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 $a \equiv b (\mathrm{mod}\, n)$. U protivnom, kažemo da a nije kongruentno b modulo n i pišemo $a \not\equiv b (\mathrm{mod}\, n)$.

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 $a \equiv b(\mathrm{mod}\, n)$ i $c \equiv d(\mathrm{mod}\, n)$, onda je $a \pm c \equiv b \pm d(\mathrm{mod}\, n)$ i $ac \equiv bd(\mathrm{mod}\, n)$;

ii) Ako je $a \equiv b(\mathrm{mod}\, n)$, $d \in \mathbb{N}$ i $d \,|\, n$, onda je $a \equiv b(\mathrm{mod}\, d)$;

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

<u>Dokaz:</u>

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

i) $a \pm nk \equiv b \pm nl \;(\mathrm{mod}\, n)$;

ii) $ak \equiv bk(\mathrm{mod}\, n)$;

iii) $a^m \equiv b^m(\mathrm{mod}\, n)$ za svaki $m \in \mathbb{N}$.

<u>Dokaz:</u>

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

<u>Dokaz:</u>

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

<u>Dokaz:</u>

Napomena:

- Iz Propozicije 2.2, ii) slijedi: Neka su $m, n \in \mathbb{N}$, tada

$$a \equiv b (\bmod mn) \implies a \equiv b (\bmod m) \ \wedge \ a \equiv b (\bmod n) \ ).$$

  Obrat ove tvrdnje općenito ne vrijedi. Kontraprimjer: Imamo

$$32 \equiv 2 (\bmod 6) \ \text{ i } \ 32 \equiv 2 (\bmod 10),$$

  ali

$$32 \not\equiv 2 (\bmod 60).$$

- Vrijedi sljedeće: *Neka su $m, n \in \mathbb{N}$ i $\gcd(m, n) = g$, tada vrijedi*

$$a \equiv b (\bmod m) \ \wedge \ a \equiv b (\bmod n) \implies a \equiv b (\bmod \frac{mn}{g}) \ .$$

  Specijalno, ako je $\gcd(m, n) = 1$, tada vrijedi

$$a \equiv b (\bmod m) \ \wedge \ a \equiv b (\bmod n) \implies a \equiv b (\bmod mn) \ .$$

Dokaz: Neka je

$$c = \frac{mn}{g}, \quad p \text{ prost} \quad \text{i} \quad p^k \,\|c\,.$$

Tada $p^k \,\|m$ ili $p^k \,\|n$. Kako je $a \equiv b (\operatorname{mod} m)$ i $a \equiv b (\operatorname{mod} n)$, tj. $m \,|(a-b)$ i $n \,|(a-b)$, tada

$$p^k \,|(a-b)\,.$$

Budući ovo vrijedi za svaki prosti faktor p od c, onda

$$c \,|(a-b)\,, \text{ tj. } a \equiv b (\operatorname{mod} c).$$

što je i trebalo pokazati.

Uočimo: ako je

$$m = \prod_p p^{\alpha(p)} \text{ i } n = \prod_p p^{\beta(p)},$$

tada je

$$g = \gcd(a, b) = \prod_p p^{\min\{\alpha(p),\beta(p)\}}$$

i

$$c = \frac{mn}{g} = \frac{\left(\prod_p p^{\alpha(p)+\beta(p)}\right)}{\prod_p p^{\min\{\alpha(p),\beta(p)\}}} = \prod_p p^{\max\{\alpha(p),\beta(p)\}} = \operatorname{lcm}(m, n)$$

tj. $p^k \,\|c \implies k = \max\{\alpha(p), \beta(p)\}$, tj. $p^k \,\|m$ ili $p^k \,\|n$ ■.

Definicija 2.2 Skup $S = \{x_1, ..., x_n\}$ se naziva *potpuni sustav ostataka modulo* n ako za svaki $y \in \mathbb{Z}$ postoji točno jedan $x_j \in S$ takav da je $y \equiv x_j (\bmod\, n)$. 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 :

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

- Sustav apsolutno najmanjih ostataka modulo n :

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

  ako je n neparan i

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

  ako je n paran.

Teorem 2.2 Neka je $\{x_1, ...x_n\}$ potpuni sustav ostataka modulo n, te neka je $\gcd(a, n) = 1$. Tada je $\{ax_1, ..., ax_n\}$ 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 i x' kažemo da su *ekvivalentna*, ako je $x \equiv x' \pmod{n}$;
- *Broj rješenja* kongruencije je broj neekvivalentnih rješenja.

Teorem 2.3 Neka su a i n prirodni brojevi te neka je b cijeli broj. Kongruencija $ax \equiv b(\mathrm{mod}\, n)$ 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 $ax \equiv b(\mathrm{mod}\, p)$ ima točno jedno rješenje. Ovo povlači da skup ostataka $\{0, 1, ..., p-1\}$ pri dijeljenju s p uz zbrajanje i množenje $(\mathrm{mod}\ p)$ čini polje koje se obično označuje s $\mathbb{Z}_p$.

Pitanje: Kako riješiti kongruenciju

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

Želimo rezultat oblika

$$x \equiv x_1(\mathrm{mod}\, n'), \text{ gdje je } \quad 0 \leq x_1 < n'.$$

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

$$a'u \equiv 1 (\operatorname{mod} n'),$$

što povlači (množenjem s b')

$$x_1 \equiv ub' (\operatorname{mod} n').$$

Primjer 2.1 Riješimo

$$555x \equiv 15 (\operatorname{mod} 5005).$$

Zadatak 2.1 Riješite kongruencije

a) $589x \equiv 209\,(\operatorname{mod} 817)$ i b) $49x \equiv 5000\,(\operatorname{mod} 999)$

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

$$x \equiv a_1 (\operatorname{mod} m_1), \quad x \equiv a_2 (\operatorname{mod} m_2), ..., x \equiv a_r (\operatorname{mod} m_r) \tag{1}$$

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

Dokaz:

Primjer 2.2 Riješimo sustav kongruencija

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Zadatak 2.2 Riješite sustav kongruencija

$$x \equiv 5 \pmod{7}, \quad x \equiv 7 \pmod{11}, \quad x \equiv 3 \pmod{13}.$$

Primjer 2.3 Riješimo sustav kongruencija

$$x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}, \quad x \equiv 5 \pmod{84}.$$

Primjer 2.4 Nađite rješenje sustava kongruencija (ako postoji)

$$x \equiv 3 \pmod{10}, \quad x \equiv 2 \pmod{12}, \quad x \equiv 8 \pmod{20}.$$

Definicija 2.3 _Reducirani sustav ostataka modulo n_ je skup brojeva r_i sa svojstvom da je

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

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

Jedan reducirani sustav ostataka modulo n je skup svih brojeva $a \in \{1, 2, ..., n\}$ 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 $1, 2, ...n$ a koji su relativno prosti sa n.

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

Dokaz:

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

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

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 $a^{\varphi(n)} \equiv 1 (\bmod n)$

Dokaz:

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

Dokaz:

Definicija 2.4 Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ 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, zvaki prirodan broj $n > 1$ vrijedi

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

<u>Dokaz:</u>

Napomena: Iz dokaza Teorema 2.8 imamo:

$$\text{Ako je } n = \prod_{i=1}^{k} p_i^{\alpha_i} \implies \varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i - 1).$$

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}.

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

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

<u>Dokaz:</u>

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

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

djeljiv s p^2.

Dokaz:

Tvrdnja: Neka je p prost broj i neka $d \,|\, p-1$. Tada kongruencija

$$x^d - 1 \equiv 0 (\operatorname{mod} p)$$

ima točno d rješenja (modulo p).

Dokaz:

- Imamo

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

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

- Po Lagrangeovom teoremu i Malom Fermatovom teoremu, kongruencija

  $$x^{p-1} - 1 \equiv 0 (\operatorname{mod} p)$$

  ima točno $p-1$ rješenje (modulo p).

- Neka je k broj rješenja kongruencije

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

tada je po Lagrangeovom teoremu

$$k \leq p - 1 - d. \tag{1}$$

- Neka je n broj rješenja kongruencije

$$x^d - 1 \equiv 0 (\mathrm{mod}\, p).$$

Kako je

$$x^{p-1} - 1 \equiv \left(x^d - 1\right) g(x) (\mathrm{mod}\, p), \tag{2}$$

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

$$\left.\begin{array}{c} n \overset{L.t.}{\leq} d \\ n \geq p - 1 - k \geq p - 1 - (p - 1 - d) = d \end{array}\right\} \Longrightarrow n = d.$$

Teorem 2.13 (Henselova lema) Neka je $f(x)$ polinom s cjelobrojnim koeficijentima. Ako je $f(a) \equiv 0 (\mathrm{mod}\, p^j)$ i $f'(a) \not\equiv 0 (\mathrm{mod}\, p)$, onda postoji jedinstveni $t \in \{0, 1, 2, ..., p-1\}$ takav da je $f\left(a + tp^j\right) \equiv 0 (\mathrm{mod}\, p^{j+1})$.

<u>Dokaz:</u>

Propozicija 2.17 Kongruencija

$$x^{p-1} - 1 \equiv 0 (\operatorname{mod} p^j)$$

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

Dokaz:

Primjer 2.11 Riješimo kongruenciju

$$x^2 + x + 47 \equiv 0 (\operatorname{mod} 7^3).$$

Zadatak 2.5 Riješite kongruenciju

$$x^3 + x^2 - 5 \equiv 0 (\operatorname{mod} 7^3).$$

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

$$a^d \equiv 1 (\mathrm{mod}\, n)$$

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 $a^k \equiv 1 (\mathrm{mod}\, n)$ ako i samo ako $d \,|\, k$. Posebno, $d \,|\, \varphi(n)$.

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 ***primitvni korijen*** modulo n.

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

Dokaz:

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

Dokaz:

Teorem 2.16 Za prirodan broj n postoji primitvni korijen modulo n ako isamo 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 $A = \prod\limits_{p-prost} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558.$

Definicija 2.6 Neka je g primitvni korijen modulo n. Tada brojevi g^l, $l = 0, 1, ..., \varphi(n) - 1$ 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 $ind_g a$ ili $ind\, a$.

Teorem 2.17

1. $ind\, a + ind\, a \equiv ind\ (ab) \pmod{\varphi(n)}$;

2. $ind\, 1 = 0$, $ind\, g = 1$;

3. $ind\ (a^m) \equiv m \cdot ind\ (a) \pmod{\varphi(n)}$ za $m \in \mathbb{N}$;

4. $ind\ (-1) = \frac{1}{2}\varphi(n)$ 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.

<u>Dokaz:</u>

Primjer 2.14 Riješimo kongruenciju

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

Primjer 2.15 Riješimo kongruenciju

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

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

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

čine reducirani sustav ostataka modulo 2^α.