UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA
MATEMATIKU I INFORMATIKU

Vojko Nestorović

BROJEVNE KONGRUENCIJE

- MASTER RAD -

Mentor, dr Siniša Crvenković

Novi Sad, 2011.

Sadržaj

Predgovor

Ovaj master rad ima za cilj da predstavi veliki broj ideja koje će biti od pomoći onima koji se susreću sa zadacima, za čije je rešavanje potrebno detaljnije poznavanje osobina brojeva i njihovih međusobnih odnosa.

Master rad je pre svega namenjen nadarenim učenicima srednjih škola koji se pripremaju za takmičenja. Međutim, rad sadrži osnovne pojmove, tvrđenja i jednostavnije primere, tako da mogu da ga koriste matematičari koji se prvi put sreću sa teorijom brojeva. Takođe, rad sadrži i složenije zadatke koji mogu da posluže kao dobar materijal za pripremu učenika za takmičenja.

Sadržaj master rada podeljen je u šest poglavlja. Prvo poglavlje sadrži osnovne osobine iz teorije deljivosti celih brojeva. U drugom poglavlju obrađeni su prosti brojevi kao i teoreme i metode za njihovo dobijanje. U trećem poglavlju definisana je relacija kongruencije brojeva i njene osnovne osobine. U četvrtom poglavlju određene su klase i sistemi ostataka po datom modulu. U ovom poglavlju precizno su definisani potpun i redukovan sistem ostataka i njihove osobine. Peto poglavlje sadrži Ojlerovu funkciju, Ojlerovu teoremu, Malu Fermaovu teoremu i Vilsonovu teoremu i njihove primene u rešavanju zadataka. Šesto poglavlje obrađuje kongruencije sa jednom nepoznatom, kao što su linearne kongruencije, sistemi linearnih kongruencija, kao i kongruncije višeg reda po prostom i složenom modulu. Smatram da bi kongruencije višeg reda po složenom modulu mogle biti tema za dalje proučavanje.

Ovom prilikom želim da se zahvalim svim mojim profesorima na pomoći u sticanju znanja tokom osnovnih, a potom i master studija. Posebno bih želeo da se zahvalim svom mentoru dr Siniši Crvenković. Takođe se zahvaljujem profesorima dr Zagorki Lazanov-Crvenković i dr Ljlji Gajić, koje su pristale da budu članovi komisije u oceni moga rada.

Novi Sad, 11. 07. 2011.
Autor

1 Deljivost celih brojeva

1.1 Osnovne osobine

Definicija 1.1 *Neka su a i b celi brojevi. Ako postoji ceo broj m takav da je $b = ma$, tada kažemo da je a* ***delitelj*** *ili* ***faktor*** *broja b i da je b* ***sadržilac*** *ili* ***višekratnik*** *broja a. To zapisujemo ovako $a \mid b$. Na primer: $3 \mid 9$, $6 \mid 30$, $5 \mid 0$.*

Ako $a \mid b$, očigledno je i $a \mid (-b)$, $(-a) \mid b$ i $(-a) \mid (-b)$. Zato se, pri proučavanju deljivosti, najčešće ograničavamo na nenegativne cele brojeve.

Definicija 1.2 *Broj a nazivamo* ***pravi delitelj*** *od b, ako je $a \mid b$ i $a \neq b$.*

U sledećoj teoremi date su neke od najvažnijih osobina relacije deljivosti.

Teorema 1.1 *Neka su a, b, c proizvoljni nenegativni celi brojevi. Tada važi:*

a) ako je $a \mid b$ i $b \mid c$, tada je $a \mid c$;

b) ako je $a \mid b$ i $b \neq 0$, tada je $0 < a \leq b$;

b) ako je $a \mid b$ i $a \mid c$, tada je, za proizvoljne cele brojeve x i y, $a \mid (bx + cy)$;

d) ako $a \mid b$ i $b \mid a$, tada je $a = b$.

Dokaz. a) Ako je $a \mid b$ i $b \mid c$, tada postoje celi brojevi m i n takvi da je $b = ma$ i $c = nb$. Tada je, $c = nma$, a kako je mn ceo broj, sledi da je $a \mid c$.

b) Ako je $a \mid b$, tada postoji nenegativan ceo broj m takav da je $b = ma$. Kako je $b > 0$, tada su i a i m pozitivni brojevi, tj. $1 \leq a$ i $1 \leq m$. Sledi da je

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

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

$$bx + cy = max + nay = a\,(mx + ny).$$

Kako je $mx + ny$ ceo broj, to je $a \mid (bx + cy)$.

d) Pretpostavimo da je $a \mid b$ i $b \mid a$. Ako je $b = 0$, tada je i $a = 0$. Ako $b > 0$ tada iz (b) sledi $a = b$. ■

Posledica 1.1 *a) Ako su a, b, c proizvoljni nenegativni celi brojevi takvi da je $a \mid b$ i $a \mid c$, tada je $a \mid (b + c)$ i $a \mid (b - c)$.*

b) Ako su u jednakosti

$$a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_s\,,$$

svi sabirci izuzev jednoga deljivi sa c, tada je i taj jedan deljiv sa c.

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

Teorema 1.2 ***(Algoritam deljivosti)*** *Neka su a i b nenegativni celi brojevi i $b \neq 0$. Tada su jednoznačno određeni nenegativni celi brojevi q i r, takvi da je*

$$a = bq + r, \qquad 0 \leq r < b.$$

Dokaz. Zaista, takav jedan način predstavljanja broja a dobija se ako uzmemo da je bq najveći sadržilac broja b koji nije veći od a. Pretpostavimo da postoji još jedan način za predstavljanje broja a.

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

Tada je $0 = b(q - q_1) + r - r_1$, odakle sledi da je $b \mid (r - r_1)$. ■

Posledica 1.1 a 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 i $q = q_1$.

Broj q naziva se količnik, a broj r ostatak pri deljenju a sa b. Algoritam deljenja se koristi u klasifikaciji brojeva. Na primer za $b = 2$, ako je $r = 1$ $(a = 2q + 1)$ tada kažemo da je a neparan broj, a ako je $r = 0$ $(a = 2q)$, tada 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 delitelji brojevi 1 i p. Za pozitivan ceo broj veći od 1 koji nije prost, kažemo da je *složen*. Svaki složen broj n, ima delitelje različite od 1 i n.

1.2 Najveći zajednički delilac

Definicija 1.3 *Neka su a i b nenegativni celi brojevi takvi da je bar jedan veći od 0. Za broj k kažemo da je* ***zajednički delitelj*** *brojeva a i b, ako je $k \mid a$ i $k \mid b$.*

Definicija 1.4 *Najveći pozitivan ceo broj koji je delitelj i od a i od b, naziva se* ***najveći zajednički delitelj*** *brojeva a i b. Označavamo ga sa $NZD\ (a, b)$ ili samo (a, b). On uvek postoji, što se lako dokazuje, polazeći od principa dobrog uređenja.*

Na primer: $NZD\ (4, 16) = 4$, $NZD\ (0, 5) = 5$, $NZD\ (30, 50) = 10$, $NZD\ (8, 15) = 1$.

Da bismo dokazali da je $d = NZD\ (a, b)$, treba dokazati tačnost sledećeg tvrđenja:
(i) $d \mid a$ i $d \mid b$
(ii) ako $k \mid a$ i $k \mid b$, tada je $k \mid d$.

Teorema 1.3 *Najveći zajednički delitelj dva cela broja, od kojih je bar jedan različit od 0, je jedinstven.*

Dokaz. Ako je $d = NZD\ (a, b)$ i $d' = NZD\ (a, b)$, tada je $d \mid d'$ i $d' \mid d$, ako primenimo teoremu 1.1 (d) sledi da je $d = d'$. ■

Teorema 1.4 *Neka su a i b nenegativni celi brojevi, pri čemu je bar jedan različit od nule. Tada je NZD (a, b) jednak najmanjem celom broju koji se može izraziti kao linearna funkcija od a i b, tj. NZD (a, b) je najmanji pozitivan ceo broj koji se može napisati u obliku $ax + by$, gde su x i y celi brojevi.*

Dokaz. Neka je S skup svih pozitivnih celih brojeva oblika $ax + by$, gde su x i y celi brojevi. S je neprazan, jer sadrži broj $a^2 + b^2$. Zato u S postoji najmanji element

$$d = ax_1 + by_1 .$$

Ako je $a = 0$ ili $b = 0$, tvrđenje važi. Pretpostavimo da je $a \neq 0$ i $b \neq 0$, i neka su q i r celi brojevi, takvi da je

$$a = qd + r, \qquad 0 \leq r < d.$$

Tada je

$$r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1).$$

Dakle, r je linearna funkcija od a i b. Međutim, r nije u skupu S, jer je $0 \leq r < d$, a d je najmanji broj u S. Zato je $r = 0$ i $a = qd$, tj. $d \mid a$. Na isti način dokazuje se da je $d \mid b$.

Pretpostavimo da je i d' zajednički delitelj od a i b. Tada je $d' \mid (ax_1 + by_1)$ (Teorema 1.1 (c)), tj. $d' \mid d$. Prema tome $d = NZD (a, b)$. ■

Očigledno je $NZD (a, a) = NZD (0, a) = a$, za $a > 0$. Za različite pozitivne brojeve a i b, algoritam za određivanje njihovog najvećeg zajedničkog delitelja zasniva se na algoritmu delenja. To je poznati **Euklidov algoritam** koji se sastoji u sledećem.

Neka su a i b pozitivni celi brojevi, $a > b$. Tada prema algoritmu delenja, jednoznačno su određeni brojevi q_i i r_i, $1 \leq i \leq k + 1$, takvi da je

$$
\begin{aligned}
a &= q_1 b + r_1, && 0 < r_1 < b;\\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1;\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2;\\
&\ldots\\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, && 0 < r_{k-1} < r_{k-2};\\
r_{k-2} &= q_k r_{k-1} + r_k, && 0 < r_k < r_{k-1};\\
r_{k-1} &= q_{k+1} r_k + 0 && (r_{k+1} = 0).
\end{aligned}
$$

Niz $r_1, r_2, r_3, \ldots, r_{k-1}, r_k$ je opadajući niz prirodnih brojeva manjih od b, što znači da se gore opisani postupak mora završiti posle konačnog broja koraka.

Teorema 1.5 *NZD (a, b) = r_k gde je r_k poslednji pozitivan ostatak dobijen primenom Euklidovog algoritma na prirodne brojeve a i b, $a > b$.*

Dokaz. Dokažimo da važe sledeća dva tvrđenja:

(i) $r_k \mid a$ i $r_k \mid b$

(ii) ako je $d \mid a$ i $d \mid b$, tada je $d \mid r_k$.

Iz Euklidovog algoritma dobijamo da je $r_k \mid r_{k-1}$. Na osnovu toga i poslednje jednakosti, zaključujemo da je $r_k \mid r_{k-2}$. Nastavljajući taj postupak dobije se da je $r_k \mid r_{k-3}$, $r_k \mid r_{k-4}, \ldots$, $r_k \mid b$, a onda iz prve jednakosti sledi da je $r_k \mid a$. Dakle uslov (i) je zadovoljen.

Neka je d prirodan broj takav da je $d \mid a$ i $d \mid b$. Tada iz prve jednakosti Euklidovog algoritma dobijamo da je $d \mid r_1$, iz druge da je $d \mid r_2, \ldots$, i konačno iz pretposlednje da je $d \mid r_k$. Time je dokazano da važi (ii). Dakle, $r_k = NZD\ (a, b)$. ■

Primer 1.1 Odredićemo *NZD (936, 588)*. Po Euklidovom algoritmu imamo

$936 = 1 \cdot 588 + 348$
$588 = 1 \cdot 348 + 240$
$348 = 1 \cdot 240 + 108$
$240 = 2 \cdot 108 + 24$
$108 = 4 \cdot 24 + 12$
$24 = 2 \cdot 12.$

Dakle, NZD (936, 588) = 12. Δ

Definicija 1.5 *Neka su* $a_1, a_2, \ldots, a_n$ *nenegativni celi brojevi, pri čemu je bar jedan različit od 0. Najveći pozitivan ceo broj d, koji je delitelj svih tih brojeva se naziva* ***najveći zajednički delitelj*** *za brojeve* $a_1, a_2, \ldots, a_n$, *a obeležavamo ga sa* $NZD(a_1, a_2, \ldots, a_n)$. *Na primer,*

NZD (21, 12, 30) = 3 .

Da bismo dokazali da je $NZD(a_1, a_2, \ldots, a_n)$ *dovoljno je dokazati:*
(i) $d \mid a_i$, *za* $i = 1, 2, \ldots, n$;
(ii) ako je $r \mid a_i$, *za* $i = 1, 2, \ldots, n$ *tada je* $r \mid d$.

Teorema 1.6 *Ako su* $a_1, a_2, \ldots, a_n$ *pozitivni celi brojevi,* $n \geq 3$, *tada je* $NZD(a_1, a_2, \ldots, a_n) = NZD(NZD(a_1, a_2, \ldots, a_{n-1}), a_n)$.

Dokaz. Neka je $d = NZD(a_1, a_2, \ldots, a_n)$ i $d' = NZD(NZD(a_1, a_2, \ldots, a_{n-1}), a_n)$. Kako je $d \mid a_i$, za $i = 1, 2, \ldots, n$, dobijamo da je $d \mid NZD(a_1, a_2, \ldots, a_{n-1})$ i $d \mid a_n$. Dakle, $d \mid d'$. Slično, iz $d' \mid NZD(a_1, a_2, \ldots, a_{n-1})$ i $d' \mid a_n$ sledi $d' \mid a_i$, za $i = 1, 2, \ldots, n$, pa dobijamo da je $d' \mid d$. Prema tome, $d = d'$. ■

Jasno da je $NZD(a_1, a_2, \ldots, a_n, 0, 0, \ldots, 0) = NZD(a_1, a_2, \ldots, a_n)$.

Na osnovu Teoreme 1.6, zaključujemo da se višestrukom primenom Euklidovog algoritma može dobiti najveći zajednički delitelj više celih brojeva.

Definicija 1.6 *Cele brojeve a i b, od kojih je bar jedan različit od nule, nazivamo* ***uzajamno prostim*** *ako je NZD (a, b) = 1. Na primer brojevi 14 i 25 su uzajamno prosti.*

Definicija 1.7 *Neka su* $a_1, a_2, \ldots, a_n$ *celi brojevi, pri čemu je bar jedan različit od nule. Ako je* $NZD(a_i, a_j) = 1$, *za* $1 \leq i < j \leq n$, *tada su brojevi* $a_1, a_2, \ldots, a_n$ ***po parovima uzajamno prosti***. *Ako je* $NZD(a_1, a_2, \ldots, a_n) = 1$, *tada su brojevi* $a_1, a_2, \ldots, a_n$ ***uzajamno prosti***.

Primer 1.2 Brojevi *6, 10 i 15* su uzajamno prosti, a nisu po parovima uzajamno prosti. Brojevi *18, 25* i *77* su po parovima uzajamno prosti. Δ

Definicija 1.7 *Najmanji pozitivan ceo broj m koji je zajednički sadržilac brojeva a i b naziva se* ***najmanji zajednički sadržilac*** *brojeva a i b i obeležavamo ga sa NZS (a, b). Jasno je da je*

$$NZS(a, b) = NZS(-a, b) = NZS(a, -b) = NZS(-a, -b) .$$

Preciznije, $m = NZS(a, b)$ *ako važi:*

(i) $a \mid m$, $b \mid m$;

(ii) *ako je* $a \mid k$ *i* $b \mid k$, *tada je* $m \mid k$.

Slično kao za najveći delitelj, definiše se najmanji zajednički sadržilac brojeva $a_1, a_2, \ldots, a_n$, *u oznaci* $NZS(a_1, a_2, \ldots, a_n)$ *kao najmanji pozitivan broj koji je sadržilac svakog od brojeva* $a_1, a_2, \ldots, a_n$.

1.3 Osnovna teorema aritmetike

U ovom odeljku dokazaćemo da se svaki ceo broj može predstaviti u obliku proizvoda prostih faktora i da je takvo predstavljanje jedinstveno do na poredak faktora.

Teorema 1.7 *Ako je n ceo broj veći od 1, onda je n proizvod prostih faktora.*

Dokaz. Ako je *n* prost broj, tvrđenje očigledno važi. Pretpostavimo da tvrđenje važi za svaki složen broj manji od *n*. Ako je *n* složen broj, tada postoji ceo broj *d* takav da je $1 < d < n$ i $d \mid n$. Označimo sa *m* najmanji takav broj. Broj *m* ne može biti složen, jer bi u tom slučaju postojao ceo broj *k*, takav da je $1 < k < m$ i $k \mid m$, što povlači da je $k \mid n$.

To je, međutim, u kontradikciji sa pretpostavkom da je m najmanji ceo broj veći od 1 koji je delitelj od n. Dakle, m je prost broj. Obeležimo ga sa p_1. Sledi da je $n = p_1 n_1$, gde je $1 < n_1 < n$. Po pretpostavci indukcije broj n_1 se može predstaviti u obliku prostih faktora, prema toma, onda može i n. ■

Grupišući jednake preostale faktore broja n, zaključujemo da se svaki ceo broj veći od 1 može predstaviti u obliku

(1) $$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

gde je $p_1 < p_1 < \ldots < p_k$ i $\alpha_i > 0$, za $i = 1, 2, \ldots, k$.

Definicija 1.9 *Predstavljanje broja n u obliku (1) nazivamo* ***kanonski oblik*** *broja n.*

Teorema 1.8 ***(Osnovna teorema aritmetike)*** *Svaki ceo broj veći od 1 ima jedinstven kanonski oblik.*

Dokaz. Kanonsko predstavljanje postoji na osnovu Teoreme 1.7. Preostaje da dokažemo da je to predstavljanje jedinstveno.

Pretpostavimo da postoji pozitivan složen broj veći od 1 koji se može na dva različita načina predstaviti u kanonskom obliku. Neka je n najmanji takav broj sa predstavljanjima

$$n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_m.$$

Ne postoji prost broj p koji se pojavljuje u obe kanonske reprezentacije broja n, jer bi u tom slučaju i broj $n' = \frac{n}{p}$, koji je manji od n, imao dve različite kanonske reprezentacije, što je u kontradikciji sa pretpostavkom o minimalnosti broja n.

Možemo da pretpostavimo da je

$$p_1 \leq p_2 \leq \ldots \leq p_k, \qquad q_1 \leq q_2 \leq \ldots \leq q_m.$$

Za proste faktore p_1 i q_1 važi $p_1 \neq q_1$, pa možemo uzeti $p_1 < q_1$. Neka je $N = p_1 q_2 \ldots q_m$. Kako je $p_1 | N$ i $p_1 | n$, sledi da je $p_1 | (n-N)$, gde je $n-N = (q_1 - p_1) \cdot q_2 \cdots q_m > 1$. Sledi da se broj $n - N$ može napisati u obliku

$$n - N = p_1 t_1 \ldots t_h,$$

gde su t_i prosti brojevi za $i = 1,2,\ldots,h$. Sa druge strane, ako je $q_1 - p_1 > 1$, onda se $q_1 - p_1$ može napisati kao proizvod prostih faktora, na primer $q_1 - p_1 = r_1 \cdot r_2 \cdots r_s$, pa dobijamo, na drugi način, u obliku proizvoda prostih faktora:

$$n - N = r_1 r_2 \ldots r_s q_2 \ldots q_m.$$

Ova poslednja faktorizacija ne sadrži prost faktor p_1. Znamo da je $p_1 \neq q_i$, za $i = 1, 2, \ldots, m$; sa druge strane $p_1 \neq r_j$, za $j = 1, 2, \ldots, s$, jer p_1 nije delitelj od $q_1 - p_1$. Dakle, broj $n - N$ ima dve različite faktorizacije, jer samo jedna od njih sadrži prost faktor p_1. To važi i u slučaju kada je $q_1 - p_1 = 1$. Međutim, $1 < n - N < n$ što je u kontradikciji sa pretpostavkom o minimalnosti broja n da ne postoji ceo broj veći od 1, koji se može predstaviti na dva načina u kanonskom obliku. ■

Teorema 1.9 *Neka su brojevi m i n dati u kanonskom obliku*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad n = \prod_{i=1}^{k} p_i^{\beta_i}$$

Tada $m | n$ ako i samo ako je $0 \leq \alpha_i \leq \beta_i$ za $i = 1, 2, \ldots, k$.

Dokaz. Sledi na osnovu toga što je $n = md$ gde je

$$d = \prod_{i=1}^{k} p_i^{\delta_i}$$

pri čemu je $\delta_i = \beta_i - \alpha_i$. ■

Posledica 1.9 *Ako je*

$$m = \prod_{i=1}^{k} p_i^{\propto_i} \qquad n = \prod_{i=1}^{k} p_i^{\beta_i}$$

Tada je

$NZD(m,n) = \prod_{i=1}^{k} p_i^{min\,(\alpha_i \beta_i)}$ $NZS(m,n) = \prod_{i=1}^{k} p_i^{max\,(\alpha_i \beta_i)}$.

1.4 Linearna Diofantova jednačina

Definicija 1.10 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 1.11 Polinomna jednačina po promenljivim *x, y, z, ...* sa celobrojnim koeficijentima naziva se *Diofantova jednačina* ako promenljive uzimaju vrednost iz skupa celih brojeva.

Teorema 1.10 *Linearna Diofantova jednačina*

$$ax + by = c$$

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

Dokaz. Neka je $d = NZD\ (a, b)$. Pretpostavimo da je (x_0, y_0) rešenje jedačine. Tada je

$$ax_0 + by_0 = c.$$

Kako $d \mid a$ i $d \mid b$, onda je i $d \mid c$.

Obratno, pretpostavimo da je $d \mid c$. Tada postoji ceo broj k takav da je $c = kd$. 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

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

odnosno

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

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

Primer 1.3 Diofantova jednačina $28x + 70y = 39$ nema rešenja, jer je $14 = NZD(28, 70)$, a 14 nije delitelj broja 39. Δ

Primer 1.4 Linearna Diofantova jednačina

$$13x + 32y = 5$$

ima rešenje. Ovde je $a = 32$, $b = 13$ koristeći Euklidov algoritam dobijamo

$$32 = 2 \cdot 13 + 6$$
$$13 = 2 \cdot 6 + 1$$
$$6 = 6 \cdot 1.$$

Brojevi 32 i 13 su uzajamno prosti, pa broj 1 možemo predstaviti kao linearnu funkciju brojeva 32 i 13:

$$1 = 13 + (-2)\,6 = (5)\,13 + (-2)\,32.$$

Konačno dobijamo da je

$$13(25) + 32(-10) = 5.$$

Dakle, jedno rešenje linearne Diofantove jednačine $13x + 32y = 5$ je

(25, -10). Lako se proverava da su rešenja i

$$x = 25 + 32t, \quad y = -10 - 13t$$

gde je t ceo broj. Δ

Teorema 1.11 *Ako je $d = NZD(a, b)$, $d \mid c$ i $(x_0\, y_0)$ jedno rešenje Diofantove jednačine $ax + by = c$, tada su sva rešenja (x, y) data formulama*

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

gde je t proizvoljan ceo broj.

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

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

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

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

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

$$a(x - x_0) = b\,(y_0 - y),$$

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

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

Dakle,

$$\frac{b}{d} \mid (x - x_0) \qquad \text{i} \qquad \frac{a}{d} \mid (y_0 - y)$$

odakle je

$$x - x_0 = \frac{b}{d}t \qquad \text{i} \qquad y_0 - y = \frac{a}{d}t;$$

gde je t ceo broj. Konačno dobijamo da je

$$x = x_0 + \frac{b}{d}t \qquad \text{i} \qquad y = y_0 + \frac{b}{d}t. \ \blacksquare$$

Primer 1.5 Linearna Diofantova jednačina $27x + 59y = 20$ ima rešenje, jer je $1 = NZD\,(27, 59)$, a 1 je delitelj broja 20. Ovde je $a = 58, b = 27$, koristeći Euklidov algoritam dobijamo

$$\begin{aligned} 59 &= 2 \cdot 27 + 5 \\ 27 &= 5 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

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

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2(27 - 5 \cdot 5) = 11 \cdot 5 - 2 \cdot 27 \\ &= 11(59 - 2 \cdot 27) - 2 \cdot 27 = 11 \cdot 59 - 24 \cdot 27. \end{aligned}$$

Konačno dobijamo da je $(-480)27 + 220 \cdot 59 = 20$.

Dakle, jedno rešenje linearne Diofantove jednačine $27x + 59y = 20$ je $(-480,\ 220)$. Lako se proverava da su rešenja i $x = -480 + 59t$, $y = 220 - 27t$, gde je t ceo broj. Može se izabrati I manje (po apsolutnoj vrednosti) početno rešenje. Na primer, za $t = 8$ se dobija $x_1 = -8,\ y_1 = 4$, pa je opšte rešenje $x = -8 + 59u,\ y = 4 - 27u$, $u \in Z$. Δ

2 Prosti brojevi

2.1 Eratostenovo sito

Problem dobijanja potpune liste prostih brojeva manjih od datog broja n, privlačio je pažnju matematičara vekovima. Jedan postupak za nalaženje prostih brojeva do datog broja n, je otkriće starogrčkog matematičara Eratostena. Pre nego što opišemo njegov algoritam, dokazaćemo sledeću teoremu.

Teorema 2.1 *Pozitivan ceo broj n je složen ako i samo ako ima prost faktor p, takav da je $p \leq \sqrt{p}$.*

Dokaz. Ako n ima prost faktor $p \leq \sqrt{n}$, tada je n, očigledno, složen broj.

Obratno, ako je p najmanji prost faktor složenog broja n, tada je $n = pm$, za neki ceo broj m i pri tome je $m \geq p$. Sledi da je $p \leq \sqrt{n}$. ■

Na ovome kriterijumu se i zasniva Eratostenov algoritam, poznati pod nazivom ***Eratostenovo sito***, po Eratostenu koji ga je prvi primenio u 3. veku pre nove ere.

Eratostenov algoritam sastoji se od sledećih koraka:

1. Ispisati u niz sve prirodne brojeve od 2 do n.

2. Uočiti u nizu prvi broj koji nije ni podvučen ni precrtan i podvući ga, a zatim precrtati sve njegove sadržioce u nizu.

3. Ako su svi brojevi u nizu označeni (podvučeni ili precrtani) postupak je završen; u protivnom, primeniti korak 2.

Po završetku postupka dobijamo sve proste brojeve ne veće od n. To su podvučeni brojevi.

2.2 Beskonačnost skupa prostih brojeva

Veliki broj matematičara bezuspešno je pokušavao da nađe opštu formulu za proste brojeve, tj. funkciju $f(n)$ čije bi vrednosti, za sve nenegativne cele brojeve bile prosti brojevi. Interesantna je funkcija $f(n) = n^2-79n+1601$ koja za $0 \leq n \leq 79$ daje proste brojeve, ali za $n = 80$ je $f(80) = 80^2 - 79 \cdot 80 + 1601 = 1681 = 41^2$.

U ovom poglavlju interesantno je pomenuti Fermaovu pogrešnu hipotezu o prostim brojevima. On je izučavao brojeve oblika $f_n = 2^{2^n} + 1$, gde je n proizvoljan ceo nenegativan broj, koji su po njemu dobili naziv Fermaovi brojevi. To su brojevi: $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$ koji su prosti, a broj $f_5 = 4294967297 = 641 \cdot 6700417$ je složen.

Što se tiče Fermaovih brojeva, nezavisno da li su prosti ili složeni, pokazali su da imaju interesantna svojstva. Sledeća teorema otkriva nam jedno takvo svojstvo.

Teorema 2.2 *Svaka dva različita Fermaova broja su uzajamno prosta.*

Dokaz. Neka su f_n i f_{n+k}, $k > 0$ dva različita Fermaova broja. Pretpostavimo da je m ceo pozitivan broj, takav da je $m \mid f_n$ i $m \mid f_{n+k}$. Neka je $x = 2^{2^n}$, tada je

$$x^{2^k} = (2^{2^n})^{2^k} = 2^{2^n \cdot 2^k} = 2^{2^{n+k}} = f_{n+k} - 1.$$

Ako posmatramo količnik

$$\frac{f_{n+k} - 2}{f_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \ldots - 1$$

zaključujemo da $f_n \mid (f_{n+k} - 2)$. Sledi da $m \mid (f_{n+k} - 2)$. Kako je i $m \mid f_{n+k}$, to je $m \mid 2$. Fermaovi brojevi su neparni, pa je $m = 1$, odakle sledi da je $NZD(f_{k+k}, f_k) = 1$. ■

Napomenimo još da do danas nije pronađen nijedan prost Fermaov broj veći od f_4.

Pitanje da li je neki Fermaov broj prost ili složen povezano je problemom konstrukcije pravilnih mnogouglova pomoću lenjira i šestara.

Gausova teorema: *Pravilan mnogougao sa n stranica može se konstruisati šestarom i lenjirom ako i samo ako je n prirodan broj oblika* $n = 2^s p_1 p_2 \ldots p_k$, *gde je s nenegativan ceo broj, a* $p_1 p_2 \ldots p_k$ *različiti Fermaovi prosti brojevi* $(k > 0)$ *ili je* $n = 2^s$, *gde je s ceo broj veći od 1.*

Teorema 2.3 *Broj prostih brojeva je beskonačan.*

Dokaz. Pretpostavimo da je broj prostih brojeva konačan i neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi, pri čemu je p_n najveći od njih. Posmatrajmo broj

$$q = p_1 p_2 \ldots p_n + 1$$

Broj q nije deljiv ni sa jednim od prostih brojeva $p_1, p_2, \ldots, p_n$, jer pri deljenju sa svakim od njih daje ostatak 1. Kako je $q > 1$, sledi da je q prost broj veći od p_n, najveći prost broj. Dakle, broj prostih brojeva ne može biti konačan. ■

U teoriji brojeva ima još dosta poznatih stavova od kojih ćemo navesti neke bez dokaza.

Svaki prost broj veći od 2 je neparan. Svi neparni brojevi se mogu podeliti u dve klase oblika $4k-1$ i $4k+1$. Svaka od ovih klasa sadrži beskonačno mnogo prostih brojeva.

Svaki paran broj veći od dva može se predstaviti u obliku zbira dva prosta broja. Svaki neparan broj veći od 7 može se predstaviti kao zbir 3 neparna prosta broja.

2.3 Mersenovi brojevi

Stari Grci su poznavali 4 prosta broja oblika $M_p = 2^p - 1$, p prost broj i to su:

$$M_2 = 2^2 - 1 = 3,$$
$$M_3 = 2^3 - 1 = 7,$$
$$M_5 = 2^5 - 1 = 31,$$
$$M_7 = 2^7 - 1 = 127.$$

U srednjem veku otkriven je još jedan prost broj oblika $2^p - 1$, a to je

$$M_{13} = 2^{13} - 1 = 8191.$$

U *XVII* veku brojeve oblika $2^p - 1$, gde je p prost broj, počinje izučavati francuski matematičar *Marin Mersen (1588 - 1648).* Ti brojevi su po njemu dobili ime *Mersenovi brojevi.* Ako je broj $M_p = 2^p - 1$ prost broj, onda se on naziva *Mersenov prost broj.*

Do *1996.* godine bila su poznata *34* Mersenova prosta broja, a *34.* prost Mersenov broj bio je $M_{1257787}$, sa *378632* cifre. Do danas je poznato *47 prostih* Mersenovih brojeva, a najveći je $M_{43112609}$, koji ima *12978189* cifara.

Mersenovi prosti brojevi, kao i prosti brojevi oblika $2^p + 1$ su od velikog značaja za druge oblasti matematike.

Sledeća teorema daje jedan potreban, ali ne i dovoljan uslov da bi broj oblika $2^n - 1$ bio prost.

Teorema 2.4 *Ako je n prirodan broj i $2^n - 1$ prost broj, tada je i n prost broj.*

Dokaz. Dokazaćemo ekvivalentno tvrđenje, tj. da je $2^n - 1$ složen broj ako je n složen broj. Neka je $n = rs, r > 1, s > 1$. Tada je

$$\begin{aligned} 2^n - 1 &= 2^{rs} - 1 \\ &= (2^r)^s - 1 \\ &= (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \ldots + 1). \blacksquare \end{aligned}$$

3 Kongruencije brojeva

3.1 Definicija relacije kongruencije

Osnovni pojam od koga polazimo je kongruencija, koja je u tesnoj vezi sa pojmom deljivosti u skupu celih brojeva.

Definicija 3.1 *Neka su a, b i $m \neq 0$ celi brojevi. Broj a je* ***kongruentan*** *broju b s obzirom na modul m, ako $m \mid a - b$.*

Ova činjenica se obeležava sa

$$a \equiv b \pmod{m} \text{ ili } a \equiv_m b.$$

i čita se „a je kongruentno b po modulu m".

Ako $a - b$ nije deljivo sa m, tada je a nekongruentno sa b po modulu m, i to zapisujemo

$$a \not\equiv b \pmod{m}.$$

Na primer:

1. $29 \equiv 5 \pmod{8}$ jer je $8 \mid 29 - 5$;

2. $17 \equiv -9 \pmod{13}$ jer je $13 \mid 17 - (-9)$;

3. $-2 \not\equiv 15 \pmod{3}$ jer je $3 \nmid (-2 - 15)$.

Prema definiciji 1.1 relacija $a \equiv b \pmod{m}$ označava da $m \mid a - b$, što znači da postoji ceo broj t takav da je $a - b \equiv mt$, odnosno

$$a = b + mt.$$

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

Definicija 3.2 Broj a *je kongruentan broju* b *po modulu m ako postoji ceo broj* t *takav da je* $a = b + mt$, $t = 0, \pm 1, \pm 2, \ldots$.

Teorema 3.1 *Brojevi* a *i* b *imaju iste ostatke pri deljenju sa* m, *tada i samo tada kada je* $a \equiv b \pmod m$.

Dokaz. Ako je $a \equiv b \pmod m$, tada postoji ceo broj t takav da je $a = b + mt$. Za b i $m \neq 0$ postoje jednoznačno određeni celi brojevi q i r takvi da je $b = mq + r$, $0 \leq r < |m|$, gde je r ostatak dobijen pri deljenju b sa m. Odavde sledi da je $a = m(t + q) + r$, $0 \leq r < |m|$. Dakle i broj a ima isti ostatak pri deljenju sa m.

Obratno, neka su a i b brojevi koji pri deljenju sa m imaju iste ostatke. Tada se može zapisati da je $a = mg_1 + r$ i $b = mg_2 + r$ pri čemu je $0 \leq r < |m|$. Odavde sledi da je $a - b = m(q_1 - q_2)$, te je $a \equiv b \pmod m$. ■

S obzirom na dokazanu teoremu relaciju kongruencije možemo definisati na sledeći način:

Broj a je kongruentan broju b po modulu m ako brojevi a i b imaju iste ostatke pri deljenju sa m ($m \neq 0$).

3.2 Osobine relacije kongruencije

Neka su a, b i $m \neq 0$ celi brojevi. Broj m ili deli $a - b$ ili ne deli, tj. ili $a \equiv b \pmod m$ ili $a \not\equiv b \pmod m$.

Relacija kongruencije je refleksivna, tj. za svaki ceo broj a važi $a \equiv a \pmod m$, jer $m \mid a - a$, odnosno $m \mid 0$.

Ako je $a \equiv b \pmod m$, tada $m \mid a - b$. Odavde sledi da $m \mid -(b - a)$, to jeste $m \mid b - a$ *pa je* $b \equiv a \pmod m$.

Ako je $a \equiv b \pmod m$ i $b \equiv c \pmod m$, tada postoje celi brojevi p i q takvi da je

$$a = b + mp \quad \text{i} \quad b = c + mq.$$

Ako saberemo ove dve jednakosti dobajemo $a - c = (p + q)\, m$ tj. $a \equiv c \pmod m$.

Na osnovu ovoga zaključujemo da je relacija kongruencije tranzitivna.

Dobijeni rezultati mogu se rezimirati sledećim tvrđenjem.

Teorema 3.2 *Relacija kongruencije po modulu je relacija ekvivalencije.*

Sada možemo dokazati još neke osobine relacije kongruencije.

Teorema 3.3 *Neka su a, b, c, d i $m \neq 0$ celi brojevi. Ako je $a \equiv b \pmod m$ i $c \equiv d \pmod m$ tada je $a + c \equiv b + d \pmod m$ i $a - c \equiv b - d \pmod m$.*

Dokaz. S obzirom na definiciju relacije kongruencije, postoje celi brojevi u i v takvi da je $a = b + mu$, $c = d + mv$.
Sabiranjem, odnosno oduzimanjem prethodne dve jednačine, dobijamo:

$$a + c \equiv b + d + m(u + v) \quad i \quad a - c \equiv b - d + m(u - v),$$

a to je

$$a + c = b + d \pmod m \quad i \quad a - c = b - d \pmod m. \ \blacksquare$$

Prethodno tvrđenje može se uopštiti.

Teorema 3.4 *Ako su $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ i $m \neq 0$ celi brojevi tada iz relacije*

$$a_1 \equiv b_1,\ a_2 \equiv b_2, \ldots, a_n \equiv b_n \pmod m$$

sledi

$$a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod m.$$

Dokaz. U dokazu ove teoreme koristićemo teoremu 3.3 i princip matematičke indukcije. Tvrđenje je tačno za $n = 2$ jer na osnovu prethodne teoreme i relacije

$$a_1 \equiv b_1 \pmod m \quad i \quad a_2 \equiv b_2 \pmod m$$

sledi

$$a_1 + a_2 \equiv b_1 + b_2 \pmod m.$$

Neka je tvrđenje tačno za $n - 1$, dokažimo da važi i za n.

Ako je tvrđenje tačno za $n - 1$ sledi da iz

$$a_1 \equiv b_1,\ a_2 \equiv b_2,\ \ldots,\ a_{n-1} \equiv b_{n-1} \pmod m$$

važi

$$a_1 + a_2 + \ldots + a_{n-1} \equiv b_1 + b_2 + \ldots + b_{n-1} \pmod m.$$

Ako je pored toga $a_n \equiv b_n \pmod m$ iz prethodne dve relacije, na osnovu prethodne teoreme, sledi da je
$a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod m$. ■

Teorema 3.5 *Ako su a, b, c i $m \neq 0$ celi brojevi, tada iz relacije*

$$a \equiv b \pmod m$$

sledi

$$ac \equiv bc \pmod m,$$

a takođe i

$$ac \equiv bc \pmod{mc}.$$

Dokaz. Iz relacije $a \equiv b \pmod m$ sledi da $m \mid a - b$. Odavde proizilazi da $m \mid (a - b)c$, tj. $m \mid ac - bc$ to je $ac \equiv bc \pmod m$ što je i trebalo dokazati.
Iz $m \mid a - b$ takođe je $mc \mid ac - bc$, a odavde sledi da je
$ac \equiv bc \pmod{mc}$. ■

Posledica. *Ako je $a \equiv b \pmod m$ tada je $-a \equiv -b \pmod m$.*

Teorema 3.6 *Za cele brojeve* a, b, c, d *i* $m \neq 0$ *iz relacije*

$$a \equiv b \pmod m \quad i \quad c \equiv d \pmod m$$

sledi

$$ac \equiv bd \pmod m .$$

Dokaz. Na osnovu prethodne teoreme važi

$$ac \equiv bc \pmod m \quad i \quad bc \equiv bd \pmod m,$$

a odavde zbog tranzitivnosti relacije kongruencije dobijamo

$$ac \equiv bd \pmod m. \quad \blacksquare$$

I ovo tvrđenje se može uopštiti.

Ako su $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ *i* $m \neq 0$ celi brojevi tada iz

$$a_1 \equiv b_1, \quad a_2 \equiv b_2, \dots, a_n \equiv b_n \pmod m$$

sledi $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod m$.

Tvrđenje se može dokazati matematičkom indukcijom.

Kao neposredna posledica ovog tvrđenja dobija se da iz

$$a \equiv b \pmod m$$

sledi

$$a^n \equiv b^n \pmod m,$$

gde je n prirodan broj, poslednja relacija važi i za $n = 0$, jer je

$$1 \equiv 1 \pmod m.$$

Primer 3.1 Koristeći prethodna tvrđenja odrediti ostatak koji se dobija deljenjem broja 3^{100} *brojem* 13.

Kako je $3 \equiv 3 \pmod{13}$ dobija se $3^3 \equiv 27 \pmod{13}$.

Kako je $27 \equiv 1 \pmod{13}$ takođe je $3^3 \equiv 1 \pmod{13}$.

Odavde je $(3^3)^{33} \equiv 1^{33} \pmod{13}$, odnosno $3^{99} \equiv 1 \pmod{13}$.

A kako je $3^{99} \cdot 3 \equiv 1 \cdot 3 \pmod{13}$ tj. $3^{100} \equiv 3 \pmod{13}$.

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

Teorema 3.7 *Ako je*

$$f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$$

polinom sa celim koeficijentima c_i, $i = 0,1,2,\ldots,n$, *tada iz relacije* $a \equiv b \pmod{m}$ *sledi*

$$f(a) \equiv f(b) \pmod{m}.$$

Dokaz. Iz $a \equiv b \pmod{m}$, sledi $a^i \equiv b^i \pmod{m}$, i $c_i a^i \equiv c_i b^i \pmod{m}$, $i = 0, 1, 2, \ldots, n$.

Takođe, prema tvrđenju 3.4 sledi

$$c_0a^n + c_1a^{n-1} + \ldots c_n \equiv c_0b^n + c_1b^{n-1} + \ldots + c_n \pmod{m},$$

tj.

$$f(a) \equiv f(b) \pmod{m}. \blacksquare$$

Teorema 3.8 *Ako je* $a \equiv b \pmod{m}$ *i* $d \mid m$, *tada je*

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

Dokaz. Ako je $a \equiv b \pmod{m}$, tada je $m \mid b - a$. Kako $d \mid m$ iz prethodne relacije sledi da $d \mid b - a$, tj. $a \equiv b \pmod{d}$. $\blacksquare$

Teorema 3.9 *Ako je* $a \equiv b \pmod m$ *i ako* $c|a$ *i* $c|b$, *tada je*

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

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

Dokaz. Iz relacije $a \equiv b \pmod m$ sledi $m|a - b$, a isto tako i

(1) $$\frac{m}{d} \mid \frac{c}{d}\ \frac{b-a}{c}\ .$$

Međutim, zbog $NZD(c,\ m) = d$ tada je $NZD\left(\frac{c}{d},\ \frac{m}{d}\right) = 1$.

Prema tome iz relacije *(1)* sledi da $\frac{m}{d} \mid \frac{a-b}{c}$
tj.

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

Ako je $NZD(m,\ c) = 1$ iz $a \equiv b \pmod m$ sledi

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

Preciznije rečeno, ako je $NZD(m,\ c) = 1$, tada se iz $ca_1 \equiv cb_1 \pmod m$ dobija $a_1 \equiv b_1 \pmod m$.

U slučaju da $c \mid m$, tada je $NZD(c, m) = c$, pa je $\frac{a}{c} \equiv \frac{b}{c} \left(mod\ \frac{m}{c}\right)$.

Iz prethodnog vidi se da se „skraćivanje“ kod kongruencije ne može uvek izvesti.

Primer 3.2 Iz relacije $42 \equiv 84 \pmod 6$ „skraćivanjem“ sa 7 dobija se $6 \equiv 12 \pmod 6$ što je tačno. Međutim, ako bi se izvršilo skraćivanje sa 14, dobija se rezultat $3 \equiv 6 \pmod 6$ što je netačno. Ovo je posledica činjenice da je $(14, 6) = 2$, pa je tačno da $3 \equiv 6 \pmod 3$. Δ

Teorema 3.10 *Ako je:* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$ *tada je* $a \equiv b \pmod{M}$ *gde je* $M = [m_1, m_2, \ldots, m_k]$ *najmanji zajednički sadržilac brojeva* $m_1, m_2, \ldots, m_k$.

Dokaz. Iz uslova teoreme sledi

$m_1 \mid a - b$, $m_2 \mid a - b$, ..., $m_k \mid a - b$,

a odavde

$[m_1, m_2, \ldots, m_k] \mid a - b$,

tj.

$a \equiv b \pmod{M}$ što je i trebalo dokazati. ■

4 Klase ostataka

4.1 Klase ostataka po datom modulu

Definicija 4.1 *Skup svih brojeva kongruentnih broju a po modulu $m \neq 0$ naziva se* ***klasa po modulu m****. Ovu klasu obeležavaćemo sa* $a_{(m)}$.

Teorema 4.1 *Klasa $a_{(m)}$ predstavlja skup brojeva $x = a + mt$, $(t = 0, \pm 1, \pm 2, \ldots)$.*
Ova činjenica se može izraziti i ovako:

$$a_{(m)} = \{\ldots, a - 2t, a - t, a, a + t, a + 2t, \ldots\}.$$

Kako je relacija kongruencije po modulu m relacija ekvivalencije, $a_{(m)}$ predstavlja klasu ekvivalencije, koju nazivamo ***klasa kongruencije po modulu m****.*

Teorema 4.2 *Klase $a_{(m)} = b_{(m)}$ ako i samo ako je $a \equiv b \pmod m$.*

Za svako $x \in a_{(m)}$ važi da je $x \equiv a \pmod m$, a tada je $x_{(m)} = a_{(m)}$.

Teorema 4.3 *Klase $a_{(m)}$ i $b_{(m)}$ su ili jednake ili disjunktne.*
Uvek važi ili $a \equiv b \pmod m$ ili $a \not\equiv b \pmod m$.

Teorema 4.4 *Dva cela broja imaju isti ostatak pri deljenju sa m, ako i samo ako pripadaju istoj klasi po modulu m.*

Dokaz. Prema teoremi 3.1 dva cela broja a i b imaju iste ostatke pri deljenju sa m ako i samo ako je $a \equiv b \pmod m$. Međutim, ova relacija važi ako i samo ako a i b pripadaju istoj klasi kongruencije po modulu m. Dakle brojevi a i b imaju iste ostatke pri deljenju sa m ako i samo ako pripadaju istoj klasi. ■

Teorema 4.5 *Ostatak r, dobijen deljenjem a sa m, je najmanji nenegativan broj klase $a_{(m)}$.*

Dokaz. Kako je r ostatak dobijen deljenjem a sa m, to je $a \equiv r \ (mod\ m)$, odakle sledi da je $r \in a_{(m)}$, tj. $r_{(m)} = a_{(m)}$.

Dakle, elementi date klase su u obliku

$$x = r + mt, \quad t = 0, \pm 1, \pm 2, \ldots$$

Kako je $m > 0$, sledi x raste sa t. Kako je $0 \leq r < m$, lako se uočava da se najmanja nenegativna vrednost od x dobija za $t = 0$, tj. najmanji nenegativan element ove klase je r. ■

Teorema 4.6 *Relacija kongruencije po modulu m deli skup celih brojeva na m disjunktnih klasa po modulu m.*

Dokaz. Pošto je relacija kongruencije po modulu m relacija ekvivalencije, skup celih brojeva je njom podeljen na izvestan broj disjunktnih klasa. Kako ostataka pri deljenju nekog celog broja sa m ima tačno m, sledi da je broj klasa tačno m: $0_{(m)}, 1_{(m)}, \ldots, (m-1)_{m}$. ■

Ako je $m = 1$, tada postoji samo jedna klasa kongruencije po modulu m, a ta je skup svih celih brojeva.

Definisaćemo neke operacije sa klasama po modulu m.

Definicija 4.2 *Zbir $a_{(m)} + b_{(m)}$ dve klase ostataka po modulu m je klasa $(a + b)_{(m)}$, tj. $a_{(m)} + b_{(m)} = (a + b)_{(m)}$. Ova operacija naziva se sabiranjem klasa po modulu m.*

Na osnovu definicije, proizilazi da je skup klasa po modulu m zatvoren u odnosu na sabiranje. Lako se dokazuje da skup klasa po modulu m u odnosu na operaciju sabiranja zadovoljava uslove Abelove grupe.

4.2 Klase ostataka relativno proste sa modulom

Delilac klase $a_{(m)}$ je svaki broj koji deli sve njene elemente, a najveći takav broj je najveći delilac ove klase.

Teorema 4.7 *Svaki delilac klase* $a_{(m)}$ *je i delilac modula* m.

Dokaz. Neka je d delilac klase $a_{(m)}$. Ako je $x \in a_{(m)}$, tada je i $x + m \in a_{(m)}$, pa $d \mid x$ i $d \mid x + m$. Iz prethodnoga sledi da d deli razliku $d \mid (x + m) - x$, tj. $d \mid m$ što je i trebalo dokazati. ■

Teorema 4.8 *Skup delilaca klase* a_m *i skup zajedničkih delilaca klase* a_m *i modul* m *poklapaju se. Najveći delilac klase* $a_{(m)}$ *je* $NZD(x, m)$, *gde je* x *proizvoljan element od* $a_{(m)}$.

Dokaz. Svaki zajednički delilac klase $a_{(m)}$ je, prema prethodnoj teoremi, takođe i delilac modula m. Međutim, svaki zajednički delilac klase $a_{(m)}$ i modula m, je delilac i klase $a_{(m)}$. Odavde sledi da skup delilaca klase $a_{(m)}$ i skup zajedničkih delilaca klase $a_{(m)}$ i modula m sadrži iste elemente. Zaključujemo, najveći delilac klase $a_{(m)}$ i najveći zajednički delilac klase $a_{(m)}$ i modula m jednaki su. ■

Definicija 4.3 *Klasa* $a_{(m)}$ *je relativno prosta sa modulom* m *ako je* $(a, m) = 1$.

S obzirom na prethodnu teoremu, klasa $a_{(m)}$ *je relativno prosta sa modulom* m *ako i samo ako je njen najveći zajednički delilac* 1.

4.3. Potpun sistem ostataka

Prethodna izlaganja omogućuju definisanje novih pojmova kao i stavove koji se odnose na njih.

Definicija 4.4 *Neka je* $0_{(m)}$, $1_{(m)}$, ..., $(m-1)_{(m)}$ *skup klasa po modulu* m. *Svaki skup celih brojeva* $x_1, x_2, \dots, x_m$, $x_i \in (i-1)_{(m)}$, $i = 1, 2, 3, \dots, m$, *naziva se potpun sistem ostataka po modulu* m.

Iz definicije sledi da je broj ostataka potpunog sistema po modulu m upravo m.

Kako je $i \in i_{(m)}$ $i = 0,1,2,\dots,(m-1)$, skup brojeva $0,1,2, \dots, m-1$ predstavlja potpun sistem ostataka po modulu m, i to ***potpun sistem najmanjih nenegativnih ostataka***.

Potpun sistem ***najmanjih pozitivnih ostataka*** po modulu m je

$$1,\ 2,\ 3,\ \dots,\ m.$$

Potpun sistem ***najmanjih ostataka po apsolutnoj vrednosti*** po modulu $m > 1$ je za m parno

$$-\frac{m}{2}+1; -\frac{m}{2}+2, \dots, -1, 0, 1, \dots \frac{m}{2},$$

a za m neparno

$$-\frac{m-1}{2}, -\frac{m-1}{2}+1, \dots, -1, 0, 1, \dots, \frac{m-1}{2}.$$

Primer 1 Potpun sistem nenegativnih ostataka po modulu 12 je skup brojeva

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,$$

a potpun sistem najmanjih pozitivnih ostataka je

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12.$$

Potpun sistem najmanjih ostataka po apsolutnoj vrednosti je

$$-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6.\ \Delta$$

Teorema 4.9 Skup od m celih brojeva predstavlja potpun sistem ostataka po modulu m, ako i samo ako ne sadrži nijedan par međusobno kongruentnih brojeva po modulu m.

Dokaz. Pošto dva elementa potpunog sistema ostataka po modulu m, pripadaju različitim klasama, oni su nekongruentni po modulu m. Prema tome, potpun sistem ostataka po modulu m ne sadrži nijedan par međusobno kongruentnih elemenata po modulu m.
Obratno, ako u skupu od m celih brojeva nema nijedan par međusobno kongruentnih elemenata, onda svaki od njegovih elemenata pripada jednoj klasi po modulu m. Prema definiciji (4.4) ovaj skup predstavlja potpun sistem ostataka po modulu m. ■

Teorema 4.10 *Neka su $a,\ m$ i b proizvoljni celi brojevi pri čemu je $(a, m) = 1$. Ako je $x_1, x_2, \dots, x_m$ potpun sistem ostataka po modulu m, tada je i skup brojeva*

$$ax_i + b, \quad i = 1, 2, \dots, m$$

potpun sistem ostataka.

Dokaz. Prema prethodnoj teoremi dovoljno je dokazati da su svaka dva broja iz skupa $ax_i + b,\ i = 1, 2, \dots, m$ međusobno nekongruentni po modulu m. Ako pretpostavimo da postoji $ax_i + b \equiv ax_j + b \pmod m$ za $i \neq j$, dobija se i $ax_1 \equiv ax_j \pmod m$, a odavde zbog $(a_i, m) = 1$ sledi $x_i \equiv x_j \pmod m$. Kako su x_i i x_j dva različita elementa potpunog sistema ostataka po modulu m, to je u kontradikciji sa uslovom teoreme. Dakle, skup

$$ax_i + b,\ i = 1,\ 2, \dots,\ m,$$

predstavlja potpun sistem ostataka po modulu m. ■

Teorema 4.11 *Neka je* $M = m_1 m_2 \dots m_r$, $M_i = \frac{M}{m_i}$ *gde su* m_i, $i = 1, 2, \dots, r$, *celi brojevi za koje važe relacije* $(m_i, m_j) = 1$, $i \neq j$, $i, j = 1, 2, \dots, r$. *Ako je skup brojeva* x_{1k_i} $k_i = 1, 2, \dots, m_i$, *potpun sistem ostataka po modulu* m_i, *tada je skup brojeva*

(4.1)

$$M_1 x_{1k_1} + M_2 x_{2k_2} \dots M_r x_{rk_r}, k_i = 1, 2, \dots, m_i, \qquad i = 1, 2, \dots, r,$$

potpun sistem ostataka po modulu m.

Dokaz. Brojeva oblika

(4.2)

$$M_1 x_{1k_1} + M_2 x_{2k_2} + \dots + M_r x_{rk_r}, \quad k_i = 1, 2, \dots, m_i, \quad i = 1, 2, \dots, r,$$

ima $m_1 m_2 \cdots m_r = M$. Kao i u prethodnoj teoremi, dovoljno je pokazati da među ovih M brojeva nema nijedan par međusobno kongruentnih brojeva po modulu M. Pretpostavimo suprotno, tj. da postoje dva broja iz skupa *(4.2)* za koje važi

(4.3)

$$M_1 x_{1k_1} + M_2 x_{2k_2} + \dots + M_r x_{k_r} \equiv M_1 x_{k_1}' + M_2 x_{k_2}' + \dots + M_r x_{k_r}' \pmod{m},$$

$$1 \leq k_i \leq m_i, \qquad 1 \leq k_i' \leq m_i, \qquad i = 1, 2, \dots, r_s$$

pri čemu postoji bar jedan par različitih brojeva

$$x_{sk_s}, x_{sk_s'}, \qquad 1 \leq s \leq r, \qquad 1 \leq k_s, \qquad k_s' \leq m_s.$$

Pošto ovi brojevi pripadaju istom sistemu ostataka, sledi da je

(4.4)

$$x_{sk_s} \not\equiv x_{sk_s'} \pmod{m_s}.$$

Kako $m_s \mid M$, iz *(4.3)* sledi

$$M_1x_{1k_1} + M_2x_{2k_2} + \ldots + M_rx_{rk_r} \equiv M_1x_{1k_1'} + M_2x_{2k_2'} + \cdots + M_rx_{rk_r}(mod\ m_s)$$

a kako je $M_i \equiv 0\ (mod\ m_s)$, za svako $i \neq s$ sledi

(4.5)

$$M_sx_{sk_s} \equiv M_sx_{sk_s'}\ (mod\ m_s).$$

Kako je za svako $i \neq s$, $NZS(m_s, m_i) = 1$, takođe važi $NZS(m_s, M_s) = 1$. Iz prethodnih uslova i kongruencije dobijamo

$$x_{sk_s} \equiv x_{sk_s'}\ (mod\ m_s),$$

što je u kontradikciji sa (*5.4)*.
Prema tome ne postoji nijedan par brojeva skupa *(4.2)* koji su međusobno kongruentni. Dakle, skup *(4.2)* predstavlja potpun sistem ostataka po modulu *m*. ■

Primer 5.2 Ako je $(a, b) = 1$, $x_1, x_2, \ldots, x_b$ potpun sistem ostataka po modulu b, $y_1, y_2, \ldots, y_a$ potpun sistem ostataka po modulu a, tada skup brojeva

$$ax_i + by_j + c, \qquad i = 1, 2, \ldots, b, \qquad j = 1, 2, \ldots, a,$$

gde je c proizvoljan ceo broj, predstavlja potpun sistem ostataka po modulu ab.

Na primer, pošto je $(6, 7) = 1$, potpun sistem ostataka po modulu *42* je skup brojeva

$$6x + 7y + 3, \quad x = 0, 2, \ldots, 6, \quad y = 0, 1, \ldots, 5,$$

jer su skupovi brojeva

$$0, 1, 2, 3, 4, 5, \qquad 0, 1, 2, 3, 4, 5, 6$$

potpuni sistemi ostataka po modulu *6*, odnosno *7*. Naravno da se mesto njih mogu uzeti i drugi potpuni sistemi ostataka po istim modulima. Δ

4.4 Redukovan sistem ostataka

Definicija 5.2 *Skup svih elemenata potpunog sistema ostataka po modulu m, koji su relativno prosti sa modulom m, naziva se* ***redukovan sistem ostataka ili sveden sistem ostataka****.*

Primer. Redukovan sistem ostataka po modulu *12* je: *1, 5, 7* i *11*.

Teorema 4.12 *Neka su*

(4.6)

$$((a_1)_{(m)},\ (a_2)_m, \dots, (a_{\varphi(m)})_{(m)})$$

sve klase ostataka po modulu m, relativno proste sa modulom m. Skup brojeva $x_1, x_2, \dots, x_{\varphi(m)}$, $x_i \epsilon (a_i)_{(m)}$, $i = 1, 2, \dots, \varphi_{(m)}$ *je redukovan sistem ostataka.*

Dokaz. Kako su klase

(4.7) $$(a_1)_{(m)}, (a_2)_{(m)}, \dots, (a_{\varphi(m)})_m$$

jedine klase relativno proste sa *m*, brojevi $x_1, x_2, \dots, x_{\varphi(m)}$ zaista predstavlja redukovan sistem ostataka.
Kako među *m* klasa ostataka po modulu *m* ima $\varphi(m)$ klasa relativno prostih sa modulom *m*, broj elemenata redukovanog sistema ostataka po modulu *m* je $\varphi(m)$. ■

Teorema 4.13 *Svaki skup celih brojeva* $x_1, x_2, \dots, x_{\varphi(m)}$, *relativno prostih sa m, ako ne sadrže nijedan par kongruentnih brojeva po modulu m, predstavlja redukovan sistem ostataka po modulu m.*

Dokaz. Ako među brojevima x_i, $i = 1, 2, \dots, \varphi(m)$ nema kongruentnih po modulu *m*, ovi brojevi pripadaju raznim klasama ostataka po modulu *m*. Međutim pošto su oni relativno prosti sa modulom *m*, tada svaki od njih pripada jednoj i samo jednoj klasi po modulu *m* relativno prostoj sa modulom *m*.
Prema prethodnoj teoremi, ovaj skup brojeva zaista predstavlja redukovan sistem ostataka po modulu *m*. ■

Teorema 4.14 *Neka su a i m > 1 celi relativno prosti brojevi. Ako je*

(4.8)

$$x_1, x_2, \dots, x_{\varphi(m)}$$

redukovani sistem ostataka po modulu m, tada je skup brojeva

(4.9)

$$ax_1, ax_2, \dots, ax_{\varphi(m)}$$

redukovan sistem ostataka.

Dokaz. Pošto je skup $x_1, x_2, \dots, x_{\varphi(m)}$ redukovan sistem ostataka po modulu *m*, tada je

$$(x_i, m) = 1, \quad i = 1, 2, \dots, \varphi(m).$$

Po pretpostavci teoreme je *(a, m) = 1,* pa je takođe

$$(ax_i, m) = 1, \quad i = 1, 2, \dots, \varphi(m),$$

tj. svi brojevi skupa $ax_1, ax_2, \dots, ax_{\varphi(m)}$ su relativno prosti sa *m*. Takođe, među elementima skupa $ax_1, ax_2, \dots, a_{\varphi(m)}$ nema nijedan par međusobno kongruentnih brojeva po modulu *m*. Prema tome, na osnovu teoreme *(4.13)* skup $\varphi(m)$ brojeva skupa $ax_1, ax_2, \dots, a\varphi(m)$ predstavlja redukovan sistem ostataka po modulu *m*. ■

Teorema 4.15 *Neka je* $M = m_1 m_2 \dots m_r$, $M_i = M/m_i$, *gde su* m_i, $i = 1, 2, \dots, r$ *celi brojevi za koje važe relacije* $(m_i, m_j) = 1$, $i \neq j$, $i, j = 1, 2, \dots, r$. *Ako je skup brojeva* x_{ik_i} $k_i = 1, 2, \dots, \varphi(m_i)$, $(i = 1, 2, \dots, r)$, *redukovan sistem ostataka po modulu* m_i, *tada je skup brojeva*

$$M_1 x_{1k_1} + M_2 x_{2k_2} + \cdots + M_r x_{rk_r}, \quad k_i = 1, 2, \dots, \varphi(m_i), \quad i = 1, 2, \dots, r,$$

redukovan sistem ostatatka po modulu M.

Dokaz. Brojeva oblika

(4.10) $M_1x_{1k_1} + M_2x_{2k_2} + \ldots + M_rx_{rk_r} = \sum_{i=1}^{r} M_ix_{ik_i}$

$$k_i = 1, 2, \ldots, \varphi(m_i), \qquad i = 1, 2, \ldots,$$

ima $\varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_r)$.
kako prema pretpostavci važi $(m_i, m_j) = 1, \quad i \neq j,$ sledi na osnovu multiplikativnosti Eulerove funkcije da je

$$\varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_r) = \varphi(M).$$

Dakle, broj elemenata skupa *(4.10)* je $\varphi(M)$.
Potrebno je još pokazati da među elementima skupa *(4.10)* nema međusobno kongruentnih po modulu M. Pokazaćemo da je svaki element skupa *(4.10)* relativno prost sa M. S obzirom na definiciju broja M_i sledi da je

(4.11) $NZS(M_i, m_s) = m_s, \quad i \neq s, \quad NZS(M_s, m_s) = 1.$

Svi elementi redukovanog sistema po modulu m_s su relativno prosti sa m_s, te je $(x_{sk_s}, m_s) = 1$. Iz *(4.11)* tada se dobija

$$NZS(M_ix_{ik_i}, m_s) = m_s, \quad i \neq s, \quad NZS(M_sx_{sk_s}, m_s) = 1,$$

te je

$$NZS(M_1x_{1k_1} + M_2x_{2k_2} + \cdots + M_rx_{rk_r}, m_s) = \\ = NZS(M_sx_{sk_s}, m_s) = 1, \qquad s = 1, 2, \ldots, r,$$

a odavde

$$NZS(M_1x_{1k_1} + M_2x_{2k_2} + \ldots + M_rx_{rk_r} + \ldots + M_rx_{rk_r}, M) = 1,$$

što je trebalo i dokazati. ■

5. Ojlerova teorema

5.1 Ojlerova funkcija

U prethodnoj glavi smo koristili pojam $\varphi(n)$ kao broj elemenata redukovanog sistema ostataka. Sada ćemo sa $\varphi(n)$ predstaviti važnu aritmetučku funkciju.

Definicija 5.1 *Za svaki prirodan broj n, sa* $\varphi(n)$ *označavamo broj prirodnih brojeva, koji nisu veći od n, a uzajamno su prosti sa n. Funkcija* $\varphi(n)$ naziva se ***Ojlerova funkcija*** *ili* ***Ojlerov indicator****. Nekoliko prvih vrednosti funkcije* $\varphi(n)$ *dato je u sledećoj tabeli.*

n	1	2	3	4	5	6	7	8	9	10	11	12	2011
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	2010

Teorema 5.1 *Ako su n i p prirodni brojevi i p prost broj, tada je*

$$\varphi(p^n) = p^{n-1}(p-1) = p^n\left(1-\frac{1}{p}\right).$$

Dokaz. Svaki od prirodnih brojeva od *1* do p^n ili je deljiv sa *p* ili je uzajamno prost sa *p*. Broj onih koji su deljivi sa *p* jednak je p^{n-1}. Dakle, onih koji su relativno prosti sa *p*, prema tome i sa p^n, ima $p^n - p^{n-1} = p^n(1 - \frac{1}{p})$. ■

Teorema 5.2 *Funkcija* φ *je multiplikativna tj. važi*

(5.1) $$\varphi(mn) = \varphi(m)\,\varphi(n).$$

Dokaz. Neka su *m* i *n* uzajamno prosti brojevi. Znamo da je broj *a* uzajamno prost sa proizvodom *mn* ako i samo ako je uzajamno prost i

sa m i sa n. Da bi smo izračunali koliko među brojevima $1, 2, 3, \ldots, mn$ ima uzajamno prostih i sa m i sa n, napisaćemo brojeve u obliku tabele:

1	2	.	.	.	k	.	.	.	m
$m + 1$	$m + 2$	.	.	.	$m + k$	.	.	.	2m
$2m + 1$	$2m + 2$	.	.	.	$2m + k$	.	.	.	3m
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
$(n - 1)m + 1$	$(n - 1)m + 2$	.	.	.	$(n - 1)m + k$	.	.	.	$(n - 1)m + m$

U k-toj koloni svi brojevi imaju oblik $am + k$, $(a = 0,1, 2, \ldots, (n - 1))$; dakle svi su oni kongruentni po modulu m, tj. svi su oni uzajamno prosti sa m ako i samo ako je k uzajamno prost sa m. U prvoj vrsti tabele ima $\varphi(m)$ brojeva uzajamno prostih sa m, što znači da u tabeli ima $\varphi(m)$ kolona koje sadrže samo sumu brojeva uzajamno prosih brojeva sa m, dok ostali brojevi u tablici nisu uzajamno prosti sa m.

Sada ćemo da utvrdimo koliko u svakoj koloni ima brojeva uzajamno prostih sa n. Posmatrajmo brojeve u k-toj koloni. Među njima ne postoje dva kongruentna broja po modulu n, jer ako postojeje, za $0 \leq s < t \leq n - 1$,

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

tada je

$$sm \equiv tm \pmod{n}$$

a kako su m i n uzajamno prosti, to je

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

Brojevi s i t pripadaju potpunom sistemu ostataka $0, 1, 2, \ldots, (n - 1)$ pa iz poslednje kongruencije sledi $s = t$.

Iz poslednjeg razmatranja sledi da n brojeva, koji pripadaju istoj koloni tablice, obrazuju potpun sistem ostataka po modulu n, a to znači da među 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 da je $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. ■

Teorema 5.3 *Ako je*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

tada je

$$\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Dokaz. Sledi na osnovu prethodne teoreme. ■

5.2 Ojlerova teorema

Teorema 5.5 (Ojler) *Ako su a i m uzajamno prosti brojevi, tada je*

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

Dokaz. Ako su a i m uzajamno prosti brojevi tj. $(a, m) = 1$ i ako je

(5.3) $$r_1, r_2, \dots, r_{\varphi(m)}$$

redukovan (sveden) sistem ostataka po modulu m, tada je i

$$ar_1, ar_2, \dots, ar_{\varphi(m)}$$

sveden sistem ostataka po modulu m. Brojevi iz skupa *(5.3)* su kongruentni nekim redom brojevima iz skupa *(5.2)*, tj.

$$\begin{aligned} ar_1 &\equiv r_{i_1} \pmod m \\ ar_2 &\equiv r_{i_2} \pmod m \\ &\vdots \\ ar_{\varphi(m)} &\equiv r_{i_{\varphi(m)}} \pmod m \end{aligned}$$

za neku permutaciju $(i_1, i_2, \dots, i_{\varphi(m)})$ elemenata $1, 2, \dots, \varphi(m)$. Množenjem dobijamo da je

$$a^{\varphi(m)} r_1 r_2 r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} (mod\ m)$$

i posle skraćivanja (šta možemo uraditi jer su $r_1, r_2 \dots r_{\varphi(m)}$ uzajamno prosti sa m), dobijamo

$$a^{\varphi(m)} \equiv 1 \pmod m. \blacksquare$$

Neposredna posledica Ojlerovog stava je Fermaov stav poznat pod nazivom ***Mala Fermaova teorema.***

Posledica 5.5a (Ferma) *Ako je p prost broj i (a, p) = 1, tada je*

$$a^{p-1} \equiv 1 \pmod p.$$

Posledica 5.5 b *Ako je p prost broj i a proizvoljan ceo broj, tada je*

$$a^p \equiv a \pmod p.$$

Primer 5.1

a) $5^{10} \equiv 1 \pmod{11}$, jer je *11* prost broj, uzajamno prost sa *5*, posledica *5.5 a*.

b) $1000^{2010} \equiv 1 \pmod{2011}$ jer je *2011* prost broj i uzajamno prost sa *1000*, posledica *5.5 a.*

c) $2^8 \equiv 1 \pmod{15}$ jer je $\varphi(15) = 8$, ali je $2^4 \equiv 1 \pmod{15}$. Interesantno. Δ

Definicija 5.2 *Najmanji od prirodnih brojeva t za koji važi* $a^t \equiv 1$ *naziva se* ***red broja*** *a po modulu m i označava se sa* $r_m(a)$.

Teorema 5.6 *Red* $r_m(a)$ *broja a po modulu m postoji, ako i samo ako su brojevi a i m uzajamno prosti.*

Dokaz. Na osnovu Ojlerove teoreme. ■

Teorema 5.7 *Ako je t red broja a po modulu m i ako je* $a^s \equiv 1 \pmod{m}$, *tada t | s. Specijalno t |* $\varphi(m)$.

Dokaz. Neka je $a^s \equiv 1 \pmod{m}$. Ako pretpostavimo suprotno tj. $s = tq + r$, $0 < r < t$, tada bi iz $a^s = (a^t)^q a^r \pmod{m}$ sledilo da $a^r \equiv 1 \pmod{m}$, što je u suprotnosti sa minimalnosti poretka *t*. Obratno, ako je $s = tq$, tada je $a^s = (a^t)^q \equiv 1 \pmod{m}$. ■

Posledica 5.7 a *Ako je t red broja a po modulu m tada je*

$$a^x \equiv a^y \pmod{m}$$

ako i samo ako $x \equiv y \pmod{t}$.

Dokaz. Neka je na primer $x \geq y$. Ako je $a^x \equiv a^y \pmod{m}$, tada zbog $(a, m) = 1$, važi $a^{x-y} \equiv 1 \pmod{m}$ pa iz prethodnog tvrđenja sledi $t \mid x - y$.
Obratno, iz $x \equiv y \pmod{t}$ sledi $x = y + ta$, $a \geq 0$ i $a^x = a^{y+tx} = a^y (a^t)^{\propto} \equiv a^y \pmod{t}$. ■

Definicija 5.3 *Ako je red broja a po modulu m jednak* $\varphi(m)$, *broj a se naziva* ***primitivni koren*** *po modulu m.*

Primer 5.2 Lako se proverava da je $\varphi(22) = 10$. Zato redovi po modulu *22* brojeva (koji su uzajamno prosti sa *22*) mogu biti samo *1, 2, 5* i *10.* Tako utvrđujemo na primer red broja *3* jednak je *5* jer je $3^1, 3^2 \not\equiv 1 \pmod{22}, 3^5 \equiv 1 \pmod{22}$), a red broja *7* je *10* jer je $7^1, 7^2, 7^5 \not\equiv 1 \pmod{22}$, a $7^{10} \equiv 1 \pmod{22}$. Δ

Primer 5.3 a) Posmatrajmo ostatke *1, 2, 3, -3, -2, -1* po modulu *7* ($\varphi(7) = 6$).

Rešenje. Lako se proverava da su njihovi redovi po modulu *7* jednaki *1, 3, 6, 3, 6, 2* redom. Brojevi *3* i *-2* su primitivni koreni po modulu *7*.

b) Ostaci po modulu *8* koji imaju red su: *1, 3, 5* i *7*. Nijedan od njih nije primitivan koren, jer lako je proveriti da je red svakog od njih (sem *1*) jednak *2*. Δ

Primer 5.4 Naći ostatke pri deljenju broja 317^{259} sa 15.

Rešenje. $317 \equiv 2\ (mod\ 15)$; $317^2 \equiv 4\ (mod\ 17)$;
$317^3 \equiv 8\ (mod\ 15)$; $317^4 \equiv 1\ (mod\ 15)$;
$259 \equiv 3\ (mod\ 4) \Rightarrow 317^{259} \equiv 317^3 \equiv 8\ (mod\ 15)$. Δ

Teorema 5.8 *Jedini brojevi koji imaju primitivne korene su brojevi 2, 4 i brojevi oblika* p^α, $2p^\alpha$ *(p neparan prost broj).*

Prvo ćemo dokazati dva pomoćna tvrđenja.

Lema 5.1 *Za svaki prirodan broj n važi* $\sum \varphi(d) = n$.

Dokaz. Tvrđenje odmah sledi iz činjenice da je, za proizvoljno *d | n* $\varphi(d)$ upravo jednako broju elemenata $a \in \{1, 2, \dots, n\}$ takvih da je *(a, n) = n/d.* ■

Lema 5.2 *Neka je p prost neparan broj i d | p - 1, tada je broj elemenata skupa {1, 2, ... , p - 1} jednak* $\varphi(d)$.

Dokaz. Tvrđenje ćemo dokazati potpunom indukcijom po *d*. Za *d = 1* ovo je očigledno. Pretpostavimo da je ono tačno za sve elemente *e* manje od *d* i odredimo broj elemenata skupa *{1, 2, ... , p - 1}* čiji je poredak jednak *d*.

Posmatrajmo kongruenciju:

(5.4) $$x^d \equiv 1\ (mod\ p).$$

Kako je

$$(x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \dots + x^d + 1) =$$

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

imaju najviše d, odnosno $p - 1 - d$ rešenja, u oba slučaja mora da važi jednakost. Dakle *(5.4)* ima tačno d rešenja, i to su svi elementi čiji red po modulu p deli d. Među njima, po indukcijskoj pretpostavci, tačno

$$\sum_{e<d} \varphi(e)$$

ima red manji od d, odakle sledi da elemenata reda d ima

$$d - \sum_{e<d} \varphi(e)$$

Da je ova razlika upravo jednaka $\varphi(d)$, sledi iz leme *(5.1)*. ■

Dokaz teoreme 5.8 Tvrđenje teoreme u slučaju prostog broja p je specijalan slučaj prethodne leme za $d = p - 1$. ■

Teorema 5.9 *Ako je a primitivan koren po modulu m, tada brojevi*

(5.5) $$1 = a^o,\ a,\ a^2, \ldots, a^{\varphi(m)-1}$$

obrazuju sveden sistem ostataka po modulu m.

Dokaz. Pošto skup *(5.5)* ima $\varphi(m)$ elemenata dovoljno je dokazati da ne postoje dva koja su kongruentna po modulu m. Pretpostavimo suprotno da postoje i i j takvi da je

$$a^i \equiv a^j \pmod{m},\quad 0 \le i < j < \varphi(m).$$

Tada je

$$a^{j-1} \equiv 1 \pmod{m},\quad 0 \le j - i < \varphi(m).$$

Suprotno pretpostavci da je a primitivan koren po modulu m. ■

Posledica 5.9 a Ako je p prost broj i a primitivan koren po modulu p, tada brojevi: $1, a, a^2, \dots, a^{p-1}$ obrazuju sveden sistem ostataka po modulu p.

Primer 5.5 *2* je primitivan koren modula *11* pa brojevi

$$1,\ 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9,\ 2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6\ (mod\ 11)$$

obrazuju sveden sistem ostataka po modulu *11*. Δ

Teorema 5.10 (Vilson) *Ako je p prost broj tada važi*

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

Dokaz. Tvrđenje je očigledno tačno za $p = 2$ ili $p = 3$. Neka je p prost broj veći od *3*. Tada je $1 \equiv 1\ (mod\ p)$; i takođe je $p - 1 \equiv -1\ (mod\ p)$.

Da bi smo dokazali teoremu dovoljno je dokazati da svaki broj k takav da je $2 \le k \le p - 2$, postoji tačno jedan broj l takav da je

$$kl \equiv 1\ (mod\ p), \qquad 2 \le l \le p - 2, \qquad k \ne l.$$

Zaista, ako je $k \in \{2, \dots, p - 2\}$, pošto je $(k, p) = 1$, skup

$$\{\ 0, k, 2k, \dots, (p-1)k\ \}$$

obrazuje potpun sistem ostataka po modulu p, i tačno jedan element iz ovog skupa (koji je različit od nule) je kongruentan *1* po modulu p.

Ako bi bilo $l = 1$, tada sledi da je $k \equiv 1\ (mod\ p)$ što je nemoguće.

Slično se dokazuje da ne može biti $l = (p - 1)$.

Najzad, ako bi bilo $k = l$, sledi da je $k^2 \equiv 1\ (mod\ p)$, tj. da $p \mid k - 1$ ili $p \mid k + 1$, odnosno $k \equiv 1\ (mod\ p)$ ili $k \equiv -1\ (mod\ p)$, što je nemoguće. ■

Važi tvrđenje obratno Vilsonovoj teoremi.

Teorema 5.11. *Ako je* $(p-1)! + 1 \equiv 0 \,(mod\, p)$, *tada je* n *prost broj.*

Dokaz. Pretpostavimo suprotno, tj. p ima prost delilac $q < p$, tada važi $q|(p-1)!$, ali tada $q \nmid (p-1)! + 1$, a samim tim i $q \nmid (p-1)! + 1$. Kontradikcija. ■

Primer 5.6 Dokazati da je prirodan broj n prost ako i samo ako $n \mid N$, gde je $N = \sum_{k=1}^{n-3} k \cdot k!$.

Rešenje. Kako je

$$k \cdot k! = k \cdot k! + k! - k! = k!\,(k+1) - k! = (k+1)! - k!,$$

to je

$$N = 1 \cdot 1! + 2 \cdot 2! + \cdots + (n-3)(n-3)!$$
$$N = (2! - 1!) + (3! - 2!) + \ldots + ((n-2)! - (n-3)!)$$
$$N = (n-2)! - 1.$$

Množenjem poslednje jednakosti sa $n-1$ dobijamo

$$(n-1)N = (n-1) \cdot (n-2)! - (n-1)$$

i dodavanjem obema stranama prethodne jednakosti n dobijamo

$$(n-1)N + n = (n-1)! + 1.$$

Na osnovu Vilsonove teoreme, broj n je prost ako i samo ako $n \mid N$, jer je $(n, n-1) = 1$. Δ

6. Kongruencije s jednom nepoznatom

6.1 Linearne kongruencije $ax \equiv b(mod\ m)$

Posmatrajmo linearnu kongruenciju

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

Njeno rešenje je svaki ceo broj x_0 takav da je $ax_0 \equiv b\ (mod\ m)$. Sledeća teorema daje potreban i dovoljan uslov da broj x_0 bude rešenje ove linearne kongruencije.

Teorema 6.1 *Broj x_0 je rešenje linearne kongruencije*

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

ako i samo ako postoji ceo broj y_0 takav da je (x_0, y_0) rešenje linearne Diofantove jednačine

$$ax - my = b.$$

Dokaz. Pretpostavimo da je x_0 rešenje kongruencije *(6.1)*. Tada postoji ceo broj y_0 takav da je

$$ax_0 - b = my_0.$$

Dakle, $ax_0 - my_0 = b$, što znači da je (x_0, y_0) rešenje Diofantove jednačine

$$ax - my = b.$$

Obratno, ako je (x_0, y_0) rešenje Diofantove jednačine $ax - my = b$, tj. $ax_0 - my_0 = b$, tada je $ax_0 - b = my_0$, odavde sledi da je

$$ax_0 \equiv b(mod\ m). \blacksquare$$

Sada se lako dokazuje tvrđenje, koje je parafraza tvrđenjima linearne Diofantove jednačine.

Teorema 6.2 *Linearna kongruencija*

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

ima rešenje ako i samo ako je $d \mid b$ *gde je* $d = NZD\ (a, m)$. *Broj različitih rešenja, ukoliko postoje, jednak je* $d = (a, m)$.

Dokaz. Ako je x_0 rešenje date kongruencije, tada je

(6.3) $$ax_0 \equiv b\ (mod\ m).$$

Pošto $NZD\ (a, m) \mid a$ takođe važi $a \equiv 0\ (mod\ NZD\ (a, m))$, zatim $ax_0 \equiv 0\ (mod\ NZD\ (a, m))$, a odavde i iz relacije *(6.3)* sledi $b \equiv 0\ (mod\ NZD\ (a, m))$, odnosno $NZD(a,m) \mid b$. Dakle, ako kongruencija ima rešenje tada $NZD=(a, m) \mid b$.

Obratno, pretpostavimo da $d \mid b$, gde je $d = (a, m)$ i stavimo da je

$$a = a_1 d; \quad m = m_1 d; \quad b = b_1 d;$$

pri čemu je $NZD\ (a_1, m_1) = 1$. Na osnovu osobina kongruncije sledi da je kongruencija *(6.2)* ekvivalentna kongruenciji

(6.4) $$a_1 x = b_1\ (mod\ m_1).$$

Kako je $0,1,2,\ldots,m - 1$ potpun sistem ostataka po modulu m_1 s obzirom da je $NZD\ (a_1, m_1) = 1$, i skup brojeva $0, a_1, 2a_1, \ldots, (m_1 - 1)a_1$ je potpun sistem ostataka po modulu m_1. Međutim, tada je broj b_1 kongruentan po modulu m_1, jednom i samo jednom od ovih ostataka – recimo ostatka $a_1 x_0\ (1 \leq x_0 \leq m_1)$. Dakle, dobijamo kongruenciju $a_1 x_0 \equiv b_1\ (mod\ m_1)$, odavde sledi

$$ax_0 \equiv b\ (mod\ m).$$

Tako da smo dokazali da, kada *(a, m)* | *b*, data kongruencija ima rešenje $x \equiv x_0 \ (mod\ m)$.

Ostalo je još da dokažemo drugi deo teoreme koji govori o broju rešenja kongruencije. Dokazaćemo prvo da kongruencija

$$a_1 x \equiv b_1 (mod\ m_1)$$

ima samo jedno rešenje, tj. da svi celi brojevi koji je zadovoljavaju pripadaju istoj klasi ostataka po modulu m_1. Ako su *x'* i *x''* dva rešenja ove kongruencije, tada važe relacije

$$a_1 x' \equiv b_1 (mod\ m_1), \quad a_1 x'' \equiv b_1\ (mod\ m_1)\ .$$

Odavde sledi da je $a_1 x' \equiv a_1 x'' (mod\ m_1)$, na osnovu teoreme o skraćivanju dobijamo

$$x' \equiv x''\ (mod\ m_1).$$

Dakle, sva rešenja kongruencije *(6.4)* pripadaju istoj klasi po modulu m_1. Neka je x_0 rešenje kongruencije *(6.4)* što znači da samo elementi klase $(x_0)_{m_1}$ zadovoljavaju tu kongruenciju. Isto tako svi elementi ove klase su rešenja kongruencije *(6.2)*. Međutim kongruencija po modulu $m = m_1 d$ deli klasu $(x_0)_{(m_1)}$ na d disjunktnih klasa.

$(x_0)_{(m)}, \ (x_0 + m_1)_{(m)}, \ldots , \ (x_0 + (d - 1)m_1)_{(m)}$.

Prema tome, različitih rešenja kongruencije *(6.2)* ima tačno *d*. Ako je rešenje kongruencije *(6.4)*

$$x \equiv x_0\ (mod\ \tfrac{m}{d}),$$

rešenja kongruencije *(6.2)* su

(6.5) $$x \equiv x_0 + k\tfrac{m}{d}\ \ (mod\ m), \quad k = 0, 1, 2, \ldots, d - 1$$ ■

Primer 6.1 Kongruencija

$$6x \equiv 9\ \ (mod\ 15)$$

ima tri rešenja jer je *NZD(6, 15) = 3* delilac broja *9*. Pošto je ona ekvivalentna kongruenciji

$$2x \equiv 3 \ (mod\ 5),$$

odredićemo prvo njeno rešenje. Izračunajmo vrednost kongruencije za najmanji nenegativan potpun sistem ostataka, tj. *0, 1, 2, 3, 4.*

$$2 \cdot 0 \not\equiv 3, \quad 2 \cdot 1 \not\equiv 3, \quad 2 \cdot 2 \not\equiv 3, \quad 2 \cdot 4 \equiv 3 \ (mod\ 5).$$

Dobili smo jedno rešenje

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

Na osnovu obrasca *(6.5)* rešenja date kongruencije su:

$$x \equiv 4, \quad x \equiv 9, \quad x \equiv 14 \ (mod\ 15). \ \Delta$$

Primer 6.2 Kongruencija

$$24x \equiv 40 \ (mod\ 18)$$

nema rešenja, jer *(24, 18) = 6* nije delilac broja *40*. Δ

Sledeći primeri pokazuju nešto drugačiji metod rešavanja.

Primer 6.3 Odrediti nekongruentna rešenja linearne kongruencije

$$64\,x \equiv 16 \ (mod\ 84) \ .$$

Rešenje kako je *NZD (64, 84) = 4* i *4 | 16*, imaćemo *4* nekongruentna rešenja po modulu *84*. Dati izraz je ekvivalentan izrazu

$$4x \equiv 1 \ (mod\ 21).$$

Dalje imamo

$$\begin{aligned} 4x &\equiv -20 \ (mod\ 21) \\ x &\equiv -5 \ (mod\ 21) \\ x &\equiv 16 \ (mod\ 21). \end{aligned}$$

Četiri nekongruentna rešenja sa

$$x \equiv 16\ (mod\ 84), \quad x \equiv 37\ (mod\ 84), \quad x \equiv 58\ (mod\ 84)$$
$$\text{i} \quad x \equiv 79\ (mod\ 84).\ \Delta$$

Primer 6.4 Rešiti kongruenciju

$$11x \equiv 25\ (mod\ 60).$$

Rešenje. Kako je *NZD(11, 60) = 1*, kongruencija ima tačno jedno nekongruentno rešenje. Rešenje x mora biti deljivo sa *5* jer je

$$11x = 25 + 60k,$$

za neki ceo broj k. Neka je $x = 5y$.
Tada je

$$11 \cdot 5y \equiv 25\ (mod\ 60).$$

Deljenjem dobijamo da je

$$\begin{aligned} 11y &\equiv 5\ (mod\ 12) \\ -y &\equiv 5\ (mod\ 12) \\ y &\equiv -5\ (mod\ 12) \\ y &\equiv 7\ (mod\ 12). \end{aligned}$$

Zato je $x \equiv 35\ (mod\ 60)$. Δ

Sledeća teorema, koja je posledica Ojlerove teoreme, ukazuje na još jedan način rešavanja linearnih kongruencija.

Teorema 6.3 *Ako je (a, m) = 1, tada je*

$$x \equiv ba^{\varphi(m)-1}\ (mod\ m)$$

rešenje kongruencije $ax \equiv b\ (mod\ m)$.

Dokaz. Prema Fermaovoj teoremi,

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

odakle je

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

Uvrstavajući umesto $a^{\varphi(m)}b$ umesto b u relaciji

$$ax \;\equiv\; ba^{\varphi(m)}\ (mod\ m)$$

dobijamo

$$x \;\equiv\; ba^{\varphi(m)-1}\ (mod\ m)$$

rešenje kongruencije $ax \;\equiv\; b\ (mod\ m)$. ■

Primer 6.5 Odrediti kongruentno rešenje linearne kongruencije $3x \equiv 20\ (mod\ 35)$,

Rešenje. Kako je *(3, 35) = 1* možemo primeniti prethodnu teoremu.

$$x \equiv\ 20 \cdot 3^{\varphi(35)-1}\ (mod\ 35),\ \text{tj.}$$
$$x \;\equiv\; 20 \cdot 3^{23}\ (mod\ 35)$$
$$x \;\equiv\; 30\ (mod\ 35). \quad \Delta$$

6.2 Sistemi linearnih kongruencija

Posmatrajmo sistem linearnih kongruencija

$$\begin{aligned} a_1x \;&\equiv\; b_1\ (mod\ m_1)\\ a_2x \;&\equiv\; b_2\ (mod\ m_2)\\ &\cdot\\ &\cdot\\ &\cdot\\ a_nx \;&\equiv\; b_n\ (mod\ m_n). \end{aligned}$$

Pod rešenjem tog sistema podrazumevaćemo ceo broj x_0 koji je rešenje svake kongruencije sistema.

Svaka kongruencija sistema određuje jednu klasu ostataka. Zato su rešenja sistema kongruencija, brojevi u preseku tih klasa. Svaka od

gornjih kongruencija može se zameniti ekvivalentnom kongruencijom koja određuje istu klasu ostataka. Sledeći primer pokazuje da se taj metod može efikasno koristiti u rešavanju sistema linearnih kongruencija.

Primer 6.6 Rešiti sistem kongruencija:

$$5x \equiv 7 \ (mod\ 12)$$
$$4x \equiv 12 \ (mod\ 14).$$

Rešavajući nezavisno prvu i drugu kongruenciju, dobijamo rešenja $x_0 \equiv 11\,(mod\ 12)$ i $x_0 \equiv 3 \ (mod\ 7)$. Zato je polazni sistem ekvivalentan sledećem.

$$x \equiv 11 \ (mod\ 12)$$
$$x \equiv 3 \ (mod\ 7).$$

Pretpostavimo da je x_0 rešenje prvog sistema. Tada možemo da pišemo

$$x_0 = 11 + 12s.$$

Zamenom u drugu kongruenciju, dobijamo

$$x_0 \equiv 11 + 12s \equiv 3 \ (mod\ 7)$$

odavde sledi da je

$$12s \equiv -8 \ (mod\ 7)$$
$$-2s \equiv -8 \ (mod\ 7)$$
$$s \equiv 4 \ (mod\ 7).$$

Kako je $s = 4 + 7t$ uvrstimo u izraz za x_0, dobijamo

$$x_0 = 11 + 12s = 59 + 84t.$$

Dakle, rešenje sistema kongruencija je

$$x_0 \equiv 59 \ (mod\ 84).$$

Uvrštavanjem u početni sistem, proveravamo da je to zaista rešenje, tj. opšte rešenje sistema je

$$x \equiv 59 \ (mod\ 84). \ \Delta$$

Teorema 6.4 *Sistem kongruencija*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

ima rešenje ako i samo ako je NZD (m, n) | (a - b). Ako je pri tome x_0 *jedno rešenje, tada je opšte rešenje toga sistema*

$$x \equiv x_0 \,(mod\ NZS\ (m,n)).$$

Dokaz. Ceo broj x_0 je rešenje gornjeg sistema kongruencija ako i samo ako postoji ceo broj k, takav da je

$$x_0 = a + km$$

i

$$a + km \equiv b \,(mod\ n).$$

Prema teoremi *(6.2)*, talav broj postoji ako i samo ako je

NZD (m, n) | (a - b).

Pretpostavimo sada da je *NZD (m, n) | (a - b)* i da je x_0 jedno rešenje sistema kongruencija. Za bilo koje drugo rešenje x_1 tog sistema je

$$x_1 \equiv a \equiv x_0 \pmod{m}$$

i

$$x_1 \equiv b \equiv x_0 \pmod{n}.$$

Dakle, $x_1 - x_0$ je zajednički sadržilac od m i n i prema tome je

NZS (m, n) | (x_1 *-* x_0*),*

odakle sledi

$$x_1 \equiv x_0 \left(mod\ NZS\ (m,n)\right).$$

Obratno, ako je $x_1 \equiv x_0 \left(mod\ NZS\ (m,n)\right)$, onda je očigledno

$$x_1 \equiv x_0 \equiv a \,(mod\, m)$$

i

$$x_1 \equiv x_0 \equiv b \;(mod\, n),$$

pa je x_n takođe rešenje sistema. Dakle, opšte rešenje je

$$x \equiv x_0 \;\big(mod\; NZS\,(m,n)\big).\ \blacksquare$$

Sledeće tvrđenje bilo je poznato kineskom matematičaru *Sun – Tse – u* u prvom veku nove ere, pa je poznato pod nazivom *Kineska teorema o ostacima.*

Teorema 6.5 (Kineska teorema) *Neka su $m_1, m_2, \ldots, m_n$ po parovima uzajamno prosti brojevi. Tada sistem kongruencija*

$$\begin{aligned} x &\equiv a_1 \,(mod\, m_1)\\ x &\equiv a_2 \,(mod\, m_2)\\ &\vdots\\ x &\equiv a_n \,(mod\, m_n). \end{aligned}$$

Ima tačno jedno rešenje po modulu $M = m_1 m_2 \ldots m_n$.

Dokaz. Neka je $M_i = \frac{M}{m_i}$, za $i = 1, 2, \ldots, n$.
Posmatrajmo n kongruenciju

$$M_i x \equiv 1 \,(mod\, m_i).$$

Kako je $NZD\,(M_i, m_i) = 1$, svaka od tih kongruencija ima jedinstveno rešenje $x \equiv x_i \;(mod\, m_i)$. Neka je

(6. 6) $$X \equiv M_1 x_1 a_1 + M_2 x_2 a_2 + \ldots + M_n x_n a_n \;(mod\, M).$$

Uvrštavanjem X umesto x u kongruenciju $x \equiv a_1 \,(mod\, m_1)$, zaključujemo da je X kao i svaki broj oblika $X + kM$, rešenje te

kongruencije. Na isti način sledi da ta važi za sve ostale kongruencije polaznog sistema.
Međutim, $X + kM$ je jedno rešenje sistema, jer ako je X_1 , takođe rešenje sistema, onda uvrštavanjem X i X_1 u te kongruencije, dobijamo da je

$$x \equiv x_1 \,(mod\, m_i)\,, \qquad i = 1, 2, \ldots, n\,,$$

pa je

$$x \equiv x_1 \;(mod\, M),$$

jer su brojevi m_i , *po parovima uzajamno prosti.*

Iz dokaza teoreme, vidi se jasno i algoritam za rešavanje odgovarajućeg sistema kongruencija.

Primer 6.7 Naći sve cele brojeve koji daju ostatke *2, 6, 5*, pri deljenju sa *5, 7* i *11* redom.

Rešenje. Zadatak se svodi na rešavanje sistema kongruencija

$$x \equiv 2 \,(mod\, 5)$$

$$x \equiv 6 \;(mod\, 7)$$

$$x \equiv 5 \;(mod\, 11).$$

Uočavamo da je $m_1 = 5,\ m_2 = 7,\ m_3 = 11,\ M = 385,\ M_1 = 77,$ $M_2 = 55,\ M_3 = 35$, pa formiramo kongruencije

$$77x \equiv 1 \;(mod\, 5)$$

$$55x \equiv 1 \;(mod\, 7)$$

$$35x \equiv 1 \;(mod\, 11)$$

koje su ekvivalentne redom kongruencijama

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

$$6x \equiv 1 \pmod 7$$

$$2x \equiv 1 \pmod{11},$$

čija su rešenja redom:

$$x \equiv 3 \pmod 5$$

$$x \equiv 6 \pmod 7$$

$$x \equiv 6 \pmod{11}.$$

Dakle,

$$x \equiv 77 \cdot 3 \cdot 2 + 55 \cdot 6 \cdot 6 + 35 \cdot 6 \cdot 5 \pmod{385},$$

$$x \equiv 27 \pmod{385}. \ \Delta$$

6.3 Kvadratne kongruencije

Definicija 6.1 *Neka je (a, m) = 1. Ako kongruencija*

(6. 7) $$x^2 \equiv a \pmod m$$

ima rešenja, tada kažemo da je a ***kvadratni ostatak modula*** *m. U protivnom kažemo da je a* ***kvadratni neostatak modula*** *m. Kvadratne ostatke označavamo sa* ***QR****, a kvadratne neostatke sa* ***NR****.*

Teorema 6.5 *Neka je p neparan prost broj. Redukovan sistem ostataka modula p sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$ *kvadratnih neostataka.*

Dokaz. Svaki kvadratni ostatak modula p kongruentan je kvadratu nekog od brojeva:

$$-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2,\ 2^2, \ldots,\ (\frac{p-1}{2})^2$. Preostaje još da pokažemo da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentni po modulu p. Pretpostavimo suprotno, tj. da je $k^2 \equiv l^2\ (mod\ p)$, gde je $1 \leq k < l \leq \frac{p-1}{2}$. Tada je $(l-k)(l+k) \equiv 0\ (mod\ p)$, pa je $l-k \equiv 0\ (mod\ p)$ ili $l+k \equiv 0\ (mod\ p)$, što je u suprotnosti sa pretpostavkama o k i l, jer je $0 < l-k < p$ i $0 < l+k < p$. ■

Teorema 6.6 *Za dati neparan broj p i ceo broj a, ako $p \nmid a$, jednačina $x^2 \equiv a\ (mod\ p)$ ili nema rešenje ili ima tačno dva rešenja.*

Dokaz. Pretpostavimo da data kongruencija ima rešenje i da je x_1 jedno od njih. Tada je očigledno i $x_2 = -x_1$ rešenje. Drugih rešenja po modulu p nema, jer $x^2 \equiv a \equiv x_1^2\ (mod\ p)$ povlači da je $x \equiv \pm x_1\ (mod\ p)$. Pri tome bi $x_1 \equiv -x_1\ (mod\ p)$ imala za posledicu $2x_1 \equiv 0\ (mod\ p)$, što je nemoguće zbog *(2, p) = (x_1, p) =1.* ■

Definicija 6.2 *Neka je p neparan prost broj.* ***Ležendrov simbol*** $(\frac{a}{p})$ *je jednak 1, ako je a kvadratni ostatak modula p, -1 ako je a kvadratni neostatak po modulu p, a 0 ako $p \mid a$. Ležendrov simbol možemo zapisati i ovako*

$$\left(\frac{a}{p}\right) = \begin{cases} 1\ za\ (a,p)=1\ i\ a\ je\ kvadratni\ ostatak\ modula\ p \\ -1\ za\ (a,p)=1\ i\ a\ je\ kvadratni\ neostatak\ modula\ p \\ 0\ za\ p\ delitelj\ od\ a. \end{cases}$$

Teorema 6.7 (Ojlerov kriterijum) *Ako je p neparan prost broj i ako je NZD(a, p) = 1, tada jednačina (6.7) ili dva ili nijedno rešenje zavisno od toga da li je $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ ili $a^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$.*

Dokaz. Prema Maloj Fermaovovoj teoremi $a^{p-1} \equiv 1\ (mod\ p)$ odnosno

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0\ (mod\ p).$$

Kako ne mogu oba člana na levoj strani poslednje kongruencije biti deljiva sa p (jer bi tada i njihova razlika koja je jednaka, *2,* bila deljiva sa p), to važi ako je jedna i samo jedna od kongruencija:

$$a^{\frac{p-1}{2}} \equiv 1 \,(mod\, p) \qquad a^{\frac{p-1}{2}} \equiv -1 \,(mod\, p).$$

Ako jednačina *(6.7) ima rešenje* x, tada važi

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \;(mod\, p).$$

Važi i obratno, ako je $a^{\frac{p-1}{2}} \equiv 1 \,(mod\, p)$, tada jednačina *(6.7)* ima rešenje, a već smo napomenuli da jednačina *(6.7)* ne može imati tačno jedno rešenje. ■

Teorema 6.8

1) Ako je $a \equiv b \,(mod\, p)$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

3) Ako je (a, p) = 1, onda je $\left(\frac{a^2}{p}\right) = 1$ *u* $\left(\frac{1}{p}\right) = 1$.

4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, *tj.* $\left(\frac{-1}{p}\right) = \begin{cases} +1 \;ako\; je \;\; p \equiv 1 \;(mod\, 4) \\ -1 \;ako\; je \;\; p \equiv 3 \;(mod\, 4) \end{cases}$.

5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Dokaz.

1) Ako je $a \equiv b \;(mod\, p)$, tada kongruencija $x^2 \equiv a \;(mod\, p)$ ima rešenje ako i samo ako rešenje ima kongruencija $x^2 \equiv b \;(mod\, p)$.

2) Iz

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) (mod\, p)$$

sledi da je $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

3) Kongruencija $x^2 \equiv a^2 \,(mod\, p)$ ima rešenje ako je $x = a$. Specijalno $x = 1$, $x^2 \equiv 1 \,(mod\, p)$.

4) Ako uvrstimo $a = -1$ u Ojlerov kriterijum, dobijamo da je

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \,(mod\, p).$$

Leva i desna strana poslednje kongruencije po apsolutnoj vrednosti jednake su jedinici, pa one mogu biti kongruentne po modulu p $(p > 2)$, jedino ako su jednake, tj. ako je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Broj $(-1)^{\frac{p-1}{2}}$ jednak je +1, ako je $p \equiv 1 \,(mod\, 4)$ tj. $p = 4k + 1$, a -1 ako je $p \equiv 3 \,(mod\, 4)$ tj. $p = 4k + 3$.

5) Ako je $p = 8n + 1$ ili $p = 8n + 7$, tada je $\frac{p^2-1}{8}$ paran broj, a ako je $p = 8n + 3$ ili $p = 8n + 5$ je neparan broj, pa treba pokazati da je

$$\left(\frac{2}{p}\right) = \begin{cases} +1 \;\; ako\; je \;\; p \equiv 1 \,(mod\, 8) \; ili \;\; p \equiv 7 \,(mod\, 8) \\ -1 \;\; ako\; je \;\; p \equiv 3 \,(mod\, 8) \; ili \;\; p \equiv 5 \,(mod\, 8) \end{cases}.$$

Prema Gausovom kriterijumu imamo da je $\left(\frac{2}{p}\right) = (-1)^k$, pri čemu je k broj elemenata skupa $\left\{1 \cdot 2,\; 2 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2 = p - 1\right\}$, tj. skupa $S = \{2, 4, 6, \ldots, p - 1\}$ parnih brojeva manjih od p - *1* čiji je najmanji po apsolutnoj vrednosti ostatak pri deljenju sa p negativan. Najmanji po apsolutnoj vrednosti ostatak pri deljenju nekog broja iz S sa p je negativan ako je taj broj veći od $\frac{p}{2}$. Pošto parnih prirodnih brojeva manjih ili jednakih $\frac{p}{2}$ ima $\left[\frac{p}{4}\right]$, sledi da je $k = \frac{p-1}{2} - \left[\frac{p}{4}\right]$. Sada,

- ako je $p = 8n + 1$, imamo $k = 4n - 2n = 2n$,
- ako je $p = 8n + 3$, imamo $k = (4n + 1) - 2n = 2n + 1$,

- ako je $p = 8n + 5$, imamo $k = (4n + 2) - (2n + 1) = 2n + 1$,
- ako je $p = 8n + 7$, imamo $k = (4n + 3) - (2n + 1) = 2(n + 1)$,

pa je $\left(\frac{2}{p}\right) = (-1)^k$ jednako *1*, ako je prost broj p oblika $8n + 1$ ili $8n + 7$, dok je jednako *-1*, ako je p oblika $8n + 3$ ili $8n + 5$. ■

Teorema 6.9 (Gausov kriterijum) *Neka je p neparan broj NZD $(a, p) = 1$. Posmatrajmo brojeve $a, 2a, 3a, \dots, \frac{p-1}{2}a$, i njihove najmanje ostatke pri deljenju sa p. Označimo sa k broj ostataka koji su veći od $\frac{p}{2}$ tada je $\left(\frac{a}{p}\right) = (-1)^n$.*

Dokaz. Neka su $r_1, \dots, r_n$, ostaci koji su veći od $\frac{p}{2}$, a neka su $s_1, \dots, s_k$ preostali ostaci. Brojevi $r_1, \dots, r_n, s_1, \dots, s_k$ su međusobno različiti (po Teoremi 4.14) i nijedan od njih nije jednak nuli. Znamo $n + k = \frac{p-1}{2}$. Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \dots, n$. Takođe nijedan od brojeva $p - r_i$ nije jednak nekom s_j. Zaista, ako je $p - r_i = s_j$, tada je $r_i \equiv \alpha a \pmod p$, $s_j \equiv \beta a \pmod p$, za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$, pa iz $a(\propto + \beta) \equiv 0 \pmod p$ i $(a, p) = 1$ sledi da je $\propto + \beta \equiv 0 \pmod p$, a to je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.

Prema tome brojevi $p - r_1, \dots, p - r_n, s_1, \dots, s_k$ su svi međusobno različiti, ima ih $\frac{p-1}{2}$ i elementi su skupa $\left\{1, \dots, \frac{p-1}{2}\right\}$. Stoga su to baš brojevi $1, 2, \dots, \frac{p-1}{2}$ samo u nekom drugom poretku. Množeći ih dobijamo

$$(p - r_1) \cdots (p - r_n)\, s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) &\equiv (-r_1) \cdots (-r_n) s_1 \cdots s_k \\ &\equiv (-1)^n r_1 \cdots r_n\, s_1 \cdots s_k \\ &\equiv (-1)^h a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \pmod p. \end{aligned}$$

Sada skratimo sa $(\frac{p-1}{2})!$, pa dobijemo

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \ (mod\ p),$$

pa je po Ojlerovom kriterijumu

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \ (mod\ p). \ \blacksquare$$

Teorema 6. 10 *Ako je p neparan prost broj i (a, 2p) = 1, tada je* $\left(\frac{a}{p}\right) = (-1)^t$, *gde je*

$$t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Takođe važi $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Dokaz. Koristićemo iste oznake kao i u prethodnoj teoremi. Neka su r_i i s_i ostaci pri delenju broja ja sa p, $j = 1, \dots, \frac{p-1}{2}$. Količnici pri tome delenju su brojevi $\left\lfloor \frac{ja}{p} \right\rfloor$. Ako je sada $(a, p) = 1$, tada imamo

$$\sum_{i=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{n} r_1 + \sum_{i=1}^{k} s_i$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_1) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Oduzimanjem ova dva izraza, dobijamo

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \right) + 2 \sum_{i=1}^{n} r_i.$$

Nadalje je

$$\sum_{i=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2 - 1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{2} \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2.$$

Ako je sada *a* neparan, tj. *(a, 2p) = 1*, tada odavde dobijamo da je

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor (mod\ 2),$$

a ako je *a = 2*, tada dobijamo $n \equiv \frac{p^2-1}{8} \pmod 2$, jer je $\left\lfloor \frac{2j}{p} \right\rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$.
Sada tvrđenje teoreme sledi iz Gausove leme. ■

Teorema 6. 11 (Gausov zakon kvadratnog reciprociteta) *Ako su p i g različiti neparni prosti brojevi tada važi*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Drugim rečima, p i q oba oblika 4k + 3, onda jedna od kongruencija $x^2 \equiv p \pmod q$, $x^2 \equiv q \pmod p$ *ima rešenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik 4k + 1, tada ili obe kongruencije imaju rešenje ili obe nemaju rešenje.*

Dokaz. Neka je $S = \left\{(x,y): x,y \in Z,\ 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$.

Skup *S* ima $\frac{p-1}{2} \cdot \frac{q-1}{2}$ članova. Podelimo *S* na dva disjunktna podskupa, S_1 i S_2 prema tome da li je $qx > py$ ili $qx < py$. Uočimo da ne može biti $qx = py$. Skup S_1 je, dakle, skup svih parova *(x, y)* takvih da je $1 \le x \frac{p-1}{2}$ i $1 \le q \frac{qx}{p}$. Takvih parova ima

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor.$$

Slično se S_2 sastoji od svih parova (x, y), takvih da je $n \leq y \leq \frac{q-1}{2}$, $1 \leq x < \frac{py}{q}$, a takvih parova ima

$$\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Prema tome je

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{y} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

pa je prema teoremi *6. 10*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \ \blacksquare$$

Primer 6.9 Odrediti Leženrdrov simbol $\left(\frac{-42}{61}\right)$.

Rešenje.

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{4}{61}\right)\left(\frac{7}{61}\right)$$

$$\left(\frac{-1}{61}\right) = (-1)^{60} = 1,$$

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1,$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{2}} = -1,$$

pa sledi

$$\left(\frac{-42}{61}\right) = 1 \cdot (-1) \cdot 1 \cdot (-1) = 1,$$

tj. *-42* je kvadratni ostatak po modulu 61.

Primer 6.10 Odrediti sve proste brojeve p takve da je -2 kvadratni ostatak po modulu p.

Rešenje. Potrebno je pronaći sve proste brojeve p za koje važi:

$$\left(\frac{-2}{\mathrm{p}}\right) = \left(\frac{-1}{\mathrm{p}}\right)\left(\frac{2}{\mathrm{p}}\right) = 1.$$

Postoje dve mogućnosti:

1° $\left(\frac{-1}{\mathrm{p}}\right) = 1$ i $\left(\frac{2}{\mathrm{p}}\right) = 1.$

Prvi uslov je ekvivalentan sa $\mathrm{p} \equiv 1 \pmod 4$, a drugi $\mathrm{p} \equiv 1 \pmod 8$ i
$\mathrm{p} \equiv 7 \pmod 8$, što zajedno daje $\mathrm{p} = 1 \pmod 8$.

2° $\left(\frac{-1}{\mathrm{p}}\right) = -1$ i $\left(\frac{2}{\mathrm{p}}\right) = -1.$

Prvi uslov je ekvivalentan sa $\mathrm{p} \equiv 3 \pmod 4$, a drugi sa $\mathrm{p} \equiv 3 \pmod 8$ i $\mathrm{p} \equiv 5 \pmod 8$, što zajedno daje $\mathrm{p} \equiv 3 \pmod 8$.

Dakle, $\left(\frac{-2}{\mathrm{p}}\right) = 1$. Ako je $\mathrm{p} \equiv 1 \pmod 8$ ili $\mathrm{p} \equiv 3 \pmod 8$.

6. 4 Kongruencije višeg reda

Polinom sa celobrojnim koeficijentima je aritmetička funkcija. Ako polinom $P(x)$ napišemo u obliku

(6. 8) $$P(x) = a_n\, x^{\mathrm{n}} + a_{n-1}x^{n-1} + \ 1 \ldots + a_0$$

tako da je $a_n \neq 0$. Keoficijent a_n nazivamo vodeći koeficijent polinoma $P(x)$. Ako je $a_n \not\equiv 0\ (mod\ m)$ gde je m proizvoljan ceo broj, kažemo da je kongruencija

$$P(x) \equiv 0\ (mod\ m)$$

reda n po modulu m.
Kongruencije višeg reda su kongruencije reda $n \geq 2$. Rešenje te kogruencije je svaki broj x za koji je $P(x)$ deljiv sa m. Broj rešenja kongruencije jednak je broju klasa ostataka koji zadovoljavaju tu kongruenciju.
Broj rešenja kongruencije višeg reda ne mora biti jednak redu kongruencije, može biti jednak redu kongruencije, može biti manji ili veći.

Primer 6.11 Kongruencija $x^2 - 2x + 3 \equiv 0\ (mod\ 4)$ nema rešenja, jer nijedan od brojeva od potpunog sistema ostataka $\{0,1,2,3\}$ ne zadovoljava kongruenciju.
Kongruencija $x^2 - 4x + 3 \equiv 0\ (mod\ 6)$ ima dva rešenja to su $x \equiv 1,3\ (mod\ 6)$.
Kongruencija $x^3 \equiv 2\ (mod\ 6)$ ima samo jedno rešenje i to je $x \equiv 2\ (mod\ 6)$.
Kongruencija $x^2 - 1 \equiv 0\ (mod\ 24)$ ima osam rešenja.
Kongruenciju zadovoljavaju sledeći brojevi iz potpunog sistema ostataka po modulu *24: 1, 5, 7, 11, 13, 17, 19, 23.* Δ

Neka su $R(x)$, $P(x)$, $Q(x)$ polinomi sa celobrojnim koeficijentima i neka je $R(x) = P(x) - Q(x)$. Ako su svi koeficijenti polinoma $R(x)$ deljivi sa m, tada su polinomi $P(x)$ i $Q(x)$ kongruentni po modulu m, tj.

$$P(x) \equiv Q(x)(mod\ m).$$

Primer 6.12 Polinomi $P(x) = 3x^3 - 4x + 1$ i *Q(x)*= $-2x^3 + x - 4$ su kongruentni po modulu *5*, jer je njihova razlika polinom $R(x) = 5x^3 - 5x + 5$ koji ima sve koeficijente deljive sa 5. Δ

Definicija 6. 3 Polinom $P(x)$ je deljiv polinomom $Q(x)$ po modulu *m*, ako postoji polinom sa celobrojnim koeficijentima $S(x)$ takav da je

$$P(x) \equiv Q(x)S(x)(mod\ m).$$

Primer 6. 13 Polinom $4x^3 + 2$ je deljiv polinomom $x^2 + 3x + 4$ po modulu *5*, jer je

$$4x^3 + 2 \equiv (x^2 + 3x + 4)(4x + 3)(mod\ 5).$$

Zaista množenjem polinoma na desnoj strani jednakosti dobijamo polinom $4x^3 + 15x^2 + 25x + 12$ koji je kongruentan sa polinomom $4x^3 + 2$ po modulu *5*. Δ

Teorema 6. 12 *Ako u polinomu sa celorojnim koeficijentima*

$$P(x) = a_n x^n + \cdots + a_0$$

vodeći koeficijent a_n *nije deljiv prostim brojem p, tada kongruencija*

$$P(x) \equiv 0\ (mod\ p)$$

Ima najviše n različitih rešenja.

Dokaz. Dokaz izvodimo indikcijom po *n*. Za *n=1*, $P(x) = a_1 x + a_0$ dat je dokaz u linearnim kongruencijama.

Pretpostavimo da trvđenje važi za polinome stepena manjeg od *n*. Ako pretpostavimo da za polinom $P(x) = a_n x^n + \cdots + a_0$ stepena $n > 1$ nekongruentno po modulu *p*. Neka su to rešenja $x_1, x_2, \ldots, x_n, x_{n+1}$. Tada je $P(x) - P(x_1) = a_n(x^n - x_1^n) + \cdots + a_1(x - x_1)$. Kako je svaka od razlika $x^n - x_1^n, \ldots, (x - x_1)$ deljiva sa $x - x_1$ to je

(6. 9) $$P(x) - P(x_1) = (x - x_1)Q(x)$$

gde je $Q(x) = a_n x^{n-1} + \cdots + a_1 x$ polinom sa celobrojnim koeficijentima. Iz prethodne jednakosti sledi da je

$$(x - x_1)Q(x) \equiv P(x) - P(x_1)(mod\ p),$$

a kako je $P(x_1) \equiv 0(mod\ p)$ dobijamo kongruenciju

$$(x - x_1)Q(x) \equiv P(x)(mod\ p).$$

Ako u poslednju kongruenciju za x uzimamo vrednosti $x_2, x_3, \ldots, x_{n+1}$ (to su rešenja kongruencije $P(x) \equiv 0(mod\ p)$ dobijamo kongruencije

$$(x_2 - x_1)Q(x_2) \equiv 0(mod\ p), \ldots, (x_{n+1} - x_1)Q(x_{n+1}) \equiv 0(mod\ p).$$

Kako su rešenja $x_1, x_2, \ldots, x_{n+1}$ po parovima nekongruentni po modulu p, tada su i sve razlike $x_2 - x_1, \ldots, x_{n+1} - x_1$ uzajamno proste sa p. Kako je $(x_i - x_1) \neq 0$ za $i = 2, \ldots, n + 1$, može se izvršiti skraćivanje prethodnih kongruencija, pa dobijamo

$$Q(x_2) \equiv 0\ (mod\ p), \ldots, Q(x_{n+1}) \equiv 0(mod\ p).$$

To znači da kongruencija $Q(x) \equiv 0(mod\ p)$, koja je stepena $n - 1$ ima n po parovima nekongruentnih rešenja po modulu p. To je kontradikcija sa pretpostavkom indukcije. Znači kongruencija stepena n ne može imati više od n nekongruentnih rešenja. ■

Teorema 6. 13 *Neka je P(x) polinom stepena n sa celobrojnim koeficijentima i p prost broj. Ako kongruencija*

$$P(x) \equiv 0(mod\ p)$$

Ima više od n različitih (nekongruentnih) rešenja, onda su svi koeficijenti polinoma $P(x)$ deljivi sa p.

Dokaz. Za $n = 1$ tvrđenje sledi na osnovu tvrđenja o linearnim kongruencijama. Pretpostavimo da ona važi i za sve polinome stepena manjeg od n. Neka je

$$P(x) = a_n x^n + \cdots + a_0 \text{ i } p \mid a_n.$$

Tada je za svaki ceo broj x, $a_n x^n \equiv 0(mod\ p)$. To važi i za sve ostale članove polinoma u kojima je koeficijent deljiv sa p. Ako nisu svi koeficijenti deljivi sa p, onda posle izdvajanja članova deljivih sa p dobijamo polinom $Q(x)$ čiji je stepen manji od n, pri čemu je

$$P(x) \equiv Q(x) \equiv 0(mod\ p).$$

Neka je $Q(x) = a_k x^k + \cdots$ gde je a_k ceo broj koji nije deljiv sa p. Ali to je kontradikcija, jer onda kongruencija $Q(x) \equiv 0(mod\ p)$ ne bi mogla imati više od k rešenja. ■

Primer 6. 14

a) Kongruencija $x^3 + x + 4 \equiv 0\ (mod\ 5)$ nema rešenja. Neposredno se proverava potpun sistem ostataka $\{0, 1, 2, 3, 4\}$;

b) Kongruencija $x^3 - x + 1 \equiv 0\ (mod\ 5)$ ima samo jedno rešenje, $x \equiv 3\ (mod\ 5)$;

c) Kongruencija $x^3 - x \equiv 0\ (mod\ 5)$ ima tri rešenja: $x \equiv 0\ (mod\ 5),\ x \equiv 1\ (mod\ 5),\ x \equiv 4\ (mod\ 5)$. U ovom slučaju se dostiže granica iz prethodne teoreme.Δ

U slučaju kada je modul složen broj, teorema **(**6.13**)** ne važi.

Primer 6. 15 Kongruencija trećeg reda $x^3 - x \equiv 0\ (mod\ 6)$ ima šest rešenja. Svaki ceo broj zadovoljava kongruenciju. Δ

Teorema 6. 14 *Neka je $P(x)$ polinom sa celobrojnim koeficijentima i m složen broj sa kanonskom faktorizacijom $m = p_1^{\propto_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Tada je kongruencija*

(6. 10) $$P(x) \equiv 0(mod\ m)$$

ekvivalentna sistemu kongruencija

(6. 11)
$$\begin{matrix} P(x) \equiv 0\left(mod\ p_1^{\propto_1}\right) \\ \vdots \\ \vdots \\ P(x) \equiv 0\left(mod\ p_k^{\propto_k}\right) \end{matrix}$$

tj. ima isti skup rešenja.

Dokaz. Ako je $x \equiv a\ (mod\ m)$ rešenje kongruencije (6.10) , onda je broj $P(x)$ deljiv sa m, prema tome i sa svakim od brojeva $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$, što znamo da je svako rešenje kongruencije (6.10) i rešenje kongruencije (6. 11).

Obratno ako je $x \equiv b(mod\ m)$ rešenje sistema (6. 11) tada je broj P*(b)* deljiv sa svakim od brojeva $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$. Kako su to, po parovima uzajamno prosti brojevi, sledi da je *P(b)* deljiv sa *m*, tj. $x \equiv b\ (mod\ m)$ je rešenje kongruencije (6.10). ■

Teorema 6. 15 *Neka je $P(x)$ polinom sa celobrojnim koeficijentima i m složen broj sa kanonskom faktorizacijom $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Ako u sistemu kongruencija 6.11 prva kongruencija ima m_1 nekongruentnih rešenja po modulu $p_1^{\alpha_1}$, a druga m_2 po modulu $p_2^{\alpha_2}$, ..., poslednja m_k nekongruentnih rešenja po modulu $p_k^{\alpha_k}$, tada kongruencija 6.10 ima $m_1 \cdot m_2 \cdots m_k$ nekongruentnih rešenja po modulu m.*

Dokaz. Neka je $x \equiv a_i\ (mod\ p_i^{\alpha_i})$ bilo koje rešenje *i-te* kongruencije sistema *7.4 i = 1, ..., k.*
Posmatrajmo sistem kongruencija

(6. 12)
$$x \equiv a_1\ (mod\ p_1^{\alpha_1})$$
$$\vdots$$
$$x \equiv a_k\ (mod\ p_k^{\alpha_k}).$$

Kako su moduli tih kongruencija po parovima uzajamno prosti, prema *Kineskoj teoremi o ostacima,* sistem *6.12* ima tačno jedno rešenje po modulu *m*. To rešenje je tada i rešenja sistema *6.11* Izredajući tako svako rešenje svake kongruencije dobijamo dokaz tvrđenja.

Primer 6. 16 Skup rešenja kongruencije $x_4 - x \equiv 0\ (mod\ 20)$ poklapa se sa skupom rešenja sistema

$$x^4 - x \equiv 0\ (mod\ 4)$$
$$x^4 - x \equiv 0\ (mod\ 5).$$

Rešenja prve kongruencije su $x \equiv 0; 1\ (mod\ 4)$, a rešenja druge kongruencije su $x \equiv 0;\ 1\ (mod\ 5)$. Na osnovu teoreme 6.15 kongruencija $x^4 - x \equiv 0\ (mod\ 20)$ ima četiri različita rešenja. Δ

Sada ćemo ispitati kongruenciju

(6.13) $$P\ (x) \equiv 0\ (mod\ p^s).$$

Kako za svaki ceo broj c iz relacije $P\ (c)\ \equiv 0\ (mod\ p^s)$ sledi da je

$$P(c)\ \equiv 0\ (mod\ p^k)\ ,\quad k\ = 1, 2, \ldots, s-1$$

tj. svako rešenje kongruencije $P(x) \equiv 0\ (mod\ p^s)$ je rešenje i kongruencije

$$P(x) \equiv 0\ \ (mod\ p^k)\quad (1 \leq k\ \leq\ s-\ 1)$$

i posebne kongruencije

$$P(x) \equiv 0\ (mod\ p).$$

Zaključujemo da se sva rešenja kongruencije

$$P(x) \equiv 0\ \ (mod\ p^s)$$

nalaze među rešenjima kongruencije

$$P(x) \equiv\ 0\ \ (mod\ p).$$

Definicija 6. 4 *Neka je dat polinom*

$$P(x) =\ \ a_n x^n\ +\ \ a_{n-\ 1} x^{n-\ 1} +\ \cdots +\ \ a_1 x\ +\ \ a_0;$$

izraz

$$P'(x) =\ na_n x^{n-\ 1} +\ (n-\ 1) a_{n-\ 1} x^{n-\ 2}\ +\ \cdots +\ \ a_1$$

Nazivamo izvodom polinoma $P(x)$.

Sada ćemo dokazati teoremu koja će nam omogućiti rešavanje kongruencije

$$P(x) \equiv 0 \ (mod\ p^s)$$

pomoću kongruencije

$$P(x) \equiv 0 \ (mod\ p).$$

Teorema 6. 16 *Neka je* $x \equiv x_0 \ (mod\ p)$, *gde je* p *prost broj, rešenje kongruencije*

(6. 14) $$P(x) \equiv 0 \ (mod\ p)$$

1. Ako je

(6. 15) $$P'^{(x)} \not\equiv 0 \ (mod\ p)$$

tada postoji jedno i samo jedno rešenje $x \equiv x_1 \ (mod\ p^s)$, $x_1 \in (x_0)_{(p)}$ *kongruencije*

(6. 16) $$P(x) \equiv 0 \ (mod\ p^s).$$

2. Ako je

(6. 17) $$P'(x) \equiv 0 \ (mod\ p),$$

a $x \equiv x_1 \ (mod\ p^k)$, $x_1 \in (x_0)_{(p)}$, *rešenje kongruencije*

(6. 18) $$P(x) \equiv 0 \ (mod\ p^k).$$

2. 1 Ako je $k \leq s-1$ *i*

(6. 19) $$P(x_1) \not\equiv 0 \ (mod\ p^{k+1})$$

tada kongruencija $P(x) \not\equiv 0 \ (mod\ p^{k+1})$ *nema rešenja među brojevima klase* $(x_0)_{(p)}$.

2. 2 Ako je $k = s - 1$ *i*

(6. 20) $$P(x_1) \equiv 0 \ (mod\ p^s)$$

tada je kongruencija $P(x_1) \equiv 0 \ (mod\ p)$ *zadovoljena za sve brojeve klase* $(x_0)_p$.

Dokaz.
1. Dokaz izvodimo indukcijom. Tvrđenje je tačno za $s = 1$ na osnovu pretpostavke da je $x \equiv x_0 \ (mod\ p)$ rešenje kongruencije *(6. 14).* Pretpostavimo sada da za $s = k$ kongruencija

(6. 21) $$P(x) \equiv 0 \ (mod\ p^k)$$

ima jedno i samo jedno rešenje

$$x \equiv x_1 \ (mod\ p^k), \qquad x_1 \in (x_0)_{(p)}.$$

Ako je

(6. 22) $$x_2 \equiv x_1 + p^k t,$$

i odredimo t tako da važi

(6. 23) $$P(x_2) \equiv 0 \ (mod\ p^{k+1}).$$

Ako polinom $P(x_1 + p^{k+1})$ uredimo po stepenima od $p^k t$ i rastućem poretku, dobija se

$$P(x_1 + p^k t) = P(x_1) + P'(x_1)\, p^k t + c_2 p^{2k} t^2 + c_3 p^{3k} t^3 + \cdots + c_n p^{nk} t^n$$

gde su $c_i,\ i = 2, 3, \ldots, n,$ celi brojevi.
Kako je $c_i p^{ik} t^i \equiv 0 \ (mod\ p^{k+1})$ za $i = 2, 3, \ldots, n,$ odavde i iz $P(x_2) \equiv 0 \ (mod\ p^{k+1})$ sledi

$$P(x_1) + P'(x_1)\, p^k t \equiv 0 \ (mod\ p^{k+1})$$

ako prethodnu jednakost podelimo sa p^k dobijamo

(6.24) $$\frac{P(x_1)}{p^k} + P'(x_1)\, t \equiv 0 \,(mod\ p),$$

$\frac{P(x_1)}{p^k}$ je ceo broj, jer prema pretpostavci x_1 je rešenje kongruencije

$$P(x) \equiv 0 \,(mod\ p^k).$$

Kako zbog $x_1 \in (x_0)_{(p)}$ važi $x_1 \equiv x_0 \,(mod\ p)$, takođe je $P'(x_1) \equiv P'(x_0) \,(mod\ p)$, što sa pretpostavkom $P'(x_0) \not\equiv 0 \,(mod\ p)$ daje

(6. 25) $$P'(x_1) \not\equiv 0 \,(mod\ p).$$

Međutim tada linearna kongruencija (6.24) ima jedno i samo jedno rešenje. Ako je to rešenje $t \equiv t_0 \,(mod\ p)$ rešenje kongruencije

(6.26) $$P(x) \equiv 0 \,(mod\ p^{k+1})$$

je $x \equiv x_2 \,(mod\ p^{k+1})$, odnosno

$$x \equiv x_1 + p^k\, t_0 \,(mod\ p^{k+1})$$

pošto na osnovu (6.22) $x_2 \equiv x_1 \,(mod\ p)$ takođe je $x_2 \in (x_0)_{(p)}$. Time je dokazano da pod datim uslovima postoji rešenje $x \equiv x_2 \,(mod\ p^{k+1})$, $x_2 \in (x_0)_{(p)}$ kongruencije (6.26).
Dokazaćemo da je to jedino rešenje iz klase $(x_0)_{(p)}$. Neka je

$$x \equiv x_3 \,(p^{k+1}), \quad x_3 \in (x_0)_{(p)}$$

rešenje kongruencije (6.26). Tada iz relacije

(6. 27) $$P(x_3) \equiv 0 \,(mod\ p^{k+1})$$

sledi $f(x_3) \equiv 0 \,(mod\ p^k)$, što znači da je $x \equiv x_1 \,(mod\ p^k)$ odakle je $x_3 \equiv x_1 + p^k t_1$, gde je t_1 ceo broj. Odavde iz relacije (6.27) dobija se $P(x_1 + p^k t_1) \equiv 0 \,(mod\ p^{k+1})$ odnosno

$$\frac{P(x_1)}{p^k} + P'(x_1)\ t_1 \equiv 0\ (mod\ p).$$

Ova relacija sa (6.24) daje

$$P'(x_1)\ (t_1 - t_0) \equiv 0\ (mod\ p),$$

s obzirom na relaciju (6.25), zaključujemo

$$t_1 - t_0 \equiv 0\ (mod\ p).$$

Kako je $x_3 - x_2 = p^k\ (t_1 - t_0)$ na osnovu prethodne relacije je

$$x_3 \equiv x_2\ (mod\ p^{k+1}).$$

Iz prethodne relacije sledi da je rešenje $x \equiv x_2\ (mod\ p^{k+1})$,
$x_2 \in (x_0)_{(p)}$ kongruencije (6.27) jednoznačno određeno.
Zaključujemo da tvrđenje *1* date teoreme važi i za $k = s$, pri čemu je *s* proizvoljan prirodan broj.

2. Ako je zadovoljen uslov (6.17) i ako je $x \equiv x_1\ (mod\ p^k)$,
$x_1 \in (x_0)_{(p)}$ rešenje kongruencije

$$P(x) \equiv 0\ (mod\ p^k).$$

Ako je

(6. 28) $$x = x_1 + p^k t$$

odredimo ceo broj *t* tako da je (6.28) rešenje kongruencije (6.16). Iz $P(x_1 + p^k t) \equiv 0\ (mod\ p^s)$, slično kao u prethodnom slučaju, imamo

$$\frac{P(x_1)}{p^k} + P'(x_1)\ t \equiv 0\ (mod\ p^{s-k}),$$

odavde i na osnovu pretpostavke $P'(x_0) \equiv 0\ (mod\ p)$ i s obzirom na relaciju $x_1 \equiv x_0\ (mod\ p)$ dobijamo

$$\frac{P'(x_1)}{p^k} \equiv 0 \ (mod\ p^{s-k})$$

odnosno

(6. 29) $$P(x_1) \equiv 0 \ \ (mod\ p^s).$$

2. 1 Ako je zadovoljen uslov (6.19) i ako je $k+1 \leq s$ tada je relacija (6.29) nemoguća. Prema tome, u tom slučaju nijedan element klase $(x_0)_{(p)}$ nije rešenje kongruencije (6.16).

2. 2 Ako je zadovoljen uslov (6.20) i ako je $k = s-1$, tada kongruencija (6.16) ima p rešenja

$$x \equiv x_1 + \ p^{s-t}t \ (mod\ p^s), \qquad t \ = 0, 1, 2, \dots, p-1,$$

koji su elementi klase $(x_0)_{(p)}$. ■

Primer 6. 17 Rešiti kongruenciju

$$P(x) = \ x^5 - 4x^4 - 2x^2 + x \ + 10 \ \equiv 0 \ (mod\ 27).$$

Rešenje: Da rešimo kongruenciju

(6. 30) $$P(x) = x^5 \ - 4x^4 - 2x^2 + \ x + 10 \equiv 0 \ (mod\ 3^3),$$

potrebno je prvo da rešimo kongruenciju

$$x^5 - 4x^4 - 2x^2 + x + 10 \equiv 0 \ (mod\ 3),$$

pošto je $27 = 3^3$. Jedino rešenje $x \equiv 1 \ (mod\ 3)$. Kako je $P'(x) = 5x^4 - 16x^3 - 4x + 1$, $P'(1) = -14$ i $P'(1) \not\equiv 0 \ (mod\ 3)$ kongruencija (6.30) ima rešenje. Sada tražimo rešenje kongruencije

(6. 31) $$P(x) \equiv 0 \ (mod\ 9)$$

oblika

(6. 32) $$x = 1 + 3t,$$

gde je t ceo broj. Prema teoremi (6.16) je

$$P(1+3t) = P(1) + P'(1)\cdot 3t \equiv 0 \ (mod\ 9).$$

Kako je $P(1) = 6$ i $P'(1) = -14$ dobija se kongruencija

$$6 - 42t \equiv 0 \ (mod\ 9)$$

odnosno

$$2 - 14t \equiv 0 \ (mod\ 3)$$

tj.

$$7t \equiv 1 \ (mod\ 3).$$

Rešenje ove kongruencije je $t \equiv 1 \ (mod\ 3)$, odnosno

$$x \equiv 4 \ (mod\ 9).$$

Rešenje kongruencije (6.31), stavljajući sada

(6. 33) $$x = 4 + 9t,$$

tražimo rešenje kongruencije

$$P(4+9t) = P(4) + P'(4)\ 9t \equiv 0 \ (mod\ 27)$$

odnosno

$$-18 + 2169t \equiv 0 \ (mod\ 27),$$

tj.

$$241t \equiv 2 \ (mod\ 3).$$

Tada se dobija da je $t \equiv -1(mod\ 3)$, tj.

$$x \equiv -5 \ (mod\ 27),$$

što predstavlja rešenje polazne kongruencije. Δ

Primer 6.18 Rešiti kongruenciju:

$$P\,(x) = x^4 + x^3 + 2x^2 - x + 2 \equiv 0\ (mod\ 125).$$

Rešenje: Da bi smo rešili kongruenciju iz primera *6.17*, rešavamo sledeću kongruenciju:

$$P(x) = x^4 + x^3 + 2x^2 - x + 2 \equiv 0\ (mod\ 5).$$

Njena rešenja su:

$$x \equiv 1\ (mod\ 5), \qquad x \equiv -1\ (mod\ 5), \quad x \equiv 2\ (mod\ 5).$$

Kako je $P'(x) = 4x^3 + 3x^2 + 4x - 1$, dobijamo da je

$$P'(1) = 5, \qquad P'(-1) = -6, \qquad P'(-2) = -29.$$

Kako je $P'(1) \equiv 0\ (mod\ 5)$ i $P(1) \not\equiv 0\ (mod\ 25)$, ne postoji rešenje polazne kongruencije u klasi ostataka $x \equiv 1\ (mod\ 5)$.
Preostala dva rešenja postoje na osnovu teoreme *6.16* stavljajući

$$x = -1 + 5t, \qquad x = -2 + 5t$$

dobijamo kongruencije:

$$f(-1 + 5t) \equiv 0\ (mod\ 25), \ \ f(-2 + 5t) \equiv 0\ (mod\ 25).$$

Odavde sledi

$$1 - 6t \equiv 0\ (mod\ 5), \ \ 4 - 29t \equiv 0\ (mod\ 5),$$

a zatim

$$-6t \equiv -1\ (mod\ 5), \ \ -29t \equiv -4\ (mod\ 5),$$

tj.

$$t \equiv 1\ (mod\ 5), \qquad t \equiv 1\ (mod\ 5).$$

Rešenja kongruencije $f(x) \equiv 0\ (mod\ 25)$ su, prema tome,

$$x \equiv 4\ (mod\ 25), \ \ x \equiv 3\ (mod\ 25).$$

Stavljajući

$$x \equiv 4 + 25t \ (mod\ 125), \quad x \ \equiv 3 + 25t \ (mod\ 125)$$

dobijaju se na sličan način kongruencije

$$14 + 319t \equiv 0 \ \ (mod\ 5), \quad 5 + 146t \equiv 0 \ (mod\ 5),$$

čija su rešenja

$$t \equiv -1 \ (mod\ 5), \quad t \equiv 0 \ (mod\ 5).$$

Rešenja date kongruencije su

$x \equiv -21 \ (mod\ 125), \ x \equiv 3 \ (mod\ 125). \ \Delta$

Zaključak

Cilj ovog rada je obrada tema koje su značajne za dodatni rad, rad sa nadarenim učenicima, kao i priprema za takmičenja učenika osnovnih i srednjih škola. U radu su obrađene teme iz teorije brojeva kao što su deljivost celih brojeva i osobine prostih brojeva. Definisane su i detaljno obrađene relacija kongruencije i njene osobine, kao i klase ostataka. Rad je fokusiran na obradu teme kongruencije s jednom nepoznatom: linearne kongruencije, sistemi linearnih kongruencija, kvadratne kongruencije i kongruencije višeg reda. U radu su korišćene metoda matematičke indukcije i diferencijalnog računa u dokazivanju tvrđenja i rešavanju složenijih zadataka. Mogućnost daljeg proučavanja i proširenja teme bi obuhvatilo obradu kongruencija s jednom nepoznatom po složenom modulu.

Naime, želeo sam da pokažem da se do rešenja matematičkog problema ne dolazi jednostavno, već da ono nastaje kao rezultat razmišljanja i logičkog rezonovanja. Rešenje zadataka mora da, pre svega, zvuči prirodno tako da deluje potpuno očigledno i razumno, da u određenom trenutku dobijamo i nove ideje. Smatram da su ciljevi mog rada u potpunosti ispunjeni.

Literatura

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

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

[3] Ratko Tošić, Vanja Vukoslavčević, ELEMENTI TEORIJE BROJEVA, Alef, Novi Sad, 1995.

[4] Milan S. Popadić, PRIRUČNIK ZA TAKMIČENJA SREDNJOŠKOLACA U MATEMATICI, III kongruencije, Zavod za izdavanje udžbenika Socijalističke Republike Srbije, Beograd, 1967.

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

[6] Zoran Kadelburg, Vladimir Mićić, Srđan Ognjanović, ANALIZA SA ALGEBROM, udžbenik sa zbirkom zadataka za 2. razred Matematičke gimnazije, Krug, Beograd, 2008.

[7] Društvo matematičara Srbije, TANGENTA 10, zadaci iz matematičkog časopisa „TANGENTA“, 1995-2005, materijal za mlade matematičare, sveska 45, Beograd, 2006.

[8] Andrej Dujella, UVOD U TEORIJU BROJEVA (skripta), PMF – matematički odjel, Sveučilište u Zagrebu.

[9] Milorad Čelebić, Slobodan Dikov Novčić, ZADACI SA TAKMIČENJA SA REŠENJIMA, matematička biblioteka 45, Zavod za udžbenike i nastavna sredstva, Beograd, 1986.

Kratka biografija

Rođen sam 06. 07. 1963. U Brčkom. Osnovnu školu sam završio u Pelagićevu, a gimnaziju u Orašju. Prirodno – matematički fakultet završio u Novom Sadu, smer – diplomirani matematičar – profesor matematike. Trenutno zaposlen u gimnaziji „20. OKTOBAR“ u Bačkoj Palanci. Živim u Gajdobri sa suprugom Snežanom i petoro dece.

Ime i prezime

Vojko Nestorović

UNIVERZITET U NOVOM SADU
PRIRODNO – MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:	
RBR	
Identifikacioni broj:	
IBR	
Tip dokumenctacije:	Monografska dokumentacija
TD	
Tip zapisa:	Tekstualni štampani materijal
TZ	
Vrsta rada:	Master rad
VR	
Autor:	Vojko Nestorović
AU	
Mentor:	Prof. dr Siniša Crvenković
MN	
Naslov rada:	Brojevne kongruencije
NR	
Jezik publikacije:	Srpski (latinica)
JP	
Jezik izvoda:	Srpski / engleski
JI	
Zemlja publikovanja:	Srbija
ZP	
Uže geografsko područje:	Vojvodina
UGP	
Godina:	Jul 2011.
GO	
Izdavač:	Autorski reprint
IZ	
Mesto i adresa:	Prirodno – matematički fakultet
MA	Trg Dositeja Obradovića 4, Novi Sad
Fizički opis rada	6 / 78 /1 / 0 / 9 / 1
(poglavlja, strana, fotografija, slika, literatura, tabela):	
FO	
Naučna oblast:	Matematika
NO	
Naučna disciplina:	Metodika nastave matematike
HND	
Predmetna odrdnica / ključne reči:	Matematika, teorija brojeva, teorema, dokaz
PO	
UDK	
Čuva se:	Biblioteka Departmana za matematiku, PMF, Novi Sad
ČU	
Važna napomena:	Nema
VN	
Izvod:	Obrada i primena brojevnih kongruencija, kongruencije s jednom nepoznatom
IZ	
Datum prihvatanja teme	
Od strane NN veća:	11.07.2011.
DP	
Datum odbrane:	jul 2011.
DO	
Članovi komislije:	
KO	
Predsednik:	prof. dr Ljljana Gajić, redovni profesor, PMF, Novi Sad
Mentor:	prof. dr Siniša Crvenković, redovni profesor, PMF, Novi Sad
Član:	prof. dr Zagorka Crvenković Lozanov, redovni profesor, PMF, Novi Sad

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCE AND MATHEMATICS
KEY WORDS DOCUMENTATION

Accession number: **ANO**	
Identification number: **INO**	
Document type: **DT**	Monograph type
Type of record: **TR**	Printed text
Contents Code: **CC**	Master examination
Author: **AU**	Vojko Nestorović
Mentor:	Professor Siniša Crvenković, Ph.D., Full Professor of Faculty of Natural Sciences and Math., Novi Sad
MN	
Title:	Numeric congruence
Language of text: **LT**	Serbian (Latin)
Language of abstract: **LA**	English
Country of publication: **CP**	Serbia
Locality of publication: **LP**	Vojvodina
Publication year: **PY**	July, 2011.
Publisher: **PU**	Author's reprint
Publication place: **PP**	Faculty of Natural Sciences and Mathematics, Trg Dositeja Obradovića 4, Novi Sad, Serbia
Physical description (chapters, pages, photographs, pictures, references, table): **PD**	6 / 78 /1 / 0 / 9 / 1
Scientific field: **SF**	Mathematics
Scientific discipline: **SD**	Methodic of Mathematics
Subject / Key words: **SKW**	Mathematics, inequality, theorem, evidece, geometry
UC	
Holding data: **PP**	Library of Department of Mathematics, Faculty of Natural Sciences and Mathematic, Novi Sad
Note: **N**	None
Abstract: **AB**	Processing and use of numeric conguence, congruence with one unknown
Accepted by the Scientific Board on: **ASB**	July 11th, 2011.
Defended on: **DE**	July 2011.

Thesis defends board:

DB

President: Ljiljana Gajić Ph.D, Full Professor, Faculty of Natural Sciences and Mathematic, Novi Sad

Mentor: Siniša Crvenković, Ph.D. Full Professor, Faculty of Natural Sciences and Mathematic, Novi Sad

Member: Zagorka Crvenkovic Lozanov , Ph .D. Full Professor, Faculty of Natural Sciences and Mathematic, Novi Sad