Sva međusobno nekongruentna rješenja modulo n početne kongruencije dana su sa*

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

Primjer 2.1. *Riješimo kongruenciju*

$$9x \equiv 12 \pmod{15}. \quad (2.5)$$

Uočimo da je $(9, 15) = 3$ i $3 \mid 12$ pa kongruencija (2.5) prema prethodnom teoremu ima 3 rješenja modulo 15. Podijelimo li tu kongruenciju s 3, dobivamo

$$3x \equiv 4 \pmod{5}. \quad (2.6)$$

Kako je $(3, 5) = 1$, ta kongruencija ima jedinstveno rješenje modulo 5. Iz Bézoutovog identiteta slijedi da postoje $u, v \in \mathbb{Z}$ takvi da je $3u + 5v = 1$, tj. $3u \equiv 1 \pmod{5}$. Oдавde se lako vidi da je $u \equiv 2 \pmod{5}$ (ako to nije slučaj, onda se u može odrediti korištenjem Euklidovog algoritma kako smo ranije pokazali). Množenjem lijeve i desne strane kongruencije (2.6) s $u = 2$ dobivamo

$$6x \equiv 8 \pmod{5}.$$

Oдавde slijedi da je $x \equiv 3 \pmod{5}$ rješenje kongruencije (2.6) i kongruencije (2.5). Rješenja modulo 15 kongruencije (2.5) dana su sa

$$x \equiv 3, 3 + 5, 3 + 10 \equiv 3, 8, 13 \pmod{15}.$$

Zadatak 2.1. *Riješite kongruenciju*

$$16x \equiv 27 \pmod{29}. \quad (2.7)$$

Rješenje. Kako je $(16, 29) = 1$, postoji jedinstveno rješenje modulo 29 kongruencije (2.7). Odredimo najprije u sa svojstvom $16u \equiv 1 \pmod{29}$. Euklidov algoritam daje

$$\begin{aligned} 29 &= 16 \cdot 1 + 13, \\ 16 &= 13 \cdot 1 + 3, \\ 13 &= 3 \cdot 4 + 1, \\ 3 &= 1 \cdot 3. \end{aligned}$$

Sada u možemo odrediti primjenom rekursivnih relacija:

i	-1	0	1	2	3
q_i			1	1	4
u_i	0	1	-1	2	-9

Stoga je $u \equiv -9 \equiv 20 \pmod{29}$. Množenjem lijeve i desne strane kongruencije (2.7) s dobivenim u dobivamo

$$16 \cdot 20x \equiv 27 \cdot 20 \pmod{29},$$

odnosno

$$x \equiv 27 \cdot 20 \equiv 18 \pmod{29}.$$

◇

Zadatak 2.2. *Riješite kongruenciju:*

$$8x \equiv 20 \pmod{36}.$$

Sada ćemo promotriti postojanje zajedničkog rješenja danog sustava kongruencija čiji su moduli u parovima relativno prosti. Tu će nam pomoći sljedeći teorem:

Teorem 2.2. (Kineski teorem o ostatcima, [3]) *Neka su $m_1, m_2, \dots, m_r \in \mathbb{N}$ u parovima relativno prosti i neka su $a_1, a_2, \dots, a_r \in \mathbb{Z}$. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots, \quad x \equiv a_r \pmod{m_r} \quad (2.8)$$

ima jedinstveno rješenje modulo $m = m_1 m_2 \cdots m_r$ i ono je dano sa

$$x \equiv n_1 x_1 + \cdots + n_r x_r \pmod{m},$$

gdje je $n_j = \frac{m}{m_j}$ i

$$n_j x_j \equiv a_j \pmod{m_j}, \quad j = 1, \dots, r.$$

Primjer 2.2. *Riješimo sustav kongruencija:*

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

Uočimo najprije da su 3, 5 i 7 u parovima relativno prosti prirodni brojevi pa možemo primijeniti Kineski teorem o ostatcima. Stavimo $m = 3 \cdot 5 \cdot 7 = 105$. Tada imamo:

- I. $n_1 = \frac{m}{3} = 35$ i tražimo rješenje linearne kongruencije $35x_1 \equiv 2 \pmod{3}$. Lako se vidi da je tada $2x_1 \equiv 2 \pmod{3}$, odnosno $x_1 = 1$.
- II. $n_2 = \frac{m}{5} = 21$ i tražimo rješenje linearne kongruencije $21x_2 \equiv 3 \pmod{5}$. Odavde je $x_2 \equiv 3 \pmod{5}$ pa možemo uzeti $x_2 = 3$.

III. $n_3 = \frac{m}{7} = 15$ i tražimo rješenje linearne kongruencije $15x_3 \equiv 2 \pmod{7}$. Tada je $x_3 \equiv 2 \pmod{7}$, odnosno $x_3 = 2$.

Stoga je rješenje polaznog sustava kongruencija dano sa

$$x \equiv 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 \equiv 23 \pmod{105}.$$

Primjer 2.3. Riješimo sustave kongruencija:

$$(a) \quad x \equiv 5 \pmod{8}, \quad x \equiv 6 \pmod{18},$$

$$(b) \quad x \equiv 5 \pmod{8}, \quad x \equiv 15 \pmod{18},$$

Kako 8 i 6 nisu u parovima relativno prosti prirodni brojevi, ne možemo direktno primijeniti Kineski teorem o ostatcima. Dane ćemo sustave kongruencija svesti na ekvivalentne sustave kongruencija.

Naime, vrijedi sljedeće:

$$\begin{aligned} x \equiv 6 \pmod{18} &\iff x \equiv 6 \pmod{2}, \quad x \equiv 6 \pmod{9} \\ &\iff x \equiv 0 \pmod{2}, \quad x \equiv 6 \pmod{9}. \end{aligned}$$

Stoga je sustav kongruencija zadan u (a) ekvivalentan sustavu:

$$x \equiv 5 \pmod{8}, \quad x \equiv 0 \pmod{2}, \quad x \equiv 6 \pmod{9}$$

Još uvijek nisu zadovoljeni uvjeti Kineskog teorema o ostatcima jer brojevi 8 i 2 nisu u parovima relativno prosti. Stoga najprije rješavamo podsustav

$$x \equiv 5 \pmod{8}, \quad x \equiv 0 \pmod{2}.$$

Uočimo da iz $x \equiv 5 \pmod{8}$ slijedi $x \equiv 1 \pmod{2}$ pa ovaj sustav nema rješenja. Slijedi da ni sustav kongruencija u (a) nema rješenja.

Lako se vidi da je sustav kongruencija zadan u (b) ekvivalentan sustavu

$$x \equiv 5 \pmod{8}, \quad x \equiv 1 \pmod{2}, \quad x \equiv 6 \pmod{9},$$

kod kojega opet najprije treba riješiti podsustav

$$x \equiv 5 \pmod{8}, \quad x \equiv 1 \pmod{2}.$$

Uočimo da iz $x \equiv 5 \pmod{8}$ slijedi $x \equiv 1 \pmod{2}$, dok obrat te tvrdnje ne vrijedi. Stoga je rješenje ovoga podsustava $x \equiv 5 \pmod{8}$ i drugi sustav kongruencija ekvivalentan je sustavu

$$x \equiv 5 \pmod{8}, \quad x \equiv 6 \pmod{9}.$$

Na taj sustav možemo primijeniti Kineski teorem o ostatcima jer su 8 i 9 relativno prosti. Stavimo $m = 8 \cdot 9 = 72$. Tada imamo:

- I. $n_1 = \frac{m}{8} = 9$ i tražimo rješenje linearne kongruencije $9x_1 \equiv 5 \pmod{8}$.
Lako se vidi da je tada $x_1 \equiv 5 \pmod{8}$, odnosno $x_1 = 5$.
- II. $n_2 = \frac{m}{9} = 8$ i tražimo rješenje linearne kongruencije $8x_2 \equiv 6 \pmod{9}$.
Odatavde je $-x_2 \equiv 6 \pmod{9}$, tj. $x_2 \equiv -6 \equiv 3 \pmod{9}$ pa možemo uzeti $x_2 = 3$.

Stoga je traženo rješenje sustava kongruencija u (b) dano sa

$$x \equiv 9 \cdot 5 + 8 \cdot 3 \equiv 69 \pmod{72}.$$

Kao što možemo vidjeti u prethodnom primjeru, ako na sustav linearnih kongruencija ne možemo direktno primijeniti Kineski teorem o ostatcima, onda dani sustav kongruencija svodimo na ekvivalentni sustav kongruencija na koji ćemo moći primijeniti Kineski teorem o ostatcima ili dobivamo da ekvivalentni sustav nema rješenje.

Zadatak 2.3. Riješite sustav kongruencija:

$$x \equiv 1 \pmod{4}, \quad x \equiv 5 \pmod{6}, \quad x \equiv 4 \pmod{7}.$$

Rješenje. Brojevi 4, 6 i 7 nisu u parovima relativno prosti pa ne možemo direktno primijeniti Kineski teorem o ostatcima. Kako je

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

početni sustav kongruencija ekvivalentan je sustavu kongruencija

$$x \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{7}.$$

Još uvijek nisu zadovoljene pretpostavke Kineskog teorema o ostatcima pa najprije rješavamo podsustav

$$x \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{2}.$$

Rješenje tog sustava kongruencija je $x \equiv 1 \pmod{4}$ pa je početni sustav kongruencija ekvivalentan sustavu kongruencija

$$x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{7}.$$

Na tako zadan sustav kongruencija možemo primijeniti Kineski teorem o ostatcima jer su 4, 3 i 7 u parovima relativno prosti brojevi.

Imamo sljedeće: $m = 4 \cdot 3 \cdot 7 = 84$ i

- I. $n_1 = \frac{m}{4} = 21$, $21x_1 \equiv 1 \pmod{4}$, tj. $x_1 \equiv 1 \pmod{4}$ pa je $x_1 = 1$,
 II. $n_2 = \frac{m}{3} = 28$, $28x_2 \equiv 2 \pmod{3}$, tj. $x_2 \equiv 2 \pmod{3}$ pa je $x_2 = 2$,
 III. $n_3 = \frac{m}{3} = 12$, $12x_3 \equiv 4 \pmod{7}$, tj. $5x_3 \equiv 4 \pmod{7}$ pa je $x_3 = 5$.

Stoga je traženo rješenje sustava kongruencija dano sa

$$x \equiv 21 \cdot 1 + 28 \cdot 2 + 12 \cdot 5 \equiv 53 \pmod{84}.$$

◇

Zadatak 2.4. *Riješite sustav kongruencija:*

$$x \equiv 5 \pmod{6}, \quad x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}.$$

3. Eulerova funkcija i Eulerov teorem

U ovom ćemo odjeljku definirati Eulerovu funkciju i iskazati važan teorem u teoriji brojeva kojega je dokazao Euler u 18. stoljeću. Prije no što navedemo osnovnu definiciju i glavni rezultat ovoga odjeljka, potrebno je promotriti i još neke skupove ostataka modulo $n \in \mathbb{N}$.

Definicija 3.1. *Neka je $n \in \mathbb{N}$. Skup $S = \{a_1, \dots, a_k\} \subseteq \mathbb{Z}$ naziva se reducirani sustav ostataka modulo n ako za svaki $b \in \mathbb{Z}$, $(b, n) = 1$ postoji jedinstveni $a_i \in S$ takav da je $b \equiv a_i \pmod{n}$.*

Primjer 3.1. *Potpun sustav ostataka modulo 8 je $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Ako želimo odrediti reducirani sustav ostataka modulo 8, onda iz tog potpunog sustava ostataka trebamo isključiti elemente koji nisu relativno prosti s 8. Stoga je $\{1, 3, 5, 7\}$ reducirani sustav ostataka modulo 8.*

Uočimo da reduciranih sustava ostataka modulo n ima beskonačno mnogo, ali svi imaju jednak broj elemenata.

Definicija 3.2. *Neka je $n \in \mathbb{N}$ i $U_n = \{a \in \mathbb{N} : a \leq n, (a, n) = 1\}$. Funkciju $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ definiranu formulom*

$$\varphi(n) = |U_n|$$

nazivamo Eulerova funkcija.

Uočimo da je s $\varphi(n)$ dan broj elemenata u reduciranom sustavu ostataka modulo n i vrijedi $\varphi(n) \leq n$.

Primjer 3.2. Iz Primjera 3.1. slijedi da je $\varphi(8) = 4$.

Primjer 3.3. Ako je p prosti broj, onda je $\{1, \dots, p-1\}$ reducirani sustav ostataka modulo p pa je $\varphi(p) = p-1$. Vrijedi i obrat te tvrdnje: iz $\varphi(p) = p-1$ slijedi da je broj prirodnih brojeva koji su manji od p i relativno su prosti s p jednak $p-1$. Stoga je 1 jedini pozitivni djelitelj od p koji je manji od p , tj. p je prosti broj.

Teorem 3.1. ([3]) Eulerova je funkcija multiplikativna. Za $n = \prod_p p^{\alpha_p}$, vrijedi

$$\varphi(n) = \prod_p p^{\alpha_p-1}(p-1).$$

Primjer 3.4. Kako je $1500 = 2^2 5^3 3$, broj prirodnih brojeva manjih od 1500 koji su relativno prosti s 1500 jednak je $\varphi(1500) = 2(2-1)3^0(3-1)5^2(5-1) = 400$.

Zadatak 3.1. Odredite sve $n \in \mathbb{N}$ za koje je $\varphi(n)$ neparni broj.

Rješenje. Uočimo da je $\varphi(1) = 1$. Kako za $n = \prod_p p^{\alpha_p}$, vrijedi

$$\varphi(n) = \prod_p p^{\alpha_p-1}(p-1),$$

odavde slijedi da ako n ima neparni prosti faktor p , onda je $p-1$ parni broj pa je i $\varphi(n)$ parni broj. Stoga zaključujemo, ako je $\varphi(n)$ neparni, on može imati samo parne proste faktore pa je $n = 2^\alpha$. Odavde je $\varphi(n) = 2^{\alpha-1}$ i neparno je samo ako je $\alpha = 1$. Time je pokazano da je $\varphi(n)$ neparni broj za $n = 1$ i $n = 2$.

◇

Zadatak 3.2. Dokažite da ne postoje $n, m \in \mathbb{N}$ sa svojstvom $\varphi(n) = 2 \cdot 7^m$.

Rješenje. U prethodnom smo zadatku komentirali da $p-1$ mora dijeliti $\varphi(n)$. Ako je $\varphi(n) = 2 \cdot 7^m$, slijedi da $p-1$ može biti neki od sljedećih brojeva: $1, 2, 2 \cdot 7^t, 7^t, t \in \{1, \dots, m\}$. Slijedi da p može biti $2, 3, 2 \cdot 7^t + 1, 7^t + 1, t \in \{1, \dots, m\}$. Kako je za $t \in \{1, \dots, m\}$

$$7^t + 1 \equiv 0 \pmod{2},$$

to je $7^t + 1$ paran i veći ili jednak od 8 pa ne može biti prost. Slično, iz

$$2 \cdot 7^t + 1 \equiv 0 \pmod{3}$$

zaključujemo da broj $2 \cdot 7^t + 1$ ne može biti prosti za $t \in \{1, \dots, m\}$. Dolazimo do zaključka da su jedini mogući prosti faktori broja n brojevi 2 i 3, tj. $n = 2^\alpha 3^\beta$. Uvjet $\varphi(n) = 2 \cdot 7^m$ vodi na jednažbu

$$2^{\alpha-1} 3^{\beta-1} 2 = 2 \cdot 7^m$$

čija su rješenja $\alpha = 1, \beta = 1, m = 0$. Zaključujemo da ne postoje $n, m \in \mathbb{N}$ s traženim svojstvom. \diamond

Zadatak 3.3. *Odredite sve $n \in \mathbb{N}$ sa svojstvom $\varphi(n) = 12$.*

Zadatak 3.4. *Dokažite da jednakost*

$$\sigma(n) + \varphi(n) = n\tau(n)$$

vrijedi ako i samo ako je n prosti broj.

Rješenje. Pretpostavimo da vrijedi gornja jednakost i pretpostavimo da n nije prosti broj. Tada n ima, osim 1 i n , još barem jednog pozitivnog djelitelja manjeg od n pa vrijedi

$$\sigma(n) < 1 + n(\tau(n) - 1).$$

No tada je

$$\varphi(n) = n\tau(n) - \sigma(n) > n\tau(n) - 1 - n(\tau(n) - 1) = n - 1,$$

što je kontradikcija.

Drugi smjer slijedi lagano jer za prosti broj n vrijedi $\varphi(n) = n - 1, \tau(n) = 2, \sigma(n) = n + 1$. \diamond

Teorem 3.2. (Eulerov teorem, [3]) *Neka je $a \in \mathbb{Z}, n \in \mathbb{N}$. Ako je $(a, n) = 1$, onda je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad (3.1)$$

Primjer 3.5. *Kako je $n = 45 = 3^2 \cdot 5$, slijedi $\varphi(45) = 24$. Iz Eulerovog teorema slijedi da za sve $a \in \mathbb{Z}, (a, 45) = 1$ vrijedi*

$$a^{24} \equiv 1 \pmod{45}.$$

Korolar 3.1. (Mali Fermatov teorem, [3]) Neka je p prosti broj i $a \in \mathbb{Z}$. Tada je

$$a^p \equiv a \pmod{p}.$$

Specijalno, ako $p \nmid a$, onda je

$$a^{p-1} \equiv 1 \pmod{p}.$$

Napomena 3.1. Obrat Malog Fermatovog teorema ne vrijedi. Može se pokazati da je

$$2^{340} \equiv 1 \pmod{341},$$

ali $341 = 13 \cdot 31$. Brojevi koji zadovoljavaju relaciju iz Malog Fermatovog teorema, ali nisu prosti nazivaju se pseudoprosti brojevi. Više o pseudoprostim brojevima možete naći u [3, 6].

Zadatak 3.5. Ako je p prosti broj, dokažite da vrijedi:

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

Rješenje. Kako je p prosti broj, za $a \in \{1, 2, \dots, p-1\}$ je $(a, p) = 1$ i prema Malom Fermatovom teoremu vrijedi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Stoga je

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv \underbrace{1 + \dots + 1}_{p-1} \equiv p-1 \equiv -1 \pmod{p}.$$

◇

Zadatak 3.6. Odredite ostatak pri dijeljenju broja $n = 3^{80} + 7^{80}$ s 11.

Rješenje. Iz $(3, 11) = (7, 11) = 1$ i Malog Fermatovog teorema slijedi

$$3^{10} \equiv 1 \pmod{11}, \quad 7^{10} \equiv 1 \pmod{11}.$$

Potenciramo li lijeve i desne strane prethodnih kongruencija s 8, dobivamo

$$3^{80} \equiv 1 \pmod{11}, \quad 7^{80} \equiv 1 \pmod{11}.$$

Zbrajanjem prethodnih kongruencija dobivamo

$$3^{80} + 7^{80} \equiv 2 \pmod{11}$$

pa je traženi ostatak jednak 2.

◇

Zadatak 3.7. *Odredite moguće ostatke pri dijeljenju 100-te potencije cijelog broja sa 125.*

Rješenje. Kako je $\varphi(125) = 100$, iz Eulerovog teorema slijedi da za sve $a \in \mathbb{Z}$, $(a, 125) = 1$ vrijedi

$$a^{100} \equiv 1 \pmod{125}. \quad (3.2)$$

Ako $(a, 125) \neq 1$, onda je a višekratnik broja 5, tj. $a = 5k, k \in \mathbb{Z}$. No onda je

$$a^{100} \equiv (5k)^{100} \equiv 5^3 5^{97} k^{100} \equiv 0 \pmod{125}. \quad (3.3)$$

Iz (3.2) i (3.3) zaključujemo da su mogući ostaci 0 i 1. \diamond

Zadatak 3.8. *Dokažite da za svaki prirodni broj n brojevi n i $n^{8k+1}, k \in \mathbb{N}$ daju isti ostatak pri dijeljenju s 15.*

Rješenje. Za $(n, 15) = 1$ iz Eulerovog teorema slijedi $n^{\varphi(15)} \equiv n^8 \equiv 1$ pa je i $n^{8k+1} \equiv n \pmod{15}, k \in \mathbb{N}$.

Ako je $(n, 15) \neq 1$, onda je $(n, 15) \in \{3, 5, 15\}$. Za $(n, 15) = 3$ slijedi $(n, 5) = 1$ pa primjenom Malog Fermatovog teorema dobivamo $n^4 \equiv 1 \pmod{5}$, odnosno

$$n^{8k+1} \equiv n \pmod{5}. \quad (3.4)$$

Kako $3 \mid n$, slijedi $n \equiv 0 \pmod{3}$ pa je

$$n^{8k+1} \equiv n \equiv 0 \pmod{3}. \quad (3.5)$$

Iz (3.4), (3.5) i $(3, 5) = 1$ slijedi tvrdnja. Slučajevi $(n, 15) \in \{5, 15\}$ dokazuju se vrlo slično i ostavljamo ih za vježbu. \diamond

Zadatak 3.9. *Neka je $n = pq$, p, q različiti su prosti brojevi. Ako su $a, b \in \mathbb{N}$ takvi da vrijedi $ab \equiv 1 \pmod{\varphi(n)}$, dokažite da za sve $x \in \mathbb{Z}$ vrijedi*

$$x^{ab} \equiv x \pmod{n}.$$

Zadatak 3.10. *Koristeći Eulerov teorem riješite linearnu kongruenciju*

$$25x \equiv 53 \pmod{62}.$$

Rješenje. Kako je $\varphi(62) = 30$ i $(25, 62) = 1$, iz Eulerovog teorema slijedi

$$25^{30} \equiv 1 \pmod{62}.$$

Pomnožimo li lijevu i desnu stranu zadane kongruencije s 25^{29} , dobivamo

$$25^{30}x \equiv 25^{29}53 \pmod{62},$$

tj.

$$x \equiv 25^{29}53 \equiv 17 \pmod{62}.$$

◇

Zadatak 3.11. *Koristeći Eulerov teorem riješite linearnu kongruenciju*

$$41x \equiv 17 \pmod{77}.$$

4. Primitivni korijeni i indeksi

Kako bismo uspješno rješavali kongruencije oblika $x^k \equiv a \pmod{n}$, $k \geq 2$, $(a, n) = 1$, upoznat ćemo se s pojmom primitivnog korijena modulo n i indeksa. Njihovom primjenom polaznu kongruenciju svest ćemo na linearnu, a metode za njeno rješavanje opisali smo u drugom odjeljku ovog poglavlja.

Definicija 4.1. *Neka je $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, n) = 1$. Najmanji prirodni broj d sa svojstvom*

$$a^d \equiv 1 \pmod{n}$$

naziva se red od a modulo n .

Propozicija 4.1. ([3]) *Neka je d red od a modulo n . Za $k \in \mathbb{N}$ vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.*

Primjer 4.1. *Odredimo red od 2 modulo 9. Ako je d traženi red, onda prema prethodnoj propoziciji slijedi $d \mid \varphi(9) = 6$, tj. $d \in \{1, 2, 3, 6\}$. Kako je*

$$\begin{aligned} 2^1 &\equiv 2 \pmod{9}, \\ 2^2 &\equiv 4 \pmod{9}, \\ 2^3 &\equiv 8 \pmod{9}, \\ 2^6 &\equiv 1 \pmod{9}, \end{aligned}$$

dobivamo $d = 6$.

Zadatak 4.1. *Neka je p neparni prosti broj i $n = 5^p + 1$. Odredite red od 5 modulo n .*

Rješenje. Iz $n = 5^p + 1$ slijedi

$$5^p \equiv -1 \pmod{n}. \quad (4.1)$$

Kvadriranjem lijeve i desne strane te kongruencije dobivamo

$$5^{2p} \equiv 1 \pmod{n}.$$

Iz Propozicije 4.1. zaključujemo $d \mid 2p$ pa je $d \in \{1, 2, p, 2p\}$. Kako je p neparni prosti broj, to je $n \geq 126$ pa

$$\begin{aligned} 5^1 &\not\equiv 1 \pmod{n}, \\ 5^2 &\not\equiv 1 \pmod{n}. \end{aligned}$$

Iz (4.1) slijedi da je $d \neq p$ pa mora biti $d = 2p$. \diamond

Zadatak 4.2. *Neka je p neparni prosti broj, $p \mid F_n = 2^{2^n} + 1, n \geq 2$. Dokažite da postoji $k \in \mathbb{Z}$ takav da je $p = k \cdot 2^{n+1} + 1$.*

Rješenje. Uočimo da će tvrdnja biti dokazna ako pokažemo da $2^{n+1} \mid p - 1$.

Iz $p \mid F_n = 2^{2^n} + 1$ slijedi

$$\begin{aligned} F_n &\equiv 0 \pmod{p}, \\ 2^{2^n} &\equiv -1 \pmod{p}, \\ 2^{2^{n+1}} &\equiv 1 \pmod{p}. \end{aligned} \quad (4.2)$$

Označimo li s d red od 2 modulo p , onda iz zadnje kongruencije i Propozicije 4.1. slijedi da $d \mid 2^{n+1}$. Ako je $d = 2^t, t \leq n$, onda je

$$2^{2^t} \equiv 1 \pmod{p}.$$

Uzastopnim kvadriranjem lijeve i desne strane te kongruencije došli bismo do kongruencije

$$2^{2^n} \equiv 1 \pmod{p},$$

što je u kontradikciji s (4.2). Zaključujemo da je red od 2 modulo p jednak 2^{n+1} . Kako $d = 2^{n+1} \mid \varphi(p) = p - 1$, slijedi tvrdnja. \diamond

Zadatak 4.3. *Neka je p prosti broj takav da je $p = 2q + 1$, gdje je q neparni prosti broj i neka je $z \in \mathbb{Z}$ takav da je $(z, p) = 1$ i $z^4 \not\equiv 1 \pmod{p}$. Odredite red od $-z^2$ modulo p .*

Definicija 4.2. Neka je $n \in \mathbb{N}, a \in \mathbb{Z}, (a, n) = 1$. Ako je red od a modulo n jednak $\varphi(n)$, onda se a naziva primitivni korijen modulo n .

Napomena 4.1. Može se pokazati da ne postoji primitivni korijen modulo n , za svaki $n \in \mathbb{N}$. Također, primitivni korijen modulo n ne mora biti jedinstven. Više detalja o svojstvima primitivnih korijena može se naći u [3].

Primjer 4.2. U Primjeru 4.1. pokazali smo da je red od 2 modulo 9 jednak $6 = \varphi(9)$ pa je 2 primitivni korijen modulo 9.

Definicija 4.3. Ako je a primitivni korijen modulo n , onda za svaki $z \in \mathbb{Z}$ takav da je $(z, n) = 1$ postoji jedinstveni $l \in \{0, 1, \dots, \varphi(n) - 1\}$ takav da vrijedi

$$a^l \equiv z \pmod{n}.$$

EkspONENT l naziva se indeks od z u odnosu na a i označava se s $\text{ind}_a z$ ili $\text{ind} z$.

Primjer 4.3. U Primjeru 4.2. komentirali smo da je 2 primitivni korijen modulo 9. Tablica indeksa toga primitivnog korijena dana je sa

z	1	2	4	5	7	8
$\text{ind } z$	0	1	2	5	4	3

Teorem 4.1. ([3]) Neka je a primitivni korijen modulo $n \in \mathbb{N}$ i $z_1, z_2 \in \mathbb{Z}, (z_1, n) = (z_2, n) = 1$. Tada vrijedi:

- (1) $z_1 \equiv z_2 \pmod{n} \iff \text{ind } z_1 \equiv \text{ind } z_2 \pmod{\varphi(n)},$
- (2) $\text{ind } z_1 + \text{ind } z_2 \equiv \text{ind } z_1 z_2 \pmod{\varphi(n)},$
- (3) $\text{ind } 1 = 0, \text{ind } a = 1,$
- (4) $\text{ind}(z_1^m) \equiv m \text{ind } z_1 \pmod{\varphi(n)}.$

Uočimo da su svojstva (2) – (4) navedena u prethodnom teoremu analogna svojstvima logaritamske funkcije.

Primjer 4.4. Riješimo kongruenciju $x^{11} \equiv 7 \pmod{9}$. Koristeći pojam indeksa i primjenom svojstava indeksa navedenih u prethodnom teoremu, dobivamo

$$11 \text{ind } x \equiv \text{ind } 7 \pmod{6}.$$

Iz tablice iz Primjera 4.3. iščitavamo $\text{ind } 7 = 4$, a kako je $11 \equiv -1 \pmod{6}$, dolazimo do kongruencije

$$-\text{ind } x \equiv 4 \pmod{6}.$$

Oдавde je

$$\text{ind } x \equiv -4 \equiv 2 \pmod{6}.$$

Iz spomenute tablice sada iščitavamo $x \equiv 4 \pmod{9}$.

Zadatak 4.4.

(i) Odredite najmanji primitivni korijen modulo 17.

(ii) Riješite sljedeće kongruencije:

(a) $7x \equiv 5 \pmod{17}$,

(b) $x^8 \equiv 8 \pmod{17}$,

(c) $x^7 \equiv 5 \pmod{17}$.

(iii) Odredite ostatak pri dijeljenju broja $2103^{729} \cdot 602^{97}$ sa 17.

Rješenje.

(i) Uočimo da je $\varphi(17) = 16$. Ako je d red nekog elementa modulo 17, onda mora vrijediti $d \mid 16$, tj. $d \in \{1, 2, 4, 8, 16\}$. Ispitajmo je li broj 2 primitivni korijen modulo 17. Vrijedi:

$$2^1 \equiv 2 \pmod{17},$$

$$2^2 \equiv 4 \pmod{17},$$

$$2^4 \equiv 16 \pmod{17},$$

$$2^8 \equiv 1 \pmod{17}.$$

Zaključujemo da je red od 2 modulo 17 jednak 8 pa 2 nije primitivni korijen modulo 17.

Promotrimo broj 3. Vrijedi:

$$3^1 \equiv 3 \pmod{17},$$

$$3^2 \equiv 9 \pmod{17},$$

$$3^4 \equiv 13 \pmod{17},$$

$$3^8 \equiv 16 \pmod{17},$$

$$3^{16} \equiv 1 \pmod{17}.$$

Zaključujemo da je 3 najmanji primitivni korijen modulo 17.

(ii) Koristit ćemo primitivni korijen 3.

(a) Prijeđemo li na indekse u kongruenciji $7x \equiv 5 \pmod{17}$, dobivamo (jer je $3^{11} \equiv 7 \pmod{17}$, $3^5 \equiv 5 \pmod{17}$)

$$\begin{aligned} \operatorname{ind}_3 7 + \operatorname{ind}_3 x &\equiv \operatorname{ind}_3 5 \pmod{16} \\ 11 + \operatorname{ind}_3 x &\equiv 5 \pmod{16} \\ \operatorname{ind}_3 x &\equiv -6 \equiv 10 \pmod{16}. \end{aligned}$$

Odavde zaključujemo da je $x \equiv 3^{10} \equiv 8 \pmod{17}$.

(b) Prelaskom na indekse u kongruenciji $x^8 \equiv 8 \pmod{17}$, dobivamo linearnu kongruenciju

$$8 \operatorname{ind}_3 x \equiv 10 \pmod{16}.$$

Ta linearna kongruencija nema rješenja jer $(8, 16) \nmid 10$ pa ni polazna kongruencija nema rješenja.

(c) Rješavanje te kongruencije ostavljamo za vježbu. Rješenje je $x \equiv 10 \pmod{17}$.

(iii) Trebamo odrediti ostatak pri dijeljenju broja $z = 2103^{729} \cdot 602^{97}$ sa 17. Uočimo najprije da je $2103 \equiv 12 \pmod{17}$, $602 \equiv 7 \pmod{17}$. Stoga je $z \equiv 12^{729} 7^{97} \pmod{17}$. Prelaskom na indekse dobivamo

$$\operatorname{ind}_3 z \equiv 729 \operatorname{ind}_3 12 + 97 \operatorname{ind}_3 7 \equiv 0 \pmod{16}.$$

Odavde je $z \equiv 3^0 \equiv 1 \pmod{17}$.

◇

Zadatak 4.5. *Koristeći indekse riješite kongruenciju*

$$7x^{15} \equiv 8 \pmod{19}.$$

5. Wilsonov i Lagrangeov teorem

Mnogi problemi vezani uz kongruencije mogu se riješiti primjenom Wilsonova i Lagrangeova teorema. Promatrat ćemo ih u ovome odjeljku.

Teorem 5.1. (Wilsonov teorem i obrat, [3]) *Prirodni broj p prost je broj ako i samo ako vrijedi*

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

Primjer 5.1. *Kako je 17 prosti broj, iz Wilsonovog teorema slijedi $16! \equiv -1 \pmod{17}$. Oдавde možemo zaključiti da je ostatak pri dijeljenju broja $16!$ sa 17 jednak 16.*

Zadatak 5.1. *Dokažite da je $18! \equiv -1 \pmod{437}$.*

Rješenje. Uočimo da je $437 = 19 \cdot 23$. Kako su 19 i 23 prosti brojevi, na njih možemo primijeniti Wilsonov teorem pa dobivamo

$$18! \equiv -1 \pmod{19}, \quad 22! \equiv -1 \pmod{23}.$$

Iz posljednje kongruencije dobiva se

$$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23},$$

tj. $18! \equiv -1 \pmod{23}$. Kako je $(19, 23) = 1$, slijedi tvrdnja. \diamond

Zadatak 5.2. *Neka je $p \geq 5$ prosti broj. Odredite ostatak pri dijeljenju broja $2^{p+1}(p-3)!$ s p .*

Teorem 5.2. (Lagrangeov teorem, [3]) *Ako je p prosti broj i $P(x)$ polinom s cjelobrojnim koeficijentima stupnja n kojemu vodeći koeficijent nije djeljiv s p , onda kongruencija*

$$P(x) \equiv 0 \pmod{p} \tag{5.1}$$

ima najviše n rješenja modulo p .

Primjer 5.2. *Prema Lagrangeovom teoremu, za svaki prosti broj p kongruencija $x^2 \equiv 1 \pmod{p}$ ima najviše dva rješenja modulo p . Za $p \neq 2$ rješenja su $x \equiv \pm 1 \pmod{p}$, dok je za $p = 2$ rješenje $x \equiv 1 \pmod{2}$ (jer je $1 \equiv -1 \pmod{2}$).*

Zadatak 5.3. *Riješite kongruencije:*

(i) $x^3 + x^2 - 2x \equiv 0 \pmod{5}$,

(ii) $100x^{100} + x^3 + x^2 - 2x \equiv 0 \pmod{5}$,

(iii) $x^3 + x^2 - 2x \equiv 0 \pmod{9}$,

(iv) $x^3 + x^2 - 2x \equiv 0 \pmod{45}$.

Rješenje.

- (i) Kako je 5 prosti broj, prema Lagrangeovom teoremu zaključujemo da kongruencija $x^3 + x^2 - 2x \equiv 0 \pmod{5}$ ima najviše tri rješenja modulo 5. Direktnom provjerom vidi se da su $x = 0, 1$ rješenja, $x = 2$ nije rješenje i $x = 3$ je rješenje. Kako kongruencija može imati najviše tri rješenja, slučaj $x = 4$ nije potrebno provjeravati. Zaključujemo da su sva rješenja $x \equiv 0, 1, 3 \pmod{5}$.

- (ii) Uočimo da vrijedi

$$100x^{100} + x^3 + x^2 - 2x \equiv x^3 + x^2 - 2x \equiv 0 \pmod{5}$$

pa je ta kongruencija ekvivalentna kongruenciji u (i).

- (iii) Uočimo da na kongruenciju $x^3 + x^2 - 2x \equiv 0 \pmod{9}$ ne možemo primijeniti Lagrangeov teorem. Direktnom provjerom svih mogućih slučajeva dobiva se $x \equiv 0, 1, 4, 7 \pmod{9}$.

- (iv) Kongruencija $x^3 + x^2 - 2x \equiv 0 \pmod{45}$ ekvivalentna je sustavu kongruencija

$$\begin{aligned} x^3 + x^2 - 2x &\equiv 0 \pmod{5}, \\ x^3 + x^2 - 2x &\equiv 0 \pmod{9}. \end{aligned}$$

Kako smo te sustave riješili u (i) i (iii), sva rješenja dobivaju se rješavanjem sustava kongruencija određenih sa:

$$\begin{aligned} x &\equiv 0, 1, 3 \pmod{5}, \\ x &\equiv 0, 1, 4, 7 \pmod{9}. \end{aligned}$$

Primjenom Kineskog teorema o ostacima dobivaju se rješenja

$$x \equiv 0, 1, 10, 13, 16, 18, 25, 28, 31, 36, 40, 43 \pmod{45}.$$

◇

Zadatak 5.4. *Riješite kongruenciju*

$$121x^{51} + x^3 - 3x \equiv -2 \pmod{11}.$$

6. Primjena kongruencija u kriptografiji

Sama teorija kongruencija ima vrlo široku primjenu. Ovdje ćemo pokazati primjenu u šifriranju i dešifriranju podataka. Znanstvena disciplina koja se bavi tim problemima zove se kriptografija. Poruku koju pošiljatelj želi poslati primatelju zovemo otvoreni tekst. Pošiljatelj šifrira otvoreni tekst koristeći ključ i kao rezultat dobiva šifrat koji šalje primatelju. Primatelj dešifrira dobivenu poruku kako bi dobio polazni otvoreni tekst. Više o metodama kriptografije može se vidjeti, primjerice, u [4].

Definicija 6.1. *Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ za koju vrijedi:*

1. \mathcal{P} je konačan skup svih mogućih osnovnih elementa otvorenog teksta.
2. \mathcal{C} je konačan skup svih mogućih osnovnih elemenata šifrata.
3. \mathcal{K} je prostor ključeva, tj. konačan skup svih mogućih ključeva.
4. Za svaki $k \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \rightarrow \mathcal{C}$ i $d_K : \mathcal{C} \rightarrow \mathcal{P}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in \mathcal{P}$.

U nastavku ćemo koristiti sljedeću korespondenciju između slova alfabeta $(A - Z)$ i cijelih brojeva.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tablica 2.1: Numerički ekvivalenti u engleskom alfabetu

6.1. Pomak alfabeta ili Cezarova šifra

Opisat ćemo najprije jednostavni kriptosustav koji se dobiva pomakom alfabeta, a naziva se i Cezarova šifra. Ovaj kriptosustav dobio je ime po Gaju Juliju Cezaru koji ga je u 1. st. pr. Kr. koristio za razmjenu poruka sa svojim generalima.

Definicija 6.2. Neka je $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1, \dots, 25\} = \mathbb{Z}_{26}$. Za $0 \leq K \leq 25$ definiramo

$$\begin{aligned} e_K(x) &= x + K \pmod{26}, \\ d_K(y) &= y - K \pmod{26}. \end{aligned}$$

Tako je zadana Cezarova šifra.

Primjer 6.1. Šifrirajmo *TB* Cezarovom šifrom koristeći numeričke ekvivalente i ključ $K = 20$. Vrijedi:

$$\begin{array}{rcll} T & B & \longrightarrow & 20 & 2 \\ & & \longrightarrow & 40 \pmod{26} & 22 \pmod{26} \\ & & \longrightarrow & 14 & 22 \\ & & \longrightarrow & N & V. \end{array}$$

Zadatak 6.1. Neka je primjenom Cezarove šifre na otvoreni tekst na hrvatskom jeziku dobiven šifrat

WXYHMVDRNIRD SHNIPY.

Odredite otvoreni tekst.

Rješenje. Uočimo najprije da su prva tri slova danog izraza tri uzastopna slova abecede pa njih lako možemo dešifrirati iz tablice. Ako uočimo da oni ne mogu predstavljati dio rečenice na hrvatskom jeziku, ne trebamo provjeravati ostala slova. Dešifriranje provodimo koristeći funkciju $d_K(y) = y - K \pmod{26}$, $K \in \{0, 1, \dots, 25\}$. Napravimo provjere:

- za $K = 1$ dobivamo *VWX*, a to nije početak riječi na hrvatskom jeziku,
- za $K = 2$ dobivamo *UVW* pa opet ne trebamo raditi daljnje provjere,
- za $K = 3$ dobivamo *TUV* pa ćemo provjeriti i iduća slova da vidimo hoće li to biti riječ na hrvatskom jeziku; kako se dobiva *TUVEJ*, na kraju opet zaključujemo da nije potrebno raditi daljnje provjere,
- za $K = 4$ dobivamo otvoreni tekst *STUDIRANJE NA ODJELU*.

◇

Zadatak 6.2. Primjenom Cezarove šifre iz otvorenog teksta na hrvatskom jeziku dobiven je šifrat

WXYQZYUCKTK.

Odredite funkciju dešifriranja i odgovarajući otvoreni tekst.

6.2. RSA kriptosustav

Ovdje ćemo opisati RSA kriptosustav koji se u praksi često koristi, a čija se sigurnost temelji na teškoći faktorizacije velikih prirodnih brojeva. Ovaj kriptosustav dobio je ime po autorima (Ron Rivest, Adi Shamir i Len Adleman) koji su ga predložili 1977. godine. Primjenu ovog kriptosustava ilustrirat ćemo na malim prirodnim brojevima.

Definicija 6.3. *Neka je $n = pq$, gdje su p i q različiti prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ te*

$$\mathcal{K} = \{(n, p, q, d, e) : \gcd(e, \varphi(n)) = 1, \\ de \equiv 1 \pmod{\varphi(n)}, d, e \in \mathbb{N} \text{ minimalni s tim svojstvom}\}.$$

Za $K = (n, p, q, d, e) \in \mathcal{K}$ i $x, y \in \mathbb{Z}_n$ definiramo

$$e_K(x) = x^e \pmod{n}, \\ d_K(y) = y^d \pmod{n}.$$

Tako zadan kriptosustav naziva se RSA kriptosustav. Parametar e naziva se enkripcijski eksponent, a d dekripcijski eksponent.

RSA kriptosustav temelji se na tvrdnji

$$(x^e)^d \equiv x \pmod{n},$$

koja je dana u Zadatku 3.9. Vrijednosti n, e u RSA kriptosustavu javne su pa uređeni par (n, e) nazivamo javni ključ. Faktorizacija broja n i parametar d tajni su jer onaj tko poznaje faktorizaciju od n , može lako odrediti $\varphi(n)$, a onda i d .

Primjer 6.2. *Primjenom RSA kriptosustava uz javni ključ $(n, e) = (143, 37)$ šifrirajmo poruku*

MATHOS

u engleskom alfabetu. Najprije odredimo numeričke ekvivalente danih slova: 13 1 20 8 15 19. Šifriranje provodimo koristeći funkciju $e_K(x) = x^{37} \pmod{143}$. Kako je

$$\begin{aligned} 13^{37} &\equiv 117 \pmod{143}, \\ 1^{37} &\equiv 1 \pmod{143}, \\ 20^{37} &\equiv 59 \pmod{143}, \\ 8^{37} &\equiv 112 \pmod{143}, \\ 15^{37} &\equiv 93 \pmod{143}, \\ 19^{37} &\equiv 123 \pmod{143}, \end{aligned}$$

šifrat je 117 1 59 112 93 123.

Zadatak 6.3. *Dešifrirajte poruku*

106 83 1 22 93

koja je šifrirana u RSA kriptosustavu s javnim ključem $(n, e) = (143, 37)$ nad engleskim alfabetom.

Rješenje. Najprije trebamo odrediti dekriptijski eksponent d . Kako je on rješenje kongruencije $de \equiv 1 \pmod{\varphi(n)}$, naprije odredimo $\varphi(143) = \varphi(11 \cdot 13) = 120$. Rješavanjem linearne kongruencije $37x \equiv 1 \pmod{120}$ dobivamo $d = 13$. Dešifriranje provodimo koristeći funkciju $d_K(x) = x^{13} \pmod{143}$. Kako je

$$\begin{aligned} 106^{13} &\equiv 2 \pmod{143}, \\ 83^{13} &\equiv 18 \pmod{143}, \\ 1^{13} &\equiv 1 \pmod{143}, \\ 22^{13} &\equiv 22 \pmod{143}, \\ 64^{13} &\equiv 15 \pmod{143}, \end{aligned}$$

šifrat je 2 18 1 22 15. Prevedemo li te numeričke ekvivalente u slova koristeći Tablicu 2.1 dobivamo *BRAVO*. \diamond

Zadatak 6.4. *U RSA kriptosustavu s javnim ključem*

$$K = (307829, 151)$$

(a) *šifrirajte poruku*

ZADATAK,

(b) *dešifrirajte poruku*

1195 45600 162514 162026.

7. Zadatci za vježbu

Zadatak 7.1. *Odredite:*

(a) *ostatak pri dijeljenju broja 2^{55} sa 17,*

(b) posljednje tri znamenke broja 2^{100} .

Zadatak 7.2. Dokažite sljedeće tvrdnje:

(a) $n \in \mathbb{N}$ djeljiv je s 3 (9) ako i samo ako je zbroj znamenki od n djeljiv s 3 (9).

(b) $n \in \mathbb{N}$ djeljiv je s 11 ako i samo ako je alternirajući zbroj znamenki od n djeljiv s 11.

Zadatak 7.3. Nađite sva rješenja sustava kongruencija

$$x + 2y \equiv 2 \pmod{23}, \quad x - 2y \equiv 3 \pmod{23}.$$

Zadatak 7.4. Riješite kongruencije:

$$(a) \quad 20x \equiv 16 \pmod{64} \quad (b) \quad 60x \equiv 185 \pmod{455}.$$

Zadatak 7.5. Riješite sustave kongruencija:

- (a) $x \equiv 5 \pmod{8}, \quad x \equiv 6 \pmod{18},$
 (b) $x \equiv 5 \pmod{8}, \quad x \equiv 15 \pmod{18},$
 (c) $x \equiv 5 \pmod{6}, \quad x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15},$
 (d) $x \equiv 5 \pmod{24}, \quad x \equiv 25 \pmod{28}, \quad x \equiv 8 \pmod{45}.$

Zadatak 7.6. Nađite najmanji $x \in \mathbb{Z}, x > 100$ koji je rješenje sustava kongruencija

$$5x \equiv 10 \pmod{18}, \quad x \equiv 2 \pmod{12}, \quad x \equiv 6 \pmod{8}.$$

Zadatak 7.7. Kojeg su oblika prirodni brojevi n za koje vrijedi $10 \mid 3n - 1, 5 \mid 4n - 3$ i $9 \mid 2n - 7$?

Zadatak 7.8. Ako se za učenike neke škole koja ima više od 100 učenika želi organizirati autobusni prijevoz, onda pri raspoređivanju u autobuse s 15 mjesta nakon popunjavanja svih autobusa u posljednjem autobusu ostane 6 učenika. Analogno, ako se popunjavaju autobusi s 40, odnosno 50 mjesta, onda u posljednjem autobusu ostane 1, odnosno 31 učenik. Može li škola imati parni broj učenika? Koliko škola ima učenika ako je poznato da ih je manje od 1000?

Zadatak 7.9. *Kineski generali prebrojavali su preživjele vojnike nakon bitke raspoređujući ih u kolone različite duljine i bilježeći koliko je vojnika ostalo kao višak u zadnjoj koloni. Ako je general na početku bitke imao 1200 vojnika, a vojnici raspoređeni u kolone duljine 5, 6, 7, 11 u zadnjem redu imaju, redom, 3, 3, 1, 11 vojnika, koliko je vojnika preživjelo bitku?*

Zadatak 7.10. *Odredite sve $0 < x \leq 1000$ koji su rješenje sustava kongruencija*

$$8x \equiv 5 \pmod{15}, \quad 5x \equiv 11 \pmod{21}, \quad 7x \equiv 55 \pmod{60}.$$

Zadatak 7.11. *Odredite sve $n \in \mathbb{N}$ takve da je $\varphi(n) = 16$.*

Zadatak 7.12. *Neka je $n \in \mathbb{N}$. Ako $\varphi(n) \mid n - 1$, pokažite da je tada n kvadratno slobodan, odnosno za $a \neq 1, a^2 \nmid n$.*

Zadatak 7.13. *Neka je $n > 4$ prirodni broj sa svojstvom da su $n - 1$ i $n + 1$ prosti brojevi. Dokažite da je tada $\varphi(n) \leq \frac{n}{3}$.*

Zadatak 7.14. *Dokažite da je $\varphi(4n) = 2\varphi(2n)$, za sve $n \in \mathbb{N}$.*

Zadatak 7.15. *Dokažite da jednačba $\varphi(n) = 14$ nema rješenja.*

Zadatak 7.16. *Odredite moguće ostatke pri dijeljenju brojeva $3a^{460} - 5$, $a \in \mathbb{Z}$ brojem 47.*

Zadatak 7.17. *Neka je $p > 3$ prosti broj. Odredite a ako je poznato da vrijedi*

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv a \pmod{p}.$$

Zadatak 7.18. *Koristeći Eulerov teorem riješite kongruenciju $41x \equiv 53 \pmod{62}$.*

Zadatak 7.19. *Neka je $n \in \mathbb{N}$ najmanji višekratnik broja 17 koji je rješenje sustava kongruencija*

$$n \equiv 10 \pmod{12}, \quad n \equiv 4 \pmod{18}.$$

Odredite ostatak pri dijeljenju broja $(n + 12)^{2200}$ sa 121.

Zadatak 7.20. *Neka su $m, n \in \mathbb{N}$, $(m, n) = 1$. Dokažite da vrijedi:*

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

Zadatak 7.21. Neka je $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, n) = 1$ i neka je d red od a modulo n . Ako je $m \in \mathbb{N}$ takav da vrijedi $a^m \equiv 1 \pmod{n}$, dokažite da $d \mid m$.

Zadatak 7.22. Odredite red od 3 modulo 91.

Zadatak 7.23. Neka je p neparni prosti broj. Ako $p \mid b^4 + 1$, $b \in \mathbb{N}$, odredite red od b modulo p .

Zadatak 7.24. Neka je $m \in \mathbb{N}$. Odredite oblik svih prostih faktora $p > 2$ broja $m^2 + 1$.

Zadatak 7.25. Neka je p prosti broj i neka je $a \in \mathbb{Z}$ takav da je red od a modulo p jednak 3. Dokažite sljedeće tvrdnje:

(a) $a^2 + a + 1 \equiv 0 \pmod{p}$,

(b) $(2a + 1)^2 \equiv -3 \pmod{p}$,

(c) red od $a + 1$ modulo p jednak je 6.

Zadatak 7.26. Pomoću indeksa riješite kongruencije:

(a) $x^{100} \equiv 16 \pmod{43}$ (b) $27x^{36} \equiv 42 \pmod{43}$.

Zadatak 7.27. Neka je p neparni prosti broj i $n_k = (p - 1)(kp + 1)$, $k \in \mathbb{N}$. Dokažite da $p \mid (p - 2)! + n_k 2^{n_k}$.

Zadatak 7.28. Ako za prirodni broj $n > 1$ vrijedi $(n - 1)! \equiv -1 \pmod{n}$, dokažite da je n prosti broj.

Zadatak 7.29. Riješite kongruenciju

$$x^{71} + x^2 - 2x \equiv 0 \pmod{71}.$$

Zadatak 7.30. Riješite sustav kongruencija

$$x^2 \equiv 1 \pmod{19}, \quad x \equiv 5 \pmod{11}.$$

Zadatak 7.31. Primjenom Cezarove šifre s pomakom 15 šifrirajte poruku **POBJEDNIK**.

Zadatak 7.32. U RSA kriptosustavu s javnim ključem $(65, 11)$ dešifrirajte poruku 49 11 28 134.

Zadatak 7.33. *Odredite najmanji dozvoljeni e takav da $(3193, e)$ bude javni ključ RSA kriptosustava i vrijedi*

$$e \equiv 1 \pmod{12}, \quad e \equiv 29 \pmod{56}.$$

Zadatak 7.34. *U RSA kriptosustavu s javnim ključem $(n, e) = (407, 103)$ odredite $a = d_K(2)$, a zatim riješite sustav kongruencija*

$$x \equiv a \pmod{9}, \quad x \equiv -1 \pmod{33}.$$

Zadatak 7.35. *Dešifrirajte brojeve 1197, 1239 ako je šifriranje izvršeno u RSA kriptosustavu s javnim ključem $(1241, 709)$. Ako je neki od tako dobivenih brojeva prost, dokažite to, a zatim odredite ostatak pri dijeljenju broja 777^{2018} tim prostim brojem.*

Upute za rješavanje zadataka

Zadatak 1.3. Slično kao u Zadatku 1.2. pokažite da je $53^{103} \equiv 14 \pmod{39}$ i $103^{53} \equiv 25 \pmod{39}$.

Zadatak 1.6. Uočite da je $1 + 3^a + 9^a = 1 + 3 \cdot (3^3)^n + 3^2(3^3)^{2n}$.

Zadatak 1.8. Danu jednadžbu promotrite modulo 4.

Zadatak 2.2. Rješenje kongruencije je $x \equiv 7, 16, 25, 34 \pmod{36}$.

Zadatak 2.4. Rješenje danog sustava kongruencija je $x \equiv 23 \pmod{30}$.

Zadatak 3.3. Primjenom Teorema 3.1. slijedi da je $n = 2^a 3^b 5^c 7^d 13^e$ i pokaže se da je $a \leq 3, b \leq 2, c \leq 1, d \leq 1, e \leq 1$. Konačno je rješenje $n \in \{13, 21, 26, 28, 36, 42\}$.

Zadatak 3.9. Iz $ab \equiv 1 \pmod{\varphi(n)}$ slijedi $ab = t(p-1)(q-1) + 1, t \in \mathbb{N}$. Promotrite slučajeve $(x, n) = 1, (x, n) \neq 1$.

Zadatak 3.11. Rješenje kongruencije je $x \equiv 53 \pmod{77}$.

Zadatak 4.3. Kako je $(z, p) = 1$ i $\varphi(p) = p - 1 = 2q$, slijedi $(-z^2)^{2q} \equiv 1 \pmod{p}$. Stoga je $d \in \{1, 2, q, 2q\}$. Sada zaključite kako pretpostavke $d = 1, 2, q$ vode do odgovarajuće kontradikcije pa je rješenje $d = 2q$.

Zadatak 4.5. Rješenja su $x \equiv 2, 3, 14 \pmod{19}$.

Zadatak 5.2. Primjenom Wilsonova teorema slijedi $2(p-3)! \equiv -1 \pmod{p}$, a primjenom Malog Fermatovog teorema $2^p \equiv 2 \pmod{p}$. Kombiniranjem tih dva izraza dobiva se da je traženi ostatak $p - 2$.

Zadatak 5.4. Rješenje kongruencije je $x \equiv 1, 9 \pmod{11}$.

Zadatak 6.2. Funkcija dešifriranja je $d_K(y) = y - 10 \pmod{26}$, a dobivena poruka je *MNOGO POKUŠAJA*.

Zadatak 6.4. Dobiva se: $d = 243751$, $p = 541$, $q = 569$, $\varphi(n) = 306720$. Šifrat je 189790 1 196709 1 304458 1 227034. Dešifrirana poruka je 2 18 15 10, odnosno *BROJ*.

Zadatak 7.1. (a) Ostatak je 9. (b) Posljednje su tri znamenke 3, 7, 6.

Zadatak 7.2. Razvijte k -znamenasti broj n po potencijama broja 10 i iskoristite svojstva kongruencija.

Zadatak 7.3. Iskoristite svojstva kongruencija. Rješenje je $x \equiv 14 \pmod{23}$, $y \equiv 17 \pmod{23}$.

Zadatak 7.4. (a) $x \equiv 4, 20, 36, 52 \pmod{64}$; (b) $x \equiv 41, 132, 223, 314, 405 \pmod{455}$.

Zadatak 7.5. (a) sustav nema rješenja; (b) $x \equiv 69 \pmod{72}$; (c) $x \equiv 23 \pmod{30}$; (d) $x \equiv 53 \pmod{2520}$.

Zadatak 7.7. Odgovor je $n = 17 + 90k, k \in \mathbb{Z}$.

Zadatak 7.6. Rješenje je $x = 110$.

Zadatak 7.8. Sustav kongruencija $x \equiv 6 \pmod{15}$, $x \equiv 1 \pmod{40}$, $x \equiv 31 \pmod{50}$ ima rješenje $x \equiv 81 \pmod{600}$. Dakle, škola ima 681 učenika.

Zadatak 7.9. Bitku je preživjelo 1023 vojnika.

Zadatak 7.10. Rješenje je $x \in \{145, 565, 985\}$.

Zadatak 7.11. Iz $n = 2^a 3^b 5^c 17^d$ slijedi $a \leq 5, b \leq 1, c \leq 1, d \leq 1$ i dobiva se $n \in \{17, 32, 34, 40, 48, 60\}$.

Zadatak 7.12. Pretpostavka $a^2 \mid n$, za neki prirodni broj $a \neq 1$, uz definiciju $\varphi(n)$ vodi do zaključka da $a \mid n, n - 1$, što nije moguće.

Zadatak 7.13. Iz $n = 2^a 3^b \cdot m$, gdje su $a, b, m \in \mathbb{N}$ i $(m, 6) = 1$. slijedi tvrdnja zadatka.

Zadatak 7.14. Pretpostavite $n = 2^k \cdot m$, gdje je $(2, m) = 1$.

Zadatak 7.15. Upotrijebite definiciju funkcije φ na kanonski rastav broja n na proste faktore.

Zadatak 7.16. Promatrajte slučajeve $(a, 47) \in \{1, 47\}$. Kada je moguće, primijenite Mali Fermatov teorem. Mogući su ostatci 42, 45.

Zadatak 7.17. Iskoristite Mali Fermatov teorem i svojstva kongruencija kako biste dobili $a \equiv 1 \pmod{p}$.

Zadatak 7.18. Rješenje je $x \equiv 27 \pmod{62}$.

Zadatak 7.19. Za određivanje broja n iskoristi se Kineski teorem o ostatcima. Dobiva se $n = 238$. Kako bi se odredio traženi ostatak primijeni se Eulerov teorem. Ostatak je 1.

Zadatak 7.20. Tvrdnja slijedi primjenom svojstava kongruencija i Eulerova teorema.

Zadatak 7.21. Zaključite da je $m > d$ i primijenite definiciju reda i teorem o dijeljenju s ostatkom.

Zadatak 7.22. Red je $d = 6$.

Zadatak 7.23. Red je $d = 8$.

Zadatak 7.24. Iskoristite svojstva reda i pokažite da je $p = 4k + 1, k \in \mathbb{N}$.

Zadatak 7.25. Koristite odgovarajuće faktorizacije i definiciju reda modulo p .

Zadatak 7.26. (a) $x \equiv 4, 39 \pmod{43}$; (b) $x \equiv 5, 8, 13, 30, 35, 38 \pmod{43}$.

Zadatak 7.27. Tvrdnja slijedi primjenom Wilsonova i Malog Fermatovog teorema.

Zadatak 7.29. Iskoristite Mali Fermatov teorem i Lagrangeov teorem. Rješenja su $x \equiv 0, 1 \pmod{71}$.

Zadatak 7.28. Pretpostavite suprotno, tj. neka je n složen broj.

Zadatak 7.29. Iskoristite Mali Fermatov teorem i Lagrangeov teorem. Rješenja su $x \equiv 0, 1 \pmod{71}$.

Zadatak 7.30. Rješenje je $x \equiv 115, 170 \pmod{209}$.

Zadatak 7.31. Slovima pridružite numerički ekvivalent i upotrijebite funkciju šifriranja $e_K(x) = x + 15 \pmod{26}$.

Zadatak 7.32. Dobivaju se sljedeći parametri: $d = 35, p = 5, q = 13, \varphi(n) = 48$. Dešifrirana je poruka 4 6 7 49.

Zadatak 7.33. Rješenje je $e = 253$.

Zadatak 7.34. Najprije se dobije $a = 128$. Rješenje sustava kongruencija je $x \equiv 65 \pmod{99}$.

Zadatak 7.35. Dešifriranjem slijedi $n_1 = 1009, n_2 = 495$. Pokaže se da je n_1 prost i $777^{2018} \pmod{n_1} = 347$.

Kvadratni ostatci

1. Legendreov simbol

Kvadratni ostatak vrlo je važan pojam u teoriji brojeva. Primjenjuje se u različitim područjima, od kriptografije do primjerice faktorizacije velikih prirodnih brojeva. Prve slutnje i rezultate koje ćemo navesti u ovom odjeljku prezentirali su Fermat, Euler, Lagrange, Legendre i ostali matematičari 17. i 18. stoljeća.

Definicija 1.1. *Neka je $n \in \mathbb{N}, a \in \mathbb{Z}, (a, n) = 1$. Ako kongruencija*

$$x^2 \equiv a \pmod{n}$$

ima rješenja, kažemo da je a kvadratni ostatak modulo n . U suprotnom, a je kvadratni neostatak modulo n .

Primjer 1.1. *Primjerice, iz $1^2 \equiv 1 \pmod{5}$ možemo zaključiti da je 1 kvadratni ostatak modulo 5 (uočite da je 1 kvadratni ostatak modulo bilo koji n). Kako je dodatno $2^2 \equiv 4 \pmod{5}, 3^2 \equiv 4 \pmod{5}, 4^2 \equiv 1 \pmod{5}$, zaključujemo da su 1 i 4 jedini mogući kvadratni ostatci modulo 5. Stoga su 2, 3 kvadratni neostatci modulo 5.*

Teorem 1.1. ([3]) *Ako je p neparni prosti broj, onda reducirani sustav ostataka modulo p sadrži $(p-1)/2$ kvadratnih ostataka i $(p-1)/2$ kvadratnih neostataka modulo p .*

Primjer 1.2. *Ako želimo odrediti sve kvadratne ostatke modulo 7, prema prethodnom teoremu trebamo naći tri kvadratna ostatka modulo 7. Kako je $1^2 \equiv 1 \pmod{7}, 2^2 \equiv 4 \pmod{7}, 3^2 \equiv 2 \pmod{7}$, zaključujemo da su 1, 2, 4 kvadratni ostatci modulo 7, dok su 3, 5, 6 kvadratni neostatci modulo 7.*

Definicija 1.2. Neka je p neparni prosti broj i $a \in \mathbb{Z}$. Legendreov simbol $\left(\frac{a}{p}\right)$ definira se na sljedeći način:

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

Primjer 1.3. Na osnovi Primjera 1.2. zaključujemo da vrijedi

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Uočimo da je

$$\left(\frac{7k}{7}\right) = 0, \quad k \in \mathbb{Z}.$$

Zadatak 1.1. Neka je p neparni prosti broj i $a \in \mathbb{Z}$. Dokažite da kongruencija

$$x^2 \equiv a \pmod{p}$$

ima $1 + \left(\frac{a}{p}\right)$ rješenja modulo p .

Rješenje. Neka je p neparni prosti broj i $a \in \mathbb{Z}$.

- Ako $p \mid a$, onda je dana kongruencija oblika $x^2 \equiv 0 \pmod{p}$ i jedino rješenje modulo p te kongruencije je $x \equiv 0 \pmod{p}$. S druge je strane $\left(\frac{a}{p}\right) = 0$ pa je $1 + \left(\frac{a}{p}\right) = 1$, a to je u skladu s tvrdnjom.
- Ako $(a, p) = 1$ i postoji $b \in \mathbb{Z}$ takav da je

$$b^2 \equiv a \pmod{p},$$

onda su $x \equiv \pm b \pmod{p}$, prema Lagrangeovom teoremu, sva rješenja modulo p te kongruencije i međusobno su nekongruentna jer je $p \neq 2$. U tom je slučaju a kvadratni ostatak modulo p pa je $\left(\frac{a}{p}\right) = 1$, odnosno $1 + \left(\frac{a}{p}\right) = 2$, što je u skladu s tvrdnjom.

- Ako $(a, p) = 1$ i dana kongruencija nema rješenja, onda je a kvadratni neostatak modulo p pa je $\left(\frac{a}{p}\right) = -1$. Stoga je $1 + \left(\frac{a}{p}\right) = 0$, što je u skladu s tvrdnjom.

◇

Zadatak 1.2. *Ako je p neparni prosti broj, odredite*

$$A_p = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right).$$

Rješenje. Uočimo da je $a \in \{1, 2, \dots, p-1\}$, a ovaj je skup reducirani sustav ostataka modulo p . Kako se prema Teoremu 1.1. reducirani sustav ostataka modulo p sastoji od $(p-1)/2$ kvadratnih ostataka i $(p-1)/2$ kvadratnih neostataka modulo p , zaključujemo da je polovina članova dane sume jednaka 1, dok je druga polovina jednaka -1 . Stoga je $A_p = 0$. \diamond

Teorem 1.2. (Eulerov kriterij, [3]) *Ako je p neparni prosti broj i $a \in \mathbb{Z}$, onda vrijedi*

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

Primjer 1.4. *Kako je 31 prosti broj i $(3, 31) = 1$, primjenom Eulerova kriterija dobivamo*

$$\left(\frac{3}{31}\right) \equiv 3^{15} \equiv -1 \pmod{31}.$$

Stoga je $(\frac{3}{31}) = -1$, odnosno 3 je kvadratni neostatak modulo 31.

Zadatak 1.3. *Neka je $n \in \mathbb{N}$ takav da je $p = 2n + 1$ prosti broj i vrijedi $2^n \equiv 1 \pmod{p}$. Je li 2 kvadratni ostatak ili kvadratni neostatak modulo p ?*

Rješenje. Ako je p prosti broj takav da je $p = 2n + 1$, onda prema Eulerovu kriteriju slijedi

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

Iz uvjeta zadatka zaključujemo $(\frac{2}{p}) = 1$ pa je 2 kvadratni ostatak modulo p . \diamond

Teorem 1.3. ([3]) *Neka je p neparni prosti broj i $a, b \in \mathbb{Z}$. Tada vrijedi:*

$$(1) \quad a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

$$(2) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right),$$

$$(3) \quad (a, p) = 1 \implies \left(\frac{a^2}{p}\right) = 1,$$

$$(4) \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

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

Primjer 1.5. *Kako su prema Primjeru 1.1. brojevi 1, 4 kvadratni ostatci, a brojevi 2, 3 kvadratni neostatci modulo 5, prema prethodnom teoremu slijedi*

$$\left(\frac{a}{5}\right) = \begin{cases} 1, & a \equiv 1, 4 \pmod{5}, \\ 0, & a \equiv 0 \pmod{5}, \\ -1, & a \equiv 2, 3 \pmod{5}. \end{cases}$$

Primjer 1.6. *Korištenjem svojstava (2) – (5) iz Teorema 1.3. dobivamo*

$$\left(\frac{-14}{53}\right) = \left(\frac{-1}{53}\right) \left(\frac{2}{53}\right) \left(\frac{7}{53}\right) = (-1)^{\frac{53-1}{2}} (-1)^{\frac{53^2-1}{8}} \left(\frac{7}{53}\right).$$

Primjenom Eulerova kriterija dobiva se $\left(\frac{7}{53}\right) \equiv 7^{26} \equiv 1 \pmod{53}$ pa je $\left(\frac{-14}{53}\right) = -1$.

Zadatak 1.4. *Dokažite da diofantska jednadžba*

$$x^2 + 11k + 12 = 0$$

nema rješenja.

Rješenje. Ako bi dana jednadžba imala cjelobrojnih rješenja, onda bi i kongruencija $x^2 + 11k + 12 \equiv 0 \pmod{11}$, tj. kongruencija $x^2 \equiv -1 \pmod{11}$ imala rješenja pa bi vrijedilo $\left(\frac{-1}{11}\right) = 1$. Međutim, Eulerov kriterij daje $\left(\frac{-1}{11}\right) \equiv 3^5 \equiv -1 \pmod{11}$ i dobivamo kontradikciju. Prema tome, dana diofantska jednadžba nema rješenja. \diamond

Zadatak 1.5. *Neka je $n \in \mathbb{N}, n \geq 4$. Dokažite da broj $A_n = 1! + 2! + \dots + n!$ nije potpun kvadrat.*

Rješenje. Uočimo da je $A_n = 1! + 2! + 3! + 4! + 5! + \dots + n! \equiv 33 \equiv 3 \pmod{5}$. Na osnovi Primjera 1.5. zaključujemo da je A_n kvadratni neostatak modulo 5 pa ne može biti potpun kvadrat. \diamond

Zadatak 1.6. *Neka je $n \in \mathbb{N}$. Dokažite: $31 \nmid 4n^2 + 8$.*

Zadatak 1.7. *Ako je p neparni prosti broj i $a, b \in \mathbb{Z}, (a, p) = (b, p) = 1$, dokažite da je barem jedan od brojeva a, b, ab kvadratni ostatak modulo p .*

2. Gaussov kvadratni zakon reciprociteta

Gaussov kvadratni zakon reciprociteta omogućava lako izračunavanje Legendrovog simbola. Gauss ga je zvao svojim zlatnim teoremom i osmislio je ukupno osam dokaza. Danas ih postoji preko 300.

Teorem 2.1. (Gaussov kvadratni zakon reciprociteta, [3]) *Neka su p i q različiti neparni prosti brojevi. Tada vrijedi*

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

Lako se vidi da se formula iz prethodnog teorema može zapisati i na ovaj način:

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

Ta formula vrijedi i ako p, q nisu različiti prosti brojevi i koristi se za određivanje vrijednosti Legendreova simbola.

Primjer 2.1. *Uočimo da nam Gaussov kvadratni zakon reciprociteta omogućava da primjerice izračunamo $\left(\frac{7}{31}\right)$ bez primjene Eulerova kriterija. Kako su 7, 31 prosti brojevi, vrijedi*

$$\left(\frac{7}{31}\right) = (-1)^{3 \cdot 15} \left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = -(-1)^{1 \cdot 3} \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Zadatak 2.1. *Ispitajte ima li kongruencija $x^2 \equiv 19 \pmod{283}$ rješenja.*

Zadatak 2.2. *Odredite sve neparne proste brojeve p za koje je 3 kvadratni ostatak modulo p .*

Rješenje. Tražimo neparne proste brojeve p za koje je $\left(\frac{3}{p}\right) = 1$. Uočimo da je p prosti broj veći od 3. Prema Gaussovom kvadratnom zakonu reciprociteta vrijedi

$$1 = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2} \frac{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right). \quad (2.1)$$

Uočimo da vrijedi:

$$\begin{aligned} (-1)^{\frac{p-1}{2}} &= \begin{cases} 1, & p \equiv 1 \pmod{4}, \\ -1, & p \equiv 3 \pmod{4}, \end{cases} \\ \left(\frac{p}{3}\right) &= \begin{cases} 1, & p \equiv 1 \pmod{3}, \\ -1, & p \equiv 2 \pmod{3}. \end{cases} \end{aligned}$$

Odavde i iz (2.1) slijedi da je $\left(\frac{3}{p}\right) = 1$ zadovoljeno ako je p rješenje jednog od sljedećih sustava kongruencija:

- $p \equiv 1 \pmod{3}$, $p \equiv 1 \pmod{4}$,
- $p \equiv 2 \pmod{3}$, $p \equiv 3 \pmod{4}$.

Primjenom Kineskog teorema o ostatcima dobivamo $p \equiv 1, 11 \pmod{12}$ i p prosti broj. \diamond

Zadatak 2.3. *Neka je $p = 4m + 3$, $m \in \mathbb{N}$ prosti broj i $a \in \mathbb{Z}$, $(a, p) = 1$. Odredite rješenje kongruencije $x^2 \equiv a \pmod{p}$.*

Rješenje. Ako rješenje postoji, onda je $\left(\frac{a}{p}\right) = 1$. Iz Eulerova kriterija slijedi

$$1 \equiv a^{\frac{p-1}{2}} \equiv a^{2m+1} \pmod{p}.$$

Pomnožimo li lijevu i desnu stranu te kongruencije sa a dobivamo

$$a^{2m+2} \equiv a \pmod{p}.$$

Stoga vrijedi

$$(a^{m+1})^2 \equiv a \pmod{p},$$

pa su $x \equiv \pm a^{m+1} \pmod{p}$, prema Lagrangeovom teoremu, sva rješenja dane kongruencije. \diamond

Zadatak 2.4. *Neka je p prosti broj takav da je $q = 4p + 1$ također prosti broj.*

- (a) *Dokažite da je $2^{2p} \equiv -1 \pmod{q}$.*
- (b) *Odredite $\left(\frac{p}{q}\right)$.*

Rješenje. Uočimo da su p i q neparni prosti brojevi.

- (a) Primjenom Eulerova kriterija dobivamo

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

Kako je

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = (-1)^{p(2p+1)} = -1,$$

slijedi tražena tvrdnja.

(b) Primjenom Gaussova kvadratnog zakona reciprociteta i svojstava Legendreova simbola dobivamo

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot 2p} \left(\frac{q}{p}\right) = \left(\frac{4p+1}{p}\right) = \left(\frac{1}{p}\right) = 1.$$

◇

Zadatak 2.5. *Dokažite: Fermatov broj $F_n = 2^{2^n} + 1, n \in \mathbb{N}$ prost je ako i samo ako je*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}. \quad (2.2)$$

Rješenje. Pretpostavimo da je F_n prosti broj. Kako je $F_n \geq 5$, to je F_n neparni prosti broj i $(F_n, 3) = 1$. Zbog Eulerova kriterija slijedi da trebamo dokazati $\left(\frac{3}{F_n}\right) = -1$. Gaussov kvadratni zakon reciprociteta i činjenica da je $\frac{F_n-1}{2}$ parni broj povlači

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

Kako je $F_n \equiv 2 \pmod{3}$ slijedi $\left(\frac{3}{F_n}\right) = -1$ i time je tvrdnja dokazana.

Obratno, pretpostavimo da vrijedi (2.2). Tada je

$$3^{F_n-1} \equiv 1 \pmod{F_n}. \quad (2.3)$$

Neka je p prosti broj i $p \mid F_n$. Zbog (2.2) i (2.3) je

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{p}, \quad (2.4)$$

$$3^{F_n-1} \equiv 1 \pmod{p}. \quad (2.5)$$

Neka je d red od 3 modulo p . Zbog (2.5), prema Teoremu 4.1., slijedi da $d \mid F_n - 1 = 2^{2^n}$. Uočimo da ne može biti $d = 2^k, k < 2^n$, tj.

$$3^{2^k} \equiv 1 \pmod{p}$$

jer bi to bilo u kontradikciji s (2.4) (uzastopnim kvadriranjem lijeve i desne strane te kongruencije ne možemo dobiti -1). Stoga je $d = F_n - 1$. Kako $d \mid p - 1$, slijedi da $F_n - 1 \mid p - 1$, što je, zbog $p \leq F_n$, moguće samo ako je $F_n - 1 = p - 1$, tj. $F_n = p$. Time je tvrdnja dokazana. ◇

Zadatak 2.6. *Prosti brojevi p i q nazivaju se brojevi blizanci ako je $q = p + 2$. Dokažite da postoji $a \in \mathbb{Z}$ takav da $p \mid a^2 - q$ ako i samo postoji $b \in \mathbb{Z}$ takav da $q \mid b^2 - p$.*

Zadatak 2.7. *Dokažite da prostih brojeva oblika $6m + 1, m \in \mathbb{N}$ ima beskonačno mnogo.*

Rješenje. Pretpostavimo da postoji konačno mnogo prostih brojeva oblika $6m + 1, m \in \mathbb{N}$. Neka su to brojevi p_1, p_2, \dots, p_n . Promatrajmo broj

$$M = (2p_1p_2 \cdots p_n)^2 + 3.$$

Ako je p prosti djeljitelj od M uočimo da on ne može biti jednak ni 2 ($M \equiv 1 \pmod{2}$) ni 3 ($M \equiv 1 \pmod{3}$) ni p_i ($M \equiv 3 \pmod{p_i}, p_i \geq 7$) pa p mora biti oblika $6k + 5, k \in \mathbb{N}_0$. Iz $M \equiv 0 \pmod{p}$ slijedi

$$(2p_1p_2 \cdots p_n)^2 \equiv -3 \pmod{p},$$

pa je -3 kvadratni ostatak modulo p . Primjenom Gaussova kvadratnog zakona reciprociteta i svojstava Legendreova simbola dobivamo

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

Kako je $p = 6k + 5$, slijedi

$$\left(\frac{-3}{p}\right) = \left(\frac{6k+5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

tj. -3 je kvadratni neostatak modulo p . Time smo došli do kontradikcije pa ne može postojati konačno mnogo prostih brojeva oblika $6m + 1$. \diamond

Zadatak 2.8. *Neka je $p > 3$ prosti broj. Dokažite da kongruencija $x^2 + 3 \equiv 0 \pmod{p}$ ima rješenja ako i samo ako postoji $m \in \mathbb{N}$ takav da je $p = 6m + 1$.*

3. Jacobijev simbol

Jacobijev simbol poopćenje je Legendreova simbola. Uveo ga je Carl Gustav Jacobi 1846. godine. Njegova je glavna primjena u računalnoj teoriji brojeva, posebno u testiranju prostosti i metodama faktorizacije prirodnih brojeva - oni su, pak važni, u kriptografiji.

Definicija 3.1. *Neka je P neparni prirodni broj, $P = p_1p_2 \cdots p_n$, gdje su $p_i, i = 1, \dots, n$ (neparni) prosti brojevi (ne nužno različiti) i a cijeli broj. Jacobijev simbol $\left(\frac{a}{P}\right)$ definira se kao*

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_n}\right),$$

gdje je $\left(\frac{a}{p_i}\right), i = 1, \dots, n$ Legendreov simbol.

Ako je P prost broj, onda je očito da se Legendreov i Jacobijev simbol podudaraju.

Primjer 3.1. *Uočimo da vrijedi*

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

Napomena 3.1. *Lako se može pokazati da vrijede sljedeća svojstva:*

- (1) *Ako je $(a, P) > 1$, onda je $\left(\frac{a}{P}\right) = 0$; inače je $\left(\frac{a}{P}\right) \in \{-1, 1\}$.*
- (2) *Ako je $\left(\frac{a}{P}\right) = -1$, onda je a kvadratni neostatak modulo P . U tom slučaju za barem jedan p_i vrijedi $\left(\frac{a}{p_i}\right) = -1$. Kada bi kongruencija $x^2 \equiv a \pmod{P}$ imala rješenja, onda bi i kongruencija $x^2 \equiv a \pmod{p_i}$ morala imati rješenja, što je kontradikcija.*
- (3) *Iz $\left(\frac{a}{P}\right) = 1$ ne slijedi da je a kvadratni ostatak modulo P . Npr., u Primjeru 3.1. pokazali smo da je $\left(\frac{2}{15}\right) = 1$, ali provjerom se lako može utvrditi da kongruencija $x^2 \equiv 2 \pmod{15}$ nema rješenja.*

Primjer 3.2. *Kako je*

$$\left(\frac{15}{143}\right) = \left(\frac{15}{11}\right) \left(\frac{15}{13}\right) = \left(\frac{4}{11}\right) \left(\frac{2}{13}\right) = \left(\frac{2}{11}\right)^2 (-1)^{\frac{13^2-1}{8}} = -1,$$

kongruencija $x^2 \equiv 15 \pmod{143}$, prema svojstvu (2) iz prethodne napomene, nema rješenja.

U idućem teoremu dana su svojstva Jacobijeva simbola.

Teorem 3.1. ([3]) *Neka su $P, Q \in \mathbb{N}$ neparan, $a, b \in \mathbb{Z}$. Tada vrijedi:*

- (1) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \left(\frac{a}{Q}\right)$,
- (2) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right)$,
- (3) $(a, P) = 1 \implies \left(\frac{a^2}{P}\right) = \left(\frac{a}{P}\right)^2 = 1$,
- (4) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$, $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$,
- (5) $\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2} \frac{Q-1}{2}} \left(\frac{Q}{P}\right)$.

Primjer 3.3. Analogon formule iz Eulerova kriterija ne vrijedi u slučaju Jacobijeva simbola. Lako se izračuna da je npr.

$$\left(\frac{2}{221}\right) = -1, \quad \text{ali} \quad 2^{110} \equiv 30 \pmod{221}.$$

Ako za dani neparan $n \in \mathbb{N}$ nađemo $a \in \{2, \dots, n-1\}$ sa svojstvom

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n},$$

na taj način možemo dokazati da je n složen broj (na ovakvoj se provjeri temelji tzv. Solovay-Strassenov test prostosti (vidi npr. [7])).

Zadatak 3.1. Izračunajte Jacobijeve simbole $\left(\frac{51}{213}\right)$, $\left(\frac{51}{355}\right)$.

Rješenje. Vrijedi:

$$\begin{aligned} \left(\frac{51}{213}\right) &= \left(\frac{51}{3}\right) \left(\frac{51}{71}\right) = 0, \\ \left(\frac{51}{355}\right) &= \left(\frac{51}{5}\right) \left(\frac{51}{71}\right) = \left(\frac{1}{5}\right) (-1)^{\frac{51-1}{2} \frac{71-1}{2}} \left(\frac{71}{51}\right) \\ &= -\left(\frac{71}{51}\right) = -\left(\frac{20}{51}\right) = \left(\frac{2}{51}\right)^2 \left(\frac{5}{51}\right) \\ &= -(-1)^{\frac{5-1}{2} \frac{51-1}{2}} \left(\frac{51}{5}\right) = -\left(\frac{1}{5}\right) = -1. \end{aligned}$$

◇

Zadatak 3.2. Izračunajte Jacobijeve simbole $\left(\frac{-200}{221}\right)$, $\left(\frac{631}{1099}\right)$.

4. Zadatci za vježbu

Zadatak 4.1. Odredite sve kvadratne ostatke modulo 11.

Zadatak 4.2. Izračunajte Legendreove simbole $\left(\frac{150}{197}\right)$, $\left(\frac{-241}{389}\right)$, $\left(\frac{8201}{8191}\right)$, $\left(\frac{122}{211}\right)$.

Zadatak 4.3. Dokažite da je $\left(\frac{9}{10^{100}-1}\right) = 0$.

Zadatak 4.4. Ispitajte postoji li rješenje sljedećih diofantskih jednadžbi:

(a) $x^2 + 1 = 7y$,

(b) $3x^2 - 4y^2 = 13$.

Zadatak 4.5. Neka je p neparni prosti broj i $a \in \mathbb{Z}$ takav da vrijedi $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Može li diofantska jednačina $x^2 + py - a = 0$ imati rješenja?

Zadatak 4.6. Neka je $p \equiv 3 \pmod{4}$ prosti broj takav da je $q = 2p + 1$ također prosti broj. Dokažite da je $2^p \equiv 1 \pmod{q}$.

Zadatak 4.7. Neka su $q \equiv 1 \pmod{4}$ i $p = 2q + 1$ prosti brojevi. Odredite red od 2 modulo p .

Zadatak 4.8. Neka je p prosti broj oblika $p = 2^k + 1, k \geq 3$. Označimo s d red od 2 modulo p . Dokažite da je $d \leq \frac{p-1}{2}$.

Zadatak 4.9. Postoji li $a \in \mathbb{Z}$ takav da vrijedi:

(a) $a^2 + 24$ djeljivo je s 1361,

(b) $2a^2 + 6$ djeljivo je s 1987?

Zadatak 4.10. Neka je $p \equiv 1 \pmod{4}$ prosti broj. Dokažite da je r kvadratni ostatak modulo p ako i samo ako je $p - r$ kvadratni ostatak modulo p .

Zadatak 4.11. Za sve $b \in \mathbb{Z}$ takve da $31 \mid b^{15} + 1$ ispitajte je li $2b$ kvadratni ostatak ili kvadratni neostatak modulo 31.

Zadatak 4.12. Odredite sve proste brojeve $p > 2$ za koje je broj -2 kvadratni ostatak modulo p .

Zadatak 4.13. Koji su mogući oblici prostih faktora brojeva oblika $16n^2 - 2, n \in \mathbb{N}$?

Zadatak 4.14. Neka je $n \geq 2$ prirodni broj i $p = 4^n + 1$ prosti broj. Ispitajte jesu li 2, 3 i 4 kvadratni ostatci ili neostatci modulo p .

Zadatak 4.15. Odredite sve neparne proste brojeve p oblika $4k + 3$ sa svojom da je 7 kvadratni ostatak modulo p .

Zadatak 4.16. Neka je p prosti broj oblika $p = q^2 + b^2, b \in \mathbb{Z}$ i q neparni prosti broj. Dokažite da je q kvadratni ostatak modulo p .

Zadatak 4.17. Neka je p prosti broj oblika $6k+5$, $k \in \mathbb{N}$. Postoje li rješenja (x, y) diofantske jednadžbe $2x^2 + 2x + 2 = yp$?

Zadatak 4.18. Neka je p prosti broj takav da postoji prirodni broj k sa svojstvom $p = 4k + 3$ i 3 je kvadratni ostatak modulo p . Dokažite ili opovrgnite: $k \equiv 2 \pmod{3}$.

Zadatak 4.19. Dokažite da prirodni broj oblika $4n^2 + 3$, $n \in \mathbb{Z}$ ne može imati prostih faktora oblika $3k + 2$, $k \in \mathbb{N}$.

Zadatak 4.20. Dokažite da za svaki prosti prirodni broj $p = 6k + 1$, $k \in \mathbb{N}$ postoje cijeli brojevi a, b takvi da je $a^2 + 3 = bp$.

Zadatak 4.21. Neka je $p > 3$ prosti broj sa svojstvom da postoji prirodni broj n takav da vrijedi $p \mid n^2 + 27$. Odredite ostatak pri dijeljenju broja p s brojem 6.

Zadatak 4.22. Neka je a neparni prosti broj, b prirodni broj i $p = a^2 + 5b^2$ prosti broj. Ako je a kvadratni ostatak modulo p , dokažite da je $p \equiv 1 \pmod{5}$.

Zadatak 4.23. Izračunajte simbole $\left(\frac{-459}{725}\right)$, $\left(\frac{152}{135}\right)$, $\left(\frac{1281}{1357}\right)$, $\left(\frac{102}{547}\right)$, $\left(\frac{-2016}{173}\right)$, $\left(\frac{-1805}{1921}\right)$, $\left(\frac{-2054}{2101}\right)$. Ima li među tim simbolima Legendreovih simbola?

Zadatak 4.24. Izračunajte Jacobijsve simbole $\left(\frac{159}{7927}\right)$, $\left(\frac{666}{777}\right)$, $\left(\frac{39}{143}\right)$.

Zadatak 4.25.

(a) Je li -2 kvadratni neostatak modulo 28405?

(b) Je li 1281 kvadratni ostatak modulo 1357?

Zadatak 4.26. Izračunajte Jacobijsve simbole $x = \left(\frac{527}{957}\right)$ i $y = \left(\frac{493}{805}\right)$, a zatim ispitajte postoji li za proizvoljan $k \in \mathbb{Z}$ cjelobrojno rješenje diofantske jednadžbe $7xu^2 + 3yv^2 = 10k - 2$ sa svojstvom $5 \nmid u$ i $5 \nmid v$.

Zadatak 4.27. Neka su $m, n \in \mathbb{N}$ sa svojstvom da je $(m, n) = 1$, $m = 4k - 1$, $n = 8k + 7$, $k \in \mathbb{Z}$ i $3 \nmid m$. Izračunajte simbol $\left(\frac{m}{n}\right)$.

Zadatak 4.28. Odredite sve $n \in \mathbb{N}$ sa svojstvom da je $3n \equiv 31 \pmod{52}$ i $\left(\frac{20}{n}\right) = 1$.

Zadatak 4.29. Neka je $n \in \mathbb{N}$, $n \equiv 5 \pmod{8}$. Izračunajte Jacobijsve simbol $\left(\frac{n^3}{n-2}\right)$.

Zadatak 4.30. U ovisnosti o neparnom $n \in \mathbb{N}$ izračunajte vrijednost Jacobijsve simbola $\left(\frac{n^5}{n+2}\right)$.

Upute za rješavanje zadataka

Zadatak 1.6. Promotrite što bi slijedilo ako vrijedi $31 \mid 4n^2 + 8$, za sve $n \in \mathbb{N}$.

Zadatak 1.7. Jasno je da je $(ab, p) = 1$ pa iz $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ zaključite kako sva tri broja ne mogu biti kvadratni neostatci modulo p .

Zadatak 2.1. Pokažite da je $\left(\frac{19}{283}\right) = -1$.

Zadatak 2.6. Primijenite definiciju kvadratnog ostatka i Gaussov kvadratni zakon reciprociteta.

Zadatak 2.8. Promotrite Zadatak 2.7. Dokažite da je $\left(\frac{-3}{p}\right) = 1$ ako i samo ako postoji $m \in \mathbb{N}$ takav da je $p = 6m + 1$. Iskoristite Gaussov kvadratni zakon reciprociteta i svojstva Legendreova simbola.

Zadatak 3.2. Vrijednost prvoga simbola je -1 , a drugoga je 1 .

Zadatak 4.1. Kvadratni ostatci modulo 11 su $1, 3, 4, 5, 9$.

Zadatak 4.2. Vrijednosti su Legendreovih simbola redom $1, -1, 1, 1$.

Zadatak 4.3. Zaključite da je $10^{100} - 1 \equiv 0 \pmod{3}$.

Zadatak 4.4. (a) Pretpostavka da zadana diofantska jednadžba ima rješenje vodi do zaključka da je -1 kvadratni ostatak modulo 7 , a to nije točno. (b) Slično, promotrite zadanu jednadžbu modulo 3 .

Zadatak 4.5. Pretpostavite da zadana jednadžba ima rješenje (pa posebno i rješenje modulo p) te primjenom Eulerova kriterija zaključite kontradikciju.

Zadatak 4.6. Uočite da je $p = \frac{q-1}{2}$. Kako biste pokazali novodobivenu kongruenciju, iskoristite Eulerov kriterij i svojstva Legendreova simbola.

Zadatak 4.7. Iskoristite Mali Fermatov teorem da zaključite da je traženi red jednak $1, 2, q$ ili $2q$. Zaključite da red ne može biti $1, 2$ i q (kod posljednjeg slučaja koristite Eulerov kriterij i svojstva Legendreovog simbola) pa je jednak $2q$.

Zadatak 4.8. Primijenite Eulerov kriterij i pokažite da je $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, a zatim iskoristite definiciju reda modulo p .

Zadatak 4.9. (a) Ako bi vrijedio uvjet zadatka, slijedilo bi da je -24 kvadratni ostatak modulo 1361 . Pokažite da to nije točno računanjem odgovarajućeg Legendreova simbola. (b) Slično, zadatak se svodi na to da trebate pokazati da je -12 kvadratni ostatak modulo 1987 .

Zadatak 4.10. Iskoristite svojstva kvadratnog ostatka modulo p i Legendreova simbola.

Zadatak 4.11. Dobiva se $\left(\frac{2b}{31}\right) = -1$.

Zadatak 4.12. Primjenom svojstava kvadratnih ostataka modulo p i Legendreova simbola dobiva se da je $p \equiv 1, 3 \pmod{8}$.

Zadatak 4.13. Jasno je da je $p = 2$. Osim toga, iz $p \mid 16n^2 - 2$ slijedi $\left(\frac{2}{p}\right) = 1$ pa je $p \equiv 1, 7 \pmod{8}$.

Zadatak 4.14. Primjenom svojstava Legendreova simbola pokaže se da su 2 i 4 kvadratni ostaci modulo p . Korištenjem Gaussova kvadratnog zakona reciprociteta pokaže se da je 3 kvadratni neostatak modulo p .

Zadatak 4.15. Traži se p sa svojstvom $\left(\frac{p}{7}\right) = 1$. Iskoristite Gaussov kvadratni zakon reciprociteta. Traženje rješenja svodi se na rješavanje sustava linearnih kongruencija. Zaključak je: p je prosti broj i $p \equiv 5, 13, 17 \pmod{28}$.

Zadatak 4.16. Dokaz slijedi direktnom primjenom Gaussova kvadratnog zakona reciprociteta.

Zadatak 4.17. Ako se pretpostavi da rješenje zadane jednadžbe postoji, slijedi $(2x + 1)^2 \equiv -3 \pmod{p}$. Međutim, to nije moguće jer se korištenjem Gaussova kvadratnog zakona reciprociteta zaključuje da je $\left(\frac{-3}{p}\right) = -1$.

Zadatak 4.18. Primjenom Gaussova kvadratnog zakona reciprociteta pokaže se da je k kvadratni neostatak modulo 3. Dakle, $k \equiv 2 \pmod{3}$.

Zadatak 4.19. Pretpostavite suprotno i zaključite $\left(\frac{-3}{p}\right) = -1$, a zatim primjenom Gaussova kvadratnog zakona reciprociteta pokažite kako je polazna pretpostavka dovela do kontradikcije.

Zadatak 4.20. Primjenom Gaussova kvadratnog zakona reciprociteta pokaže se da je $\left(\frac{-3}{p}\right) = 1$ pa iz definicije kongruencije slijedi postojanje cijelih brojeva a, b .

Zadatak 4.21. Iz $n^2 \equiv -27 \pmod{p}$ primjenom Gaussova kvadratnog zakona reciprociteta, slijedi $p \equiv 1 \pmod{3}$. Kako je i $p \equiv 1 \pmod{2}$, konačno je rješenje $p \equiv 1 \pmod{6}$.

Zadatak 4.22. Primijenite Gaussov kvadratni zakon reciprociteta i svojstva Jacobijeva simbola.

Zadatak 4.23. Vrijednosti su simbola redom $1, 1, -1, -1, 1, 1, -1$. Legendreovi su simboli $\left(\frac{102}{547}\right)$ i $\left(\frac{-2016}{173}\right)$.

Zadatak 4.24. Vrijednosti su simbola redom $1, 0, 0$.

Zadatak 4.25. (a) Broj -2 je kvadratni neostatak modulo 28405 . (b) 1281 nije kvadratni ostatak modulo 1357 .

Zadatak 4.26. Vrijednosti su Jacobijevih simbola $x = 1, y = -1$. Zadana jednadžba nema rješenja modulo 5 ni za jedan $k \in \mathbb{Z}$.

Zadatak 4.27. Vrijednost simbola je -1 . Primijenite Gaussov kvadratni zakon reciprociteta.

Zadatak 4.28. Rješenje je linearne kongruencije $n \equiv 45 \pmod{52}$. Prirodni brojevi n koji zadovoljavaju navedeni simbol su $n \equiv 1, 4 \pmod{5}$ (iskoristite Gaussov kvadratni zakon reciprociteta). Primjenom Kineskog teorema o ostatcima dobiva se $n \equiv 149, 201 \pmod{260}$.

Zadatak 4.29. Primjenom svojstava Jacobijeva simbola i Gaussova kvadratnog zakona reciprociteta, za vrijednost simbola dobiva se -1 .

Zadatak 4.30. Pokaže se da je $\left(\frac{n^5}{n+2}\right) = (-1)^{3 \cdot \frac{n^2-1}{8}}$ pa je dani simbol jednak 1 za $n \equiv 1, 7 \pmod{8}$ i -1 za $n \equiv 3, 5 \pmod{8}$.

Diofantske jednađbe

U ovom ćemo poglavlju opisati metode za rješavanje nekih oblika diofantskih jednađbi.

1. Linearne diofantske jednađbe

Pod pojmom diofantske jednađbe najćešće se podrazumijevaju polinomialne jednađbe s cjelobrojnim koeficijentima, a rješavaju se u skupu cijelih brojeva. U ovom odjeljku promatrat ćemo probleme vezane uz najjednostavniji oblik takve jednađbe, to jest uz tzv. linearnu diofantsku jednađbu.

Definicija 1.1. *Neka je $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$. Jednađba oblika*

$$a_1x_1 + \dots + a_nx_n = b \tag{1.1}$$

naziva se linearna diofantska jednađba s n nepoznanica.

Prisjetimo se da smo se u poglavlju *Djeljivost* kod problema vezanih uz primjenu Euklidova algoritma već susreli s takvim jednađbama, ali s dvjema nepoznicama.

Teorem 1.1. ([3]) *Linearna diofantska jednađba (1.1) ima rješjenja ako i samo ako $d = (a_1, \dots, a_n) \mid b$. U tom se slučaju svako rješjenje može zapisati pomoću $n - 1$ cjelobrojnih parametara.*

Korolar 1.1. ([3]) *Neka je $(a_1, a_2) = 1$. Ako je uređeni par (x_0, y_0) jedno rješjenje jednađbe*

$$a_1x + a_2y = b,$$

onda su sva rješjenja te jednađbe dana s

$$\begin{cases} x = x_0 + a_2t \\ y = y_0 - a_1t \end{cases}, \quad t \in \mathbb{Z}.$$

Svaka linearna diofantska jednadžba s dvjema nepoznicama koja ima rješenje svodi se na oblik iz prethodnog korolara te se može riješiti na taj način. Naime, ako jednadžba $ax+by = m$ ima rješenja, onda je $d = (a, b) \mid m$ pa je dana jednadžba ekvivalentna jednadžbi

$$\frac{a}{d}x + \frac{b}{d}y = \frac{m}{d}, \quad \left(\frac{a}{d}, \frac{b}{d}\right) = 1,$$

na koju se može primijeniti prethodni korolar.

Primjer 1.1. *Odredimo sva rješenja jednadžbe $4x + 6y = 8$. Kako je $(4, 6) = 2 \mid 8$, dijeljenjem s 2 dobivamo jednadžbu $2x + 3y = 4$ za koju je $(2, 3) = 1$. Jedno konkretno, pojedinačno, tzv. partikularno rješenje jednadžbe $2x + 3y = 4$ možemo dobiti tako da najprije odredimo parametre u i v u Bézoutovom identitetu $2u + 3v = 1$ (može se koristiti prošireni Euklidov algoritam ili redom uvrštavati cjelobrojne vrijednosti za u i v dok jednadžba ne bude istinita). Lako se vidi da je, primjerice, $(u, v) = (-1, 1)$ rješenje navedenog Bézoutovog identiteta, a onda je $(x_0, y_0) = (4u, 4v) = (-4, 4)$ partikularno rješenje polazne jednadžbe. Sva su rješenja, prema Korolaru 1.1., dana s*

$$\begin{cases} x = -4 + 3t \\ y = 4 - 2t \end{cases}, \quad t \in \mathbb{Z}.$$

Zadatak 1.1. *Riješite jednadžbe:*

(i) $12x - 13y = 15$,

(ii) $6x + 10y - 15z = 1$.

Rješenje.

- (i) Kako je $(12, -13) = 1 \mid 15$, dana jednadžba ima rješenja. Lako se vidi da je jedno rješenje jednadžbe $12u - 13v = 1$ dano s $(u, v) = (-1, -1)$ pa je $(x_0, y_0) = (-15, -15)$ i sva su rješenja polazne jednadžbe

$$\begin{cases} x = -15 - 13t \\ y = -15 - 12t \end{cases}, \quad t \in \mathbb{Z}.$$

- (ii) Promotrimo jednadžbu $6x + 10y - 15z = 1$. Kako je $(6, 10, -15) = 1$, prema Teoremu 1.1. slijedi da jednadžba ima rješenja i rješenje se može izraziti pomoću dvaju cjelobrojnih parametara. Promotrimo sljedeću jednadžbu:

$$6x + 10y = 1 + 15z.$$

Ona mora imati rješenja pa $(6, 10) = 2$ povlači $2 \mid 1 + 15z$, odnosno postoji $t \in \mathbb{Z}$ takav da je $1 + 15z = 2t$. Stoga postoji rješenje jednadžbe $2t - 15z = 1$. Rješenja te linearne diofantske jednadžbe s dvjema nepoznicama su

$$\begin{cases} t = 8 - 15s \\ z = 1 - 2s \end{cases}, \quad s \in \mathbb{Z}. \quad (1.2)$$

Uvrštavanjem posljednje jednakosti u početnu jednadžbu, dolazimo do jednadžbe

$$3x + 5y = 8 - 15s. \quad (1.3)$$

Kako je jedno rješenje jednadžbe $3u + 5v = 1$ dano s $(u, v) = (2, -1)$, jedno rješenje jednadžbe (1.3) je $(x_0, y_0) = (2(8 - 15s), -(8 - 15s))$. No onda su sva rješenja jednadžbe (1.3) dana s

$$\begin{cases} x = 16 - 30s + 5r \\ y = -8 + 15s - 3r \end{cases}, \quad s, r \in \mathbb{Z}.$$

Uzimanjem u obzir (1.2) dobivamo sva rješenja polazne jednadžbe:

$$\begin{cases} x = 16 - 30s + 5r \\ y = -8 + 15s - 3r \\ z = 1 - 2s, \end{cases}, \quad s, r \in \mathbb{Z}.$$

◇

Zadatak 1.2. *Vlasnik prodavaonice cipela kupuje proljetne cipele po cijeni 18 EUR i zimске po cijeni 11 EUR za svaki par. Ukupna je cijena cipela 1188 EUR. Koliki je najmanji ukupan broj parova cipela koji je mogao kupiti?*

Rješenje. Označimo s x broj parova proljetnih cipela te neka nam y označava broj parova zimskih cipela. Potrebno je promotriti jednadžbu $18x + 11y = 1188$. Jasno je $(18, 11) = 1 \mid 1188$ i rješenje postavljene jednadžbe zaista postoji. Uočimo da je $18 \cdot (-3) + 11 \cdot 5 = 1$ pa je $(x_0, y_0) = (-3564, 5940)$ i sva rješenja zadane jednadžbe dana su sa

$$\begin{cases} x = -3564 + 11t \\ y = 5940 - 18t \end{cases}, \quad t \in \mathbb{Z}.$$

Kako broj parova cipela ne može biti negativan, mora biti $x, y \geq 0$ te dobivamo

$$t \geq \frac{3564}{11} = 324 \quad \text{i} \quad t \leq \frac{5940}{18} = 330.$$

Dakle, $324 \leq t \leq 330$ te ukupan broj parova cipela iznosi

$$x + y = (-3564 + 11t) + (5940 - 18t) = 2376 - 7t$$

i najmanji je za $t = 330$. Dobivamo $x + y = 66$ i $x = 66, y = 0$. Prema tome, vlasnik prodavaonice kupio je 66 parova proljetnih cipela. \diamond

2. Pitagorine trojke

Definicija 2.1. Uređenu trojku prirodnih brojeva (x, y, z) zovemo Pitagorina trojka ako su x i y duljine kateta, a z duljina hipotenuze nekog pravokutnog trokuta, tj. ako vrijedi

$$x^2 + y^2 = z^2. \quad (2.1)$$

Takav trokut zovemo Pitagorin trokut.

Ako su x, y, z relativno prosti, onda kažemo da je (x, y, z) primitivna Pitagorina trojka. Takav trokut zovemo primitivni Pitagorin trokut.

Dakle, proučavanje Pitagorinih trokuta usko je povezano s promatranjem diofantske jednadžbe (2.1). Kako su i x i y duljine kateta u Pitagorinom trokutu, dogovorno uzimamo da je $(x, y, z) = (y, x, z)$.

U ovom odjeljku razmatrat ćemo probleme postojanja Pitagorinih trokuta (trojki) koji posjeduju i neka dodatna svojstva. Svaki takav problem svodi se na rješavanje neke diofantske jednadžbe ili sustava diofantskih jednadžbi.

Primjer 2.1. Lako se vidi da je u primitivnoj Pitagorinoj trojci (x, y, z) jedan od brojeva x, y paran, dok je drugi neparan. Naime, ako bi oba bila parna, onda bi i z bio paran pa trojka ne bi bila primitivna. Ako bi oba bila neparna, onda bi vrijedilo $x^2 \equiv y^2 \equiv 1 \pmod{4}$ pa dobivamo $z^2 = x^2 + y^2 \equiv 2 \pmod{4}$, što je nemoguće. Svojstva potpunih kvadrata koja smo ovdje koristili mogu se naći u Zadatku 1.11. iz poglavlja Djeljivost, odnosno u Primjeru 1.2. iz poglavlja Kongruencije.

Uočite da odavde slijedi da je u primitivnoj Pitagorinoj trojci z neparan.

Zadatak 2.1. Dokažite da je u svakom primitivnom Pitagorinom trokutu duljina barem jedne stranice djeljiva s 5.

Rješenje. Ako je duljina jedne od stranica djeljiva s 5, gotovi smo. Pretpostavimo da ni jedna od stranica nije djeljiva s 5. Potpun kvadrat broja

koji nije djeljiv s 5 pri dijeljenju s 5 može dati ostatke 1 i 4 pa je $z^2 = x^2 + y^2 \equiv 2, 0, 3 \pmod{5}$. Kako je $z^2 \equiv 2, 3 \pmod{5}$ nemoguće, slijedi $z^2 \equiv 0 \pmod{5}$, tj. $z \equiv 0 \pmod{5}$, što je kontradikcija pa slijedi tvrdnja. \diamond

Zadatak 2.2. *Dokažite da je u svakom primitivnom Pitagorinom trokutu umnožak duljina stranica djeljiv sa 60.*

Zadatak 2.3. *Odredite sve primitivne Pitagorine trojke oblika $(a, a+d, a+2d)$.*

Rješenje. Iz

$$a^2 + (a+d)^2 = (a+2d)^2$$

sređivanjem dobivamo jednadžbu

$$a^2 - 2ad - 3d^2 = 0.$$

Promatramo li tu jednadžbu kao kvadratnu jednadžbu s nepoznanicom a dobivamo

$$a_{1,2} = d \pm 2d.$$

Kako je slučaj $a = -d$ nemoguć jer $a+d$ mora biti prirodni broj, zaključujemo $a = 2d$. Stoga su Pitagorine trojke toga oblika dane s $(3d, 4d, 5d)$, $d \in \mathbb{N}$. Primitivna Pitagorina trojka s ovim svojstvom dana je s $d = 1$, tj. to je trojka $(3, 4, 5)$. \diamond

Teorem 2.1. ([3]) *Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran dane su formulama*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2,$$

gdje su $m, n \in \mathbb{N}$ različite parnosti, $(m, n) = 1$ i $m > n$.

Općenit zapis Pitagorinih trojki prvi se put spominje u Diofantovom djelu *Aritmetika* i Euklidovom djelu *Elementi*.

Primjer 2.2. *Želimo li odrediti sve primitivne Pitagorine trokute u kojima je jedna kateta jednaka 15, trebamo riješiti jednadžbu $m^2 - n^2 = 15$, jer jednadžba $2mn = 15$ očito nema rješenja. Kako je $m^2 - n^2 = (m-n)(m+n)$, $m-n < m+n$ i $15 = 1 \cdot 15 = 3 \cdot 5$, imamo dva slučaja:*

- iz $m - n = 1, m + n = 15$ slijedi $m = 8, n = 7$ pa prema formulama iz prethodnog teorema dobivamo trojku $(15, 112, 113)$,
- iz $m - n = 3, m + n = 5$ slijedi $m = 4, n = 1$ i analogno dobivamo trojku $(15, 8, 7)$.

Zadatak 2.4. *Odredite sve primitivne Pitagorine trokute kojima je površina jednaka 6.*

Rješenje. Kako je površina pravokutnog trokuta kojemu katete imaju duljine x i y dana s $P = \frac{xy}{2}$, uvrštavanjem formula iz Teorema 2.1. dobivamo jednadžbu

$$mn(m^2 - n^2) = mn(m - n)(m + n) = 6.$$

Kako je $m, m + n > 1$ i $m < m + n$, može biti samo $m = 2, m + n = 3$, odnosno $m = 3, n = 1$. Kako je u tom slučaju $m - n = 1$, vidimo da je zadovoljena tražena jednakost. Stoga je tražena trojka $(3, 4, 5)$. \diamond

Zadatak 2.5. *Odredite sve primitivne Pitagorine trokute (x, y, z) u kojima je duljina hipotenuze za dva veća od duljine jedne od kateta. Odredite najmanji $z > 2023$ s tim svojstvom.*

Rješenje. Pretpostavimo da je duljina hipotenuze u primitivnom Pitagorinom trokutu (x, y, z) za 2 veća od duljine jedne od kateta, tj. $z = x + 2$. Uvrstimo li u taj izraz $x = m^2 - n^2, z = m^2 + n^2$, dobivamo $n^2 = 1$ pa je $n = 1$. Uzmemo li u obzir uvjet da su m i n različite parnosti, $(m, n) = 1$ i $m > n$, slijedi $x = m^2 - 1, b = 2m, c = m^2 + 1$ i m je paran.

Najmanji $z > 2023$ s tim svojstvom dobiva se određivanjem najmanjeg parnog broja m za koji vrijedi $m^2 + 1 > 2023$, a to je $m = 46$. Stoga je traženo rješenje $z = 2117$. \diamond

Zadatak 2.6. *Neka je n neparni prirodni broj. Dokažite da postoji primitivna Pitagorina trojka u kojoj je duljina jedne katete jednaka n .*

Iz Teorema 2.1. slijedi da su sve Pitagorine trojke dane identitetom

$$[d(m^2 - n^2)]^2 + [2dmn]^2 = [d(m^2 + n^2)], \quad (2.2)$$

gdje su $d, m, n \in \mathbb{N}$, m, n različite parnosti, $(m, n) = 1$ i $m > n$.

Zadatak 2.7. *Odredite sve Pitagorine trokute u kojima je duljina jedne stranice jednaka 12.*

Rješenje. Trebamo riješiti diofantske jednadžbe $d(m^2 - n^2) = 12$, $2dmn = 12$, $d(m^2 + n^2) = 12$, gdje su $m, n \in \mathbb{N}$ različite parnosti, $(m, n) = 1$ i $m > n$. Uočimo da $d \mid 12$ i da za tako zadane m, n vrijedi $m^2 - n^2, mn, m^2 + n^2 > 1$. Slijedi $d \in \{1, 2, 3, 4, 6\}$.

Promotrimo moguće slučajeve za $d(m^2 - n^2) = 12$:

- Uočimo da su m, n različite parnosti pa je $m^2 - n^2$ neparni broj. Lako se vidi da su stoga slučajevi $d = 1, 2, 3, 6$ nemogući.
- Slučaj $d = 4$ vodi na $d = 2$ $m^2 - n^2 = (m - n)(m + n) = 3 = 1 \cdot 3$, odnosno na sustav jednadžbi $m - n = 1, m + n = 3$ kojemu je rješenje $(m, n) = (2, 1)$. Odavde dobivamo trojku $(12, 16, 20)$.

Ako je $2dmn = 12$, tj. $dmn = 6$, onda je $d \in \{1, 2, 3\}$ ($d \neq 6$ jer je $mn > 1$) i imamo:

- $d = 1$: tada je $mn = 6 = 6 \cdot 1 = 3 \cdot 2$, $(m, n) = (6, 1)$ generira trojku $(35, 12, 37)$, dok $(m, n) = (3, 2)$ generira trojku $(5, 12, 13)$,
- $d = 2$ vodi na $mn = 3$, što je nemoguće jer jedan od m i n mora biti paran,
- $d = 3$: tada je $mn = 2 = 2 \cdot 1$, $(m, n) = (2, 1)$ generira trojku $(9, 12, 15)$.

Promotrimo moguće slučajeve za $d(m^2 + n^2) = 12$. Kako su m i n različite parnosti, slijedi da je $m^2 + n^2 \equiv 1 \pmod{4}$. Lako se vidi da taj uvjet nije zadovoljen za $d \in \{1, 2, 3, 4, 6\}$ pa ovaj slučaj ne daje ni jedno rješenje. \diamond

Zadatak 2.8. *Odredite sve Pitagorine trokute u kojima je duljina jedne stranice jednaka 39.*

Zadatak 2.9. *Odredite sve Pitagorine trokute čiji opseg nije veći od 60.*

Rješenje. Traže se Pitagorine trojke sa svojstvom $x + y + z \leq 60$. Primjenom formula (2.2) dobivamo

$$dmn(m + n) \leq 30, \quad (2.3)$$

pri čemu su $m, n \in \mathbb{N}$ različite parnosti, $(m, n) = 1$ i $m > n$.

Izgenerirat ćemo najprije Primitivne Pitagorine trojke s traženim svojstvom (tj. slučaj $d = 1$):

- Za $(m, n) = (2, 1)$, dobivamo trojku $(3, 4, 5)$. Uočite da je to jedina mogućnost u kojoj je $m = 2$.

- Za $(m, n) = (3, 2)$, dobivamo trojku $(12, 5, 3)$. Također, to je jedina mogućnost u kojoj je $m = 3$.
- Za $(m, n) = (4, 1)$, dobivamo trojku $(8, 15, 17)$. Za $(m, n) = (4, 3)$ dobivamo $mn(m+n) > 30$ pa je taj slučaj nemoguć.
- Za $(m, n) = (5, 1)$, dobivamo $mn(m+n) > 30$. Taj je slučaj nemoguć, kao i svi ostali slučajevi koji uključuju $m \geq 5$.

Lako se provjeri da su, s obzirom na nejednakost (2.3), dodatne moguće vrijednosti parametra d koje generira trojka $(3, 4, 5)$ jednake 2, 3, 4, 5, dok je jedina dodatna moguća vrijednosti parametra d koju generiraju trojke $(12, 5, 3)$ i $(8, 15, 17)$ dana s $d = 2$. Stoga su sve tražene Pitagorine trojke dane s:

$$(3, 4, 5), (6, 8, 10), (9, 12, 15), (15, 20, 25), \\ (5, 12, 13), (10, 24, 26), (8, 15, 17), (7, 24, 25).$$

◇

Zadatak 2.10. *Neka je $(n^4 - 4, 4n^2, n^4 + 4)$, $n \in \mathbb{N}$ Pitagorina trojka. Dokažite da postoji beskonačno mnogo parametara n za koje je ta trojka primitivna.*

Rješenje. Promotrimo neparni prirodni broj n . Uočimo da za $d = (n^4 - 4, n^4 + 4)$ vrijedi $d \mid n^4 - 4 - (n^4 + 4) = -8$. Kako su $n^4 - 4, n^4 + 4$ neparan, slijedi da je $d = 1$. Time je tvrdnja dokazana. ◇

Zadatak 2.11. *Neka su $m, n, k \in \mathbb{N}$ i (m, n, k) Pitagorin trokut. Dokažite da postoji Pitagorin trokut kojemu je duljina hipotenuze k^2 .*

3. Pellove jednadžbe

U ovom ćemo se odjeljku baviti još jednom poznatom kvadratnom diofant-skom jednadžbom, Pellovom jednadžbom. Jednadžba je dobila ime prema engleskom matematičaru Johnu Pellu, kojemu je Euler greškom pripisao zasluge za njezino rješavanje. Jednadžbu su sustavno proučavali srednjovjekovni indijski matematičari, dok je prvi Europljanin koji ju je riješio bio William Brouncker u 17. st.

Kao što ćemo vidjeti, rješenja Pellove jednadžbe generiraju se pomoću konvergenti razvoja kvadratnih iracionalnosti u verižni razlomak. Više detalja o razvoju u verižni razlomak realnog broja i svojstvima takvog razvoja

može se naći u [3]. Mi ćemo ovdje samo navesti definicije i osnovna svojstva pojmova koji će nam biti potrebni.

Definicija 3.1. *Za beskonačni verižni razlomak*

$$[a_0, a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

kažemo da je *periodski* ako postoje cijeli brojevi $k \geq 0, m \geq 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geq k$. U tom slučaju verižni razlomak pišemo u obliku

$$[a_0, a_1, \dots, a_{k-1}, \overline{a_k, a_{k+1}, \dots, a_{k+m-1}}],$$

gdje “crtā” iznad brojeva a_k, \dots, a_{k+m-1} znači da se taj blok brojeva ponavlja unedogled. Najmanji m s tim svojstvom je duljina perioda verižnog razlomka.

Napomena 3.1. *Racionalni broj $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$ je n -ta konvergenta u razvoju broja α u verižni razlomak. Brojevi p_n i q_n zadovoljavaju rekurzivne relacije ([3]):*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad p_{-2} = 0, \quad p_{-1} = 1, \quad (3.1)$$

$$q_n = a_n q_{n-1} + q_{n-2}, \quad q_{-2} = 1, \quad q_{-1} = 0. \quad (3.2)$$

Definicija 3.2. *Za iracionalni broj α kažemo da je kvadratna iracionalnost ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Svaka je kvadratna iracionalnost oblika $\frac{s \pm \sqrt{d}}{t}$, $s \in \mathbb{Z}, d \in \mathbb{N}, d \neq \square, t \in \mathbb{Z} \setminus \{0\}$. Vrijedi sljedeći teorem.

Teorem 3.1. (Euler, Lagrange, [3]) *Razvoj u verižni razlomak realnog broja α periodski je ako i samo ako je α kvadratna iracionalnost.*

Napomena 3.2. *Razvoj broja $\alpha_0 = \frac{s_0 + \sqrt{d}}{t_0}$, $d \in \mathbb{N}, d \neq \square$, u verižni razlomak može se dobiti sljedećim algoritmom:*

$$a_i = \left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \quad i \in \mathbb{N}_0.$$

Teorem 3.2. ([3]) *Ako $d \in \mathbb{N}, d \neq \square$, onda razvoj u verižni razlomak broja \sqrt{d} ima oblik*

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_{r-1}, 2a_0}].$$

Primjer 3.1. Za razvoj broja $\sqrt{23}$ u verižni razlomak, prema algoritmu u Napomeni 3.2., dobivamo

- $s_0 = 0, t_0 = 1 \implies a_0 = \lfloor \sqrt{23} \rfloor = 4,$
- $s_1 = a_0 t_0 - s_0 = 4, t_1 = \frac{23 - s_1^2}{t_0} = 7 \implies a_1 = \left\lfloor \frac{4 + \sqrt{23}}{7} \right\rfloor = 1,$
- $s_2 = a_1 t_1 - s_1 = 3, t_2 = \frac{23 - s_2^2}{t_1} = 2 \implies a_2 = \left\lfloor \frac{3 + \sqrt{23}}{2} \right\rfloor = 3,$
- $s_3 = a_2 t_2 - s_2 = 3, t_3 = \frac{23 - s_3^2}{t_2} = 7 \implies a_3 = \left\lfloor \frac{3 + \sqrt{23}}{7} \right\rfloor = 1,$
- $s_4 = a_3 t_3 - s_3 = 4, t_4 = \frac{23 - s_4^2}{t_3} = 1 \implies a_4 = \left\lfloor \frac{4 + \sqrt{23}}{1} \right\rfloor = 8,$
- $s_5 = a_4 t_4 - s_4 = 4, t_5 = \frac{23 - s_5^2}{t_4} = 7 \implies a_5 = a_1 = 1.$

Oдавде je $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$. Uočimo da teorijski rezultat dan u Teoremu 3.2. možemo iskoristiti u sljedećem smislu: ako dobijemo razvoj koji nije oblika navedenog u tom teoremu, jasno je da smo nešto krivo izračunali.

Definicija 3.3. Neka je $d \in \mathbb{N}, d \neq \square$. Diofantska jednađžba oblika

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

naziva se Pellova jednađžba, dok se diofantska jednađžba oblika

$$x^2 - dy^2 = N,$$

gdje je $N \in \mathbb{Z} \setminus \{0\}$ naziva pelovska jednađžba.

Lako se vidi da Pellova jednađžba uvijek ima sljedeća trivijalna rješenja: $(x, y) = (\pm 1, 0)$. Zanimat će nas ima li ta jednađžba netrivialnih rješenja. Uočimo da je zbog kvadrata dovoljno promatrati postojanje rješenja u skupu prirodnih brojeva.

U ovom odjeljku promatrat ćemo rješivost diofantskih jednađžbi

$$x^2 - dy^2 = \pm 1,$$

gdje je $d \in \mathbb{N}, d \neq \square$ u skupu prirodnih brojeva. Vezano uz rješivost tih jednađžbi istaknut ćemo dva teorema. Napomenimo da pod najmanjim rješenjem (x, y) dane jednađžbe u skupu prirodnih brojeva smatramo ono s najmanjim x .

Teorem 3.3. ([3]) *Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, onda su sva rješenja te jednadžbe u prirodnim brojevima dana s $(x_n, y_n), n \in \mathbb{N}$, gdje su x_n, y_n prirodni brojevi definirani s*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Rješenje (x_1, y_1) iz prethodnog teorema naziva se i fundamentalno rješenje Pellove jednadžbe.

Teorem 3.4. ([3]) *Neka je r duljina perioda u razvoju u verižni razlomak broja \sqrt{d} i $\frac{p_i}{q_i}$ i-ta konvergenta u razvoju od \sqrt{d} .*

- (1) *Ako je r paran, onda jednadžba oblika $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja u prirodnim brojevima od $x^2 - dy^2 = 1$ dana su s $x = p_{nr-1}, y = q_{nr-1}, n \in \mathbb{N}$.*
- (2) *Ako je r neparan, onda su sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = -1$ dana s $x = p_{nr-1}, y = q_{nr-1}, n$ neparan, dok su sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ dana s $x = p_{nr-1}, y = q_{nr-1}, n$ paran.*

Uočimo da jednadžba $x^2 - dy^2 = 1$ uvijek ima beskonačno mnogo rješenja u prirodnim brojevima, dok jednadžba $x^2 - dy^2 = -1$ ima beskonačno rješenja u prirodnim brojevima ako je duljina perioda u razvoju broja \sqrt{d} u verižni razlomak neparna; inače nema rješenja.

Primjer 3.2. *Promotrimo diofantske jednadžbe*

$$x^2 - 23y^2 = \pm 1.$$

Kako je prema Primjeru 3.1. $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$, slijedi da je duljina perioda u razvoju broja $\sqrt{23}$ u verižni razlomak jednaka 4, tj. $r = 4$. Prema Teoremu 3.4. slijedi da jednadžba $x^2 - 23y^2 = -1$ nema rješenja, dok su sva rješenja jednadžbe $x^2 - 23y^2 = 1$ dana s $x = p_{4n-1}, y = q_{4n-1}, n \in \mathbb{N}$. Za $n = 1$ dobivamo najmanje rješenje $(x_1, y_1) = (p_3, q_3)$. Kako je $\frac{p_3}{q_3} = [4, 1, 3, 1] = \frac{24}{5}$, slijedi da je $(x_1, y_1) = (24, 5)$. Prema Teoremu 3.3. sva su rješenja jednadžbe $x^2 - 13y^2 = 1$ dana s $(x_n, y_n), n \in \mathbb{N}$, gdje su x_n, y_n prirodni brojevi definirani s

$$x_n + y_n\sqrt{23} = (24 + 5\sqrt{23})^n.$$

Kako je

$$(24 + 5\sqrt{23})^2 = 1151 + 24\sqrt{23},$$

to je $(x_2, y_2) = (1151, 24)$. Analogno, iz

$$(24 + 5\sqrt{23})^3 = 55224 + 11515\sqrt{23}$$

dobivamo $(x_3, y_3) = (55224, 11515)$. Jasno je da sasvim analogno možemo izgenirirati proizvoljan broj rješenja.

Zadatak 3.1. Nađite barem dva rješenja u prirodnim brojevima jednadžbi

$$x^2 - 13y^2 = \pm 1.$$

Rješenje. Korištenjem algoritma iz Napomene 3.2. lako se pokaže da je $\sqrt{13} = [3, \overline{1}, 1, 1, 6]$ (za vježbu sami provedite račun). Stoga je $r = 5$ i prema Teoremu 3.4. slijedi da su sva rješenja jednadžbe $x^2 - 13y^2 = -1$ dana s $x = p_{5n-1}, y = q_{5n-1}$, n neparan, dok su sva rješenja jednadžbe $x^2 - 13y^2 = 1$ dana s $x = p_{5n-1}, y = q_{5n-1}$, n paran.

Kako bismo odredili dva rješenja jednadžbe $x^2 - 13y^2 = -1$, trebamo, na primjer, odrediti (p_4, q_4) i (p_{14}, q_{14}) . U tu je svrhu najbolje iskoristiti rekurzivne relacije za p_n i q_n spomenute u Napomeni 3.1. To možemo provesti na način da vrijednosti popunjavamo tablično. Za određivanje (p_4, q_4) tablični bi dio izgledao ovako:

n	-2	-1	0	1	2	3	4
a_n			3	1	1	1	1
p_n	0	1	3	4	7	11	18
q_n	1	0	1	1	2	3	5

Da biste pokazali da je $(p_{14}, q_{14}) = (23382, 6485)$, za vježbu odredite ostatak tablice.

Već smo komentirali da su rješenja jednadžbe $x^2 - 13y^2 = 1$ dana s $x = p_{5n-1}, y = q_{5n-1}$, n paran. Najmanje rješenje te jednadžbe je (p_9, q_9) . Ako ste u prvom dijelu zadatka odredili (p_{14}, q_{14}) , onda u tablici već imate ove vrijednosti. Dobiva se $(p_9, q_9) = (649, 180)$. Kako bi se odredilo drugo rješenje u prirodnim brojevima, nije nužno određivati (p_{19}, q_{19}) , nego možemo koristiti relaciju iz Teorema 3.3. Kako je

$$(649 + 180\sqrt{13})^2 = 8442401 + 233640\sqrt{13},$$

slijedi da je drugo rješenje u prirodnim brojevima $(842401, 233640)$. \diamond

Zadatak 3.2. Nađite, ako postoje, sva rješenja u cijelim brojevima jednadžbi $x^2 - 7y^2 = \pm 1$ koja zadovoljavaju uvjet $0 < x < 500$.

Zadatak 3.3. *Dokažite da u skupu \mathbb{N} postoji beskonačno mnogo rješenja jednadžbe*

$$1 + 2 + \cdots + k = m^2$$

te odredite barem tri rješenja.

Rješenje. Uočimo da se zadana jednadžba može zapisati u obliku

$$\frac{k(k+1)}{2} = m^2,$$

tj.

$$k^2 + k = 2m^2.$$

Množenjem prethodne jednadžbe s 4 i nadopunjavanjem na potpun kvadrat dobivamo jednadžbu

$$(2k+1)^2 - 8m^2 = 1. \quad (3.3)$$

Uz supstituciju $x = 2k+1$ i $y = m$, jednadžba (3.3) ekvivalentna je Pellovoj jednadžbi

$$x^2 - 8y^2 = 1.$$

Kako Pellova jednadžba ima beskonačno mnogo rješenja (x, y) , pri čemu je x neparan, to će postojati beskonačno mnogo rješenja (k, m) jednadžbe (3.3).

Kako bismo odredili barem tri rješenja, iskoristit ćemo, kao i ranije, Napomenu 3.1., Teorem 3.4. i Teorem 3.3. Iz $\sqrt{8} = [2, \overline{1, 4}]$ slijedi da je $r = 2$ pa su sva rješenja jednadžbe $x^2 - 8y^2 = 1$ dana s (p_{2n-1}, q_{2n-1}) , $n \in \mathbb{N}$. Kako je $(p_1, q_1) = (3, 1)$, sva rješenja te Pellove jednadžbe dana su i s

$$x_l + y_l\sqrt{8} = (3 + \sqrt{8})^l, \quad l \in \mathbb{N}.$$

Odavde se za $l = 2, 3$ dobivaju rješenja $(17, 6), (99, 35)$. Rješenja $(x, y) \in \{(3, 1), (17, 6), (99, 35)\}$ generiraju rješenja $(k, m) \in \{(1, 1), (8, 6), (49, 35)\}$.
 \diamond

Zadatak 3.4. *Neka je $n \in \mathbb{N}, n \geq 3$. Ispitajte imaju li jednadžbe $x^2 - (n^2 - 1)y^2 = \pm 1$ rješenja u skupu prirodnih brojeva.*

Zadatak 3.5. *Ako je duljina perioda u razvoju u verižni razlomak broja \sqrt{d} neparni broj, dokažite da $d \not\equiv 3 \pmod{4}$.*

Rješenje. Pretpostavimo da je duljina razvoja u verižni razlomak broja \sqrt{d} neparni broj. Prema Teoremu 3.4. slijedi da jednačbe $x^2 - dy^2 = \pm 1$ imaju rješenja u prirodnim brojevima.

Vrijedi sljedeće

$x^2 \pmod{4}$	$y^2 \pmod{4}$	$(x^2 - dy^2) \pmod{4}$
0	0	0
1	0	1
0	1	$-d$
1	1	$1 - d$

Uočimo da će jednačba $x^2 - dy^2 = -1$ imati rješenja samo ako je $-d \equiv -1 \pmod{4}$ ili $1 - d \equiv -1 \pmod{4}$. Lako se vidi da za $d \equiv 3 \pmod{4}$ te relacije ne mogu biti zadovoljene. \diamond

Zadatak 3.6. *Odredite tri prirodna broja n sa svojstvom da su $2n + 1$ i $n + 1$ potpuni kvadrati.*

Rješenje. Iz $n + 1 = x^2$, $2n + 1 = y^2$ dobivamo jednačbu $y^2 - 2x^2 = -1$. Kako je $\sqrt{2} = [1, \overline{2}]$, slijedi da su rješenja jednačbe $y^2 - 2x^2 = -1$ dana s $y = p_{n-1}$, $x = q_{n-1}$, n neparan. Dobivamo

n	-2	-1	0	1	2	3	4	5	6
a_n			1	2	2	2	2	2	2
p_n	0	1	1	3	7	17	41	99	239
q_n	1	0	1	2	5	12	29	70	169

Kako je $n \in \mathbb{N}$ i $n + 1 = x^2$, dobivamo $x \in \{5, 29, 169\}$, odnosno $n \in \{24, 840, 28560\}$. \diamond

Zadatak 3.7. *Odredite četiri prirodna broja n sa svojstvom da je $3n^2$ umnožak dvaju susjednih prirodnih brojeva.*

4. Zadatci za vježbu

Zadatak 4.1. *Riješite sljedeće diofantske jednačbe:*

a) $6x + 9y = 21$,

b) $11x + 13y = 369$,

c) $858x + 253y = 99$,

d) $3x - 6y + 5z = 4$,

e) $8x + 14y + 5z = 11$.

Zadatak 4.2. *Riješite sustav jednadžbi*

$$x + 10y + 25z = 200,$$

$$x + y + z = 50.$$

Zadatak 4.3. *Prodavaonica parketa na raspolaganju ima parket prve klase kvalitete po cijeni od 69 EUR/m² i druge klase kvalitete po cijeni od 27 EUR/m². Za obnovu je stambene zgrade investitor kupio određen broj parketa ukupne cijene 1218 EUR. Koliko je mogao kupiti parketa prve, a koliko parketa druge klase kvalitete?*

Zadatak 4.4. *Koliko se nogometnih ulaznica može kupiti za 1490 EUR ako se one prodaju po cijeni od 30 EUR i 50 EUR?*

Zadatak 4.5. *Odredite sve Pitagorine trokute čija je površina jednaka opsegu.*

Zadatak 4.6. *Nadite sve Pitagorine trokute čiji zbroj duljina stranica nije veći od 60.*

Zadatak 4.7. *Odredite sve primitivne Pitagorine trojke u kojima je barem jedan član manji od 8.*

Zadatak 4.8. *Neka je $p \equiv 3 \pmod{4}$ prosti broj. Odredite sve primitivne Pitagorine trojke u kojima je jedan član jednak p .*

Zadatak 4.9. *Odredite sve Pitagorine trojke u kojima je jedan član jednak 18.*

Zadatak 4.10. *Odredite sve primitivne Pitagorine trojke u kojima je točno jedan član manji od 9.*

Zadatak 4.11. *Nadite sve Pitagorine trojke (x, y, z) u kojima je jedna stranica jednaka 72 i vrijedi $(x, y, z) = 3$.*

Zadatak 4.12. *Dokažite da postoji beskonačno mnogo Pitagorinih trokuta kod kojih je duljina jedne katete potpun kvadrat.*

Zadatak 4.13. U skupu prirodnih brojeva riješite jednadžbu $z^2 = xy(x+y)$ uz uvjet $(x, y) = 1$.

Zadatak 4.14. Nađite sve primitivne Pitagorine trokute u kojima je duljina hipotenuze z za 8 veća od duljine jedne katete. Koji je najmanji $z > 1000$ s tim svojstvom?

Zadatak 4.15. Nađite, ako postoje, najmanja rješenja u prirodnim brojevima jednadžbi $x^2 - 41y^2 = \pm 1$.

Zadatak 4.16. U skupu \mathbb{N}_0 nađite sva rješenja jednadžbi $x^2 - 29y^2 = \pm 1$, uz uvjet da je $y < 2000$.

Zadatak 4.17. Nađite u prirodnim brojevima barem dva rješenja jednadžbe $x^2 = 96y^2 + 1$.

Zadatak 4.18. Ako je moguće, odredite po dva rješenja u prirodnim brojevima jednadžbi $x^2 - 28y^2 = \pm 1$.

Zadatak 4.19. U skupu prirodnih brojeva, ako je moguće, nađite po dva rješenja jednadžbi $55x^2 - y^2 = \pm 1$.

Zadatak 4.20. U skupu cijelih brojeva nađite sva rješenja jednadžbi $x^2 - 15y^2 = \pm 1$ sa svojstvom da je $|y| < 50$.

Zadatak 4.21. Odredite dva prirodna broja n sa svojstvom da su brojevi $n - 2$ i $7n - 13$ potpuni kvadrati.

Zadatak 4.22. Dokažite da postoji beskonačno mnogo prirodnih brojeva m i n sa svojstvom

$$m^2 + 2m - 7n^2 + 14n - 7 = 0,$$

a zatim odredite tri takva para (m, n) .

Zadatak 4.23. Odredite prirodni broj $n > 100$ takav da je $\frac{n^2 + 1}{2}$ potpun kvadrat.

Zadatak 4.24. Odredite dva prirodna broja n sa svojstvom da je $7n^2$ umnožak dvaju uzastopnih prirodnih brojeva.

Zadatak 4.25. Dokažite da postoji beskonačno mnogo prirodnih brojeva m sa svojstvom da je $2 + 2\sqrt{33m^2 + 1}$ prirodni broj i odredite barem tri takva prirodna broja m .

Zadatak 4.26. *Neka su $n \geq 2$ i $d \neq \square$ prirodni brojevi.*

i) Odredite razvoj broja $\sqrt{n^2 - 1}$ u verižni razlomak.

ii) Dokažite da je period razvoja broja $\sqrt{k^2 d}$ u verižni razlomak jednak 2 za beskonačno mnogo prirodnih brojeva k .

Zadatak 4.27. *Odredite tri para $(x, y) \in \mathbb{N}^2$ koji su rješenja jednadžbe $-7x^2 + 18xy - 7y^2 = 1$.*

Zadatak 4.28. *Dokažite da postoji beskonačno mnogo prirodnih brojeva n takvih da je $n^2 + (n + 1)^2$ potpun kvadrat. Odredite prvih pet brojeva n s prethodnim svojstvom.*

Zadatak 4.29. *Dokažite da je $p = 7$ jedini prosti broj sa svojstvom da je $47p^2 + 1$ potpun kvadrat.*

Zadatak 4.30. *Neka je k neparni broj i $k \geq 3$. Odredite razvoj u jednostavni verižni razlomak broja $\sqrt{k^2 + 4}$. Nađite fundamentalno rješenje Pelllove jednadžbe $x^2 - (k^2 + 4)y^2 = 1$.*

Upute za rješavanje zadataka

Zadatak 2.2. Iskoristite Primjer 2.1., Zadatak 2.1. i pokažite da duljina barem jedne stranice mora biti djeljiva s 5.

Zadatak 2.8. Dobiva se: $(x, y, z) \in \{(39, 760, 761), (39, 80, 89), (39, 252, 255), (15, 36, 39), (39, 52, 65)\}$.

Zadatak 2.11. Tvrdnja slijedi iz osnovne relacije za Pitagorine trojke, množenjem s k^2 .

Zadatak 3.2. Najprije se odredi $\sqrt{7} = [2, \overline{1, 1, 4}]$. Kako je $r = 4$, dobiva se da jednadžba $x^2 - 7y^2 = 1$ ima sljedeća cjelobrojna rješenja s traženim svojstvom: $(x, y) \in \{(1, 0), (8, \pm 3), (127, \pm 48)\}$. Druga jednadžba nema rješenja.

Zadatak 3.4. Pokažite da je $\sqrt{n^2 - 1} = [n - 1, \overline{1, 2n - 2}]$, a zatim na osnovu perioda zaključite kako jednadžba $x^2 - (n^2 - 1)y^2 = 1$ ima beskonačno mnogo rješenja, dok jednadžba $x^2 - (n^2 - 1)y^2 = -1$ nema rješenja.

Zadatak 3.7. Zadatak se svodi na traženje rješenja jednadžbe $x^2 - 12n^2 = 1$. Dobiva se $n \in \{2, 28, 390, 5432\}$.

Zadatak 4.1. a) $x = 2 + 3t, y = 1 - 2t, t \in \mathbb{Z}$; b) $x = 2214 + 13t, y = -1845 - 11t, t \in \mathbb{Z}$; c) $x = 1 + 23t, y = -3 - 78t, t \in \mathbb{Z}$; d) $x = -2 - u - 2v, y = -u + 2v, z = 3v + 2, u, v \in \mathbb{Z}$; e) $x = -44 + 10u + 7v, y = 22 - 5u - 4v, z = 11 - 2u, u, v \in \mathbb{Z}$.

Zadatak 4.2. Oduzimanjem slijedi jednadžba $9y + 24z = 150$, a njena su rješenja $y = -2 + 8t, z = 7 - 3t, t \in \mathbb{Z}$. Sada iz polazne jednadžbe slijedi $x = 45 - 5t$.

Zadatak 4.3. Ako se sa x i y označi broj paketa pojedine klase kvalitete, potrebno je promotriti jednadžbu $69x + 27y = 1218$. Rješenja su $x = 812 - 9t, y = -2030 + 23t, t \in \mathbb{Z}$. S obzirom da je $x, y \geq 0$, slijedi $t \in \{89, 90\}$. Tada dobivamo $(x, y) \in \{(11, 17), (2, 40)\}$. Dakle, investitor je mogao na dva načina kupiti parket pojedine klase kvalitete da bi ukupna cijena iznosila 1218 EUR.

Zadatak 4.4. Označite li s x i y pojedinu vrstu nogometnih ulaznica, dobit ćete jednadžbu $30x + 50y = 1490$. Njena su rješenja $x = 48 + 5t, y = 1 - 3t, t \in \mathbb{Z}$. Iz uvjeta $x, y \geq 0$ slijedi $-9 \leq t \leq 0$ pa je $(x, y) \in \{(3, 28), (8, 25), (13, 22), (18, 19), (23, 16), (28, 13), (33, 10), (38, 7), (43, 4), (48, 1)\}$. Prema tome, postoji deset načina kupnje pojedine vrste ulaznica da bi ukupna cijena iznosila 1490 EUR.

Zadatak 4.5. Dani uvjet vodi na $dn(m - n) = 2$, odakle se dobivaju rješenja $(5, 12, 13), (6, 8, 10)$.

Zadatak 4.6. Slijedi: $(x, y, z) \in \{(3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25), (6, 8, 10), (10, 24, 26), (15, 20, 25), (9, 12, 15), (12, 16, 20)\}$.

Zadatak 4.7. Rješenja su: $(x, y, z) \in \{(3, 4, 5), (5, 12, 13), (7, 24, 25)\}$.

Zadatak 4.8. Primjenom definicije primitivnih Pitagorinih trojki dobiva se $(x, y, z) = (p, \frac{p^2-1}{2}, \frac{p^2+1}{2})$.

Zadatak 4.9. Rješenja su: $(x, y, z) \in \{(18, 24, 30), (18, 80, 82)\}$.

Zadatak 4.10. Dobiva se $(x, y, z) \in \{(5, 12, 13), (7, 24, 25), (8, 15, 17)\}$.

Zadatak 4.11. Rješenja su $(x, y, z) \in \{(21, 72, 75), (429, 72, 435)\}$.

Zadatak 4.12. Uočite da se množenjem osnovne relacije za Pitagorin trokut s npr. $x^2 d^4$ dobiva beskonačno mnogo Pitagorinih trokuta s traženim svojstvom.

Zadatak 4.13. Najprije zaključite da su brojevi x, y i $x + y$ u parovima relativno prosti. Tada primjenom Osnovnog teorema aritmetike slijedi $x = x_1^2, y = y_1^2, x + y = u^2$, gdje su x_1, y_1, u također u parovima relativno prosti

cijeli brojevi pa tražimo primitivnu Pitagorinu trojku (x_1, y_1, u) . Primjenom definicije direktno slijedi $(x, y, z) \in \{((m^2 - n^2)^2, 4m^2n^2, 2mn(m^4 - n^4)), (4m^2n^2, (m^2 - n^2)^2, 2mn(m^4 - n^4))\}$.

Zadatak 4.14. Dobiva se $n = 2$ i $(x, y, z) = (m^2 - 4, 8m, m^2 + 4)$, gdje je $m > 2$ neparni prirodni broj. Iz $m^2 + 4 > 1000$ slijedi $m = 33$.

Zadatak 4.15. Lako se pokaže da je $\sqrt{41} = [6, \overline{2, 2, 12}]$. Stoga je odgovarajuće rješenje jednadžbe s -1 jednako $(x, y) = (p_2, q_2) = (32, 5)$, a pripadno rješenje jednadžbe s 1 je $(x, y) = (p_5, q_5) = (2049, 320)$.

Zadatak 4.16. Dobiva se $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$. Najmanje rješenje u prirodnim brojevima jednadžbe s -1 je $(x, y) = (p_4, q_4) = (70, 13)$ i to je jedino rješenje ove jednadžbe s traženim svojstvima. Najmanje rješenje u prirodnim brojevima jednadžbe s 1 jednako je $(x, y) = (p_9, q_9) = (9801, 1820)$ pa su rješenja s traženim svojstvima $(x, y) \in \{(0, 1), (9801, 1820)\}$.

Zadatak 4.17. Vrijedi: $\sqrt{96} = [9, \overline{1, 3, 1, 18}]$ pa su dva rješenja jednaka $(x, y) = (p_3, q_3) = (49, 5)$ i $(x, y) = (p_7, q_7) = (4801, 490)$.

Zadatak 4.18. Dobiva se $\sqrt{28} = [5, \overline{3, 2, 3, 10}]$, $(x, y) = (p_3, q_3) = (127, 24)$ i $(x, y) = (p_7, q_7) = (32257, 6096)$.

Zadatak 4.19. Pokaže se da je $\sqrt{55} = [7, \overline{2, 2, 2, 14}]$. Slijedi: $(x, y) \in \{(12, 89), (2136, 15841)\}$.

Zadatak 4.20. Dobiva se $\sqrt{15} = [3, \overline{1, 6}]$, stoga jednadžba s -1 nema cjelobrojnih rješenja. Tražena su rješenja jednadžbe s 1 $(x, y) \in \{(1, 0), (-1, 0), (4, 1), (-4, 1), (4, -1), (-4, -1), (31, 8), (-31, 8), (31, -8), (-31, -8)\}$.

Zadatak 4.21. Uvjeti $n - 2 = y^2$, $7n - 3 = x^2$, $x, y \in \mathbb{Z}$ vode na Pellovu jednadžbu $x^2 - 7y^2 = 1$. U Zadatku 3.2. određen je razvoj broja $\sqrt{7}$ u verižni razlomak. Korištenjem tamo dobivenih rješenja $(x, y) \in \{(8, 3), (127, 48)\}$, dobiva se $n \in \{11, 2306\}$.

Zadatak 4.22. Slijedi promatranje Pellove jednadžbe $(m+1)^2 - 7(n-1)^2 = 1$. Jasno je da ona ima beskonačno mnogo rješenja. Dobiva se $(m, n) \in \{(7, 4), (126, 49), (2023, 766)\}$.

Zadatak 4.23. Promatranjem rješenja jednadžbe $n^2 - 2m^2 = -1$ dobiva se $n = 239$.

Zadatak 4.24. Iz $7n^2 = m(m+1)$, $m \in \mathbb{N}$, zadatak se svodi na traženje rješenja jednadžbe $(2m+1)^2 - 28n^2 = 1$. Dobiva se $n \in \{24, 6096\}$.

Zadatak 4.25. Uvjet zadatka vodi nas do traženja rješenja jednadžbe $33m^2 + 1 = n^2$ u prirodnim brojevima m i n . Vrijedi: $\sqrt{33} = [5, \overline{1, 2, 1, 10}]$. Dobiva se $n \in \{4, 184, 8460\}$.

Zadatak 4.26. *i)* $\sqrt{n^2 - 1} = [n - 1, \overline{1, 2n - 2}]$; *ii)* Kako je period razvoja broja $\sqrt{n^2 - 1}$ jednak dva, dovoljno je pokazati da je $k^2d = n^2 - 1$ za beskonačno mnogo prirodnih brojeva k i n .

Zadatak 4.27. Ekvivalentno je promotriti jednadžbu $(x+y)^2 - 8(x-y)^2 = 1$. Dobiva se $(x, y) \in \{(2, 1), (67, 32), (2276, 1087)\}$.

Zadatak 4.28. Iz $n^2 + (n+1)^2 = k^2$, $k \in \mathbb{N}$ slijedi jednadžba $(2n+1)^2 - 2k^2 = -1$. Traženjem njenih rješenja dobiva se $n \in \{3, 20, 119, 696, 4059\}$.

Zadatak 4.29. Sva rješenja jednadžbe $x^2 - 47p^2 = 1$ u prirodnim brojevima dana su sa $x_n + p_n\sqrt{47} = (48 + 7\sqrt{47})^n$. Za $n > 1$ broj p_n nije prost pa slijedi $p = p_1 = 7$.

Zadatak 4.30. Za neparan $k \geq 3$ dobiva se $\sqrt{k^2 + 4} = [k, \overline{\frac{k-1}{2}, 1, 1, \frac{k-1}{2}, 2k}]$. Fundamentalno rješenje dane jednadžbe je $(x, y) = (p_9, q_9) = (k^6 + 6k^4 + 9k^2 + 2, k^5 + 4k^3 + 3k)$.

Literatura

- [1] A. ADLER, J. E. COURY, *The Theory of Numbers; A text and source book of problems*, Jones and Bartlett Publishers, London, 1995.
- [2] C. K. CALDWELL, *The Largest Known Primes*,
<https://primes.utm.edu/largest.html>
- [3] A. DUJELLA, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.
- [4] A. DUJELLA, M. MARETIĆ, *Kriptografija*, Element, Zagreb, 2007.
- [5] R. K. GUY, *Unsolved problems in Number theory*, Springer, New York, 2004.
- [6] A. JURASIĆ, M. RUKAVINA, *Pseudoprosti brojevi*, Matematičko fizički list **62** (2011), 20–25.
- [7] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Springer, New York, 1994.
- [8] I. MATIĆ, *Uvod u teoriju brojeva*, Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2015.
- [9] B. PAVKOVIĆ, B. DAKIĆ, P. MLADINIĆ, *Elementarna teorija brojeva*, Hrvatsko matematičko društvo, Zagreb, 1994.
- [10] J. J. TATTERSALL, *Elementary Number Theory in Nine Chapters*, Cambridge University Press, Cambridge, 1999.

Kazalo

- Bézoutov identitet, 9
broj svih pozitivnih djelitelja, 22
brojevi blizanci, 71
- Cezarova šifra, 55
- dekriptijski eksponent, 57
diofantska jednađba, 9, 81
djelitelj, 1
djeljivost, 1
- enkriptijski eksponent, 57
Eratostenovo sito, 18
Euklidov algoritam, 9
Eulerov kriterij, 67
Eulerov teorem, 45
Eulerova funkcija, 43
- Fermatov broj, 19
fundamentalno rješenje Pellove jednađbe, 91
- Gaussov kvadratni zakon reciprociteta, 69
- indeks, 50
- Jacobijev simbol, 72
javni ključ, 57
- kanonski rastav prirodnog broja, 16
Kineski teorem o ostatcima, 40
kongruencija, 33
- konvergenta u razvoju u verižni razlomak, 89
- kriptografija, 55
kriptosustav, 55
kvadrat, 5
kvadratna iracionalnost, 89
kvadratni neostatak, 65
kvadratni ostatak, 65
- Lagrangeov teorem, 53
Legendreov simbol, 66
linearna diofantska jednađba, 81
linearna kongruencija, 37
- Mali Fermatov teorem, 46
Mersenneov broj, 20
multiplikativna funkcija, 23
- najmanji zajednički višekratnik, 17
najveći zajednički djelitelj, 8
- Osnovni teorem aritmetike, 16
- Pellova jednađba, 90
pelovska jednađba, 90
periodski razvoj, 89
Pitagorin trokut, 84
Pitagorina trojka, 84
pomak alfabeta, 55
potpun kvadrat, 5
potpun sustav ostataka, 34
prijateljski brojevi, 25
primitivni korijen, 50

- prosti broj, 15
- prošireni Euklidov algoritam, 13
- pseudoporosti broj, 46

- red elementa, 48
- reducirani sustav ostataka, 43
- relativno prosti cijeli brojevi, 8
- RSA kriptosustav, 57

- savršen broj, 25
- složen broj, 15

- Teorem o dijeljenju s ostatkom, 4

- u parovima relativno prosti cijeli brojevi, 8

- verižni razlomak, 89
- višekratnik, 1

- Wilsonov teorem, 52

- zajednički djelitelj, 8
- zajednički višekratnik, 17
- zbroj svih pozitivnih djelitelja, 22

