Primjena kongruencija

Paripović, Suzana

Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike i računarstva

Suzana Paripović

Primjena kongruencija

Diplomski rad

Osijek, 2018.

Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike i računarstva

Suzana Paripović

Primjena kongruencija

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Ivan Matić

Osijek, 2018.

Sadržaj

Uvod **iii**

I Kongruencije **1**

1.1 Definicija i osnovna svojstva kongruencija 1

1.2 Linearne kongruencije 9

II Ispitivanje djeljivosti **13**

2.1 Djeljivost s 2^j 13

2.2 Djeljivost s 5^j 14

2.3 Djeljivost s 10 14

2.4 Djeljivost s 3 i 9 15

2.5 Djeljivost s 11 15

2.6 Djeljivost s 7, 11 i 13 16

2.7 Djeljivost s 37 18

2.8 Metoda izbacivanja devetki 19

2.9 Digitalni korijen 21

2.10 Metoda izbacivanja dvojki 24

III Sheme kodiranja i kontrolne znamenke **25**

3.1 Binarni kodovi 25

3.2 Kontrolne znamenke u identifikacijskim brojevima 26

3.3 Poštanski brojevi 30

3.4 ISBN i ISSN 33
3.5 EAN-13 barkod 34
3.6 Broj vozačke dozvole 36
3.7 Sheme s dvije kontrolne znamenke 38
3.8 Identifikacijski broj vozila 39

IV Modularni dizajni **42**

4.1 Zvijezda s m krakova 42
4.2 (m, n) dizajni ostatka 43
4.3 Quilt dizajni 45

V Problem p-kraljica **48**

VI Raspored turnira **52**

Bibliografija **57**

Sažetak **58**

Title and summary **59**

Životopis **60**

Uvod

Uz pojam djeljivosti, koji je jedan od osnovnih pojmova u teoriji brojeva, direktno je vezan i pojam kongruencija, koji je uveo i razvio njemački matematičar Carl Friedrich Gauss (1777.-1855.). Gauss je, uz Archimeda i Isaac Newtona, jedan od najvećih matematičara svih vremena. Dobio je nadimak "princ matematike" zbog svog velikog doprinosa razvoju matematike. Osim matematici, dao je značajan doprinos fizici, astronomiji, geometriji, geodeziji, optici, ali u njegovo vrijeme vjerojatno je bio najpoznatiji kao astronom. Gauss je bio mnogo godina ravnatelj opservatorija u Göttingenu. Teorija brojeva, za koju je znao govoriti da je *"kraljica matematike"*, je bila jedna od njegovih velikih strasti. Gauss je tretirao teoriju brojeva kao granu matematike, a ne samo kao zbirku zanimljivih problema.

Gauss je predstavio teoriju kongruencija na prvoj stranici njegovog izvanrednog rada *Disquisitiones Arithmeticae* koji sadržava bogatstvo novih pojmova i teorema i kojim je postavio temelje moderne teorije brojeva. Disquisitiones Arithmeticae je završen kada je Gauss imao samo 21 godinu, a objavljen je tri godine kasnije 1801. godine. To je bio jedan od posljednjih matematičkih tekstova koji su pisani na latinskom jeziku. Logička struktura ove knjige postavila je standard koji je uslijedio u mnogim kasnijim tekstovima. Gaussova knjiga je počela s definicijom kongruencije i modula: *ako broj m dijeli razliku $a - b$, onda je a kongruentan b modulo m.* Ova naizgled jednostavna definicija naglašava veliko otkriće: u modernoj terminologiji, kongruencija je relacija ekvalencije. Također, on je izabrao izuzetno dobar način zapisa kongruencije koji koristimo i danas. Relacija kongruencije ima mnoga zajednička svojstva s relacijom jednakosti, tako da nije slučajno da znak kongruencije "$\equiv$" podsjeća na znak jednakosti "$=$". Znak kongruencije olakšava proučavanje teorije djeljivosti i ima mnogo fascinantnih primjena.

Teorija kongruencija, koju ćemo predstaviti u prvom dijelu rada, izmjenjuje način pogleda na probleme koji se odnose na djeljivost te ima mnoge primjene u teoriji brojeva, ali nalazi široku primjenu i izvan teorije brojeva. Primjene, kojima ćemo se baviti u ovom radu, uključuju standardna ispitivanja djeljivosti, metode za provjeru rezultata računskih operacija, određivanje kontrolnih znamenki u identifikacijskim brojevima kojima je svrha otkrivanje pogrešaka koje se događaju tijekom prijenosa tih brojeva putem interneta, telefona ili čak preko pošte. Osim toga, vidjeti ćemo kako se teorija kongruencija može primjeniti u stvaranju zanimljivih dizajna koji su često inspiracija umjetnicama za njihove umjetničke radove. Na kraju ćemo se baviti primjenom kongruencija na rješavanje interesantnih problema poput problema p-kraljica i konstruiranje rasporeda susreta u turnirima.

Poglavlje I

Kongruencije

U ovom poglavlju upoznati ćemo se s definicijom i uvesti neka osnovna svojstva kongruencija. Osim toga, osvrniti ćemo se na linearne kongruencije i njihovo rješavanje.

1.1 Definicija i osnovna svojstva kongruencija

Za početak uvesti ćemo definiciju kongruencije.

Definicija 1.1. *Neka je m pozitivan cijeli broj i neka su a i b cijeli brojevi. Kažemo da a je **kongruentan** s b **modulo** m ako $m|(a-b)$. Pišemo $a \equiv b \pmod{m}$. Ako $m \nmid (a-b)$, kažemo da a **nije kongruentan** s b modulo m. Tada pišemo $a \not\equiv b \pmod{m}$.*

Sljedeći primjer ilustrira ovu definiciju.

Primjer 1.1.
Budući da $3|(16-4)$*, iz definicije 1.1 slijedi* $16 \equiv 4 \pmod{3}$*. Također vrijedi* $23 \equiv -2 \pmod{5}$*. Ali* $30 \not\equiv 5 \pmod{6}$*, jer* 6 *ne dijeli razliku* $30-5$*.*

Tijekom proučavanja kongruencija u ovom radu, pretpostaviti ćemo da slova označavaju cijele brojeve i svi moduli su pozitivni cijeli brojevi budući da razlika $a-b$ je djeljiva s m ako i samo ako je djeljiva s $-m$. Dakle, bez smanjenja općenitosti možemo promatrati pozitivne module.

U radu s kongruencijama je često korisno zapisati ih pomoću jednakosti. To nam omogućuje sljedeći teorem.

Teorem 1.1. *$a \equiv b \pmod{m}$ ako i samo ako je $a = b + km$ za neki cijeli broj k.*

Dokaz.
Pretpostavimo da $a \equiv b \pmod{m}$. Tada, prema definiciji 1.1, vrijedi da m dijeli razliku $a-b$. To znači da postoji cijeli broj k za kojeg je $a-b=km$, odnosno $a=b+km$.
Obratno, pretpostavimo da je $a = b+km$ za neki cijeli broj k. Tada je $a-b=km$, odnosno $m|(a-b)$. Stoga, $a \equiv b \pmod{m}$. □

Primjer 1.2.
Imamo, $29 \equiv 1 \pmod{7}$ *i* $29 = 1 + 7 \cdot 4$*. S druge strane, imamo* $64 = -8 + 9 \cdot 8$*. Prema tome,* $64 \equiv -8 \pmod{9}$*.*

Napomena 1.1. *Iz definicije 1.1, ali također i iz prethodnog teorema 1.1 slijedi da* $a \equiv 0 \pmod{m}$ *ako i samo ako* $m|a$. *Odnosno, cijeli broj je kongruentan s* 0 *ako i samo ako je djeljiv s* m. *Na primjer,* $25 \equiv 0 \pmod{5}$ *i* $5|25$.

Sljedeći teorem predstavlja tri dodatna svojstva kongruencija.

Teorem 1.2. *"Biti kongruentan" modulo* m *je relacija ekvivalencije na skupu cijelih brojeva i vrijede sljedeća svojstva:*

(a) $a \equiv a \pmod{m}$. *(**Svojstvo refleksivnosti**)*

(b) Ako $a \equiv b \pmod{m}$, *tada* $b \equiv a \pmod{m}$. *(**Svojstvo simetričnosti**)*

(c) Ako $a \equiv b \pmod{m}$ *i* $b \equiv c \pmod{m}$, *tada* $a \equiv c \pmod{m}$. *(**Svojstvo tranzitivnosti**)*

Dokaz.

(a) Budući da $m|(a-a) = 0$, vidimo da je $a \equiv a \pmod{m}$.

(b) Ako je $a \equiv b \pmod{m}$, tada prema definiciji 1.1 $m|(a-b)$. Stoga, prema teoremu 1.1 postoji cijeli broj k za kojeg je $km = a - b$. To pokazuje da je $(-k)m = b - a$, odnosno $m|(b-a)$. Iz toga slijedi da je $b \equiv a \pmod{m}$.

(c) Ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, tada prema definiciji 1.1 $m|(a-b)$ i $m|(b-c)$. Stoga, prema teoremu 1.1 postoje cijeli brojevi k i l takvi da vrijedi $km = a - b$ i $lm = b - c$. Prema tome, $a - c = (a-b) + (b-c) = km + lm = (k+l)m$. Iz toga slijedi da $m|(a-c)$ i $a \equiv c \pmod{m}$.

□

Primjer 1.3.

(a) $5 \equiv 5 \pmod{7}$

(b) Budući da $18 \equiv 4 \pmod{7}$, $4 \equiv 18 \pmod{7}$

(c) Budući da $25 \equiv 5 \pmod{5}$ *i* $5 \equiv -10 \pmod{5}$. *Tada* $25 \equiv -10 \pmod{5}$

Sada ćemo se prisjetiti najznačajnijeg teorema teorije djeljivosti koji će nam biti potreban za rezultate koje ćemo proučavati u nastavku rada.

Teorem 1.3. *(**Teorem o dijeljenju s ostatkom**) Neka je* a *cijeli broj i* b *pozitivan cijeli broj. Tada postoje jedinstveni cijeli brojevi* q *i* r *takvi da je* $a = b \cdot q + r$, *gdje je* $0 \leq r < b$.

Sljedeći teorem također karakterizira kongruencije.

Teorem 1.4. $a \equiv b \pmod{m}$ *ako i samo ako* a *i* b *daju isti ostatak pri djeljenju s* m.

Dokaz.
Pretpostavio da $a \equiv b \pmod{m}$. Tada, prema teoremu 1.1 postoji cijeli broj k takav da je $a = b + km$. Prema teoremu o djeljenju s ostatkom 1.3, $b = mq + r$, gdje je $0 \leq r < m$. Tada $a = b + km = (mq + r) + km = m(q + k) + r$. Stoga, prema teoremu o djeljenju s ostatkom, a ostavlja isti ostatak r pri djeljenju s m.

Obratno, pretpostavimo da i a i b daju isti ostatak r pri djeljenju s m. Sada, ponovno prema teoremu o djeljenju s ostatkom 1.3 je $a = mq + r$ i $b = mq' + r$, gdje je $0 \leq r < m$. Tada, $a - b = (mq + r) - (mq' + r) = m(q - q')$. Stoga, $a \equiv b \pmod{m}$. □

Na primjer, imamo $14 \equiv 20 \pmod{3}$. Vidimo da i 14 i 20, pri djeljenju s 3, daju ostatak 2. S druge strane, kada 24 i -1 djelimo s 5, ostatak je isti, odnosno 4. Dakle, $24 \equiv -1 \pmod{5}$.

Sljedeći korolar slijedi iz prethodnog teorema 1.4.

Korolar 1.4.1. *Cijeli broj r je ostatak pri djeljenju a sa m ako i samo ako $a \equiv r \pmod{m}$, gdje je $0 \leq r < m$.*

Prema ovom korolaru, svaki cijeli broj a je kongruentan njegovom ostatku r modulo m. Ostatak r se naziva **najmanji pozitivni ostatak** od a modulo m. Radi jednostavnosti, u nastavku rada koristiti ćemo termin najmanji ostatak.

Na primjer, najmanji ostaci od 37, 15 i -3 modulo 7 su 2, 1 i 4, redom.
Budući da r ima točno m izbora $0, 1, 2, 3, .., (m - 1)$, a je kongruentan s točno jednim od njih, modulo m.

Prema tome, imamo sljedeći rezultat.

Korolar 1.4.2. *Svaki cijeli broj je kongruentan s točno jednim najmanjim ostatkom $0, 1, 2, 3, .., (m - 1)$ modulo m.*

Sljedeći primjer koristi taj rezultat.

Primjer 1.4.
Prost broj oblika $4n + 3$ ne može se prikazati kao zbroj kvadrata dva cijela broja.

Dokaz.
Neka je x prost broj oblika $4n + 3$, odnosno $x = 4n + 3$. Prema teoremu 1.1 to možemo zapisati pomoću kongruencije $x \equiv 3 \pmod{4}$.
Pretpostavimo suprotno, odnosno x se može prikazati kao zbroj kvadrata dva cijela broja. Tada, $x = a^2 + b^2$ za neke cijele brojeve a i b. Budući da je x neparan, jedan od kvadrata cijelih brojeva , recimo a^2, mora biti neparan. Stoga, b^2 mora biti paran. Tada, a mora biti neparan i b paran. Neka je $a = 2q + 1$ i $b = 2r$ za neke cijele brojeve q i r. Imamo,

$$\begin{aligned} x &= (2q + 1)^2 + (2r)^2 \\ &= 4(q^2 + r^2 + q) + 1 \\ &\equiv 1 \pmod{4}, \end{aligned}$$

što je u kontadikciji s pretpostavkom da je $x \equiv 3 \pmod{4}$. Dakle, prost broj oblika $4n+3$ ne može se prikazati kao zbroj kvadrata dva cijela broja.

□

Korištenjem najmanjih ostataka, skup cijelih brojeva $\mathbb{Z}$ može se podjeliti na m nepraznih, u parovima disjunktnih klasa, koje se nazivaju **klase kongruencija modulo** m. Radi pojašnjenja, neka $[r]$ označava skup cijelih brojeva koji sadrži r kao njegov najmanji ostatak modulo m. Na primjer, različite klase modulo 6 su

$$\begin{aligned}
[0] &= \{..., -12, -6, 0, 6, 12, ...\} \\
[1] &= \{..., -11, -5, 1, 7, 13, ...\} \\
[2] &= \{..., -10, -4, 2, 8, 14, ...\} \\
[3] &= \{..., -9, -3, 3, 9, 15, ...\} \\
[4] &= \{..., -8, -2, 4, 10, 16, ...\} \\
[5] &= \{..., -7, -1, 5, 11, 17, ...\}.
\end{aligned}$$

Očito, ove su klase neprazne, u parovima disjunktne, a njihova unija je skup cijelih brojeva. Najmanji ostaci $0, 1, 2, 3, 4$ i 5 služe kao predstavnici klasa $[0], [1], [2], [3], [4]$ i $[5]$, redom.

Općenito, ne trebamo odabrati najmanje ostatke za predstavnike klasa kongruencija. Prema teoremu 1.4, dva cijela broja pripadaju istoj klasi ako i samo ako su oni daju isti ostatak pri dijeljenju s m. Dakle, bilo koji element klase $[r]$ može poslužiti kao važeći predstavnik.

Na primjer, $12, 7, -4, -3, 10$ i -1 mogu poslužiti kao predstavnici klasa $[0], [1], [2], [3], [4]$ i $[5]$, redom. Takav skup cijelih brojeva je potpuni sustav ostataka modulo 6.

Definicija 1.2. *Skup od m cijelih brojeva je **potpuni sustav ostataka modulo** m ako svaki cijeli broj je kongruentan modulo m s točno jednim od njih.*

Dakle, skup cijelih brojeva $\{a_1, a_2, .., a_m\}$ je potpuni sustav ostataka modulo m, ako su oni kongruenti modulo m s najmanjim ostacima $0, 1, 2, .., (m-1)$ u nekom poretku.

Na primjer, skup $\{-15, 11, 7, 23, 9\}$ je potpuni sutav ostataka modulo 5 budući da je $-15 \equiv 0 \pmod 5$, $11 \equiv 1 \pmod 5$, $7 \equiv 2 \pmod 5$, $23 \equiv 3 \pmod 5$, $9 \equiv 4 \pmod 5$.

Sljedeći teorem pokazuje da se dvije kongruencije s istim modulom mogu zbrojiti i množiti, isto kao i kod jednakosti.

Teorem 1.5. *Neka je $a \equiv b \pmod m$ i $c \equiv d \pmod m$. Tada*

(a) $a + c \equiv b + d \pmod m$

(b) $ac \equiv bd \pmod m$

Dokaz.
Imamo $a \equiv b \pmod m$ i $c \equiv d \pmod m$, prema teoremu 1.1 vrijedi da je $a = b + lm$ i $c = d + km$ za neke cijele brojeve l i m. Tada

(a)

$$\begin{aligned}
a + c &= (b + lm) + (d + km) \\
&= (b + d) + (l + k)m \\
&\equiv b + d \pmod m.
\end{aligned}$$

(b)

$$\begin{aligned} ac - bd &= (ac - bc) + (bc - bd) \\ &= c(a - b) + b(c - d) \\ &= clm + bkm \\ &= (cl + bk)m. \end{aligned}$$

Dakle, $ac \equiv bd \pmod{m}$.

□

Primjer 1.5.
Vrijedi $13 \equiv 3 \pmod{5}$ *i* $21 \equiv -4 \pmod{5}$.

Prema prethodnom teoremu 1.5 $13 + 21 \equiv 3 + (-4) \pmod{5}$, *odnosno* $34 \equiv -1 \pmod{5}$.
Također, $13 \cdot 21 \equiv 3 \cdot (-4) \pmod{5}$, *odnosno* $273 \equiv -12 \pmod{5}$.
Dakle, dvije kongruencije se mogu zbrojiti i množiti pod uvjetom da imaju isti modul.

Sljedeći primjer je interesantna primjena korolara 1.4.1 i teorema 1.5.

Primjer 1.6.
Potrebno je pronaći ostatak pri djeljenju $1! + 2! + 3! + ... + 10!$ *s* 5.

Primijetimo da za $k \geq 5$, $k! \equiv 0 \pmod{5}$. *Stoga,*

$$\begin{aligned} 1! + 2! + 3! + ... + 10! &\equiv 1! + 2! + 3! + 4! + 0 + ... + 0 \pmod{5} \\ &\equiv 1 + 2 + 6 + 24 \pmod{5} \\ &\equiv 1 + 2 + 0 \pmod{5} \\ &\equiv 3 \pmod{5}. \end{aligned}$$

Dakle, kada danu sumu podijelimo s 5, *ostatak je* 3.

Teorem 1.5 povlači da se jedna kongruencija može oduzeti od druge, pod uvjetom da imaju isti modul, kao što stoji u slijedećem korolaru.

Korolar 1.5.1. *Ako* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *tada* $a - c \equiv b - d \pmod{m}$.

Primjer 1.7.
Vrijedi $13 \equiv 3 \pmod{5}$ *i* $21 \equiv -4 \pmod{5}$.

Tada, prema prethodnom korolaru 1.5.1, $13 - 21 \equiv 3 - (-4) \pmod{5}$.
Odnosno $-8 \equiv 7 \pmod{5}$.

Sljedeći korolar je također direktna posljedica teorema 1.5.

Korolar 1.5.2. *Ako* $a \equiv b \pmod{m}$ *i* c *je bilo koji cijeli broj, tada*

(a) $a + c \equiv b + c \pmod{m}$

(b) $a - c \equiv b - c \pmod{m}$

(c) $ac \equiv bc \pmod{m}$

(d) $a^2 \equiv b^2 \pmod{m}$.

Primjer 1.8.
Vrijedi $15 \equiv -5 \pmod{5}$. *Iz prethodnog korolara 1.5.2 slijedi da je*

(a) $24 = 15 + 9 \equiv -5 + 9 = 4 \pmod{5}$

(b) $6 = 15 - 9 \equiv -5 - 9 = -14 \pmod{5}$

(c) $135 = 15 \cdot 9 \equiv -5 \cdot 9 = -45 \pmod{5}$.

Dio (d) prethodnog korolara 1.5.2 može se generalizirati kao što se slijedi.

Teorem 1.6. *Ako* $a \equiv b \pmod{m}$, *tada* $a^n \equiv b^n \pmod{m}$ *za bilo koji pozitivni cijeli broj* n.

Dokaz.
Tvrdnja je očito istinita za $n = 1$. Pretpostavimo da je tvrdnja istinita za pozitivan cijeli broj k: $a^k \equiv b^k \pmod{m}$. Zatim, pomoću teorema 1.5, $a \cdot a^k \equiv b \cdot b^k \pmod{m}$, odnosno $a^{k+1} \equiv b^{k+1} \pmod{m}$. Dakle, rezultat slijedi po indukciji.

□

Teoremi 1.5 i 1.6 mogu se učinkovito iskoristiti za računanje ostatka pri djeljenju cijelog broja b^n sa m, kao što to sljedeći primjer pokazuje.

Primjer 1.9.
Pronađimo ostatak pri djeljenju 17^{67} *s* 5.

Prvo, znamo da je $17 \equiv 2 \pmod{5}$. *Zatim, prema teoremu 1.6,* $17^{67} \equiv 2^{67} \pmod{5}$. *Također, lako se vidi da* $2^4 \equiv 1 \pmod{5}$. *Primjenom teorema o djeljenju s ostatkom 1.3 s* 4 *kao djeliteljem imamo:*

$$\begin{aligned} 2^{67} &= 2^{4 \cdot 16 + 3} = (2^4)^{16} \cdot 2^3 \\ &\equiv 1^{16} \cdot 2^3 \pmod{5} \\ &\equiv 8 \pmod{5} \\ &\equiv 3 \pmod{5}. \end{aligned}$$

Imamo, $17^{67} \equiv 2^{67} \pmod{5}$ *i* $2^{67} \equiv 3 \pmod{5}$. *Tada, iz svojstva tranzitivnosti (teorem 1.2) slijedi da je* $17^{67} \equiv 3 \pmod{5}$. *Dakle,* 3 *je ostatak pri djeljenju* 17^{67} *s* 5.

Možemo primijetiti veliku snagu kongruencija u pronalaženju ostatka brzo i lako pri djeljenju velikog broja b^n sa m.

Modularno eksponenciranje je još jedna od metoda za određivanje ostatka pri djeljenju b^n s m. Prvo, izrazimo eksponent n u binarnom zapisu: $n = (n_k n_{k-1} ... n_1 n_0)_2$. Zatim, nađemo najmanji pozitivan ostatak od $b, b^2, b^4, ..., b^{2^k}$ modulo m uzastopnim kvadriranjem i uzimanjem ostataka modulo m. Konačno, pomnožimo najmanje pozitivne ostatke modulo m od b^{2^j}, za one j za koje $a_j = 1$, uzimanjem ostataka modulo m nakon svakog množenja.

Sljedeći primjer ilustrira ovu metodu.

Primjer 1.10.
Potrebno je riješiti primjer 1.9 pomoću metode modularnog eksponenciranja.
Najprije ćemo izraziti eksponent 67 *u binarnom zapisu:*

$$(67)_{10} = (1000011)_2.$$

Zatim, računamo najmanje pozitivne ostatke od $17, 17^2, 17^4, ..., 17^{2^6} = 17^{64}$ *uzastopnim kvadriranjem i uzimanjem ostataka modulo* 5. *Primijetimo da je* 64 *najveća potencija od* 2 *sadržana u* 67. *To nam daje kongruencije*

$$\begin{aligned} 17 &\equiv 2 \pmod 5, \\ 17^2 &\equiv 4 \pmod 5, \\ 17^4 &\equiv 1 \pmod 5, \\ 17^8 &\equiv 1 \pmod 5, \\ 17^{16} &\equiv 1 \pmod 5, \\ 17^{32} &\equiv 1 \pmod 5, \\ 17^{64} &\equiv 1 \pmod 5. \end{aligned}$$

Sada možemo izračunati 17^{67} *modulo* 5 *množenjem najmanjih ostataka modulo* 5 *od* $17, 17^2$ *i* 17^{64} *jer u binarnom zapisu od* 67 *su* $n_0 = 1$, $n_1 = 1$ *i* $n_6 = 1$. *To nam daje*

$$17^{67} = 17^{64+2+1} = 17^{64} \cdot 17^2 \cdot 17 \equiv 1 \cdot 4 \cdot 2 = 8 \equiv 3 \pmod 5.$$

Primijetimo da je rezultat isti kao i u prethodnom primjeru, odnosno 3 *je ostatak pri djeljenju* 17^{67} *s* 5.

Za razliku od prethodnog primjera, često su moduli nešto veći brojevi pa samim time i najmanji ostaci su veći. U takvim problemima se količina posla može znatno smanjiti ako uvedemo negativne ostatke.

Metoda pronalaženja ostataka pomoću kongruencija može se proširiti na izraze s eksponentima koji su *toranj potencija modulo* m, kao što to sljedeći primjer pokazuje.

Primjer 1.11.
Potrebno je pronaći zadnju znamenku u decimalnoj vrijednosti broja $1077^{1177^{1277^{1377}}}$.

Neka N označava dani broj. Zadnja znamenka u N jednaka je najmanjem ostatku od N modulo 10. S obzirom da je $1077 \equiv 7 \pmod{10}$, promotriti ćemo različite potencije od 7: $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$, $7^5 \equiv 7 \pmod{10}$ i uočavamo uzorak:

$$7^a \equiv \begin{cases} 1 \pmod{10}, & ako \ \ a \equiv 0 \pmod{4} \\ 7 \pmod{10}, & ako \ \ a \equiv 1 \pmod{4} \\ 9 \pmod{10}, & ako \ \ a \equiv 2 \pmod{4} \\ 3 \pmod{10}, & ako \ \ a \equiv 3 \pmod{4} \end{cases}$$

Sada promotrimo 1177.
Vidmo da je $1177 \equiv 1 \pmod{4}$ pa iz teorema 1.7 slijedi da je $1177^n \equiv 1 \pmod{4}$, $\forall\, n \geq 1$.
S obzirom da je $1277^{1377} > 1$, onda je $1177^{1277^{1377}} \equiv 1 \pmod{4}$.
Prema tome, $N \equiv 7 \pmod{10}$. Drugim riječima, zadnja znamenka u decimalnoj vrijednosti od N je 7.

Sada ćemo iskazati još neka dodatna svojstva kongruencija.
Što bi se dogodilo kada bi obje strane kongruencije podijelili s istim cijelim brojem? Primijetimo da $28 = 7 \cdot 4 \equiv 3 \cdot 4 = 12 \pmod{8}$, ali $7 \not\equiv 3 \pmod{8}$. To nam pokazuje da nije nužno točno da dijeljenjem s obje strane kongruencije istim brojem ćemo očuvati kongruenciju.
Međutim, sljedeći teorem nam daje valjanu kongruenciju kada obje strane kongruencije dijelimo s isim cijelim brojem.

Teorem 1.7. *Ako $ac \equiv bc \pmod{m}$ i $(c, m) = 1$, tada $a \equiv b \pmod{m}$.*

Dakle, možemo ukloniti isti broj c s obje strane kongruencije, pod uvjetom da su c i m relativno prosti, kao što pokazuje slijedeći primjer.

Primjer 1.12.
Primijetimo da $54 \equiv 12 \pmod{7}$. To je, $9 \cdot 6 \equiv 2 \cdot 6 \pmod{7}$. Budući da $(6, 7) = 1$, možemo ukloniti 6 s obje strane:

$$9 \cdot \not{6} \equiv 2 \cdot \not{6} \pmod{7}$$

Prema tome,

$$9 \equiv 2 \pmod{7}.$$

Prethodni teorem 1.7 je zapravo specijalni slučaj sljedećeg teorema te ga možemo generalizirati kao što slijedi.

Teorem 1.8. *Ako $ac \equiv bc \pmod{m}$ i $(c, m) = d$, tada $a \equiv b \pmod{m/d}$.*

Primjer 1.13.
Može se provjeriti da je $9 \cdot 4 \equiv 3 \cdot 4 \pmod 8$. *Budući da* $(4, 8) = 4$, *možemo ukloniti* 4 *s obje strane:*

$$9 \cdot \cancel{4} \equiv 3 \cdot \cancel{4} \pmod{8/4}$$

Prema tome,

$$9 \equiv 3 \pmod 2.$$

Sada ćemo vidjeti kako mogu biti kongruencije dva broja s različitim modulima kombinirane u jednu kongruenciju.

Teorem 1.9. *Ako* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$, *tada* $a \equiv b \pmod{[m_1, m_2, ..., m_k]}$, *gdje je* $[m_1, m_2, ..., m_k]$ *najmanji zajednički višekratnik od* $m_1, m_2, ..., m_k$.

Sljedeći primjer ilustrira ovaj rezultat.

Primjer 1.14.
Može se provjeriti da je $152 \equiv 32 \pmod{12}$, $152 \equiv 32 \pmod{10}$, *i* $152 \equiv 32 \pmod 4$. *Prema prethodnom teoremu 1.9,* $152 \equiv 32 \pmod{[12, 10, 4]}$, *odnosno* $152 \equiv 32 \pmod{60}$.

Direktna i korisna posljedica prethodnog teorema 1.9 je sljedeći rezultat.

Korolar 1.9.1. *Ako* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$, *gdje su moduli u parovima relativno prosti, tada* $a \equiv b \pmod{m_1 \cdot m_2 \cdot ... \cdot m_k}$.

1.2 Linearne kongruencije

U prethodnom dijelu smo proučavali neka osnovna svojstva kongruencija. Sada gledamo kongruencije koje sadrže varijable, kao što su $6x \equiv 4 \pmod 7$, $x^2 \equiv 1 \pmod 3$ i $x^2 + 3 \equiv 3x \pmod 7$. Najjednostavnija takva kongruencija je **linearna kongruencija** $ax \equiv b \pmod m$.

Rješenjem linearne kongruencije smatramo cijeli broj x_0 takav da je $ax_0 \equiv b \pmod m$.

Na primjer, $5 \cdot 5 \equiv 4 \pmod 7$, pa je 5 rješenje kongruencije $5x \equiv 4 \pmod 7$. No, kongruencija $10x \equiv 1 \pmod 5$ nema rješenja, budući da $5 \nmid (10x - 1)$ za bilo koji cijeli broj x.

Pretpostavimo da x_0 predstavlja rješenje kongruencije $ax \equiv b \pmod m$. Tada, $ax_0 \equiv b \pmod m$. Osim toga, pretpostavimo da je $x_1 \equiv x_0 \pmod m$. Zatim, prema korolaru 1.5.2 imamo da je $ax_1 \equiv ax_0 \pmod m$. Iz svojstva tranzitivnosti (teorem 1.2) slijedi da je $ax_1 \equiv b \pmod m$. Dakle, x_1 je također rješenje linearne kongruencije. Ali x_1 i x_0 pripadaju istoj klasi kongruencije. Prema tome, ako je x_0 rješenje linearne kongruencije, onda je svaki član njegove klase također rješenje.

Napomena 1.2. *Za dva rješenja x_0 i x_1 linearne kongruencije $ax \equiv b \pmod{m}$ kažemo da su ekvivalentna ako je $ax_0 \equiv ax_1 \pmod{m}$.*

Na primjer, budući da je 5 rješenje kongruencije $5x \equiv 4 \pmod{7}$, svaki član klase $[5] = \{..., -9, -2, 5, 12, 19, ...\}$ je također rješenje. Rješenja su dana s $x = 5 + 7t$:

$$\begin{aligned} 5(5 + 7t) &= 25 + 35t \\ &\equiv 4 + 0 \pmod{7} \\ &\equiv 4 \pmod{7}. \end{aligned}$$

Dakle, ako je kongruencija $ax \equiv b \pmod{m}$ rješiva, ona ima beskonačno mnogo rješenja. Zbog toga smo zainteresirani samo za njena međusobno neekvivalentna rješenja.

Na primjer, kongruencija $8x \equiv 4 \pmod{12}$ ima četiri međusobno neekvivalentna rješenja: $8 \cdot 2 \equiv 4 \pmod{12}$, $8 \cdot 5 \equiv 4 \pmod{12}$, $8 \cdot 8 \equiv 4 \pmod{12}$ i $8 \cdot 11 \equiv 4 \pmod{12}$. Dakle, rješenja su: $2, 5, 8$ i 11.

Sljedeći teorem daje nužan i dovoljan uvjet da bi linearna kongruencija imala rješenja. Ovaj teorem također daje broj međusobno neekvivalentih rješenja i formulu za njihovo pronalaženje kada je kongruencija rješiva.

Teorem 1.10. *Linearna kongruencija $ax \equiv b \pmod{m}$ ima rješenje ako i samo ako $d|b$, gdje je $d = (a, m)$. Ako $d|b$, tada kongruencija ima d međusobno neekvivalentih rješenja.*

Napomena 1.3. *$x = x_0 + (\frac{m}{d})t$, gdje je $0 \leq t < d$, je **općе rješenje** linearne kongruencije.*

Ovaj teorem ima koristan korolar.

Korolar 1.10.1. *Linearna kongruencija $ax \equiv b \pmod{m}$ ima jedinstveno rješenje ako i samo ako $(a, m) = 1$.*

Sljedeća dva primjera ilustriraju prethodne rezultate.

Primjer 1.15.
Potrebno je odrediti jesu li sljedeće kongruencije rješive:

(1) $6x \equiv 5 \pmod{7}$

(2) $5x \equiv 7 \pmod{10}$

(3) $9x \equiv 6 \pmod{12}$.

Također, potrebno je pronaći broj međusobno neekvivalentih rješenja kada je kongruencija rješiva.

(1) $(6, 7) = 1$. *Prema korolaru 1.10.1 kongruencija* $6x \equiv 5 \pmod{7}$ *ima jedinstveno rješenje modulo* 7.

(2) $(5, 10) = 2$, *ali* $2 \nmid 7$. *Prema tome, kongruencija* $5x \equiv 7 \pmod{10}$ *nema rješenja.*

(3) $(9, 12) = 3$ *i* $3|6$. *Prema tome, kongruencija* $9x \equiv 6 \pmod{12}$ *je rješiva i ima* 3 *međusobno neekvivalentna rješenja modulo* 12.

Sljedeći primjer pokazuje kako pronaći međusobno neekvivalentna rješenja linearne kongruencije.

Primjer 1.16.
Potrebno je riješiti kongruenciju $8x \equiv 56 \pmod{12}$.

Budući da $(8, 12) = 4$ *i* $4|56$ *kongruencija ima* 4 *međusobno neekvivalentna rješenja modulo* 12. *Ona su dana s* $x = x_0 + (\frac{m}{d})t = x_0 + (\frac{12}{4})t = x_0 + 3t$, *gdje je* $0 \leq t < 4$. *Metodom pokušaja i pogreške lako se vidi da je* $x_0 = 1$. *Dakle,* 4 *međusobno neekvivalentna rješenja modulo* 12 *su* $1 + 3t$, *gdje je* $0 \leq t < 4$, *odnosno,* $1, 4, 7$ *i* 10.

Primjenom teorema 1.8, ista kongruencija može se riješiti na nešto drugačiji način. Prvo, podijeliti ćemo kongruenciju s 4*:*

$$2x \equiv 14 \pmod{3}.$$

Sada ćemo pomnožiti obje strane za 2 *(da bismo dobili jedan* x *s lijeve strane kongruencije):*

$$\begin{aligned} 2(2x) &\equiv 2 \cdot 14 \pmod{3} \\ x &\equiv 1 \pmod{3}. \end{aligned}$$

Dakle, rješenja ove kongruencije su $x = 1 + 3t$. *Sada se nastavlja kao i prije i dobivamo sva željena rješenja.*

Razmotrimo sada poseban slučaj kada je $b = 1$ u korolaru 1.10.1. Linearna kongruencija $ax \equiv 1 \pmod{m}$ ima jedinstveno rješenje ako i samo ako $(a, m) = 1$. Drugim riječima, kada $(a, m) = 1$, postoji jedinstveni najmanji ostatak x takav da je $ax \equiv 1 \pmod{m}$. Tada za a se kaže da je **invertibilan**, a x se naziva **inverz** od a modulo m i označava sa a^{-1}: $aa^{-1} \equiv 1 \pmod{m}$. Ako $a^{-1} = a$, onda je a **samoinvertibilan**.

Primjer 1.17.
Budući da je $6 \cdot 11 \equiv 1 \pmod{13}$, 6 *je invertibilan i* 11 *je inverz od* 6 *modulo* 13. 12 *je vlastiti inverz modulo* 13, *budući da* $12 \cdot 12 \equiv 1 \pmod{13}$.

Inverzi su korisni u rješavanju linearnih kongruencija. Da bismo to vidjeli, vratiti ćemo se na $ax \equiv b \pmod{m}$, gdje je $(a, m) = 1$. Budući $(a, m) = 1$, a ima inverz a^{-1} modulo m. Množenjem obje strane kongruencije s a^{-1}, dobivamo

$$\begin{aligned} a^{-1}(ax) &\equiv a^{-1}b \pmod{m} \\ (a^{-1}a)x &\equiv a^{-1}b \pmod{m} \\ 1 \cdot x &\equiv a^{-1}b \pmod{m}. \end{aligned}$$

Zbog toga,

$$x \equiv a^{-1}b \pmod{m}.$$

Prema tome, imamo sljedeći rezultat.

Teorem 1.11. *Jedinstveno rješenje linearne kongruencije* $ax \equiv b \pmod{m}$*, gdje je* $(a, m) = 1$*, je najmanji ostatak od* $a^{-1}b \pmod{m}$*.*

Sljedeći primjer koristi prethodni teorem 1.11

Primjer 1.18.
Koristeći inverze potrebno je pronaći međusobno neekvivalenta rješenja sljedećih linearnih kongruencija.

(1) $5x \equiv 3 \pmod{6}$

(2) $19x \equiv 29 \pmod{16}$.

(1) Primijetimo da je $5 \cdot 5 \equiv 1 \pmod{6}$*, odnosno* $5^{-1} \equiv 5 \pmod{6}$*. Prema tome,*

$$\begin{aligned} 5(5x) &\equiv 5 \cdot 3 \pmod{6} \\ x &\equiv 15 \pmod{6} \\ &\equiv 3 \pmod{6}. \end{aligned}$$

Dakle, prema teoremu 1.11 3 *je jedinstveno rješenje linearne kongruencije* $5x \equiv 3 \pmod{6}$*, gdje je* $(5, 6) = 1$*.*

(2) Primijetimo da je $3^{-1} \equiv 11 \pmod{16}$*. Prema tome,*

$$\begin{aligned} 19x &\equiv 29 \pmod{16} \\ 3x &\equiv 13 \pmod{16} \\ 11(3x) &\equiv 11 \cdot 13 \pmod{16} \\ x &\equiv 143 \pmod{16} \\ x &\equiv 15 \pmod{16}. \end{aligned}$$

Dakle, prema teoremu 1.11 15 *je jedinstveno rješenje linearne kongruencije* $19x \equiv 29 \pmod{16}$*, gdje je* $(19, 16) = 1$*.*

Poglavlje II

Ispitivanje djeljivosti

Dobro su nam poznati određeni kriteriji djeljivosti. Na primjer, broj (zapisan u sustavu s bazom 10) je djeljiv s 10 ako i samo ako je njegova posljednja znamenka jednaka 0, a djeljiv sa 100 ako i samo ako su mu posljednje dvije znamenke 00, itd. Broj je djeljiv s 5 ako i samo ako njegova posljednja znamenka jednaka 0 ili 5, a djeljiv je s 25 ako i samo ako su mu posljednje dvije znamenke 00, 25, 50 ili 75. Možda manje poznata činjenica je da je broj djeljiv s 9 ako i samo mu je zbroj znamenki djeljiv s 9. Isto vrijedi ako zamijenimo 9 sa 3. Kako se dokazuju takve činjenice? Kako ih možemo generalizirati? Kao što ćemo vidjeti, teorija kongruencija je vrlo korisna za proučavanje takvih pitanja. Pomoću kongruencija, možemo razviti kriterije djeljivosti za ispitivanje je li dani cijeli broj n djeljiv s cijelim brojem m. Koristit ćemo zapis broja n u brojevnom sustavu s bazom 10. Neka $n = (a_k a_{k-1}...a_1 a_0)_{10}$. Tada je $n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$, gdje $0 \leq a_j \leq 9$, za $j = 0, 1, 2, ..., k$ raspis broja n po bazi 10. U ovom dijelu rada ispitati ćemo djeljivost cijelog broja n s brojevima $2^j, 5^j, 10, 3, 9, 11$ i 37. Također ćemo razviti kriterij s kojim možemo istodobno ispitati djeljivost nekog cijelog broja n s prostim brojevima $7, 11$ i 13.
Nakon toga upoznati ćemo se s metodama izbacivanja devetki i izbacivanja dvojki. Osim toga, osvrnit ćemo se i na pojam digitalnog korijena koji je usko povezan s metodom izbacivanja devetki.

2.1 Djeljivost s 2^j

Budući da je $10 \equiv 0 \pmod 2$, imamo da je $10^j \equiv 0 \pmod{2^j}$ za sve pozitivne cijele brojeve j. Stoga, prema teoremima 1.5 i 1.6 imamo da je

$$\begin{aligned} n &\equiv (a_0)_{10} \pmod 2 \\ n &\equiv (a_1 a_0)_{10} \pmod{2^2} \\ n &\equiv (a_2 a_1 a_0)_{10} \pmod{2^3} \\ &\vdots \\ n &\equiv (a_{j-1} a_{j-2}...a_2 a_1 a_0)_{10} \pmod{2^j}. \end{aligned}$$

Dakle, da bi se utvrdilo je li n djeljiv s 2, moramo ispitati je li njegova zadnja znamenka a_0 djeljiva s 2.

Slično, broj n je djeljiv s 4 ako i samo ako je broj formiran od zadnje dvije znamenke broja n, dvoznamenkasti broj a_1a_0, djeljiv s 4.
Također, broj n je djeljiv s 8 ako i samo ako je troznamenkasti broj $a_2a_1a_0$ djeljiv s 8.

Općenito, cijeli broj n je djeljiv s 2^j ako i samo ako je broj formiran od zadnjih j znamenki broja n djeljiv s 2^j.

Primjer 2.1.
Neka je $n = 75623576$. *Vidimo da* $2|n$ *budući da* $2|6$ *i* $4|n$ *budući da* $4|76$. *Također,* $8|n$ *budući da* $8|576$. *Ali,* $16 \nmid n$ *budući da* $16 \nmid 3576$.

2.2 Djeljivost s 5^j

Budući da je $10 \equiv 0 \pmod 5$, imamo da je $10^j \equiv 0 \pmod{5^j}$ za sve pozitivne cijele brojeve j. Stoga, ispitivanje djeljivosti za brojeve koji su potencija broja 5 je analogno kao za brojeve koji su potencija broja 2.
Zbog

$$\begin{aligned} n &\equiv a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0 \\ &\equiv a_0 \pmod 5), \end{aligned}$$

n je djeljiv s 5 ako i samo ako je a_0 djeljiv s 5. Kako su 0 i 5 jedini jednoznamenkasti brojevi djeljivi s 5, broj je djeljiv s 5 ako i samo ako završava na 0 ili 5.
Slično, broj n je djeljiv s 25 ako i samo ako je broj formiran od zadnje dvije znamenke broja n, dvoznamenkasti broj a_1a_0, djeljiv s 25.
Dakle, broj je djeljiv s 25 ako i samo ako završava na 00, 25, 50 ili 75.

Općenito, cijeli broj n je djeljiv s 5^j ako i samo ako je broj formiran od zadnjih j znamenki broja n djeljiv s 5^j.

Primjer 2.2.
Neka je $n = 125875$. *Budući da* $5|5$, $5|n$. $25|n$ *jer* $25|75$ *i* $125|n$ *budući da* $125|875$. *Ali,* $625 \nmid n$ *budući da* $625 \nmid 5875$.

2.3 Djeljivost s 10

Budući da je $10 \equiv 0 \pmod{10}$, prema teoremu 1.6 imamo da je $10^k \equiv 0 \pmod{10}$. Zatim, iz teorema 1.5 slijedi da je

$$\begin{aligned} n &\equiv a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0 \pmod{10} \\ &\equiv a_0 \pmod{10}. \end{aligned}$$

Dakle, cijeli broj n je djeljiv s 10 ako i samo ako je a_0 je djeljiv s 10, odnosno ako i samo ako je njegova posljednja znamenka $a_0 = 0$.

2.4 Djeljivost s 3 i 9

Primijetimo da vrijedi da je $10 \equiv 1 \pmod 3$ i $10 \equiv 1 \pmod 9$. Stoga, prema teoremu 1.6 slijedi da je $10^k \equiv 1 \pmod 3$ i $10^k \equiv 1 \pmod 9$.
Prema teoremu 1.5 imamo da je

$$\begin{aligned} n = (a_k a_{k-1} ... a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 \\ &\equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 3 \ i \pmod 9. \end{aligned}$$

Prema tome, cijeli broj n je djeljiv s 3 ili s 9 ako i samo ako je zbroj njegovih znamenki djeljiv s 3 ili s 9.

Primjer 2.3.
Neka je $n = 1129764$. *Zbroj znamenaka broja* n *je* $1+1+2+9+7+6+4 = 30$. *Budući da* $3|30$, $3|n$. *Ali,* $9 \nmid n$ *jer* $9 \nmid 30$.

2.5 Djeljivost s 11

Primijetimo da je $10 \equiv -1 \pmod{11}$. Tada, prema teoremu 1.6 slijedi da je $10^k \equiv (-1)^k \pmod{11}$.
Zatim, opet prema teoremu 1.6 imamo da je

$$\begin{aligned} n = (a_k a_{k-1} ... a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0 \\ &\equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + ... + a_2 (-1)^2 + a_1 (-1)^1 + a_0 (-1)^0 \pmod{11} \\ &\equiv a_k (-1)^k + ... + a_2 - a_1 + a_0 \pmod{11}. \end{aligned}$$

To povlači da je cijeli broj n djeljiv brojem 11 ako i samo ako je alternirajuća suma njegovih znamenki $a_k(-1)^k + ... + a_2 - a_1 + a_0$ djeljiva s 11.

Primjer 2.4.
Neka je $n = 575698122$. *Vidimo da je* n *djeljiv s* 11, *budući da naizmjenično zbrajanje i oduzimanje njegovih znamenaka daje* $5+7-5+6-9+8-1+2-2 = 11$, *što je djeljivo s* 11. *S druge strane, broj* $m = 33221100$ *nije djeljiv s* 11 *jer* $3+3-2+2-1+1-0+0 = 6$ *nije djeljivo s* 11.

Sljedeći teorem identificira klasu cijelih brojeva koji su djeljivi s 11.

Teorem 2.1. *Palindrom s parnim brojem znamenki je djeljiv s* 11.

Dokaz.
Neka je $n = (a_{2k-1} a_{2k-2} ... a_1 a_0)_{10}$ palindrom s parnim brojem znamenki.

Budući da je $10^k \equiv (-1)^k \pmod{11}$, prema teoremu 1.6 slijedi da je

$$\begin{aligned} n &= (a_{2k-1}a_{2k-2}...a_3a_2a_1a_0)_{10} \\ &= a_{2k-1}10^{2k-1} + a_{2k-2}10^{2k-2} + ... + a_3 10^3 + a_2 10^2 + a_1 10^1 + a_0 10^0 \\ &\equiv -a_{2k-1} + a_{2k-2} - ... - a_3 + a_2 - a_1 + a_0 \pmod{11} \\ &\equiv 0 \pmod{11} \end{aligned}$$

jer je n palindrom s parnim brojem znamenki. Dakle, $11|n$.

□

Primjer 2.5.
Neka su $n = 2442$ i $m = 98700789$ palindromi s parnim brojem znamenki. Prema prethodnom teoremu 2.1 slijedi da su i n i m djeljivi s 11, što se lako može provjeriti.

Napomena 2.1. *Teorem 2.1 se ne može primjeniti na palindrome s neparnim brojem znamenki.*
Na primjer, broj 62126 je palindrom koji sadrži neparan broj znamenki. Međutim, taj palindrom nije djeljiv s 11.

2.6 Djeljivost s 7, 11 i 13

Najprije pogledajmo jedan primjer.

Primjer 2.6.
Potrebno je pokazati da je svaki šesteroznamenkasti broj oblika abcabc djeljiv s $7, 11$ i 13.

Označimo s N dani broj abcabc. Dakle, $N = (abcabc)_{10}$.
Budući da je $7 \cdot 11 \cdot 13 = 1001$ i $10^3 = 1000 \equiv -1 \pmod{1001}$ imamo da je

$$\begin{aligned} N = (abcabc)_{10} &= a \cdot 10^5 + b \cdot 10^4 + c \cdot 10^3 + a \cdot 10^2 + b \cdot 10 + c \\ &= 10^3(a \cdot 10^2 + b \cdot 10 + c) + (a \cdot 10^2 + b \cdot 10 + c) \\ &\equiv (-1)(a \cdot 10^2 + b \cdot 10 + c) + (a \cdot 10^2 + b \cdot 10 + c) \pmod{7 \cdot 11 \cdot 13} \\ &\equiv 0 \pmod{7 \cdot 11 \cdot 13} \end{aligned}$$

Dakle, dani broj N je djeljiv s $7, 11$ i 13.

Sada ćemo razviti kriterij s kojim možemo istodobno ispitati djeljivost nekog cijelog broja n s prostim brojevima $7, 11$ i 13.

Primijetimo da je $7 \cdot 11 \cdot 13 = 1001$ i $10^3 = 1000 \equiv -1 \pmod{1001}$. Stoga,

$$\begin{aligned} n = (a_k a_{k-1} ... a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0 \\ &= (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) + \\ &\quad + (1000)^2(a_6 + 10a_7 + 100a_8) + ... \\ &\equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + \\ &\quad + (100a_8 + 10a_7 + a_6) - ... \pmod{1001} \\ &\equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - ... \pmod{1001}. \end{aligned}$$

Dakle, cijeli broj n je kongruentan modulo 1001 s cijelim brojem koji je dobiven naizmjeničnim zbrajanjem i oduzimanjem troznamenkastih blokova od n. Blokovi su dobiveni grupiranjem po tri uzastopne znamenke broja n počevši s desne strane broja n. U zadnjem bloku može se pojaviti jedna ili dvije znamenke, odnosno zadnji blok sadrži znamenke broja n koje su preostale nakon formiranja svih prethodnih blokova. Također, ukoliko u nekom od blokova prva znamenka ili i prva i druga znamenka su nule, imati ćemo blokove brojeva koji sadrže manje od tri znamenke. Dakle, prvi blok sadržava znamenke a_2 i a_1 i a_0, drugi blok a_5, a_4 i a_3, treći blok a_8, a_7 i a_6 i tako nastavimo dok sve znamenke broja n ne budu iskorištene.
Budući da su $7, 11$ i 13 djelitelji broja 1001, da bismo ispitali je li cijeli broj n djeljiv s $7, 11$ ili 13, potrebno je provjeriti je li alternirajuća suma troznamenkastih blokova broja n djeljiva s $7, 11$ ili 13.

Drugim riječima, cijeli broj n je djeljiv s $7, 11$ odnosno 13 ako i samo ako je alternirajuća suma $(a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - ...$ blokova koji se sastoje od po tri uzastopne znamenke broja n djeljiva sa $7, 11$ odnosno 13.

Na sljedećem primjeru ćemo ilustrirati kako istodobno provjeravati djeljivost s prostim brojevima $7, 11$ i 13.

Primjer 2.7.
Neka je $n = 11234496$. *Budući da je alternirajuća suma troznamenkastih blokova,* $496 - 234 + 11 = 273$, *djeljiva sa* 7 *i* 13, *ali nije sa* 11, *vidimo da je* n *djeljiv s* 7 *i* 13, *ali nije s* 11.

2.7 Djeljivost s 37

Sada, vrlo slično kao u prethodnom kriteriju djeljivosti sa $7, 11$ i 13, ćemo razviti kriterij djeljivosti sa 37.

Primijetimo da je $10^3 = 1000 \equiv 1 \pmod{37}$. Stoga,

$$\begin{aligned} n = (a_k a_{k-1} ... a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0 \\ &= (a_0 + 10a_1 + 100a_2) + 10^3(a_3 + 10a_4 + 100a_5) + \\ &\quad + (10^3)^2(a_6 + 10a_7 + 100a_8) + ... \\ &\equiv (a_0 + 10a_1 + 100a_2) + 1(a_3 + 10a_4 + 100a_5) + \\ &\quad + 1^2(a_6 + 10a_7 + 100a_8) + ... \pmod{37} \\ &\equiv (100a_2 + 10a_1 + a_0) + (100a_5 + 10a_4 + a_3) + \\ &\quad + (100a_8 + 10a_7 + a_6) + ... \pmod{37} \\ &\equiv (a_2 a_1 a_0)_{10} + (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} + ... \pmod{37}. \end{aligned}$$

I u ovom slučaju, znamenke broja n se grupiraju u troznamenkaste blokove sastavljene od uzastopnih znamenaka broja n. Dakle, prvi blok sadržava znamenke a_2, a_1 i a_0, drugi blok sadržava znamenke a_5, a_4 i a_3, itd. Postupak se nastavlja sve dok ne iskoristimo sve znamenke broja n. Zadnji blok može sadržavati jednu, dvije ili tri znamenke, odnosno zadnji blok sadrži znamenke broja n koje su preostale nakon formiranja svih prethodnih blokova. Svi ostali blokovi su troznamenkasti brojevi, osim ako u nekom od blokova prva znamenka ili i prva i druga znamenka nije nula. Ukoliko je zbroj tako formiranih blokova djeljiv s 37, onda je i broj n djeljiv s 37.

Dakle, cijeli broj n je djeljiv sa 37 ako i samo ako je suma $(a_2 a_1 a_0)_{10} + (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} + ...$ blokova koji se sastoje od po tri uzastopne znamenke broja n djeljiva sa 37.

Primjer 2.8.
Neka je $n = 3153732$. *Budući da je zbroj* $732 + 153 + 3 = 888$ *djeljiv sa* 37, *onda je i* n *djeljiv sa* 37.

Primijetimo da se sva ispitivanja djeljivosti, koja smo razvili u ovom poglavlju, mogu proširiti na ispitivanja djeljivosti koja koriste zapis cijelog broja n u sustavima s nedecimalnim bazama.

2.8 Metoda izbacivanja devetki

Metoda izbacivanja devetki (Casting Out Nines) se temelji na činjenici da je svaki cijeli broj $n = (a_k a_{k-1}...a_1 a_0)_{10}$ kongruentan sumi svojih znamenki modulo 9, odnosno $n \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 9$.

Izraz "izbacivanje devetki" odnosi se na izbacivanje znamenke 9 ili znamenki koje zbrojene daju višekratnik broja 9 pri zbrajanju znamenki nekog pozitivnog cijelog broja n. Rezultat ove metode je broj manji od n (ako n ima više od jedne znamenke) koji daje isti ostatak kao n pri dijeljenju s 9. Zapravo, dobiveni broj može se dobiti iz n oduzimanjem višekratnika broja 9 od n. Upravo zbog tog svojstva ova metoda je i dobila naziv "Izbacivanje devetki".

Kada izbacujemo devetke pri zbrajanju znamenki broja n, bilo koji skup znamenki, koje zbrojene daju 9 ili višekratnika od 9, može se zanemariti.
Na primjer, u broju 4532 suma znamenki 4 i 5 je 9 te njih možemo zanemariti. Preostale znamenke, odnosno 3 i 2, zbrojimo i imamo $2 + 3 = 5$. Budući da je $5 = 4532 - 503 \cdot 9$, ovim računanjem smo izbacili 503 devetke iz broja 4532.
Neka je $n = (a_k a_{k-1}...a_1 a_0)_{10}$. Njegova suma znamenki je $a_k + a_{k-1} + ... + a_1 + a_0$. Razlika između n i njegove sume znamenki je

$$\begin{aligned} &10^k a_k + 10^{k-1} a_{k-1} + ... + 10a_1 + a_0 - (a_k + a_{k-1} + ... + a_1 + a_0) \\ &= (10^k - 1)a_k + (10^{k-1} - 1)a_{k-1} + ... + (10 - 1)a_1 + a_0 - a_0 \\ &= (10^k - 1)a_k + (10^{k-1} - 1)a_{k-1} + ... + 9a_1. \end{aligned}$$

Budući da su brojevi oblika $10^i - 1$ uvijek djeljivi s 9 ($10^i \equiv 1 \pmod 9$), zamjena broja n s njegovim zbrojem znamenki ima posljedicu izbacivanja $\frac{10^k-1}{9}a_k + \frac{10^{k-1}-1}{9}a_{k-1} + ... + a_1$ devetki.

Metoda izbacivanja devetki se može koristiti za provjeru i otkrivanje pogrešaka u rezultatima računskih operacija. Da bi smo provjerili rezultat računske operacije metodom izbacivanja devetki, na svaki operand računske operacije primjenimo metodu izbacivanja devetki i zatim na dobivene brojeve primjenimo isti slijed računskih operacija kao i na same operande. Ako u računanju nisu napravljene pogreške dobiveni rezultat mora biti isti kao prvotni rezultat koji provjeravmo. Ako su različiti, onda je barem jedna pogreška napravljena tijekom računanja.
Ovu metodu ilustrirati ćemo na sljedećim primjerima.

Primjer 2.9.
Pomoću metode izbacivanja devetki, potrebno je provjeriti je li zbroj brojeva 4562, 30256 *i* 17021 *jednak* 51829.

Imamo sljedeće kongruencije:

$$\begin{aligned} 4562 &\equiv \cancel{4} + \cancel{5} + 6 + 2 \equiv 8 \pmod 9, \\ 30256 &\equiv \cancel{3} + 0 + 2 + 5 + \cancel{6} \equiv 7 \pmod 9, \\ 17021 &\equiv 1 + \cancel{7} + 0 + \cancel{2} + 1 \equiv 2 \pmod 9. \end{aligned}$$

Njihov zbroj je $4562 + 30256 + 17021 \equiv 8 + 7 + 2 \equiv 8 \pmod 9$.
Sada, vidimo da dano rješenje je $51829 \equiv 5 + 1 + 8 + 2 + 9 \equiv 7 \pmod 9$.
Prema tome, dano rješenje nije kongruentno stvarnom zbroju znamenki modulo 9. *Stoga, dani zbroj je definitivo pogrešan. Točno rješenje je* 51839.

Primjer 2.10.
Pomoću metode izbacivanja devetki, potrebno je provjeriti je li umnožak brojeva 136 *i* 181 *jednak* 24661.

Imamo sljedeće kongruencije:

$$\begin{aligned} 136 &\equiv 1 + 3 + 6 \equiv 1 \pmod 9, \\ 181 &\equiv 1 + 8 + 1 \equiv 1 \pmod 9. \end{aligned}$$

Njihov umnožak je $136 \cdot 181 \equiv 1 \cdot 1 \equiv 1 \pmod 9$.
S druge strane dano rješenje je $24661 \equiv 2 + 4 + 6 + 6 + 1 \equiv 1 \pmod 9$.
Budući da je dano rješenje kongruentno stvarnom umnošku danih brojeva modulo 9, *mogli bismo biti u iskušenju da kažemo da je dano rješenje točno. Zapravo, sve što možemo reći jest da je dano rješenje vjerovatno ispravno jer bilo koja preraspodjela znamenki cijelog broja daje isti najmanji pozitivni ostatak modulo* 9.
Dano rješenje 24661 *je zapravo netočno. Točno rješenje je* 24616.

Iz danih primjera možemo zaključiti da jedini odgovor koji možemo pružiti pomoću metode izbacivanja devetki je da je dano rješenje definitivno pogrešno ili vjerojatno ispravno.

Primjer 2.11.
Pomoću metode izbacivanja devetki, potrebno je pronaći nepoznatu znamenku d *u rezultatu izračuna* $5243 - 1489 = 37d4$.

Najprije imamo sljedeće kongruencije:

$$\begin{aligned} 5243 &\equiv 5 + 2 + 4 + 3 \equiv 5 \pmod 9, \\ 1489 &\equiv 1 + 4 + 8 + 9 \equiv 4 \pmod 9. \end{aligned}$$

Njihova razlika je $5243 - 1489 \equiv 5 - 4 \equiv 1 \pmod 9$.
Zatim, vidimo da dano rješenje je $37d4 \equiv 3 + 7 + d + 4 \equiv 5 + d \pmod 9$.
Budući da dano rješenje mora biti kongruentno njihovoj razlici modulo 9 *imamo*

$$\begin{aligned} 5 + d &\equiv 1 \pmod 9 \\ d &\equiv -4 \pmod 9 \\ &\equiv 5 \pmod 9. \end{aligned}$$

Dakle, tražena znamenka je 5.

Iako je ova metoda iznimno korisna, ona ne može otkriti sve pogreške nastale prilikom računanja. Na primjer, bilo koji od pogrešnih rezultata kao što su $8, 17, 26$, odnosno bilo koji rezultat kongruentan 8 modulo 9, koji se dobije množenjem 5 s 7, ova metoda neće prepoznati kao pogrešan. Zapravo, metoda otkriva jedino ona pogrešna rješenja čija suma znamenki modulo 9 je jedna od 8 znamenki koja je različita od znamenke koja se dobije zbrajanjem znamenki točnog rezultata.

2.9 Digitalni korijen

Određivanje digitalnog korijena pozitivnog cijelog broja N je usko povezno s metodom izbacivanja devetki. Digitani korijen od N je jednoznamenkasti cijeli broj d i izračunava se metodom iteracije na sljedeći način:

1. Pronađite zbroj znamenki s broja N.
2. Pronađite zbroj znamenki od s.
3. Postupak se nastavlja sve dok dok se ne pojavi jedna znamenka d.
4. d je digitalni korijen od N.

Primjer 2.12.
Pronađimo digitalni korijen broja $N = 157$.

1. *Najprije zbrojimo sve njegove znamenke:* $s = 1 + 5 + 7 = 13$.
2. *Sada zbrojimo znamenke od* s*:* $1 + 3 = 4$.
3. *Pojavila se jedna znamenka i postupak se završava.*
4. *Digitalni korijen broja* $N = 157$ *je* $d = 4$.

Primijetimo da pomoću metode izbacivanja devetki vrlo lako možemo izračunati traženi digitalni korijen. Imamo da je $157 \equiv 1 + 5 + 7 \equiv 4 \pmod 9$.

Općenito, neka je $N = (a_k a_{k-1} ... a_1 a_0)_{10}$ i neka je d njegov digitalni korijen. Tada je $d \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 9$. Prema tome, digitalni korijen od N je ostatak pri djeljenju N s 9, s jednom iznimkom: d je 9 ako je ostatak 0.

Primjer 2.13.
Pretpostavimo da je digitani korijen cijelog broja n *jednak* 9*. Potrebno je pokazati da digitalni korijen bilo kojeg višekratnika broja* n *je isto* 9*.*

Neka je d *digitalni korijen broja* n*. Znamo da je digitalni korijen od* n *ostatak pri djeljenju broja* n *s* 9*.*
Budući da je $d = 9 \equiv 0 \pmod 9$*, ostatak pri djeljenju broja* n *s* 9 *je* 0*. Prema tome,* $n \equiv d \equiv 0 \pmod 9$*. Tada je i* $n \cdot m \equiv 0 \pmod 9$*.*
Dakle, digitalni korijen od $m \cdot n$ *je također* 9*.*

Primjer 2.14.
Potrebno je pronaći digitalni korijen broja $5^{3001} + 5^{3002} + ... + 5^{3009}$.

Neka N označava dani broj. Budući da je $5^3 \equiv -1 \pmod 9$ i prema teoremu o djeljenju s ostatkom 1.3, imamo da je

$$\begin{aligned}
N &= 5^{3\cdot 1000+1} + 5^{3\cdot 1000+2} + 5^{3\cdot 1001} + 5^{3\cdot 1001+1} + 5^{3\cdot 1001+2} + ... + 5^{3\cdot 1003} \\
&= (5^3)^{1000} \cdot 5 + (5^3)^{1000} \cdot 5^2 + (5^3)^{1001} + (5^3)^{1001} \cdot 5 + (5^3)^{1001} \cdot 5^2 + ... + (5^3)^{1003} \\
&\equiv (-1)^{1000} \cdot 5 + (-1)^{1000} \cdot 5^2 + (-1)^{1001} + (-1)^{1001} \cdot 5 + (-1)^{1001} \cdot 5^2 + \\
&\quad + (-1)^{1002} + (-1)^{1002} \cdot 5 + (-1)^{1002} \cdot 5^2 + (-1)^{1003} \pmod 9 \\
&\equiv 5 + 5^2 + (-1) + (-1)5 + (-1)5^2 + 1 + 5 + 5^2 + (-1) \pmod 9 \\
&\equiv 29 \pmod 9 \\
&\equiv 2 \pmod 9.
\end{aligned}$$

Budući da je digitalni korijen broja N ostatak pri djeljenju N sa 9, onda je digitalni korijen od N jednak 2.

Primjer 2.15.
Potrebno je pronaći digitalni korijen broja $n = 2^{p-1}(2^p - 1)$, gdje su p i $2^p - 1$ prosti brojevi.

Ako je $p = 2$, onda je $n = 6$ pa je i digitalni korijen broja n jednak 6.
Sada, pretpostavimo da je $p > 2$. Tada je p neparan prost broj i zbog $2 \equiv -1 \pmod 3$, imamo

$$2^{p-1} \equiv (-1)^{p-1} \equiv 1 \pmod 3.$$

Prema teoremu 1.1, kongruenciju $2^{p-1} \equiv 1 \pmod 3$ možemo zapisati kao $2^{p-1} = 3k + 1$ za neki cijeli broj k. Primijetimo da je

$$\begin{aligned}
2^{p-1} = 2^{-1}2^p = 3k + 1 \qquad & / \cdot 2 \\
(2 \cdot 2^{-1}) \cdot 2^p = 2 \cdot (3k + 1) & \\
2^p = 6k + 2 & \\
2^p - 1 = 6k + 1 &
\end{aligned}$$

Prema tome, imamo da je

$$\begin{aligned}
n &= (3k + 1)(6k + 1) \\
&= 18k^2 + 9k + 1 \equiv 1 \pmod 9.
\end{aligned}$$

Budući da je digitalni korijen broja n ostatak pri djeljenju n sa 9, onda je digitalni korijen od n jednak 1.

Sljedeći primjer identificira moguće digitalne korijene potpunih kvadrata.

Primjer 2.16.
Potrebno je pronaći digitalni korijen kvadrata bilo kojeg broja.

Prema teoremu o djeljenju s ostatkom 1.3, svaki cijeli broj n je oblika $9k + r$, gdje je $0 \leq r < 9$. Tada teorem 1.2 povlači da je $n \equiv r \pmod 9$. Iz korolara 1.5.2 slijedi da je $n^2 \equiv r^2 \pmod 9$.
Budući da je $r \equiv r - 9 \pmod 9$, imamo

$$\begin{aligned} 0^2 &\equiv 0 \pmod 9, \\ (\pm 1)^2 &\equiv 1 \pmod 9, \\ (\pm 2)^2 &\equiv 4 \pmod 9, \\ (\pm 3)^2 &\equiv 0 \pmod 9, \\ (\pm 4)^2 &\equiv 7 \pmod 9. \end{aligned}$$

Prema tome, n^2 je kongruentan s $0, 1, 4$ ili 7. Dakle, njegov digitalni korijen je $1, 4, 7$ ili 9.

Prethodni primjer nam može poslužiti za ispitivanje može li pozitivan cijeli broj biti kvadrat nekog broja. Dakle, ako je cijeli broj kvadrat nekog broja, tada njegov digitalni korijen mora biti $1, 4, 7$, ili 9.

Primjer 2.17.
Potrebno je ispitati može li $N = 1776^{1776}$ biti kvadrat nekog broja.

Najprije imamo sljedeću kongruenciju:

$$1776 \equiv 1 + 7 + 7 + 6 \equiv 3 \pmod 9.$$

Iz korolara 1.5.2 slijedi da je

$$1776^2 \equiv 3^2 \equiv 0 \pmod 9.$$

Prema tome, teorem 1.6 povlači da je

$$1776^k \equiv 0^k \equiv 0 \pmod 9, \forall\, k > 1.$$

Budući da je $1776 > 1$, tada

$$1776^{1776} \equiv 0 \pmod 9.$$

Dakle, N je kongruentan 0 modulo 9 i njegov digitalni korijen je $d = 9$. Stoga, N može biti kvadrat nekog broja.

Primijetimo da obrat prethodne tvrdnje ne vrijedi, odnosno ako je digitalni korijen od N $1, 4, 7$ ili 9, tada N ne mora biti kvadrat nekog broja.
Na primjer, digitalni korijen od 27 je 9, ali 27 nije kvadrat nekog broja.

2.10 Metoda izbacivanja dvojki

Metoda slična metodi izbacivanja devetki, koja se zove metoda izbacivanja dvojki (Casting Out Twos), može se primjeniti za provjeru točnosti rezultata računskih operacija s binarnim brojevima. U ovom postupku, izbacujemo sve parove bitova ("dvojke") koji zbrojeni daju 0 modulo 2.

Primjer 2.18.
Pomoću metode izbacivanja dvojki, potrebno je provjeriti jesu li rezultati danih računskih operacija vjerovatni točni ili definitivno netočni.

(1)

$$\begin{array}{rr} & 1000111010111 \\ \times & 0000101101110 \\ \hline & 11001110000101100010 \end{array}$$

(2)

$$\begin{array}{rr} & 101101101101 \\ - & 0111011101011 \\ \hline & 001111110000 \end{array}$$

(1)

$$\begin{array}{rr} & \not{1}000\not{1}\not{1}\not{1}0\not{1}0\not{1}\not{1}\not{1} \quad \Rightarrow 0 \\ \times & 0000\not{1}0\not{1}\not{1}0\not{1}\not{1}\not{1}0 \quad \Rightarrow 0 \\ \hline & \not{1}\not{1}00\not{1}\not{1}0000000\not{1}0\not{1}\not{1}000\not{1}0 \\ & \Downarrow \quad \Downarrow \\ & 0 \Longleftrightarrow 0 \end{array}$$

Slijedi da je umnožak $1000111010111 \cdot 0000101101110 \equiv 0 \cdot 0 \equiv 0 \pmod 2$. *Također, dano rješenje je* $11001110000101100010 \equiv 0 \pmod 2$.
Prema tome, dano rješenje je kongruentno stvarnom umnošku modulo 2. *Dakle, sve što možemo zaključiti je da dano rješenje je vjerovatno točno.*

(2)

$$\begin{array}{rr} & \not{1}0\not{1}\not{1}0\not{1}\not{1}0\not{1}\not{1}0\not{1} \quad \Rightarrow 0 \\ - & 0\not{1}\not{1}\not{1}0\not{1}\not{1}\not{1}0\not{1}0\not{1}1 \quad \Rightarrow 1 \\ \hline & 00\not{1}\not{1}\not{1}\not{1}\not{1}\not{1}0000 \\ & \Downarrow \quad \Downarrow \\ & 0 \Longleftrightarrow \textit{-1} \end{array}$$

Vidimo da je razlika $101101101101 - 0111011101011 \equiv 0 - 1 \equiv 1 \pmod 2$. *S druge strane, za dano rješenje vrijedi* $00111110000 \equiv 0 \pmod 2$.
Prema tome, dano rješenje nije kongruentno stvarnoj razlici modulo 2. *Stoga, dano rješenje je definitivno pogrešno.*

Poglavlje III

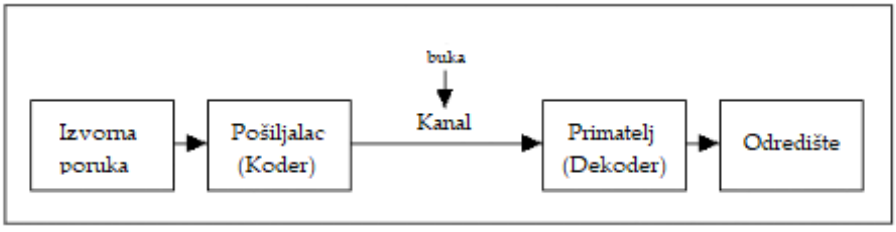
Sheme kodiranja i kontrolne znamenke

Teorija kodiranja je grana matematike koja se bavi oblikovanjem kodova koji se koriste za pouzdan prijenos informacija preko bučnih kanala te otkrivanje i ispravljanje pogrešaka u prenesenim podacima. Cilj je osigurati da prenesene poruke budu lako čitljive. U ovom dijelu rada ćemo vidjeti kako se kongruencije mogu koristiti u svrhu otkrivanja i ispravljanja pogrešaka u prenesenim porukama. Najprije ćemo se osvrnuti na binarne kodove.

3.1 Binarni kodovi

Izvorna poruka se šifrira i šalje u obliku binarnih znamenki ili bitova, nizova 0 ili 1. Ti bitovi se moraju prenijeti duž kanala (poput telefonske linije) u kojima se pogreške pojavljuju slučajno. Za nadoknadu pogrešaka mora se prenijeti više bitova nego što je u izvornoj poruci. Primatelj pokušava otkriti izvornu poruku dešifriranjem primljene poruke. Sve pogreške u primljenim porukama moraju biti otkrivene, a zatim i ispravljene.

Slika 3.1



Metoda koja igra značajnu ulogu u otkrivanju i ispravljanju pogrešaka u binarnim podacima je metoda izbacivanja dvojki (2.10). Prije prijenosa poruke, svakom binarnom nizu $x_1x_2...x_n$ dodaje se paritetni kontrolni bit x_{n+1}, koji je definiran s

$$x_{n+1} \equiv x_1 + x_2 + ... + x_n \pmod 2.$$

Dakle, na kraj binarnog niza dodaje se 1 ako je broj jedinica u binarnom nizu neparan, a u suprotnom dodaje 0 na kraj niza. Ova metoda, dodavanjem kontrolnog bita, održava

broj jedinica u binarnom nizu uvijek parnim. Stoga, ukoliko se u primljenoj poruci, koja je u obliku nizova 0 ili 1, pojavi neparan broj jedinica možemo zaključiti da se neparan broj pogreški pojavio tijekom prijenosa poruke.

Sljedeći primjer ilustrira ovu metodu.

Primjer 3.1.
Promotrimo 12*-bitni niz* 111010101010.
Sada je $x_{13} \equiv 1+1+1+0+1+0+1+0+1+0+1+0 \equiv 1 \pmod 2$.
Prema tome, kontrolni bit je 1 *i prenesena poruka je* 1110101010101.

Sada, pretpostavimo da smo primili binarni niz 1110101010010.
Budući da binarni niz sadrži neparan broj jedinica, znamo da se neparan broj pogreški pojavio tijekom prijenosa poruke. Ako postoji samo jedna pogreška u primljenoj poruci i poznato je na kojem mjestu se ona nalazi, zamjenom tog bita možemo dobiti izvornu poruku.

3.2 Kontrolne znamenke u identifikacijskim brojevima

Kontrolne znamenke se koriste za učinkovito otkrivanje i otklanjanje učestalih pogreški, u broju ili nizu koji je sastavljen od decimalnih znamenki, koje nastaju prilikom prepisivanja identifikacijskih brojeva (obično dvije znamenke zamjene mjesta ili se dogodi pogreška u zapisu jedne znamenke). Kontrolne znamenke su brojevi koji su dodani identifikacijskom broju koji se nalazi na proizvodima, knjigama, kreditnim karticama, identifikacijskim dokumentima itd. U identifikacijskom broju se obično nalazi jedna, ali nekad i više kontrolnih znamenki koje se određuju algoritmom iz ostalih znamenki ili slova koda. Banke, knjižnice, izdavači knjiga te razne tvrtke, koje prate veliki broj artikala, koriste kontrolne znamenke kako bi pronašle pogreške u njihovim identifikacijskim brojevima, kao što ćemo vidjeti u sljedećih nekoliko primjera.
Prije primjera, uvesti ćemo jednu jednostavnu definiciju koja će nam biti potrebna u nastavku rada.

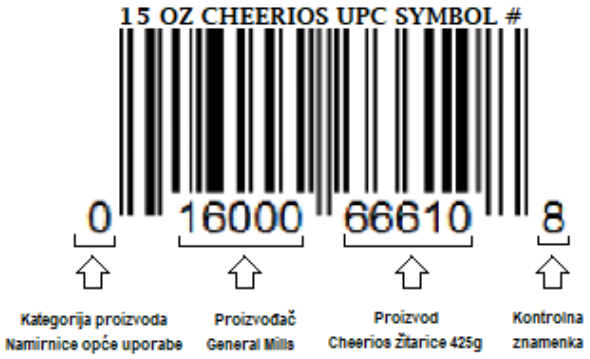
Definicija 3.1. *Skalarni umnožak vektora* $(x_1, x_2, ..., x_n)$ *i* $(x_1, y_2, ..., y_n)$ *je definiran s*

$$(x_1, x_2, ..., x_n) \cdot (x_1, y_2, ..., y_n) = \sum_{i=1}^{n} x_i y_i.$$

Univerzalni kôd proizvoda ***UPC*** (akronim od eng. The Universal Product Code), koji se može pronaći na proizvodima u supermarketima, sadrži kontrolnu znamenku. UPC se koristi u SAD-u, Kanadi, Velikoj Britaniji, Australiji, Novom Zelandu, Europi i drugim zemljama za praćenje trgovačkih artikala. UPC broj sadrži 12 znamenki $d_1, d_2, d_3, ..., d_{12}$ koje su jedinstveno dodijeljene svakom trgovinskom artiklu. UPC broj je podijeljen u četiri skupine. Prva skupina sastoji se od jedne znamenke i označava kategoriju proizvoda. Sljedećih 5 znamenki identificira zemlju u kojoj je proizvod proizveden i proizvođača. Zatim, sljedećih 5 znamenki su kôd proizvoda koji određuje proizvođač, a zadnja znamenka

d_{12} je kontrolna znamenka.
Na primjer, UPC broj za *Cheerios žitarice General Mills, Inc.* je
$0 - 16000 - 66610 - d_{12}$. Kodovi kategorije proizvoda, proizvođača i proizvoda su redom $0, 16000$ i 66610. Znamenka 0 u kodu kategorije proizvoda je rezervirana za namirnice opće uporabe.

Slika 3.2



Kontrolna znamenka d_{12} u UPC broju mora zadovoljavati

$$(d_1, d_2, ..., d_{12}) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) \equiv 0 \pmod{10}.$$

Odnosno,

$$d_{12} \equiv -(d_1, d_2, ..., d_{11}) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10}.$$

Sljedeći primjer ilustrira ovu metodu.

Primjer 3.2.
Potrebno je odrediti kontrolnu znamenku d_{12} u UPC broju $0 - 16000 - 66610 - d_{12}$ za proizvod Cheerios žitarice General Mills, Inc.

Imamo

$$\begin{aligned} d_{12} &\equiv -(d_1, d_2, ..., d_{11}) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(0, 1, 6, 0, 0, 0, 6, 6, 6, 1, 0) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(0 + 1 + 18 + 0 + 0 + 0 + 18 + 6 + 18 + 1 + 0) \pmod{10} \\ &\equiv -2 \equiv 8 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je 8 i potpuni UPC identifikacijski broj proizvoda je $0-16000-66610-8$.

Broj MasterCard kreditne kartice sadrži 16 znamenki $d_1 d_2 d_3 ... d_{15} d_{16}$, gdje d_{16} označava kontrolnu znamenku. Ona se određuje kao

$$d_{16} \equiv -\Big[\sum_{i=1}^{8} \rho(2d_{2i-1}) + \sum_{i=1}^{7} d_{2i}\Big] \pmod{10},$$

gdje $\rho(m)$ označava digitalni korijen od m.

Primjer 3.3.
Potrebno je odrediti kontrolnu znamenku ako petnaesteroznamenkasti MasterCard identifikacijski broj kreditne kartice je $6764 - 5904 - 0068 - 035$.

Imamo

$$\begin{aligned} d_{16} &\equiv -\Big[\rho(2d_1) + \rho(2d_3) + \rho(2d_5) + \rho(2d_7) + \rho(2d_9) + \rho(2d_{11}) + \rho(2d_{13}) + \rho(2d_{15}) + \\ &\quad + d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12} + d_{14}\Big] \pmod{10} \\ &\equiv -\Big[\rho(12) + \rho(12) + \rho(10) + \rho(0) + \rho(0) + \rho(12) + \rho(0) + \rho(10) + \\ &\quad + 7 + 4 + 9 + 4 + 0 + 8 + 3\Big] \pmod{10} \\ &\equiv -(3 + 3 + 1 + 0 + 0 + 3 + 0 + 1 + 7 + 4 + 9 + 4 + 0 + 8 + 3) \pmod{10} \\ &\equiv -46 \pmod{10} \\ &\equiv 4 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je $d_{16} = 4$, *a potpuni MasterCard identifikacijski broj je* $6764 - 5904 - 0068 - 0354$.

Knjižnice koriste sofisticirani *code-a-bar sustav* kako bi dodijelile svakoj knjizi trinaesteroznamenkasti identifikacijski broj $d_1 d_2 ... d_{13}$ i kontrolnu znamenku d_{14}. Kontrolna znamenka se određuje kao

$$d_{14} \equiv \Big[- (d_1, d_2, ..., d_{13}) \cdot (2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2) - k\Big] \pmod{10},$$

gdje k označava broj znamenki među $d_1, d_3, d_5, d_7, d_9, d_{11}$ i d_{13} koje su veće ili jednake 5.

Primjer 3.4.
Potrebno je odrediti kontrolnu znamenku d_{14} *za identifikacijski broj knjige* $2 - 2041 - 00055 - 037$.

Imamo

$$\begin{aligned} d_{14} &\equiv \Big[- (2, 2, 0, 4, 1, 0, 0, 0, 5, 5, 0, 3, 7) \cdot (2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2) - 2\Big] \pmod{10} \\ &\equiv -(4 + 2 + 0 + 4 + 2 + 0 + 0 + 0 + 10 + 5 + 0 + 3 + 14) - 2) \pmod{10} \\ &\equiv -46 \pmod{10} \\ &\equiv 4 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je $d_{14} = 4$ *i potpuni identifikacijski broj knjige je* $2 - 2041 - 00055 - 037 - 4$.

Mnoge europske zemlje koriste kontrolne znamenke kako bi otkrile pogreške u identifikacijskim brojevima putovnica. Kontrolna znamenka d_8 dodaje se na kraj identifikacijskog broja $d_1d_2...d_7$ i definirana je s

$$d_8 \equiv (d_1, d_2, ..., d_7) \cdot (7, 3, 1, 7, 3, 1, 7) \pmod{10}.$$

Primjer 3.5.
Potrebno je odrediti kontrolnu znamenku ako je prvih sedam brojeva putovnice 3157406.

Imamo

$$\begin{aligned} d_8 &\equiv (d_1, d_2, ..., d_7) \cdot (7, 3, 1, 7, 3, 1, 7) \pmod{10} \\ d_8 &\equiv (3, 1, 5, 7, 4, 0, 6) \cdot (7, 3, 1, 7, 3, 1, 7) \pmod{10} \\ d_8 &\equiv 21 + 3 + 5 + 49 + 12 + 0 + 42 \pmod{10} \\ d_8 &\equiv 132 \pmod{10} \\ d_8 &\equiv 2 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je $d_8 = 2$*, a potpuni identifikacijski broj putovnice je* 31574062.

Svaki bankovni ček ima osmeroznamenkasti identifikacijski broj $d_1d_2...d_8$ iza kojeg slijedi kontrolna znamenka d, koja se određuje na sljedeći način:

$$d \equiv (d_1, d_2, ..., d_8) \cdot (7, 3, 9, 7, 3, 9, 7, 3) \pmod{10}.$$

Primjer 3.6.
Potrebno je odrediti nepoznatu znamenku x *u identifikacijskom broju bankovnog čeka* $3313x4473$.

Primjetimo da je kontrolna znamenka $d = 3$*. Imamo*

$$\begin{aligned} 3 &\equiv (d_1, d_2, ..., d_8) \cdot (7, 3, 9, 7, 3, 9, 7, 3) \pmod{10} \\ &\equiv (3, 3, 1, 3, x, 4, 4, 7) \cdot (7, 3, 9, 7, 3, 9, 7, 3) \pmod{10} \\ &\equiv 3 \cdot 7 + 3 \cdot 3 + 1 \cdot 9 + 3 \cdot 7 + x \cdot 3 + 4 \cdot 9 + 4 \cdot 7 + 7 \cdot 3 \pmod{10} \\ &\equiv 21 + 9 + 9 + 21 + 3x + 36 + 28 + 21 \pmod{10} \\ &\equiv 3x + 5 \pmod{10}. \end{aligned}$$

Zbog svojstva simetričnosti (teorem 1.2) imamo

$$\begin{aligned} 3x + 5 &\equiv 3 \pmod{10} \\ 3x &\equiv -2 \equiv 8 \pmod{10}. \end{aligned}$$

Primjetimo da je $3 \cdot 7 \equiv 1 \pmod{10}$, *odnosno* $3^{-1} \equiv 7 \pmod{10}$. *Budući da je* $(3, 10) = 1$, *prema teoremu 1.11 linearna kongruencija* $3x \equiv 8 \pmod{10}$ *ima jedinstveno rješenje modulo* 10. *Sada je*

$$\begin{aligned} 7(3x) &\equiv 7 \cdot 8 \pmod{10} \\ x &\equiv 56 \pmod{10} \\ x &\equiv 6 \pmod{10}. \end{aligned}$$

Dakle, $x = 6$ *i deveteroznamenkasti identifikacijski broj bankovnog čeka je* 331364473.

VISA Travelers Checks je za kontrolnu znamenku koristila broj suprotan ostatku pri dijeljenju s 9, modulo 9. Sljedeći primjer ilustrira ovu metodu određivanja kontrolne znamenke.

Primjer 3.7.
Potrebno je odrediti kontrolnu znamenku za ček s identifikacijskim brojem 300706202013.

Prvo, imamo

$$\begin{aligned} 300706202013 &\equiv 3 + 0 + 0 + 7 + 0 + 6 + 2 + 0 + 2 + 0 + 1 + 3 \pmod{9} \\ &\equiv 6 \pmod{9}. \end{aligned}$$

Nakon što smo dobili najmanji ostatak modulo 9, *za izračun kontrolne znamenke uzimamo broj suprotan dobivenom ostatku pri dijeljenju s* 9, *modulo* 9*:*

$$d \equiv -6 \equiv 3 \pmod{9}.$$

Dakle, tražena kontrolna znamenka je 3.

3.3 Poštanski brojevi

POSTNET (akronim od eng. Postal Numeric Encoding Technique) je barkod poštanskog ureda u SAD-u . Barkod se koristi za šifriranje podataka o poštanskom broju primatelja u strojno čitljiv format, što poboljšava brzinu sortiranja i dostavljanja pošte. POSTNET barkod može biti u tri varijante koje se razlikuju u duljini podataka: *peteroznamenkasti poštanski kôd* (sadrži 32 bara), *deveteroznamenkasti poštanski +4 kôd* (sadrži 52 bara) ili *jedanaesteroznamenkasti kôd mjesta isporuke* (sadrži 62 bara). Za kreiranje POSTNET barkoda koriste se i binarni brojevi i kontrolne znamenke. POSTNET barkod sadrži početni bar, šifrirane podatake o poštanskom broju, kontrolnu znamenku i završni bar. Neki barovi u kodu su dugi (puni bar), a neki kratki (polu bar). Dugi bar predstavlja bit 1, a kratki bar predstavlja bit 0. Dva krajnja bara POSTNET barkoda su uvijek duga i mogu se zanemariti. Preostali barovi sadrže šifrirane podatke o poštanskom broju i dijele se u skupine po 5 barova, s tim da zadnja skupina od 5 barova predstavlja kontrolnu znamenku. Dakle, jedna POSTNET znamenka sastoji se od 5 barova, točnije 2 duga i 3 kratka bara kao što vidimo na slici 3.3.

Slika 3.3

Postoji točno $\frac{5!}{2!3!} = 10$ kombinacija od dva duga i tri kratka bara i one predstavljaju znamenke $0, 1, 2, ..., 8, 9$, kao što možemo vidjeti u tablici 3.1. S iznimkom za znamenku 0, numerička vrijednost svake kombinacije od 5 barova dobije se zbrajanjem težina koje su dodijeljene dugim barovima. Težine $0, 1, 2, 4$ i 7 se dodjeljuju od desna prema lijevo bar pozicijama. Na primjer, numerička vrijednost POSTNET znamenke na slici 3.3 je 4. Jedino odstupanje od ovog pravila je kombinacija  , koja ima ukupnu težinu 11, ali joj je dodijeljena numerička vrijednost 0.

	Težine bar pozicija	
Numerička vrijednost	Binarni zapis **74210**	Barkod **74210**
1	00011	
2	00101	
3	00110	
4	01001	
5	01010	
6	01100	
7	10001	
8	10010	
9	10100	
0	11000	

Tablica 3.1

Promotrimo *peteroznamenkasti poštanski broj* $x_1x_2...x_5$. Kontrolna znamenka d, koja se dodaje kodu u svrhu otkrivanja pogrešaka, definirana je s

$$d \equiv -\sum_{i=1}^{5} x_i \pmod{10}.$$

Na primjer, kontrolna znamenka za poštanski broj 97101 je

$$\begin{aligned} d &\equiv -(9+7+1+0+1) \pmod{10} \\ &\equiv -18 \equiv 2 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je $d = 2$ i potpuni poštanski broj je $97101 - 2$.

Kontrolna znamenka je također dodana svakom *poštanskom +4 kodu*, koji je uveden od strane pošte SAD-a u 1983. godini. Sada, promotrimo deveteroznamenkasti poštanski broj $x_1x_2...x_9$. Kontrolna znamenka d je definirana s

$$d \equiv -\sum_{i=1}^{9} x_i \pmod{10}.$$

Na primjer, kontrolna znamenka za deveteroznamenkasti poštanski broj $97101 - 9155$ je dana s

$$\begin{aligned} d &\equiv -(9+7+1+0+1+9+1+5+5) \pmod{10} \\ &\equiv -38 \equiv 2 \pmod{10}. \end{aligned}$$

Dakle, $d = 2$ i poštanski +4 kôd je $97101 - 9155 - 2$.

Jedanaesteroznamenkasti *kôd mjesta isporuke DPBC* (akronim od eng. delivery point bar code) je uveden od strane pošte SAD-a u 1993. godini za jedinstvenu identifikaciju svakog od 115 milijuna mjesta isporuke u SAD-u. To uklanja potrebu za razvrstavanjem pošte prije isporuke. DPBC nastaje dodavanjem 10 barova na postojeći poštanski +4 kôd. Deset barova predstavlja 2 dodatna broja (obično, posljednja dva broja adrese ulice, poštanskog sandučića, sandučića ruralne rute ili sandučića ugovorene rute na autocesti).

Kontrolna znamenka d, koja je dodana svakom jedanaesteroznamenkastom DPBC broju $x_1x_2...x_{11}$, definirana je s

$$d \equiv -\sum_{i=1}^{11} x_i \pmod{10}.$$

Na primjer, kontrolna znamenka za DPBC broj $97101 - 9155 - 04$, gdje 04 označava mjesto dostave, je dana s

$$\begin{aligned} d &\equiv -(9+7+1+0+1+9+1+5+5+0+4) \pmod{10} \\ &\equiv -42 \equiv 8 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je $d = 8$. Potpuni DPBC broj je $97101 - 9155 - 04 - 8$ i odgovarajući barkod je prikazan na slici 3.4.

Slika 3.4

3.4 ISBN i ISSN

ISBN (akronim od eng. International Standard Book Number) je međunarodni standardni knjižni broj za identifikaciju knjiga koji ima gotovo svaka knjiga izdana bilo gdje u svijetu od 1972 godine. ISBN koriste izdavači, knjižare, knjižnice, internetske trgovine i ostali sudionici opskrbnog lanca u svrhu naručivanja, unošenja i spremanja podataka, evidencije prodaje i kontrole zaliha. ISBN broj sadrži deset znamenki koje su podijeljene u 4 skupine odvojene crticama. Prva znamenka označava jezik ili zemlju izdavanja, sljedeće dvije znamenke označavaju nakladnika, zatim sljedećih šest znamenki označava kôd knjige i zadnja znamenka je kontrolna znamenka.
Na primjer, ISBN broj knjige T.Koshy(2007) [6] je $0-12-372487-d$. Kôd 0 ukazuje da je knjiga izdana u zemlji engleskog govornog područja. Zatim, kôd 12 identificira nakladnika Academic Press. Šesteroznamenkasti broj 372487, koji knjizi dodjeljuje njezin nakladnik i sadži informacije o naslovu, izdanju, vrsti uveza i broju sveska knjige, je kôd knjige.

Zadnja znamenka d je kontrolna znamenka, gdje je $0 \leq d \leq 10$, definirana je s

$$d \equiv -(x_1, x_2, ..., x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11},$$

gdje $x_1, x_2, ..., x_9$ označavaju prvih devet znamenki ISBN identifikacijskog broja knjige. Ukoliko je $d \equiv 10 \pmod{11}$, tada se na posljednje mjesto upisuje X.

Sljedeći primjer demonstrira ovu shemu kodiranja.

Primjer 3.8.
Pomoću ISBN sheme kodiranja, potrebno je izračunati kontrolnu znamenku d ako prvih devet znamenki ISBN broja su $0-12-372487$.

$$\begin{aligned} d &\equiv -(x_1, x_2, ..., x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0, 1, 2, 3, 7, 2, 4, 8, 7) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0 + 9 + 16 + 21 + 42 + 10 + 16 + 24 + 14) \pmod{11} \\ &\equiv -152 \equiv 2 \pmod{11}. \end{aligned}$$

Dakle, kontrolna znamenka je 2. Identifikacijski broj knjige (ISBN) je $0-12-372487-2$.

Primjer 3.9.
Potrebno je provjeriti je li dani ISBN broj $0-21-057603-1$ ispravan.

Znamenka na desetoj poziciji je kontrolna znamenka. Da bi provjerili ispravnost danog broja izračunati ćemo kontrolnu znamenku iz prvih devet znamenki $0-21-057603$ i provjeriti da li se podudara s kontrolnom znamenkom koja se nalazi u danom broju. Tada

$$\begin{aligned} d &\equiv -(x_1, x_2, ..., x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0, 2, 1, 0, 5, 7, 6, 0, 3) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0 + 18 + 8 + 0 + 30 + 35 + 24 + 0 + 6) \pmod{11} \\ &\equiv -121 \equiv 0 \pmod{11}. \end{aligned}$$

Primijetimo da je kontrolna znamenka u danom broju $d = d_{10} = 1$. Dakle, dani ISBN broj nije ispravan.

ISSN (akronim od eng. International Serial Book Number) je međunarodni priznati kôd za identifikaciju periodične (serijske) publikacije kao što su novine, časopisi, bilteni. Korisiti se za obilježavanje tiskanih i elektroničkih periodičnih publikacija. Sadrži dvije skupine po četiri znamenke odvojene crticom. Osma znamenka d, gdje je $0 \leq d \leq 10$, je kontrolna znamenka i definirana je s

$$d \equiv -(x_1, x_2, ..., x_7) \cdot (8, 7, 6, 5, 4, 3, 2) \pmod{11},$$

gdje $x_1, x_2, ..., x_7$ označavaju prvih sedam znamenki ISSN identifikacijskog broja periodične publikacije. Ukoliko je $d \equiv 10 \pmod{11}$, tada se na posljednje mjesto upisuje X.

Primjer 3.10.
Potrebno je izračunati kontrolnu znamenku d ako prvih sedam znamenki ISSN broja su $1233 - 667$.

$$\begin{aligned} d &\equiv -(x_1, x_2, ..., x_7) \cdot (8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(1, 2, 3, 3, 6, 6, 7) \cdot (8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(8 + 14 + 18 + 15 + 24 + 18 + 14) \pmod{11} \\ &\equiv -111 \equiv 10 \pmod{11}. \end{aligned}$$

Dakle, kontrolna znamenka je X. Osmeroznamenkasti ISSN broj je $1233 - 667X$.

3.5 EAN-13 barkod

ISBN i ISSN brojevi se mogu prevesti u EAN-13 barkod. Svi EAN-13 barkodovi počinju s EAN prefiksom koji identificira zemlju podrijetla artikla (na primjer 385 za Hrvatsku, $00 - 09$ za SAD) koji dodjeljuje EAN International, s iznimkom za knjige i periodične publikacije gdje je EAN prefiks zamjenjen s prefiksom 978 za knjige, a 977 za periodične publikacije. Iza prefiksa 978 slijedi prvih 9 ISBN znamenki, a iza prefiksa 977 slijedi prvih 7 ISSN znamenki i dodatne dvije znamenke koje označavaju inačicu izdanja. Kontrolna znamenka kod ISBN/ISSN broja se odbacuje i zamjenjuje se s kontrolnom znamenkom koja se računa uzimajući u obzir "EAN pravila".
Na primjer, EAN-13 barkod periodične publikacije s ISSN brojem $1233-667X$, iz primjera 3.10, možemo vidjeti na slici 3.5.

Slika 3.5

EAN kontrolna znamenka d , gdje je $0 \leq d \leq 10$, je definirana s

$$d \equiv -(x_1, x_2, ..., x_{12}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3)) \pmod{10},$$

gdje $x_1, x_2, ..., x_{12}$ označavaju prvih dvanaest znamenki EAN-13 barkoda.

Kontrolna znamenka omogućava provjeru je li barkod točno skeniran ili jesu li sve znamenke koda dobro zapisane.

Na primjer, EAN broj knjige, koju smo koristili u prethodnom primjeru za objašnjenje ISBN koda, je $978-0-12-372487-d$, gdje je d kontrolna znamenka koju ćemo odrediti u sljedećem primjeru.

Primjer 3.11.
*Koristeći EAN-*13 *shemu kodiranja, potrebno je izračunati kontrolnu znamenku* d *ako prvih dvanaest znamenki ISBN broja su* $978 - 0 - 12 - 372487$.

$$\begin{aligned} d &\equiv -(x_1, x_2, ..., x_{12}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(9, 7, 8, 0, 1, 2, 3, 7, 2, 4, 8, 7) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(9 + 21 + 8 + 0 + 1 + 6 + 3 + 21 + 2 + 12 + 8 + 21) \pmod{10} \\ &\equiv -2 \equiv 8 \pmod{10}. \end{aligned}$$

Dakle, kontrolna znamenka je 8 *i trinaesteroznamenkasti broj knjige koji se nalazi na EAN barkodu je* $978 - 0 - 12 - 372487 - 8$. *Odgovarajući barkod je prikazan na slici 3.6.*

U SAD-u i nekoliko drugih zemalja koristi se peteroznamenkasti dodatni kôd kako bi se pružile dodatne informacije. Taj kôd se često koristi za informacije o cijeni knjige. Prva znamenka u tom kodu označava nacionalnu valutu. Na primjer, 5 označava američki dolar, a 6 kanadski dolar. Izdavači koji ne žele istaknuti cijenu proizvoda u dodatnom peteroznamenkastom kodu ispisuju 90090, kao što možemo vidjeti na slici 3.6.

Slika 3.6

3.6 Broj vozačke dozvole

U SAD-u metoda koja se koristi za označavanje vozačke dozvole uvelike varira od države do države. Neke države koriste kontrolne znamenke kada označavaju vozačke dozvole s ciljem pronalaska krivotvorina ili pogrešaka. Na primjer, Utah označava vozačke dozvole osmeroznamenkastim brojem $d_1d_2...d_8$ i zatim određuje devetu kontrolnu znamenku d_9 koja je je definirana s

$$d_9 \equiv \sum_{i=1}^{8}(10-i)d_i \pmod{10}.$$

Sljedeći primjer ilustrira ovu shemu kodiranja.

Primjer 3.12.
Potrebno je izračunati kontrolnu znamenku d_9 na vozačkoj dozvoli u državi Utah ako su prvih osam brojeva koji se nalaze u vozačkoj dozvoli 23756321*.*

Imamo

$$\begin{aligned} d_9 &\equiv (d_1, d_2, ..., d_8) \cdot (9,8,7,6,5,4,3,2) \pmod{10} \\ &\equiv (2,3,7,5,6,3,2,1) \cdot (9,8,7,6,5,4,3,2) \pmod{10} \\ &\equiv 18+24+49+30+30+12+6+2 \pmod{10} \\ &\equiv 1 \pmod{10}. \end{aligned}$$

Dakle, potpuni broj vozačke dozvole je 237563211*.*

Neke države koriste nešto kompliciranije sheme kodiranja u označavanju vozačkih dozvoli. Na primjer Novi Meksiko, Arkansas, Tennessee dodaju kontrolnu znamenku d_8 sedmeroznamenkastom broju $d_1d_2...d_7$ koja se određuje kako slijedi:
Neka je

$$x \equiv -(d_1, d_2, ..., d_7) \cdot (2,7,6,5,4,3,2) \pmod{11}.$$

Tada

$$d_8 = \begin{cases} 1, & \text{ako je } x = 0 \\ 0, & \text{ako je } x = 10 \\ x, & \text{inače} \end{cases}$$

Vermont koristi istu shemu kodiranja, osim za slučaj kada je $x = 0$, tada se slovo A koristi kao kontrolni znak.

Primjer 3.13.
Potrebno je odrediti kontrolnu znamenku d_8 u broju vozačke dozvole izdane od strane države Arkansas, ako su prvih sedam brojeva koji se nalaze u vozačkoj dozvoli 0365832*.*

Najprije ćemo izračunati x:

$$\begin{aligned} x &\equiv -(d_1, d_2, ..., d_7) \cdot (2, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0, 3, 6, 5, 8, 3, 2) \cdot (2, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0 + 21 + 36 + 25 + 32 + 9 + 4) \pmod{11} \\ &\equiv -127 \equiv 5 \pmod{11}. \end{aligned}$$

Dakle, prema definiciji, $d_8 = 5$. Potpuni broj vozačke dozvole je 03658325.

Južna Dakota i kanadska provincija Saskatchewan koriste kompleksne sheme razvijene od IBM za računanje kontrolne znamenke d_7 koja se dodaje šesteroznamenkastom identifikacijskom broju $d_1d_2...d_6$ koji se nalazi u vozačkoj dozvoli. Ona se računa na sljedeći način:

Algoritam 3.1.

1. *Pomnoži d_2, d_4 i d_6 s 2.*
2. *Zbroji znamenke u dobivenim umnoščima.*
3. *Zbroji dobivene sume sa d_1, d_3 i d_5 da bi dobili s.*
4. *Tada je $d_7 \equiv -s \pmod{10}$.*

Ovu shemu kodiranja su koristile tvrtke koje proizvode kredite kartice (Visa, American Express, MasterCard i dr.), knjižnice i ljekarne u SAD-u te banke u Njemačkoj.

Primjer 3.14.
Potrebno je odrediti kontrolnu znamenku d_7 za šesteroznamenkasti identifikacijski broj vozačke dozvole izdane u Južnoj Dakoti: 764076.

Neka je $n = (d_1d_2d_3d_4d_5d_6)_{10} = (764076)_{10}$. Ukoliko pratimo korake algoritma imamo da je:

1.
$$\begin{aligned} 2 \cdot d_2 &= 2 \cdot 6 = 12, \\ 2 \cdot d_4 &= 2 \cdot 0 = 0, \\ 2 \cdot d_6 &= 2 \cdot 6 = 12. \end{aligned}$$

2.
$$\begin{aligned} 1 + 2 &= 3, \\ 0, & \\ 1 + 2 &= 3. \end{aligned}$$

3. $s = 3 + 0 + 3 + d_1 + d_3 + d_5 = 3 + 0 + 3 + 7 + 4 + 7 = 24.$
4. *Tada je* $d_7 \equiv -24 \equiv 6 \pmod{10}$.

Dakle, tražena kontrolna znamenka je 6 *i potpuni identifikacijski broj vozačke dozvole je* 7640766.

3.7 Sheme s dvije kontrolne znamenke

Sheme kodiranja se koriste ponekad i za izradu identifikacijskih brojeva građana. Norveška, na primjer, koristi shemu s dvije kontrolne znamenke kako bi dodijelila nacionalne identifikacijske brojeve svojim građanima. Norveški nacionalni identifikacijski broj, koji se dodjeljuje rođenjem ili registracijom u narodnom registru stanovništva (National Population Registar), sastoji se od 11 znamenki. Prvih šest znamenki predstavlja datum rođenja u formatu DDMMGG. Sljedeće tri znamenke su osobni broj koji se odabire iz određene serije brojeva ovisno o stoljeću rođenja. Osobama rođenim između 1854. i 1899. dodjeljuje se troznamenkasti broj iz serije $749-500$, osobama rođenim između 1900. i 1999. iz serije $499-000$, a rođenim između 1940. i 1999. iz serije $999-900$. Također brojevi iz serije $999-900$ koriste se i za posebne namjene, kao što su posvojenja iz inozemstva i imigratni. Zadnja skupina su osobe rođene između 2000. i 2039. godine te im se dodijeljuju brojevi iz serije $999-500$. Treća znamenka u osobnom broju predstavlja spol. Neparni brojevi su rezervirani za osobe muškog spola, a parni brojevi za osobe ženskog spola.
Na primjer, osoba kojoj nacionalni identifikacijski broj počinje s deveteroznamenkastim brojem 040180551 je muškog spola i rođena je 04.01.1880.

Posljednje dvije znamenke jedanesteroznamenkastog identifikacijskog broja $d_1d_2...d_{11}$ su kontrolne znamenke i definirane su na sljedeći način:

$$d_{10} \equiv -(d_1, d_2, ..., d_9) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11}$$
$$d_{11} \equiv -(d_1, d_2, ..., d_{10}) \cdot (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \pmod{11}.$$

Ako je d_{10} ili d_{11} jednak 10, identifikacijski broj je nevažeći i odbacuje se.

Posljednjih 5 znamenki (osobni broj plus kontrolne znamenke) nacionalnog identifikacijskog broja čine osobni identifikacijski broj.

Sljedeći primjer ilustrira ovu shemu.

Primjer 3.15.
Identifikacijski broj u Norveškoj počinje s 040180551. *Potrebno je izračunati dvije kontrolne znamenke koje treba dodijeliti tom broju.*

Imamo

$$\begin{aligned} d_{10} &\equiv -(d_1, d_2, ..., d_9) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11} \\ &\equiv -(0, 4, 0, 1, 8, 0, 5, 5, 1) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11} \\ &\equiv -(0 + 28 + 0 + 1 + 64 + 0 + 20 + 25 + 2) \pmod{11} \\ &\equiv -140 \equiv 3 \pmod{11}. \end{aligned}$$

Sada, kada znamo prvu kontrolnu znamenku pomoću nje možemo izračunati i drugu kontrolnu znamenku.

Imamo

$$\begin{aligned} d_{11} &\equiv -(d_1, d_2, ..., d_{10}) \cdot (5,4,3,2,7,6,5,4,3,2) \pmod{11} \\ &\equiv -(0,4,0,1,8,0,5,5,1,3) \cdot (5,4,3,2,7,6,5,4,3,2) \pmod{11} \\ &\equiv -(0+16+0+2+56+0+25+20+3+6) \pmod{11} \\ &\equiv -128 \equiv 4 \pmod{11}. \end{aligned}$$

Dakle, dvije kontrolne znamenke su 3 *i* 4. *Stoga, potpuni identifikacijski broj je* 04018055134.

Primjer 3.16.
Potrebno je provjeriti je li norveški identifikacijski broj 04566220625 *ispravan.*

Primijetimo da su dvije kontrolne znamenke u registracijskom broju 2 *i* 5.
Sada je

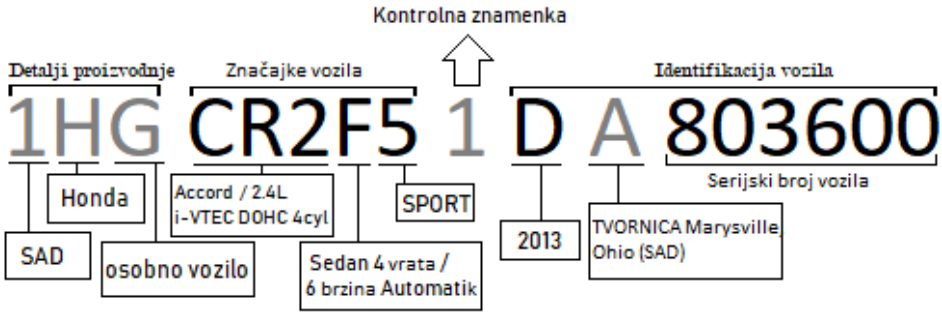
$$\begin{aligned} d_{10} &\equiv -(d_1, d_2, ..., d_9) \cdot (3,7,6,1,8,9,4,5,2) \pmod{11} \\ &\equiv -(0,4,5,6,6,2,2,0,6) \cdot (3,7,6,1,8,9,4,5,2) \pmod{11} \\ &\equiv -(0+28+30+6+48+18+8+0+12) \pmod{11} \\ &\equiv -150 \equiv 4 \pmod{11}. \end{aligned}$$

Identifikacijski broj 04566220625 *nije valjan jer prva kontrolna znamenka* d_{10} *u danom broju nije kongruentna s* 4 *modulo* 11.

3.8 Identifikacijski broj vozila

Identifikacijski broj vozila VIN (akronim od eng. Vehile Identification Number) ili broj šasije koristi proizvođač vozila za identificiranje vozila. VIN služi kao "otisak prsta" vozila budući da dva prodana vozila u prometu nemaju isti VIN. VIN je koristan za praćenje povijesti vozila, provjeru vlasništva vozila i trenutnog statusa vozila. VIN sa 17 alfanumeričkih znakova, koji ne uključuje slova I, O, Q (kako bi se izbjeglo brkanje s brojevima 0 i 1), počinje se upotrebljavati za obilježavanje automobila i kamiona koji su proizvedeni nakon 1981. Od 1954. do 1981. godine za VIN brojeve nije bilo prihvaćenih standarda, pa su različiti proizvođači koristili različite formate u kojima je VIN varirao u duljini od 11 do 17 znakova.
VIN pruža specifične i važne informacije o vozilu te svako slovo ili znamenka u VIN broju ima određenu svrhu. Ako izuzmemo kontrolnu znamenku, VIN možemo podijeliti u tri osnovne skupine. Prva skupina (prva tri znaka) sadrži pojedinosti o proizvodnji vozila (zemlja proizvodnje vozila, proizvođač, vrsta vozila). Sljedeća skupina od 5 znakova sadrži informacije o značajkama vozila kao što su marka vozila, model vozila, linija vozila, veličina i tip motora, tip karoserije, sustav prijenosa, serija vozila, sigurnosni sustav. Deveti znak se nalazi u sredini identifikacijskog broja i rezerviran je za kontrolnu znamenku. Zadnja skupina od posljednjih 8 znakova služi za identifikaciju vozila. U zadnjoj skupini nalazi se deseti znak koji označava godinu modela vozila, jedanaesti znak označava kôd tvornice koja je sastavila vozilo, a zadnjih 6 znamenki odnosi se na serijski broj vozila.

Slika 3.7



Primijetimo da za razliku od kontrolnih znamenki u shemama kojima smo se bavili ranije, kontrolna znamenka u VIN nije dodana na kraj identifikacijskog broja, nego je smještena u sredini.

Za određivanje kontrolne znamenke d_9, koristiti ćemo sljedeći algoritam:

Algoritam 3.2.
Neka je $d_1d_2...d_{17}$ identifikacijski broj vozila koji sadrži 17 alfanumeričkih znakova.

1. *Pretvori slova A do Z u brojeve $1-9$, $1-9$, i $2-9$, redom (vidi tablicu 3.2). Zamjena slova koja se pojavljuju u VIN s njihovim numeričkim parovima i izbacivanje kontrolne znamenke d_9 nam daje 16-znamenkasti broj $d_1d_2...\not{d_9}...d_{17}$.*

A	B	C	D	E	F	G	H	N/A	J	K	L	M
1	2	3	4	5	6	7	8		1	2	3	4
N	N/A	P	N/A	R	S	T	U	V	W	X	Y	Z
5		7		9	2	3	4	5	6	7	8	9

Tablica 3.2

2. *Pridruži težine $8, 7, ..., 2, 10, 9, ..., 2$ pozicijama $d_1, ..., \not{d_9}, ..., d_{17}$, redom.*

3. *Izračunaj najmanji pozitivan ostatak*

$$r \equiv (d_1, d_2, ..., \not{d_9}, ..., d_{17}) \cdot (8, 7, ..., 2, 10, 8, ..., 2) \pmod{11}.$$

4. *Kontrolna znamenka je*

$$d_9 = \begin{cases} r, & ako\ 0 \leq r < 10 \\ X, & inače \end{cases}$$

Sljedeći primjer ilustrira ovaj algoritam.

Primjer 3.17.
Potrebno je odrediti kontrolnu znamenku u identifikacijskom broju $1HGCR2F5{-}DA803600$ *vozila Honda Accord.*

Prvo ćemo ukloniti kontrolnu znamenku u svrhu izračuna.
Zamjena slova, u identifikacijskom broju vozila, s njihovim numeričkim parovima daje sljedeće numeričke ekvivalente:

VIN	1	*H*	*G*	*C*	*R*	2	*F*	5	-	*D*	*A*	8	0	3	6	0	0
Numerički kod	1	8	7	3	9	2	6	5	-	4	1	8	0	3	6	0	0

Zatim, svakom numeričkom kodu pridružimo odgovarajuću težinu:

Numerički kod	1	8	7	3	9	2	6	5	-	4	1	8	0	3	6	0	0
Težine	8	7	6	5	4	3	2	10	-	9	8	7	6	5	4	3	2

Sada računamo težinsku sumu modulo 11*:*

$$\begin{aligned} s &= 1\cdot 8 + 8\cdot 7 + 7\cdot 6 + 3\cdot 5 + 9\cdot 4 + 2\cdot 3 + 6\cdot 2 + 5\cdot 10 + \\ &\quad + 4\cdot 9 + 1\cdot 8 + 8\cdot 7 + 0\cdot 6 + 3\cdot 5 + 6\cdot 4 + 0\cdot 3 + 0\cdot 2 \\ &\equiv 364 \pmod{11} \\ &\equiv 1 \pmod{11}. \end{aligned}$$

Budući da je $0 \leq 1 < 10$*, tražena kontrolna znamenka je* 1*, kao što je zahtjevano.*

Poglavlje IV

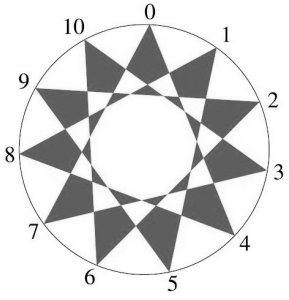
Modularni dizajni

Postoji uska veza između matematike i umjetnosti. Matematičari koriste kreativna sredstva kako bi definirali i istražili nove matematičke strukture. Umjetnici tragaju za oblicima na kojima će temeljiti nove slike. I jedni i drugi proučavaju razne pojave kako bi otkrili jedinstvene ili neobične uzorke i veze. Zbog toga nije neobično za umjetnike da primijenjuju matematičke strukture kao osnovu za generiranje zanimljivih dizajna. Kroz povijest, u različitim kulturama postoje primjeri ove jedinstvene veze između matematike i vizualnih umjetnosti. Umjetnici u antičkoj Grčkoj koristili su zlatni rez, takozvanu božansku proporciju, u stvaranju njihovih arhitektonskih dizajna i skulptura. Maori su generirali zamršene simetrične uzorke u đamijama. Tijekom renesanse, umjetnici poput Da Vincija, Michelangela i Tiziana su koristili matematičke strukture kao temelj za njihove izvrsne radove i umjetnine.
U ovom poglavlju, pokazati ćemo kako se teorija kongruencija može primjeniti za kreiranje interesantnih dizajna. Predstavit ćemo tri dizajna: zvijezdu s m krakova, (m, n) dizajn ostatka i quilt dizajn.

4.1 Zvijezda s m krakova

Kako bi konstruirali zvijezdu s m krakova, istakniti ćemo m jednako udaljenih točaka na kružnici i označiti ih s najmanjim ostacima $0, 1, ..., m-1$ modulo m. Zatim, izaberemo ostatak i modulo m takav da je $(i, m) = 1$. Svaku točku x spojimo s točkom $x+i$ modulo m. Obojimo različita područja unutar kružnice, koja su nastala spajanjem točaka na kružnici, s nekim jednobojnim bojama. Na kraju trebamo dobiti lijepu zvijezdu s m krakova.

Slika 4.1



Na slici 4.1 je prikazana zvijezda s 11 krakova koju smo dobili spajanjem svake točke x s točkom $x + 4$ modulo 11.

4.2 (m, n) dizajni ostatka

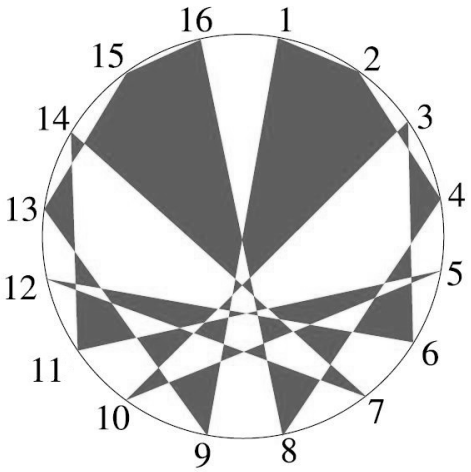
Pod nazivom (m, n) dizajn ostatka podrazumijeva se dizajn ostatka koji je konstruiran s modulom m i faktorom n koji je konstanta. Da bi konstruirali (m, n) dizajn ostatka, gdje je $1 \leq n < m$ i $(m, n) = 1$, istaknemo $m - 1$ jednako udaljenih točaka na kružnici i označimo ih brojevima $1, 2, ..., m - 1$. Zatim, spojimo svaku točku x s točkom nx modulo m. Nakon toga prostaje nam obojati dobivena područja unutar kružnice.

Konstukciju (m, n) dizajna ostatka je najprikladnije ilustrirati primjerom. Na primjer, da bi konstuirali $(17, 9)$ dizajn ostatka, podijelimo kružnicu na 16 jednakih lukova i označimo točke brojevima $1, 2, 3, \ldots, 16$. Zatim, pomnožimo svaki nenul ostatak s 9 modulo 17.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$9x \pmod{17}$	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8

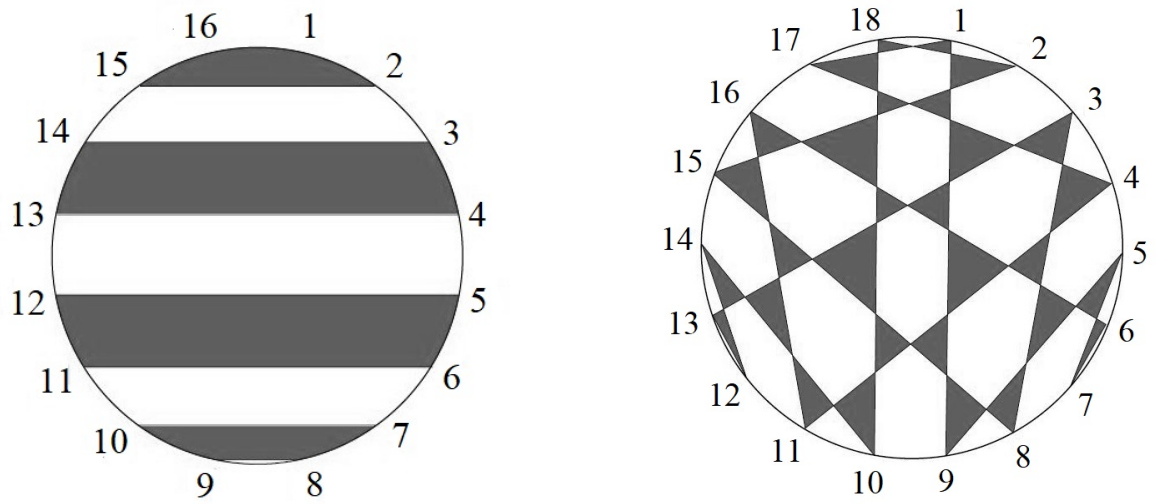
Nakon toga, spojimo svaku točku x s točkom $9x$ modulo 17. Dakle, spojimo točke 1 i 9, 2 i 1, 3 i 19, ..., 15 i 16, 16 i 8. Konačno, obojamo dobivena područja unutar kružnice kako bismo istakli dizajn. Dobiveni $(17, 9)$ dizajn ostatka možemo vidjeti na slici 4.2.

Slika 4.2



Još neki primjeri dizajna ostatka, kao što su $(17, 16)$ i $(19, 17)$, su prikazani na slici 4.3.

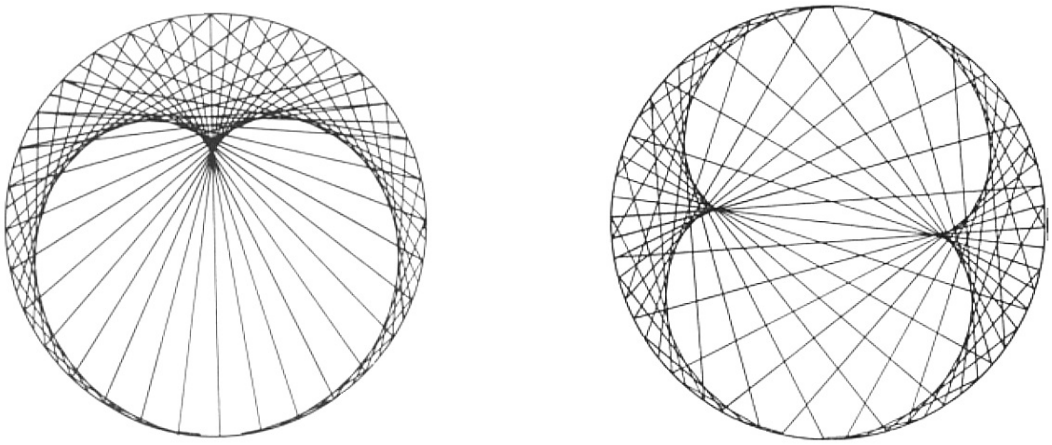
Slika 4.3



Možemo primijetiti da su svi $(m, m-1)$ dizajni linijskog oblika, kao i prvi dizajn na slici 4.3. Budući da vrijedi $m - 1 \equiv -1 \pmod{m}$, prema korolaru 1.5.2 slijedi da je $(m-1)x \equiv -x \pmod{m}$, a tetive su nacrtane između točaka x i $-x$ (što je isto što i $m - x$ modulo m).

Ponekad kreacije s istim modulom m, ali različitim odabirom n daju isti dizajn. Zapravo, dizajn $(19, 17)$ na slici 4.3 isti je kao i $(19, 9)$ dizajn ostatka. To je zato jer vrijedi $17 \cdot 9 \equiv 1 \pmod{19}$, odnosno jer 17 ima multiplikativni inverz modulo 19. Time se smanjuje ukupan broj različitih dizajna modulo m.

Slika 4.4



Kod dizajna $(65, 2)$ i $(65, 3)$, koji se nalaze na slici 4.4, motivacija za odabir modula 65 je činjenica da je 64 broj koji je potencija broja 2. Stoga je jednostavno, iako zamorna stvar, podijeliti kružnicu na 64 jednakih lukova. Primijetimo da nije moguće, a niti poželjno obojati takav dizajn. Možemo također primijetiti da ukoliko je m velik, a n mali broj tada takav (m, n) dizajn ostatka proizvodi unutar kružnice $n - 1$ "šiljak".

4.3 Quilt dizajni

Za kreiranje quilt dizajna koristiti ćemo tablice zbrajanja i množenja najmanjih ostataka modulo m. Ukoliko zamijenimo elemente iz tablice s kreativnim uzorcima i adekvatno smijestimo te uzorke u kvadratnu mrežu kreirati ćemo dizajn koji predstavlja tablicu zbrajanja ili množenja modulo m.

Kako bi kreirali ovakav dizajn izabrati ćemo m i konstruirati tablicu zbrajanja za skup ostataka $0, \ldots, m-1$ modulo m.
Na primjer, neka je $m = 8$. Konstruiramo tablicu zbrajanja za skup ostataka $0, 1, 2, 3, 4, 5, 6, 7$ modulo 8 kao što je prikazano u tablici 4.1.

$+$	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tablica 4.1

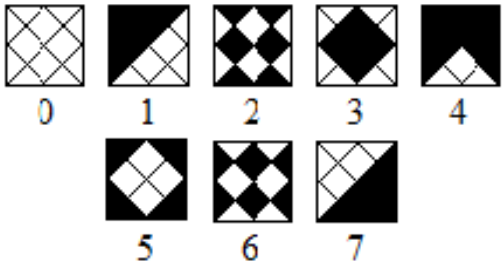
Sada, izaberemo osnovni oblik dizajna koji predstavlja ostatak 0 modulo m. Jedno od mnoštva mogućih izgleda osnovnog oblika dizajna, koji ćemo koristiti za naš primjer, pikazan je na slici 4.5.

Slika 4.5

Možemo osmisliti m osnovnih elemenata dizajna tako da obojamo ili osjenčamo osnovni oblik na različite načine kako bi ti elementi predstavljali svaki od brojeva $0, ..., m-1$.

Osam odabranih osnovnih elemenata dizajna, koji predstavljaju svaki od brojeva $0, 1, 2, 3, 4, 5, 6, 7$, su prikazani na slici 4.6.

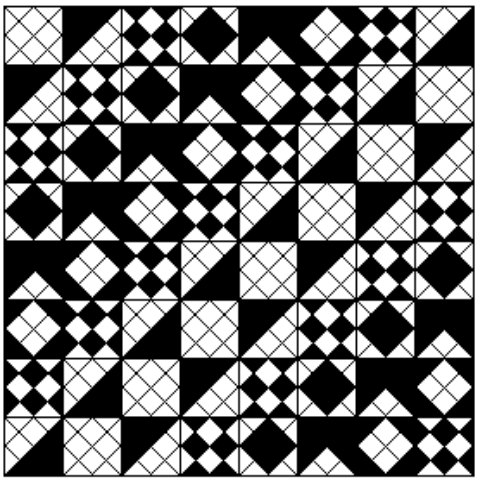
Slika 4.6



Prikazi brojeva su odabrani s obzirom na činjenicu da svaki broj ima aditivni inverz. Oblici su dodijeljeni brojevima $1, 2, 3, 4, 5, 6$ i 7 tako da su aditivni inverzi predstavljeni komplementarnim oblicima.

Sada, jednostavno zamijenimo svaki broj u tablici 4.1 s odgovarajućim elementom dizajna. Dizajn prikazan na slici 4.7 predstavlja tablicu zbrajanja modulo 8.

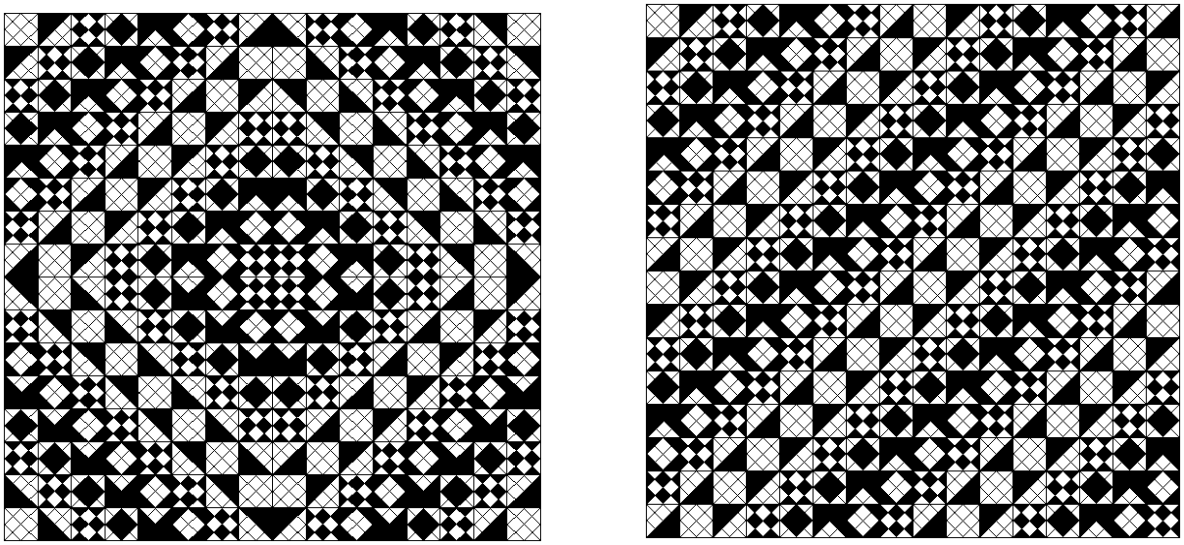
Slika 4.7



Mreža u kojoj se pojavio uzorak se naziva standardna ili kvadratna mreža (sva polja su jednaka).

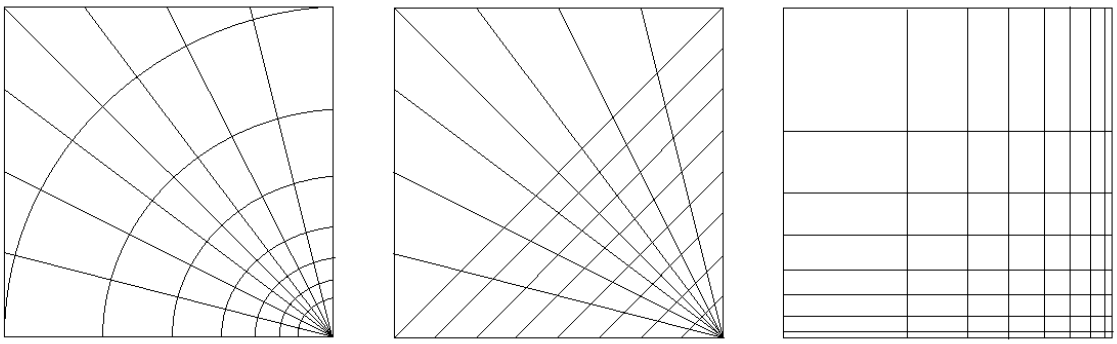
Dobiveni dizajn je osnovni dizajn koji može biti proširen na nekoliko načina kako bi proizveli druge zanimljive dizajne.
Na primjer, ako preslikamo osnovni dizajn na slici 4.7 u donosu na vertikalnu liniju i zatim preslikamo dobiveni dizajn u odnosu na horizontalnu liniju, proizvesti ćemo interesantan dizajn koji je prikazan na slici 4.8. Drugi dizajn na istoj slici dobiven je ponavljanjem osnovnog dizajna četiri puta.

Slika 4.8



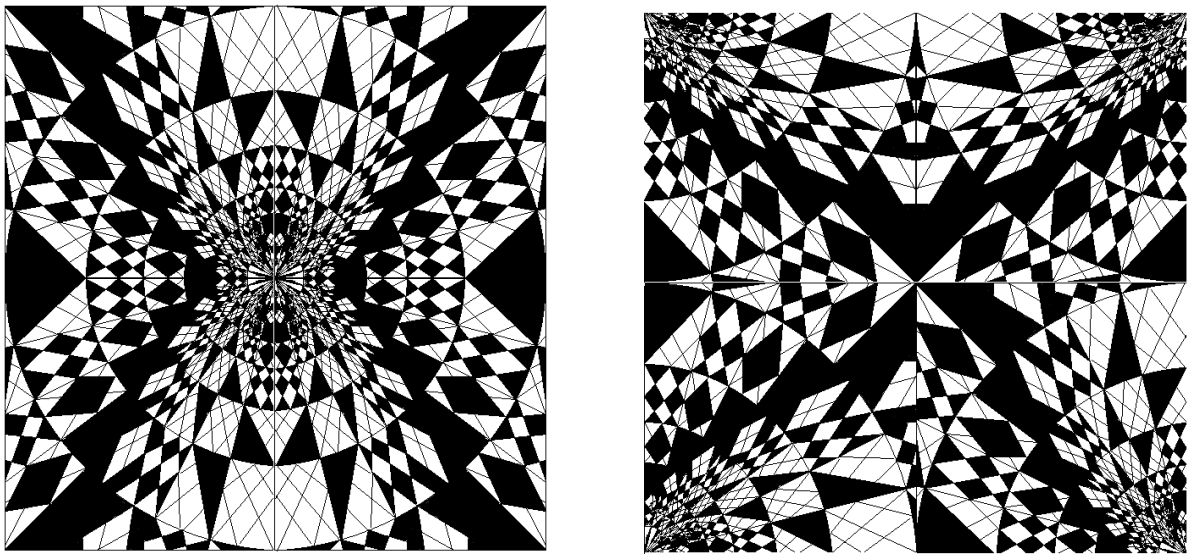
Interesantan efekt se može postići i ako umjesto standardne kvadratne mreže iskoristimo i neke druge mreže. Nekoliko primjera različitih mreža možemo vidjeti na slici 4.9.

Slika 4.9



Primjerice, ukoliko osnovne elemente dizajna sa slike 4.6 umjesto u standardnu mrežu smjestimo u prvu mrežu prikazanu na slici 4.9, a nakon toga i proširimo dobiveni osnovni dizajn preslikavanjem ili rotacijom, dobivamo prekrasne dizajne prikazane na slici 4.10.

Slika 4.10



Poglavlje V

Problem p-kraljica

Problem n-kraljica je klasičan i dobro poznat problem koji se primjenjuje u matematici, ali i u računarstvu kao izvrstan primjer za ilustriranje i pojašnjavanje algoritama unatražnog pretraživanja. Problem n-kraljica se temelji na pravilima šahovske igre, a cilj je smjestiti n kraljica na $n \times n$ šahovsku ploču tako da se nikoje dvije kraljice međusobno ne napadaju. U šahu, kraljica može napadati horizontalno, vertikalno i dijagonalno. Prema tome, pronašli smo sva moguća rješenja problema ukoliko pokažemo da se dvije kraljice ne nalaze u istom stupcu, retku ili na istoj dijagonali. Rješenje problema n-kraljica postoji za svaki pozitivan cijeli broj n veći od 3.

U ovom dijelu rada, primjenom kongruencija, razvit ćemo formulu za uspješno smještanje p kraljica na $p \times p$ šahovsku ploču, gdje je p prost broj veći od 3.

Kako bi predstavili formulu za rješavanje problema p-kraljica, stavljamo kraljice na šahovsku ploču redak po redak. Neka $f(i)$ označava položaj (indeks stupca) i-te kraljice, gdje je $1 \leq i \leq p$. Tada, $f(i)$ je definiran sljedećom rekurzivnom formulom:

$$\begin{aligned} &f(0) = 0 \\ &f(i) \equiv f(i-1) + \frac{p+1}{2} \pmod{p}, \qquad 1 \leq i \leq p-1 \\ &f(p) = p. \end{aligned} \tag{5.1}$$

Pomoću metode iteracije, možemo upotrijebiti formulu (5.1) kako bi dobili sljedeću eksplicitnu formulu za $f(i)$:

$$f(i) = \left(\frac{p+1}{2}\right) i \pmod{p}, \qquad \text{ako } 1 \leq i \leq p. \tag{5.2}$$

Ovdje je $f(i)$ najmanji ostatak pri dijeljenju $(p+1)i/2$ s p, gdje je ostatak 0 modulo p prikazan kao p.

Teorem 5.1. *Funkcija f je injektivna.*

Dokaz.
Neka su i i j najmanji nenegativni ostaci modulo p takvi da je

$$f(i) = f(j).$$

Prema (5.2), imamo

$$\left(\frac{p+1}{2}\right) i \equiv \left(\frac{p+1}{2}\right) j \pmod{p}.$$

Budući da $((p+1)/2, p) = 1$, prema teoremu 1.7 slijedi da je $i \equiv j \pmod{p}$.
Kako su i i j najmanji nenegativni ostaci modulo p, slijedi da je $i = j$.
Dakle, funkcija f je injektivna.

□

Ovim teoremom smo pokazali da funkcija f pridružuje točno jednu kraljicu svakom retku i svakom stupcu, kao što je prikazano u tablici 5.1 za $p = 5$.

i \ j	1	2	3	4	5
1	.	.	Q	.	.
2	Q	.	.	.	.
3	.	.	.	Q	.
4	.	Q	.	.	.
5	.	.	.	.	Q

Tablica 5.1

Sada možemo pokazati da se nikoje dvije kraljice, smještene na $p \times p$ šahovsku ploču prethodnom raspodjelom, međusobno ne napadaju.

Teorem 5.2. *Nikoje dvije kraljice, smještene na $p \times p$ šahovsku ploču prema raspodjeli f, se međusobno ne napadaju.*

Dokaz.
Budući da svaki redak i svaki stupac sadrži točno jednu kraljicu, nikoje dvije kraljice se međusobno ne napadaju duž retka ili stupca. Prema tome, da bi dokazali tvrdnju teorema dovoljno je dokazati da se nikoje dvije kraljice međusobno ne napadaju ni duž bilo koje jugoistočne ili sjeveroistočne dijagonale.

Za svaku sjeveroistočnu dijagonalu suma, $i+j$, indeksa retka i i indeksa stupca j je konstanta k, gdje je $2 \leq k \leq 2p$. Jasno je da trebamo promatrati samo dijagonale gdje je $3 \leq k \leq 2p-1$, budući da dijagonale s jednim poljem zasigurno ne sadrže dvije kraljice.

Pretpostavimo da na sjeveroistočnoj dijagonali postoje dvije takve kraljice na položajima (i_1, j_1) i (i_2, j_2). Prema (5.2) imamo

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p}$$
$$f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}.$$

Odnosno,

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \text{ i } j_2 \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}, \tag{5.3}$$

gdje je $i_1 + j_1 = k = i_2 + j_2$. Tada

$$i_1 + j_1 \equiv i_1 + \left(\frac{p+1}{2}\right) i_1 \equiv \left(\frac{p+3}{2}\right) i_1 \pmod{p}.$$

Odnosno,

$$k \equiv \left(\frac{p+3}{2}\right) i_1 \pmod{p}. \tag{5.4}$$

Slično se dobije da je

$$k \equiv \left(\frac{p+3}{2}\right) i_2 \pmod{p}. \tag{5.5}$$

Kongruencije (5.4) i (5.5) impliciraju da je $(p+3)i_1/2 \equiv (p+3)i_2/2 \pmod{p}$.
Budući da je $(p, (p+3)/2) = 1$, prema teoremu 1.7 slijedi da je $i_1 \equiv i_2 \pmod{p}$.
Prema tome, $i_1 = i_2$ jer su i_1 i i_2 najmanji nenegativni ostaci modulo p.
Tada, prema kongruencijama (5.3), $j_1 = j_2$.
Dakle, sjeveroistočna dijagonala ne sadrži dvije kraljice.

Sada ćemo pokazali da jugoistočna dijagonala ne sadrži dvije kraljice.
Prvo, primijetimo da za svaku takvu dijagonalu razlika, $i-j$, indeksa retka i i indeksa stupca j je konstanta l, gdje je $1-p \leq l \leq p-1$. Očito, trebamo promatrati samo dijagonale gdje je $1-p < l < p-1$.

Sada, pretpostavimo da jugoistočna dijagonala sadrži dvije kraljice na položajima (i_1, j_1) i (i_2, j_2). Tada, prema (5.2) imamo

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p}$$
$$f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}.$$

Odnosno,

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \text{ i } j_2 \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}, \tag{5.6}$$

gdje je $i_1 - j_1 = l = i_2 - j_2$. Tada

$$i_1 - j_1 \equiv i_1 - \left(\frac{p+1}{2}\right) i_1 \equiv \left(\frac{1-p}{2}\right) i_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p}.$$

Odnosno,

$$l \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p}. \tag{5.7}$$

Slično se dobije da je

$$l \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}. \tag{5.8}$$

Kongruencije (5.7) i (5.8) impliciraju da je $(p+1)i_1/2 \equiv (p+1)i_2/2 \pmod{p}$.
Budući da je $(p, (p+1)/2) = 1$, prema teoremu 1.7 slijedi da je $i_1 \equiv i_2 \pmod{p}$.
Prema tome, $i_1 = i_2$ jer su i_1 i i_2 najmanji nenegativni ostaci modulo p.
Tada, prema kongruencijama (5.6), $j_1 = j_2$.
Stoga, jugoistočna dijagonala ne sadrži dvije kraljice.

Prema tome, nikoje dvije kraljice, na $p \times p$ šahovskoj ploči, se međusobno ne napadaju. □

Na kraju, uvesti ćemo algoritam za smještanje p kraljica, redak po redak, na $p \times p$ šahovsku ploču.

Algoritam 5.1.

(1) Postavi prvu kraljicu u prvo polje stupca $(p+1)/2$.

(2) U svakom sljedećem retku, ciklički se pomiči udesno za $(p+1)/2$ *polja i postavi kraljicu u dobiveno polje.*

(3) Nastavi na ovaj način sve dok u svaki redak nije smještena jedna kraljica.

Poglavlje VI

Raspored turnira

Kongruencije se mogu primjeniti za konstruiranje rasporeda susreta u turniru u kojem natjecatelji igraju po principu "svaki sa svakim" (Round-Robin Tournaments). Takav način izrade rasporeda susreta se često primjenjuje pri organizaciji sportskih natjecanja. U ovom poglavlju, pokazat ćemo kako napraviti raspored susreta u turniru koji se sastoji od n timova, označenih brojevima $1, 2, 3, ..., n$, tako da svaki tim igra sa svakim drugim timom točno jednom. Primijetimo, ukoliko imamo neparan broj timova tada se ne mogu, u svakom krugu, svi timovi međusobno upariti. No, ukoliko bi svi timovi bili međusobno upareni, ukupan broj timova koji igraju na turniru bi bio paran. Stoga, ako je n neparan, možemo dodati fiktivni tim tako da tim koji je uparen s fiktivnim timom u određenom krugu nema protivnika i automatski dobiva slobodan prolaz u sljedeći krug. Stoga, možemo pretpostaviti da uvijek imamo paran broj timova, s dodatnim fiktivnim timom ukoliko je potrebno.

Neka g_n označava broj susreta u turniru koji se sastoji od n timova. Tada je g_n definiran sljedećom rekurzivnom formulom:

$$\begin{aligned} g_1 &= 0 \\ g_n &= g_{n-1} + (n-1), \quad n \geq 2. \end{aligned} \tag{6.1}$$

Rješavanjem (6.1) dobivamo

$$g_n = 0 + [1 + 2 + ... + (n-1)]$$

$$g_n = \frac{n(n-1)}{2} = \binom{n}{2}.$$

Na primjer, u natjecanju u kojem sudjeluje 5 timova održati će se $g_5 = \frac{5(5-1)}{2} = 10$ susreta.

Sada, možemo napraviti raspored susreta u turniru koji se sastoji od p timova, gdje je p prost broj veći od 2.
Neka $g(i,t)$ označava označava tim koji igra u krugu i s timom t. Ako je $g(i,t) = t$, onda tim t ne igra u krugu i i dobiva slobodan prolaz u sljedeći krug. Definiramo g kao što slijedi:

$$g(i,t) \equiv i - t \pmod{p}, \tag{6.2}$$

gdje je namanji ostatak 0 modulo p prikazan kao p.
Na primjer, neka je $n = 5$. Tada $g(1,1) \equiv 0 \pmod 5$, odnosno $g(1,1) = 5$. Slično, $g(2,3) \equiv -1 \pmod 5$, pa je $g(2,3) = 4$, itd.

Pokazati ćemo da g konstruira raspored susreta u turniru koji se sastoji od p timova. Prvo, moramo dokazati sljedeća tri teorema.

Teorem 6.1. *Točno jedan tim je slobodan u svakom krugu turnira.*

Dokaz.
Pretpostavimo da dva tima, t_1 i t_2, ne igraju u krugu i. Tada je

$$g(i,t_1) \equiv t_1 \pmod p \text{ i } g(i,t_2) \equiv t_2 \pmod p.$$

Imamo sljedeća dva slučaja.
Prvi slučaj: Ako je $i = t_1$, prema (6.2) imamo $g(i,t_1) \equiv i - t_1 \equiv 0 \equiv p \pmod p$. Odnosno, $i = t_1 = p$.
Zbog $g(i,t_2) \equiv t_2 \pmod p$, (6.2) i $i = p$, slijedi da je $i - t_2 \equiv p - t_2 \equiv t_2 \pmod p$. Tada, prema teoremima 1.2 i 1.7 slijedi da je

$$\begin{aligned} 2t_2 &\equiv 0 \pmod p \\ t_2 &\equiv 0 \equiv p \pmod p. \end{aligned}$$

Dakle, $t_2 = p$. Odnosno, $t_1 = t_2$.
Drugi slučaj: Ako $i \neq t_1$, tada prema (6.2) i pretpostavci dokaza imamo $g(i,t_1) \equiv i - t_1 \equiv t_1 \pmod p$. Odnosno, $i \equiv 2t_1 \pmod p$.

- Ako $i = t_2$, onda je $g(i,t_2) \equiv t_2 \equiv i \pmod p$ i $g(i,t_2) \equiv t_2 - t_2 \equiv p \pmod p$. Sada je

  $$\begin{aligned} i &\equiv p \pmod p \\ 2t_1 &\equiv 0 \pmod p \\ t_1 &\equiv 0 \equiv p \pmod p. \end{aligned}$$

  Odnosno, $t_1 = p$. Tada $i \equiv 2t_1 \equiv 2p \equiv 0 \pmod p$, pa je $i = p$. Stoga, $i = t_1$, što je u kontradikciji s pretpostavkom da su i i t_1 različiti.

- Ako $i \neq t_2$, tada tada prema (6.2) i pretpostavci dokaza imamo $g(i,t_2) \equiv i - t_2 \equiv t_2 \pmod p$. Odnosno, $i \equiv 2t_2 \pmod p$. Kako je $i \equiv 2t_1 \pmod p$ i prema teoremu 1.7 slijedi da je

  $$\begin{aligned} 2t_1 &\equiv 2t_2 \pmod p \\ t_1 &\equiv t_2 \pmod p. \end{aligned}$$

  Stoga, $t_1 = t_2$, budući da su t_1 i t_2 najmanji nenegativni ostaci modulo p.

Prema tome, vidimo da je u oba slučaja $t_1 = t_2$, pa možemo zaključiti da u svakom krugu turnira točno jedan tim ne igra i dobiva prolaz u sljedeći krug turnira.

□

Sljedećim ćemo teoremom identificirati tim koji je slobodan u pojedinom krugu turnira.

Teorem 6.2. *$g(i,t) \equiv t \pmod{p}$ ako i samo ako $t \equiv \left(\frac{p+1}{2}\right) i \pmod{p}$.*

Dokaz.
Pretpostavimo da je $g(i,t) \equiv t \pmod{p}$.

- Ako je $i = t$, tada prema definciji (6.2) od g je $g(i,t) \equiv 0 \equiv p \pmod{p}$. Odnosno, $i \equiv t \equiv p \equiv 0 \pmod{p}$. Prema tome,

$$t \equiv \left(\frac{p+1}{2}\right) i \pmod{p}.$$

- Ako, $i \neq t$, onda prema (6.2) je $g(i,t) \equiv i - t \pmod{p}$. Tada

$$\begin{aligned} i - t &\equiv t \pmod{p} \\ i &\equiv 2t \pmod{p}. \end{aligned}$$

  Prema tome, $(p+1)i/2 \equiv (p+1)2t/2 \equiv pt + t \equiv t \pmod{p}$. Odnosno,

$$t \equiv \left(\frac{p+1}{2}\right) i \pmod{p}.$$

Dakle, u oba slučaja, tim t ne igra u krugu i ako $t \equiv (p+1)i/2 \pmod{p}$.
Obratno, pretpostavimo da je $t \equiv (p+1)i/2 \pmod{p}$. Tada prema (6.2) od g je

$$\begin{aligned} g(i,t) &\equiv i - t \pmod{p} \\ &\equiv i - (p+1)i/2 \equiv (1-p)i/2 \pmod{p} \\ &\equiv (p+1)i/2 \equiv t \pmod{p}. \end{aligned}$$

Dakle, tim t ne igra u krugu i.

□

Sljedeći teorem pokazuje da g raspoređuje svaki tim točno jednom u svaki krug. Odnosno, g daje svaku od vrijednosti $1, 2, ..., p$ točno jednom.

Teorem 6.3. *Za svaki fiksirani i je funkcija g injektivna ($t \mapsto g(i,t)$).*

Dokaz.
Pretpostavimo da je $g(i,t_1) = g(i,t_2)$. Tada prema (6.2) je $i - t_1 \equiv i - t_2 \pmod{p}$. Odnosno, zbog svojstva kongruencija iz teorema 1.7 je $t_1 \equiv t_2 \pmod{p}$. Prema tome, $t_1 = t_2$ i g je injektivna. □

Iz teorema 6.1, 6.2 i 6.3 slijedi da funkcija g jedinstveno određuje protivnika tima t u svakom krugu i, gdje je $1 \leq i,\ t \leq p$. U krugu i, gdje je $t \equiv (p+1)i/2 \pmod{p}$, tim t nema protivnika. Zanimljivo da je to zapravo ista vrijednost (5.2) koja je dobivena ranije za smještanje $i-te$ kraljice, gdje je $1 \leq i \leq p$. Dakle, oznaka "ne igra" za slobodan tim u krugu i se pojavljuje u tablici rasporeda susreta u turniru upravo u istom polju kao ono u kojem se pojavljuje i kraljica u retku i na $p \times p$ šahovskoj ploči. S ovim rezultatom možemo, pomoću funkcije g, izmjeniti algoritam za smještanje p-kraljica kako bi razvili algoritam za raspored turnira u kojem sudjeluje p timova, gdje je $p \geq 3$. Prva tri koraka će biti ista kao i u algoritmu za smještanje p-kraljica, osim što ćemo oznaku Q zamjeniti s oznakom "ne igra".

Algoritam 6.1.

(1) Postavi prvu oznaku "ne igra" u prvo polje stupaca $(p+1)/2$

(2) U svakom sljedećem retku, ciklički se pomiči udesno za $(p+1)/2$ *polja i postavi oznaku "ne igra" u dobiveno polje.*

(3) Nastavi na ovaj način sve dok u svaki redak nije smještena jedna oznaka "ne igra".

(4) Počevši s prvim poljem u retku 1, unesi brojeve $p, ..., 3, 2, 1$ *u prazna polja (tj. prekoči zauzeto polje u kojem se nalazi oznaka "ne igra") za dobivanje permutacije* $p, p-1, ..., "neigra", ..., 2, 1$.

(5) U svakom sljedećem retku, ciklički permutiraj udesno brojeve u prethodnom retku (uvijek preskoči oznaku "ne igra") i unesi ih u prazna polja.

Sada, pretpostavimo da broj timova n nije prost broj. Napraviti ćemo raspored turnira, uparivanjem timova na sljedeći način. Imamo, tim t_1, gdje je $t_1 \neq n$, igra s timom t_2, gdje je $t_2 \neq n$ i $t_1 \neq t_2$ u r-tom krugu ako je

$$t_1 + t_2 \equiv r \pmod{n-1}.$$

Na taj način se raspoređuju svi timovi u krugu r, osim tim n i jedan tim t za kojeg vrijedi da je

$$2t \equiv r \pmod{n-1}.$$

Postoji jedan takav tim jer nam korolar 1.10.1 kaže da linearna kongruencija $2t \equiv r \pmod{n-1}$, gdje je $1 \leq t \leq n-1$, ima jedinstveno rješenje t, budući da je $(2, n-1) = 1$. U tom slučaju uparujemo tim t s timom n u r-tom krugu.

Sada moramo pokazati da svaki tim igra sa svakim drugim timom točno jednom. Razmotrimo prvih $n-1$ timova. Primjetimo da tim t_1, gdje je $1 \leq t_1 \leq n-1$, igra s timom n u krugu r gdje je $2t_1 \equiv r \pmod{n-1}$ i to se događa točno jednom.
U drugim krugovima, tim t_1 ne igra s istim timom dva puta. Kada bi tim t_1 igrao s timom t_2 u dva različita kruga, r i r', tada bi $t_1 + t_2 \equiv r \pmod{n-1}$ i $t_1 + t_2 \equiv r' \pmod{n-1}$, što je očito kontradikcija jer $r \not\equiv r' \pmod{n-1}$. Odnosno, timovi t_1 i t_2 neće se susresti u dva različita kruga.
Stoga, budući da svaki od prvih $n-1$ timova igra $n-1$ utakmica i ne igra ni s jednim timom više od jednom, igra sa svakim timom točno jednom. Također, tim n igra $n-1$ igri i budući da svaki drugi tim igra s timom n točno jednom, tim n igra svakim drugim timom točno jednom.

Primjer 6.1.
Potrebno je izraditi raspored turnira s 5 *timova.*

Da bismo napravili raspored turnira s 5 *timova, koji su označeni brojevima* $1, 2, 3, 4$ *i* 5*, uključiti ćemo jedan dodatni fiktivni tim.*
Prvi krug:

- *Tim* 1 *igra s timom t, gdje je* $1 + t \equiv 1 \pmod{5}$. *Tada je* $t = 5$ *, pa tim* 1 *igra s timom* 5 *u prvom krugu.*

- *Timu* 2 *u prvom krugu je dodijeljen tim* 4*, budući da je* $t = 4$ *rješenje kongruencije* $2 + t \equiv 1 \pmod 5$.

- *Budući da je* $t = 3$ *rješenje kongruencije* $2t \equiv 1 \pmod 5$*, tim* 3 *je uparen s fiktivnim timom* 6*, odnosno tim* 3 *je slobodan u prvom krugu.*

Drugi krug:

- *Kako je* $t = 1$ *rješenje linearne kongruencije* $2t \equiv 2 \pmod 5$*, tim* 1 *je uparen s dodatnim šestim timom, odnosno u ovom krugu ne igra.*

- *Tim* 2 *igra s timom* t*, gdje je* $2 + t \equiv 2 \pmod 5$*. Tada je* $t = 5$*, pa tim* 2 *igra s timom* 5.

- *Budući da rješnje kongruencije* $3 + t \equiv 2 \pmod 5$ *je* $t = 4$*, tim* 3 *je uparen s timom* 4.

Ako nastavimo ovaj postupak i uparimo timove i u ostalim krugovima, završiti ćemo s parovima prikazanim u tablici 6.1, gdje protivnik tima i *u krugu* j *je dan u* j*-tom retku i* i*-tom stupcu.*

Krug \ Tim	1	2	3	4	5
1	5	4	”ne igra”	2	1
2	”ne igra”	5	4	3	2
3	2	1	5	”ne igra”	3
4	3	”ne igra”	1	5	4
5	4	3	2	1	”ne igra”

Tablica 6.1

Bibliografija

[1] M. Bruckheimer, R. Ofir, A. Arcavi: *The Case for and against "Casting Out Nines"*; For the Learning of Mathematics, 15 (1995), FLM Publishing Association, 23-28.

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

[3] A. Dujella: *Uvod u teoriju brojeva*; skripta, Prirodoslovno-matematički fakultet - Matematički odsjek, Sveučilište u Zagrebu, 2003, `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`.

[4] S. Forseth, A. Troutman: *Using Mathematical Structures to Generate Artistic designs*; The Mathematics Teacher, 67 (1974), 393-397.

[5] D.L. Herrmann, P.J. Sally Jr.: *Number, Shape, Symmetry: An Introduction to Number Theory, Geometry, and Group Theory*; CRC Press, 2012.

[6] T. Koshy: *Elementary Number Theory with Applications – 2nd ed.*; Academic Press, 2007.

[7] P. Locke: *Residue Designs*; The Mathematics Teacher, 65 (1972), 260-263.

[8] I. Matić: *Uvod u teoriju brojeva*; Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2015.

[9] K.H. Rosen: *Elementary Number Theory and Its Applications*; Addison-Wesley, Reading, 1993.

[10] M.L. Wheeler: *Check-Digit Schemes*; The Mathematics Teacher, 87 (1994), 228-230.

Sažetak

Glavni cilj ovog rada je predstaviti kongruencije i proučiti neke konkretne primjene kongruencija. Glavni dio rada podijeljen je u 6 poglavlja. U prvom poglavlju predstaviti ćemo kongruencije i razviti osnovna svojstva kongruencija. Osim toga, proučiti ćemo linearne kongruencije s jednom nepoznanicom te ćemo pokazati kako riješiti linearne kongruencije. Pomoću teorije kongruencija možemo razviti jednostavne kriterije za provjeru je li dani cijeli broj n djeljiv s cijelim brojem m. U drugom poglavlju ćemo razviti kriterije djeljivosti za 2^j, 5^j, 10, 3, 9, 11, 37 i $7, 11, 13$. Također ćemo demostrirati metode izbacivanja dvojki i izbacivanja devetki koje se koriste za otkrivanje pogreški u rezultatima računskih operacija. Uvesti ćemo pojam digitalnog korijena koji je usko povezan s metodom izbacivanja devetki. U trećem poglavlju ćemo vidjeti kako se pomoću kongruencija mogu otkriti i ispraviti pogreške u decimalnim stringovima koji se koriste za identifikaciju knjiga, proizvoda, pošiljki i drugih informacija te vrste. Pomoću teorije kongruencija možemo generirati umjetničke i zanimljive dizajne. U četvrtom poglavlju istražujemo tri takva dizajna: zvijezdu s m krakova, (m, n) dizajn ostatka i quilt dizajn. U petom poglavlju razvijamo formulu za uspješno smještanje p kraljica na $p \times p$ šahovsku ploču tako da se nikoje dvije kraljice međusobno ne napadaju, gdje je p prost broj veći od 3. Kongruencije se mogu primjeniti i za konstruiranje rasporeda susreta u turniru u kojem natjecatelji igraju po principu "svaki sa svakim". U zadnjem poglavlju, pokazati ćemo kako konstrurati raspored susreta u turniru za n različitih timova.

Ključne riječi:
kongruencije, linearne kongruencije, ispitivanje dijeljivosti, izbacivanje devetki, izbacivanje dvojki, digitalni korijen, kontrolne znamenke, modularni dizajni, quilt dizajn, (m, n) dizajn ostatka, zvijezda s m krakova, problem p-kraljica, raspored turnira.

Title and summary

Applications of Congruences

The main goals of this paper are to introduce congruences, and to study some concrete applications of congruences. The main part of this paper is divided into six chapters. In the first chapter we will introduce congruences and develop their fundamental properties. We will also study a linear congruences with one unknown and describe some methods for solving linear congruences. The theory of congruences can be used to develop simple tests for checking whether a given integer n is divisible by an integer m. In the second chapter we will develop divisibility tests for 2^j, 5^j, 10, 3, 9, 11, 37 and $7, 11, 13$. We will also demonstrate two techniques called casting out nines and casting out twos. These techniques can be used to detect computational errors. We will introduce the concept of the digital root of a positive integer N which is closely related to casting out nines. In the third chapter we will see how congruences are used to detect and correct errors in strings of decimal digits used in identfications of books, products, mails and other information of this type. The theory of congruences can be used to generate artistic and interesting designs. In fourth chapter we explore three such designs: m-pointed star, (m, n) residue design, and quilt design. In fifth chapter we develop a formula for successfully placing p queens on a $p \times p$ chessboard in such a way that no two queens can attack each other, where p is a prime > 3. Congruences can be applied to schedule round-robin tournaments. In the last chapter, we will show how to schedule a tournament for n different teams.

Keywords:
congruence, linear congruence, divisibility tests, casting out nines, casting out twos, digital root, check digits schemes, modular designs, quilt design, m-pointed star, (m, n) residue design, the p-queens problem, round-robin tournaments.

Životopis

Suzana Paripović rođena je 11. prosinca 1989. godine u Vinkovcima. Pohađala je Osnovnu školu Ivana Kozarca Županja te je nakon završetka osnovne škole upisala Prirodoslovno-matematičku gimnaziju u Gimnaziji Županja. Daljnje obrazovanje nastavlja na Odjelu za matematiku Sveučilišta Josipa Jurja Strossmayera u Osijeku. Prvotno upisuje petogodišnji Sveučilišni nastavnički studij matematike i informatike, ali tijekom studija se preusmjerava na Sveučilišni preddiplomski studij matematike te studij završava izradom rada na temu *Hermitski operatori* pod vodstvom mentora izv. prof. dr. sc. Ivana Matića i stječe akademski naziv *sveučilišna prvostupnica (baccalaurea) matematike*. Nakon toga upisuje Sveučilišni diplomski studij matematike, smjer Matematika i računarstvo, na istom fakultetu. Tijekom studiranja daje poduke iz područja matematike i informatike, obavlja razne studentske poslove te stječe radno iskustvo u Osnovnoj školi Lug kao učiteljica matematike. Tijekom završne godine diplomskog studija stječe praktična znanja u tvrtki *Adacta d.o.o Zagreb*.