Uvod u teoriju brojeva

2. Kongruencije

Borka Jadrijević

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

$$n \mid (a-b) \quad \Longleftrightarrow \quad -n \mid (a-b),$$

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 $\mathbb{Z}$.

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:

Korolar (2.1)

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

<u>*Dokaz:*</u>

Teorem (2.1)

Neka su $a, b, c \in \mathbb{Z}$ *tada vrijedi:* $ca \equiv cb \pmod{n}$ *ako i samo ako*

$$a \equiv b \left(\mathrm{mod}\ \frac{n}{\gcd(c, n)}\right).$$

Specijalno, ako je $ca \equiv cb \pmod{n}$ *i* $\gcd(c, n) = 1$, *onda je* $a \equiv b \pmod{n}$.

<u>*Dokaz:*</u>

Napomena

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

$$a \equiv b (\mathrm{mod}\, mn) \implies \left(a \equiv b (\mathrm{mod}\, m) \quad \wedge \quad a \equiv b (\mathrm{mod}\, n) \right).$$

Obrat ove tvrdnje općenito ne vrijedi. <u>Kontraprimjer:</u> Imamo

$$32 \equiv 2 (\mathrm{mod}\, 6) \;\; i \;\; 32 \equiv 2 (\mathrm{mod}\, 10),$$

ali

$$32 \not\equiv 2 (\mathrm{mod}\, 60).$$

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

$$\left(a \equiv b (\mathrm{mod}\, m) \quad \wedge \quad a \equiv b (\mathrm{mod}\, n) \right) \implies a \equiv b (\mathrm{mod}\, \frac{mn}{g}) \; .$$

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

$$\left(a \equiv b (\mathrm{mod}\, m) \quad \wedge \quad a \equiv b (\mathrm{mod}\, n) \right) \implies a \equiv b (\mathrm{mod}\, mn) \; .$$

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 $a \equiv b \pmod m$ i $a \equiv b \pmod n$, tj. $m \,|\, (a-b)$ i $n \,|\, (a-b)$, tada

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

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

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

što je i trebalo pokazati. ■

Uočimo: Ako je

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

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 $S = \{x_1, \ldots, x_n\}$ *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 :
$$\{0, 1, \ldots, n-1\}.$$
- Sustav apsolutno najmanjih ostataka modulo n :
$$\left\{-\frac{n-1}{2}, -\frac{n-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-3}{2}, \ \frac{n-1}{2}\right\},$$
ako je n neparan i
$$\left\{-\frac{n-2}{2}, -\frac{n-4}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-2}{2}, \ \frac{n}{2}\right\},$$
ako je n paran.

Teorem (2.2)

Neka je $\{x_1, \ldots x_n\}$ *potpuni sustav ostataka modulo* n*, te neka je* $\gcd(a, n) = 1$*. Tada je* $\{ax_1, \ldots, ax_n\}$ *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 $ax \equiv b \pmod{n}$ 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 $\{0, 1, ..., p-1\}$ pri dijeljenju s p uz zbrajanje i množenje $(\mathrm{mod}\ p)$ čini polje koje se obično označuje s $\mathbb{Z}_p$ jer kongruencija $ax \equiv 1 \pmod{p}$, $a \in \{1, ..., p-1\}$ ima (točno jedno) rješenje.
- Općenito, $\mathbb{Z}_m$ je komutativni prsten s jedinicom jer $ax \equiv 1 \pmod{m}$, $a \in \{1, ..., m-1\}$ ima rješenje ako i samo ako je $\gcd(a, m) = 1$. U tom slučaju a je invertibilan u prstenu $\mathbb{Z}_m$ i a^{-1} je (jedinstveno) rješenje te kongruencije.

Pitanje: Kako riješiti kongruenciju

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

Želimo rezultat oblika

$$x \equiv x_1 \pmod{n'}, \text{ gdje je } \quad 0 \leq x_1 < n'.$$

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

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

što povlači (množenjem s b')

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

Primjer (2.1)

Riješimo

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

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*

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

ima rješenje. Ako je x_0 *jedno rješenje, onda su sva rješenja od* (1) *dana sa*

$$x \equiv x_0 \pmod{m_1 m_2 \cdot ... \cdot m_r}.$$

Dokaz:

Primjer (2.2)

Riješimo sustav kongruencija

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

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

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

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 $a \in \{1, 2, ..., n\}$ *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* $\varphi : \mathbb{N} \to \mathbb{N}$ *nazivamo Eulerova funkcija. Dakle,* $\varphi(n)$ *je broj brojeva u nizu* $1, 2, ..., n$ *a koji su relativno prosti s n.*

Teorem (2.5)

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

Dokaz:

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:

Napomena

Lako je vidjeti da obrat Malog Fermatovog teorem općenito ne vrijedi. Primjerice, broj $341 = 11 \cdot 31$ *je složen i vrijedi*

$$2^{340} \equiv 1 (\bmod 341), \ \textit{tj.} \quad 2^{341} \equiv 2 \, (\bmod 341) \, .$$

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

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

Dokaz:

Napomena

Iz dokaza Teorema 2.8 imamo:

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

Primjer (2.5)

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

Primjer (2.6)

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

Teorem (2.9)

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

Dokaz:

Teorem (2.10)(Wilsonov teorem)

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

Dokaz:

Napomena

Vrijedi i jači oblik Wilsonovog teorema:

Teorem (Wilsonov teorem) *Neka je p prirodan broj veći od 1. Tada je p prost ako i samo ako $(p-1)! \equiv -1 \pmod{p}$.*

Teorem (2.11)(Lagrangeov teorem)

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 (2.7)

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: Kako $d \mid p-1$, imamo

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

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

- Po Lagrangeovom i Malom Fermatovom teoremu, kongruencija
$$x^{p-1} - 1 \equiv 0 (\mathrm{mod}\, p)$$
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
$$\left.\begin{array}{c} n \overset{L.t.}{\leq} d \\ n \overset{(2)}{\geq} p - 1 - k \overset{(1)}{\geq} p - 1 - (p - 1 - d) = d \end{array}\right\} \Longrightarrow n = d.$$

Teorem (2.12. 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* $t \in \{0, 1, 2, ..., p-1\}$ *takav da je* $f\left(a + tp^j\right) \equiv 0 \pmod{p^{j+1}}$.

Dokaz:

Primjer (2.8)

Riješimo kongruenciju

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

Definicija (2.5)

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

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

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

Propozicija (2.4)

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:

Definicija (2.6)

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

Teorem (2.13)

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

Dokaz:

Primjer (2.9)

Nađimo najmanji primitivni korijen

a) *modulo* 5; **b)** *modulo* 23.

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

Teorem (2.14)

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 $j \in \mathbb{N}$.

Teorem (2.15)

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

Definicija (2.7)

Neka je g primitvni korijen modulo n. Tada brojevi

$$g^l, \quad l = 0, 1, ..., \varphi(n) - 1$$

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 (2.16)

1. $ind\ a + ind\ b \equiv ind\ (ab) \pmod{\varphi(n)}$;
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 (2.5)

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 (2.10)

Riješimo kongruenciju

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