Kineski teorem o ostatcima

Tobijas, Tomislav

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:258546

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-23**

Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science

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

Kineski teorem o ostacima

Tomislav Tobijas

Završni rad

Osijek, 2019.

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

Kineski teorem o ostacima

Tomislav Tobijas

Završni rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2019.

Sadržaj

Uvod **1**

1 Kineski teorem o ostacima **2**

2 Druga metoda rješavanja **9**

3 Neke primjene u RSA kriptografiji **13**

4 Homomorfizmi i Eulerova φ-funkcija **16**

5 Sažetak **20**

6 Summary **21**

Literatura **22**

Uvod

U ovom završnom radu prisjetiti ćemo se definicije kongruencija i kako se one rješavaju te ćemo proučavati sustav od dvije ili više jednadžbe, odnosno kongruencije. Kada su u sustavu kongruencija svaka dva modula međusobno relativno prosta, glavni teorem za rješavanje sustava poznat je kao Kineski teorem o ostacima jer su posebni slučajevi teorema bili poznati drevnim Kinezima. Prema predaji, Kinezi su se često u primjenama koristili upravo prethodnim rezultatom. Neki navodi govore kako je postupak određivanja rješenja sustava kongruencija prvenstveno korišten u vojne svrhe prilikom prebrojavanja preživjelih vojnika nakon bitke. Naime, umjesto da se nepotrebno troši vrijeme na dugačka prebrojavanja, preživjeli vojnici bi se jednostavno postrojili u redove od po 3, 4, 5, 7, 11 i eventualno 13 vojnika (ukoliko bi se radilo o većem broju preživjelih vojnika), a potom bi se pomoću broja vojnika preostalih u zadnjem redu dobivao sustav kongruencija. Rješavanje tako dobivenog sustava bi rezultiralo kongruencijom iz koje bi se direktno dobio točan broj preživjelih vojnika. Naravno, broj vojnika u pojedinom redu se mogao i mijenjati, jedino se uvijek moralo paziti da brojevi budu međusobno relativno prosti te njihov produkt dovoljno velik kako bi se iz završne kongruencije mogao očitati točan broj preživjelih vojnika. U modernoj algebri, Kineski teorem o ostacima je vrlo koristan alat koji ima mnoštvo različitih primjena.

Slika 1: Ilustracija drevne kineske vojske

1 Kineski teorem o ostacima

Na početku, prisjetimo se samo definicije kongruencija: Neka je n prirodan broj, te neka su a i b cijeli brojevi. Ako n dijeli razliku $a - b$ tada kažemo da je a kongruentan b modulo n, ili da su a i b kongruentni modulo n, te pišemo $a \equiv b(\text{mod } n)$.

Primjetimo da je a djeljiv s n ako i samo ako je $a \equiv 0(\text{mod } n)$. Također, ako je c prirodan broj i $a \equiv b(\text{mod } n)$, tada je i $ac \equiv bc(\text{mod } nc)$.

U ovom poglavlju ćemo prvo proučavati sustav od dvije linearne kongruencije te ćemo promotriti par primjera vezanih uz takve sustave. Nadalje prikazati ćemo i specifični oblik Kineskog teorema o ostacima koji se odnosi na sustav od samo dvije linearne jednadžbe, dok ćemo nakon toga proučavati i kompleksnije sustave koji se sastoje od tri ili više liearnih jednadžbi, tj. kongruencija.

Lema 1.1. *Neka su m i n relativno prosti prirodni brojevi. Tada za svaki par cijelih brojeva a,b postoji jedinstveno (modulo mn) rješenje sustava kongruencija*

$$x \equiv a(\text{mod } m)$$
$$x \equiv b(\text{mod } n).$$

Teorem. 1.2. *Neka su m i n prirodni brojevi > 1 (moduli) i neka su a i b bilo koja dva cijela broja. Tada je $x = x_0$ rješenje sustava*

$$x \equiv a(\text{mod } m)$$
$$x \equiv b(\text{mod } n),$$

ako i samo ako najveći zajednički djelitelj brojeva m i n dijeli $b - a$. Ako je $x = x_0$ rješenje, tada je skup rješenja cijelih brojeva x koji zadovoljavaju dvije kongruencije jednak skupu od x koji zadovoljava

$$x \equiv x_0(\text{mod } [m, n])$$

gdje je $[m,n]$ najmanji zajednički višekratnik od m i n.

Prije samih primjera prisjetimo se Euklidovog algoritma koji će nam biti potreban za rješavanje daljnjih primjera.

Teorem. 1.3. *Neka su a,b cijeli brojevi, $a > 0$. Tada postoje jedinstveni cijeli brojevi q i r takvi da je $b = q \cdot a + r$, pri čemu je $0 \leq r < a$.*

Neka su a i b cijeli brojevi te neka smo uzastopnom primjenom Teorema 1.3 dobili sljedeći niz jednakosti:

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

(postupak završava kada dobijemo ostatak jednak nuli). Kako je $a > r_1 > r_2 > \dots$ čitav postupak završava nakon konačno mnogo koraka.

Iz prve jednakosti slijedi $(a, b)|r_1$ te da je svaki zajednički djelitelj brojeva a i r_1 ujedno i djelitelj broja b. Prema tome, $(a, b) = (a, r_1)$. Na isti način dobivamo i niz jednakosti $(a, b) = (a, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$ jer r_n dijeli r_{n-1}. Prema tome, (a, b) jednak je posljednjem nenul ostatku. Opisani postupak određivanja najvećeg zajedničkog djelitelja naziva se *Euklidov algoritam.*

Primjetimo da iz prve jednakosti Euklidova algoritma možemo zapisati $r_1 = b - q_1 a$. Uvrštavanjem u idući redak dobivamo $r_2 = (1 + q_1 q_2)a - q_2 b$. Nastavljajući na isti način, uvrštavanjem u naredne jednakosti, možemo zaključiti da postoje cijeli brojevi x i y za koje vrijedi

$$ax + by = r_n = (a, b).$$

Prethodni identitet se obično naziva *Bezoutov identitet* .

Pogledajmo sada nekoliko primjera.

Primjer 1.4. Neka je dan par kongruencija

$$x \equiv 11 (\text{mod } 74)$$
$$x \equiv 13 (\text{mod } 63),$$

Ako je x rješenje, tada

$$x = 11 + 74r$$

za neki $r \in \mathbb{Z}$, i

$$x = 13 + 63s$$

za neki $s \in \mathbb{Z}$. Nakon izjednačavanja tih dviju jednadžbi slijedi

$$11 + 74r = 13 + 63s$$

odnosno

$$74r - 63s = 2.$$

Jednadžbu je moguće rješiti pomoću proširenog **Euklidovog algoritma**, jer najveći zajednički djelitelj od 74 i 63, koji je 1, dijeli 2. Euklidov algoritam za 74 i 63 je:

$$74 = 63 + 11$$
$$63 = 11 \cdot 6 - 3$$
$$11 = 3 \cdot 3 + 2$$

Koristeći pristup rješavanja po recima imamo

	koef. od 74	koef. od 63
74	1	0
63	0	-1
11	1	-1
66	6	6
3	6	-7
9	18	-21
2	-17	20

Iz zadnjeg retka tablice očito je

$$2 = 74 \cdot (-17) + 63 \cdot 20.$$

Kako želimo pronaći r i s takve da $74r - 63s = 2$, postaviti ćemo da je $r = -17$ te $s = -20$. Kako je $x = 13 + 63s$, slijedi da je $x = 13 - 63 \cdot 20 = 13 - 1260 = -1247$ rješenje danih kongruencija. Kao sa jednom linearnom kongruencijom, nakon što pronađemo partikularno rješenje $x = -1247$ od

$$x \equiv 11 (\text{mod } 74) \tag{1}$$
$$x \equiv 13 (\text{mod } 63) \tag{2}$$

možemo pronaći opće rješenje tako što ćemo partikularno rješenje dodati općem rješenju homogenog sustava kongruencija

$$x \equiv 0 (\text{mod } 74)$$
$$x \equiv 0 (\text{mod } 63)$$

Cijeli broj x koji rješava homogeni sustav mora biti višekratnik od 74 i višekratnik od 63, odnosno višekratnik od 74 i 63. Kako su 74 i 63 relativno prosti, najmanji zajednički višekratnik [74,63] od 74 i 63 je $74 \cdot 63 = 4662$. Partikularnom rješenju općih (nehomogenih) kongruencija, kao što je $x = -1247$, možemo dodati bilo koji višekratnik od 4662 i dobiti novo rješenje. Skup svih rješenja za sustav linearnih jednadžbi (1) i (2) je skup svih cijelih brojeva x oblika

$$x = -1247 + 4662k$$

za $k \in \mathbb{Z}$. Odnosno ovo je jednako skupu svih cijelih brojeva x koji zadovoljavaju kongruenciju

$$x \equiv -1247 (\text{mod } 4662).$$

Primjer 1.5. Neka je dan sustav od dvije linearne kongruencije

$$x \equiv 2 (\text{mod } 24)$$
$$x \equiv 8 (\text{mod } 39)$$

Neka je sada $x = 2 + 24r = 8 + 39s$ iz čega slijedi $24r - 39s = 6$. Kako je $(24, 39) = 3$ te kako 3 dijeli 6, imamo rješenje. Analognim postupkom kao u primjeru 1.4 dolazimo do jednakosti $39 \cdot 2 - 24 \cdot 3 = 6$ pa tako slijedi $x = 2 + 24(-3) = -70$. Opće rješenje je $x = -70 + [24, 39]k$, $k \in \mathbb{Z}$. Kako je $[24, 39] = 312$, slijedi da su rješenja oblika $x = -70 + 312k$, $k \in \mathbb{Z}$, odnosno

$$x \equiv -70 (\text{mod } 312).$$

Iz toga slijedi kako je $x = -70 + 312 = 242$ najmanje pozitivno rješenje.

Primjer 1.6. Pogledajmo sustav

$$x \equiv 5 (\text{mod } 20)$$
$$x \equiv 15 (\text{mod } 16).$$

Postavimo sada da je $x = 5 + 20r = 15 + 16s$ te prebacimo nepoznanice na jednu stranu:

$$20r - 16s = 10.$$

U ovom primjeru, najveći zajednički dijelitelj od 20 i 16 je 4, ali 4 ne dijeli 10 pa proizlazi da ne postoje cijeli brojevi r i s takvi da je $5 + 20r = 15 + 16s$ te da ne postoji rješenje danog para kongruencija.

Dokaz teorema 1.2 slijedi metodu korištenu u navedenim primjerima. Također za rješavanje jednadžbi u dokazu teorema 1.2 koristi se i **Bezoutov identitet** odnosno postupak za nalaženje cjelobrojnih rješenja jednadžbe $a \cdot x + b \cdot y = r_n = (a, b)$ koji smo naveli nešto ranije u ovom poglavlju.

Kao neposredni korolar koji proizlazi iz teorema 1.2 dobivamo Kineski teorem o ostacima za sustav koji se sastoji od dvije kongruencije:

Korolar 1.7. *Neka su m i n relativno prosti prirodni brojevi veći od 1 (moduli) te a i b cijeli brojevi. Tada postoji rješenje $x = x_0$ od*

$$x \equiv a(\text{mod } m)$$
$$x \equiv b(\text{mod } n).$$

Skup rješenja svih cijelih brojeva x koji zadovoljavaju ove dvije kongruencije jednak je skupu x-eva koji zadovoljavaju

$$x \equiv x_0(\text{mod } mn)$$

Ukoliko imamo par kongruencija gdje je jedan od modula relativno malen, možemo smanjiti broj potrebnih operacija koristeći Bezoutov identitet tako što ćemo rješavati samo jednu kongruenciju modulo manji od dva dana modula.

Primjer 1.8. Pogledajmo sustav

$$x \equiv 38(\text{mod } 60)$$
$$x \equiv 7(\text{mod } 11).$$

Tada je $x = 38 + 60r = 7 + 11s$ za neke $r, s \in \mathbb{Z}$. Kako bi odredili x nije potrebno odrediti obje nepoznanice odnosno i r i s u jednadžbi

$$38 + 60r = 7 + 11s,$$

već samo jednu od nepoznanica. Stoga umjesto pristupanju jednadžbi i rješavanju iste pomoću Bezoutovog identiteta, pogledajmo jednadžbu kao kongruenciju modulo manji od dva dana modula:

$$38 + 60r \equiv 7(\text{mod } 11).$$

Skraćivanjem 38 i 60 modulo 11 slijedi

$$5 + 5r \equiv 7(\text{mod } 11)$$

što je ekvivalentno

$$5r \equiv 2(\text{mod } 11).$$

Kako je inverz od 5 modulo 11 jednak 9, množimo zadnju kongruenciju sa 9 te dobivamo

$$r \equiv 9 \cdot 5r \equiv 9 \cdot 2 \equiv 7(\text{mod } 11).$$

Sada je $x = 38 + 7 \cdot 60 = 458$ rješenje početnih kongruencija. Kako je najmanji zajednički višekratnik od 11 i 60 jednak 660, opće rješenje jednako je

$$x \equiv 458(\text{mod } 660).$$

Tri ili više kongruencija. Ključna stvar kod rješavanja sustava koji se sastoji od 3 ili više kongruencije je zapažanje da možemo izraziti skup cijelih brojeva koji su rješenje dvije istodobne kongruencije kao skup cijelih brojeva koji zadovoljavaju jednu kongruenciju.

Primjer 1.9. Pronađimo sva rješenja sustava

$$x \equiv 2(\text{mod } 12)$$
$$x \equiv 8(\text{mod } 10)$$
$$x \equiv 9(\text{mod } 13).$$

Prvo rješavamo prve dvije kongruencije: tražimo x takav da je $x = 2 + 12r = 8 + 10s$. Vrlo je jednostavno pokazati da je $x = 38$ rješenje. Kako je $[12, 10] = 60$, opće rješenje prve dvije kongruencije jednako je $x = 38 + 60k$ za $k \in \mathbb{Z}$. Tako je rješavanje sustava dane 3 kongruencije jednako rješavanju sustava

$$x \equiv 38(\text{mod } 60)$$
$$x \equiv 9(\text{mod } 13).$$

Ovaj par kongruencija ima svojstvo da je modul 13 u trećoj početnoj kongruenciji manji od modula 60 koji proizlazi iz prve dvije kongruencije. Stoga je metoda kongruencija iz prethodnog primjera vrlo korisna. Stoga kako bi našli t takav da je $x = 38 + 60t = 9 + 13u$ za neki u, možemo postaviti kongruenciju

$$38 + 60t \equiv 9(\text{mod } 13)$$

koja nakon dijeljenja modulo 13 izgleda ovako:

$$-1 - 5t \equiv 9(\text{mod } 13)$$

odnosno

$$-5t \equiv 10(\text{mod } 13).$$

Stoga

$$t \equiv -2 \equiv 11(\text{mod } 13),$$

pa je $x = 38 + 60 \cdot (11) = 698$. Opće rješenje početne tri kongruencije tada je jednako

$$x \equiv 698(\text{mod } 780)$$

jer je $[10, 12, 13] = 60 \cdot 13 = 780$.

Ako imamo sustav od n kongruencija u kojima su moduli u parovima međusobno relativno prosti, tada uvijek postoji rješenje i to rješenje je jedinstveno do na modulo produkt svih modula. Stoga imamo:

Teorem. 1.10. (Kineski teorem o ostacima.) *Neka su $m_1, m_2, \ldots, m_n$ u parovima relativno prosti prirodni brojevi veći od 1 (moduli) te neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi. Tada postoji rješenje sustava kongruencija*

$$x \equiv a_1(\text{mod } m_1)$$
$$x \equiv a_2(\text{mod } m_2)$$
$$\vdots$$
$$x \equiv a_n(\text{mod } m_n).$$

Ako je x_0 jedno rješenje, tada su sva rješenja dana s

$$x \equiv x_0 (\text{mod } M),$$

gdje je $M = m_1 m_2 \cdot \ldots \cdot m_n$.

Za dokaz ovog teorema biti će nam potrebna još jedna dodatna tvrdnja.

Lema 1.11. *Ako je p prost broj i p dijeli umnožak bc, tada p dijeli b ili p dijeli c.*

Dokaz. Znamo da ako a dijeli umnožak bc i $(a, b) = 1$, slijedi da a dijeli c.

Pretpostavimo da je p prost broj i da p dijeli bc. Kako je p prost slijedi da ili p dijeli b ili $(p, b) = 1$. Ako $(p, b) = 1$ onda proizlazi da p dijeli c. □

Iz Leme 1.11 indukcijom slijedi da ako prost broj dijeli produkt od m brojeva tada proizlazi da taj prost broj dijeli jedan od faktora. Odnosno za specijalni slučaj da ukoliko je $m = bc$ te da p dijeli produkt bc dva broja b i c tada p dijeli b ili p dijeli c.

Dokaz. (Kineski teorem o ostacima) Dokaz ide indukcijom po n gdje je n broj kongruencija. U slučaju dvije kongruencije imamo upravo Korolar 1.7. Za $n > 2$ mi pretpostavljamo da bilo koji skup od $n-1$ kongruencija, čiji moduli su u paru relativno prosti ima rješenje. Pretpostavimo da imamo skup od n kongruencija kao u tvrdnji teorema. Koristiti ćemo teorem za dvije kongruencije kako bi zamijenili prve dvije kongruencije sa jednom kongruencijom, oblika

$$x \equiv x_0 (\text{mod } m_1 m_2).$$

Tada kako bi pokazali da postoji rješenje početnog skupa od n kongruencija, moramo pokazati da postoji skup od $n - 1$ kongruencija koji se sastoji od svih osim prve dvije od n početnih kongruencija, zajedno s kongruencijom

$$x \equiv x_0 (\text{mod } m_1 m_2).$$

Kako bi primijenili pretpostavku indukcije, jedina stvar koju moramo promatrati je da novi zadnji modul, $m_1 m_2$, ima svojstvo da su $m_1 m_2$ i m_j relativno prosti za $j = 3, \ldots, n$. Iz Leme 1.11 sada proizlazi da ako je $(m_j, m_1) = 1$ i $(m_j, m_2) = 1$, tada je $(m_j, m_1 m_2) = 1$. Stoga skup od $n - 1$ kongruencija ima rješenje po indukciji hipoteze i to rješenje će biti rješenje početnih n kongruencija. □

Kao prvu primjenu Kineskog teorema s ostacima gledati ćemo jednu linearnu kongruenciju složenog modula.

Primjer 1.12. Kako bi rješili sustav

$$\begin{aligned} 11x &\equiv 13 (\text{mod } 20) \\ 9x &\equiv 17 (\text{mod } 25), \end{aligned}$$

prvo ćemo rješiti $11x \equiv 13 (\text{mod } 20)$. Primjetimo da je $11 \cdot 11 = 121 \equiv 1 (\text{mod } 20)$, pa

$$x = 13 \cdot 11 \equiv 143 \equiv 3 (\text{mod } 20).$$

Nakon toga rješavamo $9x \equiv 17 (\text{mod } 25)$. Primjetimo da je $9 \cdot 11 \equiv -1 (\text{mod } 25)$, pa

$$x \equiv -17 \cdot 11 \equiv 8 \cdot 11 \equiv 88 \equiv 13 (\text{mod } 25).$$

Stoga je početni sustav ekvivalentan

$$x \equiv 3(\text{mod } 20)$$
$$x \equiv 13(\text{mod } 25).$$

Ili, kako smo zaključili da je prva kongruencija ekvivalentna $x \equiv 3(\text{mod } 20)$, možemo napraviti supstituciju $x = 3 + 20k$ u drugu kongruenciju kako bi dobili

$$9(3 + 20k) \equiv 17(\text{mod } 25)$$

te pojednostavili da dobijemo

$$5k \equiv -10(\text{mod } 25),$$

koje za rješenje ima $k = 3$, $x = 3 + 20 \cdot 3 = 63$. Nakon što pronađemo jedno rješenje, tada je zbog $[25, 20] = 100$ opće rješenje dano s

$$x \equiv 63(\text{mod } 100).$$

2 Druga metoda rješavanja

U ovome poglavlju dati ćemo alternativnu metodu za rješavanje sustava od n kongruencija kada su moduli u parovima međusobno relativno prosti. Ova metoda korisna je za rješavanje više sustava kongruencija u kojima se pojavljuje isti modul.

Ideja ove metode je da rješavamo posebne sustave kongruencija i tako dobijemo rješenje početne kongruencije kao linearnu kombinaciju rješenja posebnih sustava. Prođimo sada kroz par takvih primjera.

Primjer 2.1. Pogledajmo par kongruencija

$$x \equiv 15 (\text{mod } 20)$$
$$x \equiv 3 (\text{mod } 17).$$

Kako su 20 i 17 relativno prosti, znamo da postoji rješenje. Kako bi riješili ovaj sustav prvo ćemo riješiti dva sustava

$$x \equiv 1 (\text{mod } 20)$$
$$x \equiv 0 (\text{mod } 17)$$

i

$$x \equiv 0 (\text{mod } 20)$$
$$x \equiv 1 (\text{mod } 17).$$

U prvom sustavu, $x = e_1$ je rješenje ako je

$$e_1 = 1 + 20r = 17s.$$

Pretvorimo li gornju jednakost u kongruenciju modulo 20, slijedi

$$17s \equiv 1 (\text{mod } 20).$$

Kako je

$$17 \equiv -3 (\text{mod } 20)$$

i inverz od 3 modulo 20 je jednak 7, možemo postaviti da je $s = -7$ pa je stoga $e_1 = -119$. Slično, u drugom sustavu, $x = e_2$ je rješenje ako je

$$e_2 = 20t = 1 + 17u.$$

Pretvorimo li i tu jednakost u kongruenciju modulo 20, dobivamo

$$17u \equiv -1 (\text{mod } 20).$$

Množenjem kongruencije sa -1 slijedi

$$3u \equiv 1 (\text{mod } 20),$$

pa možemo staviti da je $u = 7$ i $e_2 = 120$. Nakon što smo pronašli e_1 i e_2, možemo pronaći rješenje x_0 početnog sustava postavljanjem da je

$$x_0 = 15e_1 + 3e_2 = 15 \cdot (-119) + 3 \cdot 120 = -1425.$$

(Provjera: modulo 20, $x_0 \equiv 15 \cdot (-119) \equiv 15 \cdot 1 = 15$, i modulo 17, $x_0 \equiv 3 \cdot 120 \equiv 3 \cdot 1 = 3$, kao što smo i željeli.) Kao i prije, jer je $[20, 17] = 20 \cdot 17 = 340$, opće rješenje je $x \equiv -1425 (\text{mod } 340)$ te je najmanje pozitivno rješenje jednako $x = -1425 + 340 \cdot 5 = 275$.

Primjetimo da ovakav način pronalaženja e_1 i e_2 neće biti moguć ukoliko moduli nisu relativno prosti. Na primjer, ukoliko probamo riješiti sustav

$$x \equiv 1 (\text{mod } 20)$$
$$x \equiv 0 (\text{mod } 18)$$

dobili bi da je $x = 1 + 20r = 18s$. Ali jednadžba $20r - 18s = 1$ nema rješenja jer brojevi 20 i 18 nisu relativno prosti.

Ukoliko planiramo riješavati samo jedan sustav od n kongruencija u kojima su moduli međusobno relativno prosti, metoda poglavlja (1) uključuje riješavanje $n - 1$ sustava koji se sastoje od dvije kongruencije, dok metoda ovog poglavlja uključuje riješavanje n sustava koji se sastoje od dvije kongruencije. Dodatna prednost metode iz 1. poglavlja je da obuhvaća sustave u kojima moduli nisu međusobno relativno prosti. Prednost metode iz ovog poglavlja je da je ona puno brža za riješavanje više sustava koji se sastoje od n kongruencija sa istim modulom.

Babilonsko množenje. Sada ćemo prikazati jednu zanimljivu primjenu metode iz ovog poglavlja.

Zamislite da se nalazite u društvu kao što su bili drevni Babilonci, gdje se "papir" sastojao od teških glinenih ploča, i gdje su brojevi bili zapisani u bazi 60. Kako bi pomnožili brojeve kao što su

$$(35, 43, 52) = 35 \cdot 60^2 + 43 \cdot 60 + 52$$

i

$$(14, 2, 47) = 14 \cdot 60^2 + 2 \cdot 60 + 47,$$

koristeći standardni algoritam za množenje, to bi značilo da bi trebali ili zapamtiti tablicu množenja s bazom 60, koja se satoji od $\frac{59 \cdot 60}{2} = 1770$ produkata, ili zapisati tablicu na glinene ploče koje bi bile preteške za prenošenje. Što u takvom slučaju napraviti? Koristiti ćemo Kineski teorem o ostacima.

Slika 2: Babilonska ploča za računanje

Prvo primjetimo da je $5 \cdot 8 \cdot 9 \cdot 11 = 3960 > 59 \cdot 59$ te da su $5, 8, 9$ i 11 u parovima međusobno relativno prosti. Pronađimo sada e_5 koji zadovoljava

$$\begin{aligned} e_5 &\equiv 1 (\text{mod } 5) \\ e_5 &\equiv 0 (\text{mod } 8 \cdot 9 \cdot 11); \end{aligned}$$

e_8 koji zadovoljava

$$\begin{aligned} e_8 &\equiv 1 (\text{mod } 8) \\ e_8 &\equiv 0 (\text{mod } 5 \cdot 9 \cdot 11); \end{aligned}$$

e_9 koji zadovoljava

$$\begin{aligned} e_9 &\equiv 1 (\text{mod } 9) \\ e_9 &\equiv 0 (\text{mod } 5 \cdot 8 \cdot 11); \end{aligned}$$

te e_{11} koji zadovoljava

$$\begin{aligned} e_{11} &\equiv 1 (\text{mod } 11) \\ e_{11} &\equiv 0 (\text{mod } 5 \cdot 8 \cdot 9). \end{aligned}$$

Nakon računa dobivamo da je $e_5 = -1584$, $e_8 = -495$, $e_9 = -440$ i $e_{11} = -1440$. Množenjem $52 \cdot 47$, slijedi

$$\begin{aligned} 52 \cdot 47 &\equiv 2 \cdot 2 \equiv -1 (\text{mod } 5) \\ 52 \cdot 47 &\equiv 4 \cdot -1 \equiv 4 (\text{mod } 8) \\ 52 \cdot 47 &\equiv -2 \cdot 2 \equiv -4 (\text{mod } 9) \\ 52 \cdot 47 &\equiv -3 \cdot 3 \equiv 2 (\text{mod } 11). \end{aligned}$$

Tada je umnožak modulo 3960 jednak izrazu

$$\begin{aligned} 52 \cdot 47 &\equiv (-1)e_5 + 4e_8 + (-4)e_9 + 2e_{11} \\ &\equiv 1584 - 1980 + 1760 - 2880 \equiv -1516 \equiv 2444 (\text{mod } 3960). \end{aligned}$$

Kako je $52 \cdot 47 < 3960$ i $52 \cdot 47 \equiv 2444 (\text{mod } 3960)$, moramo imati $52 \cdot 47 = 2444$.

Sada možemo kreirati tablicu svih produkata koji mogu proizaći iz ovakvih računa.

Jer je svaki broj modulo 5 kongruentan 0, 1, 2 ili njihovim suprotnim elementima, naša tablica treba jedino e_5 i $2e_5$. Slično, za modulo 8, 9 i 11 tablica treba sadržavati jedino $e_8, 2e_8, 3e_8$ i $4e_8$; $e_9, 2e_9, 3e_9$ i $4e_9$; te $e_{11}, 2e_{11}, 3e_{11}, 4e_{11}$ i $5e_{11}$, sve modulo 3960:

$\cdot$	e_5	e_8	e_9	e_{11}
1	-1584	-495	-440	-1440
2	792	-990	-880	1080
3		-1485	-1320	-360
4		-1980	-1760	-1800
5				720

Na primjer, $3e_9$ modulo 3960 je kongruentno -1320; dok je $4e_{11}$ modulo 3960 kongruentno -1800.

Primjer 2.2. U ovom primjeru koristiti ćemo tablicu kako bi izračunali $43 \cdot 47$.

Promotrimo da je

$$\begin{aligned} 43 \cdot 47 &\equiv 1 (\text{mod } 5) \\ &\equiv -3 (\text{mod } 8) \\ &\equiv -4 (\text{mod } 9) \\ &\equiv -3 (\text{mod } 11), \end{aligned}$$

pa slijedi

$$43 \cdot 47 \equiv 1 \cdot e_5 - 3 \cdot e_8 - 4 \cdot e_9 - 3 \cdot e_{11} (\text{mod } 3960).$$

Nakon kreiranja tablice slijedi

$$43 \cdot 47 \equiv -1584 + 1485 + 1760 + 360 \equiv 2021 (\text{mod } 3960).$$

Kako je $43 \cdot 47 < 3960$, $43 \cdot 47 = 2021$.

Ovim postupkom možemo riješiti problem starog Babilonskog računanja izradom glinene ploče te tablice koja sadrži svega 15 brojeva u sebi. S tom tablicom možemo pomnožiti bilo koja dva broja < 60 koristeći kongruencije s modulima 5, 8, 9 i 11 te koristeći zbrajanje.

3 Neke primjene u RSA kriptografiji

RSA dešifriranje. Ova primjena korištenja sustava kongruencija odnosi se na RSA kriptografiju detaljnije opisanu u literaturi [[4], str. 35-37.].

Slika 3: Vizualna asocijacija na RSA kriptografiju

Pretpostavimo da Marko planira izraditi RSA kriptosustav kako bi Ana mogla slati poruke Marku. Prisjetimo se da Marko radi redom: prvo pronađe dva veća prosta broja p i q te postavi $m = pq$, gdje će m predstavljati modul. Nakon toga Marko izabire eksponent za šifriranje e koji je relativno prost s $\varphi(m) = (p-1)(q-1)$, pronalazi eksponent za dešifriranje d koji zadovoljava $ed \equiv 1 (\text{mod } \varphi(m))$ te Ani šalje brojeve m i e. Kako bi Ani olakšao računanje, Marko bira e koji je što manji (kao npr. $e = 3$, ili $e = 7$).

Kako bi poslala poruku Marku, Ana računa $c = w^e$ modulo m te Marku javlja koliki je broj c. Da bi odredio w, Marko mora izračunati c^d modulo m. Ali c će biti broj koji će imati skoro jednako znamenaka kao i m. Stoga određivanje c^d modulo m zahtijeva malo truda.

Ali Marko ima malu prednost jer zna da je $m = pq$. Pa stoga može nastaviti kako slijedi:

(i) Izračunati $c_1 \equiv c^d (\text{mod } p)$ te $c_2 \equiv c^d (\text{mod } q)$ gdje su c_1 i c_2 nenegativni i najmanji mogući.

(ii) Odrediti y takav da je

$$y \equiv c_1 (\text{mod } p)$$
$$y \equiv c_2 (\text{mod } q).$$

Stoga

$$y \equiv c^d (\text{mod } p)$$
$$y \equiv c^d (\text{mod } q),$$

pa je

$$y \equiv c^d (\text{mod } pq)$$

i $pq = m$. Ako odaberemo $0 < y < m$, tada Anina početna riječ w zadovoljava

$$w \equiv c^d (\text{mod } m)$$

gdje je $0 < w < m$, pa moramo imati $y = w$.

Prije samog primjera prisjetimo se **Frematovog teorema:**

Teorem. 3.1. *Ako je p prost broj i a cijeli broj koji nije djeljiv s p, tada vrijedi*

$$a^{p-1} \equiv 1 (\text{mod } p).$$

U terminima kongruencija, Frematov teorem glasi:
Ako je p prost broj i $[a]_p$ element iz $\mathbb{Z}/p\mathbb{Z}$, tada je $[a]_p^{p-1} = [1]_p$.

U terminima djeljivosti imamo:
Ako je p prost broj i a relativno prost sa p, tada p dijeli $a^{p-1} - 1$.
Pogledajmo sada primjer:

Primjer 3.2. Kako bi ilustrirati kako ovo sve funkcionira, pretpostavimo da je modul $m = 187 = 11 \cdot 17$, eksponent šifriranja $e = 3$ i da Ana želi Marku poslati da je $w = 127$. Ana šifrira w da dobije $c = 127^3 \equiv 172 (\text{mod } 187)$ te šalje broj c Marku. Eksponent za dešifriranje d jednak je 107 pa Marko mora pronaći $c^d = 172^{107} (\text{mod } 187)$. Stoga računa

$$172^{107} (\text{mod } 11)$$

i

$$172^{107} (\text{mod } 17).$$

Sada je $172 \equiv 7 (\text{mod } 11)$, pa imamo $172^{107} \equiv 7^{107}$ i ovo je kongruentno 7^7, jer je $7^{10} \equiv 1 (\text{mod } 11)$, prema **Fermatovom teoremu** 3.1. Lako je provjeriti da je $7^7 \equiv 6 (\text{mod } 11)$.

Također, $172 \equiv 2 (\text{mod } 17)$ pa ponovno korištenjem Fermatovog teorema slijedi $172^{107} \equiv 2^{107} \equiv 2^{11} (\text{mod } 17)$. Ali $2^4 \equiv -1 (\text{mod } 17)$, pa je $2^{11} \equiv 2^3 = 8 (\text{mod } 17)$. Stoga $w \equiv c^d = 172^{107} (\text{mod } 187)$ zadovoljava

$$w \equiv 6 (\text{mod } 11)$$
$$w \equiv 8 (\text{mod } 17).$$

Možemo vidjeti da je $w = 127$, jer:

$$w = 8 + 17r = 6 + 11s,$$

pa je

$$17r \equiv -2 (\text{mod } 11),$$

odnosno

$$r \equiv -4 (\text{mod } 11)$$

pa imamo $w \equiv 8 + 17(-4) = -60 (\text{mod } 187)$. Stoga slijedi $0 < w < 187$, $w = -60 + 187 = 127$.

Procijenjeno je da dešifriranje korištenjem Kineskog teorema o ostacima ovakvim postupkom zahtijeva svega 1/4 ili 1/3 vremena potrebnog za računanje c^d modulo m direktno. Primijetimo da samo onaj koji zna točnu faktorizaciju modula m može koristiti ovu metodu. Stoga, jer je Marko dizajnirao postupak, bi eksponent koji je Ana koristila trebao biti malen kako bi minimizirao njen račun zbog toga jer ona nije u mogućnosti koristiti Kineski teorem o ostacima.

Zajednički eksponenti šifriranja. Pretpostavimo da Ana, financijska savjetnica, ima tri klijenta, Petra, Marka i Ivana te da svaki od njih ima svoj modul m_1, m_2 i m_3. Ana želi poslati povlaštene informacije o određenim dionicama svakome od njih. Kako bi joj bilo lakše, Ana uvijek koristi eksponent šifriranja $e = 3$. Ana tada šalje poruku w svakome od njih, kao što slijedi: Petru šalje $c_1 \equiv w^3 (\text{mod } m_1)$. Marku šalje $c_2 \equiv w^3 (\text{mod } m_2)$. I na kraju Ivanu šalje $c_3 \equiv w^3 (\text{mod } m_3)$. Marija (agentica koja provjerava sve neregularnosti prilikom trgovanja) presreće c_1, c_2, c_3 te zna m_1, m_2, m_3 i $e = 3$. Ipak ne zna w ili w^3 ali zna da je

$$\begin{aligned} w^3 &\equiv c_1 (\text{mod } m_1) \\ w^3 &\equiv c_2 (\text{mod } m_2) \\ w^3 &\equiv c_3 (\text{mod } m_3). \end{aligned}$$

Stoga Marija rješava sustav

$$\begin{aligned} t &\equiv c_1 (\text{mod } m_1) \\ t &\equiv c_2 (\text{mod } m_2) \\ t &\equiv c_3 (\text{mod } m_3) \end{aligned}$$

za neki broj $t < m_1 m_2 m_3$. Tada je

$$t \equiv w^3 (\text{mod } m_1 m_2 m_3).$$

Ali $w < m_i$ za $i = 1, 2, 3$, pa je $w^3 < m_1 m_2 m_3$. Stoga je $t = w^3$.

Nakon što pronađe t, Marija jednostavno može izvaditi treći korijen od t kako bi dobila poruku w.

Ovim primjerom je prikazano da se različitim ljudima ne bi trebala slati ista poruka sa istim malim eksponentom šifriranja.

4 Homomorfizmi i Eulerova φ-funkcija

U početku samo ponovimo osnovnu definiciju prstena. **Prsten** je neprazan skup R na kome su zadane dvije binarne operacije, *zbrajanje* $(a,b) \mapsto a+b$ i *množenje* $(a,b) \mapsto ab$, sa sljedećim svojstvima:

1. U odnosu na zbrajanje R je komutativna grupa; neutralni element označava se sa 0 i zove se *nula*.
2. U odnosu na množenje R je polugrupa (odnosno, množenje je asocijativno)
3. Množenje je i slijeva i zdesna distributivno u odnosu na zbrajanje, tj. vrijedi:

$$a(b+c) = ab + ac \text{ i } (a+b)c = ac + bc \text{ , } \forall a, b, c \in R.$$

Prisjetimo se da i ako su R, S prsteni, funkcija $f : R \to S$ je homomorfizam prstena ako

$$\begin{aligned} f(r_1 + r_2) &= f(r_1) + f(r_2) \\ f(r_1 r_2) &= f(r_1) f(r_2) \\ f(1) &= 1. \end{aligned}$$

Jezgra homomorfizma prstena $f : R \to S$ je skup

$$\text{Ker } f = \{r \in R | f(r) = 0\}.$$

Od prije znamo da je homomorfizam prstena $f : \mathbb{Z} \to S$ jedinstveno određen sa $f(1)$, pa je tada $f(n) = f(1) + \cdots + f(1)$ (n sumanada) u S ako je $n > 0$, i $f(-n) = -f(n)$. Nadalje, nije teško pokazati da svaki homomorfizam prstena $\mathbb{Z}/m\mathbb{Z}$ u S proizlazi iz homomorfizma prstena iz $\mathbb{Z}$ u S.

Propozicija 4.1. (Teorem o homomorfizmu). *Neka je S komutativan prsten te neka je $f : \mathbb{Z} \to S$ homomorfizam definiran s $f(n) = n \cdot 1_S$ za svaki n iz $\mathbb{Z}$. Ako f nije injekcija i $\text{Ker}(f) \supseteq m\mathbb{Z}$ za neki $m \neq 0$ u $\mathbb{Z}$, tada f inducira homomorfizam $\overline{f}$ iz $\mathbb{Z}/m\mathbb{Z}$ u $\{n \cdot 1_S | n \in \mathbb{Z}\}$, definiran sa $\overline{f}([a]_m) = f(a) = a \cdot 1_S$.*

Prikažimo još što je produkt dva prstena.

Produkt prstena. Neka su R, S skupovi. Produkt od R i S, zapisan kao $R \times S$, je skup svih uređenih parova oblika (r, s) gdje je $r \in R$ i $s \in S$.

Pretpostavimo da R i S nisu samo skupovi, nego i komutativni prsteni. Produkt $R \times S$ može se pretvoriti u komutativan prsten pomoću operacija s koordinatama, kao što slijedi:

$$\begin{aligned} (r, s) + (r', s') &= (r + r', s + s'), \\ (r, s) \cdot (r', s') &= (rr', ss'), \\ -(r, s) &= (-r, -s). \end{aligned}$$

Operacije na $R \times S$ definirane su korištenjem operacija od R i S u odgovarajućim koordinatama.

Nula i jedinica u prstenu su

$$\begin{aligned} 0 &= (0, 0), \\ 1 &= (1, 1). \end{aligned}$$

Ovako definiranim operacijama lagano je vidjeti da ako su R i S komutativni prsteni, tada je i $R \times S$ komutativan prsten.

Ako su R i S konačni prsteni te ako R ima m elemenata i S ima n elemenata, tada $R \times S$ ima mn elemenata.

Primjer 4.2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ima 6 elemenata. Pogledajmo sada tablicu:

·	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,2)	(0,0)	(0,2)	(0,1)	(0,0)	(0,2)	(0,1)
(1,0)	(0,0)	(1,0)	(0,0)	(1,0)	(0,0)	(1,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,0)	(0,1)	(0,2)
(1,2)	(0,0)	(1,2)	(0,1)	(1,0)	(0,2)	(1,1)

Očigledno (0,0) ima ulogu nul elementa dok (1,1) ima ulogu jedinice.

Teorem. 4.3. *Neka je $m = rs$ gdje su r i s relativno prosti brojevi veći od 1. Tada postoji izomorfizam prstena*

$$\psi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

takav da je $\psi([a]_m) = ([a]_r, [a]_s)$.

Na primjer, Teorem 4.3 govori da prsten $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ izgleda isto kao i prsten $\mathbb{Z}/6\mathbb{Z}$. Zapravo, ψ u ovom slučaju djeluje na sljedeći način: ovdje oznaka $[a]$ znači $[a]_6$ te (a, b) označava $([a]_2, [b]_3)$.

$$\begin{aligned}
\psi([0]) &= (0,0),\\
\psi([1]) &= (1,1),\\
\psi([2]) &= (2,2) = (0,2),\\
\psi([3]) &= (3,3) = (1,0),\\
\psi([4]) &= (4,4) = (0,1),\\
\psi([5]) &= (5,5) = (1,2).
\end{aligned}$$

Stoga dvije elementi [1] i [5] iz $\mathbb{Z}/6\mathbb{Z}$ preko izomorfizma ψ odgovaraju elementima (1,1) i (1,2) u $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; djelitelji nule [2], [3] i [4] iz $\mathbb{Z}/6\mathbb{Z}$ odgovaraju djeliteljima nule (0,2), (1,0) i (0,1) iz $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Dokaz teorema 4.3 poziva se na korištenje Kineskog teorema o ostacima.

Dokaz. Neka je $m = rs$ i neka je

$$\varphi : \mathbb{Z} \to r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

takav da je $\varphi(a) = ([a]_r, [a]_s)$. Ako je $a = mk$, tada je $([mk]_r, [mk]_s) = 0$ pa je stoga $m = rs$. Slijedi da je mk u jezgri od φ za svaki k.

Prema teoremu o homomorfizmu (propozicija 4.1) dobivamo inducirani homomorfizam

$$\psi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}/s\mathbb{Z}$$

takav da je $\psi([a]_m) = ([a]_r, [a]_s)$. Kako bi pokazali da je ψ injekcija, gledati ćemo jezgru od ψ, odnosno skup $[a]_m$ takav da je $\psi([a]_m) = 0$ u $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Sada je $\psi([a]_m) = 0$ ako i

samo ako $[a]_r = 0$ i $[a]_s = 0$ odnosno r dijeli a i s dijeli a. Ali kako su r i s relativno prosti, iz toga slijedi da m dijeli a, pa je $[a]_m = 0$. To znači da jezgra od ψ sadrži samo nul element od $\mathbb{Z}/m\mathbb{Z}$ koji označavamo $[0]_m$. Stoga slijedi da je ψ injekcija.

Kako bi pokazali da je ψ izomorfizam, preostaje pokazati u što se ψ preslika te ovdje imamo dvije mogućnosti. Jedna mogućnost koristi dok druga ne koristi Kineski teorem o ostacima.

Pokažimo prvu mogućnost koja koristi Kineski teorem o ostacima:

Neka je $([b]_r, [c]_s)$ proizvoljan element iz $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Kako bi pokazali da je $([b]_r, [c]_s) = ([a]_r, [a]_s) = \psi(a)$ za neki cijeli broj a mod m, moramo pronaći cijeli broj a takav da

$$a \equiv b (\text{mod } r),$$
$$a \equiv c (\text{mod } s).$$

Ali kako su r i s relativno prosti, uvijek je moguće pronaći cijeli broj a koji je rješenje para kongruencija. Stoga ψ je surjekcija. Obrnuto, ako možemo pokazati da je ψ surjekcija bez korištenja Kineskog teorema o ostacima, tada za r, s koji su relativno prosti, par kongruencija

$$x \equiv b (\text{mod } r),$$
$$x \equiv c (\text{mod } s),$$

ima rješenja za svaki b, c te tako Kineski teorem o ostacima sadrži skup od dvije kongruencije sa relativno prostim modulima.

Zašto je ψ surjekcija? Dokaz koji ne koristi Kineski teorem o ostacima je dokaz brojanjem. Znamo da je ψ injekcija iz skupa od m elemenata, odnosno skupa $\mathbb{Z}/m\mathbb{Z}$, u drugi skup od m elemenata, odnosno skup $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Funkcija koja je injekcija iz skupa R koji sadrži m elemenata u drugi skup S koji sadrži m elemenata mora biti surjekcija, jer ukoliko je ψ injekcija, tada $\psi(R)$ mora imati isti broj elemenata kao i R. Stoga $\psi(R)$ je podskup od m elemenata skupa S koji također sadrži m elemenata. Iz toga slijedi $\psi(R) = S$. □

U teoriji prstena, jednoj grani algebre, s U_m označavamo grupu svih elemenata prstena $\mathbb{Z}/m\mathbb{Z}$. Svi elementi U_m imaju svoj multiplikativni inverz, odnosno oni su invertibilni što u ovakvim prstenima znači da su to svi brojevi koji su relativno prosti s m.

Propozicija 4.4. *Ako je $m = rs$ gdje su r i s relativno prosti te gdje je*

$$\psi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

izomorfizam Teorema 4.3*, tada je ψ restrikcija izomorfizma iz grupe U_m u grupu $U_r \times U_s$.*

Dokaz. Primijetimo da je

$$U_r \times U_s = \{([b], [c]) \in \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} | (b, r) = 1 \text{ i } (c, s) = 1\}.$$

Ako je a element iz $\mathbb{Z}/m\mathbb{Z}$, tada je $(a, m) = 1$ pa je stoga $(a, r) = 1$ i $(a, s) = 1$. Sada je $\psi([a]) = ([a], [a])$, odnosno ψ preslikava element $[a]$ iz U_m u uređeni par $([a], [a])$ iz $U_r \times U_s$. Stoga ψ definira funkciju ψ_u iz U_m u $U_r \times U_s$.

Kako je ψ homomorfizam prstena, ψ_u je homomorfizam grupa.

ψ_u je injekcija jer je ψ injekcija.

Kako bi pokazali da je ψ_u surjekcija, pretpostavimo da je $([b], [c])$ u $U_r \times U_s$. Tada postoji neki $[a]$ iz U_m takav da je $\psi_u([a]) = ([a], [a]) = ([b], [c])$. Zato je $[a] = [b]$ u $\mathbb{Z}/r\mathbb{Z}$ i $[a] = [c]$ u $\mathbb{Z}/s\mathbb{Z}$. Ali tada je a relativno prost s r, i a relativno prost sa s pa slijedi da je a relativno prost sa $rs = m$. Jer je a element modulo m slijedi da je $[a]$ u U_m. Ovime smo pokazali da ψ_u preslikava elemente iz U_m u $U_r \times U_s$. □

Iz ovog teorema proizlazi formula za Eulerovu φ-funkciju:

Korolar 4.5. *Ako je $m = rs$, gdje su r i s relativno prosti, tada je $\varphi(m) = \varphi(r)\varphi(s)$.*

Dokaz. Znamo da $\varphi(m)$ predstavlja broj elemenata $\mathbb{Z}/m\mathbb{Z}$ i da je $\varphi(r)\varphi(s)$ broj parova $([b]_r, [c]_s)$ gdje je $[b]_r$ element iz $\mathbb{Z}/r\mathbb{Z}$ i $[c]_s$ je element iz $\mathbb{Z}/s\mathbb{Z}$. Stoga je $\psi_u : U_m \to U_r \times U_s$ izomorfizam, odnosno bijekcija te rezultat slijedi iz Propozicije 4.4. □

5 Sažetak

U ovom završnom radu prisjetili smo se definicije kongruencija te smo kroz razne primjere prošli kroz par realističnih primjena kongruencija. Nadalje, upoznali smo i sustave od dvije i više kongruencija u kojima smo promatrali specifične oblike kongruencija od kojih je jedan i Kineski teorem o ostacima. Osvrnuli smo se i na druge metode rješavanja sustava koje koriste posebne, dodatne sustave kao pomoć pri rješavanju početnog zadanog sustava kongruencija. Sve metode navedene u ovom završnom radu imaju podudaranja u dijelovima načina rješavanja te se većina ovih metoda koristila u starim civilizacijama kao promoć pri računanju zahtjevnijih i kompliciranijih zadataka i problema. Također, dotaknuli smo se i primjena kongruencija u kriptografiji te mogućnosti korištenja istih pri raznim šifriranjima i dešifriranjima podataka. Naposlijetku dotaknuli smo se i algebarskih prstena te homomorfizama prstena u kojima se pri dokazu određenih teorema i propozicija između ostaloga koristi i Kineski teorem o ostacima.

Ključne riječi: Teorija brojeva, kongruencije, prosti brojevi, relativno prosti brojevi, u parovima međusobno prosti brojevi, modul, sustav kongruencija, Euklidov algoritam, partikularno rješenje, opće rješenje, homogen sustav, Bezoutov identitet, Kineski teorem o ostacima, Babilonsko množenje, RSA kriptografija, prsteni, homomorfizmi, Eulerova ϕ-funkcija

6 Summary

In this paper, we recalled the definition of congruences and we presented a couple of examples which show few realistic applications of congruences. Furthermore, we introduced systems of two or more congruences in which we were looking at specific forms of congruences of which one method of solving given system is known as the Chinese Remainder Theorem. We also looked at other solution methods which use special additional systems which serve as help for solving the original given system of congruences. All solving methods that are named in this paper have some similarities in the way they solve certain systems of congruences and also, most of these methods were used in ancient civilizations as a help in solving more demanding and more complicated tasks and problems. Also, we mentioned few applications of congruences in cryptography and the possibility of using them in different encriptions and decriptions of data. In the end, we've talked about algebraic rings and ring homomorphisms which use Chinese Remained Theorem for proving certain theorems and propositions.

Keywords: Number theory, congruences, prime numbers, coprime numbers, pairwise coprime, modulo, systems of congruences, Euclidean algorithm, particular solution, general solution, homogeneous system, Bezout's identity, Chinese Remainder Theorem, Babylonian multiplication, RSA Cryptography, rings, homomorphism, Euler's ϕ-Function

Literatura

[1] Ivana Brkić, *Osnovni teorem aritmetike, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2014.* , dostupno na
https://www.mathos.unios.hr/~mdjumic/uploads/diplomski/BRK12.pdf

[2] Lindsay N. Childs, *A Concrete Introduction to Higher Algebra, 3rd edition, Springer, 2009.*

[3] Hrvoje Kraljević, *Algebra, Osijek, 2007.*, dostupno na
https://www.mathos.unios.hr/~dbrajkovic/Materijali/Algebra/algebra2007.pdf

[4] Ivan Matić, *Uvod u teoriju brojeva, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2013.* , dostupno na
https://www.mathos.unios.hr/images/homepages/mirela/UUTB/uvod_u_teoriju_brojeva.pdf

[5] *Were Chinese military formations more technically advanced than Roman military formations?, Quora*, dostupno na
https://www.quora.com/Were-Chinese-military-formations

[6] *An Exhibition That Gets to the (Square) Root of Sumerian Math, The New York Times*, dostupno na
https://www.nytimes.com/2010/11/23/science/23babylon.html

[7] *Is it still safe to use RSA Encryption?, The SSL Store*, dostupno na,
https://www.thesslstore.com/blog/is-it-still-safe-to-use-rsa-encryption/