Uvod u teoriju brojeva
3. Kvadratni ostatci

Borka Jadrijević

3. Kvadratni ostaci

Definicija (3.1)

Neka je $\gcd(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

Primjer (3.1)

Kvadratni ostaci modulo 5 *su* 1 *i* 4, *a neostaci* 2 *i* 3.

Teorem (3.1)

Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ *kvadratnih ostaka i* $\frac{p-1}{2}$ *kvadratnih neostaka.*

Dokaz:

Zadatak (3.1)

Odredite sve kvadratne ostatke:

a) *modulo* 7; **b)** *modulo* 17;

Definicija (3.2)

Neka je p neparan prost broj. *Legenderov simbol* $\left(\frac{a}{p}\right)$ *je jednak* 1 *ako je a kvadratni ostatak modulo p,* -1 *ako je a kvadratni neostatak modulo p, a* 0 *ako* $p \mid a$.

Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{p}$ *je jednak* $1 + \left(\frac{a}{p}\right)$.

Teorem (3.2) (Eulerov kriterij)

Neka je p neparan prost broj. Tada je

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

Dokaz:

Propozicija (3.1)

1. *Ako je* $a \equiv b \pmod{p}$, *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* $\gcd(a, p) = 1$, *onda je* $\left(\frac{a^2}{p}\right) = 1$;
4. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

   Dokaz:

Teorem (3.3) (Gaussova lema)

Neka je p neparan prost broj i $\gcd(a,p)=1$. *Promotrimo brojeve* a, $2a$, $3a$, ..., $\frac{p-1}{2}\cdot a$, *te njihove najmanje nenegativne ostatke pri dijeljenju s* p. *Označimo s* n *broj ostataka koji su veći od* $\frac{p}{2}$. *Tada je* $\left(\frac{a}{p}\right)=(-1)^n$.

Dokaz:

Teorem (3.4)

Ako je p neparan prost broj i $\gcd(a,2p)=1$, *onda je*

$$\left(\frac{a}{p}\right)=(-1)^t,$$

gdje je $t=\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor$. *Također vrijedi:*

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

tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k\pm1$.

Dokaz:

Teorem (3.5) (Gaussov kvadratni zakon reciprociteta)

Ako su p i q različiti neparani prosti brojevi, onda vrijedi

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

Drugim riječima, ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenje, a druga nema. Ako je barem jedan od brojeva p i q oblika $4k+1$, onda obje kongruencije ili imaju rješenje ili obje nemaju rješenje.

Dokaz:

Primjer (3.2)

Izračunajmo

$$\left(\frac{-42}{61}\right).$$

Primjer (3.3)

Odredimo sve proste brojeve p takve da je -2 kvadratni ostatak modulo p.

Definicija (3.3)

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdot \ldots \cdot q_s$, gdje su $q_1, \ldots, q_s$ neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right).$$

gdje je $\left(\frac{a}{q_j}\right)$ Legenderov simbol.

Napomena

- *Ako je Q prost broj, onda se Legenderov i Jacobijev simbol podudaraju;*
- *Ako je* $\gcd(a, Q) > 1$, *onda je* $\left(\frac{a}{Q}\right) = 0$, *inače* $\left(\frac{a}{Q}\right) \in \{1, -1\}$;
- *Ako je a kvadratni ostatak modulo Q, onda je a kvadratni ostatak modulo q_j, za svaki $j = 1, ..., s$.*

  Ovo povlači: Ako je a kvadratni ostatak modulo Q, onda je $\left(\frac{a}{Q}\right) = 1$;
- $\left(\frac{a}{Q}\right) = 1$ *ne povlači da je a kvadratni ostatak modulo Q.*

  Primjer: Imamo

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

ali kongruencija

$$x^2 \equiv 2 \pmod{15}$$

nema rješenja;

- Da bi a bio kvadratni ostatak modulo Q nužno je i dovoljno da je $\left(\frac{a}{q_j}\right) = 1$ za svaki $j = 1, ..., s$.

Propozicija (3.2)

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi:

1. $\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \left(\frac{a}{QQ'}\right)$;
2. $\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \left(\frac{aa'}{Q}\right)$;
3. *Ako je* $\gcd(a, Q) = 1$, *onda je* $\left(\frac{a^2}{Q}\right) = \left(\frac{a}{Q^2}\right) = 1$;
4. *Ako je* $a \equiv a' \pmod{Q}$, *onda je* $\left(\frac{a}{Q}\right) = \left(\frac{a'}{Q}\right)$

Dokaz:

Propozicija (3.3)

Ako je Q neparan prirodan broj, onda je:

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

Dokaz:

Propozicija (3.4)

Ako su P i Q neparani prirodni brojevi takvi da je $(P, Q) = 1$, onda je:

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

Dokaz:

Primjer (3.4)

Izračunajmo

$$\left(\frac{105}{317}\right).$$