Matematički fakultet
Univerzitet u Beogradu

KONGRUENCIJE CELIH BROJEVA

MASTER RAD

Student: Petra Šarčević
Mentor: Dr Tanja Stojadinović

Beograd,
2019.

„Matematika je kraljica nauka,
a teorija brojeva je kraljica matematike."
Karl Fridrih Gaus

Sadržaj

1 Uvod **3**

2 Deljivost celih brojeva **4**
2.1 Osnovne osobine 4
2.2 Najveći zajednički delilac 5
2.3 Euklidov algoritam 6
2.4 Linearna Diofantova jednačina 8

3 Kongruencije brojeva **11**
3.1 Definicija relacije kongruencije 11
3.2 Osobine relacije kongruencije 12
3.3 Zadaci 16

4 Ojlerova teorema **18**
4.1 Potpuni sistem ostataka 18
4.2 Redukovani sistem ostataka 19
4.3 Ojlerova funkcija 19
4.4 Ojlerova teorema 22
4.5 Mala Fermaova teorema i Vilsonova teorema 22
4.6 Zadaci 24

5 Kongruencije sa jednom nepoznatom **27**
5.1 Linearne kongruencije $ax \equiv b\ (mod\ m)$ 27
5.2 Metoda svodjenja na Diofantovu jednačinu 28
5.3 Metoda transformacije koeficijenata 30
5.4 Ojlerova metoda 31

6 Sistemi linearnih kongruencija **32**
6.1 Kineska teorema o ostacima 33

7 Zadaci **37**

8 Literatura **42**

1 Uvod

Teorija brojeva je oblast matematike koja je interesovala matematičare hiljadama godina. Kao prvo, javilo se pitanje reprezentacije brojeva. Različiti narodi su imali različite načine reprezentacije brojeva. Naš sistem reprezentacije brojeva je najrasprostranjeniji sistem za zapis brojeva i prvi put je korišćen u Indiji oko 600. godine. U istoriji su poznati razni drugi brojevni sistemi. Na primer Vavilonci su koristili sistem sa šezdeset različitih cifara, a Maje sa dvadeset. Danas se koristi i binarni sistem koji je svoju glavnu primenu našao u računarstvu.

Teorija brojeva se uglavnom bavi proučavanjem celih brojeva ($\mathbf{Z}$). Skup $\mathbf{Z}$ je zatvoren u odnosu na operacije sabiranja, oduzimanja i množenja, ali nije zatvoren u odnosu na operaciju deljenja i baš pitanje deljivosti leži u osnovi velikog dela teorije brojeva.

Ovaj master rad ima za cilj da predstavi veliki broj ideja koje se mogu koristiti u rešavanju složenijih zadataka, što narocito mogu iskoristiti ucenici koji se spremaju za srednjoškolska takmičenja. Rad, takodje, sadrži i osnovne pojmove i jednostavnije primere koji će pomoći učenicima da bolje razumeju osobine i deljivost brojeva. U osnovnim školama se koriste opšte prihvaćena tvrdjenja iz oblasti teorije brojeva, kao na primer ona da je broj deljiv sa 3 ukoliko je zbir cifara tog broja deljiv sa 3. To zna svako dete u osnovnoj školi, ali kada biste ga pitali zbog čega je to tako, ono verovatno ne bi znalo odgovor na to pitanje. Odgovor na takva pitanja daje teorija kongruencije, specifična algebra unutar teorije brojeva, koja je razvila poseban jezik za rešavanje problema o deljivosti brojeva.

Za podrsku i pomoć u realizaciji rada želim posebno da se zahvalim svojoj mentorki dr Tanji Stojadinović.

2 Deljivost celih brojeva

2.1 Osnovne osobine

Definicija 1 *Neka su a i b celi brojevi. Ako postoji ceo broj m takav da je $b = ma$, tada kažemo da je a* ***delilac*** *broja b i da je b* ***sadržalac*** *broja a. To zapisujemo: $a|b$ (čitamo: "a deli b").*

Primer 1 $3|12, 10|100, 5|35$.

Ako $a|b$, onda i $a|(-b), (-a)|b, (-a)|(-b)$. Zato se pri proučavanju deljivosti najčešće ograničavamo na nenegativne cele brojeve.

Definicija 2 *Broj a nazivamo* ***pravi delilac*** *broja b ako $a|b$ i $a \neq b$.*

Teorema 1 *Neka su a, b, c proizvoljni celi nenegativni brojevi. Tada važi:*

a) Ako $a|b$ i $b|c$, tada i $a|c$.

b) Ako $a|b$ i $b \neq 0$, tada je $0 < a \leq b$.

c) Ako $a|b$ i $a|c$, tada za proizvoljne brojeve k i l važi $a|(kb + lc)$.

d) Ako $a|b$ i $b|a$, tada je $a = b$.

Dokaz 1 *a) Ako $a|b$ i $b|c$ tada postoje celi brojevi k i l takvi da je $b = ka$ i $c = lb$. Tada je $c = kla$, a kako je kl ceo broj, sledi da i $a|c$.*

b) Ako $a|b$, tada postoji nenegativni ceo broj k takav da je $b = ka$. Kako je $b > 0$, tada su i k i a pozitivni brojevi, tj. $a, k \geq 1$. Sledi da je

$$b = ka \geq a \cdot 1 = a > 0.$$

c) Ako $a|b$ i $a|c$, tada postoje celi brojevi m i n takvi da je $b = ma$ i $c = na$. Dakle,

$$bk + cl = mak + nal = a(mk + nl).$$

Kako je $mk + nl$ ceo broj, sledi $a|(bk + cl)$.

d) Pretpostavimo da $a|b$ i $b|a$. Ako je $b = 0$, tada je i $a = 0$. Ako je $b > 0$ tada iz b) sledi da je $a = b$.

■

U teoriji brojeva važnu ulogu ima sledeća teorema jedinstvenosti o deljenju sa ostatkom.

Teorema 2 ***(Algoritam deljenja)*** *Neka su a i b nenegativni celi brojevi i $b \neq 0$. Tada su jednoznačno odredjeni nenegativni celi brojevi q i r, takvi da je $a = bq + r, 0 \leq r < b$.*

Dokaz 2 *Takav način predstavljanja broja a dobija se ako uzmemo da je bq najveći sadržalac broja b koji nije veći od a.*
Pretpostavimo da postoji još jedan način za predstavljanje broja a:

$$a = bq_1 + r_1, 0 \leq r_1 < b.$$

Tada je $0 = b(q-q_1)+(r-r_1)$, odakle sledi da $b|(r-r_1)$. Kako je $| r-r_1 | < b$, sledi da je $r - r_1 = 0$, tj. $r = r_1$. Kako je $b \neq 0$, sledi da je $q = q_1$.

■

Broj q se naziva ***količnik****, a broj r je* ***ostatak*** *pri deljenju broja a brojem b. Algoritam deljenja se koristi u klasifikaciji brojeva. Na primer za $b = 2$, ako je $r = 1$, tada je $a = 2q + 1$, pa kažemo da je a neparan broj, a ako je $r = 0$, a $a = 2q$, tada kažemo da je a paran broj. Slična klasifikacija se uspostavlja za $b = 3, 4, \ldots$*

Pozitivan ceo broj p veći od 1 je ***prost****, ako su mu jedini pozitivni delioci brojevi 1 i p. Za pozitivan ceo broj veći od 1 koji nije prost, kažemo da je* ***složen****.*

2.2 Najveći zajednički delilac

Definicija 3 *Neka su a i b nenegativni celi brojevi takvi da je bar jedan veći od 0. Za broj n kažemo da je* ***zajednički delilac*** *brojeva a i b, ako $n|a$ i $n|b$.*

Definicija 4 *Najveći pozitivan ceo broj koji je delilac i broja a i broja b naziva se* ***najveći zajednički delilac*** *brojeva a i b. Označavamo ga sa NZD(a,b) ili samo (a,b). On uvek postoji, sto se lako dokazuje.*

Primer 2 *NZD(8,16)=8, NZD(40,70)=10, NZD(8,11)=1.*

Da bismo dokazali da je $d = NZD(a, b)$, treba dokazati tačnost tvrdjenja:

(1) $d|a$ i $d|b$

(2) ako $n|a$ i $n|b$, tada $n|d$.

Definicija 5 *Celi brojevi a i b su* ***uzajamno prosti*** *ako i samo ako je $NZD(a, b) = 1$.*

Primer 3 *NZD(14,27)=1, pa su brojevi 14 i 27 uzajamno prosti brojevi.*

Teorema 3 *Najveći zajednički delilac dva broja, od kojih je bar jedan različit od 0, je jedinstven.*

Dokaz 3 *Ako je* $d = NZD(a, b)$ *i* $d_1 = NZD(a, b)$*, tada* $d|d_1$ *i* $d_1|d$ *pa sledi da je* $d = d_1$*.*

■

$NZD(a, a) = NZD(0, a) = a$, za $a > 0$.

2.3 Euklidov algoritam

Euklidov algoritam za odredjivanje najvećeg zajedničkog delioca, za dva prirodna broja, prvi put je opisan u Euklidovim *Elementima*, antičkom delu o matematici koje je nastalo oko 300. godine p.n.e. Veruje se da je algoritam bio poznat bar 200 godina ranije. U VII knjizi *Elemenata* iskazan je za prirodne brojeve, a u X knjizi je data njegova primena na duži.

Euklidov algoritam je prvi netrivijalni algoritam koji se koristi i danas. Vrlo je efikasan za računanje najvećeg zajedničkog delioca dva prirodna broja i ne zahteva njihovu prethodnu faktorizaciju.

Za različite pozitivne brojeve a i b, **Euklidov algoritam** zasniva se na algoritmu deljenja.

Neka su a i b pozitivni celi brojevi, $a > b$. Tada su jednoznačno odredjeni brojevi q_i i r_i, $1 \leq i \leq n + 1$, takvi da je

$$a = q_1 b + r_1, \quad 0 < r_1 < b,$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2,$$

$$\dots$$

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = q_{n+1} r_n + 0, \quad r_{n+1} = 0.$$

Niz $r_1, r_2, \dots, r_n$ je opadajući niz prirodnih brojeva manjih od b, što znači da se postupak Euklidovog algoritma mora završiti posle konačnog broja koraka.

Teorema 4 *NZD(a,b)=*r_n*, gde je* r_n *poslednji pozitivan ostatak dobijen primenom Euklidovog algoritma na prirodne brojeve* a *i* b*,* $a > b$*.*

Dokaz 4 *Dokažimo da važe sledeća dva tvrdjenja:*

1) $r_n|a$ *i* $r_n|b$

2) Ako $d|a$ *i* $d|b$*, tada* $d|r_n$

Iz Euklidovog algoritma dobijamo da $r_n|r_{n-1}$*. Na osnovu toga i poslednje jednakosti, zaključujemo da je* $r_n|r_{n-2}$*. Nastavljajući taj postupak, dobija se da* $r_n|r_{n-3}, r_n|r_{n-4}, \ldots, r_n|b$*, a onda iz prve jednakosti sledi da* $r_n|a$*. Dakle, uslov* 1) *je ispunjen.*
Neka je d prirodan broj takav da $d|a$ *i* $d|b$*. Tada iz prve jednakosti Euklidovog algoritma dobijamo da* $d|r_1$*, iz druge jednakosti dobijamo da* $d|r_2, \ldots$*, i konačno iz pretposlednje da* $d|r_n$*. Time je dokazano da važi i uslov* 2)*. Dakle,* r_n*=NZD(a,b).*

■

Posledica 1 *Za svaka dva cela broja a i b postoje celi brojevi m i n tako da je* $am + bn = d$*, gde je* $d = NZD(a, b)$*.*

Dokaz 5 *Iz poslednje jednakosti Euklidovog algoritma sledi da je*

$$d = r_n = r_{n-2} - q_n r_{n-1},$$

zatim

$$\begin{aligned} r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2}, \\ r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3}, \\ &\cdots \\ r_3 &= r_1 - q_3 r_2, \\ r_2 &= b - q_2 r_1, \\ r_1 &= a - q_1 b. \end{aligned}$$

Nakon što su svi ostaci zamenjeni, dobijena jednakost prikazuje d kao linearnu kombinaciju brojeva a i b, tj. postoje celi brojevi m i n tako da je $d = ma + bn$*.*

■

Zadatak 1 *Primenom Euklidovog algoritma odrediti NZD(85,15).*

Rešenje 1

$$\begin{aligned} 85 &= 5 \cdot 15 + 10 \\ 15 &= 1 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 + 0 \end{aligned}$$

Dakle, $NZD(85, 15) = 5$*.*

2.4 Linearna Diofantova jednačina

Definicija 6 *Ako su a, b, c celi brojevi i $ab \neq 0$, linearna jednačina oblika*

$$ax + by = c,$$

pri čemu su vrednosti x i y iz skupa celih brojeva, naziva se ***linearna Diofantova jednačina****.*

Definicija 7 *Polinomna jednačina po promenljivim x, y, z, ... sa celobrojnim koeficijentima naziva se* Diofantova jednačina *ako promenljive uzimaju vrednost iz skupa celih brojeva.*

Teorema 5 *Linearna Diofantova jednačina*

$$ax + by = c$$

ima rešenje ako i samo ako $d|c$, gde je d=NZD(a,b).

Dokaz 6 *Neka je d=NZD(a,b). Pretpostavimo da je (x_0, y_0) rešenje jednačine. Tada je*

$$ax_0 + by_0 = c.$$

Kako $d|a$ i $d|b$, onda $d|c$.
Obratno, pretpostavimo da $d|c$. Tada postoji ceo broj k takav da je $c = dk$. S druge strane d se može predstaviti kao linearna funkcija od a i b, tj. postoje celi brojevi x' i y' takvi da je

$$ax' + by' = d.$$

Množeći poslednju jednakost sa k, dobijamo

$$akx' + bky' = dk,$$

tj.

$$a(kx') + b(ky') = c.$$

Dakle, dobijeno je jedno rešenje $(x_0, y_0) = (kx', ky')$ Diofantove jednačine $ax + by = c$.

■

Primer 4 *Diofantova jednačina $36x+54y = 40$ nema rešenja, jer je NZD(36,54)=18, a 18 nije delilac broja 40.*

Primer 5 *Linearna Diofantova jednačina* $27x + 59y = 20$ *ima rešenje, jer je* $NZD(27, 59) = 1$, *a 1 je delilac broja 20. Koristeći Euklidov algoritam dobijamo:*

$$59 = 2 \cdot 27 + 5$$

$$27 = 5 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

Brojevi 27 i 59 su uzajamno prosti, pa broj 1 možemo predstaviti kao linearnu funkciju brojeva 27 i 59.

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (27 - 5 \cdot 5) = 5 - 2 \cdot 27 + 10 \cdot 5 = 11 \cdot 5 - 2 \cdot 27 =$$

$$= 11 \cdot (59 - 2 \cdot 27) - 2 \cdot 27 = 11 \cdot 59 - 22 \cdot 27 - 2 \cdot 27 = 11 \cdot 59 - 24 \cdot 27.$$

Konačno dobijamo da je $(-480) \cdot 27 + 220 \cdot 59 = 20$. *Dakle, jedno rešenje linearne Diofantove jednačine* $27x + 59y = 20$ *je* $(-480, 220)$. *Lako se proverava da su rešenja ove Diofantove jednačine*

$$x = -480 + 59t, \quad y = 220 - 27t,$$

gde je t ceo broj. Može se izabrati i manje (po apsolutnoj vrednosti) početno rešenje, ali se teško drugačije mogu odrediti osim intuicijom ili pogadjanjem. Na primer, za $t = 8$ *dobija se* $x_1 = -8$, $y_1 = 4$, *pa je opšte rešenje* $x = -8 + 59m$, $y = 4 - 27m$, $m \epsilon \boldsymbol{Z}$.

Teorema 6 *Ako je* $d = NZD(a, b)$, $d|c$ *i* (x_0, y_0) *jedno rešenje Diofantove jednačine* $ax + by = c$, *tada su sva rešenja* (x, y) *data formulama*

$$x = x_0 + \frac{b}{d}t \quad i \quad y = y_0 - \frac{a}{d}t$$

gde je t proizvoljan ceo broj.

Dokaz 7 *Ako je* (x_0, y_0) *rešenje Diofantove jednačine* $ax + by = c$, *tada zamenom dobijamo:*

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 = c.$$

Neka je (x,y) proizvoljno rešenje jednačine $ax + by = c$. *Tada dobijamo*

$$ax + by = ax_0 + by_0,$$

$$ax - ax_0 = by_0 - by,$$

$$a(x - x_0) = b(y_0 - y)$$
$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Kako je $d = NZD(a, b)$, *dobijamo da je* $NZD(\frac{a}{d}, \frac{b}{d}) = 1$. *Dakle,*

$$\frac{b}{d}|(x - x_0) \quad i \quad \frac{a}{d}|(y_0 - y)$$

odakle je

$$x - x_0 = \frac{b}{d}t \quad i \quad y_0 - y = \frac{a}{d}t,$$

gde je t *ceo broj. Konačno dobijamo da je*

$$x = x_0 + \frac{b}{d}t \quad i \quad y = y_0 - \frac{a}{d}t.$$

3 Kongruencije brojeva

Pojam kongruencije prvi je uveo Karl Fridrih Gaus (1777-1855), 1801.godine u svom delu *Disquisitiones Arithmeticae* (Aritmetička istraživanja). On je uveo i oznaku za kongruencije $\equiv$ koja se i danas koristi.

3.1 Definicija relacije kongruencije

Definicija 8 *Neka su dati a,b* $\in \boldsymbol{Z}$ *i* $m \in \boldsymbol{N}$ *tako da je* $m > 1$. *Tada kažemo da su brojevi a i b kongruentni po modulu m ako* $m|a-b$. *Pišemo:*

$$a \equiv b \,(mod\, m) \;\; ili \;\; a \equiv_m b. \tag{1}$$

U suprotnom, kažemo da a nije kongruentan b po modulu m i pišemo:

$$a \not\equiv b \,(mod\, m) \;\; ili \;\; a \not\equiv_m b. \tag{2}$$

Primer 6 *31*$\equiv$ *3 (mod 7) zato što* $7|31-3$.

Kako relacija $a \equiv b \,(mod\, m)$ označava da $m|a-b$, tada postoji $t \in \mathbf{Z}$ takav da je $a-b=tm$, odnosno

$$a = tm + b. \tag{3}$$

Na osnovu prethodnog izlaganja, relaciju kongruencije možemo definisati i na sledeći način:

Definicija 9 *Neka su dati celi brojevi a i b. Broj a je kongruentan broju b po modulu m ako postoji ceo broj t takav da je* $a = tm + b$.

Teorema 7 *Neka su dati a,b* $\in \boldsymbol{Z}$ *i* $m \in \boldsymbol{N}$ *gde je* $m > 1$. *Brojevi a i b imaju iste ostatke pri deljenju sa m ako i samo ako je* $a \equiv b \,(mod\, m)$.

Dokaz 8 *Ako je* $a \equiv b \,(mod\, m)$ *onda znamo da* $m|a-b$, *tada postoji* $t \in \boldsymbol{Z}$ *takav da je* $a = mt+b$. *Za b i m postoje jednoznačno odredjeni celi brojevi q i r (koje nazivamo* količnikom *i* euklidskim ostatkom *) takvi da je* $b = mq+r$, $0 \leq r < m$, *gde je r ostatak dobijen pri deljenju b sa m. Odatle sledi da je* $a = mt + b = mq + r + mt = m(q+t) + r$. *Dakle i broj a ima isti ostatak kao i broj b pri deljenju sa m.*

Obratno, neka su a i b brojevi koji pri deljenju sa m imaju isti ostatak tj $a = mt_1 + r$, $b = mt_2 + r$ *pri čemu je* $0 \leq r < m$. *Odavde sledi da je:*
$a - b = mt_1 + r - (mt_2 + r) = m(t_1 - t_2)$,
što znači da $m|a-b$ *tj.* $a \equiv b \,(mod\, m)$.

■

3.2 Osobine relacije kongruencije

Teorema 8 *Relacija "biti kongruentan po modulu" je relacija ekvivalencije u skupu celih brojeva.*

Dokaz 9 *Da bismo dokazali da je neka relacija, relacija ekvivalencije, moramo dokazati da je ona refleksivna,simetrična i tranzitivna.*

(1) $a \equiv a \,(mod\, m)$ *zato što* $m|a - a$ *tj.* $m|0$. *(refleksivnost)*

(2) Ako je $a \equiv b \,(mod\, m)$ *tada je* $a - b = km$. *Medjutim* $b - a = -km$ *pa onda* $m|b - a$ *tj.* $b \equiv a \,(mod\, m)$. *(simetričnost)*

(3) Ako je $a \equiv b \,(mod\, m)$ *i* $b \equiv c \,(mod\, m)$ *tada je* $a - b = km$ *i* $b - c = lm$. *Tada je* $a - c = km + b - (b - lm) = m(k - l)$, *odavde sledi da* $m|a - c$ *tj* $a \equiv c \,(mod\, m)$. *(tranzitivnost)*

■

Teorema 9 *Ako su a,b,c i* $m > 1$ *celi brojevi, tada ako je* $a \equiv b \,(mod\, m)$ *sledi* $ac \equiv bc \,(mod\, m)$, *a takodje i* $ac \equiv bc \,(mod\, mc)$.

Dokaz 10 *Kako je* $a \equiv b \,(mod\, m)$ *sledi da* $m|a - b$. *Odavde proizilazi da* $m|(a - b) \cdot c$ *tj. da* $m|ac - bc$ *što je i trebalo dokazati.*
Iz $m|a - b$ *takodje je i* $mc|ac - bc$ *pa sledi da je* $ac \equiv bc \,(mod\, mc)$.

■

Posledica 2 *Ako je* $a \equiv b \,(mod\, m)$ *tada je* $-a \equiv -b \,(mod\, m)$.

Teorema 10 *Relacija kongruencije po modulu je saglasna sa operacijama sabiranja, oduzimanja i množenja.*
Neka su a,b,c,d i $m > 1$ *celi brojevi. Ako je* $a \equiv b \,(mod\, m)$ *i* $c \equiv d \,(mod\, m)$, *tada vazi:*

(1) $a + c \equiv b + d \,(mod\, m)$

(2) $a - c \equiv b - d \,(mod\, m)$

(3) $ac \equiv bd \,(mod\, m)$

Dokaz 11 *(1) Kako znamo da je* $a \equiv b \,(mod\, m)$ *i* $c \equiv d \,(mod\, m)$*, odatle sledi da:*

$$a - b = km \;\; i \;\; c - d = lm,$$

pa je:

$$a - b + c - d = km + lm,$$

tj.

$$a + c - (b + d) = m(k + l),$$

odakle sledi da:

$$m|(a + c) - (b + d),$$

pa na kraju dobijamo da je

$$a + c \equiv b + d \,(mod\, m).$$

(2) Znamo da važi:

$$a - b = km \;\; i \;\; c - d = lm,$$

pa je:

$$a - b - c + d = km - lm,$$

odakle sledi:

$$a - c - (b - d) = m(k - l),$$

pa zato dobijamo da:

$$m|(a - c) - (b - d),$$

tj.

$$a - c \equiv b - d \,(mod\, m).$$

(3) Na osnovu teoreme 9 vazi:

$$ac \equiv bc \,(mod\, m) \;\; i \;\; bc \equiv bd \,(mod\, m).$$

Kako je relacija kongruencije tranzitivna, dobijamo da je:

$$ac \equiv bd \,(mod\, m).$$

■

Teorema 11 *Ako su a_1,a_2,...,a_n,b_1,b_2,...,b_n i $m > 1$ celi brojevi, tada iz relacije*

$$a_1 \equiv b_1, a_2 \equiv b_2, \ldots, a_n \equiv b_n \ (mod\ m)$$

sledi:

(1) $a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \ (mod\ m)$.

(2) $a_1 \cdot a_2 \cdot \ldots \cdot a_n \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_n \ (mod\ m)$.

Dokaz 12 *(1) U dokazu ove teoreme koristićemo teoremu 10, slučaj (1) i princip matematičke indukcije.*
Tvrdjenje je tačno za $n = 2$ jer na osnovu teoreme 10 i relacije $a_1 \equiv b_1$ i $a_2 \equiv b_2$ sledi da je $a_1 + a_2 \equiv b_1 + b_2 \ (mod\ m)$.
Neka je tvrdjenje tačno za $n - 1$, dokažimo da važi za n.
Pošto je tvrdjenje tačno za $n - 1$ sledi da iz relacije $a_1 \equiv b_1$,...,$a_{n-1} \equiv b_{n-1} \ (mod\ m)$ sledi $a_1 + \ldots + a_{n-1} \equiv b_1 + \ldots + b_{n-1} \ (mod\ m)$. Kako je i $a_n \equiv b_n \ (mod\ m)$ iz prethodne dve relacije na osnovu teoreme 10 sledi da je $a_1 + \ldots + a_n \equiv b_1 + \ldots + b_n \ (mod\ m)$.

(2) Tvrdjenje se takodje dokazuje matematičkom indukcijom i teoremom 10, slučaj (3).

■

Posledica 3 *Ako je $a \equiv b \ (mod\ m)$ tada vazi da je $a^n \equiv b^n \ (mod\ m)$, gde je n prirodan broj.*
Relacija $a^n \equiv b^n \ (mod\ m)$ važi i za $n = 0$, jer je $1 \equiv 1 \ (mod\ m)$.

Teorema 12 *Neka su a, b, c, d i $m > 1$ celi brojevi. Ako je $a \equiv b \ (mod\ m)$ i $d|m$, onda je $a \equiv b \ (mod\ d)$.*

Dokaz 13 *Znamo da je $a - b = km$, kako $d|m$, onda je $m = ld$, pa je $a - b = ldk$, odakle sledi da $d|a - b$ tj. $a \equiv b \ (mod\ d)$.*

■

Teorema 13 *Ako je $f(x) = c_0 + c_1x + \ldots + c_nx^n$ polinom sa celim koeficijentima $c_i, i = 0, 1, \ldots, n$, tada iz relacije $a \equiv b \ (mod\ m)$ sledi $f(a) \equiv f(b) \ (mod\ m)$.*

Dokaz 14 *Iz* $a \equiv b \,(mod\, m)$ *sledi* $a^i \equiv b^i \,(mod\, m)$ *i* $c_i a^i \equiv c_i b^i \,(mod\, m), i = 0, 1, \ldots, n.$
Prema teoremi 11 sledi

$$c_0 + c_1 a + \ldots + c_n a^n \equiv c_0 + c_1 b + \ldots + c_n b^n \,(mod\, m),$$

tj.

$$f(a) \equiv f(b) \,(mod\, m).$$

■

Teorema 14 *Ako je* $a \equiv b \,(mod\, m)$ *i ako* $c|a$ *i* $c|b$ *tada je*

$$\frac{a}{c} \equiv \frac{b}{c} \,(mod\, \frac{m}{d}),$$

gde je $d = NZD(m, c)$.

Dokaz 15 *Iz relacije* $a \equiv b \,(mod\, m), m|a - b$, *a isto tako i*

$$\frac{m}{d} | \frac{a-b}{d},$$

pa i

$$\frac{m}{d} | \frac{a-b}{c} \cdot \frac{c}{d}.$$

Medjutim, kako je $NZD(c, m) = d$ *tada je* $NZD(\frac{c}{d}, \frac{m}{d}) = 1$ *(uzajamno su prosti) pa prema tome:*

$$\frac{m}{d} | \frac{a-b}{c},$$

tj.

$$\frac{a}{c} \equiv \frac{b}{c} \,(mod\, \frac{m}{d}).$$

■

Ako je $NZD(c, m) = 1$ iz $a \equiv b \,(mod\, m)$ sledi $\frac{a}{c} \equiv \frac{b}{c} \,(mod\, m)$.
A u slučaju da $c|m$ tada je $NZD(c, m) = c$, pa je $\frac{a}{c} \equiv \frac{b}{c} \,(mod\, \frac{m}{c})$.

Primer 7 *Iz relacije* $42 \equiv 84 \,(mod\, 6)$ *"skraćivanjem" sa* 7 *dobijamo da je* $6 \equiv 12 \,(mod\, 6)$ *zato što je* $NZD(6, 7) = 1$. *Ako bi se izvršilo "skraćivanje" sa 14, dobili bismo* $3 \equiv 6 \,(mod\, 3)$, *zato što je* $NZD(6, 14) = 2$.

Teorema 15 *Ako je* $a \equiv b\,(mod\, m_1)$,$a \equiv b\,(mod\, m_2)$,. . . ,$a \equiv b\,(mod\, m_n)$, *tada je* $a \equiv b\,(mod\, M)$, *gde je* $M = NZS(m_1, \ldots, m_n)$.

Dokaz 16 *Neka je* $NZS(m_1, \ldots, m_n) = M$.
Iz uslova teoreme sledi da

$$m_1|a-b, \ldots, m_n|a-b,$$

pa i

$$M|a-b,$$

tj.

$$a \equiv b\,(mod\, M).$$

■

3.3 Zadaci

Zadatak 2 *Odrediti ostatak koji se dobija pri deljenju broja* 3^{100} *brojem 13.*

Rešenje 2 *Kako je*

$$3^3 = 27 \equiv 1\,(mod\, 13)$$

$$3^{100} = (3^3)^{33} \cdot 3 \equiv 1 \cdot 3\,(mod\, 13)$$

$$3^{100} \equiv 3\,(mod\, 13)$$

Pošto je $0 \leq 3 < 13$, *zaključujemo da je 3 ostatak pri deljenju broja* 3^{100} *brojem 13.*

Zadatak 3 *Dokazati da je broj* $2222^{5555} + 5555^{2222}$ *deljiv sa 3.*

Rešenje 3 *Znamo da je:*

$$2222 \equiv 2\,(mod\, 3)$$

$$2222^{5555} \equiv 2^{5555}\,(mod\, 3)$$

Kako je $2^2 = 4 \equiv 1\,(mod\, 3)$

$$2^{5555} = (2^2)^{2777} \cdot 2 \equiv 1 \cdot 2 = 2\,(mod\, 3)$$

Slično,

$$5555 \equiv 2 \ (mod\ 3)$$
$$5555^{2222} \equiv 2^{2222} \ (mod\ 3)$$
$$2^2 = 4 \equiv 1 \ (mod\ 3)$$
$$2^{2222} = (2^2)^{1111} \equiv 1 \ (mod\ 3)$$
$$2222^{5555} + 5555^{2222} \equiv 2 + 1 = 0 \ (mod\ 3)$$

Kako nema ostatka pri deljenju $2222^{5555} + 5555^{2222}$ *sa 3 sledi da je broj* $2222^{5555} + 5555^{2222}$ *deljiv sa 3.*

Zadatak 4 *Kojom cifrom se završava broj* 7^{2006}*?*

Rešenje 4 *Poslednja cifra nekog broja je u stvari ostatak pri deljenju tog broja brojem 10.*

$$7^2 = 49 \equiv -1 \ (mod\ 10)$$
$$7^{2006} = (7^2)^{1003} \equiv (-1)^{1003} = -1 \ (mod\ 10)$$

Kako je $9 \equiv -1 \ (mod\ 10)$*, a* $0 \leq 9 < 10$*, znači da je poslednja cifra broja* 7^{2006} *cifra 9.*

Zadatak 5 *Dokazati da je broj deljiv sa 9 ako je zbir njegovih cifara deljiv sa 9.*

Rešenje 5 *Uzmimo neki broj* m*, tako da on ima decimalni prikaz:*

$$m = c_n 10^n + c_{n-1} 10^{n-1} + \ldots + c_0.$$

Ako posmatramo polinom:

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0,$$

tada je $f(10) = m$*. Zbir cifara broja* m *je* $c_0 + c_1 + \ldots + c_n$*, tj* $f(1)$*.*
Kako je

$$10 \equiv 1 \ (mod\ 9),$$

sledi da je i

$$f(10) \equiv f(1) \ (mod\ 9).$$

Odakle sledi da su oba broja i $f(10)$ *i* $f(1)$ *istovremeno ili deljiva sa 9 ili nisu.*

4 Ojlerova teorema

4.1 Potpuni sistem ostataka

Definicija 10 *Skup od m celih brojeva u kome ne postoji ni jedan par brojeva kongruentnih po modulu m zove se* ***potpuni sistem ostataka po modulu m.***

Teorema 16 *(1) Skup {0,1,2,...,m-1} je potpuni sistem ostataka po modulu m.*

(2) Ako je m neparan broj, skup $\{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\}$ *je potpuni sistem ostataka po modulu m.*
Ako je m paran tada svaki od skupova $\{-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}\}$ *i* $\{-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1\}$ *predstavlja potpuni sistem ostataka po modulu m.*

(3) Ako je $\{x_1, x_2, \ldots, x_m\}$ *potpuni sistem ostataka i (a,m)=1, tada je i* $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ *potpuni sistem ostataka po modulu m, za svaki ceo broj b.*

Dokaz 17 *(3) Dovoljno je dokazati da skup* $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ *sadrži cele brojeve takve da ne postoji nijedan par brojeva kongruentnih po modulu m.*
Ako bi za neke i i j važilo

$$ax_i + b \equiv ax_j + b \ (mod\, m),$$

tada bi

$$m|(ax_i + b) - (ax_j + b),$$

tj.

$$m|a(x_i - x_j).$$

Kako su (a,m)=1, tada

$$m|x_i - x_j,$$

tj.

$$x_i \equiv x_j \ (mod\, m),$$

što je nemoguće zbog pretpostavke da je skup $\{x_1, x_2, \ldots, x_m\}$ *potpuni sistem ostataka po modulu m, pa ne postoji par brojeva kongruentnih po modulu m.*

■

Primer 8 *Skupovi {0,1,2,3,4,5} i {6,13,26,-3,46,35} su potpuni sistemi ostataka po modulu 6.*

4.2 Redukovani sistem ostataka

Definicija 11 *Skup svih elemenata potpunog sistema ostataka po modulu m koji su relativno prosti sa m naziva se* ***redukovani (svedeni) sistem ostataka po modulu m.***

Primer 9 *Skupovi $\{1,5\}$ i $\{13,35\}$ su svedeni sistemi ostataka po modulu 6.*

Leonard Ojler (1707-1789) je bio švajcarski matematičar i fizičar. Živeo je i radio u Berlinu i u Sankt Peterburgu.
Ojler je došao do velikih otkrića u različitim oblastima matematike kao što su matematička analiza, geometrija, teorija brojeva... Uveo je u upotrebu veliki broj termina koji se i danas koriste u matematici. Uveo je pojam funkcije i prvi je upotrebio oznaku $f(x)$ za funkciju f primenjenu na promenljivu x. Pored toga, uveo je i moderan zapis trigonometrijskih funkcija, grčko slovo Σ za označavanje sumiranja, slovo i za označavanje imaginarne jedinice i slovo e kao oznaku za osnovu prirodnog algoritma (danas poznatu i kao Ojlerov broj).

4.3 Ojlerova funkcija

Definicija 12 *Za svaki prirodan broj m, sa $\varphi(m)$ označavamo broj prirodnih brojeva, koji nisu veći od m, a relativno su prosti sa m. Funkcija $\varphi(m)$ se naziva* ***Ojlerova funkcija.***

Nekoliko prvih vrednosti funkcije $\varphi(m)$ dato je u sledećoj tabeli:

m	1	2	3	4	5	6	7	8	9	10	11
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10

Teorema 17 *Ako je p prost broj, tada je $\varphi(p) = p - 1$.*

Teorema 18 *Ako je $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ svedeni sistem ostataka po modulu m i (a,m)=1, tada je i $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ svedeni sistem ostataka po modulu m.*

Dokaz 18 *Tvrdjenje sledi iz činjenice da skup $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ sadrži $\varphi(m)$ celih brojeva, medju kojima nema kongruentnih brojeva po modulu m i svaki od njih je relativno prost sa m.*

■

Primer 10 *Neka je* $m = 8$, *a* $a = 5$.*Tada su* m *i* a *uzajamno prosti, pa je skup* $\{5 \cdot 0, 5 \cdot 1, \ldots, 5 \cdot 7\} = \{0, 5, 10, \ldots, 35\}$ *potpuni sistem ostataka po modulu 8, a skup* $\{5 \cdot 1, 5 \cdot 3, 5 \cdot 5, 5 \cdot 7\} = \{5, 15, 25, 35\}$ *je svedeni sistem ostataka po modulu 8.*

Teorema 19 *Ojlerova funkcija* φ *je multiplikativna. Odnosno, za (m,n)=1 važi*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Dokaz 19 *Neka su* m *i* n *uzajamno prosti brojevi tj. (m,n)=1. Broj će biti uzajamno prost sa proizvodom* mn, *ako i samo ako je uzajamno prost i sa brojem* m *i sa brojem* n.
Da bismo izračunali koliko medju brojevima 1,2,3,. . . ,mn ima uzajamno prostih i sa m *i sa* n, *zapisaćemo brojeve u vidu tabele:*

1	*2*	$\ldots$	k	$\ldots$	m
$m+1$	$m+2$	$\ldots$	$m+k$	$\ldots$	$2m$
$2m+1$	$2m+2$	$\ldots$	$2m+k$	$\ldots$	$3m$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$(n-1)m+1$	$(n-1)m+2$	$\ldots$	$(n-1)m+k$	$\ldots$	mn

Dokaz izvodimo tako što prvo prebrojimo koliko u tabeli ima uzajamno prostih sa m, *a zatim medju njima koliko ima uzajamno prostih sa* n.
Brojevi svake kolone iz gornje tabele pripadaju istoj klasi ekvivalencije u odnosu na relaciju $\equiv \pmod m$, *pa svi brojevi jedne kolone imaju isti najveći zajednički delilac sa* m, *tj. ako je jedan broj u nekoj koloni uzajamno prost sa* m, *onda su i svi ostali brojevi te kolone uzajamno prosti sa* m. *Takvih kolona, uzajamno prostih sa* m, *ima* $\varphi(m)$.
Posmatrajmo sada jednu kolonu brojeva uzajamno prostih sa m, *da bismo utvrdili koliko medju njima ima brojeva uzajamno prostih sa* n:

$$k, m+k, 2m+k, \ldots, (n-1)m+k.$$

Brojevi ove kolone su oblika $mx + k, x \epsilon \{0, 1, 2, \ldots, n-1\}$. *Medju njima ne postoje dva kongruentna broja po modulu* n, *jer ako bi postojala dva takva broja, za* $0 \leq s < t \leq n-1$, *tada je*

$$sm + k \equiv tm + k \pmod n,$$

pa je i

$$sm \equiv tm \pmod n.$$

Kako su (m,n)=1, dobijamo da je

$$s \equiv t \pmod n.$$

Kako s i t pripadaju potpunom sistemu ostataka {0,1,2,...,n-1} iz poslednje kongruencije sledi da jedino može da važi $s = t$.
Odavde sledi da n brojeva, koji pripadaju istoj koloni tabele, obrazuju potpun sistem ostataka po modulu n, a to znači da medju njima ima $\varphi(n)$ brojeva uzajamno prostih sa n.
Dakle, u svakoj od $\varphi(m)$ kolona koje sadrže brojeve uzajamno proste sa m, ima tačno $\varphi(n)$ brojeva uzajamno prostih sa n. Time je dokazano:

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

■

Primer 11 *Naći* $\varphi(40)$.
$\varphi(40) = \varphi(5 \cdot 8) = \varphi(5) \cdot \varphi(8) = 4 \cdot 4 = 16$

Ova formula za odredjivanje $\varphi(n)$ nije toliko pogodna ukoliko je n veliki broj. Zato ćemo formulisati jednu efektniju teoremu za odredjivanje $\varphi(n)$.

Teorema 20 *Ako je* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *kanonska faktorizacija broja n, onda je:*

$$\begin{aligned} \varphi(n) &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_k}) && (4) \\ &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \ldots (p_k - 1) && (5) \end{aligned}$$

Dokaz 20 *Neka je* $n = p^\alpha$, *za neki prost broj p i neki prirodan broj* α. *Medju prirodnim brojevima od 1 do* p^α *ima* $p^{\alpha-1}$ *brojeva koji nisu uzajamno prosti sa* p^α, *to su brojevi koji su deljivi sa p:* $p, 2p, \ldots, p^2, \ldots, p^\alpha$.
Dakle, medju prirodnim brojevima od 1 do p^α *ima* $p^\alpha - p^{\alpha-1}$ *brojeva koji su uzajamno prosti sa* p^α, *tj.*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p}).$$

Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *kanonska faktorizacija broja n, primenom prethodne teoreme (primenjene više puta) imamo:*

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) && (6) \\ &= p^{\alpha_1}(1 - \frac{1}{p_1})p^{\alpha_2}(1 - \frac{1}{p_2}) \cdot \ldots \cdot p^{\alpha_k}(1 - \frac{1}{p_k}) && (7) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_k}). && (8) \end{aligned}$$

■

Primer 12 *Naći* $\varphi(120)$

$$\varphi(120) = \varphi(2^3 \cdot 3^1 \cdot 5^1) = 2^2 \cdot 3^0 \cdot 5^0 \cdot (2-1)(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32.$$

4.4 Ojlerova teorema

Teorema 21 *(**Ojler**) Ako su a i m uzajamno prosti brojevi onda je*

$$a^{\varphi(m)} \equiv 1 \,(mod\, m).$$

Dokaz 21 *Neka je* $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ *svedeni sistem ostataka po modulu m. Tada je i* $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ *svedeni sistem ostataka po modulu m, jer je (a,m)=1. Prema tome, za svako* x_i *postoji tačno jedan* ax_j *takav da je* $ax_j \equiv x_i \,(mod\, m)$*, pa je*

$$(ax_1)(ax_2)\cdots ax_{\varphi(m)} \equiv x_1x_2\cdots x_{\varphi(m)} \,(mod\, m),$$

odnosno

$$a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \equiv x_1x_2\cdots x_{\varphi(m)} \,(mod\, m).$$

Kako je svaki od $x_1, x_2, \ldots, x_{\varphi(m)}$ *uzajamno prost sa m, tako je i* $(x_1x_2\cdots x_{\varphi(m)}, m) = 1$ *pa imamo da je*

$$a^{\varphi(m)} \equiv 1 \,(mod\, m).$$

■

4.5 Mala Fermaova teorema i Vilsonova teorema

Neposredna posledica Ojlerove teoreme je Fermaova teorema, poznatija kao Mala Fermaova teorema.

Teorema 22 *(**Mala Fermaova teorema**) Ako je p prost broj i* $p \nmid a$*, onda je*

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

Dokaz 22 *Ako p ne deli a, onda su p i a uzajamno prosti. Kako za svaki prost broj p važi* $\varphi(p) = p - 1$*, Mala Fermaova teorema je specijalan slučaj Ojlerove teoreme.*

■

Posledica 4 *(Posledica Male Fermaove teoreme) Ako je p prost broj i* $a \in N$*, tada je* $a^p \equiv a \,(mod\, p)$.

Dokaz 23 *Moguća su dva slučaja:*

(1) $p \nmid a$
Tada je $a^{p-1} \equiv 1 \,(mod\, p)$*, a nakon množenja sa a, dobijamo* $a^p \equiv a \,(mod\, p)$.

(2) $p \mid a$
Tada je $a^p \equiv 0 \,(mod\, p)$ *i* $a \equiv 0 \,(mod\, p)$, *sledi* $a^p \equiv a \,(mod\, p)$.

■

Teorema 23 *(**Vilsonova teorema**) Ako je p prost broj, tada važi:*

$$(p-1)! \equiv -1 \,(mod\, p).$$

Dokaz 24 *Razlikujemo dva slučaja:*

(1) Tvrdjenje vazi za $p = 2$ *i* $p = 3$.

- *Neka je* $p = 2$, *tada je* $(p-1)! = (2-1)! = 1! = 1 \equiv -1 \,(mod\, 2)$.
- *Neka je* $p = 3$, *tada je* $(p-1)! = 2! = 2 \equiv -1 \,(mod\, 3)$.

(2) Neka je p prost broj i $p > 3$.
Da bismo dokazali teoremu, dovoljno je dokazati da za svaki broj x takav da je $2 \leq x \leq p-2$, *postoji tačno jedan broj y takav da je*

$$x \cdot y \equiv 1 \,(mod\, p), \quad 2 \leq y \leq p-2, x \neq y.$$

Ako $x \in \{2, \ldots, p-2\}$, *pošto je (x,p)=1, skup* $\{0, x, 2x, \ldots, (p-1)x\}$ *obrazuje potpun sistem ostataka po modulu p i tačno jedan element ovog skupa (koji je različit od nule) je kongruentan sa 1 po modulu p.*
Ako bi bilo $y = 1$, *onda bismo imali i da je* $x \equiv 1 \,(mod\, p)$, *što je nemoguće.*
Slično se dokazuje da ne može biti ni $y = p-1$.
A ako bi bilo $x = y$, *imali bismo da je* $x^2 \equiv 1 \,(mod\, p)$, *tj. da* $p|x-1$ *ili* $p|x+1$, *odnosno da je* $x \equiv 1 \,(mod\, p)$ *ili* $x \equiv -1 \,(mod\, p)$, *što je nemoguće.*

■

Napomenimo da važi i obrnuto tvrdjenje Vilsonove teoreme.

Teorema 24 *(**Obrat Vilsonove teoreme**)Ako je* $(p-1)! \equiv -1 \,(mod\, p)$, *tada je p prost broj.*

Dokaz 25 *Pretpostavimo suprotno, da je p složen broj. To bi značilo da postoji prost broj* $q < p, q|p$, *pa bi važilo da* $q|(p-1)!$, *tj.* $q \nmid (p-1)! + 1$ *pa samim tim* $p \nmid (p-1)! + 1$. *Kontradikcija.*

■

4.6 Zadaci

Zadatak 6 *Naći ostatak pri deljenju* 3^{10^5} *sa 35.*

Rešenje 6 *Kako je (3,35)=1, na osnovu Ojlerove teoreme, sledi*

$$3^{\varphi(35)} \equiv 1 \ (mod\ 35)$$

$$\varphi(35) = \varphi(7) \cdot \varphi(5) = 6 \cdot 4 = 24$$

$$10^5 = 10000 = 24 \cdot 4166 + 16,$$

odavde sledi

$$3^{10^5} \equiv (3^{24})^{4166} \cdot 3^{16} \ (mod\ 35).$$

Kako je

$$3^{24} \equiv 1 \ (mod\ 35) \Rightarrow 3^{10^5} \equiv 3^{16} \ (mod\ 35)$$

$$3^4 \equiv 11 \ (mod\ 35) \Rightarrow 3^{16} \equiv 11^4 \ (mod\ 35)$$

$$11^2 \equiv 16 \ (mod\ 35) \Rightarrow 11^4 \equiv 16^2 \ (mod\ 35)$$

$$16^2 \equiv 11 \ (mod\ 35).$$

Dakle, ostatak je 11.

Zadatak 7 *Naći ostatak pri deljenju* 317^{259} *sa 15.*

Rešenje 7

$$317 \equiv 2 \ (mod\ 15) \Rightarrow 317^{259} \equiv 2^{259} \ (mod\ 15)$$

Kako su (2,15)=1, na osnovu Ojlerove teoreme sledi

$$2^{\varphi(15)} \equiv 1 \ (mod\ 15)$$

$$\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$$

pa je

$$2^8 \equiv 1 \ (mod\ 15)$$

$$259 = 8 \cdot 32 + 3 \Rightarrow 2^{259} \equiv (2^8)^{32} \cdot 2^3 \ (mod\ 15)$$

Odavde sledi,

$$2^{259} \equiv 2^3 \ (mod\ 15).$$

Dakle, ostatak je 2^3*, tj. 8.*

Zadatak 8 *Odrediti ostatak pri deljenju broja* 8^{453} *sa 5.*

Rešenje 8 *Kako su (8,5)=1, tada prema Maloj Fermaovoj teoremi sledi*

$$8^{5-1} \equiv 1 \ (mod\ 5),$$

tj.

$$8^4 \equiv 1 \ (mod\ 5),$$

$$453 = 4 \cdot 113 + 1 \Rightarrow 8^{453} = (8^4)^{113} \cdot 8 \ (mod\ 5),$$

pa je onda

$$8^{453} \equiv 8 \ (mod\ 5),$$

a

$$8 \equiv 3 \ (mod\ 5).$$

Dakle, ostatak je 3.

Zadatak 9 *Dokazati da* $13 \mid 2^{70} + 3^{70}$.

Rešenje 9 *Kako su (2,13)=1, po Maloj Fermaovoj teoremi* $2^{12} \equiv 1 \ (mod\ 13)$*,*

$$70 = 12 \cdot 5 + 10$$

$$2^{70} \equiv (2^{12})^5 \cdot 2^{10} \ (mod\ 13),$$

pa je

$$2^{70} \equiv 2^{10} \ (mod\ 13)$$

$$2^{10} = 1024,$$

$$1024 \equiv -3 \ (mod\ 13),$$

odakle sledi da je

$$2^{70} \equiv -3 \ (mod\ 13)$$

Kako je (3,13)=1, po Maloj Fermaovoj teoremi je $3^{12} \equiv 1 \ (mod\ 13)$

$$70 = 12 \cdot 5 + 10,$$

pa je

$$3^{70} \equiv (3^{12})^5 \cdot 3^{10} \ (mod\ 13),$$

sledi

$$3^{70} \equiv 3^{10} \ (mod\ 13),$$
$$3^3 \equiv 1 \ (mod\ 13),$$
$$3^{10} \equiv (3^3)^3 \cdot 3 \ (mod\ 13),$$

tj.

$$3^{10} \equiv 3 \ (mod\ 13),$$
$$2^{70} + 3^{70} \equiv 0 \ (mod\ 13).$$

Dakle, $13|2^{70} + 3^{70}$.

Zadatak 10 *Dokazati da za svaki prost broj p važi* $(p-2)! \equiv 1 \ (mod\ p)$.

Rešenje 10 *Prema Vilsonovoj teoremi važi*

$$(p-1)! + 1 \equiv 0 \ (mod\ p),$$
$$(p-2)! \cdot (p-1) + 1 \equiv 0 \ (mod\ p),$$
$$(p-2)! \cdot p - (p-2)! + 1 \equiv 0 \ (mod\ p),$$
$$p(p-2)! - ((p-2)! - 1) \equiv 0 \ (mod\ p),$$
$$(p-2)! - 1 \equiv 0 \ (mod\ p).$$

Odakle sledi,

$$(p-2)! \equiv 1 \ (mod\ p).$$

Zadatak 11 *Neka su p i q prosti brojevi,* $p \neq q$. *Dokazati da je*

$$q \cdot 2q \cdots (p-1)q \equiv -1 \ (mod\ p).$$

Rešenje 11 *Kako su (p,q)=1, prema Maloj Fermaovoj teoremi sledi:*

$$q^{p-1} \equiv 1 \ (mod\ p),$$

a prema Vilsonovoj teoremi sledi

$$(p-1)! \equiv -1 \ (mod\ p).$$

Množenjem ovih kongruencija dobijamo

$$q^{p-1}(p-1)! \equiv -1 \ (mod\ p),$$

tj.

$$q \cdot 2q \cdots (p-1)q \equiv -1 \ (mod\ p).$$

5 Kongruencije sa jednom nepoznatom

5.1 Linearne kongruencije $ax \equiv b\,(mod\,m)$

Rešenje kongruencije $ax \equiv b\,(mod\,m)$ jeste svaki ceo broj x koji je zadovoljava. Ako je x_1 neko rešenje kongruencije $ax \equiv b\,(mod\,m)$ i $x_2 \equiv x_1\,(mod\,m)$, onda je i x_2 takodje rešenje te kongruencije.

Za dva rešenja x i x' kažemo da su *ekvivalentna* ako je $x \equiv x'\,(mod\,m)$. Pod brojem rešenja kongruencije podrazumevamo broj neekvivalentnih rešenja.

Teorema 25 *Neka su a i m prirodni brojevi i neka je b ceo broj. Kongruencija*

$$ax \equiv b\,(mod\,m)$$

ima rešenje ako i samo ako $d|b$, gde je $d = NZD(a, m)$. Ako je ovaj uslov ispunjen, onda kongruencija $ax \equiv b\,(mod\,m)$ ima tačno d rešenja nekongruentnih po modulu m i to:

$$x_0 + \frac{m}{d}t, \quad t = 0, 1, \ldots, d-1,$$

gde je x_0 jedinstveno rešenje kongruencije

$$\frac{a}{d}x \equiv \frac{b}{d}\,(mod\,\frac{m}{d}).$$

Ukoliko $d \nmid b$, kongruencija $ax \equiv b\,(mod\,m)$ nema rešenja.

Teorema 25 je dokazana već u sledećem paragrafu.

Posledica 5 *Ukoliko su a i m uzajamno prosti brojevi, kongruencija $ax \equiv b\,(mod\,m)$ ima jedinstveno rešenje po modulu m.*

Primer 13 *Kongruencija*

$$4x \equiv 25\,(mod\,10)$$

nema rešenja, jer je NZD(4,10)=2, a broj 2 nije delilac broja 25.

U radu ćemo opisati tri metode koje koristimo pri rešavanju linearnih kongruencija sa jednom nepoznatom i to:

(1) Metoda svodjenja na Diofantovu jednačinu

(2) Metoda transformacije koeficijenata

(3) Ojlerova metoda

5.2 (1) Metoda svodjenja na Diofantovu jednačinu

Iz kongruencije $ax \equiv b\ (mod\ m)$ sledi da $m|(ax-b)$, pa postoji $y\epsilon\mathbf{Z}$ takvo da je

$$my = ax - b,$$

tj.

$$ax - my = b.$$

Ovo je linearna Diofantova jednačina koja ima rešenje ako i samo ako $d|b$, $d = NZD(a, m)$.
Neka $d|b$ i neka su $(x_0,\ y_0)$ neka rešenja Diofantove jednačine $ax - my = b$. Tada $(x_0,\ y_0)$ mora zadovoljavati ovu jednačinu, pa važi:

$$ax_0 - my_0 = b.$$

Ako od jednačine $ax-my = b$ oduzmemo jednačinu $ax_0-my_0 = b$ dobijamo:

$$a(x - x_0) - m(y - y_0) = 0,$$

odnosno

$$y - y_0 = \frac{a(x - x_0)}{m}$$

Kako je $d = NZD(a, m)$, možemo brojilac i imenilac desne strane jednakosti podeliti sa d. Tada ćemo dobiti:

$$y - y_0 = \frac{\frac{a}{d}(x - x_0)}{\frac{m}{d}}.$$

Kako je $y-y_0$ ceo broj, sledi da i desna strana jednakosti mora biti ceo broj. Pošto je $NZD(\frac{a}{d}, \frac{m}{d}) = 1$, važi:

$$\frac{x - x_0}{\frac{m}{d}} = t$$

$$x - x_0 = \frac{m}{d}t$$

pa dobijamo da je

$$x = x_0 + \frac{m}{d}t, \quad t\epsilon\mathbf{Z}.$$

Rešenja ima beskonačno, medjutim dokažimo da ih ima d nekongruentnih. Ako su dva rešenja kongruentna po modulu m, tada je

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2\ (mod\ m),$$

sledi

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \ (mod\, m).$$

Kako je $d = NZD(a, m)$, sledi da je $NZD(m, \frac{m}{d}) = \frac{m}{d}$ pa je

$$t_1 \equiv t_2 \ (mod\ \frac{m}{\frac{m}{d}}),$$

tj.

$$t_1 \equiv t_2 \ (mod\, d).$$

Dakle, skup nekongruentnih rešenja dobijamo za $t\epsilon\{0, 1, 2, 3, \ldots, d-1\}$, tj. sva nekongruentna rešenja su oblika

$$x = x_0 + \frac{m}{d}t, \quad t\epsilon\{0, 1, 2, 3, \ldots, d-1\}$$

i ima ih tačno d.

Zadatak 12 *Metodom svodjenja na Diofantovu jednačinu rešiti kongruencije:*

a) $3x \equiv 5 \ (mod\, 7)$

b) $2x \equiv 6 \ (mod\, 10)$

Rešenje 12 *a) Kako je NZD(3,7)=1, a* $1|5$*, ova kongruencija ima jedinstveno rešenje.*
Iz date kongruencije sledi da $7|3x-5$*, tj. postoji* $y\epsilon\boldsymbol{Z}$ *takvo da je*

$$\frac{3x-5}{7} = y,$$

odakle sledi

$$3x - 7y = 5.$$

Očito je jedno rešenje ove Diofantove jednačine $(x_0,y_0)=(4,1)$*, pa sledi*

$$3x_0 - 7y_0 = 5.$$

Oduzimajući jednačine dobijamo:

$$3(x - x_0) - 7(y - y_0) = 0,$$

pa sledi

$$y - y_0 = \frac{3(x - x_0)}{7}.$$

Kako je $y - y_0$ *ceo broj, onda mora i* $\frac{3(x-x_0)}{7}$ *biti ceo broj, a kako su 3 i 7 uzajamno prosti brojevi, sledi da* $x - x_0$ *mora biti deljiv sa 7, tj.*

$$x - x_0 = 7t, \quad t\epsilon \boldsymbol{Z}$$

Zaključujemo da je rešenje polazne kongruencije

$$x = 7t + 4, \quad t\epsilon \boldsymbol{Z}$$

tj.

$$x \equiv 4 \ (mod\ 7).$$

b) NZD(2,10)=2, pa kako $2|6$*, polazna kongruencija ima dva rešenja. Analogno prethodnom primeru dobijamo Diofantovu jednačinu*

$$2x - 10y = 6,$$

čije je jedno rešenje (8,1), pa je rešenje kongruencije

$$x = 8 + \frac{-10}{2}t = 8 - 5t, \quad t\epsilon\{0, 1\}$$

Tako smo dobili da je rešenje date kongruencije

$$x \equiv 8 \ (mod\ 5) \quad i \quad x \equiv 3 \ (mod\ 5).$$

5.3 (2) Metoda transformacije koeficijenata

Koristeći činjenicu da je relacija "biti kongruentan" jedna relacija ekvivalencije, mi zadatoj kongruenciji dodajemo (oduzimamo) neku prikladno odabranu istinitu kongruenciju kako bismo pojednostavili postupak nalaženja rešenja.

Zadatak 13 *Metodom transformacije koeficijenata rešiti kongruencije:*

a) $7x \equiv 3 \ (mod\ 11)$

b) $17x \equiv 25 \ (mod\ 28)$

Rešenje 13 *a) Kako je NZD(7,11)=1 i kako* $1|3$*, naša kongruencija ima jedinstveno rešenje. Dodamo li zadatoj kongruenciji kongruenciju* $0 \equiv 11 \ (mod\ 11)$*, koja je očigledno istinita, dobijamo kongruenciju* $7x \equiv 14 \ (mod\ 11)$*. Skratimo li ovu kongruenciju sa 7 (što je dozvoljeno) dobijamo*

$$x \equiv 2 \ (mod\ 11),$$

što i predstavlja rešenje polazne kongruencije.
b) Kako je NZD(17,28)=1 i ova kongruencija ima jedinstveno rešenje. Dodamo li joj kongruenciju $28x \equiv 0\ (mod\ 28)$ *dobijamo kongruenciju* $45x \equiv 25\ (mod\ 28)$ *koju možemo skratiti sa 5. Nakon skraćivanja dobijamo kongruenciju* $9x \equiv 5\ (mod\ 28)$ *kojoj dodajemo kongruenciju* $0 \equiv -140\ (mod\ 28)$ *i dobijamo* $9x \equiv -135\ (mod\ 28)$. *Nakon skraćivanja sa 9 dobijamo kongruenciju* $x \equiv -15\ (mod\ 28)$, *tj.*

$$x \equiv 13\ (mod\ 28).$$

5.4 (3) Ojlerova metoda

Za rešavanje linearne kongruencije Ojlerovom metodom potrebna nam je Ojlerova teorema, koja je opisana u četvrtom poglavlju.
Prema Ojlerovoj teoremi imamo da je $a^{\varphi(m)} \equiv 1\ (mod\ m)$, a zbog refleksivnosti relacije kongruencije važi $b \equiv b\ (mod\ m)$. Ako pomnožimo ove dve kongruencije, dobijamo da je

$$a^{\varphi(m)} \cdot b \equiv b\ (mod\ m),$$

tj.

$$a \cdot (a^{\varphi(m)-1} \cdot b) \equiv b\ (mod\ m).$$

Uporedimo li ovu kongruenciju sa kongruencijom $ax \equiv b\ (mod\ m)$, čije rešenje i tražimo, vidimo da je njeno rešenje

$$x \equiv a^{\varphi(m)-1} \cdot b\ (mod\ m).$$

Zadatak 14 *Ojlerovom metodom rešiti kongruencije:*

a) $5x \equiv 4\ (mod\ 12)$

b) $3x \equiv 5\ (mod\ 10)$

Rešenje 14 *a) Kako je NZD(5,12)=1, a* $1|4$*, naša kongruencija ima jedinstveno rešenje.*
Ako iskoristimo Ojlerovu teoremu i opisanu metodu, dobijamo da je rešenje polazne kongruencije

$$\begin{aligned} x &\equiv 5^{\varphi(12)-1} \cdot 4\ (mod\ 12) && (9)\\ &\equiv 5^{4-1} \cdot 4\ (mod\ 12) && (10)\\ &\equiv 5^3 \cdot 4\ (mod\ 12) && (11)\\ &\equiv 5 \cdot 4\ (mod\ 12) && (12)\\ &\equiv 20\ (mod\ 12) && (13)\\ &\equiv 8\ (mod\ 12) && (14)\\ & && (15) \end{aligned}$$

Dakle, rešenje početne kongruencije je $x \equiv 8 \ (mod\ 12)$.
b) NZD(3,10)=1, a 1 je delilac broja 5, pa naša početna kongruencija ima jedinstveno rešenje.

$$\begin{aligned} x &\equiv 3^{\varphi(10)-1} \cdot 5 \ (mod\ 10) && (16)\\ &\equiv 3^{4-1} \cdot 5 \ (mod\ 10) && (17)\\ &\equiv 3^3 \cdot 5 \ (mod\ 10) && (18)\\ &\equiv 3 \cdot 5 \ (mod\ 10) && (19)\\ &\equiv 15 \ (mod\ 10) && (20)\\ &\equiv 5 \ (mod\ 10) && (21)\\ & && (22) \end{aligned}$$

Rešenje početne kongruencije je $x \equiv 5 \ (mod\ 10)$.

6 Sistemi linearnih kongruencija

Ukoliko imamo sistem od dve linearne kongruencije, jedna od metoda za rešavanje sistema je da se reši jedna od kongruencija sistema, a zatim se odaberu ona rešenja koja zadovoljavaju drugu kongruenciju.

Primer 14 *Rešiti sistem kongruencija*

$$2x \equiv 3 \ (mod\ 7)$$

$$4x \equiv 5 \ (mod\ 11).$$

Rešenje 15 *Kako je* $2x \equiv 3 \ (mod\ 7)$*, tada* $7|(2x-3)$*, tj. postoji* $y \in \boldsymbol{Z}$ *tako da je* $2x - 3 = 7y$*, tj. dobijamo* $2x - 7y = 3$*. Očigledno je da je rešenje ove Diofantove jednačine* $(x_0,y_0)=(5,1)$*, a kako rešenje* (x_0,y_0) *zadovoljava jednačinu tada važi* $2x_0 - 7y_0 = 3$*. Oduzimanjem ove dve jednacine dobijamo:*

$$2(x - x_0) - 7(y - y_0) = 0,$$

tj.,

$$y - y_0 = \frac{2(x - x_0)}{7}.$$

Pa važi:

$$\frac{(x - x_0)}{7} = t, \quad t \in \boldsymbol{Z},$$

odakle dobijamo da je $x = 7t + 5$, $t \in \boldsymbol{Z}$*. Uvrstimo li to rešenje u drugu kongruenciju, dobijamo:*

$$4(7t + 5) \equiv 5 \ (mod\ 11),$$

$$28t + 20 \equiv 5 \ (mod\ 11)$$

$$28t \equiv -15 \ (mod\ 11)$$

$$6t \equiv 7 \ (mod\ 11).$$

Rešimo li sada kongruenciju $6t \equiv 7 \ (mod\ 11)$ *dobijamo da je njeno rešenje* $t \equiv 3 \ (mod\ 11)$*, tj.* $t = 11k + 3$, $k \in \boldsymbol{Z}$*. Uvrstimo li to u formulu za* x *dobijamo*

$$x = 7(3 + 11k) + 5 = 26 + 77k, \ k \in \boldsymbol{Z},$$

pa je rešenje polaznog sistema

$$x \equiv 26 \ (mod\ 77).$$

Ako bi trebalo rešiti sistem od tri linearne kongruencije sa jednom nepoznatom, onda bismo prvo na opisani nacin rešili sistem od dve kongruencije, a onda iz dobijenih rešenja odredili ona koja zadovoljavaju i treću kongruenciju.
Kao što se može primetiti, sa većim brojem kongruencija, naš postupak rešavanja sistema linearnih kongruencija se znatno komplikuje. Zbog toga bi bilo dobro imati jednu metodu za rešavanje sistema od proizvoljnog broja linearnih kongruencija sa jednom zajedničkom nepoznatom.
O tome nam upravo govori sledeća teorema.

6.1 Kineska teorema o ostacima

Sistem od dve ili više kongruencija ne mora da ima rešenja, iako svaka pojedinačno kongruencija ima rešenje. Sledeća teorema, poznata kao **Kineska teorema o ostacima** daje uslove pod kojima više linearnih kongruencija ima zajedničko rešenje ako su moduli kongruencija uzajamno prosti u parovima.

Kineska teorema je dobila naziv po kineskom matematičaru Sun Tzu-u ("Gospodar Sun"). Sun Tzu je bio i general i strateg, poznat po najstarijoj knjizi o ratovanju: "*Umeće ratovanja*".

Sun Tzu postavio je sebi sledeći problem:
"Podeli broj sa 3, ostatak je 2; podeli broj sa 5, ostatak je 3; podeli broj sa 7, ostatak je 2. Koji je to broj?"

Primetimo da su brojevi kojima delimo 2, 5 i 7 u parovima uzajamno prosti. Upravo je rešenje ovakvog problema dato narednom teoremom.

Teorema 26 ***(Kineska teorema o ostacima)*** *Neka su m_1, m_2,..., m_k u parovima uzajamno prosti brojevi, a neka su a_1, a_2,..., a_k celi brojevi. Tada sistem kongruencija:*

$$x \equiv a_1 \,(mod\, m_1)$$

$$x \equiv a_2 \,(mod\, m_2)$$

$$\dots$$

$$x \equiv a_k \,(mod\, m_k)$$

ima tačno jedno rešenje po modulu $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Dokaz Kineske teoreme o ostacima daje algoritam za rešavanje sistema linearnih kongruencija sa jednom nepoznatom.

Dokaz 26 *Neka je* $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, *zatim*

$$M_j = \frac{M}{m_j}, \quad j \in \{1, 2, \ldots, k\}.$$

Kako su $m_1, m_2, \ldots, m_k$ *u parovima uzajamno prosti, sledi da je* (M_j, m_j)=1. *Tada postoji* $y_j \in \boldsymbol{Z}$ *takav da je*

$$M_j y_j \equiv 1 \ (mod\, m_j).$$

Posmatrajmo sada sumu:

$$x_0 = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k.$$

Ova suma uvek postoji, zato što postoji i $y_j \in \boldsymbol{Z}$. *Dokažimo da je* x_0 *rešenje sistema, tj. da je* $x_0 \equiv a_j \ (mod\, m_j)$, *za svako* $j = 1, 2, \ldots, k$. *Dakle, treba dokazati da je*

$$a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k \equiv a_j \ (mod\, m_j), j = 1, 2, \ldots, k.$$

Jasno je da $m_j | a_l M_l y_l$, *za* $(l \neq j)$, *tj.*

$$a_l M_l y_l \equiv 0 \ (mod\, m_j), \quad (l \neq j) \quad \boldsymbol{(1)}.$$

Treba još i pokazati da $m_j | a_j M_j y_j$.
Iz $M_j y_j \equiv 1 \ (mod\, m_j)$, *množeći kongruenciju sa* a_j *dobijamo*

$$a_j M_j y_j \equiv a_j \ (mod\, m_j). \quad \boldsymbol{(2)}$$

Dakle, sada sabirajući **(1)** *za sve* $l \neq j$ *dobijamo da je:*

$$a_1 M_1 y_1 + \ldots + a_{j-1} M_{j-1} y_{j-1} + a_{j+1} M_{j+1} y_{j+1} + \ldots + a_k M_k y_k \equiv 0 \ (mod\, m_j). \quad \boldsymbol{(3)}.$$

Sabirajući kongruencije **(2)** *i* **(3)** *dobijamo*

$$x_0 \equiv a_j \ (mod\, m_j), \ j = 1, 2, \ldots, k,$$

što znači da je x_0 *rešenje sistema.*
Ostaje još i da dokažemo da su svaka dva rešenja sistema kongruentna po modulu M. *Neka su* x_1, x_2 *dva rešenja sistema. Tada je:*

$$x_1 \equiv x_2 \equiv a_j \ (mod\, m_j), \ j = 1, 2, \ldots, k.$$

Odavde sledi,

$$m_j | x_2 - x_1, \ j = 1, 2, \ldots, k.$$

Kako su m_1, m_2,..., m_k *u parovima uzajamno prosti, tada sledi da* $m_1 \cdot m_2 \cdot \ldots \cdot m_k | x_2 - x_1$, *a ovo znači da je*

$$x_1 \equiv x_2 \ (mod\, M).$$

Dakle, ako su x_1 *i* x_2 *bilo koja dva rešenja sistema, tada su ona kongruentna po modulu* M.

■

Primer 15 *Odrediti najmanji prirodan broj koji pri deljenju sa 6 daje ostatak 4, pri deljenju sa 7 daje ostatak 5, a pri deljenju sa 11 daje ostatak 6.*

Rešenje 16 *Treba rešiti sistem linearnih kongruencija*

$$x \equiv 4 \ (mod\, 6)$$

$$x \equiv 5 \ (mod\, 7)$$

$$x \equiv 6 \ (mod\, 11).$$

Kako je $m_1 = 6$, $m_2 = 7$, $m_3 = 11$, *oni su u parovima uzajamno prosti pa možemo primeniti Kinesku teoremu o ostacima da bismo dobili rešenje ovog sistema. Imamo da je* $M = 6 \cdot 7 \cdot 11 = 462$.

$$M_1 = \frac{M}{m_1} = \frac{462}{6} = 77$$

$$M_2 = \frac{M}{m_2} = \frac{462}{7} = 66$$

$$M_3 = \frac{M}{m_3} = \frac{462}{11} = 42.$$

Da bismo došli do rešenja sistema, potrebno je rešiti sledeće tri linearne kongruencije:

$$77y_1 \equiv 1 \ (mod\, 6)$$

$$66y_2 \equiv 1 \ (mod\, 7)$$

$$42y_3 \equiv 1 \ (mod\, 11)$$

Njihova rešenja nalazimo koristeći obrat Euklidovog algoritma, u stvari, tražimo rešenja Diofantovih jednačina:

$$77y_1 - 6k = 1$$

$$66y_2 - 7m = 1$$

$$42y_3 - 11n = 1$$

Dakle, dobijamo:

$$77 = 6 \cdot 12 + 5$$

$$6 = 5 \cdot 1 + 1$$

Sledi da je $1 = 6 - 5 = 6 - (77 - 6 \cdot 12) = 13 \cdot 6 + 77 \cdot (-1)$, *dakle* $y_1 = -1$.

$$66 = 7 \cdot 9 + 3$$

$$7 = 3 \cdot 2 + 1$$

Sledi da je $1 = 7 - 3 \cdot 2 = 7 - (66 - 7 \cdot 9) \cdot 2 = -2 \cdot 66 + 19 \cdot 7$, *pa dobijamo da je* $y_2 = -2$.

$$42 = 11 \cdot 3 + 9$$

$$11 = 1 \cdot 9 + 2$$

$$9 = 4 \cdot 2 + 1$$

Odakle dalje dobijamo da $1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 9) = 9 - 4 \cdot (11 - (42 - 11 \cdot 3)) = 9 - 4 \cdot (11 - 42 + 11 \cdot 3) = 9 - 4 \cdot (4 \cdot 11 - 42) = 9 - 16 \cdot 11 + 4 \cdot 42 = 42 - 33 - 16 \cdot 11 + 4 \cdot 42 = 5 \cdot 42 - 19 \cdot 11$, *pa dobijamo da je* $y_3 = 5$. *Traženo rešenje je:*

$$x = 4 \cdot 77 \cdot (-1) + 5 \cdot 66 \cdot (-2) + 6 \cdot 42 \cdot 5 = 292.$$

Dakle, $x = 292$ *je rešenje datog sistema.*

7 Zadaci

U ovom poglavlju će biti rešeni takmičarski zadaci, koji mogu biti od pomoí učenicima koji se spremaju za takmičenja.

Zadatak 1 ***(SSSR, 1990.)*** *Za koje prirodne brojeve n je broj $3^{2n+1} - 2^{2n+1} - 6^n$ složen?*

Rešenje 1 *Dati izraz možemo zapisati u obliku*

$$3 \cdot (3^n)^2 - 2 \cdot (2^n)^2 - 3^n \cdot 2^n.$$

Uvodimo smene: $x = 3^n$, $y = 2^n$, pa dobijamo $3x^2 - 2y^2 - xy$, što se može rastaviti na sledeći način:

$$3x^2 - 2y^2 - xy = 3x^2 - 3xy + 2xy - 2y^2 = (x - y)(3x + 2y).$$

Uvrštavajući vrednosti za x,y, imamo

$$3^{2n+1} - 2^{2n+1} - 6^n = (3^n - 2^n)(3^{n+1} + 2^{n+1}).$$

Kako za $n \geq 2$ važi $3^n - 2^n > 1$, dati broj je složen za sve prirodne brojeve $n \neq 1$. Za $n = 1$, on je jednak prostom broju 13.

Zadatak 2 ***(Čehoslovačka, 1988.)*** *Postoji li 23-cifren prirodan broj takav da zamenom proizvoljne cifre nikada ne dobijamo broj deljiv sa 11?*

Rešenje 2 *Pretpostavimo da takav broj postoji. Neka je to*

$$x = \sum_{k=0}^{22} a_k 10^k.$$

Kako je $10^{2k} \equiv 1 \,(mod\, 11)$ i $10^{2k-1} \equiv -1 \,(mod\, 11)$, ako je r ostatak pri deljenju x sa 11, imamo:

$$r \equiv \sum_{k=0}^{11} a_{2k} - \sum_{k=1}^{11} a_{2k-1} \,(mod\, 11).$$

Ako je $a_{2k} \geq r$, za neko k, tada a_{2k} možemo zameniti sa $a'_{2k} = a_{2k} - r$ (što je cifra, jer je $a'_{2k} \leq a_{2k}$), a u slučaju $a_{2k} \leq r - 2$ sa $a'_{2k} = 11 + a_{2k} - r$ (pri čemu $a'_{2k} \leq 9$ sledi iz $a_{2k} \leq r - 2$), pa će tako dobijeni broj biti deljiv sa 11. Dakle, sve cifre na parnim mestima broja x su jednake $r - 1$, $r \neq 0$.

Analogno, ako je $a_{2k-1} \leq 9 - r$, *tada zamenom cifre* a_{2k-1} *cifrom* $a'_{2k-1} = a_{2k-1} + r \leq (9 - r) + r = 9$, *odnosno za* $a_{2k-1} \geq 11 - r$ *cifrom* $a'_{2k-1} = a_{2k-1} + r - 11 \leq a_{2k-1}$ *dobijamo broj deljiv sa 11, pa su sve cifre na neparnim mestima jednake* $10 - r$.

Tada je,

$$r \equiv 12(r-1) - 11(10-r) \equiv r - 1 \ (mod\ 11),$$

što je nemoguće. Dakle, takav broj ne postoji.

Zadatak 3 ***(Balkanska olimpijada, 1984.)*** *Dokazati da za sve prirodne brojeve* m *postoji prirodan broj* $n > m$ *takav da se dekadni zapis broja* 5^n *dobija dopisivanjem izvesnog broja cifara sleva dekadnom zapisu broja* 5^m.

Rešenje 3 *Uslov zadatka se može zapisati kao* $10^r | (5^n - 5^m)$, *gde je* r *broj cifara u dekadnom zapisu broja* 5^m. *Pošto je* $r \leq m$, *posmatrana relacija deljivosti je ekvivalentna sa* $2^r | (5^n - 5^m) = 5^m(5^{n-m} - 1)$, *tj. sa*

$$2^r | (5^{n-m} - 1).$$

Prema Ojlerovoj teoremi, važi:

$$5^{\varphi(2^r)} \equiv 1 \ (mod\ 2^r).$$

Ali, tada je očito da se za n *oblika*

$$n = m + \varphi(2^r)k = m + 2^{r-1}k, \ \ k \in \boldsymbol{N}.$$

dobija:

$$5^n = 5^m(5^{\varphi(2^r)})^k \equiv 5^m \ (mod\ 2^r),$$

što se i tražilo.

Zadatak 4 (a)***(Madjarska, 1990.)****Pokazati da postoji* $n \in \boldsymbol{N}$, *tako da*

$$2^{1990} | (1989^n - 1).$$

Naći najmanje takvo n.

(b) ***(Medjunarodna olimpijada, Rumunija, 1989.)****Neka je* $m \geq 3$ *neparan prirodan broj. Odrediti najmanje* n *za koje*

$$2^{1989} | (m^n - 1)$$

Rešenje 4 ***(a)*** *Treba odrediti minimalno n za koje je $2^k|(m^n-1)$, gde je k dati prirodan broj.*

Neka je $n=2^t q$, gde je q neparan broj. Tada imamo faktorizaciju

$$m^n-1=(m^{2^t})^q-1=(m^{2t}-1)[(m^{2^t})^{q-1}+\ldots+(m^{2^t})+1].$$

Broj u uglastoj zagradi je neparan, zato što je reč o q neparnih brojeva, pa $2^k|(m^n-1)$ ako i samo ako $2^k|(m^{2^t}-1)$. Otuda sledi da je $q=1$ za traženo minimalno n.

Sa druge strane važi:

$$m^{2^t}-1=(m^2-1)(m^2+1)\cdot\ldots\cdot(m^{2^{t-1}}+1).$$

Budući da je ovde m neparan broj, m^2 daje ostatak 1 pri deljenju sa 4, a isto važi i za broj oblika $m^{2^r}, r\geq 1$. Zbog toga su u gornjem proizvodu sa desne strane svi činioci sem prvog deljivi sa 2, ali ne i sa 4, što znači da je najviši stepen kojim dvojka deli ovaj proizvod $t-1$. Prema tome, preostaje da se razmotri stepen dvojke u faktoru $m^2-1=(m-1)(m+1)$.

Kako m može davati ostatak 1 ili 3 pri deljenju sa 4, posebno ćemo razmotriti ova dva slučaja:

$$m\equiv 1\ (mod\ 4)$$

i

$$m\equiv 3\ (mod\ 4).$$

Ako je $m\equiv 1\ (mod\ 4)$, uočimo najveći broj $s\geq 2$ sa osobinom da $2^s|(m-1)$. Tada je $m+1$ deljiv sa 2, ali ne i sa 4, pa je najviši stepen kojim 2 deli m^2-1 jednak $s+1$. S druge strane, ako je $m\equiv 3\ (mod\ 4)$, posmatramo najveći broj $s\geq 2$ za koje važi $2^s|(m+1)$. Slično kao i malopre, sledi da je broj m^2-1 deljiv sa 2^{s+1}, ali ne i sa 2^{s+2}.

Dakle, ako je broj s odredjen kao što je to opisano u prethodnom pasusu, tada je najviši stepen kojim 2 deli $m^{2^t}-1$ jednak $(t-1)+(s+1)=t+s$. Traženo minimalno rešenje je $n=2^{k-s}$ u slučaju $s\leq k$, u suprotnom je u pitanju $n=1$.

U zadatku (a) *je $m=1989=4\cdot 494+3$, pa je u tom slučaju $s=2$, dok je $k=1990$, što znači da je rešenje zadatka $n=2^{1988}$. Za zadatak pod* (b) *treba primeniti gornje rešenje za $k=1989$.*

Zadatak 5 ***(Predlog za Medjunarodnu olimpijadu, Rumunija, 1995.)*** *Neka je k dati prirodan broj. Dokazati da postoji beskonačno mnogo potpunih kvadrata oblika $2^k n-7$.*

Rešenje 5 *Dokažimo prvo da za svaki prirodan broj k postoji prirodan broj a_k sa osobinom*

$$a_k^2 \equiv -7 \,(mod\, 2^k).$$

Primetimo da izbor $a_k = 1$ zadovoljava traženi uslov za $k \leq 3$. Za $k \geq 4$, podjimo od pretpostavke $a_k^2 \equiv -7 \,(mod\, 2^k)$. Sada očito imamo dve mogućnosti:

$$a_k^2 \equiv -7 \,(mod\, 2^{k+1}),$$

ili

$$a_k^2 \equiv 2^k - 7 \,(mod\, 2^{k+1}).$$

U prvom slučaju definišimo $a_{k+1} = a_k$, a u drugom $a_{k+1} = a_k + 2^{k-1}$. Pošto je a_k neparno, sledi:

$$a_{k+1}^2 = a_k^2 + 2^k a_k + 2^{2k-2} \equiv a_k^2 + 2^k a_k \equiv a_k^2 + 2^k \equiv -7 \,(mod\, 2^{k+1}),$$

koristeći induktivnu pretpostavku.

Najzad, primetimo da niz a_k nije ograničen, pošto mora biti $a_k^2 \geq 2^k - 7$, što znači da posmatrani niz ima beskonačno mnogo različitih vrednosti. Otuda dobijamo traženi rezultat, pošto za $m \geq k$ imamo $a_m^2 \equiv -7 \,(mod\, 2^k)$ i možemo definisati

$$n = \frac{a_m^2 + 7}{2^k}.$$

Zadatak 6 ***(Rumunija, 1978.)*** *Neka su m i n prirodni brojevi sa osobinom da za sve prirodne brojeve k važi $(11k - 1, m) = (11k - 1, n)$. Dokazati da tada za neki ceo broj s važi $\frac{m}{n} = 11^s$.*

Rešenje 6 *Neka je $m = 11^a p, n = 11^b q$, pri čemu je $a, b \geq 0$ i brojevi p, q nisu deljivi sa 11. Dokazaćemo da je $p = q$, odakle sledi tvrdjenje zadatka.*

Kako je (p,11)=1, prema Kineskoj teoremi o ostacima postoji prirodan broj x koji zadovoljava:

$$x \equiv 0 \,(mod\, p), \quad x \equiv -1 \,(mod\, 11).$$

Ali, tada je $x = 11k - 1$ za neki prirodan broj k, pa je:

$$p = (x, 11^a p) = (11k - 1, m) = (11k - 1, n) = (x, 11^b q) = (x, q) \leq q.$$

Potpuno analogno možemo pokazati da je $q \leq p$, pa sledi da je $p = q$.

Zadatak 7 ***(Predlog za Medjunarodnu Olimpijadu, SSSR, 1985.)*** *Predstaviti broj $5^{1985} - 1$ kao proizvod tri prirodna broja od kojih je svaki veći od 5^{100}.*

Rešenje 7 *Primetimo da je* $1985 = 5 \cdot 397$. *Zbog toga, označimo* $x = 5^{397}$. *Sada je razmatrani broj* $x^5 - 1$. *Tada imamo faktorizaciju*

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

Naš cilj je da izraz u drugoj zagradi predstavimo kao razliku dva kvadrata, pri čemu treba imati na umu da je x *neparan stepen od 5, zbog čega je* $5x$ *potpun kvadrat* ($5x = 5^{398} = (5^{199})^2$). *Imajući to u vidu, tražićemo cele brojeve* a, b, c *tako da važi:*

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + 1)^2 - 5x(bx + c)^2.$$

Razvijanjem izraza sa desne strane, dobijamo:

$$x^4 + (2a - 5b^2)x^3 + (a^2 + 2 - 10bc)x^2 + (2a - 5c^2)x + 1,$$

odakle nije teško videti da će jednakost važiti za $a = 3, b = c = 1$. *Prema tome, sledi:*

$$x^5 - 1 = (x-1)[(x^2 + 3x + 1)^2 - 5x(x+1)^2].$$

Izraz u uglastoj zagradi je razlika kvadrata, pa se on može faktorisati. Neposredno se proverava da su sva tri ovako dobijena faktora od $x^5 - 1$ *veća od* 5^{100}.

Zadatak 8 ***(Rumunija, 1978.)*** *Naći sve prirodne brojeve* n *za koje*

$$n | (2^n - 1).$$

Rešenje 8 *Očigledno,* $n = 1$ *zadovoljava traženi uslov. Pretpostavimo da postoji* $n \geq 2$ *koje zadovoljava navedeni uslov. Neka* q_n *označava najmanji prost faktor broja* n. *Dokažimo da važi: ako je* $n > 1$ *i* $p|(2^n - 1)$ *, tada je* $p > q_n$. *U tom slučaju, imaćemo očiglednu kontradikciju, jer* $n|(2^n - 1)$ *povlači* $q_n|(2^n - 1)$. *Treba primetiti, da ako za prirodne brojeve* a *i* b *važi*

$$2^a \equiv 2^b \equiv 1 \ (mod\, p),$$

tada je

$$2^{(a,b)} \equiv 1 \ (mod\, p).$$

Ako je $a \geq b$ *i* $a = qb + r$, *tada važi*

$$2^r \equiv (2^b)^q 2^r = 2^a \equiv 1 \ (mod\, p).$$

Nastavljajući očiglednu primenu Euklidovog algoritma u eksponentu, dobijamo upravo željeni zaključak. Kako prema Maloj Fermaovoj teoremi važi $2^{p-1} \equiv 1 \ (mod\, p)$, *za* $d = (n, p-1)$ *imamo* $2^d \equiv 1 \ (mod\, p)$. *Zbog toga je* $d > 1$, *pa važi* $q_n \leq d$. *S druge strane,* $d|(p-1)$ *pa sledi* $p > d \geq q_n$.

Prema tome, $n = 1$ *je jedino rešenje.*

8

Literatura

[1] Marija Stanić, Nebojša Ikodinović, TEORIJA BROJEVA, zbirka zadataka, Zavod za udžbenike i nastavna sredstva, Beograd, 2004.

[2] Vladimir Mićić, Zoran Kadelburg, Dušan Djukić, UVOD U TEORIJU BROJEVA, materijali za mlade matematičare, sveska 15, Društvo matematičara Srbije, Beograd, 2004.

[3] Igor Dolinka, ELEMENTARNA TEORIJA BROJEVA, moji omiljeni zadaci, Društvo matematičara Srbije, Beograd, 2007.

[4] Gojko Kalajdžić, ALGEBRA, Matematički fakultet, 2004.