Primjena kongruencija

Užar, Irena

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Irena Užar

Primjena kongruencija

Diplomski rad

Osijek, 2016.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

Irena Užar

Primjena kongruencija

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2016.

Sadržaj

1 Uvod **1**

2 Testovi djeljivosti **4**
2.1 Test djeljivosti s 10 4
2.2 Test djeljivosti s 5 4
2.3 Test djeljivost s 2^i 5
2.4 Testovi djeljivosti s 3 i 9 5
2.5 Test djeljivosti s 11 6
2.6 Odbacivanje devetki 6
2.7 Digitalni korijen 8

3 Modularni dizajni **11**
3.1 Zvijezda s m vrhova 11
3.2 (m, n) dizajn ostataka 11
3.3 Quilt dizajn 13

4 Provjera znamenki **16**
4.1 Binarni kodovi 16
4.2 Identifikacijski brojevi 16
4.3 UPC i EAN-13 18
4.4 Poštanski brojevi 19
4.5 ISBN 22
4.6 Broj vozačke dozvole 23
4.7 Identifikacijski broj vozila 26

5 Problem p-kraljica **28**

6 Round-robin turnir **32**

7 Perpetual kalendar **37**

8 Zaključak **41**

9 Sažetak i ključne riječi **43**

10 Title, summary and keywords **44**

11 Životopis **45**

1 Uvod

Jednu od najznačajnijih relacija u teoriji brojeva, relaciju kongruencija, predstavio je i razvio njemački matematičar Karl Friedrich Gauss 1801. u svom djelu „Disquistiones Arithmeticae“. Gauss se usredotočio na ostatak koji se dobije kada se jedan prirodan broj dijeli s drugim prirodnim brojem. Kongruencija je omogućila da se lakše formuliraju rezultati koji se dobiju u teoriji djeljivosti, tako da se ne prenose nepotrebni izračuni. Relacija kongruencija dijeli puno svojstava s relacijom jednakosti, stoga nije slučajno da je simbol kongruencija „$\equiv$“, koji je uveo Gauss, sličan znaku jednakosti „$=$“.

Definicija. Neka je m pozitivan cijeli broj. Tada je cijeli broj a kongruentan cijelom broju b modulo m ako $m \mid (a-b)$. U simbolima pišemo $a \equiv b \pmod{m}$, m je modul relacije kongruencije.
Ako $m \nmid (a-b)$ onda kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.

Budući da je $a-b$ djeljivo s m ako i samo ako je djeljivo s $-m$, bez smanjenja općenitosti možemo se usredotočiti na pozitivne module i ubuduće će modul m biti prirodan broj.

U sljedećim teoremima su navedena svojstva kongruencija.

Teorem 1.1. *„Biti kongruentan“ je relacija ekvivalencije.*

- $a \equiv a \pmod{m}$ *(refleksivnost).*
- *Ako* $a \equiv b \pmod{m}$, *onda* $b \equiv a \pmod{m}$ *(simetričnost).*
- *Ako* $a \equiv b \pmod{m}$ *i* $b \equiv c \pmod{m}$, *onda* $a \equiv c \pmod{m}$ *(tranzitivnost).*

Teorem 1.2. *Neka je m prirodan broj, a, b, c i d cijeli brojevi, $c \neq 0$. Tada vrijedi:*

1. *Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$ *vrijedi* $a+c \equiv b+d \pmod{m}$.
2. *Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$ *vrijedi* $a-c \equiv b-d \pmod{m}$.
3. *Ako je* $a \equiv b \pmod{m}$ *tada* $ca \equiv cb \pmod{m}$.
4. *Za bilo koji zajednički djeljitelj c od a, b i m,* $a \equiv b \pmod{m}$ *ako i samo ako je* $a/c \equiv b/c \pmod{m/c}$.
5. *Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$ *vrijedi* $ac \equiv bd \pmod{m}$.
6. *Ako je* $a \equiv b \pmod{m}$ *vrijedi* $a^n \equiv b^n \pmod{m}$ *za bilo koji prirodan broj n.*
7. $a \equiv b \pmod{m}$ *ako i samo ako je* $a = b + km$, *za neki cijeli broj k.*
8. $a \equiv b \pmod{m}$ *ako i samo ako a i b imaju isti ostatak pri dijeljenju s m.*
9. *Cijeli broj r je ostatak pri dijeljenju a s m ako i samo ako je* $a \equiv r \pmod{m}$.

Prema teoremu 1.2 (9), svaki cijeli broj a je kongruentan sa svojim ostatkom r modulo m: r se zove najmanji nenegativni ostatak modulo m, ali nadalje u radu ćemo ga zbog jednostavnosti zvati najmanji ostatak. Na primjer, najmanji ostatak od 21, -6 i 7 modulo 4 su 1, 2 i 3, redom. Kako r možemo izabrati između točno m brojeva 0, 1, 2, ..., $(m-1)$, a je kongruentan s točno jednim od njih modulo m.

Skup cijelih brojeva $\mathbb{Z}$ može se podijeliti na m nepraznih disjunktnih klasa koristeći najmanje ostatke, koje zovemo klase kongruencije modulo m. Na primjer, klase kongruencije za modulo 4 su:

$$[0] = (\dots, -8, -4, 0, 4, 8, \dots)$$
$$[1] = (\dots, -7, -3, 1, 5, 9, \dots)$$
$$[2] = (\dots, -6, -2, 2, 6, 10, \dots)$$
$$[3] = (\dots, -5, -1, 3, 7, 11, \dots)$$

Predstavnici klasa [0], [1], [2] i [3] su najmanji ostatci 0, 1, 2 i 3, redom. Općenito, oni ne moraju predstavljati klase, po teoremu 1.2(8) dva cijela broja pripadaju istoj klasi ako i samo ako imaju isti ostatak pri dijeljenju s m, što znači da bilo koji element iz klase $[r]$ može poslužiti kao predstavnik. Na primjer, -4, 5, 10 i 7 mogu biti predstavnici klase [0], [1], [2] i [3], redom. Takav skup brojeva je potpun skup ostataka modulo 4.
Skup od m cijelih brojeva je potpun skup ostataka modulo m ako je svaki cijeli broj kongruentan modulo m s točno jednim od njih.
Dakle, skup cijelih brojeva $\{a_1, \dots, a_m\}$ je potpun skup ostataka modulo m, ako su oni kongruentni modulo m s najmanjim ostacima 0, 1, 2, ..., $(m-1)$ u nekom redoslijedu. Na primjer, skup $\{-12, 9, 6, 23\}$ je potpun skup ostataka modulo 4 jer $-12 \equiv 0 \pmod 4$,
$9 \equiv 1 \pmod 4$, $6 \equiv 2 \pmod 4$ i $23 \equiv 3 \pmod 4$.

Kongruencije oblika $ax \equiv b \pmod m$ zovemo linearne kongruencije. Rješenjem smatramo cijeli broj x_0 takav da vrijedi $ax_0 \equiv b \pmod m$. Na primjer, rješenje kongruencije $2x \equiv 1 \pmod 5$ je 8 jer vrijedi $2 \cdot 8 \equiv 1 \pmod 5$.
Ako je x_0 rješenje kongruencije $ax \equiv b \pmod m$, tada je $ax_0 \equiv b \pmod m$. Pretpostavimo da je $x_1 \equiv x_0 \pmod m$ tada po teoremu 1.2 je $ax_1 \equiv ax_0 \pmod m$ i prema svojstvu tranzitivnosti vrijedi $ax_1 \equiv b \pmod m$. Dakle i x_1 je rješenje kongruencije. Ali x_1 i x_0 su iz iste klase kongruencije, iz toga slijedi da ako je x_0 rješenje, svaki član iz te klase je također rješenje. Za dva rješenja x_0 i x_1 kongruencije $ax \equiv b \pmod b$ kažemo da su ekvivalentna ako je $ax_1 \equiv ax_0 \pmod m$. Ako postoje rješenja kongruencija ima ih beskonačno mnogo. Nas zanimaju samo neekvivalentna rješenja. Sljedeći teorem daje broj neekvivalentnih rješenja i formulu kako ih pronaći ako je kongruencija rješiva.

Teorem 1.3. *Linearna kongruencija $ax \equiv b \pmod m$ je rješiva ako i samo ako $d \mid b$, gdje je $d = (a, m)$. Ako $d \mid b$ tada postoje d neekvivalentna rješenja. Opće rješenje linearne kongruencije dano je s $x = x_0 + \left(\frac{m}{d}\right)t$, gdje $0 \leq t < d$.*

Korolar 1.1. *Linearna kongruencija $ax \equiv b \pmod m$ ima jedinstveno rješenje ako i samo ako vrijedi $(a, m) = 1$.*

U ovom radu ćemo se posvetiti primjeni kongruencija i vidjeti da je ona sastavni dio svakodnevnog života. Najpoznatija primjena je sat. Vrijeme na satu pomiče se koristeći kongruenciju modulo 12. Na primjer ako je 10 sati za 4 sata će biti 14 sati, no međutim sat je podijeljen na 12 jednako raspoređenih točaka, zato se na satu prikazuje $10 + 4 \equiv 14 \pmod{12} \equiv 2 \pmod{12}$. Također svagdje oko nas su brojevi, brojevi na vozačkim dozvolama, knjigama, proizvodima i pokazat ćemo da i ti brojevi koriste kongruencije kao oblik zaštite i provjere. Vidjet ćemo da se pomoću kongruencija mogu stvoriti i prekrasni dizajni. Mnogi sportovi također koriste kongruenciju pri rasporedu po skupinama. I na kraju ćemo vidjeti kako pomoću kongruencija se mogu odrediti dani u tjednu.

2 Testovi djeljivosti

Jedan od jednostavnih primjena teorije kongruencija je u razvijanju testova djeljivosti, odnosno u provjeravanju je li cijeli broj djeljiv s drugim cijelim brojem. Kako bi to pokazali koristit ćemo decimalni prikaz broja n. U svakom brojevnom sustavu vrijedi da svaka znamenka u nizu ima jedinstvenu težinsku vrijednost. Težinska se vrijednost svake znamenke dobije na način da se osnova brojevnog sustava potencira eksponentom čija vrijednost ovisi o položaju znamenke. Krajnji desni eksponent ima vrijednost 0, predzadnji ima 1, itd. Dakle n možemo prikazati u obliku $n = n_k 10^k + n_{k-1}10^{k-1} + \ldots + n_1 10^1 + n_0$. U ovom poglavlju ćemo pokazati testove djeljivosti za 10, 5, 2^i, 3, 9, i 11.

2.1 Test djeljivosti s 10

Propozicija 2.1. *Prirodan broj je djeljiv s* 10 *ako i samo ako mu je zadnja znamenka jednaka* 0.

Dokaz. Kako je $10 \equiv 0 \pmod{10}$ i iz toga po teoremu 1.2 slijedi da je $10^k \equiv 0^k \pmod{10} \equiv 0 \pmod{10}$ za $k = 1, 2, 3 \ldots$ i

$$\begin{aligned} n &\equiv n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \ldots + n_1 \cdot 10 + n_0 \pmod{10} \\ &\equiv n_0 \pmod{10}. \end{aligned}$$

Zbog toga je n djeljiv s 10 ako i samo ako je n_0 djeljiv s 10; to znači, ako i samo ako je $n_0 = 0$, drugim rječima broj je djeljiv s 10 ako mu je zadnja znamenka nula. □

2.2 Test djeljivosti s 5

Dokaz za test djeljivost s 5 je sličan dokazu za test djeljivost s 10.

Propozicija 2.2. *Prirodan broj n je djeljiv s* 5 *ako i samo ako mu je zadnja znamenka jednaka* 0 *ili* 5.

Dokaz. Znamo da je $10 \equiv 0 \pmod{5}$, pa iz teorema 1.2 slijedi $10^k \equiv 0^k \pmod{10} \equiv 0 \pmod{10}$ za $k = 1, 2, 3 \ldots$, pa prema teoremu 1.2 se dobije

$$\begin{aligned} n &\equiv n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \ldots + n_1 \cdot 10 + n_0 \pmod{5} \\ &\equiv n_0 \pmod{5}. \end{aligned}$$

n je djeljiv s 5 ako i samo ako je n_0 djeljiv s 5, a jednoznamenkasti brojevi djeljivi s 5 su samo 0 i 5. □

2.3 Test djeljivost s 2^i

Propozicija 2.3. *Prirodan broj n je djeljiv s 2^i ako i samo ako mu je i zadnjih znamenaka djeljivo s 2^i.*

Dokaz. Zbog toga što je $10 \equiv 0 \pmod 2$, $10^i \equiv 0 \pmod{2^i}$ za sve pozitivne cijele brojeve i. Zbog toga, po teoremu 1.2 slijedi

$$\begin{aligned} n &\equiv n_0 \pmod 2 \\ &\equiv n_1 n_0 \pmod{2^2} \\ &\equiv n_2 n_1 n_0 \pmod{2^3} \\ &\vdots \\ &\equiv n_{i-1} n_{i-2} \cdots n_1 n_0 \pmod{2^i}. \end{aligned}$$

Ova kongruencija dokazuje teorem jer ako je lijeva strana kongruentna s 0 modulo 2^i, onda mora biti i desna strana, a to je jedino moguće ako je $n_{i-1}n_{i-2}\cdots n_1 n_0$ djeljivo s 2^i. □

Iz prethodnog teorema slijedi da je n djeljiv s 2 ako i samo ako mu je zadnja znamenka djeljiva s 2, djeljiv je s 4 ako su mu zadnje dvije znamenke djeljive s 4, djeljiv je s 8 ako su mu zadnje tri znamenke djeljive s 8 itd.
Na primjer broj $n = 245196$, 2 dijeli 6 pa je broj n djeljiv s 2, 4 dijeli 96 pa je broj djeljiv s 4, 8 ne dijeli 196, broj n nije djeljiv s 8.

2.4 Testovi djeljivosti s 3 i 9

Propozicija 2.4. *Prirodan broj je djeljiv s 9 ako i samo ako mu je zbroj znamenaka djeljiv s 9.*

Dokaz. Kako je $10 \equiv 1 \pmod 9$ po teoremu 1.2 vrijedi $10^i \equiv 1 \pmod 9$. Opet prema teoremu 1.2 slijedi

$$\begin{aligned} n &\equiv n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \ldots + n_1 \cdot 10 + n_0 \pmod 9 \\ &\equiv n_k + n_{k-1} + \ldots + n_1 + n_0 \pmod 9. \end{aligned}$$

□

Sličan dokaz vrijedi i s test djeljivosti za 3 jer je $10 \equiv 1 \pmod 3$. Stoga je prirodan broj djeljiv s 3 ako i samo ako mu je zbroj znamenki djeljiv s tri. Primjetimo da to ne vrijedi općenito u testovima s 3^i jer $10 \not\equiv 1 \pmod{27}$.
Primjer, neka je $n = 154305174$. Suma znamenki je 30, kako 3 dijeli 30, 3 dijeli n, ali 9 ne dijeli 30, stoga n nije djeljiv s 9.

2.5 Test djeljivosti s 11

Propozicija 2.5. *Prirodan broj n je djeljiv s* 11 *ako i samo ako je* $(n_0 + n_2 + \ldots) - (n_1 + n_3 + \ldots)$ *djeljiv s* 11*, odnosno djeljiv je ako i samo ako je suma "parnih" pozicija minus suma "neparnih" pozicija (tzv. alternirajuća suma) djeljiva s* 11*.*

Dokaz. Treba primjetiti da je $10 \equiv -1 \pmod{11}$, $10^i \equiv (-1)^i \pmod{11}$, po teoremu 1.2. Dakle ponovno po teoremu 1.2

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

□

Na primjer, broj $n = 125478964$ nije djeljiv s 11 jer razlika $(4 + 9 + 7 + 5 + 1) - (6 + 8 + 4 + 2) = 26 - 20 = 6$ nije djeljiva s 11, a broj $m = 613173825$ je djeljiv s 11 zbog $(5 + 8 + 7 + 3 + 6) - (2 + 3 + 1 + 1) = 22$, a broj 22 je djeljiv s 11, stoga je i m djeljiv 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 $n = n_{2kn}n_{2k-1}\ldots n_1n_0$ palindrom s parnim brojem znamenki. Tada

$$n = (n_0 + n_2 + \ldots + n_{2k-1}) - (n_1 + n_3 + \ldots + n_{2k-1}) \pmod{11} \equiv 0 \pmod{11}$$

jer je n palindrom s parnim brojem znamenki. Dakle, 11 dijeli n. □

Na primjer, palindrom 8456886548 sadrži paran broj znamenki i djeljivi su s 11.

2.6 Odbacivanje devetki

Metoda odbacivanje devetki (casting out nines) odbacuje brojeve koji zbrojeni daju devet, temelji se na kongruenciji $10^i \equiv 1 \pmod{9}$ odnosno da je svaki cijeli broj kongruentan zbroju svojih znamenki modulo 9. Koristi se za provjeru rješenja pri računskim operacijama i otkrivanje eventualnih grešaka.

Primjer 2.1. *Koristeći odbacivanje devetki, provjerite da li je* 309791 *suma brojeva* 25416*,* 69852 *i* 214523*.*

Rješenje.
Računamo

$$\begin{aligned} 25416 &\equiv 2 + 5 + 4 + 1 + 6 \equiv 0 \pmod{9} \\ 69852 &\equiv 6 + 9 + 8 + 5 + 2 \equiv 3 \pmod{9} \\ 214523 &\equiv 2 + 1 + 4 + 5 + 2 + 3 \equiv 8 \pmod{9}. \end{aligned}$$

Nakon toga se zbroje ostatci modulo 9: $0 + 3 + 8 \equiv 11 \pmod 9 \equiv 2 \pmod 9$. Sada treba provjeriti odgovara li to zadanoj sumi: $309791 \equiv 3 + 0 + 9 + 7 + 9 + 1 \equiv 2 \pmod 9$.
Rješenje je vjerojatno točno.

Naime u prošlom primjeru 309791 je suma brojeva 25416, 69852 i 214523, no metodom odbacivanja devetki ukoliko se promijeni redoslijed znamenki također bi dobili da je, na primjer $307991 = 3 + 0 + 7 + 9 + 9 + 1 \equiv 2 \pmod 9$ također točno rješenje, pa stoga odgovor koji daje metoda odbacivanja devetke je definitivno pogrešno ili vjerojatno točno.

Primjer 2.2. *Provjerite da li je produkt brojeva* 3215 *i* 8526 *jednak* 27411090*, koristeći odbacivanje devetki.*

Rješenje.

$$\begin{aligned} 3215 &\equiv 3 + 2 + 1 + 5 \equiv 2 \pmod 9 \\ 8526 &\equiv 8 + 5 + 2 + 6 \equiv 3 \pmod 9. \end{aligned}$$

Pomnožimo dobivene ostatke modulo 9 i dobijemo $2 \cdot 3 \pmod 9 \equiv 6 \pmod 9$. Provjerimo zadani produkt. Suma znamenaka je jednaka $27411090 \equiv 2 + 7 + 4 + 1 + 1 + 0 + 9 + 0 \pmod 9 \equiv 6 \pmod 9$. Dakle produkt brojeva 3215 i 8526 je vjerojatno jednak 27411090.

Za provjeru rezlutata pri računskoj operaciji djeljenja koristi se teorem o djeljenju s ostatkom.

Teorem 2.2. *Neka je a bilo koji cijeli broj i b pozitivan cijeli broj. Tada postoje jedinstveni cijeli brojevi q i r takvi da vrijedi*

$$a = b \cdot q + r,$$

gdje je $0 \leqslant r < b$.

Primjer 2.3. *Koristeći odbacivanje devetki, provjerite da li je* $80387/39 = 2061$ *s ostatkom* 7*.*

Rješenje.
$80387 = (2061 \cdot 39) + 9$

$$\begin{aligned} 2061 &\equiv 2 + 0 + 6 + 1 \equiv 8 \pmod 9 \\ 39 &\equiv 3 \pmod 9 \\ 7 &\equiv 7 \pmod 9. \end{aligned}$$

Izračunamo: $(8 \cdot 3) + 7 \equiv 31 \pmod 9 \equiv 4 \pmod 9$.
Sada pogledamo sumu znamenki od zadanog rješenja $80387 \equiv 8+0+3+8+7 \equiv 8 \pmod 9$.
Rješenje je definitivno krivo (točno rješenje je 2061 s ostatkom 8).

2.7 Digitalni korijen

Digitalni korijen od pozitivnog cijelog broja n je jednoznamenkasti pozitivan cijeli broj čija se vrijednost računa iteracijom da se pronađe suma s znamenaka broja n, ukoliko se ne dobije jednoznamenkasti broj traži se suma znamenaka od s, sve dok se ne dođe do jednoznamenkastog broja $\rho(n)$, koji je digitalni korijen od broja n.
Ako želimo pronaći digitalni korijen od broja 547, zbrojimo njegove znamenke $5+4+7 = 16$, dobili smo dvoznamenkasti broj čije znamenke nastavljamo dalje zbrajati $16 = 1 + 6 = 7$. Primjetimo da koristeći metodu odbacivanja devetki možemo izračunati digitalni korijen, vrijedi $547 \equiv 7 \pmod 9$.
Generalno, neka je $n = (a_n \cdots a_1 a_0)_{10}$ i neka je $\rho(n)$ njegov digitalni korijen. Tada je $\rho(n) \equiv (a_n + \cdots + a_1 + a_0) \pmod 9$. Dakle, digitalni korijen broja n je ostatak pri djeljenju n s 9, s jednim izuzetkom, ako je ostatak 0 onda je digitalni korijen 9.
Svojstva digitalnog korijena:

1. $\rho(\rho(n)) = \rho(n)$.

   Dokaz. Zato što je $0 \leq \rho(n) < 9$ vrijedi $\rho(\rho(n)) = \rho(n)$. □

2. $\rho(m + n) = \rho(\rho(m) + \rho(n))$.

   Dokaz. Ako je $n = (a_n \dots a_1 a_0)_{10}$ i $m = (b_n \dots b_1 b_0)_{10}$, tada je $\rho(n) = (a_n + \ldots + a_1 + a_0) \pmod 9$ i $\rho(m) = (b_n + \ldots + b_1 + b_0) \pmod 9$ tada je po teoremu 1.2 $\rho(\rho(n) + \rho(m)) \equiv (a_n + \ldots + a_1 + a_0) + (b_n + \ldots + b_1 + b_0) \pmod 9$.
   S druge strane $m + n = ((a_n \dots a_1 a_0) + (b_n \dots b_1 b_0))_{10}$ i $\rho(n + m) \equiv (a_n + \ldots + a_1 + a_0) + (b_n + \ldots + b_1 + b_0) \pmod 9$.
   Dakle $\rho(m + n) = \rho(\rho(m) + \rho(n))$. □

3. $\rho(mn) = \rho(\rho(m)\rho(n))$.

   Dokaz. Neka su m i n zadani kao u prethodnom slučaju pod 2.
   Tada $mn \equiv ((a_n \dots a_1 a_0)(b_n \dots b_1 b_0))_{10}$ iz čega slijedi
   $\rho(nm) \equiv (a_n + \ldots + a_1 + a_0)(b_n + \ldots + b_1 + b_0) \pmod 9$.
   S druge srane prema teoremu 1.2 $\rho(\rho(n)\rho(m)) \equiv (a_n + \ldots + a_1 + a_0)(b_n + \ldots + b_1 + b_0) \pmod 9$. Iz čega slijedi $\rho(mn) = \rho(\rho(m)\rho(n))$.

   □

Primjer 2.4. *Pronađite digitalni korijen potpunih kvadratnih brojeva.*

Rješenje.
Po teoremu 2.2, svaki cijeli broj se može prikazati u obliku $9k + r$, $0 \leqslant r < 9$ tako $n \equiv r \pmod 9$ i kao je $n^2 \equiv r^2 \pmod 9$. Kako je $r \equiv r - 9 \pmod 9$,

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

Dakle, n^2 je kongruentno 0, 1, 4 ili 7 i njegov digitalni korijen može biti 1, 4, 7 ili 9.

Na temelju ovog primjera može se provjeriti da li je pozitivan cijeli broj kvadrat nekog broja.

Primjer 2.5. *Odredite može li* $2^{2011} + \cdots + 2^{2016}$ *biti kvadrat nekog broja.*

Rješenje.
Pomoću kongruencije $2^3 \equiv -1 \pmod 9$ slijedi da je digitalni korijen:

$$\begin{aligned} 2^{2011} + \cdots + 2^{2016} &= (2^3)^{670} \cdot 2 + (2^3)^{670} \cdot 2^2 + (2^3)^{671} + (2^3)^{671} \cdot 2 + (2^3)^{671} \cdot 2^2 + (2^3)^{672} \\ &= (-1) \cdot 2 + (-1) \cdot 4 + (-1) + (-1) \cdot 2 + (-1) \cdot 4 + (-1) \\ &= -2 - 4 - 1 - 2 - 4 - 1 \equiv -14 \pmod 9 \equiv 4 \pmod 9. \end{aligned}$$

Digitalni korijen je jednak 4, što znači da broj $2^{2011} + \cdots + 2^{2016}$ može biti kvadrat nekog broja.

Treba primjetiti da ako je neki broj kvadrat tada mu digitalni korijen mora biti 1, 4, 7 ili 9. No ako mu je digitalni korijen jedan od 1, 4, 7 ili 9, broj ne mora biti kvadrat, primjerice digitalni korijen broja 67 je broj 4, a broj 67 nije kvadrat niti jednog broja.

Primjer 2.6. *Dokažite da je digitalni korijen od produkta prostih blizanaca brojeva, osim* 3 *i* 5*, jednak* 8*.*

Rješenje.
Blizanci prostih brojeva su parovi prostih brojeva čija razlika iznosi 2. Svaki prosti broj p veći od tri je kongruentan $\pm 1 \pmod 6$. To je radi toga što ukoliko bi bio kongruentan 0, 2 ili 4 modulo 6, bio bi paran broj, a ako bi bio kongruentan 3 modulo 6, onda bi trebao biti 3 (jedini brojevi kongruentni 3 modulo 6 su višekratnici broja 3). Dakle svaki $p > 3$ mora biti kongruentan 1 ili 5 modulo 6. Budući da je $5 \pmod 6 \equiv -1 \pmod 6$, svaki prost broj

$p > 3$ se može zapisati u obliku $6k + 1$ i $6k - 1$.
Uzmimo par blizanaca prostih brojeva $6k + 1$ i $6k - 5$. Njihov produkt je

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

Dakle digitalni korijen produkta je jednak 8.

Brojevi oblika $f(n) = 2^{2^n} + 1$ zovu se Fermatovi brojevi, gdje je n nenegativan cijeli broj. Fermat je smatrao da su svi brojevi toga oblika prosti. Prvih pet članova niza f_0, f_1, f_2, f_3, f_4 jesu prosti, no za f_5 se pronašao rastav na faktore. U sljedećem primjeru ćemo pogledati kako izgleda digitalni korijen Fermatovih brojeva.

Primjer 2.7. *Digitalni korijen $\rho(f_n)$ od n-tog Fermatovog broja f_n za $n \geqslant 1$ je zadan s*

$$\rho(f_n) = \begin{cases} 5, \textit{ ako je } n \textit{ paran} \\ 8, \textit{ inače} \end{cases}$$

Rješenje.
Upotrijebit ćemo rekurzivnu relaciju koju zadovoljavaju Fermatovi brojevi

$$f_n = (f_{n-1} - 1)^2 + 1$$

iz koje slijedi

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2.$$

Dokaz ćemo provesti indukcijom.

Pogledajmo za $n = 1$, $f_1 = 5$ pa vrijedi da je digitalni korijen od neparnog broja jednak 5.
Pretpostavimo da je istina za $n - 1$ i napravimo korak indukcije za n.

$$\begin{aligned} \rho(f_n) &= \rho(f_{n-1}^2 - 2f_{n-1} + 2) \\ &= \rho(f_{n-1}^2) - 2\rho(f_{n-1}) + 2. \end{aligned}$$

Ako je n neparan tada vrijedi

$$\rho(f_n) = 5^2 - 2 \cdot 5 + 2 \equiv 8 \pmod 9.$$

Ako je n paran tada vrijedi

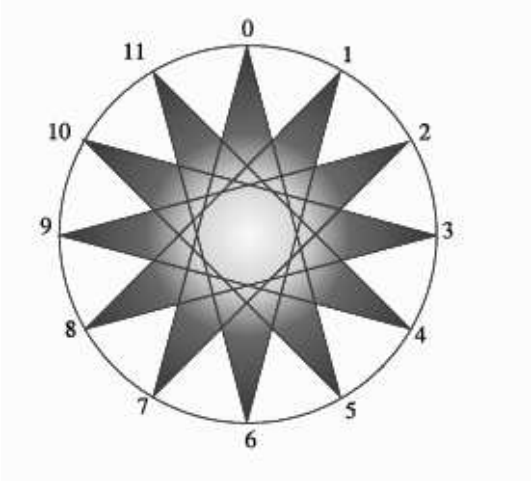
$$\rho(f_n) = 8^2 - 2 \cdot 8 + 2 \equiv 5 \pmod 9.$$

3 Modularni dizajni

Kongruencije se mogu koristiti za kreiranje različitih dizajna. U ovom poglavlju ćemo pokazati kako se kreira zvijezda s m vrhova, dizajn ostataka (m, n) i dizajn dobiven pomoću tablica množenja i zbrajanja najmanjih ostataka modulo m (quilt dizajni).

3.1 Zvijezda s m vrhova

Kako bi konstruirali zvijezdu s m vrhova na kružnici proizvoljnog polumjera označimo m jednako udaljenih točaka i označimo ih s 0 do $m-1$ modulo m. Izaberemo najmanji ostatak i modulo m za koji vrijedi da su i i m relativno prosti, tj. $(i, m) = 1$. Spojimo svaku točku x s točkom $x + i$ modulo m, točnije 0 spojimo s $i \pmod m$, 1 spojimo s $1 + i \pmod m$ i nastavimo tako dok sve točke ne budu spojene te obojimo dobivenu zvijezdu.
Primjer, konstruirajmo zvijezdu s 12 vrhova i odaberemo ostatak 7, $(12, 7) = 1$. Spojimo 0 s 7, 1 s 8, 2 s 9, ... i 11 s 6. Na taj smo način dobili zvijezdu s 12 vrhova prikazanu na slici 1.



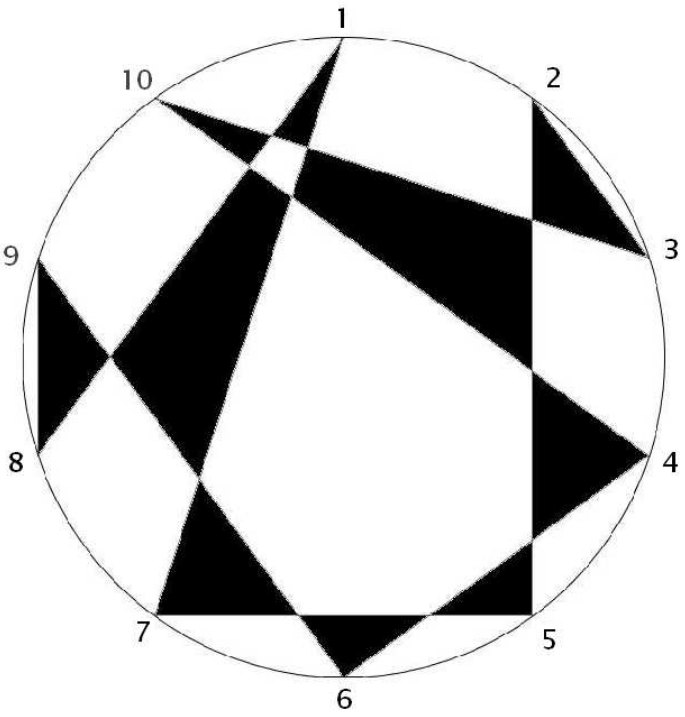
Slika 1. Zvijezda s 12 vrhova

3.2 (m, n) dizajn ostataka

Da bi konstruirali (m, n) dizajn ostataka, gdje je $1 \leqslant n < m$ i $(m, n) = 1$, podijelimo kružnicu pomoću $m-1$ točaka na $m-1$ lukova jednake duljine i označimo ih s 1 do $m-1$ te svaku točku x spojimo s točkom nx modulo m. Obojimo različite regije formirane na ovaj način da bi kreirali zanimljive dizajne.
Za konstruiranje $(11, 8)$ dizajna ostataka podijelimo krug na 10 jednako raspoređenih točaka i označimo ih s 1 do 10. Pomnožimo svaki nenul ostatak modulo 11 s 8, označimo ostatke modulo 11 s x:

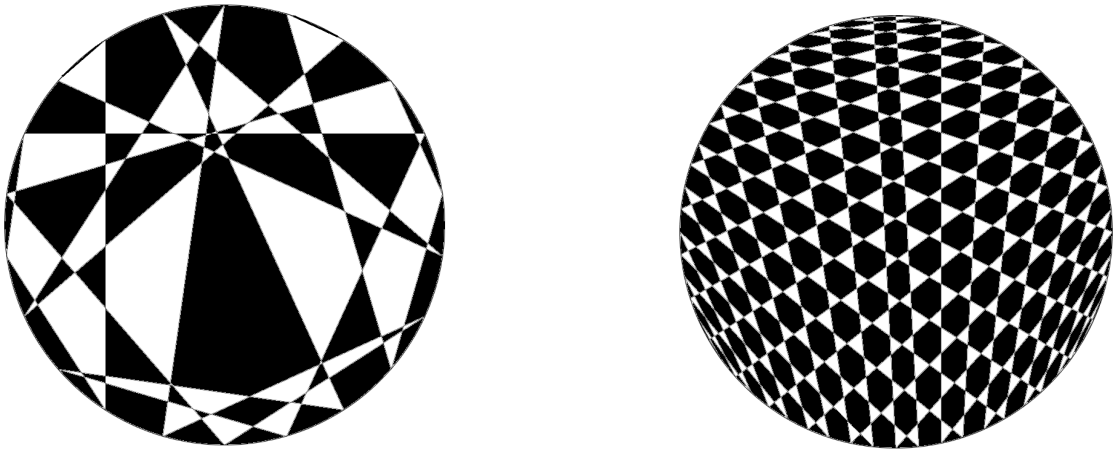
x	1	2	3	4	5	6	7	8	9	10
$x \cdot 8$	8	16	24	32	40	48	56	64	72	80
$8x \pmod{11}$	8	5	2	10	7	4	1	9	6	3

Dakle, spajanjem točaka 1 i 8, 2 i 5, ... te 10 i 3 nastaje dizajn prikazan na slici 2.



Slika 2. (11,8) dizajn ostataka

Na slici 3. su prikazani još neki dizajni.



Slika 3. (23,16) i (61,59) dizajn ostataka

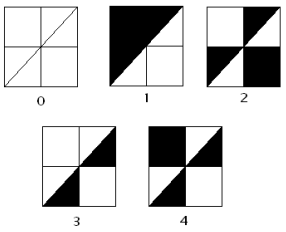
3.3 Quilt dizajn

Zanimljivi dizajni mogu se kreirati koristeći tablice zbrajanja i množenja najmanjih ostataka modulo m, odnosno možemo na taj način kreirati quilt dizajne.

Na primjer, za $m = 5$ prvo treba konstruirati tablicu zbrajanja najmanjih ostataka 0 do 4 modulo 5.

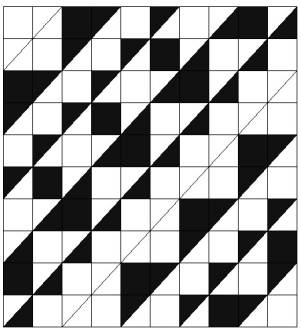
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Zatim se svakom unosu u tablici dodijeli neki element dizajna. Elementi dizajna koji će se upotrijebiti za zbrajanje najmanjih ostataka modulo 5 su prikazani na slici 4.



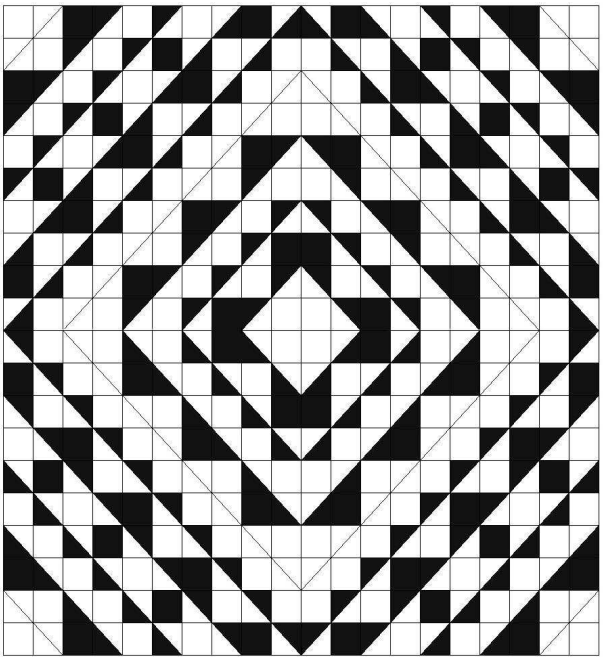
Slika 4. Osnovni dizajni modulo 5

Sada se zamijeni svaki unos u glavnom dijelu tablice s odgovarajućim elementom dizajna. Slika 5. prikazuje dobiveni dizajn.



Slika 5. Quilt dizajn modulo 5

Ovaj dizajn se može koristiti za dobivanje novih dizajna. Ako se ovaj dizajn okrene prvo njegovoj desnoj strani ruba, i zatim taj dobiveni dizajn se okrene o donji rub (zrcalno se preslika prema dolje) dobije se dizajn prikazan na slici 6.

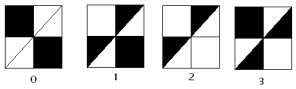


Slika 6. Quilt dizajn s okretajima modulo 5

Za sljedeći primjer konstruira se tablica množenja najmanjih ostatak modulo 4.

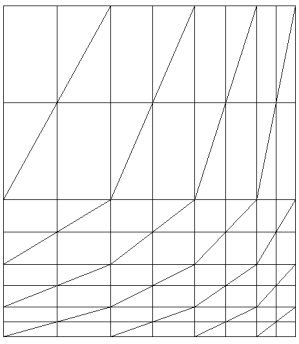
+	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Za svaki unos u tablici upotrijebit će elementi dizajna prikazani na slici 7.

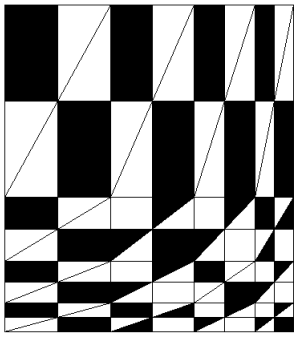


Slika 7. Elementi dizajna modulo 4

Svaki unos u tablici množenja najmanjih ostataka modulo 4 zamijeni se s elementima dizajna i ukoliko ih se postavi u mrežu oblika:

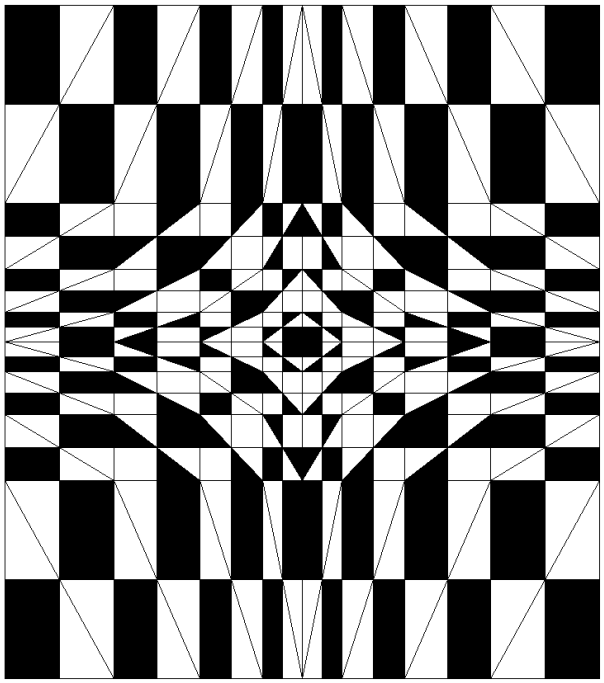


Dobije se dizajn prikazan na slici 8.



Slika 8. Quilt dizajn modulo 4

Također okretanjem dizajna prvo o njegovom desnom rubu, a zatim okretanjem dobivenog dizajna o njegov donji rub dobijemo dizajn na slici 9.



Slika 9. Quilt dizajn s okretajima modulo 4

4 Provjera znamenki

Teorija kodiranja je grana matematike koja se bavi analiziranjem kodova koji se prenose kanalima te otkrivanjem i ispravljanjem grešaka koje pri tome mogu nastati. U ovom poglavlju ćemo pokazati kako kongruencije mogu pomoći pri pronalaženju i ispravljanju grešaka u poslanim porukama.

4.1 Binarni kodovi

Kada se poruka šalje kanalima (kao što je telefonska linija), poruka se pretvara (kodira) u bitove i postaje binarni kod. Primatelj, kada primi poruku, pokušava dekodiranjem vratiti poruku u prvobitno stanje. Naravno pri procesu slanja mogu se dogoditi greške koje se trebaju otkriti i popraviti.
Kako bi se otkrile greške binarnom kodu se, prije slanja, dodaje paritetni bit. To je zapravo znamenka provjere koja broj jedinica u binarnom kodu uvijek održava parnim. Paritetni bit x_{n+1} se dodaje na svaki binarni string $x_1x_2 \dots x_n$ i definiran je s $x_{n+1} \equiv x_1 + x_2 + ... + x_n \pmod 2$. Ukoliko binarni string sadrži neparan broj jedinica dodaje se 1, a 0 ako ima paran broj jedinica.
Pretpostavimo da je dan osmobitni niz 11101001. Paritetni bit je $x_9 \equiv 1+1+1+0+1+0+0+1 \pmod 2 \equiv 1 \pmod 2$, te je poslana poruka 111010011. Pretpostavimo da primimo string 111010111, kako on sadrži neparan broj jedinica, pogreška se dogodila tijekom slanja poruke. Paritetnim bitom možemo otkriti greške, a ako znamo lokaciju greške, promjenom toga bita možemo dobiti prvobitnu poruku.

4.2 Identifikacijski brojevi

Mnoge institucije (kao što su banke, izdavači knjiga, pošte, ...) i kompanije koriste identifikacijske brojeve za označavanje svojih proizvoda, dokumenata, računa, ljudi i mnogih drugih stvari. Identifikacijski brojevi sadrže kodirane informacije stvari koje označavaju i tipično mogu biti numerički (sastoje se od znamenki) ili alfanumerički (tj. sastoje se od znamenki i slova engleske abecede). Dvije informacije koje nose su bitne, dužina identifikacijskog broja (ukupan broj znamenki ili slova) i pozicija svake znamenke ili slova. Identifikacijski broj dužine n označava se s $d_1d_2 \dots d_n$, gdje je d_1 prva znamenka ili slovo broja, d_2 druga znamenka ili slovo sve od d_n koja je zadnja znamenka ili slovo.
Svaki dan identifikacijski brojevi se šalju putem telefona, skeniraju ili unose u računala, prenose internetom ili šalju putem pošte. Pri tome mogu nastati pogreške, odnosno mogu se zamijeniti jedna ili više znamenki.
Bitno je da se identifikacijski brojevi prenose točno. Na primjer, ukoliko se u prodavaonici bar-kod s proizvoda skenira pogrešno, moguće je da će kupcu biti naplaćena cijena od 100 kn za proizvod koji košta 15 kn.
Najčešće pogreške pri slanju koje se događaju su greška jedne znamenke (jedna znamenka u identifikacijskom broju promijeni vrijednost) i greška zamjene mjesta dvije uzastopne znamenke.

Kako bi se to spriječilo trebalo je razviti metodu koja bi takve pogreške prepoznala, odnosno koja bi prepoznala kada je identifikacijski broj pogrešan. Ta metoda je metoda znamenke provjere koja najviše ovisi o skalarnom produktu dva vektora i modulu.
Znamenka provjere je najčešće dodatna znamenka koja služi kako bi se provjerio primljeni identifikacijski broj. Može se nalaziti na bilo kojem mjestu u identifikacijskom broju, no najčešće je to zadnja znamenka broja.

Definicija. Skalarni produkt vektora $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ i $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ je definiran s

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i y_i.$$

Primjer 4.1. *Svaki bankovni ček se sastoji od osmoznamenkastog broja $d_1 d_2 \ldots d_8$ iza kojeg slijedi znamenka provjere d, definirana s $d \equiv (d_1, d_2, \ldots, d_8) \cdot (7, 3, 9, 7, 3, 9, 7, 3) \pmod{10}$. Treba izračunati znamenku provjere za identifikacijski broj* 24512932.

Rješenje.

$$\begin{aligned} d &\equiv (2, 4, 5, 1, 2, 9, 3, 2) \cdot (7, 3, 9, 7, 3, 9, 7, 3) \pmod{10} \\ &\equiv 2 \cdot 7 + 4 \cdot 3 + 5 \cdot 9 + 1 \cdot 7 + 2 \cdot 3 + 9 \cdot 9 + 3 \cdot 7 + 2 \cdot 3 \equiv 2 \pmod{10}. \end{aligned}$$

Devetoznamenkasti broj čeka je 245129322.

Najčešće metode znamenke provjere su linearne metode koje znamenku provjere računaju na sljedeći način $d_n \equiv -(d_1, d_2, \ldots, d_{n-1})(w_1, \ldots, w_{n-1}) \pmod{n}$, gdje je $d_1 \ldots d_{n-1}$ identifikacijski broj, d_n znamenka provjere, $(w_1, \ldots, w_{n-1})$ težinski vektor i n modul metode znamenke provjere.

Teorem 4.1. *Pretpostavimo da je $d_n \equiv -(d_1, d_2, \ldots d_{n-1})(w_1, \ldots, w_{n-1}) \pmod{n}$. Greška zamjene jedne znamenke (d_i se zamijeni s d_i') neće biti otkrivena ako i samo ako je $(d_i' - d_i)w_i$ djeljivo s n. Greška zamjene dvije uzastopne znamenke ($d_i d_j \to d_j d_i$) neće biti otkrivena ako i samo ako je $(d_i - d_j)(w_i - w_j)$ djeljivo s n.*

Dokaz. Ako je d_i zamijenjena da d_i' tada se skalarni produkt znamenke provjere poslanog i primljenog identifikacijskog broja razlikuje za $(d_i' - d_i)w_i$ i ukoliko je to djeljivo s n slijedi da je $(d_i' - d_i)w_i \equiv 0 \pmod{n}$, tj. tada zamijenjena znamenka nema utjecaja na rezultat te se pogreška ne može otkriti.
Slično vrijedi i za pogrešku zamjene dvije uzastopne znamenke. Poslani i primljeni identifikacijski broj, odnosno znamenka provjere se razlikuje za

$$(d_i w_i + d_j w_j) - (d_j w_i + d_i w_j) = (d_i - d_j)(w_i - w_j).$$

Ukoliko je $(d_i - d_j)(w_i - w_j) \equiv 0 \pmod{n}$ grešku nije moguće otkriti.

□

4.3 UPC i EAN-13

UPC (The Universal Product Code) koristi se u Sjedinjenim Američkim Državama za identificiranje proizvoda. Sastoji se od 12 znamenki $d_1, \ldots, d_{12}$ od kojih prvih šest znamenki označavaju državu i proizvođača, sljedećih 5 identificiraju proizvod i znamenke provjere d_{12} koja se računa po formuli

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

Primjer 4.2. *Izračunati znamenku provjere Kellogg's proizvoda Product* 19*, ako je* 11*-znamenkasti broj* $0 - 38000 - 01912$.

Rješenje.

$$\begin{aligned} d_{12} &\equiv -(d_1, d_2, \ldots, d_{11}) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(0, 3, 8, 0, 0, 0, 0, 1, 9, 1, 2) \cdot (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(0 + 3 + 24 + 0 + 0 + 0 + 0 + 1 + 27 + 1 + 6) \pmod{10} \\ &\equiv 8 \pmod{10}. \end{aligned}$$

Znamenka provjere je 8, a UPC broj je 0-38000-01912-8.

1974. osnovana je radna skupina iz dvanaest europskih zemalja koja je razvila sustav EAN (European Article Number) koji se koristi za kodiranje proizvoda i koji je kompatibilan s UPC sustavom.

Slika 10. EAN-13 bar-kod

EAN-13 se sastoji od trinaestoznamenkastog broja $d_1 d_2 \ldots d_{13}$ od kojih prve tri znamenke označavaju zemlju proizvođača (385 je Hrvatska), sljedećih 9 znamenki označavaju proizvođača i proizvod i zadnja znamenka je znamenka provjere. EAN bar-kod sastoji se od tamnih i svijetlih linija koje predstavljaju čitljivu prezentaciju informacija.
Znamenka provjere d_{13} u EAN-13 kodu mora zadovoljiti uvjet

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

dakle

$$d_{13} \equiv -(d_1, d_2, \ldots, d_{12}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10}.$$

Sada ćemo pokazati tu metodu na primjeru.

Primjer 4.3. *Izračunati znamenku provjere d_{13} u EAN-13 kodu Kandit čokolade s rižom čiji je 12-znamenkasti kod* 385888104047*.*

Rješenje.

$$\begin{aligned} d_{13} &\equiv -(d_1, d_2, \ldots, d_{12}) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ d_{13} &\equiv -(3, 8, 5, 8, 8, 8, 1, 0, 4, 0, 4, 7) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3) \pmod{10} \\ &\equiv -(3 + 24 + 5 + 24 + 8 + 24 + 1 + 0 + 4 + 0 + 4 + 21) \pmod{10} \\ &\equiv 2 \pmod{10}. \end{aligned}$$

Znamenka provjere je 2, a EAN-13 identifikacijski broj je 385-8881-04047-2.

Primjetimo da znamenka provjere UPC-a i EAN-13 mogu otkriti sve pogreške zamjene jedne znamenke. Prema teoremu 4.1 ukoliko d_i zamijenimo s d_i' mogu se dogoditi dva slučaja:

- Ukoliko su obje znamenke pomnožene s težinskom vrijednosti 3. Tada vrijedi $3(d_i' - d_i) \not\equiv 0 \pmod{10}$, zato što $d_i' \neq d_i$, $d_i' - d_i \neq 0$, a d_i i d_i' su znamenke od 0 do 9 i 3 i 10 su relativno prosti brojevi, $3(d_i' - d_i)$ nikad neće biti djeljivo s 10.
- Ukoliko su obje znamenke pomnožene s težinskom vrijednosti 1. Tada vrijedi $(d_i' - d_i) \neq 0$ zato što $d_i' \neq d_i$, $d_i' - d_i \neq 0$, a d_i i d_i' su znamenke od 0 do 9 te $(d_i' - d_i)$ nikad neće biti djeljivo s 10.

Ako zamijenimo dvije uzastopne znamenke, ukoliko d_i je pomnožena s težinom 3, a d_j s težinom 1, težinska suma se razlikuje za $(3d_i + d_j) - (3d_j + d_i) = 2(d_i - d_j)$, greške dva uzastopna broja se neće prepoznati ukoliko $2(d_i - d_j) \equiv 0 \pmod{10}$, odnosno greške zamjene neće biti prepoznate ako je razlika $d_i - d_j = 5$. Na isti način, ako d_i je pomnožena s težinom 1, a d_j s 3, suma se razlikuje za $(d_i + 3d_j) - (d_j + 3d_i) = 2(d_j - d_i)$, također se greška neće prepoznati ako je $d_j - d_i = 5$. Dakle, metoda znamenke provjere UPC i EAN-13 identifikacijskog broja neće prepoznati grešku zamjene dva uzastopna broja ukoliko je $|d_i - d_j| = 5$.

4.4 Poštanski brojevi

Kako bi ubrzala isporuku pošte, pošta u Sjedinjenim Američkim Državama koristi bar-kodove za kodiranje poštanskih brojeva. POSTNET (POSTal Numeric Encoding Technique) bar-kod mogu biti petoznamenkasti poštanski broj (32 stupca), devetoznamenkasti poštanski broj plus četveroznamenkasti kod (52 stupca) ili jedanaestoznamenkasti kôd mjesta dostave (62 stupca), koji sadrže i binarne brojeve i znamenku provjere.

Slika 11. Znamenka POSTNET koda

Bar-kodovi se sastoje od dugih stupaca (ili cijelih stupaca) koji predstavljaju 1 i kratkih stupaca (pola stupca) koji predstavljaju nulu. Dva krajnja stupca su uvijek dugi i oni se ignoriraju. Jednu znamenku predstavlja 5 stupaca, pa se stupci grupiraju u blokove od 5 stupaca i znamenku provjere čini zadnjih 5 stupaca. Kako bi pretvorili decimalne brojeve u binarne koristi se shema koja je temeljena na shemi koju su 1940-tih koristili Bell Telephone Labs (danas Lucent Technologies).

Koriste se dva duga stupca i tri kratka stupca čijih kombinacija ima točno $\frac{5!}{2!3!} = 10$ i oni predstavljaju 10 znamenki.

	Težina pozicije stupca	
Numerička	Binarni zapis	Bar-kod
Vrijednost	74210	74210
1	00011	
2	00101	
3	00110	
4	01001	
5	01010	
6	01100	
7	10001	
8	10010	
9	10100	
0	11000	

Svakoj kombinaciji od 5 stupaca se izračunava numerička vrijednost dodavanjem težina na dva duga stupca. Težina se dodjeljuje na pozicije stupaca, i to s lijeva na desno, 7, 4, 2, 1 i 0. Jedina kombinacija  koja predstavlja nulu je izuzetak jer joj je težina 11, a prepisuje se vrijednost nula.
Ako imamo poštanski broj $z_1z_2z_3z_4z_5$, kako bi otkrili moguću grešku na njega se dodaje znamenka provjere d koja se računa na sljedeći način:

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

Na primjer, znamenka provjere poštanskog broja 90210 je

$$\begin{aligned} d &\equiv -(9+0+2+1+0) \pmod{10} \\ &\equiv -12 \pmod{10} \equiv 8 \pmod{10}. \end{aligned}$$

Znamenka provjere je 8, bar-kod je prikazan na slici 12.

Slika 12. Bar-kod poštanskog broja

1983. godine pošta u SAD-u predstavila je poštanski broj + 4 koda, koji je također sadržavao znamenku provjere. Na primjer, ako devetoznamenkasti poštanski broj iznosi 90210-9049, njegovu znamenku provjeru izračunali bi na sljedeći način:

$$\begin{aligned} d &\equiv -(9+0+2+1+0+9+0+4+9) \pmod{10} \\ &\equiv -34 \pmod{10} \equiv 6 \pmod{10}. \end{aligned}$$

Na slici 13. je prikazan bar-kod.

Slika 13. Bar-kod poštanskog broja

Pošta u SAD-u je 1993. godine uvela jedinstveni kôd mjesta dostave kako bi se identificirala sva moguća mjesta dostave i omogućilo razvrstavanje pošte neposredno prije dostave. Kreiran je dodavanjem 10 stupaca na postojeći poštanski broj + 4 koda. Dodani stupci predstavljaju dva dodatna broja koji mogu predstavljati dva zadnja broja kućne adrese, broja poštanskog sandučića, sandučić ruralnog puta (rural route box) ili sandučić ugovorenog puta autoceste (highway contract route box). Na primjer ako je 90210-9049-01 kôd mjesta dostave, mjesto dostave je 01, a znamenku provjere d računamo na sljedeći način:

$$\begin{aligned} d &\equiv -(9+0+2+1+0+9+0+4+9+0+1) \pmod{10} \\ &\equiv -35 \pmod{10} \equiv 5 \pmod{10}. \end{aligned}$$

Znamenka provjere iznosi 5, a bar-kod za kôd mjesta isporuke je prikazan na slici 14.

Slika 14. Bar-kod poštanskog broja

4.5 ISBN

Pojavom računala izdavači knjiga počeli su razmišljati o tome kako stvoriti efikasan računalni sustav koji bi na jedinstven i jednostavan način identificirao broj izdanih knjiga. Osmišljen je sustav ISBN (International standard book number) kojeg su u Ujedinjenom Kraljevstvu 1968. godine predstavili J.Whitaler & Sons., a godinu dana kasnije R.R Bowker Company ISBN sustav je predstavio u SAD-u. Od 1972. godine gotovo sve izdane knjige u svijetu imaju jedinstveni ISBN broj.
ISBN se prvo sastojao od 10 znamenaka podijeljenih u 4 dijela: prva znamenka je označavala govorno područje države u kojoj je izdana (0 englesko govorno područje[1], 1 ostale države), sljedeće dvije znamenke su označavale izdavača knjiga, zatim sljedećih 6 znamenki kôd knjige koje je odredio izdavač i na kraju znamenka provjere d, $0 \leq d \leq 9$ i X označava 10, računala se na način: $d \equiv -(x_1, x_2, \ldots, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11}$, gdje $x_1, \ldots, x_9$ označavaju prvih devet znamenki ISBN broja.

Primjer 4.4. *Koristeći ISBN shemu kodiranja, treba izračunati znamenku provjere d ako je prvih devet znamenki* $0-19-28004-1$ *(The Concise Dictionary of Mathematics, C. Clapham, 2ed edition, Oxford University Press,* 1996.*).*

Rješenje.

$$\begin{aligned} d &\equiv -(x_1, x_2, \ldots, x_9) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0, 1, 9, 2, 8, 0, 0, 4, 1) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0 \cdot 10 + 1 \cdot 9 + 9 \cdot 8 + 2 \cdot 7 + 8 \cdot 6 + 0 \cdot 5 + 0 \cdot 4 + 4 \cdot 3 + 1 \cdot 2) \pmod{11} \\ &\equiv -157 \pmod{11} \equiv 8 \pmod{11}. \end{aligned}$$

[1]Australija, Engleski govorni dio Kanade, Novi Zeland, Južnoafrička republika, Velika Britanija, Sjedinjene Američke Države i Zimbabve.

Dakle, znamenka provjere je 8 i ISBN je 0-19-280041-8.

ISBN shema kodiranja s 10 znamenki je otkrivala sve greške zamjene jedne znamenke. Pretpostavimo da je d_i zamijenjena s d_i' ($d_i \neq d_i'$). Težinske sume znamenke provjere bi se tada razlikovale za $k(d_i - d_i')$, za $2 \leq k \leq 10$. Budući da je 11 prost broj, tada su k i 11 relativno prosti brojevi i $d_i - d_i' \neq 0$, $k \cdot (d_i - d_i')$ nikad neće biti djeljivo s 11.
Također je otkrivala sve greške zamjene dvije uzastopne znamenke. Ukoliko zamijenimo dvije znamenke d_i s d_j ($d_i \neq d_j$) tada će se težinske sume razlikovati za $(d_i - d_j)(k - (k-1)) = (d_i - d_j)(k - k + 1) = (d_i - d_j) \neq 0$.

Kako bi se uskladio ISBN broj s EAN-13 2001. godine povećan je broj znamenki s 10 na 13, dodavanjem prefiksa 978 ispred devetoznamenkosatog ISBN broja i izračunavanjem nove znamenke provjere po pravilima EAN-13 koda. Od 1. siječnja 2007. ISBN agencije omogućuju samo dobivanje ISBN 13 identifikacijskog broja, a desetoznamenkasti ISBN više ne vrijedi.

Primjer 4.5. *Koristeći EAN-*13 *shemu kodiranja, treba izračunati znamenku provjere d ako je prvih dvanaest znamenki* $978 - 019 - 280041$.

Rješenje.

$$\begin{aligned} d &\equiv -(x_1, x_2, \ldots, x_{12}) \cdot (1,3,1,3,1,3,1,3,1,3,1,3) \pmod{10} \\ &\equiv -(9,7,8,0,1,9,2,8,0,0,4,1) \cdot (1,3,1,3,1,3,1,3,1,3,1,3) \pmod{10} \\ &\equiv -(9+21+8+3+9+6+8+12+1) \pmod{10} \\ &\equiv -99 \pmod{10} \equiv 1 \pmod{10}. \end{aligned}$$

ISBN 13 je 978-019-280041-1.

4.6 Broj vozačke dozvole

U Sjedinjenim Američkim Državama, metoda koja se koristi pri određivanju broja vozačke dozvole varira od savezne države do savezne države. Neke savezne države koriste metodu provjere znamenaka kada dodjeljuju broj vozačke dozvole kako bi otkrili krivotvorine ili greške. Na primjer, savezna država Utah dodjeljuje osmoznamenkasti broj $d_1 d_2 \ldots d_8$ u sekvencijalnom poretku i onda slijedi znamenka provjere d_9 definirana $d_9 \equiv \sum_{i=1}^{8} (10-i) d_i \pmod{10}$. Američko Kemijsko Društvo koristi isti princip pri registriranju kemikalija, dok Kanadska provincija Newfoundland koristi skoro identičnu shemu za vozačke dozvole.

Primjer 4.6. *Izračunati znamenku provjere d_9 u vozačkoj dozvoli u saveznoj državi Utah ako je osmoznamenkasti broj* 14921994.

Rješenje.

$$\begin{aligned} d_9 &\equiv \sum_{i=1}^{8}(10-i)d_i \pmod{10} \\ &\equiv (9,8,7,6,5,4,3,2)\cdot(1,4,9,2,1,9,9,4) \pmod{10} \\ &\equiv (9+32+63+12+5+36+27+8) \pmod{10} \\ &\equiv 192 \pmod{10} \equiv 2 \pmod{10}. \end{aligned}$$

Cijeli broj vozačke dozvole iznosi 149219942.

Primjetimo da ova metoda kao i metoda ISBN 10 otkriva sve greške zamjene jedne znamenke i greške zamjene dviju uzastopnih znamenki.

Pri dodjeljivanju broja vozačkih dozvola mogu se koristiti i kompliciranije metode znamenke provjere, kao što neke savezne države i čine. Arkansas, Novi Meksiko i Tennessee dodaju znamenku provjere d_8 na sedmeroznamenkasti broj $d_1d_2\ldots d_7$ definiranu na način:
Neka je

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

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, osim kada je $x=0$, koristi se slovo A kao znamenka provjere.

Primjer 4.7. *Ako je sedmeroznamenkasti identifikacijski broj vozačke dozvole, u saveznoj državi Tenneesse, jednak* 0243579*, odredite znamenku provjere* d_8*.*

Rješenje.

$$\begin{aligned} x &\equiv -(d_1,d_2,\ldots,d_7)\cdot(2,7,6,5,4,3,2) \pmod{11} \\ &\equiv -(0,2,4,3,5,7,9)\cdot(2,7,6,5,4,3,2) \pmod{11} \\ &\equiv -(0+14+24+15+20+21+18) \pmod{11} \\ &\equiv 192 \pmod{11} \equiv 2 \pmod{11}. \end{aligned}$$

Kako je $x=9$, tada je $d_8=9$ i cijeli broj vozačke dozvole je 02435799.

Primjetimo također da ova metoda provjere znamenke otkriva sve greške zamjene jedne znamenke, i hvata sve greške zamjene dva uzastopna broja, ukoliko se zamjene prve dvije znamenke d_1 i d_2, tada $(d_2-d_1)(7-2)=5(d_2-d_1)$, 5 i 11 su relativno prosti.

Pri konstruiranju identifikacijskih brojeva ponekad se koriste i egzotične sheme kodiranja. Tako, na primjer, Norveška koristi shemu dvije znamenke provjere pri dodijeli registracijskog broja svojim građanima. Registracijski broj se sastoji od jedanaest znamenki $d_1, d_2, \ldots, d_{11}$, gdje zadnje dvije znamenke su znamenke provjere i računaju se na sljedeći način:

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

Registracijski brojevi kojima je d_{10} ili d_{11} jednaka "10" nisu dodijeljeni.

Primjer 4.8. *Registracijski broj u Norveškoj počinje s devetoznamenkastim brojem* 051268214. *Treba izračunati dvije znamenke provjere u identifikacijskom broju.*

Rješenje.
Prvo ćemo izračunati d_{10}:

$$\begin{aligned} d_{10} &\equiv -(d_1, d_2, \ldots, d_9) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11} \\ &\equiv -(0, 5, 1, 2, 6, 8, 2, 1, 4) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11} \\ &\equiv -(0 + 35 + 6 + 2 + 48 + 72 + 8 + 5 + 8) \pmod{11} \\ &\equiv -184 \pmod{11} \equiv 3 \pmod{11}. \end{aligned}$$

Druga znamenka provjere d_{11} je:

$$\begin{aligned} d_{11} &\equiv -(d_1, d_2, \ldots, d_{10}) \cdot (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0, 5, 1, 2, 6, 8, 2, 1, 4, 3) \cdot (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \pmod{11} \\ &\equiv -(0 + 20 + 3 + 4 + 42 + 48 + 10 + 4 + 12 + 6) \pmod{11} \\ &\equiv -149 \pmod{11} \equiv 5 \pmod{11}. \end{aligned}$$

Dakle dvije znamenke provjere su 3 i 5, i stoga je identifikacijski broj 05126821435.

Također se može provjeriti je li identifikacijski broj ispravan.

Primjer 4.9. *Provjerite da li je* 06516330708 *ispravan norveški identifikacijski broj.*

Rješenje.
Treba provjeriti znamenke 0 i 8. Prvo provjeravamo znamenku 0.

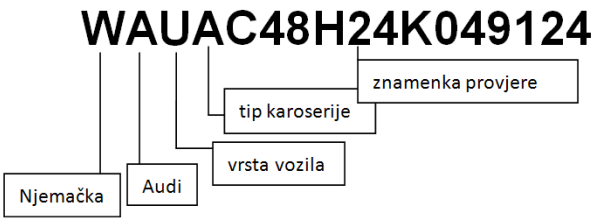
$$\begin{aligned} d_{10} &\equiv -(0, 6, 5, 1, 6, 3, 3, 0, 7, 3) \cdot (3, 7, 6, 1, 8, 9, 4, 5, 2) \pmod{11} \\ &\equiv -(0 + 42 + 30 + 4 + 48 + 27 + 12 + 0 + 14) \pmod{11} \\ &\equiv -177 \pmod{11} \equiv 10 \pmod{11}. \end{aligned}$$

Dakle d_{10} je trebala biti 0, no međutim ona iznosi 10, a identifikacijski brojevi kojima je znamenka provjere 10 nisu ni dodjeljivani, stoga ovo nije ispravan identifikacijski broj u Norveškoj.

Ova metoda otkriva sve greške zamjene jedne znamenke i sve greške zamjene dvije uzastopne znamenke.

4.7 Identifikacijski broj vozila

Ranih 80-tih godina prošlog stoljeća automobilima i kamionima proizvođači su počeli dodjeljivati jedinstvene identifikacijske brojeve vozila (VIN). VIN se tipično sastoji od 17 alfanumeričkih simbola (tj. slova engleske abecede ili znamenki), te sadrži kodirane informacije za zemlju u kojoj je vozilo napravljeno, proizvođača, vrstu vozila, tip karoserije, tip motora, seriju, sigurnosni sustav, liniju vozilu, znamenku provjere, godinu modela, kôd tvornice i redni broj tvornice.



Slika 15. Identifikacijski broj vozila za Audi A4 iz 2004. godine [2]

Znamenka provjere se nalazi na devetom mjestu (nije smještena na kraj, nego u sredini). Za izračunavanje d_9 koristi se sljedeći algoritam:

- Pretvori slova A do Z u brojeve prema tablici 1. Koriste se sva slova i brojevi, osim slova I, O i Q. To daje broj $d_1 d_2 \ldots \not{d}_9 \ldots d_{17}$.

Tablica 1:

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

- Dodijeli težine $8, 7, \ldots, 2, 10, 9, \ldots, 2$ na pozicije $d_1 d_2 \ldots \not{d}_9 \ldots d_{17}$, svakom posebno.
- Izračunaj najmanji nenegativni ostatak $r \equiv (d_1 d_2 \ldots \not{d}_9 \ldots d_{17}) \cdot (8, 7, \ldots, 2, 10, 9, \ldots, 2) \pmod{11}$.

[2] Generiran pomoću `http://randomvin.com/`.

- Znamenka provjere je jednaka:

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

Algoritam ćemo demonstrirati na sljedećem primjeru.

Primjer 4.10. *Izračunati znamenku provjere identifikacijskog broja vozila* $WAUAC48H-4K049124$.

Rješenje.
Prvo treba pretvoriti slova iz VIN u numerički kod:

VIN:	W	A	U	A	C	4	8	H	-	4	K	0	4	9	1	2	4
numerički kod	6	1	4	1	3	4	8	8	-	4	2	0	4	9	1	2	4

Vertikalno poredamo svaki numerički kod s odgovarajućom težinom:

numerički kod	6	1	4	1	3	4	8	8	-	4	2	0	4	9	1	2	4
Težina:	8	7	6	5	4	3	2	10	-	9	8	7	6	5	4	3	2

Sada treba izračunati težinsku sumu r modulo 11:

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

Kako je $0 \leq 2 < 10$, znamenka provjere je 2.

5 Problem p-kraljica

Veoma poznat problem i u matematici i u računarstvu je problem n-kraljica, gdje je ideja postaviti n-kraljica na $n \times n$ šahovsku ploču na takav način da se one međusobno ne napadaju. U ovom poglavlju ćemo pokazati kako se kongruencije mogu primjeniti za rješavanje postavljanja p-kraljica na $p \times p$ šahovsku ploču, gdje je p prost broj veći od 3.
Problem p-kraljica se rješava tako da se se kraljice postavljaju redak po redak. Definira se funkcija $f(i)$ koja označava poziciju (indeks stupca) od i-te kraljice, gdje je $1 \leq i \leq p$.
Rekurzivna definicija od f dana je na sljedeći način:

$$\begin{aligned} &f(0) = 0 \\ &f(i) \equiv f(i-1) + \left(\frac{p+1}{2}\right) \pmod{p}, \quad \text{gdje je } 1 \leq i \leq p \\ &f(p) = p. \end{aligned}$$

Rješavanjem rekurzivne definicije, pomoću iteracija, dolazi se do eksplicitne formule za $f(i)$ koja glasi:

$$f(i) \equiv \left(\frac{p+1}{2}\right) i \pmod{p}, \quad \text{gdje je } 1 \leq i \leq p, \tag{1}$$

gdje $f(i)$ predstavlja najmanji ostatak od $(p+1)i/2$ modulo p, a ostatak 0 je interpretiran s p.

Teorem 5.1. *Funkcija f je injekcija.*

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

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

Tada

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

Kako je $((p+1)/2, p) = 1$, slijedi da je $i \equiv j \pmod{p}$. Ali i i j su najmanji ostatci modulo p, dakle $i = j$.

□

Budući da je funkcija f injekcija, ona dodjeljuje u svaki redak i svaki stupac točno jednu kraljicu, kao što pokazuje sljedeća tablica.

Tablica 2: Problem 7-kraljica

i \ j	1	2	3	4	5	6	7
1	·	·	·	Q	·	·	·
2	Q	·	·	·	·	·	·
3	·	·	·	·	Q	·	·
4	·	Q	·	·	·	·	·
5	·	·	·	·	·	Q	·
6	·	·	Q	·	·	·	·
7	·	·	·	·	·	·	Q

Idući teorem dokazuje da ovako postavljene kraljice ne napadaju jedna drugu, što nam je preostalo dokazati.

Teorem 5.2. *Ne postoje dvije kraljice smještene na $p \times p$ šahovsku ploču prema raspodijeli f koje napadaju jedna drugu.*

Dokaz. Kako svaki stupac i svaki redak sadrži točno jednu kraljicu, ne postoje dvije kraljice koje napadaju jedna drugu preko retka ili stupca. Dakle dovoljno je pokazati da se ne mogu napasti preko bilo koje jugoistočne ili sjevernoistočne dijagonale.
Za svaku sjeveroistočnu dijagonalu, suma $i + j$ od indeksa retka i i stupca j je konstanta k, gdje je $2 \leq k \leq 2p$. Očito, trebamo samo gledati dijagonalu, gdje je $3 \leq k \leq 2p - 1$.
Pretpostavimo da imamo dvije takve kraljice na pozicijama (i_1, j_1) i (i_2, j_2). Onda

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

Prema tome,

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

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

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

Odatle je,

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

Slično,

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

Te dvije kongruencije povlače da je $(p+3)i_1/2 \equiv (p+3)i_2/2$, dakle $i_1 \pmod p \equiv i_2 \pmod p$, zbog $(p,(p+3)) = 1$. Dakle $i_1 = i_2$, jer su najmanji pozitivni ostaci modulo p. Tada, po kongruenciji (2), $j_1 = j_2$. Dakle, ne postoji sjeveroistočna dijagonala koja sadrži dvije kraljice.
Kako bi pokazali da ne postoji jugoistočna dijagonala koja sadrži dvije kraljice, primjetimo da za svaku takvu dijagonalu $i - j$ je konstanta l, gdje je $1 - p \leq l \leq p - 1$. Očito možemo pretpostaviti $l \neq 1 - p$ i $l \neq p - 1$.
Pretpostavimo da jugoistočna dijagonala sadrži dvije kraljice na poziciji (i_1, j_1) i (i_2, j_2). Tada

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

Odnosno,

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod p \quad \text{i} \quad j_2 \equiv \left(\frac{p+1}{2}\right) i_2 \pmod p. \tag{3}$$

Gdje $i_1 - j_1 = l = i_2 - j_2$. Tada

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

Na sličan način bi dobili i

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

Te dvije kongruencije pokazuju $i_1 = i_2$, jer $((p+1)/2, p) = 1$ i i_1 i i_2 su najmanji ostatci modulo p. Po kongruenciji (3) $j_1 = j_2$, dakle niti jedna jugoistočna dijagonala ne sadrži dvije kraljice.
Iz toga slijedi, da ne postoje dvije kraljice na $p \times p$ šahovskoj ploči koje napadaju jedna drugu.

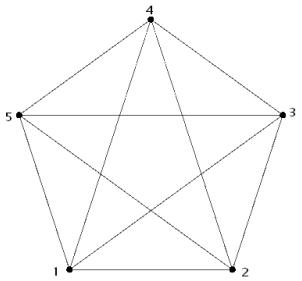
□

Algoritam za postavljanje p-kraljica na $p \times p$ šahovsku ploču

- Postavi prvu kraljicu u stupac $(p+1)/2$. U svaki sljedeći redak, u pomaku za $(p+1)/2$ polja (modulo p) u smjeru kazaljke postavi kraljicu na dobiveno polje i nastavi tako sve dok kraljica nije postavljena u svaki redak.

6 Round-robin turnir

U svijetu sporta, često se timovi i igrači raspoređuju u skupine po n na takav način da svaki tim igra sa svakim drugim timom točno jedanput. Turnir koji se odigrava prema takvom rasporedu se naziva round-robin turnir, te ćemo pokazati kako se sastavlja raspored za takav turnir. Pretpostavimo da imamo n timova, označimo ih s 1 do n. Turnir se može predstaviti potpunim grafom s n vrhova, gdje svaki vrh predstavlja tim i svaki brid spojen s vrhovima i i j predstavlja utakmicu između timova i i j.
Na primjer na slici 16. je prikazan round-robin turnir s pet timova.



Slika 16. Round-Robin turnir s pet timova

Neka g_n označava broj utakmica koji ukupno n timova odigra u round-robin turiniru. Može se prikazati rekurzivno:

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

Rješavanjem rekurzivne relacije, dobivamo

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

Na primjer, pet timova će igrati 10 utakmica.
Kongruencija se može upotrijebiti za sastavljanje rasporeda turnira po skupinama. Ako imamo paran broj timova, svaki tim može igrati s drugim timom, ali ako je broj timova neparan tada nemaju svi timovi par, dakle jedan tim je slobodan u tom kolu. Dakle, kadgod je n neparan, dodajemo jedan umjetni tim X, ako tim igra s timom X u nekom kolu, to znači da je slobodan u tom kolu.

Neka $g(i,j)$ označava tim koji igra u kolu i s timom j. Ako je $g(i,j) = j$, tim j je slobodan u tom kolu. Definiramo g s

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

gdje se 0 modulo p označava s p.

Na primjer, neka je $p = 5$. Tada $g(1,1) \equiv 0 \pmod 5$, dakle $g(1,1) = 5$, $g(1,2) \equiv -1 \pmod 5$, odnosno $g(1,2) = 4$, $g(1,3) \equiv -2 \pmod 5$, tj. $g(1,3) = 3$, tim 3 je slobodan u prvom kolu. Tako nastavimo dalje i dobijemo raspored za turnir po skupinama za 5 timova, prikazan u tablici 3.

Tablica 3: Raspored po skupinama za 5 timova

Kolo i \ Tim j	1	2	3	4	5
1	5	4	slobodan	2	1
2	slobodan	5	4	3	2
3	2	1	5	slobodan	3
4	3	slobodan	1	5	4
5	4	3	2	1	slobodan

Preostaje dokazati da ovako definirana funkcija g konstruira raspored po skupinama.

Teorem 6.1. *Točno je jedan tim slobodan u svakom kolu.*

Dokaz. Pretpostavimo da su timovi j_1 i j_2 slobodni u kolu i. Tada

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

Slučaj 1. Ako je $i = j_1$, onda $i = j_1 = p$. Zato što $g(i, j_2) \equiv j_2$, $i - j_2 \equiv j_2 \pmod p$. Iz toga slijedi

$$\begin{aligned} p - j_2 &\equiv j_2 \pmod p \\ 2j_2 &\equiv 0 \pmod p \\ j_2 &\equiv 0 \pmod p. \end{aligned}$$

Odnosno $j_2 = p$. Dakle $j_1 = j_2$.
Slučaj 2. Ako $i \neq j_1$, onda $g(i, j_1) \equiv i - j_1 \pmod p \equiv j_1 \pmod p$, stoga $i \equiv 2j_1 \pmod p$. Ako $i = j_2$ onda $g(i, j_2) \equiv i \pmod p \equiv p \pmod p$. Tada $p \equiv 2j_1 \pmod p$, dakle $2j_1 \equiv 0 \pmod p$. To znači $j_1 \equiv 0 \pmod p$ ili $j_1 = p$. Tada je $i \equiv 2p \pmod p \equiv 0 \pmod p$ iz čega slijedi da je $i = p$. Dakle tada bi imali $i = j_1$, što nije moguće.
Dakle $i \neq j_2$. Iz toga slijedi $g(i, j_2) \equiv i - j_2 \pmod p \equiv j_2 \pmod p$. To povlači $i \equiv 2j_2 \pmod p$ i imamo

$$\begin{aligned} 2j_1 &\equiv 2j_2 \pmod p \\ j_1 &\equiv j_2 \pmod p. \end{aligned}$$

Zbog toga je $j_1 = j_2$, jer su oni najmanji ostaci modulo p.
U oba slučaja $j_1 = j_2$, što znači da je točno jedan tim slobodan u svakom kolu. □

Tim koji će biti slobodan u određenom kolu identificira se pomoću sljedećeg teorema.

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

Dokaz. Pretpostavimo $g(i,j) \equiv j \pmod{p}$.
Ako je $i = j$, tada je $g(i,j) \equiv p \pmod{p}$ i iz toga slijedi $i \equiv j \equiv p \equiv 0 \pmod{p}$. Stoga, $j \equiv (p+1)i/2 \pmod{p}$.
Ako $i \neq j$, tada $g(i,j) \equiv i - j \pmod{p}$. Zatim

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

Što znači

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

Dakle, $(p+1)i/2 \equiv (p+1)2j/2 \equiv pj + j \equiv j \pmod{p}$.
Prema tome, u oba slučaja, tim j je slobodan u kolu i ako je $j \equiv (p+1)i/2 \pmod{p}$.
Sada pretpostavimo da je $j \equiv (p+1)i/2 \pmod{p}$. Tada imamo

$$\begin{aligned} g(i,j) &\equiv i - j \pmod{p} \\ &\equiv i - \left(\frac{p+1}{2}\right)i \pmod{p} \equiv \left(\frac{1-p}{2}\right)i \pmod{p} \\ &\equiv \left(\frac{p+1}{2}\right)i \pmod{p} \equiv j \pmod{p}. \end{aligned}$$

Dakle tim j će biti slobodan u kolu i.

□

Sljedeći teorem pokazuje da g raspoređuje svaki tim točno jednom u svakom kolu.

Teorem 6.3. *Funkcija g je injekcija.*

Dokaz. Pretpostavimo $g(i,j_1) = g(i,j_2)$. Onda je $i - j_1 \equiv i - j_2 \pmod{p}$, i vrijedi $j_1 \equiv j_2 \pmod{p}$. Dakle, $j_1 \equiv j_2 \pmod{p}$ te slijedi da je g injekcija. □

Iz teorema 6.1, 6.2 i 6.3 slijedi da funkcija g na jedinstven način određuje protivnike tima j u svakom kolu i, gdje $1 \leq i,\ j \geq p$. U kolu i, tim j je slobodan ako $j \equiv \left(\frac{p+1}{2}\right)i \pmod{p}$. Zanimljivo je da je to upravo ista vrijednost od (1) iz prošlog poglavlja na koju se postavlja i-ta kraljica, gdje je $1 \leq i \leq p$. Dakle, tim koji je slobodan u i-tom kolu u round-robin rasporedu bi se nalazio na istom polju na kojem se pojavljuje kraljica Q u redu i na $p \times p$ šahovskoj ploči.
Možemo upotrijebiti funkciju g kako bi modificirali algoritam p-kraljica za dobivanje algoritma za raspored turnira s p timova, $p \geq 3$.

Algoritam za izradu rasporeda igranja po skupinama za p timova

- Staviti prvi slobodan tim u stupac $(p+1)/2$, sljedeći red sa slobodnim timom se popunjava u smjeru kazaljke na satu pomakom za $(p+1)/2$ gdje se postavlja slobodan tim u polje prema dobivenom rezultatu. Nastaviti tako dok slobodan tim nije u svakom redu.

- Počevši s prvim poljem u redu odbrojavaju se brojevi i upisuju u praznu ćeliju kako bi se održala permutacija $p, p-1, \ldots, \ldots 2, 1$ (preskočiti polje u kojoj je slobodan tim). Kako bi se popunili svi redovi kružno permutirajte brojeve na desno u sljedeći red.

Ako broj timova n, nije prost broj, timovi se uparuju u k kola, na sljedeći način[3]: tim $i(\neq n)$ igra protiv tima $j(\neq n)$ ako je $i+j \equiv k \pmod{n-1}$, gdje je $i \neq j$. Tako se raspoređuju svi timovi osim n i i, gdje je $2i \equiv k \pmod{n-1}$. Linearna kongurencija $2i \equiv k \pmod{n-1}$, po korolaru 1.1 ima jedinstveno rješenje kada je $(2, n-1) = 1$, dakle tim i i tim n igraju u kolu k. Ista se procedura primjenjuje sa svim ostalim timovima u svim kolima. Promotrimo na primjeru tima i, gdje je $1 \leq i < n$. S obzirom da je i jedinstveno rješenje kongurencija $2i \equiv k \pmod{n-1}$, timovi i i n igraju zajedno, slijedi da tim n igra $n-1$ različitih utakmica. Ako pretpostavimo da tim i i tim j igraju zajedno dva različita kola k i k' tada je $i+j \equiv k \pmod{n-1}$ i $i+j \equiv k' \pmod{n-1}$, što znači da je $k \equiv k' \pmod{n-1}$, odnosno timovi i i j se ne susreću u dva različita kola. Dakle svaki od prvih $n-1$ timova igra točno $n-1$ utakmica, a dva tima ne igraju dva puta zajedno, tj. svaki tim igra točno $n-1$ utakmica. Tim n također igra $n-1$ utakmica.

Primjer 6.1. *Napravite raspored po skupinama za šest timova.*

Rješenje.
Imamo šest timova, koje označimo s 1, 2, 3, 4, 5 i 6. Imamo paran broj timova tako da svaki tim može igrati u svakom kolu.

Jedinstveno rješenje kongruencije $2i \equiv 1 \pmod{5}$ je 3, $(2,5) = 1$. Iz toga slijedi da tim 3 igra s timom 6 u prvom kolu.

Tim 1 igra s timom j ako $i+j \equiv k \pmod{n-1} \equiv 1+j \equiv 1 \pmod{5}$, odnosno tim 1 igra s timom 5.
Tim 2 igra timom $2+j \equiv 1 \pmod{5}$, odnosno tim 2 igra s timom 4.
U drugom kolu kongruencija ima jedinstveno rješenje za $i = 1$, $(2,5) = 1$. Tim 1 u drugom kolu igra s timom 6.
Tim 2 igra s timom $2+j \equiv 2 \pmod{5}$, odnosno igra s timom 5.
Tim 3 igra s timom $3+j \equiv 2 \pmod{5}$, tj. igra a timom 4.

U trećem kolu rješenje kongruencije $2i \equiv 3 \pmod{5}$ je 4, $(2,5) = 1$, tim 4 igra s timom 6.

[3]metoda koju je razvio J.E. Freund, 1956.

Tim 1 igra s timom $1 + j \equiv 3 \pmod 5$, odnosno igra s timom 2.
Tim 3 igra s timom $3 + j \equiv 3 \pmod 5$, tj. igra s timom 5.

U četvrtom kolu jedinstveno rješenje od $2i \equiv 4 \pmod 5$ je 2, $(2, 5) = 1$, tim 2 igra s timom 6.
Tim 1 igra s timom $1 + j \equiv 4 \pmod 5$, tj. igra s timom 3.
Tim 4 igra s timom $4 + j \equiv 4 \pmod 5$, tj. igra s timom 5.

U zadnjem petom kolu jedinstveno rješenje kongruencije $2i \equiv 5 \pmod 5$ je 5, dakle tim 5 igra s timom 6.
Tim 1 igra s timom $1 + j \equiv 5 \pmod 5$, tj. igra s timom 4.
Tim 2 igra s timom $2 + j \equiv 5 \pmod 5$, tj. igra s timom 3.

Tablica 4: Raspored 6 timova po skupinama

Kolo i \ Tim j	1	2	3	4	5	6
1	5	4	6	2	1	3
2	6	5	4	3	2	1
3	2	1	5	6	3	4
4	3	6	1	5	4	2
5	4	3	2	1	6	5

7 Perpetual kalendar

Ideja ovog poglavlja je odrediti dan u tjednu za bilo koji datum u bilo kojoj godini. Svakih sedam dana dolazi isti dan, pa da bi se mogla provesti ideja primjenjuje se modul 7. Prvo slijedi povijest razvoja kalendara.
Prema legendi, oko 738. godine pr. Kr. osnivač Rima Romul je predstavio kalendar koji se sastojao od 304 dana i 10 mjeseci i nije obuhvaćao 61 zimskih dana. Taj kalendar nije bio dugo u upotrebi jer se nije slagao s godišnjim dobima, pa je nasljednik Romula Numa Pompilias oko 700 pr. Kr. reformirao kalendar dodavanjem dva mjeseca i produžio godinu na 355 dana. No međutim niti taj kalendar nije pratio godišnja doba, odnosano postojala su odstupanja. Bio je u upotrebi do 46. pr. Kr. kada je car Julije Cezar predstavio novi Julijanski kalendar. Napravljen je na aproksimaciji da Zemlji treba 365 dana i 6 sati da se okrene oko Sunca. Prosjećno bi godina trebala imati 365.25 dana pa se svake 4 godine uvela prijestupna godina s 366, koji se dodavao na veljaču koja je tada bila zadnji mjesec u godini. No međutim Zemlji treba 365 dana 5 sati, 48 minuta i 46 sekundi da se okrene oko Sunca, pa se pojavio višak od 11 minuta i 14 sekundi u kalendaru svake godine. Kroz 128 godina tih 11 minuta čine jedan dan. Do 16. stoljeća Julijanski kalendar je imao 10 dana viška. Astronomi Christopher Clavius i Aloysius Giglio su na zahtjev pape Grgura XIII. u listopadu 1582. godine predstavili novi kalendar koji je trebao ispraviti greške staroga. Greška od 10 dana je ispravljena izbacivanjem 10 dana u listopadu 1582. (5.10. postao je 15.10.). Stoljetne godine su prijestupne ako su djeljive s 400, a obične godine su prijestupne ako su djeljive s 4 (1900. godina nije bila prijestupna, a 2000. godina je prijestupna). Gregorijanski kalendar je sad općeprihvaćen u svijetu, ali se još uvijek razlikuje od sunčeve godine, trajanje Gregorijanske godine je 365.2425 dana, a stvarna sunčeva godina (okret Zemlje oko Sunca) traje 365.2421897 dana. To znači grešku od 3 dana svakih 10000 godina.
Cilj je odrediti dan u tjednu d, za bilo koji dan, mjesec i godinu prema Gregorijanskom kalendaru. Prva stoljetna prijestupna godina je bila 1600., 18 godina poslije predstavljanja Gregorijanskog kalendara. Treba razviti formulu koja obuhvaća godine poslije 1600. Kako je prijestupana godina dodana u veljači, nova godina će se u formuli računati od 1. ožujka (siječanj će se računati kao jedanaesti mjesec u godini, a veljača kao dvanaesti).
Brojevima od 1 do 12 označit će se mjeseci u godini od ožujka do veljače, $1 \leq m \leq 12$. Brojevima od 0 do 6 ćemo označiti dane u tjednu od subote do nedjelje $0 \leq d \leq 6$, s r dan u mjesecu $1 \leq r \leq 31$.
Neka d_y označava dan u tjednu od 1. ožujka (prvi dan godine) u godini y, $y \geq 1600$.

Ako imamo 365 dana u godini, $365 \equiv 1 \pmod 7$, d_y se razlikuje od d_{y-1} za jedan ako nije prijestupna ili za dva ako je prijestupna godina odnosno:

$$d_y = \begin{cases} d_{y-1} + 1, \text{ ako } y \text{ nije prijestupna} \\ d_{y-1} + 2, \text{ inače} \end{cases}$$

Za izračunavanje d_y od d_{1600} treba znati broj prijestupnih godina l poslije 1600.

Neka je y dana godina. Broj prijestupnih godina l između 1600. *i dane godine y (uključujući y) dan je formulom:*

$$l = \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388.$$

(Neka su a i b pozitivni cijeli brojevi. Tada je broj pozitivnih cijelih brojeva koji su $\leq a$ i djeljivi s b jednak $\lfloor a/b \rfloor$.)

Dokaz. Neka je n godina za koju vrijedi $1600 < n \leq y$. Dokaz se sastoji od nekoliko koraka:

- Treba naći broj godina n koje su djeljive s 4.
  Neka je $4n_1$ takva godina, onda $1600 < 4n_1 \leq y$, odnosno $400 < n_1 \leq y/4$. Znači da postoji $n_1 = \lfloor y/4 \rfloor - 400$ takvih godina.

- Treba pronaći broj od godina stoljeća koje su djeljive s 100.
  Neka je $100n_2$ takva godina, onda $1600 < 100n_2 \leq y$, odnosno $16 < n_2 \leq y/100$. Znači da postoji $n_2 = \lfloor y/100 \rfloor - 16$ takvih godina.

- Treba pronaći broj od godina stoljeća koje su djeljive s 400.
  Neka je $400n_3$ takva godina, onda $1600 < 400n_3 \leq y$, odnosno $4 < n_3 \leq y/400$. Znači da postoji $n_3 = \lfloor y/400 \rfloor - 4$ takvih godina.

- Dakle:

$$\begin{aligned} l &= n_1 - n_2 + n_3 \\ l &= \lfloor y/4 \rfloor - 400 - \lfloor y/100 \rfloor + 16 + \lfloor y/400 \rfloor - 4 \\ l &= \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388. \end{aligned}$$

□

Iz teorema o djeljenju s ostatkom je

$$y = 100C + D,$$

gdje je C broj stoljeća, a $0 \leq D < 100$ ostatak i vrijedi:

$$C = \lfloor y/100 \rfloor \quad \text{i} \quad D \equiv y \pmod{100}.$$

Tada slijedi

$$\begin{aligned} l &= \lfloor (100C + D)/4 \rfloor - \lfloor (100C + D)/100 \rfloor + \lfloor (100C + D)/400 \rfloor - 388 \\ &= \lfloor 25C + D/4 \rfloor - \lfloor C + D/100 \rfloor + \lfloor C/4 + D/400 \rfloor - 388 \\ &= 25C + \lfloor D/4 \rfloor - C + \lfloor C/4 \rfloor - 388, \quad \text{zbog toga što je } D < 100 \\ &= 24C + \lfloor D/4 \rfloor + \lfloor C/4 \rfloor - 388 \\ &\equiv 3C + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor - 3 \pmod{7}. \end{aligned}$$

Zbog toga je

$$\begin{aligned} d_y &\equiv d_{1600} + (1 \text{ dan za svaku godinu poslije 1600.}) \\ &\quad + (1 \text{ dan za svaku prijestupnu godinu poslije 1600.}) \pmod 7 \\ &\equiv d_{1600} + (y - 1600) + l \pmod 7. \end{aligned}$$

Uvrštavanjem $y = 100C + D$ i $l \equiv 3C + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor - 3 \pmod 7$ dobiva se

$$\begin{aligned} d_y &\equiv d_{1600} + (100C + D - 1600) + (3C + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor - 3) \pmod 7 \\ &\equiv d_{1600} + (2C + D - 4 + 3C - 3) + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor \pmod 7 \\ &\equiv d_{1600} + 5C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor \pmod 7 \\ &\equiv d_{1600} - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor \pmod 7. \end{aligned}$$

Da bi se odredio d_y, odnosno, dan 1. ožujka u godini y treba znati i koji je dan bio 1. ožujak 1600., odnosno treba znati d_{1600}. Da bi to izračunali iskoristit ćemo također tu formulu za određivanje d_{1600}.
Treba znati jedan poznati dan za 1. ožujka neke godine, ove godine je 1. ožujka 2016. bio utorak, odnosno $d_y = 2$. Za $y = 2016$, $C = \lfloor 2016/100 \rfloor = 20$ i $D = 16$ i $d_y = 2$ je:

$$\begin{aligned} d_{1600} &\equiv 2 + 2 \cdot 20 - 16 - \lfloor 20/4 \rfloor - \lfloor 16/4 \rfloor \pmod 7 \\ &\equiv 2 + 40 - 16 - 5 - 4 \pmod 7 \\ &\equiv 17 \pmod 7 \equiv 3 \pmod 7. \end{aligned}$$

1. ožujak 1600. godine je bio srijeda. Sada vraćanjem d_{1600} u formulu za d_y dobije se

$$d_y \equiv 3 - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor. \tag{4}$$

Sada se može odrediti dan za 1. ožujka bilo koje godine. Ova formula se treba proširiti kako bi mogli odrediti dan za bilo koji dan i bilo koji mjesec. Kako bi se to ostvarilo treba znati za koliko se dana prvi u mjesecu pomiče u odnosu na prethodni mjesec modulo 7. Prvi u mjesecu u odnosu na prvi u mjesecu prethodnog mjeseca se pomiče za dva dana ako je prethodni mjesec imao 30 dana, odnosno ako je prethodni mjesec imao 31 dan onda se pomiče 3 dana unaprijed ($30 \equiv 2 \pmod 7$ i $31 \equiv 3 \pmod 7$). Točnije:

1. travanj u odnosu na 1. ožujak:	3 dana
1. svibanj u odnosu na 1. travanj:	2 dana
1. lipanj u odnosu na 1. svibanj:	3 dana
1. srpanj u odnosu na 1. lipanj:	2 dana
1. kolovoz u odnosu na 1. srpanj:	3 dana
1. rujan u odnosu na 1. kolovoz:	3 dana
1. listopad u odnosu na 1. rujan:	2 dana
1. studeni u odnosu na 1. listopad:	3 dana
1. prosinac u odnosu na 1. studeni:	2 dana
1. siječanj u odnosu na 1. prosinac:	3 dana
1. veljače u odnosu na 1. siječanj:	3 dana

Ako se zbroje ti dani dobije se 29. Dakle prosjećno povećanje broja dana prvog u mjesecu u odnosu na prethodni prvi je $29/11 \approx 2.6$, to je promatrao Christian Zeller i uočio da se funkcija $f(m) = \lfloor 2.6m - 0.2 \rfloor - 2$ može upotrijebiti za mjesece m od 2 do 12. Ako pogledamo,

$$\begin{aligned} f(5) - f(4) &= (\lfloor 2.6 \cdot 5 \rfloor - 0.2) - 2) - (\lfloor 2.6 \cdot 4 - 0.2 \rfloor - 2) \\ &= (\lfloor 13 - 0.2 \rfloor) - (\lfloor 10.4 - 0.2 \rfloor) - 2 = 12 - 10 = 2. \end{aligned}$$

To je povećanje od 3 dana od 1. ožujka mjeseca 4 (lipnja) do 1. ožujka mjeseca 5 (srpnja). Pomoću (4) sada se može izračunati prvi u mjesecu za bilo koji mjesec i on je dan s:

$$\begin{aligned} d' &\equiv d_y + \lfloor 2.6m - 0.2 \rfloor - 2 \pmod 7 \\ &\equiv 3 - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor + \lfloor 2.6m - 0.2 \rfloor - 2 \pmod 7 \\ &\equiv 1 + \lfloor 2.6m - 0.2 \rfloor 3 - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor \pmod 7. \end{aligned}$$

Još treba samo pronaći formulu za r-ti dan mjeseca m i ona glasi:

$$d \equiv d' + (r-1) \pmod 7 \equiv r + \lfloor 2.6m - 0.2 \rfloor - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor \pmod 7. \quad (5)$$

I na taj način smo dobili formulu koja omogućava određivanje dana u tjednu za bilo koji datum prema Gregorijanskom kalendaru.

Primjer 7.1. *Odredite koji će dan u tjednu biti na* 12. *siječanj* 2125.

Rješenje.

Budući da je prvi dan u godini 1. ožujak, zadnji je 28. ili 29. veljače, stoga je siječanj 2125. zapravo jedanaesti mjesec 2124. Znači $y = 2124$, $C = 21$, $D = 24$, $m = 11$ i $r = 12$, kada se to ubaci u formulu (5) dobiva se

$$\begin{aligned} d &\equiv 12 + \lfloor 2.6 \cdot 11 - 0.2 \rfloor - 2 \cdot 21 + 24 + \lfloor 21/4 \rfloor + \lfloor 24/4 \rfloor \pmod 7 \\ &\equiv 12 + 28 - 42 + 24 + 5 + 6 \pmod 7 \\ &\equiv 5 \pmod 7. \end{aligned}$$

Znači 12. siječanj 2125. će biti u petak.

8 Zaključak

Jedna od najstarijih grana matematike je teorija brojeva, a dio teorije brojeva je teorija kongruencija.

Kongruencija kao jednostavna ideja pronalazi široku primjenu te ponekad nismo ni svjesni njene primjene u svakodnevnom životu. Gledajući na sat ili sjetivši se dana u tjednu primjenjujemo kongruenciju. Također i prije nego smo znali njenu definiciju koristili smo ju i u osnovnoj školi pri određivanju kada je neki broj djeljiv s nekim drugim brojem.

Razvojem tehnologije i sve većim brojem proizvoda i usluga trebalo se pronaći jednostavan i lak način da se oni prate te su se počeli označavati brojevima. Identifikacijski brojevi sadrže kodirane informacije proizvoda, ljudi, dokumenata i ostalih stvari. Budući da su kodirani bitno je da se greške pri njihovom slanju, skreniranju ili unosu u računalo otkriju. Naravno da nam ne bi bilo svejedno da se recimo bar-kod EAN-13 skenira pogrešno i da se naplati veća cijena proizvoda nego što ona je. Olakšana je i ubrzana isporuka pošte u Sjedinjenim Američkim državama. Metoda znamenke provjere ima i nedostataka, jer se ponekad greške ne mogu otkriti, no u većini slučajeva se greške otkriju.

U umjetnosti kongruencija se može primijeniti za dizajniranje predivnih modularnih dizajna, na sportskim terenima za određivanje utakmica po skupinama, te za određivanje dana u tjednu za bilo koji datum bilo koje godine. To su samo neki primjeri primjene kongruencija koji su prikazani u radu, jer se kongruencija može primijeniti i u glazbi, kemiji, kriptografiji itd.

Literatura

[1] Andrew Adler, John E. Coury, The Theory of Numbers (A Text And Source Book of Problems), Jones And Barlett Publication, 1995.

[2] Santo D'Agostino, Fundamentals of Mathematics, The Online Mathematics Textbook, 2013.

[3] Tom Cooper, Tony Watson, Mathematics and Modulo Art, Queensland University of Technology, Electrion edition, 2013.

[4] Joseph A. Gallian, The Mathematics of Identification Numbers, The College Mathematics Journal, Vol. 22, No. 3. (May, 1991), pp. 194-202

[5] Joseph Kirtland, Identification Numbers and Check Digit Schemes 1st edition, The Mathematical Association of America, 2001.

[6] Thomas Koshy, Elementary Number Theory with Applications 2ed edition, Academic Press, 2007.

[7] I. Matić, Uvod u teoriju brojeva, skripta, Odjel za matematiku, Sveučilište J.J. Strossmayera, Osijek, 2013.

[8] http://web.efzg.hr/dok/TRG/tbakovic/2.

9 Sažetak i ključne riječi

U diplomskom radu pokazat ćemo kako se kongruencija može primjeniti na različite načine. Prvo ćemo definirati kongruenciju i navesti njezina svojstva koja ćemo koristiti u radu. Zatim ćemo prikazati neke od njezinih primjena. Prvo neke od jednostavnjih poput testa djeljivosti za brojeve 10, 5, 2^i, 3 , 9 i 11 koje se dokazuju primjenom kongruencija, zatim metoda odbacivanja devetki i digitalni korijen. Nakon toga ćemo vidjeti kako se kongruencija koristi za modeliranje dizajna, preko zvijezde s m vrhova, (m, n) dizajna ostataka do quilt dizajna. Zatim slijede primjene koje omugućavaju otkrivanje grešaka u identifikacijskim brojevima (UPC, EAN-13, ISBN,...).
I na kraju ćemo prikazati kako se primjenom kongruencija može rješiti problem p-kraljica, raspored timova po skupinama (round-robin turnir) te određivanje dana u tjednu za bilo koji datum i bilo koju godinu (Perpetual kalendar).

Ključne riječi: kongruencija, primjena kongruencija, testovi djeljivosti, odbacivanje devetke, digitalni korijen, modularni dizajni, znamenka provjere, problem p-kraljica, round-robin turnir, Perpetual kalendar

10 Title, summary and keywords

Title: Congruence Applications

Summary

In this work we will show how congruence has applications on many different ways.
First we will define congruence and show it properties that we will use in work. Then we will show some simple applications like divisibility test for numbers 10, 5, 2^i, 3 , 9 and 11, prove them with congruence. Then we will show method casting out nines and digital roots. After that we will see how congruence is applied on design modular designs, from m-pointed star, (m, n) residue design to quilt design.
In third part we will show how congruence is used to detect mistakes in identification numbers (UPC, EAN-13, ISBN,...)
In the final three parts we will show how congruence applications can help to solve the p-Queens Puzzle, Round-Robin tournaments and to determinate the day of the week for any date and any year.

Keywords: Congruence, Congruence Applications, divisibility test, casting out nines, digital roots, modular designs, check digit, p-Queens Puzzle, Round-Robin tournament, Perpetual calendar

11 Životopis

Rođena sam 6. lipnja 1988. u Osijeku. Osnovnu školu sam završila u Petrijevcima, te sam upisala Ekonomsku i Upravnu školu u Osijeku. Nakon završene srednje škole upisujem studij matematike na Odjelu za matematiku u Osijeku, a nakon završenog preddiplomskom studija upisujem Diplomski studij, smjer Financijska matematika i statistika na Sveučilištu J.J. Strossmayera u Osijeku.