Kongruencije i neke njihove primjene

Radaković, Maja

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Radaković

Kongruencije i neke njihove primjene

Završni rad

Osijek, 2021.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Radaković

Kongruencije i neke njihove primjene

Završni rad

Mentor: izv. prof. dr. sc. Ivan Soldo

Osijek, 2021.

Sažetak

Ovim završnim radom obradit će se tema kongruencija i nekih njihovih primjena. Teorija kongruencija uvedena je u djelu njemačkog matematičara Carla Friedricha Gaussa pod nazivom Disquisitiones Arithmeticae. Uveo je oznaku za kongruencije koju koristimo i danas. U uvodu ćemo definirati kongruencije te navesti neke primjere i osnovna svojstva. U prvom poglavlju osvrnut ćemo se na linearne kongruencije te navesti neke njihove primjene. U drugom poglavlju iskazat ćemo i dokazati Kineski teorem o ostatcima te detaljnije opisati sustave kongruencija i njihove primjene. U trećem poglavlju bazirat ćemo se na Eulerovu funkciju i njena svojstva te iskazati i dokazati Euler-Fermatov teorem i upoznati se s reduciranim sustavom ostataka. Nadalje, u četvrtom poglavlju proučit ćemo kongruencije po prostom modulu te iskazati i dokazati Wilsonov i Lagrangeov teorem. Naposljetku, u petom poglavlju vidjet ćemo neke primjene kongruencija u kriptografiji, ispitivanju djeljivosti i u generiranju barkodova proizvoda.

Ključne riječi

Kongruencije, linearne kongruencije, Kineski teorem o ostatcima, sustavi kongruencija, Eulerova funkcija, Eulerov teorem, Fermatov teorem, reducirani sustav ostataka, kongrunecije po prostom modulu, Wilsonov teorem, Lagrangeov teorem, kriptografija, barkodovi

Congruences and some of their applications

Summary

In this final paper, we will analyze congruences and some of their applications. The theory of congruence was introduced by the German mathematician Carl Friedrich Gauss in his work Disquisitiones Arithmeticae. He introduced the congruence sign that we still use. In the introduction, we will define congruences and give some examples and basic properties. In the first chapter, we will consider linear congruences and some of their applications. In the second chapter, we will state and prove the Chinese theorem of residues and in more detail describe the systems of congruences and their applications. The theme of the next chapter will be Euler's function and its properties. We will also state and prove the Euler-Fermat theorem, and consider the reduced system of residues. Furthermore, in the fourth chapter, we will study congruences by a simple module, express and prove Wilson's and Lagrange's theorem. Finally, in chapter five, we will see some of applications of congrunces in cryptography, divisibility testing and in generating product barcodes.

Keywords

Congruences, linear congruences, Chinese residual theorem, congruence systems, Euler's function, Euler's theorem, Fermat's theorem, reduced system of residues, congruences by a simple module, Wilson's theorem, Lagrange's theorem, cryptography, barcodes

Sadržaj

Uvod

Za početak definirajmo što su to kongruencije:

Definicija 1. *Ukoliko je $n \in \mathbb{Z}$, $n > 0$ i ukoliko su $c, d \in \mathbb{Z}$, tada kažemo da je c kongruentan s d modulo n ako $n \mid (c-d)$. Pišemo $c \equiv d \pmod{n}$. Ukoliko vrijedi $n \nmid (c-d)$, onda kažemo da c nije kongruentan s d modulo n i pišemo $c \not\equiv d \pmod{n}$.*

Dakle, u Definiciji 1 možemo se usredotočiti samo na pozitivne module jer n dijeli $c-d$ onda i samo onda kada $-n$ dijeli $c-d$.

Sljedeći primjer ilustrira ovu definiciju.

Primjer 1. *Budući da $14 \mid (19-5)$, prema Definiciji 1 vrijedi da je $19 \equiv 5 \pmod{14}$, ali $18 \not\equiv 2 \pmod{9}$, jer 9 ne dijeli razliku $18-2$.*

U sljedećoj propoziciji možemo vidjeti neka od jednostavnijih svojstava kongruencija.

Propozicija 1 (vidi [3, Propozicija 3.1.])**.** *Relacija "biti kongruentan modulo n" relacija je ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz: (1) Kako $n \mid 0 = (c-c)$, slijedi $c \equiv c \pmod{n}$ (svojstvo refleksivnosti).

(2) Ukoliko je $c \equiv d \pmod{n}$, tada $\exists e$ iz skupa $\mathbb{Z}$ za kojeg vrijedi $c - d = n \cdot e$, iz čega imamo da je $d - c = n \cdot (-e)$, stoga je $d \equiv c \pmod{n}$ (svojstvo simetričnosti).

(3) Kako vrijedi $c \equiv d \pmod{n}$ i $d \equiv g \pmod{n}$, postoje cijeli brojevi e, f za koje je $c-d = n \cdot e$ i $d-g = n \cdot f$. Zbrajanjem prethodnih jednakosti imamo $c-g = n \cdot (e+f)$, iz čega slijedi $c \equiv g \pmod{n}$ (svojstvo tranzitivnosti).

□

Na sljedećem primjeru možemo vidjeti ova svojstva.

Primjer 2. *(1) Vrijedi $3 \equiv 3 \pmod{5}$.*

(2) Budući da vrijedi $7 \equiv 1 \pmod{2}$, tada vrijedi i $1 \equiv 7 \pmod{2}$.

(3) Budući da $30 \equiv 5 \pmod{5}$ i $5 \equiv -20 \pmod{5}$, imamo da je $30 \equiv -20 \pmod{5}$.

Kongruencije imaju mnoga svojstva zajednička s jednakostima, što pokazuje sljedeća propozicija.

Propozicija 2 (vidi [3, Propozicija 3.2.])**.** *Pretpostavimo da su $c, d, g, h \in \mathbb{Z}$. Tada vrijede sljedeća svojstva:*

(1) Ukoliko je $c \equiv d \pmod{n}$ te $g \equiv h \pmod{n}$, tada je $c+g \equiv d+h \pmod{n}$, $c-g \equiv d-h \pmod{n}$ i $c \cdot g \equiv d \cdot h \pmod{n}$.

(2) Ukoliko vrijedi $h \mid n$ i $c \equiv d \pmod{n}$, tada je $c \equiv d \pmod{h}$.

(3) Ukoliko je $c \equiv d \pmod{n}$, tada vrijedi $c \cdot g \equiv d \cdot g \pmod{ng}$, za sve $g \neq 0$.

Dokaz: (1) Pretpostavimo da je $c - g = n \cdot e$ te $g - h = n \cdot f$. Sada imamo da je $(c+g) - (d+h) = n \cdot (e+f)$ i $(c-g) - (d-h) = n \cdot (e-f)$, pa vrijedi $c+g \equiv d+h \pmod{n}$ i $c - g \equiv d - h \pmod{n}$. Iz $cg - dh = c \cdot (g-h) + h \cdot (c-d) = n \cdot (cf + he)$ znamo da je $cg \equiv dh \pmod{n}$.

(2) Pretpostavimo da je $n = z \cdot e$. Zbog $c - d = nf$ dobivamo $c - d = z \cdot (ef)$, pa vrijedi $c \equiv d \pmod{z}$.

(3) Jer vrijedi $c - d = n \cdot e$ slijedi $cg - dg = (ng) \cdot e$, pa vrijedi $cg \equiv dg \pmod{ng}$.

□

Dakle, kongruencije s istim modulom možemo zbrajati, oduzimati i množiti, ali za njihovo kraćenje potreban nam je sljedeći teorem.

Teorem 1 (vidi [3, Teorem 3.4.]). *Kongruencija* $cx \equiv dy \pmod{n}$ *ekvivalentna je kongruenciji* $x \equiv y \pmod{\frac{n}{nzd(c,n)}}$. *Posebno, ukoliko je* $cx \equiv dy \pmod{n}$ *te* $(c, n) = 1$, *tada vrijedi* $x \equiv y \pmod{n}$.

Dokaz:
Ukoliko označimo $nzd(c, n) = g$, onda imamo $nl = c(x - y) \Leftrightarrow \frac{n}{g} l = \frac{c}{g}(x - y)$. Kako je $nzd(\frac{n}{g}, \frac{c}{g}) = 1$, po definiciji najvećeg zajedničkog djelitelja zaključujemo da $\frac{n}{g}$ dijeli $x - y$, odnosno da vrijedi
$x \equiv y \pmod{\frac{n}{g}}$. □

Na sljedećem primjeru možemo vidjeti primjenu prethodnog teorema.

Primjer 3. *Kako za kongruenciju* $120 \equiv 45 \pmod{15}$ *vrijedi* $15 \cdot 8 \equiv 15 \cdot 3 \pmod{15}$ *i* $nzd(15, 15) = 15$, *imamo* $8 \equiv 3 \pmod{1}$.

1 Linearne kongruencije

Kako bismo definirali linearne kongruencije, definirajmo najprije potpuni sustav ostataka modulo n.

Definicija 2. *Potpunim sustavom ostataka modulo n nazivamo skup $\{x_1, \ldots, x_n\}$ ukoliko $\forall y \in \mathbb{Z}$, $\exists! x_j$, za $j = 1, \ldots, n$, za kojeg vrijedi $y \equiv x_j \pmod{n}$. Dakle, ako iz svake klase ekvivalencije modulo n uzmemo po jedan član, onda ćemo dobiti potpuni sustav ostataka modulo n.*

Iz Definicije 2 očito je da postoji beskonačno mnogo potpunih sustava ostataka modulo n. Pogledajmo primjer potpunog sustava ostataka u nekom modulu.

Primjer 4. *Potrebno je odrediti potpun sustava ostataka modulo 4.*

Rješenje:
Sljedeći skupovi su potpuni sustavi ostataka modulo 4:

$$\begin{aligned} A_1 &= \{0, 1, 2, 3\}, \\ A_2 &= \{1, 2, 3, 4\}, \\ A_3 &= \{-4, -3, -2, -1\}. \end{aligned}$$

U nastavku ćemo navesti teorem Euler-Fermatov teorem.

Teorem 2 (Euler-Fermatov teorem, vidi [4, Teorem 1])**.** *Pretpostavimo da je $n \in \mathbb{Z}$, $n > 0$ i da je A neprazan skup brojeva iz skupa $\mathbb{Z}$. A je potpun sustav ostataka modulo n ako i samo ako vrijedi:*

(1) A sadrži n elemenata;

(2) elementi od A nisu međusobno kongruentni modulo n.

Detalji o dokazu teorema nalaze se u [4].
U sljedećem primjeru vidjet ćemo kako pomoću Euler-Fermatova teorema možemo odrediti je li neki skup potpun sustav ostataka po nekom modulu.

Primjer 5. *Potrebno je provjeriti je li skup $A = \{-4, 0, 1, 2\}$ potpun sustav ostataka modulo 4.*

Rješenje:
Kako bismo provjerili je li skup A potpun sustav ostataka modulo 4, treba vidjeti jesu li svi elementi tog skupa u različitim klasama, a budući da A ima 4 elementa sve klase moraju biti predstavljene među elementima od A. Kako vrijedi $-4 \equiv 0 \pmod{4}$ imamo da su -4 i 0 predstavnici iste klase pa nije zadovoljen uvjet da niti jedan element skupa A nije međusobno kongruentan modulo 4. Time dobivamo da A nije potpun sustav ostataka modulo 4.
U sljedećem teoremu vidjet ćemo jedno od svojstava potpunog sustava ostataka modulo n.

Teorem 3 (vidi [3, Teorem 3.5.]). *Pretpostavimo da je $\{x_1, \ldots, x_n\}$ potpuni sustav ostataka modulo n te da vrijedi $nzd(c, n) = 1$. Tada je $\{cx_1, \ldots, cx_n\}$ također potpuni sustav ostataka modulo n.*

Dokaz:
Pretpostavimo da je $A = \{cx_1, \ldots, cx_n\}$, $(c, n) = 1$. A ima n elemenata. Potrebno je pokazati da su svaka dva elementa međusobno nekongruentna modulo n, odnosno $cx_1 \not\equiv cx_j \pmod{n}$, za $i \neq j$. Sada pretpotavimo da je $cx_i \equiv cx_j \pmod{n}$. Teorem 3 nam daje da da je $x_i \equiv x_j \pmod{n}$, odnosno da je $i = j$, iz čega slijedi da su različiti elementi skupa A u različitim klasama modulo n. □

U sljedećem primjeru ilustrirat ćemo prethodni teorem.

Primjer 6. *Skup $A = \{1, 2, 3, 4, 5\}$ je potpun sustav ostataka modulo 5 te vrijedi $(7, 5) = 1$. Iz prethodnog teorema znamo da je i skup $\{7 \cdot 1, 7 \cdot 2, 7 \cdot 3, 7 \cdot 4, 7 \cdot 5\}$, odnosno $\{7, 14, 21, 28, 35\}$ također potpun sustav ostataka modulo 5.*

Sada ćemo se upoznati s linearnim kongruencijama. Kongruencija oblika $cx \equiv d \pmod{n}$ naziva se linearna kongruencija. U nastavku ćemo komentirati rješivost ovakvih kongruencija. To nas dovodi do teorema o linearnim kongruencijama:

Teorem 4 (vidi [3, Teorem 3.6.]). *Pretpostavimo da su $c, n \in \mathbb{N}$, te $d \in \mathbb{Z}$. Kongruencija $cx \equiv d \pmod{n}$ ima rješenja ako i samo ako $g = nzd(c, n)$ dijeli d. Ukoliko je ispunjen ovaj uvjet, onda postoji točno g rješenja prethodne kongruencije modulo n.*

Dokaz:
Ukoliko kongruencija $cx \equiv d \pmod{n}$ ima rješenja, tada $\exists y \in \mathbb{Z}$ za koji vrijedi $cx - ny = d$. Iz ovoga imamo da $nzd(c, n)$ dijeli d.
Ako sada pretpostavimo da $g = (c, n)$ dijeli d. Označimo $c' = \frac{c}{g}$, $d' = \frac{d}{g}$ i $n' = \frac{n}{g}$. Sada imamo kongruenciju $c'x \equiv d' \pmod{n'}$. Dana kongruencija ima točno jedno rješenje modulo n'. Kako je $(c', n') = 1$, svaki od ostataka modulo n' (pa tako i d') dobiva se za točno jedan x iz potpunog sustava ostataka modulo n'. Ukoliko je x' neko rješenje od $c'x' \equiv d' \pmod{n'}$, tada su sva rješenja od $cx \equiv d \pmod{n}$ iz skupa cijelih brojeva dana s $x = x' + mn'$, za $m \in \mathbb{Z}$, a sva rješenja koja su međusobno neekvivalentna dana su s $x = x' + mn'$, gdje je $m = 0, 1, \ldots, g - 1$. Dakle, kongruencija $cx \equiv d \pmod{n}$ ima točno g rješenja modulo n.
□

Iz Teorema 4 vidimo da ukoliko c nije djeljiv nekim prostim brojem p, tada kongruencija $cx \equiv d \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno. Opće rješenje linearne kongruencije pišemo u obliku $x = x_0 + (\frac{n}{g})t$, gdje je $0 \leq t < g$.

Sljedeći primjeri ilustriraju prethodni teorem.

Primjer 7. *Potrebno je odrediti imaju li sljedeće kongruencije rješenja:*

(1) $16x \equiv 27 \pmod{29}$,

(2) $9x \equiv 12 \pmod{15}$,

(3) $5x \equiv 7 \pmod{10}$.

Rješenje:

(1) Kako $(16, 29) = 1 \mid 27$, postoji jedinstveno rješenje kongruencije $16x \equiv 27 \pmod{29}$.

(2) Kako $(9, 15) = 3 \mid 12$, postoji 3 rješenja kongruencije $9x \equiv 12 \pmod{15}$.

(3) Kako $(5, 10) = 2$, ali $2 \nmid 7$, kongruencija nema rješenja.

Na sljedećem primjeru možemo vidjeti kako se rješava linearna kongruencija.

Primjer 8. *Potrebno je riješiti kongruenciju* $42x \equiv 21 \pmod{93}$

Rješenje:
Budući da $(42, 93) = 3$ i $3 \mid 21$ dana kongruencija ima 3 međusobno neekvivalentna rješenja. Sada imamo kongruenciju oblika $14x \equiv 7 \pmod{31}$ za koju vrijedi $(14, 31) = 1$, iz čega slijedi da $\exists u, v \in \mathbb{Z}$, za koje vrijedi $14u + 31v = 1$ i koji se mogu naći pomoću Euklidova algoritma. Dobivamo kongruenciju oblika $14u \equiv 1 \pmod{31}$. Primjenimo Euklidov algoritam:

$$\begin{aligned} 14 &= 0 \cdot 31 + 14 \\ 31 &= 2 \cdot 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 1 \cdot 2, \end{aligned}$$

i	-1	0	1	2	3	4
q_i			0	2	4	1
u_i	1	0	1	-2	9	-11
v_i	0	1	0	1	-4	5

.

Sada imamo $u \equiv -11 \pmod{31}$, odnosno $u \equiv 20 \pmod{31}$. Kako je $u = 20$, imamo $x_1 \equiv 20 \cdot 7 \pmod{31}$, odnosno $x_1 \equiv 140 \pmod{31}$ te nadalje $x_1 \equiv 16 \pmod{31}$. Rješenja kongruencije su $x \equiv 16, 16 + 31, 16 + 2 \cdot 31 \pmod{93}$, odnosno $x \equiv 16, 47, 78 \pmod{93}$.

2 Sustavi kongruencija

U ovom poglavlju proučavat ćemo sustave kongruencija.
Navest ćemo, analizirati i primjerom potkrijepiti osnovni rezultat za analizu rješenja sustava kongruencija.

Teorem 5 (vidi [1, Teorem 5.4.]). *Pretpostavimo da su $n_1, n_2, \ldots, n_r$ u parovima relativno prosti brojevi iz skupa $\mathbb{N}$ i da su $c_1, c_2, \ldots, c_r \in \mathbb{Z}$. Tada postoji jedinstveno rješenje sustava kongruencija modulo n*

$$x \equiv c_1 \pmod{n_1}, x \equiv c_2 \pmod{n_2}, \ldots, x \equiv c_r \pmod{n_r}.$$

Dokaz:
Egzistencija:
Pretpostavimo da je $n = n_1 \cdot n_2 \cdots n_r$ i definiramo $m_j = \frac{n}{n_j}$, $j = 1, 2, \ldots, r$. Brojevi $n_1, \ldots, n_r$ su u parovima relativno prosti, odnosno $(n_i, n_j) = 1$ za $i \neq j$, iz čega slijedi da je i $(m_j, n_j) = 1$, za $j = 1, 2, \ldots, r$. Kako imamo da su dani brojevi u parovima relativno prosti, prema Teoremu 4 kongruencije oblika $m_j x_j \equiv c_j \pmod{n_j}$, za $j = 1, 2, \ldots, r$ uvijek imaju rješenje. Promatrajmo sada broj $x_0 = m_1 x_1 + m_2 x_2 + \cdots + m_r x_r$. Kako $n_j \mid m_i$ za $i \neq j$ slijedi $x_0 \equiv m_1 x_1 + m_2 x_2 + \cdots + m_r x_r \pmod{n_j} \equiv 0 \cdot x_1 + \cdots + m_j x_j + \cdots + 0 \cdot x_r \pmod{n_j} \equiv a_j \pmod{n_j}$ te je dani x_0 rješenje polaznog sustava kongruencija.
Jedinstvenost:
Pretpostavimo da su x_0 i x_1 rješenja polaznog sustava kongruencija. Tada $\forall j = 1, 2, \ldots, r$ imamo $x_0 \equiv c_j \pmod{n_j}$ i $x_1 \equiv c_j \pmod{n_j}$, iz čega slijedi da je $x_0 \equiv x_1 \pmod{n_j}$, za $j = 1, 2, \ldots, r$. Kako su $n_1, \ldots, n_r$ u parovima relativno prosti, slijedi da je $x_0 \equiv x_1 \pmod{n}$, čime je dokazana jedinstvenost rješenja. □

Dakle, dokaz prethodnog teorema je konstruktivan. Stoga ćemo u sljedećem primjeru vidjeti kako se rješava navedeni sustav kongruencija.

Primjer 9. *Potrebno je riješiti sljedeće sustave kongruencija:*

$$x \equiv 5 \pmod 7, \quad x \equiv 2 \pmod 3, \quad x \equiv 4 \pmod 5.$$

Rješenje:
Kako je $(3, 5) = (5, 7) = (3, 7) = 1$ smijemo primjeniti Teorem 5.

$$m = 3 \cdot 5 \cdot 7,$$

$$n_1 = \frac{3 \cdot 5 \cdot 7}{7} = 15, \quad n_2 = \frac{3 \cdot 5 \cdot 7}{3} = 35, \quad n_3 = \frac{3 \cdot 5 \cdot 7}{5} = 21.$$

Sada imamo linearne kongruenije:

$$15x_1 \equiv 5 \pmod 7 \Leftrightarrow x_1 \equiv 5 \pmod 7,$$

$$35x_2 \equiv 2 \pmod 3 \Leftrightarrow 2x_2 \equiv 2 \pmod 3 \Leftrightarrow x_2 \equiv 1 \pmod 3,$$

$$21x_3 \equiv 4 \pmod 5 \Leftrightarrow x_3 \equiv 4 \pmod 5.$$

Uzmimo $x_1 = 5, x_2 = 1, x_4 = 5$. Rješenja sustava su $x \equiv 5 \cdot 15 + 1 \cdot 35 + 4 \cdot 21 \pmod{105}$, odnosno $x \equiv 194 \pmod{105} \equiv 89 \pmod{105}$.

U slučaju kada u sustavu kongruencija $x \equiv c_i \pmod{ni}$, za $i = 1, 2, \ldots, r$ u kojem n_i nisu nužno relativno prosti, dani sustav ne mora imati rješenje. Za postojanje rješenja potrebno je osigurati uvjet $c_i \equiv c_j \pmod{nzd(n_i, n_j)}$, za sve $i \neq j$.

Ilustrirajmo sada na primjeru situaciju kada moduli nisu relativno prosti.

Primjer 10. *Riješimo sustav:*

$$x \equiv 5 \pmod 6, \quad x \equiv 7 \pmod{10}, \quad x \equiv 3 \pmod 7.$$

Rješenje:
Vidimo da dani moduli nisu u parovima relativno prosti pa ne vrijede pretpostavke Kineskog teorema o ostatcima. Zadani sustav ekvivalentan je sustavu kojemu su moduli potencije prostih brojeva, odnosno :

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

Ako sada usporedimo potencije istog brostog broja, dobivamo:

$$x \equiv 5 \pmod 2 \Leftrightarrow x \equiv 1 \pmod 2,$$

$$x \equiv 5 \pmod 3 \Leftrightarrow x \equiv 2 \pmod 3,$$

$$x \equiv 7 \pmod 5 \Leftrightarrow x \equiv 2 \pmod 5,$$

$$x \equiv 7 \pmod 2 \Leftrightarrow x \equiv 5 \pmod 2 \Leftrightarrow x \equiv 3 \pmod 2 \Leftrightarrow x \equiv 1 \pmod 2,$$

$$x \equiv 3 \pmod 7.$$

Dakle, početni sustav ekvivalentan je sustavu:

$$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7.$$

Dani sustav rješavamo primjenom Kineskog teorema o ostatcima kao u prethodnom primjeru.

3 Eulerova funkcija

U ovom poglavlju definirat ćemo Eulerovu funkciju, iskazati i dokazati Eulerov i Mali Fermatov teorem te vidjeti na primjerima neke njihove primjene. Kako bismo definirali Eulerovu funkciju, najprije ćemo definirati reducirani sustav ostataka po nekom modulu.

Definicija 3. *Pretpostavimo da su* $n, k \in \mathbb{N}$. *Skup* $A = \{c_1, \ldots, c_k\}$ *naziva se reducirani sustav ostataka modulo* n, *ukoliko* $\forall b \in \mathbb{Z}$ *takav da je* $(b, n) = 1$ $\exists! c_i \in A$ *sa svojstvom da je* $b \equiv c_i \pmod{n}$.

Potrebno je uočiti broj elemenata u reduciranom sustavu ostataka modulo n, koji se razlikuje u odnosu na potpun sustav ostataka modulo n. Kod reduciranog sustava ostataka modulo n nalazi se točno n elemenata zbog uvjeta $(b, n) = 1$ kojeg u potpunom sustavu ostataka modulo n nije bilo.

Primjer 11. *Reducirani sustav ostataka modulo 3 je skup* $A = \{1, 2\}$ *koji se dobije tako da iz potpunog sustava ostataka* $\{1, 2, 3\}$ *modulo 3 isključimo one elemente koji nisu relativno prosti s 3.*

U nastavku ćemo definirati važnu funkciju koja je usko povezana sa reduciranim sustavom ostataka modulo n.

Definicija 4. *Pretpostavimo da je* $n \in \mathbb{N}$ *i* $A_n = \{c \in \mathbb{N} : 1 \leq c \leq n \text{ i } (n, c) = 1\}$. *Eulerova funkcija je funkcija* $\varphi : \mathbb{N} \to \mathbb{N}$ *definirana formulom* $\varphi(n) = |A_n|$.

Iz definicije možemo uočiti kako se u skupu A_n nalaze svi elementi potpunog sustava ostataka $\{1, 2, \ldots, n\}$ i oni su relativno prosti s danim n. Dakle, A_n je reduciran sustav ostataka modulo n, čime dolazimo do zaključka da Eulerova funkcija broji koliko ima elemenata u tom sustavu.

Primjer 12. *Reduciran sustav ostataka modulo 8 je skup* $\{1, 3, 5, 7\}$ *koji se dobije tako da iz potpunog sustava ostataka* $\{0, 1, 2, 3, 4, 5, 6, 7\}$ *modulo 8 izbace elementi koji nisu relativno prosti s 8. Tada je* $\varphi(8) = 4$.

Važno svojstvo Eulerove funkcije možemo vidjeti u sljedećem korolaru.

Korolar 1 (vidi [4, Teorem 4.]). *Ukoliko je* $n = \prod_p p^{\alpha_p}$, *tada vrijedi*

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

Prethodni korolar možemo koristiti kako bismo odredili broj brojeva iz skupa $\mathbb{N}$ manjih od zadanog broja koji su relativno prosti s danim brojem. To možemo vidjeti u sljedećem primjeru.

Primjer 13. *Potrebno je odrediti broj brojeva iz skupa* $\mathbb{N}$ *manjih od 500 koji su relativno prosti s 500.*

Rješenje:

$$\varphi(500) = \varphi(2^2 \cdot 5^3) = 2 \cdot (2-1) \cdot 5^2 \cdot (5-1) = 200$$

U sljedećem teoremu, kojeg ćemo kasnije koristiti, navest ćemo svojstvo reduciranog sustava ostataka modulo n.

Teorem 6 (vidi [3, Teorem 3.8.]). *Pretpostavimo da je $\{r_1, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n te da vrijedi $(c, n) = 1$. Tada je $\{cr_1, \ldots, cr_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n.*

Dokaz:
Dokaz ovog teorema slijedi iz Teorema 4. □

Sljedeći primjer ilustrira prethodni teorem.

Primjer 14. *Pretpostavimo da je $A = \{1, 2, 3, 4\}$ reducirani sustav ostataka modulo 5, kojeg smo dobili tako što smo iz potpunog sustava ostataka $\{1, 2, 3, 4, 5\}$ isključili elemente koji nisu relativno prosti s 5. Kako vrijedi da je $(3, 5) = 1$, tada je i skup $\{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3\}$, odnosno $\{3, 6, 9, 12\}$ reducirani sustav ostataka modulo 5.*

Eulerova funkcija glavni je dio Eulerova teorema kojeg ćemo sada navesti.

Teorem 7 (Eulerov teorem, vidi [3, Teorem 3.9.]). *Pretpostavimo da je $c \in \mathbb{Z}$ i da je $(c, n) = 1$. Tada je*

$$c^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dokaz:
Pretpostavimo da je $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Prema Teoremu 6 zaključujemo da je $\{cr_1, cr_2, \ldots, cr_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n. Sada imamo

$$\prod_{j=1}^{\varphi(n)} (cr_j) \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}, \tag{1}$$

iz čega slijedi

$$c^{\varphi(n)} \prod_{j=1}^{\varphi(n)} r_j \equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n}. \tag{2}$$

Znamo da je $(r_i, n) = 1$. Tada iz Teorema 1 imamo $c^{\varphi(n)} \equiv 1 \pmod{n}$. □

U sljedećim primjerima možemo vidjeti primjenu Eulerova teorema.

Primjer 15. *Skup $A = \{1, 2, 3, 4\}$ je reducirani sustav ostataka modulo 5 i $(3, 5) = 1$. Iz definicije Eulerove funkcije znamo da je $\varphi(5) = 4$ jer imamo 4 elementa u reduciranom sustavu ostataka modulo 5. Sada prema Eulerovom teoremu imamo da je $3^4 \equiv 1 \pmod{5}$.*

Primjer 16. *Potrebno je odrediti sve ostatke pri dijeljenju dvadesete potencije cijelog broja s 25.*

Rješenje:
Znamo da je $\varphi(25) = \varphi(5^2) = 5 \cdot 4 = 20$. Imamo dva slučaja:

1) Ako $(c, 25) = 1$, onda $c^{20} \equiv 1 \pmod{25}$.

2) Ako $(c, 25) \neq 1$, odnosno $(c, 5) \neq 1$, onda je $c = 5 \cdot k$, za $k \in \mathbb{Z}$ pa imamo $c^{20} = (5k)^{20} = 5^{20} \cdot k^{20} = 5^{2 \cdot 10} \cdot k^{20} = (5^2)^{10} \cdot k^{20} \equiv 0 \pmod{25}$. Dakle, ostatci pri dijeljenju dvadesete potencije nekog broja s 25 su 0 i 1.

Posljedica Eulerovog teorema je Mali Fermatov teorem kojeg ćemo navesti u nastavku.

Teorem 8 (Mali Fermatov teorem, vidi [3, Teorem 3.10.])**.** *Pretpostavimo da je b prost broj i $c \in \mathbb{Z}$. Tada je $c^b \equiv c \pmod{b}$. Posebno, ukoliko $b \nmid c$, tada je $c^{b-1} \equiv 1 \pmod{b}$.*

Dokaz:
Ukoliko $b \nmid c$, tada vrijedi $(c, b) = 1$ pa prema Teoremu 7 imamo da je $c^{b-1} \equiv 1 \pmod{b}$. Pomnožimo li lijevu i desnu stranu kongruencije s c imamo da je $c^b \equiv c \pmod{b}$. Ukoliko $b \mid c$, onda je $(c, b) = b$ iz čega opet slijedi da je $c^b \equiv c \pmod{b}$. □

Primjenu Malog Fermatovog teorema možemo vidjeti u sljedećim primjerima.

Primjer 17. *Kako je reducirani sustav ostataka modulo 5 skup $\{1, 2, 3, 4\}$, znamo da je $\varphi(5) = 4$. Uz činjenicu da je $(107, 5) = 1$, možemo primijeniti Mali Fermatov teorem i slijedi da je $107^5 \equiv 1 \pmod{5}$. Nadalje, slijedi da je i $107^{5 \cdot z} \equiv 1 \pmod{5}$, $\forall z \in \mathbb{N}$.*

Primjer 18. *Potrebno je odrediti ostatak pri dijeljenju broja $n = 3^{60} + 7^{60}$ s 11.*

Rješenje:
Znamo da je 11 prost broj, $\varphi(11) = 10$ te kako je $(3, 11) = (7, 11) = 1$ prema Malom Fermatovom teoremu imamo $3^{10} \equiv 1 \pmod{11}$ i $7^{10} \equiv 1 \pmod{11}$. Dakle, imamo $3^{60} + 7^{60} \equiv (3^{10})^6 + (7^{10})^6 \equiv 1^6 + 1^6 \equiv 2 \pmod{11}$.

Kako bismo naveli jedno važno svojstvo Eulerove funkcije, najprije ćemo definirati multiplikativne funkcije.

Definicija 5. *Multiplikativna funkcija je funkcija $\phi : \mathbb{N} \to \mathbb{C}$ za koju vrijede svojstva:*

1) $\phi(1) = 1$;

2) $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b$ takve da je $(a, b) = 1$.

Sada možemo navesti sljedeći teorem.

Teorem 9 (vidi [3, Teorem 3.11.])**.** *Eulerova funkcija φ je multiplikativna funkcija. Osim toga, $\forall b \in \mathbb{N}, b > 1$ vrijedi*

$$\varphi(b) = b \prod_{p \mid b} (1 - \frac{1}{p}).$$

Dokaz:
Prema definiciji multiplikativne funkcije trebamo pokazati da je $\varphi(1) = 1$ i $\varphi(ab) = \varphi(a)\varphi(b)$, za $(a, b) = 1$. Iz definicije se odmah vidi da je $\varphi(1) = 1$. Pretpostavimo da su a, b takvi da vrijedi $(a, b) = 1$ te da m i n prolaze skupom svih reduciranih ostataka modulo a i b. Potrebno je pokazati da se $na + mb$ nalazi u reduciranom sustavu ostataka modulo ab. Ukoliko to pokažemo, dobit ćemo da je $\varphi(a)\varphi(b) = \varphi(ab)$. Kako je $(m, a) = 1$ i $(n, b) = 1$, broj $(mb + na)$ je relativno prost s a i b pa stoga i s ab. Bilo koja dva broja tog oblika su međusobno nekongruentna. Iz $mb + na \equiv m'b + n'a \pmod{ab}$ slijedi $(m - m')b \equiv (n' - n)a \pmod{ab}$. Iz toga zaključujemo da $a \mid m - m', b \mid n' - n$ pa imamo $m = m', n = n'$. Sada preostaje samo pokazati da ukoliko je $(c, ab) = 1$, tada je $c \equiv mb + na \pmod{ab}$. Kako je $(a, b) = 1$, $\exists x, y \in \mathbb{Z}$ za koje vrijedi $ax + by = 1$. Kako možemo zaključiti da vrijedi $(cy, a) = 1$ i $(cx, b) = 1$, brojevi m, n definirani s $cy \equiv m \pmod{a}$, $cx \equiv n \pmod{b}$ imaju tražena svojstva. Pretpostavimo da je sada $b = p_1^{\alpha_1} \cdot \ldots \cdot {}_k^{\alpha_k}$. Zbog multipliktivnosti od φ imamo

$$\varphi(b) = \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = b\prod_{i=1}^{k}(1 - \frac{1}{p_i}) = b\prod_{p|b}(1 - \frac{1}{p}).$$

□

4 Kongruencije po prostom modulu

Ovdje ćemo iskazati i dokazati Wilsonov i Lagrangeov teorem te vidjeti na primjerima neke njihove primjene. Kako bismo dokazali Wilsonov teorem najprije ćemo definirati multiplikativni inverz.

Definicija 6. *Pretpostavimo da je b prost broj i $c \in \mathbb{Z}$ sa svojstvom $(c, b) = 1$. Broj $x \in \mathbb{N}$ sa svojstvom*

$$cx \equiv 1 \pmod{b}$$

naziva se multiplikativni inverz od c modulo b.

U prethodnoj definiciji možemo uočiti da je multiplikativni inverz jedinstven jer vrijedi da je $(c, b) = 1$ prema Teoremu 2.
U sljedećem primjeru možemo vidjeti ilustraciju pojma multiplikativnog inverza.

Primjer 19. *Kako je 5 prost broj i 3 cijeli broj takav da vrijedi $(3, 5) = 1$ prirodan broj x sa svojstvom $3x \equiv 1 \pmod{5}$ naziva se multiplikativni inverz od 5. Taj broj u ovom slučaju je 7.*

Uočimo da ukoliko vrijedi $c^2 \equiv 1 \pmod{b}$ onda je c sam sebi inverzan modulo b.
Navedimo sada Wilsonov teorem.

Teorem 10 (Wilsonov teorem, vidi [3, Teorem 3.13.])**.** *Ukoliko je b prost broj, vrijedi*

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

Dokaz:
Brojevi iz skupa $\{1, 2, \ldots, b-1\}$ su faktori u $(b-1)! = 1 \cdot 2 \cdots (b-1)$ te prema prethodnim razmatranjima svaki od njih ima točno jedan multiplikativni inverz modulo b. Odredimo sada sve one faktore koji su sami sebi inverz, odnosno one $x \in \{1, 2, \ldots, b-1\}$ za koje vrijedi $x^2 \equiv 1 \pmod{b}$ jer inače produkt svakog faktora s njegovim multiplikativnim inverzom daje 1 modulo b. Odavde možemo zaključiti da $b \mid x^2 - 1 = (x-1)(x+1)$, a kako je b prost broj iz skupa $x \in \{1, 2, \ldots, b-1\}$, imamo dvije mogućnosti:

1) $b \mid x - 1$ i vrijedi $0 \leq x - 1 \leq b - 2$, iz čega slijedi da je $x - 1 = 0$, odnosno $x = 1$;

2) $b \mid x + 1$ i vrijedi $2 \leq x + 1 \leq b$, iz čega slijedi da je $x + 1 = b$, odnosno $x = b - 1$.

Zaključujemo da vrijedi

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

□

Pogledajmo sada na primjerima ilustraciju ovog teorema.

Primjer 20. *Kako je 7 prost broj, imamo da je $(7-1)! \equiv -1 \pmod{7}$. Odnosno, $720 \equiv -1 \pmod{7}$.*

Primjer 21. *Potrebno je odrediti ostatak pri dijeljenju broja* $17!$ *s 19.*

Rješenje:
Znamo da je 19 prost broj. Prema Wilsonovom teoremu imamo $18! \equiv -1 \pmod{19}$. Kako je $18 \cdot 17! \equiv -1 \pmod{19}$, odnosno $-1 \cdot 17! \equiv \pmod{19}$ imamo $17! \equiv 1 \pmod{19}$.
U sljedećoj napomeni iskazat ćemo kako vrijedi i obrat Wilsonova teorema.

Napomena 1 (Obrat Wilsonova teorema)**.** *Ukoliko* $n \in \mathbb{N}$ *zadovoljava kongruenciju*

$$(n-1)! \equiv -1 \pmod{n},$$

onda je n *prost broj.*
Zaista, uzmimo $n \in \mathbb{N}$ *za kojeg vrijedi* $(n-1)! \equiv -1 \pmod{n}$*. Pretpostavimo da je* $m \in \{1, 2, \ldots, n-1\}$ *takav da vrijedi* $m \mid n$*. Jer je* n *višekratnik od* m*, znamo da je*

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

Budući da je $1 \leq m < n$*, slijedi da* $m \mid (n-1)!$*, odnosno,*

$$(n-1)! \equiv 0 \pmod{m}.$$

Sada imamo da je

$$-1 \equiv 0 \pmod{m},$$

odnosno, $m = 1$*. Iz toga možemo zaključiti da je* n *prost broj.*

Pogledajmo na primjeru prethodnu tvrdnju.

Primjer 22. *Kako broj 59 zadovoljava kongruenciju* $(59-1)! \equiv -1 \pmod{59}$*, možemo zaključiti da je 59 prost broj.*

U nastavku iskazat ćemo i dokazati teorem poznat pod nazivom Lagrangeov teorem.

Teorem 11 (Lagrangeov teorem, vidi [3, Teorem 3.15.])**.** *Ukoliko je* b *prost broj i* $P(x)$ *polinom s cjelobrojnim koeficijentima stupnja* n *kojemu vodeći koeficijent nije djeljiv s* b*, onda kongruencija*

$$P(x) \equiv 0 \pmod{b}$$

ima najviše n *rješenja modulo* b*.*

Dokaz:
Dokaz ćemo provesti metodom matematičke indukcije po stupnju polinoma.

(B) Ako je $n = 1$, onda je polinom oblika $P(x) = a_1 x + a_0$, $b \nmid a_1$. U tom slučaju imamo linearnu kongruenciju koja ima jedinstveno rješenje modulo b.

(P) Neka je tvrdnja ispunjena za polinome stupnja manjeg od n.

(K) Promatrajmo sada polinom oblika

$$P(x) = a_n x^n + \cdots + a_1 x + a_0, b \nmid a_n.$$

Ukoliko kongruencija $P(x) \equiv 0 \pmod{b}$ nema rješenja, onda smo gotovi. Ukoliko kongruencija $P(x) \equiv 0 \pmod{b}$ ima rješenja, onda postoji x_0 za kojeg vrijedi $P(x_0) \equiv 0 \pmod{b}$. Tada vrijedi $P(x) \equiv P(x) - P(x_0) \pmod{b} \equiv a_n(x^n - x_0^n) + \cdots + a_1(x - x_0) \pmod{b}$. Za svaki od izraza $x^k - x_0^k$ vrijedi $x^k - x_0^k = (x - x_0)(x^{k-1} + x^{k-2}x_0 + \cdots + x x_0^{k-2} + x_0^{k-1})$. Sada možemo zaključiti da postoji polinom $Q(x)$ stupnja $n-1$ sa svojstvom da je $P(x) \equiv (x - x_0)Q(x) \pmod{b}$. Dobivamo jednadžbu $(x - x_0)Q(x) \equiv 0 \pmod{b}$. Iz uvjeta $b \mid (x - x_0)Q(x)$ imamo kongruenciju $x \equiv x_0 \pmod{b}$, a ta kongruencija ima rješenje x_0 ili $(x - x_0)Q(x) \equiv 0 \pmod{b}$, za koju vrijedi da ima najviše $n-1$ rješenja modulo b. Možemo zaključiti da polazna kongruencija ima najviše n rješenja modulo b.

□

Sljedeći primjer ilustrira ovaj teorem.

Primjer 23. *Kako je 5 prost broj i* $P(x) = 17 \cdot x^3 + 6 \cdot x^2 + 7 \cdot x + 18$ *polinom s cjelobrojnim koeficijentima stupnja 3 kojemu vodeći koeficijent, odnosno 17 nije djeljiv s 5, onda kongruencija* $17x^3 + 6x^2 + 7x + 18 \equiv 0 \pmod{5}$ *ima najviše 3 rješenja modulo 5. U ovom primjeru uvrštavanjem* $x \equiv 0, 1, 2, 3, 4 \pmod{5}$ *kongruencija* $17x^3 + 6x^2 + 7x + 18 \equiv 0 \pmod{5}$ *ima samo jedno rješenje i to je* $x \equiv 4 \pmod{5}$.

5 Još neke primjene kongruencija

Kongruencije imaju široku primjenu u raznim znanstvenim disciplinama. U ovom poglavlju bavit ćemo se upravo proučavanjem još nekih primjena kongruencija, kao što je ispitivanje djeljivosti brojeva. Osim toga, vidjet ćemo njihovu primjenu u kriptografiji i generiranju barkodova proizvoda.

5.1 Ispitivanje djeljivosti

Pomoću kongruencija možemo izvesti testove za djeljivost na osnovi svojstava grupa znamenaka danog broja. Uzmimo broj $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0$, gdje su $a_i \in \{0, 1, 2, 3, 4, \ldots, 9\}$ i $a_k \neq 0$. Promatrajmo najprije djeljivost s brojevima 2 i 5. Kako je $10^m \equiv 0 \pmod 2$ i $10^m \equiv 0 \pmod 5$ za $m \geqslant 1$, dobivamo da je $n \equiv a_0 \pmod 2$ i $n \equiv a_0 \pmod 5$ iz čega slijede pravila za djeljivost:

1) 2 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zadnja znamenka djeljiva s 2, odnosno ukoliko je a_0 jednaka 0,2,4,6 ili 8;

2) 5 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zadnja znamenka djeljiva s 5, odnosno ukoliko je a_0 jednaka 0 ili 5.

Općenito, za potencije brojeva 2 i 5 vrijedi da 2^k dijeli $n \in \mathbb{N}$ onda i samo onda kada je broj formiran od zadnjih k znamenki promatranog broja n djeljiv s 2^k, odnosno djeljiv je s 5^k onda i samo onda kada je broj sačinjen od zadnjih k znamenki broja n djeljiv s 5^k.
Za djeljivost s brojevima 3 i 9 imamo:

1) 3 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj znamenaka $a_0 + a_1 + \cdots + a_k$ djeljiv s 3;

2) 9 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj znamenaka $a_0 + a_1 + \cdots + a_k$ djeljiv s 9.

Pogledajmo sada djeljivost s brojevima 7,11,13,37:

1) 7 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj troznamenastih grupa znamenaka s alternirajućim predznacima, odnosno $(a_2a_1a_0)_{10} - (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} - \ldots$ djeljiv sa 7;

2) 11 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj znamenaka s alternirajućim predznacima $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$ djeljiv s 11;

3) 13 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj troznamenastih grupa znamenaka s alternirajućim predznacima $(a_2a_1a_0)_{10} - (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} - \ldots$ djeljiv s 13;

4) 37 dijeli $n \in \mathbb{N}$ onda i samo onda mu je zbroj troznamenasth grupa znamenaka, odnosno $(a_2a_1a_0)_{10} + (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} + \ldots$ djeljiv s 37.

Na primjeru možemo vidjeti neke brojeve za koje vrijede navedena svojstva djeljivosti sa 7,11,13 i 37.

Primjer 24. *Broju 110 250 125 247 311 zbroj troznamenastih grupa znamenaka s alternirajućim predznacima je* $311 - 247 + 125 - 250 + 110 = 49$*, a kako je 49 djeljivo sa 7 i dani broj djeljiv je sa 7.*
Broju 72 919 altenirajuća suma znamenki je $9 - 1 + 9 - 2 + 7 = 22$*. Kako je 22 djeljivo s 11 i broj 72919 djeljiv je s 11.*
Broju 186 999 852 zbroj troznamenastih grupa znamenki s alternirajućim predznacima je $852 - 999 + 186 = 39$*. Kako je 39 djeljivo s 13 i dani broj djeljiv je s 13.*
Broju 100 000 011 zbroj troznamenastih suma znamenki iznosi $011 + 000 + 100 = 111$*, a kako je dana suma djeljiva s 37 i polazni broj djeljiv je s 37.*

5.2 Kriptografija

Kriptografija je znanstvena disciplina proučavanja metoda za slanje poruka u obliku da ih samo primatelj kome su namijenjene može pročitati. U daljnem tekstu navest ćemo osnovne pojmove koji se koriste u kriptografiji te pobliže objasniti postupak kriptografije.
Poruku koju pošiljatelj želi poslati nazivamo otvoreni tekst, a skup svih elemenata otvorenog teksta nazivamo alfabet otvorenog teksta. Pošiljatelj transformira dani otvoreni tekst koristeći ključ. Taj postupak naziva se šifriranje, a dobiveni rezultat nazivamo šifrat. Osnovne elemente šifrata nazivamo alfabet šifrata. Nadalje imamo kriptografski algoritam, odnosno šifru. Šifra je uređen par (e_k, d_k), gdje su e_k i d_k dvije funkcije za šifriranje, odnosno dešifriranje te ih biramo u ovisnosti o ključu. Dakle, ako ključu K odgovara šifra (e_k, d_k) te ako je x element alfabeta otvorenog teksta onda je $e_k(x)$ element alfabeta šifrata i tražmo da vrijedi $d_k(e_k(x)) = x$. Možemo uočiti da e_k mora biti injekcija kako bi dešifriranje bilo moguće jer u suprotnom primatelj bi imao više opcija za elemente otvorenog teksta. Za šifriranje i dešifriranje obično se koristi međunarodni (engleski) alfabet. Slovima $A, B, \ldots, Z$ (ima ih 26) pridruženi su numerički ekvivalenti $0, 1, \ldots, 25$, redom. Najstariji i najjednostavniji način šifriranja je tzv. Cezarova šifra. Ona pripada klasi supstitucijskih šifri, gdje se svakom slovu otvorenog teksta pridružuje neko drugo slovo. Preciznije, slova otvorenog teksta potrebno je zamijeniti slovima koja se nalaze tri mjesta udesno, ciklički. Za slučaj engleskog alfabeta imamo da je $K \in \{0, 1, \ldots, 25\}$, te su funkcije šifriranja i dešifriranja dane sa

$$e_k(x) \equiv (x + 3) \pmod{26}, \qquad d_k(y) \equiv (y - 3) \pmod{26}.$$

Primjer 25. *Potrebno je šifrirati riječ primjer koristeći Cezarovu šifru.*

Rješenje:
Šifriramo li riječ *primjer* dobivamo slijed znakova *sulpmhu.*
Postoje i druge šifre koje koriste kongruencije npr. RSA kriptosustav, koji je primjer kriptosustava s javnim ključem. Detaljnije o ostalim šiframa može se pronaći u [2].

5.3 Barkodovi

Još neku od primjena kongruencija pronalazimo u generiranju barkodova proizvoda. Postoje različiti standardni barkodovi u ovisnosti o broju znamenki, odnosno mogu se sastojati

od 8,12,13,14,17 ili 18 znamenki. Ako imamo barkod koji se sastoji od 13 znamenki, odnosno barkod oblika $n_1 \cdots n_{13}$ zadnja, odnosno trinaesta znamenka je kontrolna znamenka koju odabiremo tako da vrijedi kongruencija oblika $n_1 + 3n_2 + n_3 + \cdots + 3n_{12} + n_{13} \equiv 0 \pmod{10}$.

Literatura

[1] G. E. Andrews, *Number theory*, Pennsylvania State University, Pennsylvania, 1971.

[2] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[4] J. E. Shockley, *Introduction to number theory*, Virginia Polytechnic Institute, Blacksburg Virginia, 1967.