Neke primjene kongruencija

Matić, Anja

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Anja Matić

NEKE PRIMJENE KONGRUENCIJA

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Zrinka Franušić

Zagreb, srpanj, 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad posvećujem svojoj majci kojoj ujedno veliko hvala što je uvijek vjerovala u mene. Hvala ti mama jer bez tvoje ljubavi i podrške ni jedan moj uspjeh ne bi bio mogući. Veliko hvala izv. prof. dr. sc. Zrinki Franušić za pomoć pri izradi i pisanju diplomskog rada. Hvala Vam što ste uvijek našli vremena i imali strpljenja za mene.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Sadržaj **iv**

Uvod **2**

1 Kongruencije **3**
1.1 Definicija . . . 3
1.2 Osnovna svojstva . . . 4
1.3 Linearne kongruencije . . . 5
1.4 Eulerova funkcija . . . 7

2 Primjene kongruencija **10**
2.1 Identifikacijske znamenke . . . 10
2.1.1 ISBN . . . 10
2.1.2 UPC . . . 11
2.1.3 Broj vozačke dozvole . . . 12
2.1.4 Identifikacijski broj vozila . . . 13
2.1.5 Luhnova formula . . . 14
2.2 Djeljivost . . . 15
2.2.1 Testovi djeljivosti . . . 15
2.2.2 Odbacivanje devetki . . . 18
2.2.3 Digitalni korijen . . . 19
2.3 Kalendar . . . 21
2.3.1 Petak 13. . . . 21
2.3.2 Gregorijanski kalendar . . . 23
2.4 Igre . . . 28
2.4.1 Problem kraljica na šahovskoj ploči . . . 28
2.4.2 Održavanje turnira . . . 32
2.5 Dizajni . . . 35
2.5.1 Zvijezda s m vrhova . . . 35
2.5.2 Dizajn ostataka . . . 38

2.5.3 Quilt dizajn 40
2.6 Diofantske jednadžbe 42

Bibliografija **45**

Uvod

Teoriju kongruencija je 1801. godine u svom dijelu *Disquisitiones Arithmeticae* uveo Gauss. Johann Karl Friedrich Gauss(1777.-1855.) jedan je od najvećih matematičara svih vremena. Spomenuto djelo napisao je sa samo 24 godine te mu je isprva djelo bilo odbijeno. Tada je njemački matematičar Leopold Kronecker napisao: "Zaista je zapanjujuće pomisliti da tako mlad čovjek može donijeti toliko novih rezultata, a da pri tome sve rezultate prikaže tako organizirano i sustavno kao novu disciplinu." Osim što je utemeljio teoriju kongruencija Gauss je uveo i oznaku za kongruenciju koju i danas koristimo.

Relacija kongruencije jedna je od najznačajnijih relacija u teoriji brojeva. Kažemo da je *a kongruentan b* modulo m ako m dijeli $a - b$ i pišemo

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

U protivnom pišemo $a \not\equiv b \pmod{m}$, tj. *a nije kongruentan b* modulo m.

U prvom poglavlju ovog rada, osim definicije kongruencije, iskazana su i neka njezina osnovna svojstva te postupak rješavanja linearnih kongruencija. Definira se i Eulerova funkcija φ koja "broji" relativno proste brojeve u nizu $1, 2, \ldots, n$ s brojem n.

U drugom poglavlju prikazane su neke primjene kongruencija što u matematici tako i u svakodnevnom životu.

Kongruencije se tako primjenjuju za identifikaciju kontrolnih znamenaka. Do 2007. g. primjenjivao se deseteroznamenkasti ISBN pri čemu je zadnja znamenka bila kontrolna. Kontrolna znamenka d kod ISBN-a poprima vrijednosti iz skupa $\{0, 1, 2, \ldots, 10\}$ i definirana je kao

$$d \equiv -(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11}$$

pri čemu $x_1, \ldots, x_9$ označavaju prvih devet znamenki ISBN-a, a $\cdot$ je skalarno množenje na $\mathbb{R}^9$. Slične kongruencije se javljaju i kod identifikacije proizvoda. Svaki proizvod sadrži UPC kod kojeg je zadnja znamenka kontrolna pa i za njezino određivanje potrebna je kongruencija. Države poput Utaha, New Mexica i Norveške koriste kongruencije pri izdavanju vozačkih dozvola. Utah i New Mexico kongruencije koriste za

određivanje posljednje znamenka, a Norveška za određivanje posljednjih dviju znamenaka u broju vozačke dozvole. Također, svako vozilo posjeduje svoj identifikacijski broj pri čemu se kontrolna znamenka nalazi u sredini broja. Na većini bankovnih kartica nalazi se broj za čiju provjeru valjanosti se koristi Luhmanov algoritam koji se temelji na kongruenciji.

Svima poznati testovi djeljivosti s brojevima $5, 10, 5, 2^n, 3, 9$ i 11 lako se dobivaju pomoću kongruencija. Metoda odbacivanja devetki, koja služi za brzu provjeru jednostavnog računa, temelji se na činjenici da je svaki cijeli broj kongruentan zbroju znamenki modulo 9. Određivanje digitalnog korijena također je u direktnoj vezi s kongruencijama.

Kongruencije se mogu iskoristiti i pri određivanju broja "nesretnih" dana u godini, odnosno za određivanje u kojem mjesecu u godini će se desiti "petak 13-ti'". Kongruencijom

$$d_y^m \equiv 1 - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor + \lfloor 2.6m - 0.2 \rfloor \pmod 7$$

određuje se na koji dan pada prvi dan u m-tom mjesecu u nekoj godini y.

Kongruencije možemo primijeniti i na rješavanje nekih jednostavnih kombinatornih problema kao što je problem raspodjele kraljica na šahovskoj ploči tako da se one međusobno ne napadaju. Osim zabave i popularizacije matematike, problem je primjenjiv za izradu različitih poslovnih i vojnih strategija.

Kongruencije mogu pomoći i pri organizaciji turnira koji se temeljeni na takozvanom *Round Robin* principu; svaka ekipa mora odigrati točno jednu utakmicu sa svakom od preostalih ekipama. Organizacija takvog turnira temelji se na jednostavnoj kongruenciji

$$g(i, j) \equiv i - j \pmod p$$

pri čemu $g(i, j)$ označava tim koji u $i-tom$ kolu igra s timom j, a p je broj prijavljenih ekipa.

Primjenom kongruencija mogu se dobiti i predivni dizajni od kojih su najzanimljivije zvijezde s m vrhova. Takvi dizajni temelje se na nizu kongruencija

$$d \equiv x + i \pmod m$$

pri čemu su $d, i \in \{0, \ldots, m-1\}$ relativno prosti, a x prolazi skupom $\{0, \ldots, m-1\}$.

U matematici je poznata primjena kongruencija je pri rješavanju jednadžbi oblika

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

pri čemu su $a_1, \ldots, a_n, b \in \mathbb{Z}$ i $n > 0$. Takve jednadžbe nazivamo linearnim diofantskim jednadžbama. One imaju široku primjenu u problemima iz svakodnevnog života.

Poglavlje 1

Kongruencije

1.1 Definicija

Definicija 1.1.1. *Neka je $m \neq 0$ cijeli broj. Kažemo da je a* kongruentan *b modulo m ako m dijeli $a - b$ i pišemo $a \equiv b \pmod{m}$. U protivnom kažemo da a* nije kongruentan *b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Na primjer, $103 \equiv 3 \pmod{5}$ i $100 \not\equiv 0 \pmod{9}$.

U daljnjem tekstu ćemo pretpostavljati da je modul m prirodan broj jer ako $m \mid a - b$, onda i $-m \mid a - b$. Nadalje, ako je $a \equiv b \pmod{m}$, onda iz same definicije odmah slijedi da je $a = b + mk$ za neki $k \in \mathbb{Z}$. Stoga je skup svih cijelih brojeva koji su kongruentni a modulo m jednak

$$\{a + mk \,:\, k \in \mathbb{Z}\}.$$

Propozicija 1.1.2. *Neka je $m \in \mathbb{N}$ i $m > 1$. Svaki cijeli broj kongruentan je modulo m točno jednom broju iz skupa $\{0, 1, \ldots, m-1\}$.*

Prethodna propozicija direktna je posljedica sljedećeg važnog teorema.

Teorem 1.1.3 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je*

$$b = qa + r,$$

pri čemu je $0 \leqslant r < a$.

Inače, skup $\{0, 1, \ldots, m-1\}$ se naziva *skup najmanjih nenegativnih (potpunih) ostataka*, a o općem skupu potpunih ostataka bit će riječi nešto kasnije.

Propozicija 1.1.4. *Neka su $a, b \in \mathbb{Z}$ i $m \in \mathbb{N}$. Nadalje, neka su r i s ostatci pri dijeljenju brojeva a i b brojem m, respektivno. Tada je $a \equiv b \pmod{m}$ ako i samo ako je $r = s$.*

Dokaz. Iz Teorema 1.1.3 slijedi $a = mq + r$ i $b = mt + s$.
Ako je $a \equiv b \pmod{m}$ vrijedi $b = a + mk$, pri čemu je $k \in \mathbb{Z}$. Tada

$$b = mq + r + mk = m(q + k) + r.$$

S obzirom da je $0 \leqslant r < m$ prema Teoremu 1.1.3 slijedi da je r ostatak pri dijeljenju b s m. Također, ostatak pri dijeljenju je jedinstven pa slijedi $r = s$.

Obratno, ako je $r = s$, onda je $a - mq = b - mt$ tj. $a - b = m(q - t)$. Sada je očito da $a \equiv b \pmod{m}$. □

1.2 Osnovna svojstva

Propozicija 1.2.1. *Relacija "biti kongruentan modulo m" je relacija ekvivalencija na skupu $\mathbb{Z}$.*

Dokaz. Treba pokazati da vrijedi svojstva refleksivnosti, simetričnosti i tranzitivnosti.

- *Refleksivnost*: Iz $m|(a - a)$ slijedi $a \equiv a \pmod{m}$.
- *Simetričnost*: Ako je $a \equiv b \pmod{m}$ onda $m|(a - b)$ tj. $m| - (b - a)$. Prema tome $m|(b - a)$ iz čega slijedi $b \equiv a \pmod{m}$.
- *Tranzitivnost*: Ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ onda $m|(a-b)$ i $m|(b-c)$. Slijedi $m|[(a - b) + (b - c)]$ odnosno $m|(a - c)$ što povlači $a \equiv c \pmod{m}$.

□

Propozicija 1.2.2. *Neka su a, b, c i d cijeli brojevi i m prirodan.*

1. *Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ i $ac \equiv bd \pmod{m}$.*
2. *Ako je $a \equiv b \pmod{m}$ i $d \mid m$, onda je $a \equiv b \pmod{d}$.*
3. *Ako je $a \equiv b \pmod{m}$ i $c \neq 0$, onda je $ac \equiv bc \pmod{mc}$.*

Dokaz. 1. Ako $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ onda je $a = b + sm$ i $c = d + tm$. Zbrajanjem, odnosno oduzimanjem prethodnih jednakosti dobivamo $a \pm c = b \pm d + (s - t)m$ pa je $a \pm c \equiv b \pm d \pmod{m}$. Analogno, množenjem se dobiva $ac = bd + m(bt + sd + stm)$ iz čega slijedi da je $ac \equiv bd \pmod{m}$.

2. Ako je $a \equiv b \pmod{m}$ i $d \mid m$ onda je $a = b+sm$ i $m = dk$. Slijedi $a = b+d(sk)$ što povlači $a \equiv b \pmod{d}$.

3. Tvrdnja slijedi množenjem jednakosti $a = b + sm$ sa c.

□

Korolar 1.2.3. *Neka je $a \equiv b \pmod{m}$, te neka je f polinom sa cjelobrojnim koeficijentima. Tada je $f(a) \equiv f(b) \pmod{m}$. Specijalno, $a^n \equiv b^n \pmod{m}$, za svaki prirodan broj n.*

Najveći zajednički djelitelj cijelih brojeva a i b označavat ćemo s (a, b). Jasno je $(a, b) \geqslant 1$. Ako je $(a, b) = 1$, tada brojevi a i b nemaju zajedničkog djelitelja većeg od 1. Za njih kažemo da su *relativno prosti*.

Uočimo da ako je $(a, b) = d$, onda su brojevi $\frac{a}{d}$ i $\frac{b}{d}$ relativno prosti, tj. $(\frac{a}{d}, \frac{b}{d}) = 1$. Ta jednostavna činjenica često se koristi, između ostalog i u dokazu sljedećeg svojstva.

Propozicija 1.2.4. *Neka su $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, te $(c, m) = d$. Tada je $ac \equiv bc \pmod{m}$ ako i samo ako $a \equiv b \pmod{\frac{m}{d}}$.*

Dokaz. Ako je $ac \equiv bc \pmod{m}$, onda $ml = c(a - b)$. Vrijedi $\frac{m}{d}l = \frac{c}{d}(a - b)$ jer je $(c, m) = d$. Kako je $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$ slijedi da $\frac{m}{d} | a - b$, tj. $a \equiv b \pmod{\frac{m}{d}}$.

Obratno, ako je $a \equiv b \pmod{\frac{m}{d}}$, onda je $ac \equiv bc \pmod{\frac{mc}{d}}$ (prema svojstvu 3. iz Propozije 1.2.2). No, $\frac{mc}{d} = m\frac{c}{d}$ pa cijeli broj $\frac{c}{d}$ dijeli $\frac{mc}{d}$. Stoga je i $ac \equiv bc \pmod{m}$. □

Korolar 1.2.5. *Neka su $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, te $(c, m) = 1$. Tada je $ac \equiv bc \pmod{m}$ ako i samo ako $a \equiv b \pmod{m}$.*

1.3 Linearne kongruencije

Definicija 1.3.1. *Skup $\{a_1, \ldots, a_m\}$ se zove* potpuni sustav ostataka modulo m *ako za svaki cijeli broj b postoji točno jedan a_j, $j \in \{1, \ldots, m\}$, takav da je $b \equiv a_j \pmod{m}$.*

Prethodna definicija je dobra jer prema Propoziciji 1.1.4 očito je da broj elemenata potpunog sustava ostataka modulo m jednak m. Već smo spominjali skup $\{0, 1, \ldots, m-1\}$ koji predstavlja potpun sustav ostataka modulo m koji se sastoji od najmanjih nenegativnih brojeva. Sustav ostataka najmanjih po apsolutnoj vrijednosti je $\{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\}$ ako je m neparan, a $\{-\frac{m-2}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}\}$ ako je m paran.

Teorem 1.3.2. *Neka je $\{x_1, \ldots, x_m\}$ potpun sustav ostataka modulo m i $(a, m) = 1$. Tada je $\{ax_1, \ldots, ax_m\}$ također potpuni sustav ostataka.*

Dokaz. Tvrdnju ćemo dokazati ako ustanovimo da su svi elementi skupa $\{ax_1, \ldots, ax_m\}$ međusobno nekongruentni modulo m. Pretpostavimo suprotno, tj. da je $ax_i \equiv ax_j \pmod{m}$ za $1 \leqslant i < j \leqslant m$ pa je prema Korolaru 1.2.5 $x_i \equiv x_j \pmod{m}$ što je u kontradikciji s činjenicom da je $\{x_1, \ldots, x_m\}$ potpun sustav ostataka modulo m. □

U onom što slijedi rješavat ćemo *linearnu kongruenciju*

$$ax \equiv b \pmod{m} \tag{1.1}$$

za dane cijele brojeve a, b, m. Jasno, ako je neki $x_0 \in \mathbb{Z}$ rješenje kongruencije (1.1) onda će i svi brojevi oblika $x_0 + mk$, $k \in \mathbb{Z}$ zadovoljavati tu kongruenciju. Dakle, ako (1.1) ima rješenja u $\mathbb{Z}$, onda ih ima beskonačno puno. Ipak, pod pojmom *broja rješenja* kongruencije smatrat ćemo broj međusobno nekongruentnih (modulo m) rješenja.

Teorem 1.3.3. *Neka su a i b cijeli brojevi te m prirodan broj. Kongruencija (1.1) ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je kongruencija (1.1) rješiva, onda je broj rješenja jednak d.*

Dokaz. Ako $ax \equiv b \pmod{m}$ ima rješenja onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$ iz čega slijedi $(a, m)|b$.

Obratno, pretpostavimo da $d|b$ i neka su $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ i $m' = \frac{m}{d}$. S obzirom da je $(a', m') = 1$ slijedi da kongruencija $a'x \equiv b' \pmod{m'}$ ima točno jedno rješenje modulo m'. Zaista, ako je $\{x_1, \ldots, x'_m\}$ potpun sustav ostataka modulo m', onda je prema Teoremu 1.3.2 i skup $\{a'x_1, \ldots, a'x'_m\}$ potpun sustav ostataka modulo m'. Stoga postoji jedinstven $a'x_j$ iz tog skupa takav da je $a'x_j \equiv b' \pmod{m'}$ pa je x_j jedinstveno rješenje kongruencije $a'x \equiv b' \pmod{m}$.

Označimo s x_0 rješenje kongruencije $a'x \equiv b' \pmod{m'}$. Lako se može provjeriti da su $x_i = x_0 + i \cdot m'$ za $i = 0, 1, \ldots, d-1$ rješenja od (1.1). Nadalje, $x_i \not\equiv x_j \pmod{m}$ za $i \neq j$. Još samo treba ustanoviti da nema drugih nekongruentnih rješenja. Ako su x_0, y_0 rješenja od (1.1), onda je $ax_0 \equiv ay_0 \pmod{m}$ pa prema Propoziciji 1.2.4 dobivamo da je $x_0 \equiv y_0 \pmod{m'}$. Dakle, kongruencija (1.1) ima točno d rješenja. □

Prethodni teorem karakterizira rješivost linearne kongruencije (1.1) i opisuje konkretnu metodu kako odrediti sva rješenja kongruencije ako odredimo jedno rješenje kongruencije $a'x \equiv b' \pmod{m'}$. Za male vrijednosti modula m', rješenje se može pronaći u nekom potpunom sustavu ostatka modulo m', no za veće vrijednosti od m'

to baš nije optimalna metoda. U tom slučaju koristimo se tzv. *proširenim Euklidovim algoritmom*. Naime, kako je $(a', m') = 1$, to znači da se broj 1 može zapisati kao cjelobrojna linearna kombinacija brojeva a' i m', $a'u + m'v = 1$. Množenjem prethodne jednakosti s b' dobivamo $a'ub' + m'vb' = b'$, tj. $a'(ub') \equiv b' \pmod{m'}$. Dakle, $x_0 = ub'$ je jedno (jedinstveno) rješenje od $a'x \equiv b' \pmod{m'}$. Koeficijente $u, v \in \mathbb{Z}$ određujemo koristeći prošireni Euklidov algoritam.

Pokažimo opisanu metodu rješavanja linearne kongruencije na sljedećem primjeru.

Primjer 1.3.4. *Riješite kongruenciju*

$$175x \equiv 252 \pmod{294}.$$

Euklidovim algoritmom dobivamo:

$$\begin{aligned} 294 &= 1 \cdot 175 + 119 \\ 175 &= 1 \cdot 119 + 56 \\ 119 &= 2 \cdot 56 + 7 \\ 56 &= 8 \cdot 7 \end{aligned}$$

Stoga je $(294, 175) = 7$. *Sada rješavamo kongruenciju*

$$25x \equiv 252 \equiv 36 \pmod{42}.$$

Njeno rješenje je $x_0 \equiv 36 \cdot y_3$. *Elemente niza* (y_i) *računamo pomoću sljedeće tablice*

	-1	*0*	*1*	*2*	*3*
q			*1*	*1*	*2*
y_i	*0*	*1*	*-1*	*2*	*-5*

Stoga je rješenje početne kongruencije

$$x \equiv -5 \cdot 36 \equiv 30 \pmod{42},$$

odnosno sva rješenja modulo 294 *dana su s*

$$x \equiv 30, 72, 114, 156, 198, 240, 282 \pmod{294}.$$

1.4 Eulerova funkcija

Definicija 1.4.1. *Neka je* $m \in \mathbb{N}$, $m > 1$. Reducirani sustav ostataka modulo m *je skup cijelih brojeva* $\{r_1, \ldots, r_k\}$ *sa svojstvom da za svaki cijeli broj* x *takav da je* $(x, m) = 1$ *postoji jedinstven* r_i, $i \in \{1, \ldots, k\}$, *takav da je* $x \equiv r_i \pmod{m}$.

Iz same definicije je jasno da reducirani sustav ostataka modulo m možemo karakterizirati kao najveći mogući skup cijelih brojeva koji su relativni prosti s m, $(r_i, m) = 1$ za sve $i = 1, \ldots, k$, i koji su međusobno nekongruentni modulo m, $r_i \not\equiv r_j \pmod{m}$ za sve $1 \leqslant i < j \leqslant m$. Nadalje, jasno da je $k < n$. Najjednostavniji način kako možemo doći do nekog reduciranog sustava ostataka modulo m jest da iz potpunog sustava ostataka modulo m izbacimo sve one brojeve koji nisu relativno prosti s m.

Definicija 1.4.2. *Broj članova niza* $1, 2, \ldots, n$ *koji su relativno prostih s brojem* n *označavamo s* $\varphi(n)$. *Na taj način je definirana funkcija* $\varphi : \mathbb{N} \mapsto \mathbb{N}$ *koja se naziva* Eulerova funkcija.

Na primjer, $\varphi(8) = 4$ jer su u nizu $1, 2, 3, 4, 5, 6, 7, 8$ točno četiri broja relativno prosta s 8, a to su brojevi $1, 3, 5, 7$.

Za prost broj p vrijedi $\varphi(p) = p - 1$ jer su u nizu $1, 2, \ldots, p-1, p$ svi osim samog p relativno prosti s p.

Ustanovimo i da je broj elemenata u reduciranom sustavu ostataka modulo m upravo jednak vrijednosti Eulerove funkcije, $\varphi(m)$.

Eulerova funkcija zadovoljava vrlo važno svojstvo *multiplikativnosti*. Naime, vrijedi

1. $\varphi(1) = 1$,
2. $\varphi(mn) = \varphi(m)\varphi(n)$ za $m, n \in \mathbb{N}$ takve da je $(m, n) = 1$.

Zahvaljujući svojstvu multiplikativnosti može se odrediti formula za $\varphi(n)$ ako je n dan kanonskim rastavom na proste faktore.

Lema 1.4.3. *Za prost broj* p *vrijedi da je* $\varphi(p^a) = p^{a-1}(p-1)$.

Dokaz. U nizu $1, 2, \ldots, p^a$ svi brojevi koji nisu relativno prosti s p, odnosno koji su višekratnici od p su oblika kp za $1 \leqslant k \leqslant p^{a-1}$. Stoga je broj onih u danom nizu koji su relativno prosti s p jednak $p^a - p^{a-1}$. □

Teorem 1.4.4. *Ako je* $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ *rastav prirodnog broja* m *na proste faktore, onda vrijedi*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right).$$

Primjer 1.4.5. *Odredite* $\varphi(120)$. *Broj* 120 *rastavimo na proste faktore:* $120 = 2^3 \cdot 3 \cdot 5$. *Po Teoremu 1.4.4 slijedi*

$$\varphi(120) = 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 32.$$

Poglavlje 2

Neke primjene kongruencija

2.1 Identifikacijske znamenke

2.1.1 ISBN

International Standard Book Numbers(ISBN) ili Međunarodni standardni knjižni kod je jedinstveni kod koji posjeduje svaka knjiga ili neka druga publikacija bez obzira na medij objavljivanja. Osim knjigama, ISBN se dodjeljuje knjigama objavljenim na CD-ovima i DVD-ovima, publikacijama pisanim na Brailleovom pismu, geografskim kartama, filmovima i sl. ISBN se primjenjuje od 1968. s namjerom lakšeg snalaženje među publikacija. Do 2007.g. primjenjivao se deseteroznamenkasti ISBN raspoređen u četiri grupe, a nakon spomenute godine primjenjuje se trinaesteroznamenkasti ISBN raspoređen u pet skupina.

Naprimjer, $0-07-035471-5$ je deseteroznamenkasti ISBN kod u kojem prva skupina brojeva (znamenka 0) označava mjesto izdavanja knjige. U našem slučaju to je zemlja engleskog govornog područja. Druga skupina je oznaka nakladnika, treća skupina je oznaka publikacije, a posljednja skupina je takozvani kontrolni broj, odnosno kontrolna znamenka. Upravo za određivanje kontrolnog broja deseteroznamenkastog ISBN-a koriste se kongruencije.

Kontrolni broj ili *kontrolna znamenka* d poprima vrijednosti iz skupa $\{0, 1, 2, \ldots, 10\}$ i definirana je kao

$$d \equiv -(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \qquad (2.1)$$

pri čemu $x_1, \ldots, x_9$ označavaju prvih devet znamenki ISBN-a, a $\cdot$ je skalarno množenje

na $\mathbb{R}^9$, odnosno

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) = \sum_{i=1}^{9} (10 - i + 1) x_i.$$

Primjer 2.1.1. *Odredite kontrolni broj d u desteroznamenkastom ISBN-u ako je dano prvih devet znamenaka* $0 - 201 - 57603$. *Vrijedi,*

$$\begin{aligned} d &\equiv -(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \\ &\equiv -(0, 2, 0, 1, 5, 7, 6, 0, 3) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \\ &\equiv -(0 + 18 + 0 + 7 + 30 + 35 + 24 + 0 + 6) \\ &\equiv -120 \equiv 1 \pmod{11}, \end{aligned}$$

pa je kontrolna znamenka jednaka 1.

2.1.2 UPC

The Universal Product Code(UPC) može se naći na svim proizvodima u Sjedinjenim Američkim Državama, a služi za identifikaciju proizvoda. Često UPC kod nazivamo i bar kodom. UPC se sastoji od 12 znamenaka koje ćemo označiti s d_1, d_2, ... , d_{12}. Prvih 6 znamenaka označavaju državu i proizvođača, sljedećih 5 označavaju vrstu proizvoda, a posljednja dvanaesta znamenka je kontrolna znamenka. Određena je tako da zadovoljava sljedeći uvjet

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

odnosno

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

Uočimo da je

$$S = (d_1, d_2, \ldots, d_{12}) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) = 3 \sum_{i=0}^{5} d_{2i+1} + \sum_{i=1}^{6} d_{2i},$$

odnosno S je zbroj trostrukog zbroja znamenaka na neparnim mjestima i zbroja znamenaka na parnim mjestima. Zbog uvjeta koji je postavljen na d_{12} vrijedi

$$S \equiv 0 \pmod{10}.$$

Za identifikacijski UPC kod sa Slike 2.1 vrijedi:

$$S = 3(0 + 6 + 0 + 2 + 1 + 5) + (3 + 0 + 0 + 9 + 4 + 2) = 60 \equiv 0 \pmod{10}.$$

Slika 2.1: Primjer UPC koda

2.1.3 Broj vozačke dozvole

Način određivanja broja vozačke dozvole u SAD-u razlikuje se u svakoj saveznoj državi. Neke zemlje, poput Utaha i New Mexica, koriste kongruencije kako bi se odredila posljednja, kontrolna znamenka u broju vozačke dozvole. Država Utah svojim građanima dodjeljuje deveteroznamenkasti broj vozačke dozvole. Neka su $d_1, \ldots, d_8$ prvih osam znamenaka u broju vozačke dozvole. Tada se deveta znamenka d_9 određuje pomoću kongruencije

$$d_9 \equiv (9,8,7,6,5,4,3,2) \cdot (d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8) \pmod{10}.$$

Primjer 2.1.2. *Ako je prvih osam znamenaka u broju vozačke dozvole izdane u Utahu* 14921994 *tada devetu znamenku određujemo pomoću kongruencije*

$$d_9 \equiv (9,8,7,6,5,4,3,2) \cdot (1,4,9,2,1,9,9,4) = 192 \equiv 2 \pmod{10}.$$

Potpuni broj vozačke dozvole je 149219942.

Američka država New Mexico koristi osmeroznamenkasti broj vozačke dozvole i kod njih je određivanje posljednje znamenke nešto kompliciranije. Neka su $d_1, \ldots, d_7$ prvih sedam znamenaka u broju vozačke dozvole. Prvo određujemo broj x pomoću kongruencije

$$x \equiv -(d_1, d_2, d_3, d_4, d_5, d_6, d_7) \cdot (2,7,6,5,4,3,2) \pmod{11}.$$

Tada je

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

Za razliku od Utaha i New Mexica, Norveška koristi kongruencije za određivanje posljednjih dviju znamenaka u broju vozačke dozvole. Norveška koristi jedanaesteroznamenkasti broj kao oznaku vozačke dozvole pojedinca. Označimo li s $d_1, \ldots, d_9$ prvih devet znamenaka tada se deseta i jedanaesta znamenka, odnosno d_{10} i d_{11} određuju pomoću sljedećih kongruencija:

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

U slučaju da se dobije $d_{10} = 10$ ili $d_{11} = 10$ tada se takav broj vozačke dozvole ne izdaje.

2.1.4 Identifikacijski broj vozila

Svako motorno vozilo proizvedeno u novije doba ima svoj identifikacijski broj. Tipičan identifikacijski broj vozila (engl. Vehicle identification number-VIN) sastoji se od 17 alfanumeričkih znakova. Iz tih 17 znakova može se iščitati zemlja proizvodnje, proizvođač, tip vozila, tip karoserije, serija vozila, model i sl. (Slika 2.2). Kontrolna znamenka, za razliku od modela koje smo upoznali ranije, nalazi se u sredini - d_9. Određivanje kontrolne znamenke provodi se pomoću sljedećih koraka:

1. Slova A do Z zamjenjuju se brojevima $1-9$, $1-9$ i $2-9$, redom. Odnosno,

$$\mathrm{A} \mapsto 1, \mathrm{B} \mapsto 2, \ldots, \mathrm{I} \mapsto 9, \mathrm{J} \mapsto 1, \ldots, \mathrm{R} \mapsto 9, \mathrm{S} \mapsto 2, \ldots, \mathrm{Z} \mapsto 9.$$

   Na taj način dobivamo 16-ero znamenkasti broj $d_1 d_2 \ldots \hat{d}_9 \ldots d_{17}$, gdje smo s $\hat{d}_9$ označili znamenku koja nedostaje, tj. kontrolnu znamenku.

2. Izračunamo najmanji nenegativan broj r takav da je

$$r \equiv (d_1, \ldots, d_8, d_{10}, \ldots, d_{17}) \cdot (8, 7, \ldots, 2, 10, 8, \ldots, 2) \pmod{11}.$$

3. Kontrolna znamenka je

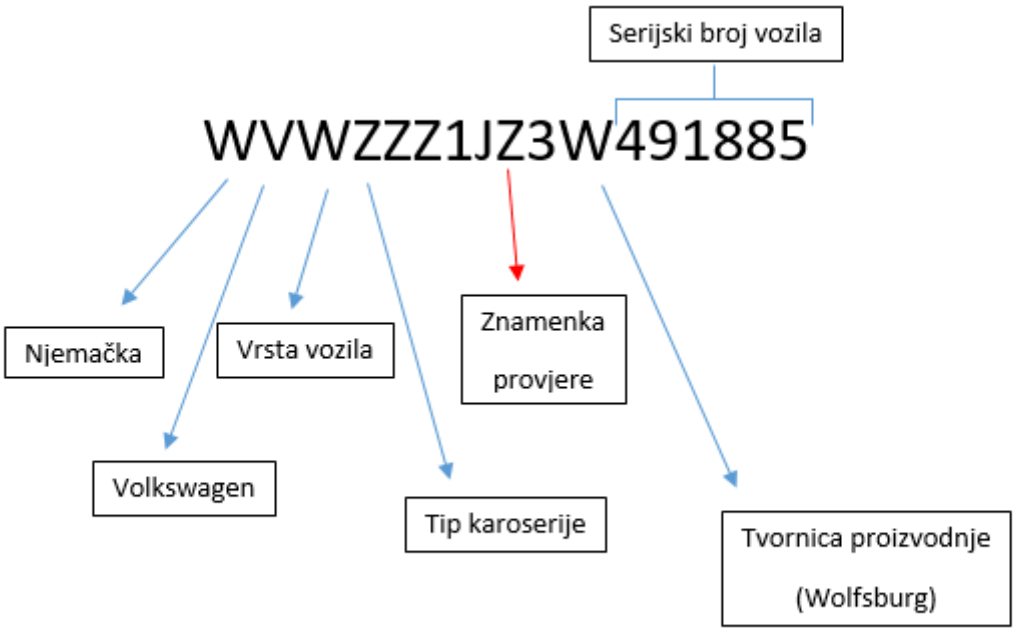
$$d_9 = \begin{cases} r & , 0 \leqslant r < 10, \\ X & , \text{inače.} \end{cases}$$

.

Primjer 2.1.3. *Neka je*

WAUAC48H_ 4K049124

VIN kod nekog motornog vozila. Odredimo mu kontrolnu znamenku.



Slika 2.2: Primjer VIN koda

1. *Zamjenom slova iz VIN koda dobivamo sljedeći broj:*

$$\text{WAUAC48H\_ 4K049124} \mapsto \text{61413488\_ 42049124}$$

2. *Izračunamo najmanji nenegativan r takav da je*

$$\begin{aligned} r &\equiv (6,1,4,1,3,4,8,8,4,2,0,4,9,1,2,4)\cdot(8,7,6,5,4,3,2,10,9,8,7,6,5,4,3,2) \\ &\equiv (48+7+24+5+12+12+16+80+36+16+0+24+45+4+6+8) \\ &\equiv 343 \equiv 2 \pmod{11} \end{aligned}$$

3. *Kontrolna znamenka $d_9 = 2$ jer je $0 \leqslant r < 10$.*

2.1.5 Luhnova formula

Na većini bankovnih kartica nalazi se šesnaesteroznamenkasti broj. Taj broj kartice nije sasvim slučajan i za njegovo dodjeljivanje koriste se kongruencije i Luhnova

formula (algoritam). Luhnov algoritam osmislio je 1954. godine njemački znanstvenik Hans Peter Luhn.

Za određivanje valjanosti broja kartice potrebna nam je funkcija p definirana na sljedeći način:

$$p(n) = \begin{cases} 0 & , n = 0, \\ 9 & , n = 9, \\ 2n \pmod 9 & , 1 \leqslant n \leqslant 8. \end{cases}$$

Dakle, funkcija p poprima sljedeće vrijednosti:

n	0	1	2	3	4	5	6	7	8	9
$p(n)$	0	2	4	6	8	1	3	5	7	9

Neka je

$$\overline{a_n a_{n-1} \dots a_2 a_1}$$

n-teroznamenkasti broj kartice. Definiramo sumu

$$S = a_1 + p(a_2) + a_3 + p(a_4) + \cdots .$$

Ako $S \not\equiv 0 \pmod{10}$ tada je broj kartice nevažeći, inače je valjan.

Primjer 2.1.4. *Odredite ispravnost broja kartice 4356 2678 9889 6473.*
Odredimo sumu S.

$$\begin{aligned} S &= 3 + p(7) + 4 + p(6) + 9 + p(8) + 8 + p(9) + 8 + p(7) + 6 + p(2) + 6 + p(5) + 3 + p(4) \\ &= 3 + 5 + 4 + 3 + 9 + 7 + 8 + 9 + 8 + 5 + 6 + 4 + 6 + 1 + 3 + 8 \\ &= 89 \end{aligned}$$

Očito $S \not\equiv 0 \pmod{10}$ *iz čega slijedi da dani broj kartice nije valjan.*

2.2 Djeljivost

2.2.1 Testovi djeljivosti

Najjednostavnija primjena teorija kongruencija je u testovima djeljivosti. Testovima djeljivosti provjeravamo je li dani prirodan broj djeljiv nekim prirodnim brojem. Najpoznatiji su testovi koji provjeravaju djeljivost s brojevima 10, 5, 2^i, 3, 9 i 11.

Svaki prirodan broj n u dekadskom sustavu ili sustavu s bazom 10 zapisujemo kao

$$n = (n_k n_{k-1} ... n_1 n_0)_{10} = n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \cdots + n_1 \cdot 10 + n_0, \tag{2.2}$$

pri čemu su $a_k, a_{k-1}, \ldots, a_0 \in \{0, 1, 2, \ldots, 9\}$ njegove znamenke. Često ćemo rabiti i sljedeći zapis:

$$n = \overline{a_k a_{k-1} \cdots a_0}.$$

Teorem 2.2.1 (Test djeljivosti s 10)**.** *Prirodan broj je djeljiv s* 10 *ako i samo ako mu je posljednja znamenka* 0*.*

Dokaz. Neka je dan prirodan broj n zapisan kao u (2.2). Očito je

$$n \equiv n_0 \pmod{10}.$$

Broj n je djeljiv s 10 ako i samo ako je $n \equiv 0 \pmod{10}$. Stoga je n je djeljiv s 10 ako i samo ako je $n_0 \equiv 0 \pmod{10}$. □

Teorem 2.2.2 (Test djeljivosti s 5)**.** *Prirodan broj je djeljiv s 5 ako i samo ako mu je posljednja znamenka 0 ili 5.*

Dokaz. Ako je n dan s (2.2), onda je $n \equiv n_0 \pmod{5}$. Stoga je n djeljiv s 5 ako i samo ako je $n_0 \equiv 0 \pmod{5}$. Jedine znamenke koje zadovoljavaju prethodni uvjet su 0 i 5. □

Teorem 2.2.3 (Test djeljivosti s 2^i)**.** *Neka je $i \in \mathbb{N}$. Prirodan broj je djeljiv s 2^i ako i samo ako mu je i-znamenkasti završetak djeljiv s 2^i .*

Dokaz. Neka je n dan s (2.2). Tada vrijedi:

$$\begin{aligned}
&n \equiv n_0 \pmod{2},\\
&n \equiv n_1 \cdot 10 + n_0 = \overline{n_1 n_0} \pmod{2^2},\\
&n \equiv n_2 \cdot 10^2 + n_1 \cdot 10 + n_0 = \overline{n_2 n_1 n_0} \pmod{2^3},\\
&\quad\vdots\\
&n \equiv n_{i-1} \cdot 10^{i-1} + n_{i-2} \cdot 10^{i-2} + \cdots + n_1 \cdot 10 + n_0 = \overline{n_{i-1} n_{i-2} \cdots n_0} \pmod{2^i}
\end{aligned}$$

pa očito vrijedi tvrdnja teorema. □

Teorem 2.2.4 (Test djeljivosti s 3)**.** *Prirodan broj je djeljiv s* 3 *ako i samo ako mu je zbroj znamenaka djeljiv s* 3 *.*

Dokaz. Uočimo da je $10^k \equiv 1 \pmod 3$, za svaki $k \in \mathbb{N}$. Stoga za (2.2) vrijedi

$$n = n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \cdots + n_1 \cdot 10 + n_0 \equiv n_k + n_{k-1} + \cdots + n_1 + n_0 \pmod 3,$$

pa slijedi tvrdnja. □

Teorem 2.2.5 (Test djeljivosti s 9)**.** *Prirodan broj je djeljiv s* 9 *ako i samo ako mu je zbroj znamenaka djeljiv s* 9 *.*

Dokaz. Kako je $10^k \equiv 1 \pmod 9$, za $k \in \mathbb{N}$, dokaz je identičan dokazu Teorema 2.2.4. □

Teorem 2.2.6 (Test djeljivosti s 11)**.** *Prirodan broj je djeljiv s 11 ako i samo ako je razlika zbroja znamenaka na parnim mjestima i zbroja znamenaka na neparnim mjestima djeljiva s 11.*

Dokaz. Kako je $10 \equiv -1 \pmod{11}$, tada je

$$10^k \equiv (-1)^k \pmod{11},\ k \in \mathbb{N}.$$

Stoga vrijedi

$$\begin{aligned} n &= n_k 10^k + n_{k-1} 10^{k-1} + \cdots + n_3 10^3 + n_2 10^2 + n_1 10 + n_0 \\ &\equiv n_k \cdot (-1)^k + n_{k-1} \cdot (-1)^{k-1} + \cdots + n_3 \cdot (-1)^3 + n_2 \cdot (-1)^2 + n_1 \cdot (-1)^1 + n_0 \\ &\equiv (n_0 + n_2 + \cdots) - (n_1 + n_3 + \cdots) \pmod{11}. \end{aligned}$$

□

Korolar 2.2.7. *Palindrom s parnim brojem znamenaka je djeljiv s 11.*

Dokaz. Neka je $n = \overline{n_{2k-1} n_{2k-2} \cdots n_1 n_0}$ palindrom s parnim brojem znamenaka. Stoga je $n_0 = n_{2k-1}, n_1 = n_{2k-2}, \ldots, n_{k-1} = n_k$ pa slijedi da je zbroj znamenaka na parnim mjestima jednak zbroju znamenaka na neparnim mjestima. Prema Teoremu 2.2.6 slijedi da 11 dijeli broj n. □

Primjer 2.2.8. *Palindrom* 1849559481 *ima paran broj znamenki pa je djeljiv s 11. Palindrom* 1365631 *ima neparan broj znamenki i nije djeljiv s 11, no* 1360631 *ima također neparan broj znamenaka i djeljiv je s* 11*. Lako se može ustanoviti da je palindrom s neparnim brojem znamenaka djeljiv s* 11 *ako i samo ako mu je središnja znamenka jednaka* 0*.*

2.2.2 Odbacivanje devetki

Metoda odbacivanja devetki, engl. *Casting out nines*, koristi se za provjeru računa i otkrivanju eventualnih pogrešaka. Ova metoda temelji se na činjenici da je svaki cijeli broj kongruentan zbroju svojih znamenki modulo 9,

$$n = n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \cdots + n_1 \cdot 10 + n_0 \equiv n_k + n_{k-1} + \cdots + n_1 + n_0 \pmod 9.$$

U sljedećih nekoliko primjera prikazano je kako se koristi metoda odbacivanja devetki.

Primjer 2.2.9. *Koristeći metodu odbacivanja devetki provjerite vrijedi li*

$$58807 + 83291 + 601756 = 748354.$$

Računamo redom:

$$\begin{aligned} 58807 &\equiv 5 + 8 + 8 + 0 + 7 \equiv 1 \pmod 9, \\ 83291 &\equiv 8 + 3 + 2 + 9 + 1 \equiv 5 \pmod 9, \\ 601756 &\equiv 6 + 0 + 1 + 7 + 5 + 6 \equiv 7 \pmod 9, \\ 748354 &\equiv 7 + 4 + 8 + 3 + 5 + 4 \equiv 4 \pmod 9. \end{aligned}$$

Kako je $1 + 5 + 7 \equiv 4 \pmod 9$*, slijedi da je početna jednakost* vjerojatno *točna.*

Na temelju prethodno primjera lako možemo zaključiti da nam metoda odbacivanja devetki daje jedan od dva moguća ishoda: *vjerojatno točno* i *netočno*. Naime, permutacijom znamenki u bilo kojem od brojeva iz prethodnog primjera, npr. ako broj 58807 zamijenimo brojem 50788, kongruencije će vrijediti i imat ćemo isti zaključak.

Primjer 2.2.10. *Koristeći metodu odbacivanja devetki provjerite vrijedi li*

$$2076 \cdot 1076 = 223766.$$

Računamo:

$$\begin{aligned} 2076 &\equiv 2 + 0 + 7 + 6 \equiv 6 \pmod 9, \\ 1076 &\equiv 1 + 0 + 7 + 6 \equiv 5 \pmod 9, \\ 223766 &\equiv 2 + 2 + 3 + 7 + 6 + 6 \equiv 8 \pmod 9. \end{aligned}$$

Kako $6 \cdot 5 \not\equiv 8 \pmod 9$ *slijedi da jednakost nije točna.*

Primjer 2.2.11. *Koristeći metodu odbacivanja devetki provjerite daje li broj 14049 podijeljen s 95 količnik 147 i ostatak 80.*
Prema teoremu o dijeljenju s ostatkom vrijedi $14049 = 147 \cdot 95 + 80$. *Kako je*

$$\begin{aligned} 147 &\equiv 1 + 4 + 7 \equiv 3 \pmod 9, \\ 95 &\equiv 9 + 5 \equiv 5 \pmod 9, \\ 80 &\equiv 8 + 0 \equiv 8 \pmod 9, \\ 14049 &\equiv 1 + 4 + 0 + 4 + 9 \equiv 0 \pmod 9 \end{aligned}$$

i $(3 \cdot 5) + 8 \not\equiv 0 \pmod 9$ *zaključujemo da račun ne vrijedi.*

2.2.3 Digitalni korijen

Neka je n prirodan broj i s suma njegovih znamenaka. Ako je s jednoznamenkasti broj, onda je *digitalni korijen* od n jednak s. Ako je s višeznamenkasti broj, onda računamo njegov zbroj znamenaka i ponavljamo postupak sve dok ne dođemo do jednoznamenkastog broja. Taj jednoznamenkasti broj predstavlja *digitalni korijen* od n i označavat ćemo ga s $d(n)$. Jasno je da $d(n) \in \{1, \ldots, 9\}$.

Primjer 2.2.12. *Odredite digitalne korijene brojeva* 1231 *i* 6799.
Računamo:

$$1231 \mapsto 1 + 2 + 3 + 1 = 7,$$

$$6799 \mapsto 6 + 7 + 9 + 9 = 31 \mapsto 4.$$

Stoga je $d(1231) = 7$ *i* $d(6799) = 4$.

Očito je da digitalni korijen prirodnog broja možemo povezati s odbacivanjem devetki. Nadalje, kako je svaki prirodan broj kongruentan zbroju svojih znamenaka modulo 9, slijedi da je

$$d(n) \equiv (a_n + \cdots + a_1 + a_0) \pmod 9,$$

gdje je $n = (a_n \ldots a_1 a_0)_{10}$. Digitalni korijen predstavlja i ostatak pri dijeljenju broja n s 9, pri čemu ostatak 0 zamjenjujemo s 9.

Teorem 2.2.13. *Neka je* $n, m \in \mathbb{N}$ *i* $d(n)$, $d(m)$ *njihovi digitalni korijeni. Vrijedi:*

(1) $d(d(n)) = d(n)$,

(2) $d(n + m) = d(d(n) + d(m))$,

(3) $d(nm) = d(d(n)d(m))$.

Dokaz. (1) Slijedi iz definicije digitalnog korijena.

(2) Kako je $n \equiv d(n) \pmod 9$ i $m \equiv d(m) \pmod 9$, slijedi da je $n + m \equiv d(n) + d(m) \pmod 9$ pa je $d(n + m) = d(d(n) + d(m))$.

(3) Analogno kao prethodno jer je $nm \equiv d(n)d(m) \pmod 9$.

□

Primjer 2.2.14. *Neka je n potpuni kvadrat, tj. $n = k^2$ za neki $k \in \mathbb{N}$. Koje sve vrijednosti može poprimiti njegov digitalni korijen?*

Za $n \in \mathbb{N}$ vrijedi da je $n \equiv r \pmod 9$, odnosno $n^2 \equiv r^2 \pmod 9$ za neki $r \in \{0, 1, \ldots, 8\}$. Nadalje, prema Teoremu 2.2.13 je

$$d(n) = d(k^2) = d(d(k)^2)$$

pa stoga treba naći digitalne korijene brojeva $1, 2^2, \ldots, 9^2$. Kako je $5 \equiv -4 \pmod 9$, $6 \equiv -3 \pmod 9$, $7 \equiv -2 \pmod 9$, $8 \equiv -1 \pmod 9$, te

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

slijedi da su digitalni korijeni potpunih kvadrata brojevi 1, 4, 7 i 9.

Primjer 2.2.15. *Broj 54 892 534 046 nije potpuni kvadrat jer je*

$$d(n) \equiv 5 + 4 + 8 + 9 + 2 + 5 + 3 + 4 + 0 + 4 + 6 \equiv 50 \equiv 5 \pmod 9. \tag{2.3}$$

U Primjeru 2.2.14 je pokazano da digitalni korijen potpunog kvadrata može poprimiti vrijednosti 1, 4, 7 i 9.

Primjer 2.2.16. *Broj $n = 2^{2013} + 2^{2014} + 2^{2015} + 2^{2016} + 2^{2017}$ nije potpuni kvadrat. Zaista, iz $2^3 \equiv -1 \pmod 9$ slijedi*

$$\begin{aligned} n &\equiv (2^3)^{671} + (2^3)^{671} \cdot 2 + (2^3)^{671} \cdot 2^2 + (2^3)^{672} + (2^3)^{672} \cdot 2 \\ &\equiv (-1)^{671} + (-1)^{671} \cdot 2 + (-1)^{671} \cdot 2^2 + (-1)^{672} + (-1)^{672} \cdot 2 \\ &\equiv -1 - 2 - 4 + 1 + 2 \equiv -4 \equiv 5 \pmod 9 \end{aligned}$$

pa prema Primjeru 2.2.14 zaključujemo da $2^{2013} + 2^{2014} + 2^{2015} + 2^{2016} + 2^{2017}$ nije potpuni kvadrat.

Primjer 2.2.17. *Pokazat ćemo da je digitalni korijen umnoška prostih brojeva blizanaca, osim* 3 *i* 5*, jednak* 8*.*

Prosti brojevi blizanci su parovi prostih brojeva čija razlika iznosi 2*. Za svaki prosti broj* $p > 3$ *vrijedi* $p \equiv \pm 1 \pmod 6$*. Zaista, ako* $p \equiv 0, 2, 4 \pmod 6$ *onda je* p *paran broj, a ako* $p \equiv 3 \pmod 6$ *onda je* p *višekratnik broja* 3*. Stoga se par prostih brojeva blizanaca može zapisati kao* $6k - 1$ *i* $6k + 1$ *za neki* $k \in \mathbb{N}$*. Tada je*

$$(6k - 1)(6k + 1) \equiv 36k^2 - 1 \equiv 0 - 1 \equiv 8 \pmod 9.$$

Dakle, digitalni korijen produkta prostih brojeva blizanaca jednak 8*.*

2.3 Kalendar

2.3.1 Petak 13.

Kako bi odredili broj "nesretnih" dana u godini možemo koristiti kongruencije. Pojava *petka trinaestog* ovisi o danu u tjednu na koji je u prethodnom mjesecu pao trinaesti dan tog mjeseca i o broju dana prethodnog mjeseca. Odredimo u kojem mjesecu 2018. se prvi puta pojavio *petak trinaesti*. S $M(i)$, $i = 1, \ldots, 12$, redom označimo mjesece počevši od siječnja 2018., a završno s prosinca 2018. Ako s $D(i)$ označimo broj dana u $M(i) - tom$ mjesecu tada $D(i)$ poprima redom sljedeće vrijednosti

$$D(i) \in \{31, 28, 31, 30, 31, 30, 31, 31, 30, 31, 30, 31\}, \tag{2.4}$$

za sve $i = 1, \ldots, 12$. Pridružimo nedjelji broj 0, ponedjeljku 1, utorku 2, srijedi 3, četvrtku 4, petku 5 i suboti 6. Promotrimo kongruencije

$$D(i) \equiv d(i) \pmod 7 \tag{2.5}$$

pri čemu je $0 \leqslant d(i) < 7$. Uvrštavanjem redom vrijednosti koje poprima $D(i)$ u gornju kongruenciju te rješavanjem dobivenih kongruencija dobivamo da je

$$d(i) \in \{3, 0, 3, 2, 3, 2, 3, 3, 2, 3, 2, 3\}, \tag{2.6}$$

za $i = 1, \ldots, 12$. Vrijednost $d(i)$ može se interpretirati kao broj dana za koliko se pomaknuo trinaesti dan $M(i + 1)$-tog mjeseca u odnosu na trinaesti dan $M(i) - tog$ mjeseca. Znamo da je 13. siječnja 2018. bila subota kojoj smo pridružili broj 6. Da bismo odredili na koji dan pada 13. veljače rješavamo kongruenciju

$$6 + 3 = 9 \equiv a \pmod 7, \tag{2.7}$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$m(i)$	3	3	0	3	2	3	2	3	3	2	3	2	3
$d(i)$	3	6	2	2	**5**	0	3	**5**	1	4	6	2	4
dan	sri	sub	ut	ut	**pet**	ned	sri	**pet**	pon	čet	sub	ut	čet

Tablica 2.1: 13. u mjesecu za godinu 2018.

za $0 \leqslant a < 7$. Slijedi da je $a = 2$ pa prema tome 13. veljače 2018. je bio utorak. Rješavanjem kongruencije

$$6 + 3 + 0 \equiv a \pmod 7 \tag{2.8}$$

dobivamo da je $a = 2$ što znači da je 13. ožujka 2018. također bio utorak. Analogno, rješenje kongruencije

$$6 + 3 + 0 + 3 \equiv a \pmod 7 \tag{2.9}$$

je $a = 5$ što znači da "nesretan" dan pada 13. travnja 2018. Na koji dan pada 13. u mjesecu možemo iščitati iz Tablice 2.3.1 gdje $a(i) \in \{0, \ldots, 6\}$ predstavlja 13. dan u k-to mjesecu i dobivamo ga kao rješenje kongruencije

$$a(k+1) \equiv a(1) + \sum_{i=1}^{k} d(i) \pmod 7,$$

pri čemu je $a(1) = 6$ za 2018., te $k = 1, \ldots, 11$, odnosno kraće kao

$$a(k+1) \equiv a(k) + d(k) \pmod 7.$$

Stoga će se *petak trinaesti* u 2018. desiti dva puta, u travnju i srpnju.

Možemo istražiti koliko se maksimalno puta godišnje može desiti događaj *petka trinaestog*. Odgovor na to dobit ćemo ako ustanovimo broj ponavljanja vrijednosti u skupu $\{a(1), \ldots, a(12)\}$, odnosno statistički rečeno određujući frekvencije u nizu $a(1), \ldots, a(12)$. Analogno tome odredit ćemo frekvencije u niza

$$s(1) = 0,\ s(k) = \sum_{i=1}^{k-1} d(i) \mod 7,\ k = 2, \ldots, 12,$$

jer se od niza $(a(k))$ razlikuje samo za konstantu $a(1)$. Vrijednosti od $s(i)$ dane su u sljedećoj tablici:

i	1	2	3	4	5	6	7	8	9	10	11	12
$s(i)$	0	3	3	6	1	4	6	2	5	0	3	5

.

Tablica frekvencijskih vrijednosti je sljedeća

	0	1	2	3	4	5	6
f_i	2	1	1	3	1	2	2

.

Sada zaključujemo da maksimalan broj petaka trinaestih jednak tri, a događa se u godinama koje nisu prijestupne i onda kada je 13. u siječnju pao u ponedjeljak, tj. $a(1) = 2$. U tim godinama petak 13. dogodit će se u veljači, ožujku i studenom.

Na isti način možemo analizirati i prijestupnu godinu. Tada je

$$d(i) \in \{3, 1, 3, 2, 3, 2, 3, 3, 2, 3, 2, 3\},$$

te

i	1	2	3	4	5	6	7	8	9	10	11	12
$s(i)$	0	3	4	0	2	5	0	3	6	1	4	6

.

Iz tablice frekvencijskih vrijednosti:

	0	1	2	3	4	5	6
f_i	2	1	1	3	1	2	2

zaključujemo da je maksimalan broj petaka trinaestih u prijestupnoj godini također jednak tri. To se će se desiti u siječnju, travnju i srpnju samo ako je 13. u siječnju pao baš u petak.

2.3.2 Gregorijanski kalendar

U poglavlju Petak 13. pomoću kongruencija određivali smo koliko "nesretnih" dana imamo u jednoj kalendarskoj godini. Sada ćemo kongruencije koristiti i pri određivanju dana u tjednu za bilo koji datum u Gregorijanskom kalendaru. Do 1582. godine u upotrebi je bio Julianski kalendar koji je u odnosu na sunčevu godinu imao 10 dana više. U listopadu te iste godine, na zahtjev pape Grgura XIII., astronomi Christopher Clavius i Aloysius Giglio predstavili su Gregorijanski kalendar kojim se poravnalo trajanje kalendarske i sunčeve godine. Gregorijanski kalendar se koristi i dan danas iako postoji mala odstupanja u trajanju kalendarske i sunčeve godine. Prema njemu kalendarska godina traje 365.2425 dana, a sunčeva 365.2421897 dana što bi značilo da se svakih 10 000 godina pojavi 3 dana viška. Clavius i Gioglio grešku od 10 dana ispravili su tako što su dana 15. listopada 1582. vratili kalendar na 5. listopad 1582. Također, dodaju uvjet da su godine djeljive sa 100 prijestupne samo ako su djeljive i s 400. Prva prijestupna godina u Gregorijanskom kalendaru bila je 1600.

Cilj nam je izvesti formulu koja obuhvaća godine nakon 1600., a pomoću koje ćemo odrediti dan u tjednu za bilo koji datum u Gregorijanskom kalendaru. Prijestupna godina ima jedan dan više u odnosu na neprijestupnu godinu i taj dan dodaje se u veljači. Zbog toga ćemo novu godinu računati od 1. ožujka, a ne od 1. siječnja.

Mjesece od ožujka do veljače redom označavamo brojevima od 1 do 12, tj.

mjesec	ožujak	travanj	svibanj	lipanj	srpanj	kolovoz
oznaka	1	2	3	4	5	6
mjesec	rujan	listopad	studeni	prosinac	siječanj	veljača
oznaka	7	8	9	10	11	12

Dane u tjednu počevši od nedjelje redom označavamo brojevima od 0 do 6, tj.

dan	nedelja	ponedjeljak	utorak	srijeda	četvrtak	petak	subota
oznaka	0	1	2	3	4	5	6

Dan u tjednu na koji pada 1. ožujka godine y označavat ćemo s d_y. Pretpostavit ćemo da je $y \geqslant 1600$ (s obzirom na to da je prva prijestupna godina bila 1600.).

Budući da je $365 \equiv 1 \pmod 7$ i $366 \equiv 2 \pmod 7$, očito vrijedi

$$d_{y+1} = \begin{cases} d_y + 1 & ; y \text{ nije prijestupna godina;} \\ d_y + 2 & ; y \text{ prijestupna godina.} \end{cases}$$

Za izračunavanje d_y potrebno je znati broj prijestupnih godina nakon 1600.

Odredimo broj prijestupnih godina nakon 1600. godine do godine y. Broj prijestupnih godina označit ćemo s l. Najprije ćemo naći broj svih godina koje su višekratnik broja 4. Za svaku takvu godinu vrijedi da je oblika $4n_1$ i da je

$$1600 < 4n_1 \leqslant y,$$

pa je

$$400 < 4n_1 \leqslant \left\lfloor \frac{y}{4} \right\rfloor,$$

pri čemu smo $\lfloor x \rfloor$ označili *najveće cijelo* od x - najveći cijeli broj koji nije veći od x. Sada slijedi da je broj godina koje su djeljive s 4 između 1600. godine i godine y jednak

$$n_1 = \left\lfloor \frac{y}{4} \right\rfloor - 400.$$

Analogno, broj godina koje su djeljive sa 100 je

$$n_2 = \left\lfloor \frac{y}{100} \right\rfloor - 16,$$

a broj onih koje su djeljive s 400 je

$$n_3 = \left\lfloor \frac{y}{400} \right\rfloor - 4.$$

Po formuli uključivanja i isključivanja slijedi

$$\begin{aligned} l &= n_1 + n_3 - n_2 \\ &= \left\lfloor \frac{y}{4} \right\rfloor - 400 + \left\lfloor \frac{y}{400} \right\rfloor - 4 - \left(\left\lfloor \frac{y}{100} \right\rfloor - 1 \right) \\ &= \left\lfloor \frac{y}{4} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor - 388. \end{aligned}$$

Teorem o dijeljenju s ostatkom povlači da y možemo zapisati na sljedeći način:

$$y = 100C + D,$$

pri čemu je C broj stoljeća i $0 \leqslant D < 100$. Dakle,

$$C = \left\lfloor \frac{y}{100} \right\rfloor, \quad D \equiv y \pmod{100}.$$

Slijedi,

$$\begin{aligned} l &= \left\lfloor \frac{y}{4} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor - 388 \\ &= \left\lfloor \frac{100C + D}{4} \right\rfloor + \left\lfloor \frac{100C + D}{400} \right\rfloor - \left\lfloor \frac{100C + D}{100} \right\rfloor - 388 \\ &= 25C + \left\lfloor \frac{D}{4} \right\rfloor - C + \left\lfloor \frac{C}{4} \right\rfloor - 388 \\ &= 24C + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor - 388 \\ &\equiv 3C + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor - 3 \pmod{7}. \end{aligned}$$

Dakle, d_y je kongruentan modulo 7 zbroju d_{1600}, svih godina nakon 1600., te svih prijestupnih godina nakon 1600., tj.

$$\begin{aligned} d_y &\equiv d_{1600} + (y - 1600) + l \\ &\equiv d_{1600} + (100C + D - 1600) + 3C + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor - 3 \end{aligned}$$

$$\begin{aligned}
&\equiv d_{1600} + 2C + D - 4 + 3C - 3 + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor \\
&\equiv d_{1600} + 5C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor \\
&\equiv d_{1600} - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor \pmod 7.
\end{aligned}$$

Preostaje odrediti d_{1600}, tj. dan na koji je pao 1. ožujka 1600. Kako bismo to odrediti treba znati dan na koji je pao 1. ožujka bilo koje godine. Na primjer, 1. ožujka 2018. godine bio je četvrtak. Odnosno, $d_{2018} = 4$, $C = \lfloor \frac{2018}{100} \rfloor = 20$, $D = 18$. Uvrštavanjem u formulu za d_y dobiva se:

$$\begin{aligned}
d_{2018} &\equiv d_{1600} - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor \pmod 7, \\
4 &\equiv d_{1600} - 2 \cdot 20 + 18 + \left\lfloor \frac{18}{4} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor \pmod 7, \\
4 &\equiv d_{1600} - 40 + 18 + 4 + 5 \pmod 7, \\
d_{1600} &\equiv 4 + 40 - 18 - 4 - 5 \pmod 7, \\
d_{1600} &\equiv 17 \pmod 7, \\
d_{1600} &\equiv 3 \pmod 7.
\end{aligned}$$

Slijedi, $d_{1600} = 3$. Dakle, 1.ožujka 1600. je bila srijeda. Uvrštavanjem $d_{1600} = 3$ u formulu za d_y dobiva se

$$d_y \equiv 3 - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor \pmod 7.$$

Gornjom formulom možemo odrediti 1. ožujka za bilo koju zadanu godinu.

Što ako smo u situaciji da ne znamo na koji dan pada 1. ožujka neke dane godine? Ta ista situacija zanimala je i njemačkog matematičara Christiana Zellera. On je uočio sljedeće. Prvi u m_i-tom mjesecu u odnosu na prvi u m_{i-1}-om mjesecu se pomiče za dva dana ako je m_{i-1}-i mjesec imao 30 dana, odnosno ako je m_{i-1}-i mjesec imao 31 dan onda se pomiče 3 dana unaprijed.

			pomak
1.4.	u odnosu na	1.3.	3 dana
1.5.	u odnosu na	1.4.	2 dana
1.6.	u odnosu na	1.5.	3 dana
1.7.	u odnosu na	1.6.	2 dana
1.8.	u odnosu na	1.7.	3 dana
1.9.	u odnosu na	1.8.	3 dana
1.10.	u odnosu na	1.9.	2 dana
1.11.	u odnosu na	1.10.	3 dana
1.12.	u odnosu na	1.11.	2 dana
1.1	u odnosu na	1.12.	3 dana
1.2.	u odnosu na	1.1.	3 dana

Ako se zbroje dani u desnom stupcu dobije se 29. Dakle, prosječno povećanje broja dana prvog u mjesecu u odnosu na prethodni prvi iznosi $\frac{29}{11} \approx 2.6$ dana. C. Zeller uočio je da funkcija

$$f(m) = \lfloor 2.6m - 0.2 \rfloor - 2$$

opisuje pomak u broja dana u odnosu na 1. ožujak za $1 \leqslant m \leqslant 12$. Tako za $m = 4$ dobivamo

$$f(4) = \lfloor 2.6 \cdot 4 - 0.2 \rfloor - 2 = \lfloor 10.4 \rfloor - 2 = 8 \equiv 1 \pmod 7,$$

što znači ako je 1. ožujka bio ponedjeljak, onda će 1. lipnja biti utorak. Nadalje, ako nam je, na primjer, poznato da je 1. srpnja bio petak i želimo znati na koji dan će pasti 1. studenog, onda računamo

$$f(9) - f(5) = \lfloor 2.6 \cdot 9 - 0.2 \rfloor - \lfloor 2.6 \cdot 5 - 0.2 \rfloor = \lfloor 23.2 \rfloor - \lfloor 12.8 \rfloor = 11 \equiv 4 \pmod 7.$$

Stoga, 1. studenog pada u utorak jer je $5 + 4 \equiv 2 \pmod 7$.

Primjenom funkcije f možemo izvesti formulu koja određuje na koji dan pada prvi dan u nekom danom mjesecu dane godine. Ako označimo s $d_y^m \in \{0, \ldots, 6\}$ dan na koji pada prvi u mjesecu m godine y, onda je

$$d_y^m \equiv d_y + f(m) \equiv 3 - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor + \lfloor 2.6m - 0.2 \rfloor - 2 \pmod 7,$$

odnosno

$$d_y^m \equiv 1 - 2C + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor + \lfloor 2.6m - 0.2 \rfloor \pmod 7.$$

Primjer 2.3.1. *Odredimo dan na koji će pasti Praznik rada u 2019. godini. Računamo*

$$d_{2019}^{5} \equiv 1 - 2 \cdot 20 + 19 + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{19}{4} \right\rfloor + \lfloor 2.6 \cdot 3 - 0.2 \rfloor = -4 \equiv 3 \pmod 7$$

i zaključujemo da 1. svibnja 2019. pada u srijedu. (Uočimo da je $m = 3$).

Primjer 2.3.2. *Odredimo dan na koji će pasti blagdan Velike Gospe u 2020. godini. Računamo*

$$d_{2020}^{8} \equiv 1 - 2 \cdot 20 + 20 + \left\lfloor \frac{20}{4} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor + \lfloor 2.6 \cdot 6 - 0.2 \rfloor = 6 \pmod 7$$

i zaključujemo da 15. kolovoza 2020. pada u subotu jer je $6 + 14 = 20 \equiv 6 \pmod 7$.

2.4 Igre

2.4.1 Problem kraljica na šahovskoj ploči

Postavljamo sljedeći zanimljiv problem vezan uz šah:

Kako postaviti n kraljica na šahovsku ploču dimenzije $n \times n$ tako da se one međusobno ne napadaju?

Pri rješavanju ovog problema treba imati na umu da se kraljica u šahu može pomicati za neodređeni broj slobodnih polja u svim smjerovima: vertikalno, horizontalno i dijagonalno. Pretpostavit ćemo da je $n = p > 3$ prost broj. Jednostavno se može ustanoviti da za $p = 2$ ili $p = 3$, kraljice nije moguće postaviti tako da se ne napadaju. Budući da se svih p kraljica ne smije međusobno napadati, jasno je da će se u svakom retku (odnosno stupcu) nalaziti točno jedna kraljica. Označimo s $g(i)$ položaj kraljice u i-tom retku, $i = 1, \ldots, p$. Pokazat ćemo da funkcija s $g : \{1, \ldots, p\} \to \{1, \ldots, p\}$ koja zadovoljava sljedeću rekurziju

$$\begin{aligned} g(1) &= \frac{p+1}{2}, \\ g(i) &\equiv g(i-1) + \frac{p+1}{2} \pmod p,\ 2 \leqslant i \leqslant p, \end{aligned} \tag{2.10}$$

daje odgovor na postavljeno pitanje. Uočimo da je $g(p) \equiv 0 \pmod p$. Eksplicitna formula za g glasi:

$$g(i) \equiv \frac{p+1}{2} i \pmod p,\ 1 \leqslant i \leqslant p, \tag{2.11}$$

pri čemu se vrijednost $g(i)$ određuje u potpunom sustavu ostataka $\{1, \ldots, p\}$ pa je $g(p) = p$.

Teorem 2.4.1. *Funkcija $g : \{1, \ldots, p\} \to \{1, \ldots, p\}$ definirana s (2.11) je injekcija.*

Dokaz. Neka su a i b iz $\{1, \ldots, p\}$ takvi da je $g(a) = g(b)$. Stoga je

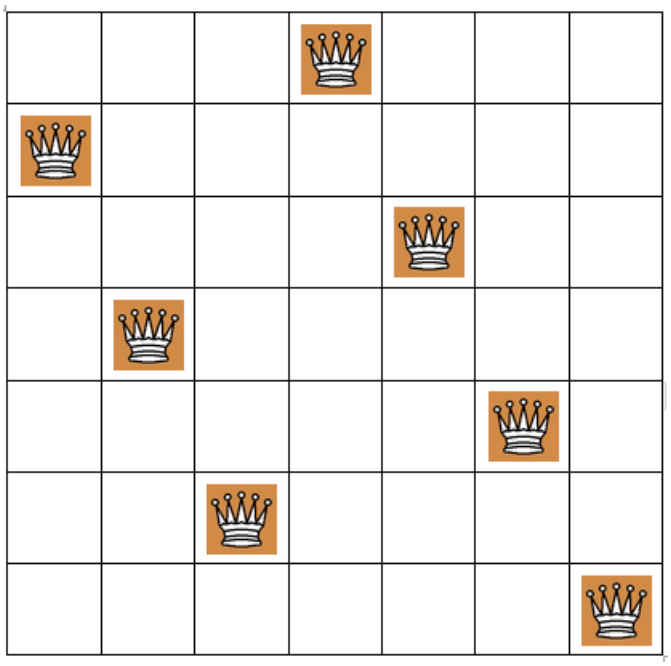
$$\left(\frac{p+1}{2}\right) a \equiv \left(\frac{p+1}{2}\right) b \pmod{p}.$$

Kako je $(\frac{p+1}{2}, p) = 1$, dobivamo

$$a \equiv b \pmod{p},$$

odnosno $a = b$ jer su a i b brojevi iz istog potpunog sustava ostataka. Dakle, g je injekcija. □

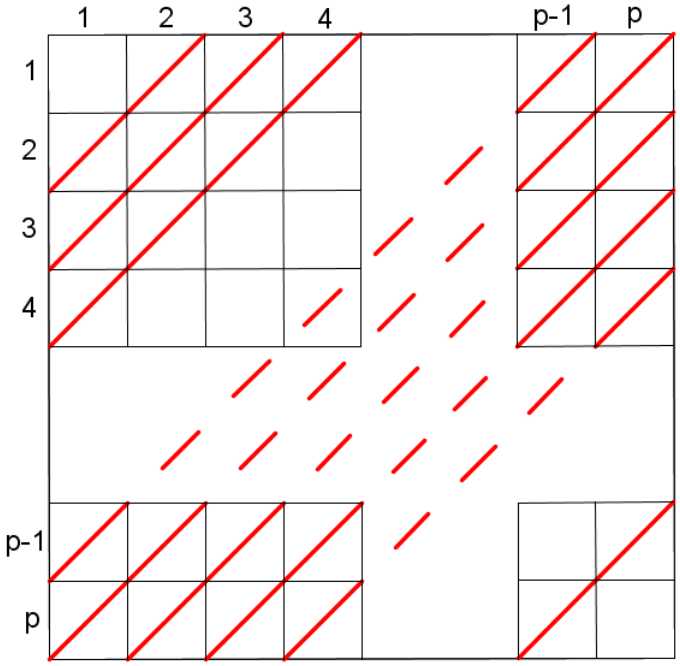
Na Slici 2.3 prikazano je djelovanje funkcije g za $p = 7$ pri čemu smo najgornji redak ploče označili kao prvi ($i = 1$). Očito se postavljene kraljice međusobno ne napadaju pa smo dobili moguće rješenje problema za $p = 7$. Pokazat ćemo da to vrijedi i općenito.



Slika 2.3: Raspored sedam kraljica na šahovskoj ploči 7×7

Teorem 2.4.2. *Neka je $p > 3$ prost broj. Ako rasporedimo p kraljica na šahovskoj ploči $p \times p$ pomoću funkcije $g : \{1, \ldots, p\} \to \{1, \ldots, p\}$ dane s (2.11), onda se kraljice međusobno ne napadaju.*

Dokaz. Podsjetimo, kraljica u šahu može se pomicati za neodređeni broj slobodnih polja u svim smjerovima: vertikalno, horizontalno i dijagonalno. Pretpostavimo da smo kraljice postavili na polja $(i, g(i))$, $i = 1, \ldots, p$. Prema Teoremu 2.4.1 slijedi da svaki redak i stupac sadrži točno jednu kraljicu. Dakle, kraljice se međusobno ne mogu napadati pomicanjem po retku i stupcu. Ostaje provjeriti da se one ne napadaju niti po dijagonali. Uočimo da za sva polja (i, j) koja leže na istoj dijagonali od $(k, 1)$ do



Slika 2.4: Šahovska ploča $p \times p$-crvene dijagonale

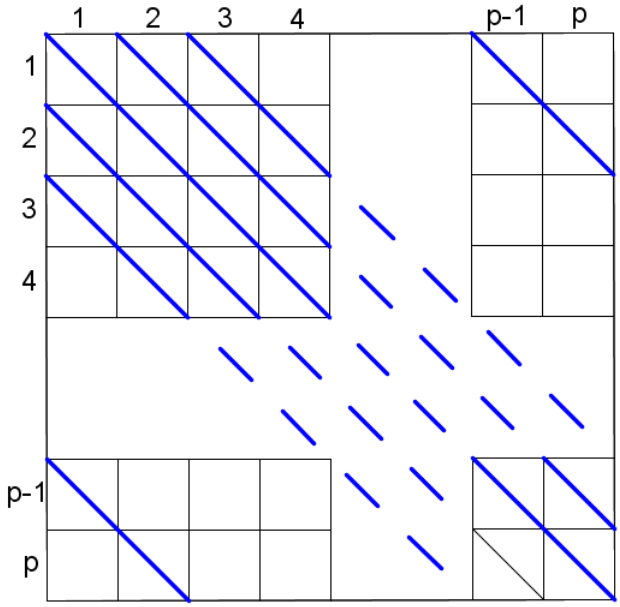
$(1, k)$, odnosno od (p, k) do (k, p), vrijedi da je $i + j = k + 1$, tj. zbroj stupca i retka je konstantan (vidi Sliku 2.5). Očito, $3 \leqslant k + 1 \leqslant 2p - 1$.

Pretpostavimo da imamo dvije kraljice na nekoj od crvenih dijagonala sa Slike 2.5. Označimo njihove pozicije s $(i_1, g(i_1))$ i $(i_2, g(i_2))$. Tada vrijedi

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

pri čemu je $i_1 + g(i_1) = k$ i $i_2 + g(i_2) = k$, $3 \leqslant k \leqslant 2p - 1$. Prema (2.11) dobivamo

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



Slika 2.5: Šahovska ploča $p \times p$-plave dijagonale

Analogno,

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

Iz predhodne dvije kongruencije slijedi

$$\left(\frac{p+3}{2}\right) i_1 \equiv \left(\frac{p+3}{2}\right) i_2 \pmod{p},$$

pa zbog $(\frac{p+3}{2}, p) = 1$ i činjenice da su $i_1, i_2 \in \{1, \ldots, p\}$ slijedi $i_1 = i_2$. Zaključujemo da ne postoji dijagonala koja sadrži dvije kraljice pa prema tome kraljice se ne mogu međusobno napadati po crvenim dijagonalama.

Ostaje pokazati da se kraljice ne mogu napadati niti po plavim dijagonalama (Slika 2.5). Uočimo da za sva polja (i, j) koja leže na istoj plavoj dijagonali vrijedi da je $i - j = l$, tj. razlika stupca i retka je konstanta (vidi Sliku 2.5). Očito, $1-p \leqslant l \leqslant p-1$. Pretpostavimo da imamo dvije kraljice na nekoj od plavih dijagonala sa Slike 2.5. Označimo njihove pozicije kao u predhodnom slučaju s $(i_1, g(i_1))$ i

$(i_2, g(i_2))$. Opet vrijedi

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

pri čemu je $i_1 - g(i_1) = l$ i $i_2 - g(i_2) = l$, $1 - p \leqslant l \leqslant p - 1$. Prema (2.11) dobivamo

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

Analogno,

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

Iz prethodne dvije kongruencije slijedi

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

pa zbog $(\frac{p+1}{2}, p) = 1$ i činjenice da su $i_1, i_2 \in \{1, \ldots, p\}$ slijedi $i_1 = i_2$. Zaključujemo da ne postoji ni plava dijagonala koja sadrži dvije kraljice pa prema tome kraljice se ne mogu međusobno napadati ni po crvenim dijagonalama, a ni po plavim dijagonalama. □

2.4.2 Održavanje turnira

Zamislimo da želimo organizirati turnir u kojem će nastupati n ekipa. Turnir se igra tako da svaka ekipa mora odigrati točnu jednu utakmicu sa svim preostalim ekipama, tzv. *Round Robin* princip. Kako ćemo organizirati takav turnir? U ovom problemu također nam mogu pomoći kongruencije. Označimo s $f(n)$ broj utakmica odigranih između n ekipa. Tada je funkcija $f : \mathbb{N} \to \mathbb{N}_0$ dana rekuzivnom formulom

$$f(1) = 0,$$
$$f(n) = f(n-1) + (n-1),\ n > 1.$$

Rješavanjem ove rekurzivne relacije dolazimo do formule

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

Ako je n paran, u svakom kolu turnira sudjelovat će sve ekipe. Ako pa je n neparan, u svakom kolu turnira jedna ekipa bit će slobodna. Pretpostavit ćemo da je $n = p > 3$ prost broj. Označimo s $g(i, j)$ tim koji u i-tom kolu igra s timom j. Za $i, j \in \{1, \ldots, p\}$ definiramo funkciju

$$g(i, j) \equiv i - j \pmod{p},$$

pri čemu $g(i, j)$ poprima vrijednosti iz potpunog sustava ostataka $\{1, \ldots, p\}$. Ako je $g(i, j) = j$ to znači da tim j igra "sam sa sobom" tj. da je u i-tom kolu slobodan.

Primjer 2.4.3. *Organizacija Round Robin turnira u kojem sudjeluje pet ekipa. Za organizaciju turnira koristit ćemo funkciju g. Označimo ekipe redom brojevima $1, 2, 3, 4$ i 5. Turnir će se odigrati u pet kola. Odredimo vrijednosti funkcije $g(1, j)$, $j = 1, \ldots, 5$. Ona će nam dati parove 1. kola. Dobivamo redom:*

$$g(1, 1) \equiv 1 - 1 = 0 \equiv 5 \pmod{5},$$

$$g(1, 2) \equiv 1 - 2 = -1 \equiv 4 \pmod{5},$$

$$g(1, 3) \equiv 1 - 3 = -2 \equiv 3 \pmod{5},$$

$$g(1, 4) \equiv 1 - 4 = -3 \equiv 2 \pmod{5},$$

$$g(1, 5) \equiv 1 - 5 = -4 \equiv 1 \pmod{5},$$

te zaključujemo da u prvom kolu 1. ekipa igra protiv 5., 2. protiv 4., dok je 3. ekipa slobodna. Na isti način izračunamo za preostala četiri kola i dobivamo sljedeći raspored turnira:

	1.kolo	2.kolo	3.kolo	4.kolo	5.kolo
Ekipa 1	5	-	2	3	4
Ekipa 2	4	5	1	-	3
Ekipa 3	-	4	5	1	2
Ekipa 4	2	3	-	5	1
Ekipa 5	1	2	3	4	-

Neka je $i \in \{1, 2, \ldots, n\}$. Definiramo funkciju $g_i : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ takvu da je

$$g_i(x) = g(i, x),\ x \in \{1, 2, \ldots, n\}.$$

Teorem 2.4.4. *Neka je $i \in \{1, 2, \ldots, n\}$. Funkcija g_i je injektivna.*

Dokaz. Pretpostavimo da vrijedi $g_i(j_1) = g_i(j_2)$ za neke $j_1, j_2 \in \{1, 2, \ldots, n\}$. Slijedi, $i - j_1 \equiv i - j_2 \pmod{p}$, odnosno $j_1 \equiv j_2 \pmod{p}$. Kako su j_1, j_2 elementi potpunog sustava ostataka modulo p slijedi da je $j_1 = j_2$, odnosno g_i je injektivna funkcija. □

Dokazavši da je za svaki $i \in \{1, 2, \ldots, n\}$, funkcija g_i injektivna, pokazali smo da svaka ekipa igra točno jedanput u svakom kolu i.

Teorem 2.4.5. *Neka je p prost. Ako na turniru sudjeluje p ekipa, onda će u svakom kolu točno jedna ekipa biti slobodna.*

Dokaz. Pretpostavimo da su u i-tom kolu ekipe j_1 i j_2 slobodne, tj.

$$g(i, j_1) \equiv j_1 \pmod{p}, \quad g(i, j_2) \equiv j_2 \pmod{p}. \tag{2.12}$$

Razlikujemo slučajeve:

1.slučaj: $i = j_1$

Vrijedi da je $g(i, i) \equiv 0 \pmod{p}$, odnosno $g(i, j_1) = p$ pa je prema pretpostavci $i = j_1 = p$. Nadalje, s obzirom da je $g(i, j_2) \equiv j_2 \pmod{p}$ slijedi

$$i - j_2 = p - j_2 \equiv j_2 \pmod{p}.$$

Stoga je $2j_2 \equiv 0 \pmod{p}$, odnosno $j_2 = p$ pa je $j_1 = j_2$.

2.slučaj: $i \neq j_1$

Ustanovimo da je $i \neq j_2$. Naime, ako bi bilo $i = j_2$, onda bi 1. slučaj povlačio da je $p = i = j_1 = j_2$, što nije.

Kako je ekipa j_1 slobodna slijedi da je $g(i, j_1) \equiv j - j_1 \equiv j_1 \pmod{p}$, odnosno $i \equiv 2j_1 \pmod{p}$. Analogno, $i \equiv 2j_2 \pmod{p}$. Stoga je

$$2j_1 \equiv 2j_2 \pmod{p},$$

tj. $j_1 \equiv j_2 \pmod{p}$ i $j_1 = j_2$.

Dakle, u oba slučaja smo pokazali da je u i-tom kolu točno jedna ekipa slobodna. □

Teorem 2.4.6. *Neka je p prosti te $i, j \in \{1, \ldots, p\}$. Ekipa j je slobodna u $i-tom$ kolu ako i samo ako je $j \equiv \left(\frac{p+1}{2}\right) i \pmod{p}$.*

Dokaz. **⇐:** Pretpostavimo da vrijedi $j \equiv \left(\frac{p+1}{2}\right) i \pmod{p}$. Tada je

$$g(i, j) \equiv i - j \equiv i - \frac{p+1}{2} i = \frac{1-p}{2} i \equiv \frac{p+1}{2} i \equiv j \pmod{p},$$

pa je ekipa j slobodna u i-tom kolu.

$\Rightarrow$: Pretpostavimo da ekipa j je slobodna u i-tom, tj. $g(i,j) \equiv j \pmod{p}$. Ako je $i = j$, onda bi kao u dokazu 1. slučaja Teorema 2.4.5 dobili $i = j = p$ pa vrijedi relacija $j \equiv \left(\frac{p+1}{2}\right) i \pmod{p}$.

Pretpostavimo da je $i \neq j$. Iz $j = g(i,j) \equiv i - j \pmod{p}$ slijedi

$$i \equiv 2j \pmod{p}.$$

Kako je $(\frac{p+1}{2}, p) = 1$, prethodna kongruencija ekvivalentna je kongruenciji

$$i \cdot \frac{p+1}{2} \equiv 2j \cdot \frac{p+1}{2} \pmod{p}.$$

Kako je

$$2j \cdot \frac{p+1}{2} = j \cdot p + j \equiv j \pmod{p},$$

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

□

2.5 Dizajni

2.5.1 Zvijezda s m vrhova

Kongruencije nam mogu pomoći pri konstruiranju zvijezde s m vrhova. Neka je dana kružnica proizvoljnog radijusa. Na njoj odaberemo m jednako udaljenih točaka i redom ih označimo s $0, 1, \ldots, m-1$. Izaberemo ostatak i pri dijeljenju s m takav da su i i m relativno prosti. Svaku točku x, pri čemu je $0 \leqslant x \leqslant m-1$, spajamo s točkom d takvom da vrijedi

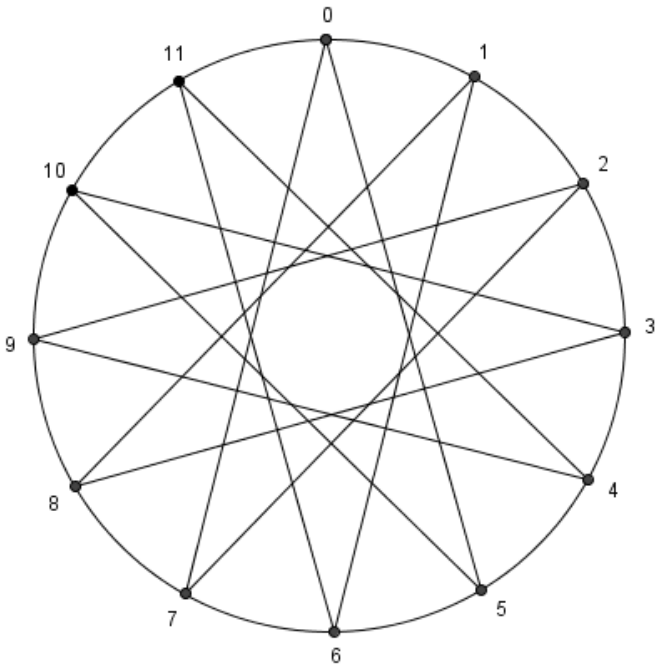
$$d \equiv x + i \pmod{m}.$$

Primjer 2.5.1. *Konstruirat ćemo zvijezdu s 12 vrhova.*

Nacrtajmo kružnicu proizvoljnog radijusa i odredimo na njoj 12 *jednako udaljenih točaka. Točke redom označimo s* $0, 1, \ldots, 11$. *Uzmemo da je* $i = 7$ *jer je* $(7, 12) = 1$.

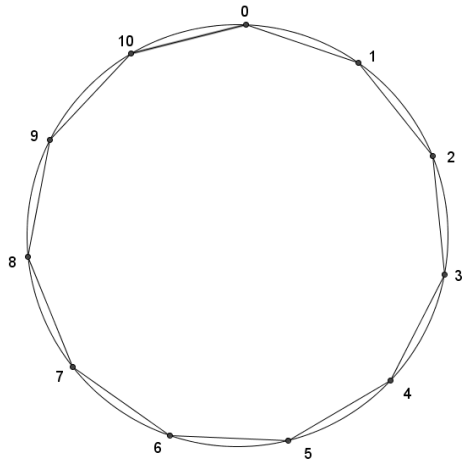
x	$d \equiv x + i \pmod{12}$	d
0	$d \equiv 0 + 7 \pmod{12}$	*7*
1	$d \equiv 1 + 7 \pmod{12}$	*8*
2	$d \equiv 2 + 7 \pmod{12}$	*9*
3	$d \equiv 3 + 7 \pmod{12}$	*10*
4	$d \equiv 4 + 7 \pmod{12}$	*11*
5	$d \equiv 5 + 7 \pmod{12}$	*0*
6	$d \equiv 6 + 7 \pmod{12}$	*1*
7	$d \equiv 7 + 7 \pmod{12}$	*2*
8	$d \equiv 8 + 7 \pmod{12}$	*3*
9	$d \equiv 9 + 7 \pmod{12}$	*4*
10	$d \equiv 10 + 7 \pmod{12}$	*5*
11	$d \equiv 11 + 7 \pmod{12}$	*6*

Točku x spajamo s točkom d prema gornjoj tablici i dobivamo Sliku 2.6. Lako se vidi da bi se isti dizajn dobio da smo uzeli $i = 5$.

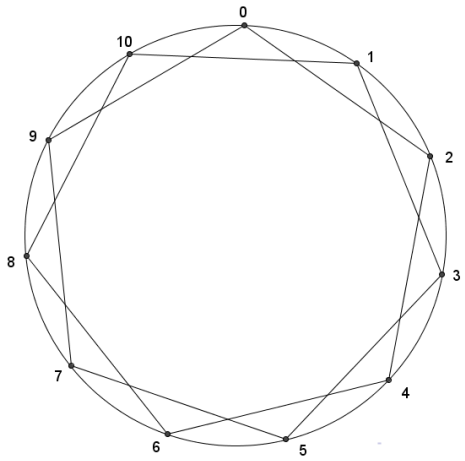


Slika 2.6: Zvijezda s 12 vrhova

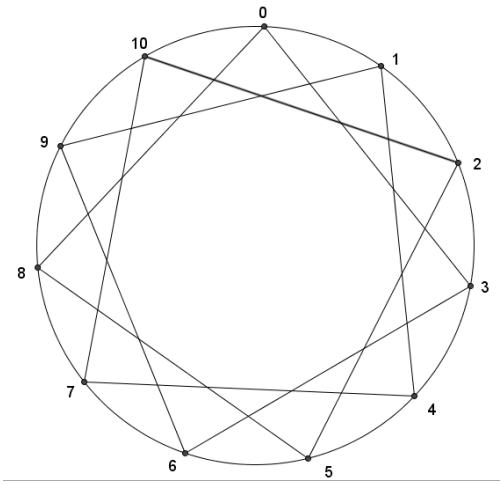
Primjer 2.5.2. *Konstruirajmo sve moguće dizajne za* $m = 11$. *Uočimo da je* m *prost broj iz čega slijedi* $i \in \{1, \ldots, 10\}$.



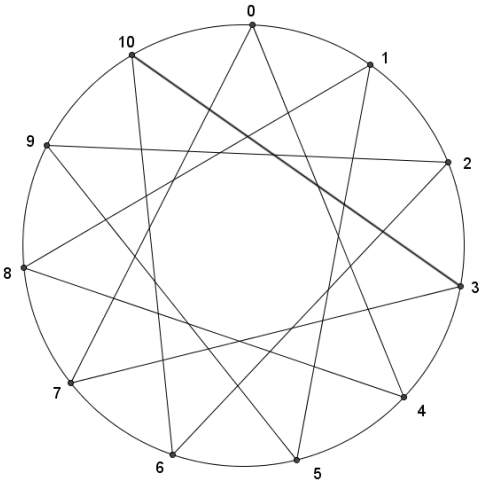
Slika 2.7: Dizaj za $m = 11$ i $i = 1$



Slika 2.8: Dizaj za $m = 11$ i $i = 2$

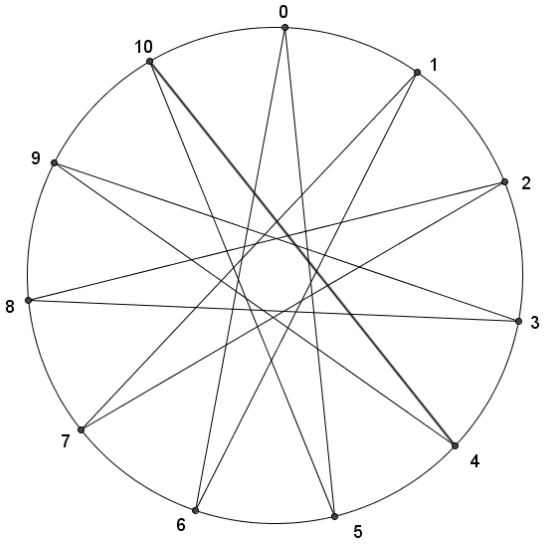


Slika 2.9: Dizaj za $m = 11$ i $i = 3$



Slika 2.10: Dizaj za $m = 11$ i $i = 4$

Lako se uoči da ćemo isti dizaj imati za i *i* j *takve da je* $i + j = 11$, *dakle za* $(i, j) \in \{(1, 20), (2, 9), (3, 8), (4, 7), (5, 6)\}$.



Slika 2.11: Dizaj dobiven za $m = 11$ i $i = 5$

Općenito, broj različitih dizajna dobiveni opisanim postupkom iznositi

$$\frac{m-1}{2}$$

za m prost broj, a

$$\frac{\varphi(n)}{2}$$

za m složen broj, pri čemu je φ Eulerova funkcija.

2.5.2 Dizajn ostataka

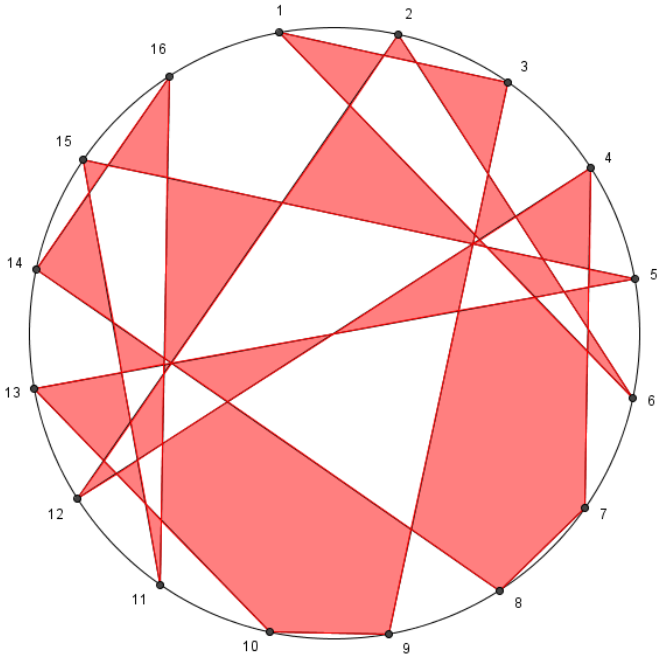
Konstruiranje dizajna ostataka (m, n) slično je konstruiranju zvijezde s m vrhova. Na kružnici proizvoljnog radijusa odaberemo $m-1$ točaka tako da su one jednako udaljene. Takve točke redom označimo $1, 2, \ldots, m-1$. Svaku točku x, pri čemu je $1 \leqslant x \leqslant m-1$, spajamo s točkom d takvom da vrijedi

$$d \equiv nx \pmod{m}.$$

Primjer 2.5.3. *Konstruiraj dizaj ostataka* $(17, 6)$.
Na kružnici proizvoljnog radijusa odaberemo 17 točaka. Točke redom označimo s $1, \ldots, 17$.

x	$d \equiv nx \pmod{m}$	d
1	$d \equiv 6 \cdot 1 \pmod{17}$	*6*
2	$d \equiv 6 \cdot 2 \pmod{17}$	*12*
3	$d \equiv 6 \cdot 3 \pmod{17}$	*1*
4	$d \equiv 6 \cdot 4 \pmod{17}$	*7*
5	$d \equiv 6 \cdot 5 \pmod{17}$	*13*
6	$d \equiv 6 \cdot 6 \pmod{17}$	*2*
7	$d \equiv 6 \cdot 7 \pmod{17}$	*8*
8	$d \equiv 6 \cdot 8 \pmod{17}$	*14*
9	$d \equiv 6 \cdot 9 \pmod{17}$	*3*
10	$d \equiv 6 \cdot 10 \pmod{17}$	*9*
11	$d \equiv 6 \cdot 11 \pmod{17}$	*15*
12	$d \equiv 6 \cdot 12 \pmod{17}$	*4*
13	$d \equiv 6 \cdot 13 \pmod{17}$	*10*
14	$d \equiv 6 \cdot 14 \pmod{17}$	*16*
15	$d \equiv 6 \cdot 15 \pmod{17}$	*5*
16	$d \equiv 6 \cdot 16 \pmod{17}$	*11*

Spajanjem točke x s pripadnom točkom d dobiva se dizajn prikazan na Slici 2.12.



Slika 2.12: Dizajn ostataka (17,6)

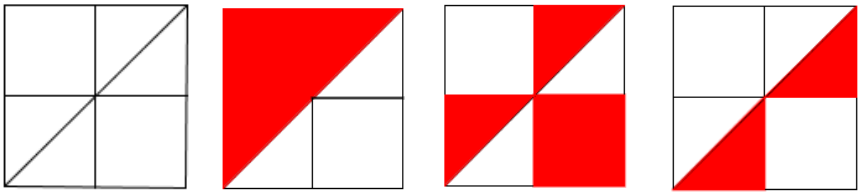
2.5.3 Quilt dizajn

Za kreiranje takozvanih Quilt dizajna poslužit ćemo se tablicama zbrajanja i množenja najmanjih ostataka modulo m. Pogledajmo konkretan primjer kako možemo "dizajnirati" Quilt dizajn.

Primjer 2.5.4. *Konstruiraj Quilt dizajn pomoću tablice zbrajanja najmanjih ostataka modulo 4. Zadano je* $m = 4$. *Konstruira se tablica zbrajanja najmanjih ostataka modulo* 4.

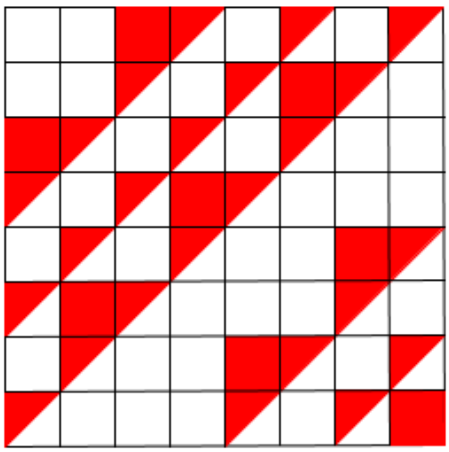
$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	4	1	2

Svakom broju u tablici pridružujemo neki proizvoljan dizaj. U ovom slučaju pridružit ćemo na sljedeći način:



Slika 2.13: Dizajni pridruženi brojevima 0,1,2,3

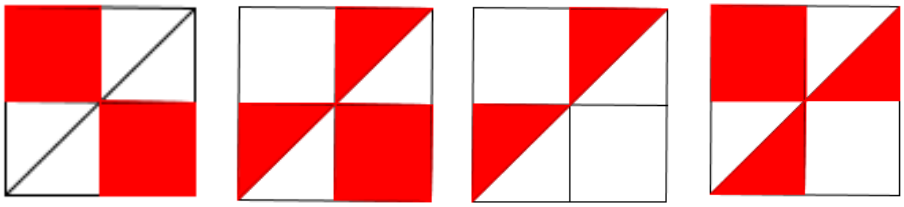
Pridruživanjem dobivamo sljedeći dizajn:



Primjer 2.5.5. *Konstruiraj Quilt dizajn pomoću tablice množenja najmanjih ostataka modulo 4. Konstruira se tablica množenja najmanjih ostataka modulo* 4.

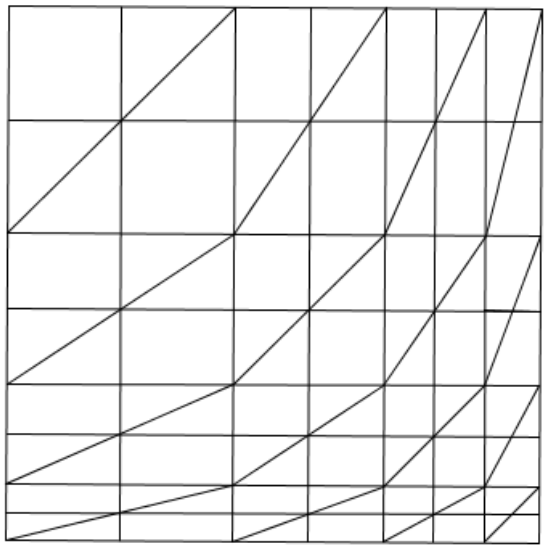
·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Svakom broju u tablici pridružujemo neki proizvoljan dizaj. U ovom slučaju pridružit ćemo na sljedeći način:

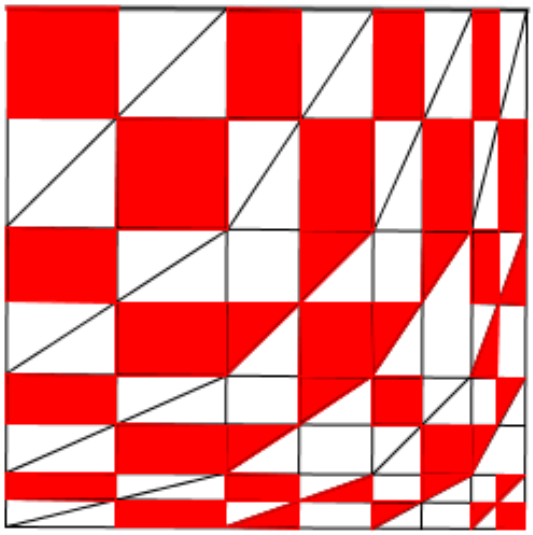


Slika 2.14: Dizajni pridruženi brojevima 0,1,2,3

Svaki broj u tablici množenja najmanjih ostataka modulo 4 se zamijeni s gore odabranim dizajnima koji se postavljaju u mrežu oblika:



Konačno se dobiva dizaj oblika:



Važno je napomenuti da su svi dizajni pridruženi pojedinim brojevima proizvoljni te da smo ih mogli dizajnirati na bilo koji drugi nama zanimljiv način.

2.6 Diofantske jednadžbe

Diofanta se smatra najvećim matematičarem postklasičnog razdoblja grčke matematike i zadnjim velikim europskim matematičarem prije Fibonaccija. Ne postoje točni izvori od kad do kad je živio, ali neka istraživanja pokazuju da je rođen između 200. i 214. godine, a umro između 284. i 298. godine. Diofant je prvi sustavno proučavao jednadžbe s više nepoznanica i tražio je njihova pozitivna racionalna rješenja. Danas njemu u čast takve jednadžbe nazivamo Diofantskim jednadžbama, ali za razliku od Diofanta mi tražimo njihova cjelobrojna rješenja.

Definicija 2.6.1. Diofantska jednadžba *je jednadžba oblika*

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{2.13}$$

pri čemu je f polinom u n varijabli, $n > 1$.
Svaka uređena $n-$torka cijelih brojeva koja zadovoljava jednadžbu (2.13) je rješenje *diofantske jednadžbe.*

Najpoznatiji oblik diofantske jednadžbe je linearna diofantska jednadžba.

Definicija 2.6.2. *Linearna jednadžba oblika*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{2.14}$$

pri čemu su $a_1, \ldots, a_n, b$ *cijeli brojevi i* $n > 0$ *naziva se* linearna diofantska jednadžba.

Upravo za rješavanje jednadžbe (2.14) koriste se kongruencije.

Teorem 2.6.3. *Neka su* a, b, c *cijeli brojevi i* $d = (a, b)$*. Ako* $d \nmid c$*, onda jednadžba*

$$ax + by = c \tag{2.15}$$

nema cjelobrojnih rješenja. Ako $d \mid c$*, onda jednadžba (2.15) ima beskonačno mnogo cjelobrojnih rješenja. Ako je* (x_1, y_1) *jedno rješenje, onda su sva rješenja dana sa*

$$x = x_1 + \frac{b}{d} \cdot t, y = y_1 - \frac{a}{d} \cdot t, t \in \mathbb{Z}. \tag{2.16}$$

Dokaz. Ako (2.15) ima rješenja onda $d \mid c$. Pretpostavimo sada $d \mid c$ i promotrimo kongruenciju

$$ax \equiv c \pmod{b} \tag{2.17}$$

Po Teoremu 1.3.3 kongruencija (2.17) ima rješenja. Ako je x_1 neko njeno rješenje, onda su sva rješenja dana sa

$$x \equiv x_1 + \frac{b}{d} \cdot k \pmod{b}$$

pri čemu je $k = 0, ..., d - 1$. Stoga sva rješenja su oblika

$$x = x_1 + \frac{b}{d} \cdot t, t \in \mathbb{Z}. \tag{2.18}$$

Uvrstimo li (2.18) u (2.15) dobivamo $by = c - ax_1 - \frac{ab}{d} \cdot t = by_1 - \frac{ab}{d} \cdot t$ pa slijedi da je

$$y = y_1 - \frac{a}{d} \cdot t. \tag{2.19}$$

□

Primjer 2.6.4. *Riješi jednadžbu* $5x - 2y = 7$.
Provjerimo prvo dali jednadžba uopće ima rješenja odnosno da li $d \mid c$*. Slijedi,* $d = (5, 2) = 1 \mid 7$ *pa dana jednadžba prema Teoremu 2.6.3 ima rješenje. Promotrimo sada kongruenciju*

$$5x \equiv 7 \pmod{2}$$

tj.

$$x \equiv 1 \pmod{2}.$$

Kako je $5 \equiv 1 \pmod{2}$ *i* $7 \equiv 1 \pmod{2}$*, slijedi da je* $x = 1 + 2t, t \in \mathbb{Z}$*. Uvrštavanjem dobivenog* x *u danu jednadžbu dobivamo da je* $y = 5t - 1, t \in \mathbb{Z}$*.*

Primjer 2.6.5. *Riješi jednadžbu*

$$4x + 8y + 5z = 7. \tag{2.20}$$

S obzirom da $4|4x$ *i* $4|8y$ *vrijedi*

$$\begin{aligned} 5z &\equiv 7 \pmod 4, \\ z &\equiv 3 \pmod 4, \\ z &= 3 + 4k; k \in \mathbb{Z}. \end{aligned}$$

Dobiveni z uvrstimo u (2.20) i dobivamo

$$4x + 8y + 5(3 + 4k) = 7,$$

odnosno

$$x + 2y = -5k - 2. \tag{2.21}$$

Promotrimo sada kongruenciju $x + 2y \equiv -5k - 2 \pmod 2$ *iz koje slijedi da je* $x \equiv k \pmod 2$*, odnosno*

$$x = 2l + k; l, k \in \mathbb{Z}.$$

Uvrštavanjem x i y u (2.20) dobivamo da je

$$y = -l - 3k - 1.$$

Dakle, rješenje diofantske jednadžbe (2.20) su

$$\begin{aligned} x &= 2l + k, \\ y &= -l - 3k - 1, \\ z &= 3 + 4k, \end{aligned}$$

pri čemu su $k, l \in \mathbb{Z}$.

Bibliografija

[1] F. M. Bruckler, *Povijest matematike 2*, Odjel za matematiku Sveučilišta J.J.Strossmayera, Osijek, 2010.

[2] L. N. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag New York, New York, 1995.

[3] T. Koshy, *Elementary Number Theory with Applications*, Elsevier, Burlington, 2007.

[4] A. Tafro, *Kongruencije*, Playmath 1(2003), 9-15.

[5] E. F. Wood, *Self-Checking Codes - An Application of Modular Arithmetic*, Mathematics Teacherk, 80 (1987), 312-316.

[6] Nacionalna i sveučilišna knjižnica u Zagrebu, *Hrvatski ured za ISBN*: `http://www.nsk.hr/isbn/`, (ožujak, 2018.)

Sažetak

Kongruencija je izjava o djeljivosti koju je uveo je C. F. Gauss 1801. Ta je jednostavna oznaka donijela obilje plodova kako u matematičkom svijetu, tako i onom praktičnom. Teorija kongruencija može primijeniti na različite matematičke probleme kao što su rješavanje diofantskih jednadžbi i ispitivanje djeljivosti ali i one iz života kao što su zanimljive slagalice, modularni dizajni, identifikacijski kodovi proizvoda (ISBN, UPC, vozila), održavanje turnira, kalendar itd.

Summary

Congruences is the divisibility statement introduced by C. F. Gauss 1801. That simple label brought abundance in the mathematical world and the practical one. The theory of congruences can be applied to various mathematical problems such as solving Diophantine equations and divisibility tests but also to daily life situations such as puzzles, modular designs, product code identifiers (ISBN, UPC, vehicles), round-robin tournaments, a calendar etc.

Životopis

Zovem se Anja Matić i rođena sam 18.travnja 1995. godine u Čakovcu. Odrasla sam u Hodošanu gdje sam završila i svoje osnovnoškolsko obrazovanje. Od 2009. godine pohađala sam Gimnaziju Josipa Slavenskog u Čakovcu, smjer opća gimnazija.Nakon završenog četvrtog razred položila sam državnu maturu te sam 2013. godine upisala Prirodoslovno-matematički fakultet u Zagrebu, matematički odsjek na kojem sam 2016. godine završila preddiplomski studij Matematika; smjer nastavnički. Te iste godine upisala sam diplomski sveučilišni studij Matematika; smjer nastavnički.