UNIVERZITET METROPOLITAN BEOGRAD

CS215 - DISKRETNE STRUKTURE

KONGRUENCIJE

Lekcija 08

PRIRUČNIK ZA STUDENTE

CS215 - DISKRETNE STRUKTURE

Lekcija 08

KONGRUENCIJE

UVOD

Cilj ovog predavanja je izučavanje teorije deljivosti celih brojeva sa fokusom na linearne jednačine kongruencije

U ovoj lekciji biće reči o:

1. Prosti brojevi
2. Pojam i algoritam deljivosti
3. Jednačine kongruencije oblika:

- $ax \equiv 1 \pmod{m}$
- $ax \equiv b \pmod{m}$

Poglavlje 1

PROSTI BROJEVI

DEFINICIJA PROSTOG BROJA

Prirodan broj p >1 je prost broj ako p ima samo trivijalne delioce, to jest, ako su njegovi jedini delioci ±1 i ±p.

Definicija
Prirodan broj p > 1 je prost broj ako p ima samo trivijalne delioce, to jest, ako su njegovi jedini delioci ±1 i ±p.
Ako prirodan broj n > 1 nije prost, onda je on složen.
Ako je prirodan broj n > 1 složen, onda se može zapisati u obliku
n = a • b
za neke cele brojeve a i b takve da 1 < a, b < n.

Primer

(a) Prirodni brojevi 2 i 5 su prosti, dok su 6 = 2 • 3 i 15 = 3 • 5 složeni.

(b) Prosti brojevi manji od 50 su

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

(c) Iako 21, 24 i 1729 nisu prosti, svaki od njih može biti zapisan u obliku proizvoda prostih brojeva:

21 = 3 • 7, 24 = 2 • 2 • 2 • 3 = 23 • 3 i 1729 = 7 • 13 • 19.

Tvrdjenje iz primera (c) važi za sve prirodne brojeve.

ERATOSTENOVO SITO

Kada implementiramo Eratostenovo sito, dovoljno je obraditi brojeve koji su manji ili jednaki $\sqrt{N}$

Eratostenovo sito (takođe Eratostenovo rešeto) je algoritam koji pronalazi sve proste brojeve u rasponu od 1 do N. Osmislio ga je starogrčki naučnik i upravnik Aleksandrijske biblioteke Eratosten.

Algoritam radi na nizu brojeva od 1 do N. Na početku, iz niza uklanja broj jedan, jer on po definiciji nije prost. Nakon toga, algoritam uzima sljedeći broj u nizu (broj 2), označava ga da je prost i iz niza uklanja sve njegove sadržioce (tj. brojeve djeljive sa 2), jer sigurno nisu prosti. Zatim se ponovo uzima sljedeći broj koji nije izbačen (broj 3) i uklanjaju se svi njegovi sadržioci. Obzirom da je broj 4 uklonjen iz niza, jer je djeljiv sa 2, algoritam će uzeti broj 5. Ovaj postupak će se ponavljati i na kraju će u nizu ostati samo prosti brojevi.

Kada implementiramo Eratostenovo sito, dovoljno je obraditi brojeve koji su manji ili jednaki $\sqrt{N}$. Dakle, ako tražimo proste brojeve od 1 do 100, dovoljno je da iz niza izbacimo sadržioce brojeva koji su manji ili jednaki 10.

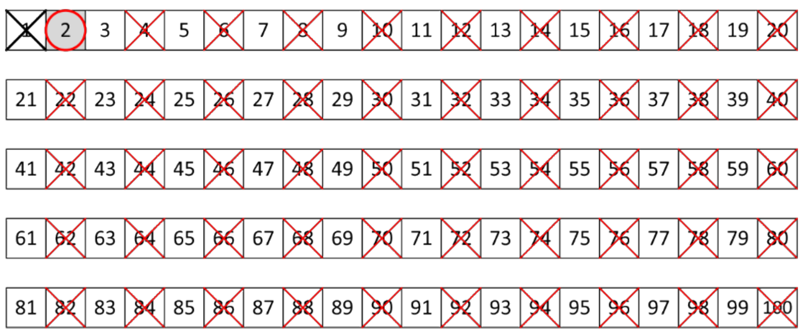
Predstavićemo rad algoritma koji traži sve proste brojeve od 1 do 100. Na početku imamo niz u kojem se nalaze svi brojevi od 1 do 100.

Izvor: https://skolakoda.github.io/eratostenovo-sito

KORACI ALGORITMA ERATOSTENOVOG SITA

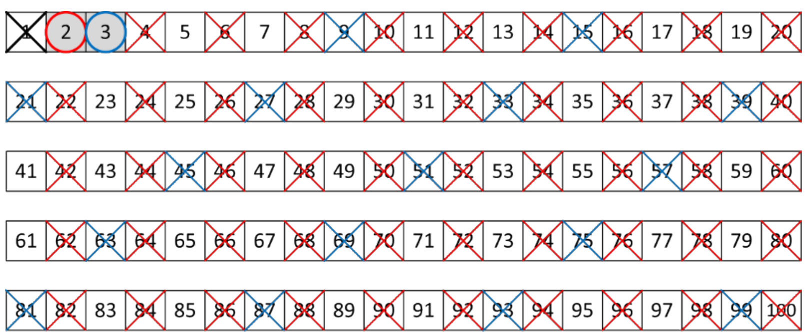
Rad algoritma koji traži sve proste brojeve od 1 do 100

Korak 1 - Na početku ćemo izbaciti broj 1, jer po definiciji nije prost. Nakon toga, obeležavamo broj 2 kao prost, i izbacujemo sve njegove sadržioce.



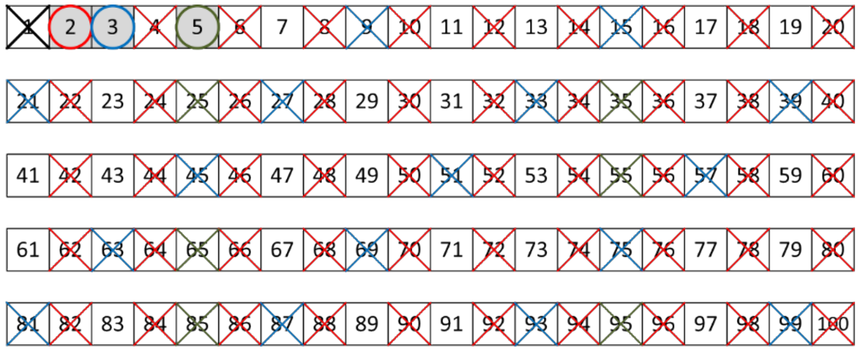
Slika 1.1.1 Korak 1 algoritme Eratostenovog sita [Izvor: https://skolakoda.github.io/eratostenovo-sito]

Korak 2 - Sledeći broj koji nije izbačen je 3. Algoritam ga označava da je prost i izbacuje sve njegove sadržioce.



Slika 1.1.2 Korak 2 algoritme Eratostenovog sita [Izvor: https://skolakoda.github.io/eratostenovo-sito]

Korak 3 - Broj 4 je ranije izbačen, tako da algoritam uzima broj 5 označava ga da je prost i izbacuje sve njegove sadržioce.



Slika 1.1.3 Korak 3 algoritme Eratostenovog sita [Izvor: https://skolakoda.github.io/eratostenovo-sito]

Korak 4 - Sada izvršavamo isti postupak za broj 7.

Slika 1.1.4 Korak 4 algoritme Eratostenovog sita [Izvor: https://skolakoda.github.io/eratostenovo-sito]

IMPLEMENTACIJA ALGORITMA ERATOSTENOVO SITO

Implementacija algoritma Eratostenovo sito u Pythonu

```
def nadji_proste_brojeve(n):
    prosti = set()
    slozeni = set()

    for i in range(2, n + 1):
        if i not in slozeni:
            prosti.add(i)
            for j in range(i * i, n + 1, i):
                slozeni.add(j)
    return prosti

print(nadji_proste_brojeve(100))
```

Izvor: https://skolakoda.github.io/eratostenovo-sito

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

1.1 UZAJAMNO PROSTI BROJEVI

DEFINICIJA UZAJAMNO PROSTIH BROJEVA

Neka su a, b ∈ Z, takvi da nisu istovremeno jednaki 0. Tada se za a i b kaže da su uzajamno prosti ako gcd(a, b) = 1

Definicija
Neka su a, b $\in \mathbb{Z}$, takvi da nisu istovremeno jednaki 0.
Tada se za a i b kaže da su uzajamno prosti ako
gcd(a, b) = 1

Napomena: U literaturi koja je pisana na srpskom jeziku se često umesto engleske skraćenice gcd, navodi nzd. U lekcijama iz ovog predmeta koristićemo skraćenicu gcd.

Ako su a i b uzajamno prosti, onda postoje x, y $\in \mathbb{Z}$ takvi da

a x + b y = 1

Obrnuto, ako a x + b y = 1, onda su a i b uzajamno prosti.
Primer
Za sledeće brojeve kažemo da su uzajamno prosti zato što je njihov najveći zajednički delilac 1
gcd(12, 35) = 1, gcd(49, 18) = 1,gcd(21, 64) = 1 i gcd(−28, 45) = 1

Primer
Ako su p i q različiti prosti brojevi, onda
gcd(p, q) = 1

Primer
Za brojeve a i a+1 važi da
gcd(a, a + 1) = 1,
pošto svaki zajednički delilac brojeva a i a + 1 mora deliti i njihovu razliku
a + 1 − a = 1

1.2 FUNDAMENTALNA TEORIJA ARITMETIKE

TEOREMA ARITMETIKE

Svaki ceo broj n > 1 je proizvod prostih brojeva; takva dekompozicija na proste brojeve je jedinstvena. Ako su p i q prosti brojevi i ako p|q, onda p = q

Svaki ceo broj n > 1 je proizvod prostih brojeva; takva dekompozicija na proste brojeve je jedinstvena. Ako su p i q prosti brojevi i ako p|q, onda p = q.
Ako su p, q_1, q_2, ... qr prosti brojevi i ako p |($q_1 q_2$ ... q_r), onda postoji k koji je 1 ≤ k ≤ r takav da p = q_k

Dokaz:

Jedini delioci broja q su $\pm$ 1 i $\pm$ q. Pošto je p > 1, imamo p = q.
Pretpostavimo

$$n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_k$$

gde su $p_1 p_2 \ldots p_k \ i \ q_1 q_2 \ldots q_k$prosti brojevi. Tada

$$p_1 | (q_1 \ldots . q_r)$$

dakle $p_1 = q_j \ za \ neko \ j \ koje \ je \ 1 \leq j \leq r.$
Preuredimo redosled prostih faktora q_j tako da bude $p_1 = q_1$, i dobijamo

$$p_1 p_2 \ldots p_k = p_1 q_2 \ldots q_r$$

pa onda $p_2 \ldots p_k = q_2 \ldots . q_r$

Primenom istog argumenta, sada možemo preurediti redosled ostalih prostih faktora q_j tako da p_2 = q_2. Nastavljanjem ovog procesa, vidimo da n može biti, na jedinstven način izražen u obliku proizvoda prostih brojeva. Prosti brojevi u faktorizaciji broja n ne moraju biti različiti. Često je korisno objediniti jednake proste faktore. Tada se n može, na jedinstven način, izraziti u obliku

$$n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$$
$$m_k \in \mathbb{N} \ \ za \ \ 1 \leq k \leq r \ \ i \ \ p_1 < p_2 < \ldots p_r.$$

FAKTORIZACIJA NA PROSTE BROJEVE

Iako izgleda dosta jednostavno, fundamentalna teorema aritmetike nije ni malo trivijalna. U nastavku sledi primer sistema brojeva koji ne zadovoljava ovu teoremu

Primer

Neka a = 24 · 33 · 7 · 11 i b = 23 · 32 · 52 · 11 · 17.
Odrediti d = gcd(a, b) i m = lcm(a, b).

Rešenje:

- Prvo određujemo d = gcd(a, b).
- Prosti brojevi p_k koji se javljaju i u razvoju a i u razvoju b, konkretno, 2, 3 i 11, se takođe javljaju i u razvoju d, a eksponent broja p_k je manji od eksponenata iz razvoja a i razvoja b.
- Tako imamo d = gcd(a, b) = 23 · 32 · 11 = 792.
  Sada određujemo m = lcm(a, b).
- Prosti brojevi p_k koji se javljaju bilo u razvoju a bilo u razvoju b, konkretno, 2, 3, 5, 7, 11 i 17 se takođe javljaju u razvoju m, a eksponent broja p_k je veći od eksponenata iz razvoja a i razvoja b.
- Tako imamo m = lcm(a, b) = 24 · 33 · 52 · 7 · 11 · 17.

Iako izgleda dosta jednostavno, fundamentalna teorema aritmetike nije ni malo trivijalna. Dajemo primer sistema brojeva koji ne zadovoljava ovu teoremu.

Neka je F = {m = 3n + 1 : n $\in \mathbb{N}_0$ }. Tako se F sastoji iz brojeva 1, 4, 7, 10, 13, 16, 19, 22, ...
Primetimo da proizvod dva broja iz F pripada F, pošto
(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1.

Naša definicija prostih brojeva se može lepo uklopiti u sistem brojeva F . Prvih nekoliko prostih brojeva iz F su **4, 7, 10, 13,19, 22, 25;**
4 je prost broj u F, pošto 4 nema faktore u F osim 1 i 4. Na isti način dobijamo da su 10, 22 i 25 prosti u F. Primetimo da
3 · 33 + 1 ∈ F
Međutim, 100 ima dve bitno različite faktorizacije u terminima prostih brojeva iz sistema F. Konkretno
100 = 4 · 25 i 100 = 10 · 10.
Tako, faktorizacija na proste brojeve iz sistema brojeva F nije jedinstvena u F.

Poglavlje 2

DELJIVOST

POJAM DELJIVOSTI

Neka a, b ∈ Z pri čemu je a = 0. Ako postoji c ∈ Z takvo da a • c = b tada kažemo da a deli b ili da je b deljivo sa a, u oznaci a|b.

Skup celih brojeva je zatvoren u odnosu na sabiranje, oduzimanje i množenje. Drugim rečima, sume, razlike i proizvodi celih brojeva su uvek celi brojevi. Ovo, medjutim, ne važi u opštem slučaju za deljenje celih brojeva. Drugim rečima, količnik dva cela broja ne mora biti ceo broj.

Zato je interesantno izučiti kada je rezultat deljenja celih brojeva, ceo broj, to jest, kada jedan ceo broj deli drugi ceo broj.

Postoji specijalna vrsta prirodnih brojeva čiji se elementi dele (pri deljenju se dobija ceo broj) samo sa 1 i samim sobom. Ovi brojevi se zovu prosti brojevi. Oni se ne mogu faktorizovati (razložiti) na manje celobrojne delove.

Definicija
Neka a, b $\in \mathbb{Z}$ pri čemu je a = 0.
Ako postoji c $\in \mathbb{Z}$ takvo da a • c = b tada kažemo
da a deli b ili da je b deljivo sa a, u oznaci
a|b
Takodje kažemo da je b umnožak broja a ili
da je a faktor ili delioc broja b.

Primer

(a) Važi 3|6, pošto 3 • 2 = 6, i −4|28, pošto (−4)(−7) = 28.

(b) Delioci broja

- 1 su ±1;
- 2 su ±1, ±2;
- 4 su ±1, ±2, ±4;
- 5 su ±1, ±5;
- 7 su ±1, ±7;
- 9 su ±1, ±3, ±9

(c) Ako a = 0, onda a|0, pošto a • 0 = 0.

(d) Svaki ceo broj a je deljiv sa ±1 i ±a. Ovi delioci se zovu trivijalni delioci broja a.

ALGORITAM DELJENJA

U algoritmu deljenja, d se naziva delilac, a se naziva deljenik, q se naziva količnik, a r se naziva ostata

Neka je a ceo broj, a d pozitivan ceo broj. Tada postoje jedinstveni celi brojevi q i r, sa 0 ≤ r < d, tako da važi a = dq + r.

U jednakosti koja se koristi u algoritmu deljenja , *d* se naziva delilac, *a* se naziva deljenik, *q* se naziva količnik, a *r* se naziva ostatak. Ova notacija se koristi za izražavanje količnika i ostatka:

q = a **div** d, r = a **mod** d.

Primer

Koji su količnik i ostatak kada se broj 101 deli sa 11?

Rešenje:

Imamo 101 = 11 * 9 + 2. Dakle, količnik kada se 101 deli sa 11 je 9 = 101 div 11, a ostatak je 2 = 101 mod 11.

Primer

Koji su količnik i ostatak kada se broj -11 deli sa 3?

Rešenje:

Imamo −11 = 3(−4) + 1.

Dakle, količnik kada se -11 deli sa 3 je −4 = −11 div 3, a ostatak je 1 = −11 mod 3.

Napomena je da ostatak ne može biti negativan.

Stoga, ostatak nije −2, iako važi −11 = 3(−3) − 2, jer vrednost r = −2 ne zadovoljava uslov 0 ≤ r < 3.

PRIMER KORIŠĆENJA MOD FUNKCIJE

Primena funkcije modulo u kompijuterskoj nauci

Primer

Primer zašto ovaj koncept može biti koristan:

“Ako je 21 juni, 1997 subota, koji je dan u nedelji 4 jula, 2000?”

Rešenje:

2000-ta godina je prestupna godina, pa je broj dana između ova dva datuma sledeći

$13 + 3 \cdot 365 + 1 = 1109$

a=1109, b=7, pa možemo pronaći broj celih nedelja (q)

1109 mod 7 = 3

odnosno q=158, r=3

odnosno 3 dana posle subote 4 juli 2000-te je utorak.

Primer

Prethodni primer je možda ograničen, ali princip cikličnosti se koristi često u matematici.

Ako želimo da odredimo 500-tu decimalu kada delimo 1 i 13, odnosno 1/13, mozemo koristiti algoritam deljenja.

Decimalno rešenje ova dva broja je ciklično, odnosno 6 cifara se ponavlja

1/13=.076923076923...
Prema tome po modulu možemo naci količnik i ostatak
500 mod 6 = 2
Rešenje:
500-ti broj će predstavljati drugi broj u nizu šest cikličnih brojeva, a to je “7”

Poglavlje 3

PROŠIRENI EUKLIDOV ALGORITAM

KARAKTERISTIKE NAJVEĆEG ZAJEDNIČKOG DELIOCA

Neka su a, b $\in \mathbb{Z}$ i neka nisu oba jednaka 0. Ceo broj d je zajednički delioc brojeva a i b ako d deli i a i b, to jest, ako d|a i d|b.

Definicija

Neka su a, b $\in \mathbb{Z}$ i neka nisu oba jednaka 0. Ceo broj d je zajednički delioc brojeva a i b ako d deli i a i b, to jest, ako d|a i d|b

Primetimo da je 1 pozitivan delioc bilo kojih celih brojeva a i b, i da nijedan zajednički delioc brojeva a i b ne može biti veći od |a| ili |b|. Zbog toga postoji najveći zajednički delioc brojeva a i b, i označava se sa nzd(a,b) ili gcd (a,b).

Neka je d najmanji prirodan broj oblika ax + by. Tada **d = gcd(a, b).**

Sledeći rezultat je neposredna posledica ove teoreme.

Neka je d = gcd(a, b). Tada postoje x, y $\in \mathbb{Z}$ ***takvi da***

d = a • x + b • y.

Primedba

(a) Jasno je da se najveći zajednički delilac d = gcd(a, b) može okarakterisati osobinom

(1) d deli i a i b. (2) Ako c deli i a i b, onda c|d.

(b) Najveći zajednički delilac brojeva a i b ima sledeće osobine

(1) gcd(a, b) = gcd(b, a).

(2) Ako x > 0, onda gcd(ax, bx) = x • gcd(a, b).

(3) Ako d = gcd(a, b), onda gcd(a/d, b/d) = 1.

(4) gcd(a, b) = gcd(a, b + ax) za neko x $\in \mathbb{Z}$.

PRIMER PROŠIRENOG EUKLIDOVOG ALGORITMA

Navedeni primer bliže objašnjava Euklidov algoritam.

Ovde dajemo vezu između Neka a = 540 i b = 168. Nalazimo d = gcd(a, b) ponavljanjem deljenja svakog ostatka sa deliocem sve dok za ostatak ne dobijemo nulu

Poslednji ne-nula ostatak je 12, pa je 12 = gcd(540, 168). Ovo sledi iz sukcesivnog deljenja ostatka u Euklidovom algoritmu

(1) $540 = 3 \bullet 168 + 36$ ili $36 = 540 - 3 \bullet 168$

(2) $168 = 4 \bullet 36 + 24$ ili $24 = 168 - 4 \bullet 36$

(3) $36 = 1 \bullet 24 + 12$ ili $12 = 36 - 1 \bullet 24$.

Dalje, nalazimo x i y takve da

$12 = 540x + 168y$

Jednačina (3) pokazuje da je 12 linearna kombinacija brojeva 36 i 24.

Koristimo (2) da bi zamenili 24 u (3) pa možemo zapisati 12 kao linearnu kombinaciju brojeva 168 i 36 na sledeći način

$12 = 36 - 1(168 - 4 \bullet 36) = 36 - 1 \bullet 168 + 4 \bullet 36 = 5 \bullet 36 - 1 \bullet 168.$

Sada koristimo (1) iz (4) da bi zapisali 12 kao linearnu kombinaciju brojeva 168 i 540

$12 = 5(540 - 3 \bullet 168) - 1 \bullet 168 = 5 \bullet 540 - 15 \bullet 168 - 1 \bullet 168 = 5 \bullet 540 - 16 \bullet 168.$

Tako dobijamo $x = 5$ i $y = -16$ u linearnoj kombinaciji.

Poglavlje 4

RELACIJA KONGRUENCIJE

DEFINICIJA RELACIJE KONGRUENCIJE

Neka je dat $m \in N$. Dva cela broja a i b su kongruentna po modulu m, u oznaci $a \equiv b(\text{mod } m)$

Definicija
Neka je dat $m \in N$. Dva cela broja a i b su kongruentna po modulu m, u oznaci $a \equiv b(\text{mod } m)$, ako m deli razliku $a - b$. Prirodan broj m se zove moduo.
Negacija iskaza $a \equiv b(\text{mod } m)$ se zapisuje na sledeći način $a \not\equiv b(\text{mod } m)$.

Primer

Imamo

(i) $87 \equiv 23(\text{mod } 4)$, pošto 4 deli $87 - 23 = 64$;

(ii) $67 \equiv 1(\text{mod } 6)$, pošto 6 deli $67 - 1 = 66$;

(iii) $72 \equiv -5(\text{mod } 7)$, pošto 7 deli $72 - (-5) = 77$;

(iv) $27 \not\equiv 8(\text{mod } 9)$, pošto 9 ne deli $27 - 8 = 19$.

OSOBINE KONGRUENCIJE PO MODULU M

a i b su kongruentna po modulu m ako i samo ako imaju isti ostatak pri deljenju sa m

Neka je $m \in \mathbb{N}$. Tada imamo

1. $a \equiv a(\text{mod } m)$ za sve $a \in \mathbb{Z}$;
2. ako $a \equiv b(\text{mod } m)$, onda $b \equiv a(\text{mod } m)$;
3. ako $a \equiv b(\text{mod } m)$ i $b \equiv c(\text{mod } m)$ onda $a \equiv c(\text{mod } m)$.

Dokaz:

1. **Kako je razlika $a - a$ deljiva sa m, imamo $a \equiv a(\text{mod } m)$**
2. Ako $a \equiv b(\text{mod } m)$, onda $m|(a - b)$. Zatim, $m| - (a - b)$,

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

pa važi $b \equiv a \pmod m$.
3. Ako $a \equiv b \pmod m$ i $b \equiv c \pmod m$, onda

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

pa onda

$m \mid (a - b) + (b - c)$,

a kako je

$(a - b) + (b - c) = a - c$,

važi

$a \equiv c \pmod m$.

Neka su dati $m \in \mathbb{N}$ i $a \in \mathbb{Z}$. Po algoritmu deljenja postoje $q, r \in \mathbb{Z}$ pri čemu $0 \le r < m$ takvi da $a = mq + r$. Prema tome, sledi

$mq = a - r$ ili $m | (a - r)$ ili $a \equiv r \pmod m$.

Tako imamo:

- **a i b su kongruentna po modulu m ako i samo ako imaju isti ostatak pri deljenju sa m.**
- **Svaki ceo broj a je kongruentan po modulu m sa jednim jedinim celim brojem iz skupa {0, 1, .., m − 1}. Jedinstvenost sledi iz činjenice da m ne može deliti dva takva broja.**
- **Bilo koja dva cela broja a i b su kongruentna po modulu m ako i samo ako imaju isti ostatak pri deljenju sa m.**

PRIMERI ARITMETIKE KONGRUENCIJE

Neka $a \equiv c \pmod m$ i $b \equiv d \pmod m$. Tada imamo $a + b \equiv c + d \pmod m$ i $a \cdot b \equiv c \cdot d \pmod m$

Sledeći rezultat pokazuje da se, u odnosu na sabiranje i množenje, relacija kongruencije ponaša vrlo slično relaciji jednakosti.

Neka

$a \equiv c \pmod m$

i

$b \equiv d \pmod m$.

Tada imamo

1. $a + b \equiv c + d \pmod m$

2. a · b ≡ c · d(mod m)

Po definiciji,

a ≡ c (mod m)

i

b ≡ d (mod m)

znači m|(a−c) i m |(b − d).

Tada imamo m |(a − c) + (b − d),
a kako je
(a − c) + (b − d) = (a + b) − (c + d),
onda imamo
a + b ≡ c + d(mod m).
Tada imamo
m |b(a − c) i m|c (b − d),
pa onda
m |(b (a − c) + c (b − d)),
a kako je,
b(a − c) + c(b − d) = ab − bc + bc − cd= ab − cd,

važi
ab ≡ cd (mod m).

ZAKONI KANCELACIJE ZA KONGRUENCIJE

Celi brojevi zadovoljavaju zakon kancelacije "ako ab = ac i a ≠ 0 onda b = c"

Skup celih brojeva po modulu m, u oznaci $\mathbb{Z}_m$, je skup

$\mathbb{Z}_m$ = {0, 1, 2, . . . , m − 1},

pri čemu se sabiranje i množenje definišu preko aritmetike po modulu m, ili, ekvivalentno, preko odgovarajućih operacija za klase ostataka.

Tablice iz prethodnog primera se mogu posmatrati i kao tablice sabiranja i množenja za $\mathbb{Z}_6$. Ovo znači da ne postoji suštinska razlika između $\mathbb{Z}_m$ i aritmetike klasa ostataka po modulu m. Zato ćemo ova dva termina upotrebljavati kao sinonime.

Setimo se da celi brojevi zadovoljavaju zakon kancelacije***.***

Ako ab = ac i a ≠ 0 onda b = c.

Značajna razlika između klasične aritmetike i aritmetike po modulu m je u tome što gornji zakonkancelacije ne važi za kongruencije.

Imamo

3 x 1 ≡ 3 x 5(mod 6),

ali 1≢ 5(mod 6),

to jest, ne možemo skratiti (poništiti) 3.

Međutim, važi sledeći rezultat. Ako

ab ≡ ac(mod m)

i

d = gcd(a, m),

onda

b ≡ c(mod m/d).

Poglavlje 5

KLASE OSTATAKA

OBJAŠNJENJE KLASE OSTATAKA

Kako je kongruencija po modulu m relacija ekvivalencije, ona deli skup Z na particije klasama ekvivalencije koje se zovu klase ostataka po modulu m

Kako je kongruencija po modulu m relacija ekvivalencije, ona deli skup **Z** na particije klasama ekvivalencije koje se zovu klase ostataka po modulu m. Jedna klasa ostatka se sastoji od svih celih brojeva koji imaju isti ostatak pri deljenju sa m.

Prema tome, postoji m takvih klasa ostataka, a svaka od njih sadrži tačno jedan broj iz skupa $\{0, 1, \ldots m - 1\}$ za mogući ostatak. Uopšteno govoreći, skup celih brojeva $\{n_1, n_2, \ldots, n_m\}$ je potpun sistem ostataka po modulu m ako svako n_k dolazi iz različite klase ostatka.

Tako celi brojevi od 0 do m −1 formiraju potpun sistem ostataka po modulu m; u stvari, bilo koji skup m uzastopnih celih brojeva formira potpun sistem ostataka po modulu m.

Oznaka $[x]_m$ ili samo [x] se koristi da označi klasu ostatka po modulu m koja sadrži ceo broj x, to jest, one cele brojeve koji su kongruentni sa x.

Drugim rečima, $[x] = \{a \in \mathbb{Z} : a \equiv x (\text{mod } m)\}$.

Tako se klase ostataka po modulu m mogu označiti sa

$[0], [1], [2], \ldots, [m - 1]$

ili pomoću bilo kog drugog izbora celih brojeva u potpunom sistemu ostataka.

Primer

Klase ostataka po modulu m = 6 su

[0] = {... , −18, −12, −6, 0, 6, 12, 18, ...},

[1] = {... , −17, −11, −5, 1, 7, 13, 19, ...},

[2] = {... , −16, −10, −4, 2, 8, 14, 20, ...},

[3] = {..., −15, −9, −3, 3, 9, 15, 21, ...},

[4] = {... , −14, −8, −2, 4, 10, 16, 22 ...},

[5] = {..., −13, −7, −1, 5, 11, 17, 23, ...},

Primetimo da je {−2, −1, 0, 1, 2, 3} potpun sistem ostataka po modulu m = 6.

SABIRANJE I MNOŽENJE KLASA OSTATAKA PO MODULU M

Sabiranje i množenje klasa kongruencije su dobro definisani, to jest, sume i proizvodi klasa ostataka ne zavise od izbora reprezentativnog elementa klase ostatka

Sabiranje i množenje klasa ostataka po modulu m se definišu na sledeći način

[a] + [b] = [a + b] i [a] x [b] = [ab]

Posmatrajmo klase ostataka po modulu 6, to jest [0], [1], [2], [3], [4] i [5]. Tada, po gornjoj definiciji, imamo

[2] + [3] = [5], [4] + [5] = [9] = [3],

[2] x [2] = [4] i [2] x [5] = [10] = [4].

Sabiranje i množenje klasa kongruencije su dobro definisani, to jest, sume i proizvodi klasa ostataka ne zavise od izbora reprezentativnog elementa klase ostatka.

Postoji samo konačan broj, m, klasa ostataka po modulu m. Zato se mogu lako ispisati tablice za sabiranje i množenje, kada je m mali broj.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Slika 5.1 Tablice sabiranja i mnozenja po modulu 6 [Izvor: autor]

Poglavlje 6

OJLEROVA FUNKCIJA

OSLABLJENI SISTEMI OSTATAKA

Broj klasa ostataka koje su uzajamno proste sa m ili, ekvivalentno, broj celih brojeva između 1 i m (uključujući i njih) koji su uzajamno prosti sa m se označava sa ϕ (m)

Modifikovani zakon poništenja, ukazuje na specijalnu ulogu koju igraju celi brojevi koji su uzajamno prosti (ko-prosti) sa modulom m. Primetimo da je a ko-prost sa m ako i samo ako je svaki element iz klase ostatka [a] ko-prost sa m. Zbog toga možemo govoriti o klasi ostatka koja je ko-prosta sa m.

Definicija
Broj klasa ostataka koje su uzajamno proste sa m ili,
ekvivalentno, broj celih brojeva između 1 i m
(uključujući i njih) koji su uzajamno prosti sa m se
označava sa ϕ (m).

Funkcija ϕ se zove Ojlerova ϕ funkcija
(engl. Euler ϕ function).

Lista brojeva između 1 i m koji su ko-prosti sa m ili, opštije, bilo koja lista od ϕ (m) nekongruentnih celih brojeva koji su ko-prosti sa m, se zove oslabljen sistem ostataka po modulu m.

Primer
Posmatrajmo moduo m = 15.
Postoji osam brojeva između 1 i 15 koji su ko-prosti sa 15, konkretno
1, 2, 4, 7, 8, 11, 13 i 14
Dakle

ϕ (15) = 8.

Gore pomenuti brojevi formiraju oslabljen sistem ostataka po modulu 15.

Primer
Neka je p proizvoljan prost broj.
Svi brojevi

1, 2, ..., p-1

su ko-prosti sa p, pa je

ϕ (p) = p − 1.

OJLEROVA ϕ FUNKCIJA

Izračunavanje Ojlerove funkcije

Posmatrajmo sada proizvoljnu kolonu matrice S . Ona se sastoji iz brojeva

k, a + k, 2a + k, 3a + k, . . . , (b − 1)a + k.

Tvrdimo da ovi celi brojevi formiraju sistem ostataka po modulu b, to jest, ne postoje dva cela broja od njih koja su konguentna po modulu b.

Pretpostavimo suprotno, to jest da

na + k ≡ n’a + k(mod b),

pa na ≡ n’a(mod b).

Kako su a i b ko-prosti, po modifikovanom zakonu poništenja, dobijamo

n ≡ n’(mod b)

Međutim, imamo da

n, n’∈ {0, 1, . . . , b − 1},

tako je

n = n’.
Prema tome, proizvoljna kolona matrice sadrži tačno $\phi(b)$ celih brojeva koji su ko-prosti sa b. Pokazali smo da matrica S sadrži $\phi(a)$ kolona koje sadrže cele brojeve koji su ko-prosti sa a, i da se svaka kolona sadrži $\phi(b)$ celih brojeva koji su ko-prosti sa b. Tako postoji $\phi(a)\phi(b)$ celih brojeva matrice S koji su ko-prosti i sa a i sa b.
Prema tome važi

ϕ (ab) = ϕ (a) ϕ (b).
Ojlerovu ϕ funkciju možemo izračunati na sledeći način, gde $p_1, p_2, \ldots p_r$ predstavljaju proste brojeve

$$\phi(n) = p_1^{k_1}(1-\frac{1}{p_1})p_2^{k_2}(1-\frac{1}{p_2})\ldots p_r^{k_r}(1-\frac{1}{p_r})$$

Odnosno
$$\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_r})$$

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

PRIMER OJLEROVE FUNKCIJE

Odrediti Ojlerovu funkciju broja 36

Primer

Odrediti ϕ (36).

Rešenje:
Broj 36 možemo prikazati kao proizvod prostih brojeva 2 i 3 na sledeći način

$36=2^3\ 3^2$

Ovu faktorizaciju koristimo za Ojlerovu funkciju
ϕ (36)= ϕ ($2^3 * 3^2$)
ϕ (36)=36(1-1/2)(1-1/3)=12

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 7

JEDNAČINE KONGRUENCIJE

DEFINICIJA JEDNAČINE KONGRUENCIJE

Jednačina kongruencije (jedne nepoznate x)

Definicija
Polinomijalna relacija kongruencije, ili jednostavno, jednačina kongruencije (jedne nepoznate x) je jednačina oblika
$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod m$,
gde
$a_k \in \mathbb{Z}$ za $k = 0, 1, \dots, n$.

Takva jednačina je stepena n ako

$a_n \not\equiv 0 \pmod m$.

Ako

$s \equiv t \pmod m$,

važi da je s rešenje jednačine kongruencije ako i samo ako je t njeno rešenje. Tako je broj rešenja određen brojem nekongruentnih rešenja ili, ekvivalentno, brojem rešenja iz skupa

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

Naravno, rešenja se uvek mogu naći testiranjem, to jest, zamenom svakog od m brojeva u jednačini. Opšte rešenje jednačine kongruencije se može odrediti dodavanjem svih umnožaka po modulu m bilo kom potpunom skupu rešenja.
Primer
Posmatramo jednačine

$(a)\ x^2 + x + 1 \equiv 0(mod\ \ 4)$
$(b)\ x^2 + 3 \equiv 0(mod\ \ 6)$
$(c)\ x^2 - 1 \equiv 0(mod\ \ 8)$

Ovde nalazimo rešenja testiranjem:

(a) Ne postoji ni jedno rešenje, pošto nijedan od brojeva 0, 1, 2 i 3 ne zadovoljava jednačinu.

(b) Postoji samo jedno rešenje među brojevima 0, 1 . . . , 5, a to je 3. Tako se opšte rešenje sastoji iz svih celih brojeva oblika 3 + 6k, gde je $k \in \mathbb{Z}$.

(c) Postoji četiri rešenja 1, 3, 5 i 7. Ovo ukazuje na činjenicu da jednačina kongruencije stepena n može imati više od n rešenja.

7.1 Linearna jednačina kongruencije oblika ax≡ 1 (mod m)

AX≡ 1 (MOD M)

Ako je gcd(a, m) = 1 onda jednačina kongruencije ax ≡ 1(mod m) ima jedinstveno rešenje; inače, ona nema rešenja

Prvo posmatramo specijalnu linearnu jednačinu kongruencije *ax ≡ 1(mod m),* gde a ≡ 0(mod m).

Ako je gcd(a, m) = 1

onda jednačina kongruencije ax ≡ 1(mod m)

ima jedinstveno rešenje; inače, ona nema rešenja.

Primer

Posmatrajmo jednačinu kongruencije

6x ≡ 1(mod 33)

Pošto je gcd(6, 33) = 3, jednačina kongruencije nema rešenja

Primer 8.16

Posmatrajmo jednačinu kongruencije 7x ≡ 1(mod 9)

Ovde je gcd(7, 9) = 1,

pa jednačina kongruencije ima jedno i samo jedno rešenje. Testiranjem brojeva 0, 1, . . . , 8, nalazimo

7 · 4 = 28 ≡ 1(mod 9)

Tako je x = 4 jedinstveno rešenje; a opšte rešenje je
x = 4 + 9k za k $\in \mathbb{Z}$.

Ako gcd(a, m) = 1, a moduo m veliki broj, onda možemo koristiti Euklidov algoritam za nalaženje rešenja jednačine ax ≡ 1(mod m)
Nalazimo x_0 i y_0 takve da
$ax_0 + my_0 = 1.$
Iz ovoga sledi da je
$ax_0 \equiv 1(mod \ \ m),$
to jest, da je x_0 rešenje jednačine
$ax \equiv 1(mod \ \ m)$

Primer

Posmatrajmo jednačinu kongruencije 81x ≡ 1(mod 256)

Euklidov algoritam nas dovodi do gcd(81, 256) = 1. Zbog toga jednačina ima jedinstveno rešenje. Testiranje nije efikasan način za nalaženje ovog rešenja pošto je moduo m = 256 veliki broj. Zbog toga primenjujemo Euklidov algoritam na brojeve a = 81 i m = 256 i nalazimo,
$x_0 = -79 \ i \ y_0 = 25$ takve da
$81x_0 + 256y_0$
Ovo znači da je $x_0 = -79$ rešenje date jednačine kongruencije.
Sabiranjem m = 256 i -79, dobijamo jedinstveno rešenje
$x = 177$
koje je između 0 i 256.

7.2 Linearna jednačina kongruencije oblika ax≡b(mod m)

AX≡B(MOD M)

ax ≡ b(mod m), gde a ≢ 0(mod m) Neka je gcd(a, m) = 1. Tada jednačina kongruencije ax ≡ b(mod m) ima jedinstveno rešenje

Sada posmatramo opštiju linearnu jednačinu kongruencije

ax ≡ b(mod m),

gde

a ≢ 0(mod m)

Neka je gcd(a, m) = 1. Tada jednačina kongruencije ax ≡ b(mod m) ima jedinstveno rešenje.

I više od toga, ako je **s** jedinstveno rešenje jednačine **ax ≡ 1(mod m)**, onda je **x = bs** jedinstveno rešenje jednačine **ax ≡ b(mod m).**

Rešenje s jednačine kongruencije **ax ≡ 1(mod m)** postoji, po teoremi

Ako je gcd(a, m) = 1 onda jednačina kongruencije

ax ≡ 1(mod m) ima jedinstveno rešenje; inače, ona nema rešenja.

Odatle imamo

as ≡ 1(mod m),

a po aritmetici kongruencije

a(bs) = (as)b ≡ 1b = b(mod m).

To jest, x = bs je rešenje jednačine

ax ≡ b(mod m).

Sada pokazujemo jedindstvenost. Neka su x_0 i x_1 dva takva rešenja.

Tada imamo

$ax_0 \equiv b \equiv ax_1 (\text{mod } m)$.

Pošto je gcd(a, m), po modifikovanom zakonu poništenja, imamo $x_0 \equiv x_1 (\text{mod } m)$, to jest, $ax \equiv b (\text{mod } m)$ ima jedinstveno rešenje po modulu m.

Primer

Rešiti jednačinu kongruencije $4x \equiv 9 (\text{mod } 14)$

Rešenje:

Imamo gcd(4, 14) = 2. Međutim, 2 ne deli 9. Zbog toga, jednačina kongruencije nema rešenje

PRIMERI JEDNAČINA KONGRUENCIJE OBLIKA AX≡B(MOD M)

ax ≡ b(mod m), gde a ≢ 0(mod m). Neka je gcd(a, m) = 1. Tada jednačina kongruencije ax ≡ b(mod m) ima jedinstveno rešenje

$ax \equiv b (\text{mod } m)$, gde $a \not\equiv 0 (\text{mod } m)$. Neka je gcd(a, m) = 1. Tada jednačina kongruencije $ax \equiv b (\text{mod } m)$ ima jedinstveno rešenje.

$ax \equiv b (\text{mod } m)$ gde je d = gcd(a, m). Ako d ne deli b, onda $ax \equiv b (\text{mod } m)$ nema rešenje

Primer

Pronaći rešenje sledeće jednačine kongruencije

$33x \equiv 38 (\text{mod } 280)$ (1)

Rešenje:

Pošto je gcd(33, 280) = 1, (postoji jedinstveno rešenje)

Primenjujemo Euklidov algoritam za nalaženje prvog rešenja jednačine

$33x \equiv 1 (\text{mod } 280)$ (2)

$x_0 = 17 \; i \; y_0 = -2$ predstavljaju rešenje jednačine $33x_0 + 280y_0$

- Ovo znači da je s = 17 rešenje jednačine kongruencije (2)
- sb = 17x 38 = 646 rešenje originalne jednačine (1)
- Deljenjem 646 sa m = 280, dobijamo ostatak x = 86 koji
- predstavlja jedinstveno rešenje jednačine kongruencije (1) između 0 i 280.
- Opšte rešenje je 86 + 280k gde je k $\in \mathbb{Z}$.

PRIMER 2 - AX ≡ B(MOD M)

ax ≡ b(mod m) gde je d = gcd(a, m). Ako d ne deli b, onda ax ≡ b(mod m) nema rešenje

Primer

Pronaći rešenje sledeće jednačine kongruencije

33x ≡ 38(mod 280) (1)

Rešenje:

Pošto je **gcd(33, 280) = 1**, (postoji jedinstveno rešenje)

Primenjujemo Euklidov algoritam za nalaženje prvog rešenja jednačine

33x ≡ 1(mod 280) (2)

$\star x_0 = 17 i y_0 = -2\, predstavljaju\ rešenje\ jednačine$
$33x_0 + 280y_0 = 1$

- Ovo znači da je s = 17 rešenje jednačine kongruencije (2)
- **sb = 17x 38 = 646** rešenje originalne jednačine (1)
- Deljenjem 646 sa m = 280, dobijamo ostatak x = 86 koji predstavlja jedinstveno rešenje jednačine kongruencije (1) između 0 i 280.
- Opšte rešenje je **86 + 280k** gde je k ∈ Z

VIDEO PRIMER REŠAVANJA 5 X ≡ 12 (MOD 19)

Primer jednačine kongruencije 5 x ≡ 12 (mod 19)

Ova lekcija sadrži video materijal. Ukoliko želite da pogledate ovaj video morate da otvorite LAMS lekciju.

Poglavlje 8

Vežba

ZADATAK 1

Primeri sa najvećim zajedničkim deliocem i najmanjim zajedničkim sadržaocem

Predviđeno vreme trajanja: 10 minuta

Neka je a = 8316 i b = 10920.

(a) Naći d = gcd(a, b), najveći zajednički delioc brojeva a i b.

(b) Naći cele brojeve m i n takve da d = ma + nb.

(c) Naći lcm(a, b), najmanji zajednički sadržalac brojeva a i b.

REŠENjE:

(a) a=8316 b=10920

10920=1•8316+2604

8316=3•2604+504

2604=5•504+84

504=6•84+0

d=gcd(10920, 8316)=84
(b) 84=2604-5•504

=2604-5•(8316-3•2604)

=16•2604-5•8316

=16•(10920-1•8316)-5•8316

=-21•8316+16•10920

d=ma+nb

d=-21a+16b

(c) $lcm(8316, 10920) = \frac{|8316*10920|}{(gcd(8316,10920)} = 1081080$

ZADATAK 2

Naredni zadatak služi za obnavljanje Euklidovog algoritma

Predviđeno vreme trajanja: 10 minuta
Odrediti NZD (368,688).

Rešenje:

Koristeći Euklidov algoritam imamo:

688=368•1+320

368=320•1+48

320=48•6+32

48=32•1+16

32=16•2
Dakle, NZD (368, 688) = 16.

ZADATAK 3

Primeri sa Ojlerovom funkcijom

Predviđeno vreme trajanja: 15 minuta

Naći:

(a) ϕ (81), ϕ (125), ϕ (7^6);

(b) ϕ (72), ϕ (76), ϕ (3000).
REŠENjE:

$$\phi(n) = \phi(p_1)^{(k_1)}) \bullet \phi(p_2)^{(k_2)})\ldots\phi(p_r)^{(k_r)})$$

$$= (p_1)^{(k_1)}(1 - \frac{1}{p_1}) * (p_2)^{(k_2)}(1 - \frac{1}{p_2})\ldots(p_r)^{(k_r)}(1 - \frac{1}{p+r})$$

$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots.(1 - \frac{1}{p_r})$$

$$\phi(81) = \phi(3^4) = 81(1 - 1/3) = 54$$

$$\phi(125) = \phi(5^3) = 125(1 - 1/5) = 100$$

$$\phi(7^6) = 7^6(1 - 1/7) = 100842$$

$$\phi(72) = \phi(3^2 2^3) = \phi(3^2)\phi(2^3) = 72(1 - 1/3)(1 - 1/2) = 24$$

$$\phi(76) = \phi(2^2 * 19) = 76(1 - 1/2)(1 - 1/19) = 36$$

$$\phi(3000) = \phi(3 * 2^3 * 5^3) = 3000(1 - 1/3)(1 - 1/2)(1 - 1/5) = 800$$

ZADATAK 4

Primer rešavanja kongruentne jednačine 10x≡5(mod 27)

Predviđeno vreme trajanja: 15 minuta

Naći sva cela rešenja za jednačinu

10x≡5(mod 27)

REŠENjE:

10x≡5(mod 27)

27=2•10+7

10=1•7+3

7=2•3+1

1=7-2•3

=7-2•(10-1•7)

=3•7-2•10

=3•(27-2•10)-2•10

=3•27-8•10

ax_0+my_0=1

-8•5=-40

-40+27=-13

-13+27=14

x=14+27k

ZADATAK 5

Primer rešavanja kongruentne jednačine 48x≡5(mod 223)

Predviđeno vreme trajanja: 15 minuta

Naći sva cela rešenja za jednačinu

48x≡5(mod 223)

REŠENjE:

48x≡5(mod 223)

223=4•48+31

48=1•31+17

31=1•17+14

17=1•14+3

14=4•3+2

3=1•2+1

1=3-1•2

=3-(14-4•3)

=5•3-14

=5•(17-1•14)-14

=5•17-6•14

=5•17-6•(31-1•17)

=11•17-6•31

=11•(48-1•31)-6•31

=11•48-17•31

=11•48-17•(223-4•48)

=79•48-17•223

79•5=395

395(mod 223)=172

x=172+223k

ZADATAK 6

Primer rešavanja kongruentne jednačine 9x≡15(mod 23)

Predviđeno vreme trajanja: 10 minuta

Naći sva cela rešenja za jednačinu

9x≡15(mod 23)

REŠENjE:

9x≡15(mod 23)

gcd(23,9)

23=2•9+5

9=1•5+4

5=1•4+1

4=1•4+0

1=5-4

=5-(9-5)

=2·5-9

=2·(2·9-23)-9

=2·23-5·9

-5•15=-75

-75(mod 23) = 17

x=17+23k

ZADATAK 7

Jedini brojevi između 1 i pn koji nisu uzajamno prosti su umnožci broja p

Predviđeno vreme trajanja: 15 minuta

Pokazati da, ako je p prost broj, onda

$\boldsymbol{\phi (p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)}$**,**

gde je ϕ Ojlerova ϕ funkcija.

REŠENjE:

$\phi (p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$

gcd(a, p_n) ≢ 1 ako je p|a

jedini brojevi između 1 i p_n koji nisu uzajamno prosti su umnožci broja p

2. 2p, 3p, p^{n-1}, p

Postoji p^{n-1} takvih umnožaka broja p

Svi ostali brojevi između 1 i p^n su uzajamno prosti sa p^n

Prema tome, imamo

$\phi\ (\mathbf{p^n}) = \mathbf{p^n - p^{n-1} = p^{n-1}(p - 1).}$

Poglavlje 9

Zadaci za samostalni rad

ZADACI

Zadaci za provežbavanje

Zadatak 1 - predviđeno vreme trajanja 10 minuta

Naći sva cela rešenje za jednačinu $22x \equiv 8 \pmod{254}$.

Zadatak 2 - predviđeno vreme trajanja 10 minuta

Naći sva cela rešenje za jednačinu $27x \equiv 72 \pmod{900}$.

Zadatak 3 - predviđeno vreme trajanja 10 minuta
Naći sva cela rešenja za jednačinu $729x \equiv 232 \pmod{256}$.

ZAKLJUČAK

U ovoj lekciji je objašnjen pojam kongruencije, uzajamno prostih brojeva i student je upoznat sa aritmetikom kongruencije, klasom ostataka. Bilo je reči o Ojlerovoj FI funkciji. U poslednjem delu lekcije akcenat je stavljen na linearne jednačine kongruencije u dva oblika.

Literatura

[1] Rosen, Kenneth H. "Discrete mathematics and its applications." AMC 10 (2007): 12.
[2] Epp, Susanna S. Discrete mathematics with applications. Cengage Learning, 2010.