

2. Kongruencije

- Kongruencija - izjava o djeljivosti;
- Teoriju kongruencija uveo je C. F. Gauss 1801.

Definicija 2.1 Ako cijeli broj n dijeli razliku $a - b$, onda kažemo da je a kongruentan b modulo n i pišemo $a \equiv b \pmod{n}$. U protivnom, kažemo da a nije kongruentno b modulo n i pišemo $a \not\equiv b \pmod{n}$.

Napomena: Budući je

$$n \mid (a - b) \iff -n \mid (a - b),$$

onda je dovoljno promatrati pozitivne module n , pa ćemo ubuduće pretpostaviti $n \in \mathbb{N}$.

Propozicija 2.1 Relacija "biti kongruentan modulo n " je relacija ekvivalencije na skupu \mathbb{Z} .

Dokaz:

Propozicija 2.2 Neka su a, b, c, d cijeli brojevi:

i) Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je $a \pm c \equiv b \pm d \pmod{n}$ i $ac \equiv bd \pmod{n}$;

ii) Ako je $a \equiv b \pmod{n}$, $d \in \mathbb{N}$ i $d \mid n$, onda je $a \equiv b \pmod{d}$;

iii) Ako je $a \equiv b \pmod{n}$, onda je $ac \equiv bc \pmod{nc}$ za svaki $c \neq 0$.

Dokaz:

Posljedica 2.2 Neka su a, b, k, l cijeli brojevi i neka je $a \equiv b \pmod{n}$, onda vrijedi:

i) $a \pm nk \equiv b \pm nl \pmod{n}$;

ii) $ak \equiv bk \pmod{n}$;

iii) $a^m \equiv b^m \pmod{n}$ za svaki $m \in \mathbb{N}$.

Dokaz:

Propozicija 2.3 Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{n}$, onda je $f(a) \equiv f(b) \pmod{n}$.

Dokaz:

Teorem 2.1 Neka su $a, b, c \in \mathbb{Z}$ tada vrijedi:
 $ca \equiv cb \pmod{n}$ ako i samo ako $a \equiv b \pmod{\frac{n}{\gcd(c,n)}}$.
 Specijalno, ako je $ca \equiv cb \pmod{n}$ i $\gcd(c, n) = 1$,
 onda je $a \equiv b \pmod{n}$.

Dokaz:

Definicija 2.2 Skup $S = \{x_1, \dots, x_n\}$ se naziva potpuni sustav ostataka modulo n ako za svaki $y \in \mathbb{Z}$ postoji točno jedan $x_j \in S$ takav da je $y \equiv x_j \pmod{n}$.
 Dakle, potpuni sustav ostataka modulo n dobivamo tako da iz svake klase ekvivalencije modulo n uzmemo po jedan član.

Potpunih sustava ostataka modulo n ima beskonačno. Jedan od njih je:

- Najmanji sustav nenegativnih ostataka modulo n :

$$\{0, 1, \dots, n - 1\}$$

- Sustav apsolutno najmanjih ostataka modulo n :

$$\left\{ -\frac{n-1}{2}, -\frac{n-3}{2}, \dots, -1, 0, 1, \dots, \frac{n-3}{2}, \frac{n-1}{2} \right\},$$

ako je n neparan i

$$\left\{ -\frac{n-2}{2}, -\frac{n-4}{2}, \dots, -1, 0, 1, \dots, \frac{n-2}{2}, \frac{n}{2} \right\},$$

ako je n paran.

Teorem 2.2 Neka je $\{x_1, \dots, x_n\}$ potpuni sustav ostataka modulo n , te neka je $\gcd(a, n) = 1$. Tada je $\{ax_1, \dots, ax_n\}$ također potpuni sustav ostataka modulo n .

Dokaz:

Neka je $f(x)$ polinom s cjelobrojnim koeficijentima.

- Rješenje kongruencije $f(x) \equiv 0 \pmod{n}$ je svaki cijeli broj x koji je zadovoljava;
- Neka je x_1 neko rješenje kongruencije $f(x) \equiv 0 \pmod{n}$ i neka je $x_2 \equiv x_1 \pmod{n}$ tada je i x_2 rješenje te kongruencije (po Prop.2.3);
- Za dva rješenja kongruencije x_1 i x_2 kažemo da su ekvivalentna, ako je $x_1 \equiv x_2 \pmod{n}$;
- Broj rješenja kongruencije je broj neekvivalentnih rješenja.

Teorem 2.3 Neka su a i n prirodni brojevi te neka je b cijeli broj. Kongruencija $ax \equiv b \pmod{n}$ ima rješenje ako i samo ako $\gcd(a, n) = d$ dijeli b . Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo n .

Dokaz:

Iz Teorema 2.3 slijedi;

- ako je p prost i $p \nmid a$, onda kongruencija $ax \equiv b \pmod{p}$ ima točno jedno rješenje.

Ovo povlači da skup ostataka $\{0, 1, \dots, p-1\}$ pri dijeljenju s p uz zbrajanje i množenje \pmod{p} čini polje koje se obično označuje s \mathbb{Z}_p .

Pitanje: Kako riješiti kongruenciju

$$a'x \equiv b' \pmod{n'}, \text{ gdje je } \gcd(a', n') = 1 ?$$

Želimo rezultat oblika

$$x \equiv x_0 \pmod{n'}, \text{ gdje je } 0 \leq x_0 < n'.$$

Budući da je

$$\gcd(a', n') = 1,$$

postoje brojevi $u, v \in \mathbb{Z}$ takvi da je

$$a'u + n'v = 1,$$

(nađemo ih pomoću Euklidovog algoritma), pa je

$$a'u \equiv 1 \pmod{n'},$$

što povlači (množenjem s b')

$$x_1 \equiv ub' \pmod{n'}.$$

Primjer 2.1 Riješimo

$$555x \equiv 15 \pmod{5005}.$$

Zadatak 2.1 Riješite kongruencije

a) $589x \equiv 209 \pmod{817}$ i b) $49x \equiv 5000 \pmod{999}$

Teorem 2.4 (Kineski teorem o ostacima) Neka su m_1, m_2, \dots, m_r u parovima relativno prosti prirodni brojevi, te neka su a_1, a_2, \dots, a_r cijeli brojevi. Tada sustav kongruencija

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots, \quad x \equiv a_r \pmod{m_r} \quad (1)$$

ima rješenje. Ako je x_0 jedno rješenje, onda su sva rješenja od (1) dana sa $x \equiv x_0 \pmod{m_1 m_2 \cdot \dots \cdot m_r}$

Dokaz:

Primjer 2.2 Riješimo sustav kongruencija

$$x \equiv 2(\text{mod } 5), \quad x \equiv 3(\text{mod } 7), \quad x \equiv 4(\text{mod } 11).$$

Zadatak 2.2 Riješite sustav kongruencija

$$x \equiv 5(\text{mod } 7), \quad x \equiv 7(\text{mod } 11), \quad x \equiv 3(\text{mod } 13).$$

Primjer 2.3 Riješimo sustav kongruencija

$$x \equiv 3(\text{mod } 10), \quad x \equiv 8(\text{mod } 15), \quad x \equiv 5(\text{mod } 84).$$

Primjer 2.4 Nađite rješenje sustava kongruencija
(ako postoji)

$$x \equiv 3(\text{mod } 10), \quad x \equiv 2(\text{mod } 12), \quad x \equiv 8(\text{mod } 20).$$

Definicija 2.3 Reducirani sustav ostataka modulo n je skup brojeva r_i sa svojstvom da je

$$\gcd(r_i, n) = 1, \quad r_j \not\equiv r_i \pmod{n}$$

i da za svaki cijeli broj x takav da je $\gcd(x, n) = 1$, postoji r_i iz tog skupa takav da je $x \equiv r_i \pmod{n}$.

Jedan reducirani sustav ostataka modulo n je skup svih brojeva $a \in \{1, 2, \dots, n\}$ takvih da je $\gcd(a, n) = 1$.

Svi reducirani sustav ostataka modulo n imaju isti broj elemenata. Taj broj označujemo s $\varphi(n)$, a funkciju φ Eulerova funkcija. Dakle, $\varphi(n)$ je broj brojeva u nizu $1, 2, \dots, n$ a koji su relativno prosti sa n .

Teorem 2.5 Neka je $\{r_1, \dots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n , te neka je $\gcd(a, n) = 1$. Tada je $\{ar_1, \dots, ar_{\varphi(n)}\}$ također reducirani sustav ostataka modulo n .

Dokaz:

Primjer 2.5 Neka su a i n relativno prosti prirodni brojevi. Izračunajmo

$$\sum_{\substack{1 \leq x \leq n \\ \gcd(x,n)=1}} \left\{ \frac{ax}{n} \right\},$$

gdje je $\{z\} = z - \lfloor z \rfloor$ razlomljeni dio od z , dok x prolazi skupom reduciranih ostataka modulo n .

Teorem 2.6 (Eulerov teorem) Ako je $\gcd(a, n) = 1$, onda je $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dokaz:

Teorem 2.7 (Mali Fermatov teorem) Neka je p prost broj. Ako $p \nmid a$ onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.

Dokaz:

Primjer 2.6 Odredimo zadnje dvije znamenke u decimalnom zapisu broja 3^{400} .

Zadatak 2.3 Odredimo zadnje dvije znamenke u decimalnom zapisu broja 2^{1000} .

Definicija 2.4 Funkciju $\vartheta : \mathbb{N} \rightarrow \mathbb{C}$ za koju vrijedi:

i) $\vartheta(1) = 1$;

ii) $\vartheta(mn) = \vartheta(m)\vartheta(n)$ za sve m, n takve da je $\gcd(m, n) = 1$,

nazivamo multiplikativna funkcija.

Teorem 2.8 Eulerova funkcija φ je multiplikativna. Nadalje, za svaki prirodan broj $n > 1$ vrijedi

$$\varphi(n) = n \prod_{\substack{p|n \\ p\text{-prost}}} \left(1 - \frac{1}{p}\right).$$

Dokaz:

Zadatak 2.4 Za koje prirodne brojeve n je $\varphi(n)$ neparan?

Primjer 2.7 Odredimo sve prirodne brojeve n za koje vrijedi $\varphi(n) = 12$.

Teorem 2.9

$$\sum_{d|n} \varphi(d) = n.$$

Dokaz:

Teorem 2.10 (Wilson) Ako je p prost broj, onda je $(p - 1)! \equiv -1 \pmod{p}$.

Dokaz:

Primjer 2.8 Neka je p prost broj. Dokažimo da je $(p - 1)! + 1$ potencija od p ako i samo ako je $p = 2, 3$ ili 5 .

Teorem 2.11 Ako je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.

Dokaz:

Primjer 2.9 Dokažimo da postoji beskonačno mnogo prostih brojeva oblika $4k + 1$.

Teorem 2.12 (Lagrange) Neka je p prost broj i neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n . Pretpostavimo da vodeći koeficijent od f nije djeljiv s p . Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p .

Dokaz:

Primjer 2.10 (Wolstenholme). Neka je $p \geq 5$ prost broj. Dokažimo da je brojnik racionalnog broja

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}.$$

djeljiv s p^2 .

Dokaz:

Tvrđnja: Neka je p prost broj i neka $d \mid p-1$. Tada kongruencija

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

ima točno d rješenja (modulo p).

Dokaz:

- Imamo

$$x^{p-1} - 1 = (x^d - 1) g(x),$$

gdje je $g(x)$ polinom s cjelobrojnim koeficijentima stupnja $p-1-d$ s vodećim koeficijentom jednakim 1;

- Po Lagrangeovom teoremu i Malom Fermatovom teoremu, kongruencija

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

ima točno $p-1$ rješenje (modulo p).

- Neka je k broj rješenja kongruencije

$$g(x) \equiv 0 \pmod{p},$$

tada je po Lagrangeovom teoremu

$$k \leq p - 1 - d. \quad (1)$$

- Neka je n broj rješenja kongruencije

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

Kako je

$$x^{p-1} - 1 \equiv (x^d - 1) g(x) \pmod{p}, \quad (2)$$

tada po Lagrangeovom teoremu, te iz (1) i (2), imamo

$$\left. \begin{array}{l} n \stackrel{L.t.}{\leq} d \\ n \geq p - 1 - k \geq p - 1 - (p - 1 - d) = d \end{array} \right\} \implies n = d.$$

Teorem 2.13 (Henselova lema) Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \not\equiv 0 \pmod{p}$, onda postoji jedinstveni $t \in \{0, 1, \dots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Dokaz:

Propozicija 2.17 Kongruencija

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

ima tačno $p - 1$ rješenje za svaki prost broj p i prirodni broj j .

Dokaz:

Primjer 2.11 Riješimo kongruenciju

$$x^2 + x + 47 \equiv 0 \pmod{7^3}.$$

Zadatak 2.5 Riješite kongruenciju

$$x^3 + x^2 - 5 \equiv 0 \pmod{7^3}.$$

Definicija 2.5 Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodan broj d sa svojstvom da je

$$a^d \equiv 1 \pmod{n}$$

naziva se red od a modulo n . Još se kaže da a pripada eksponentu d modulo n .

Propozicija 2.18 Neka je d red od a modulo n . Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.

Dokaz:

Primjer 2.12 Dokažimo da svaki prosti djelitelj Fermatovog broja $2^{2^n} + 1$ za $n > 1$, ima oblik $p = k2^{n+1} + 1$.

Definicija 2.6 Ako je red a modulo n jednak $\varphi(n)$, onda se naziva primitivni korijen modulo n .

Teorem 2.14 Ako je p prost broj, onda postoji točno $\varphi(p - 1)$ primitivnih korijena modulo p .

Dokaz:

Teorem 2.15 Neka je p neparan prost broj, te neka je g primitivni korijen modulo p . Tada postoji $x \in \mathbb{Z}$ takav da je $g' = g + px$ primitivni korijen modulo p^j za sve $j \in \mathbb{N}$.

Dokaz:

Teorem 2.16 Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, gdje je p neparan prost broj.

Dokaz:

Primjer 2.13 Nađimo najmanji primitivni korijen

a) modulo 5; b) modulo 11; c) modulo 23.

Zadatak 2.6 Nađite najmanji primitivni korijen

a) modulo 13; b) modulo 17; c) modulo 41.

Napomena: Artinova slutnja: Neka je $\pi(N)$ broj prostih brojeva $\leq N$, a $v_2(N)$ broj prostih brojeva $q \leq N$ za koje je 2 primitivni korijen. Tada je

$$v_2(N) \sim A \cdot \pi(N),$$

gdje je $A = \prod_{p-\text{prost}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558$.

Definicija 2.6 Neka je g primitivni korijen modulo n . Tada brojevi $g^l, l = 0, 1, \dots, \varphi(n) - 1$ tvore reducirani sustav ostataka modulo n . Stoga za svaki cijeli broj a takav da je $\gcd(a, n) = 1$ postoji jedinstven l takav da je $g^l \equiv a \pmod{n}$. Eksponent l naziva se indeks od a u odnosu na g i označava se sa $\text{ind}_g a$ ili $\text{ind } a$.

Teorem 2.17

- 1.** $\text{ind } a + \text{ind } b \equiv \text{ind } (ab) \pmod{\varphi(n)}$;
- 2.** $\text{ind } 1 = 0, \text{ind } g = 1$;
- 3.** $\text{ind } (a^m) \equiv m \cdot \text{ind } (a) \pmod{\varphi(n)}$ za $m \in \mathbb{N}$;
- 4.** $\text{ind } (-1) = \frac{1}{2}\varphi(n)$ za $n \geq 3$.

Dokaz:

Propozicija 2.19 Neka je p prost broj. Ako je $\gcd(n, p - 1) = 1$, onda kongruencija $x^n \equiv a \pmod{p}$ ima jedinstveno rješenje.

Dokaz:

Primjer 2.14 Riješimo kongruenciju

$$x^5 \equiv 2 \pmod{7}.$$

Primjer 2.15 Riješimo kongruenciju

$$5x^4 \equiv 3 \pmod{11}.$$

Zadatak 2.7 Riješite kongruencije

a) $2x^8 \equiv 5 \pmod{13}$; **b)** $x^6 \equiv 5 \pmod{17}$;

c) $x^{12} \equiv 37 \pmod{41}$;

Primjer 2.16 Riješimo kongruenciju

$$3^x \equiv 2 \pmod{23}.$$

Zadatak 2.7 Riješite kongruenciju

$$7^x \equiv 6 \pmod{17}.$$

Primjer 2.17 Neka je $\alpha \geq 3$. Dokažimo da brojevi

$$\pm 5, \pm 5^2, \pm 5^3, \dots, \pm 5^{2^{\alpha-2}}$$

čine reducirani sustav ostataka modulo 2^α .