1 Kvadratna kongruencija

Definicija 1.1. Neka su $a, m \in \mathbb{Z}$, i $(a, m) = 1$. Kažemo da je a *kvadratni ostatak* modulo m ako kongruencija $x^2 \equiv a \pmod{m}$ ima rešenja.

Mi ćemo posmatrati slučaj kada je m prost broj. Pri proveravanju da li je neki broj kvadratni ostatak ili ne, od koristi će nam biti sledeći pojam:

Definicija 1.2. Ležandrov simbol $\left(\frac{a}{p}\right)$ je funkcija od brojeva a i p, koja je 1 ako je a kvadratni ostatak modulo p, 0 ako je a deljivo sa p i -1 ako a nije kvadratni ostatak modulo p. Drugim rečima:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ je kvadratni ostatak modulo } p, \\ 0, & a \text{ je deljivo sa } p, \\ -1 & a \text{ nije kvadratni ostatak modulo } p. \end{cases}$$

Ovaj simbol ima sledeća svojstva:

Tvrđenje 1.3. *Za proste brojeve $p > 2$ i $q > 2$, $p \neq q$, i cele brojeve a i b važi:*

1. $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

2. *Ako je $a \equiv b \pmod{p}$, tada je*
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

3. $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \ \left(\frac{1}{p}\right) = 1, \ \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\left[\frac{p+1}{4}\right]}.$$

4. *(Gausov zakon reciprociteta)*
Ako su p i q različiti prosti, tada je
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

5. *U skupu $\{1, 2, \ldots, p-1\}$ ima $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.*

Primer 1.4. *Primetimo da je* $3^2 = 9 \equiv 2 \pmod 7$*, pa je* $\left(\frac{2}{7}\right) = 1$*. Sa druge strane, imamo da je* $1^2 = 1$*,* $2^2 = 4$*,* $3^2 \equiv 2$*,* $4^2 \equiv 2$*,* $5^2 \equiv 4$*,* $6^2 \equiv 1 \pmod 7$*, pa pošto se među kvadratima ne javlje ništa sto je kongruentno sa* 3 *modulo* 7*, to je* $\left(\frac{3}{7}\right) = -1$*.*

1. **a)** Da li $x^2 \equiv 2013 \pmod{2311}$ ima rešenja?

Primetimo da je $2013 = 3 \cdot 11 \cdot 61$, pa po prvom svojstvu imamo da je $\left(\frac{2013}{2311}\right) = \left(\frac{3}{2311}\right)\left(\frac{11}{2311}\right)\left(\frac{61}{2311}\right)$.

Po Gausovom zakonu reciprociteta, $\left(\frac{3}{2311}\right)\left(\frac{2311}{3}\right) = (-1)^{\frac{3-1}{2}\frac{2311-1}{2}} = (-1)^{1155} = -1$. Dakle, $\left(\frac{3}{2311}\right) = -\left(\frac{2311}{3}\right)$, a $\left(\frac{2311}{3}\right)$ je po drugom svojstvu (pošto je $2311 \equiv 1 \pmod 3$) jednako 1. Prema tome, $\left(\frac{3}{2311}\right) = -1$.

Po Gausovom zakonu reciprociteta, $\left(\frac{11}{2311}\right)\left(\frac{2311}{11}\right) = (-1)^{\frac{11-1}{2}\frac{2311-1}{2}} = -1$. Dakle, $\left(\frac{11}{2311}\right) = -\left(\frac{2311}{11}\right)$, a $2311 \equiv 1 \pmod{11}$, pa je $\left(\frac{2311}{11}\right) = 1$, odakle je $\left(\frac{11}{2311}\right) = -1$.

Po Gausovom zakonu reciprociteta, $\left(\frac{61}{2311}\right)\left(\frac{2311}{61}\right) = (-1)^{\frac{61-1}{2}\frac{2311-1}{2}} = 1$, pa je $\left(\frac{61}{2311}\right) = \left(\frac{2311}{61}\right)$, a pošto je $2311 \equiv 54 = 2 \cdot 3^3 \pmod{61}$, to je $\left(\frac{2311}{61}\right) = \left(\frac{54}{61}\right) = \left(\frac{2}{61}\right)\left(\frac{3}{61}\right)^3 = \left(\frac{2}{61}\right)\left(\frac{3}{61}\right)$ (ako p ne deli a, tada je $\left(\frac{a}{p}\right)^2 = 1$). Kako je $\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1$, i $\left(\frac{3}{61}\right)\left(\frac{61}{3}\right) = (-1)^{\frac{3-1}{2}\frac{61-1}{2}} = 1$, to je $\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) = \left(\frac{1}{3}\right) = 1$, pa je $\left(\frac{61}{2311}\right) = -1$.

Na kraju, imamo da je $\left(\frac{2013}{2311}\right) = (-1) \cdot (-1) \cdot (-1) = -11$. Dakle, kongruencija $x^2 \equiv 2013 \pmod{2311}$ nema rešenja.

1. **b)** Izračunati $\left(\frac{34}{79}\right)$.

Imamo da je $34 = 2 \cdot 17$, pa je $\left(\frac{34}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{17}{79}\right) = (-1)^{\frac{79^2-1}{8}}\left(\frac{17}{79}\right) = (-1)^{\frac{78 \cdot 80}{8}}\left(\frac{17}{79}\right) = \left(\frac{17}{79}\right)$. Kada primenimo Gausov zakon reciprociteta, dobijamo $\left(\frac{17}{79}\right)\left(\frac{79}{17}\right) = (-1)^{\frac{79-1}{2}\frac{17-1}{2}} = 1$, pa je $\left(\frac{17}{79}\right) = \left(\frac{79}{17}\right) = \left(\frac{11}{17}\right)$. Kada opet primenimo Gausov zakon, dobijamo $\left(\frac{11}{17}\right)\left(\frac{17}{11}\right) = (-1)^{\frac{11-1}{2}\frac{17-1}{2}} = 1$, pa je $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)^{\frac{10 \cdot 12}{8}}\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right)$. Na kraju, $\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = (-1)^{\frac{3-1}{2}\frac{11-1}{2}} = -1$, pa je $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$, jer 2 nije kvadrat modulo 3. Dakle, $\left(\frac{34}{79}\right) = -1$.

1. **c)** Izračunati $\left(\frac{442}{139}\right)$.

Pošto je $442 \equiv 25 \pmod{139}$, to je $\left(\frac{442}{139}\right) = \left(\frac{25}{139}\right) = \left(\frac{5}{139}\right)^2 = 1$ (Pošto 5 nije deljivo sa 139, to je $\left(\frac{5}{139}\right)$ jednako 1 ili -1. U svakom slučaju, kvadrat tog broja će biti jednak 1).

2. Da li sledeće kongruencije imaju rešenje?

1. $x^2 \equiv 68 \pmod{113}$,
2. $x^2 \equiv 310 \pmod{521}$,
3. $x^2 + 174 \equiv 0 \pmod{619}$.

Važi sledeće tvrđenje:

Tvrđenje 1.5. *Ako su a, b, c celi brojevi, i p prost broj koji ne deli a. Tada kongruencija $ax^2 + bx + c \equiv 0 \pmod{p}$ ima rešenja ako i samo ako kongruencija $x^2 \equiv D = b^2 - 4ac \pmod{p}$ ima rešenja.*

3. a) Ima li $2x^2 + 5x + 8 \equiv 0 \pmod{37}$ rešenja?

U ovom slučaju, diskriminanta je $D = 5^2 - 4 \cdot 2 \cdot 8 = -39$, i posmatramo kongruenciju $x^2 \equiv -39 \equiv 35 \pmod{37}$, tj. simbol $\left(\frac{35}{37}\right)$. Odavde je $\left(\frac{35}{37}\right) = \left(\frac{5}{37}\right)\left(\frac{7}{37}\right)$.

Po Gausu, $\left(\frac{5}{37}\right)\left(\frac{37}{5}\right) = (-1)^{\frac{5-1}{2}\frac{37-1}{2}} = 1$, pa je $\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right)$. Jedini kvadrati modulo 5 su 1 i 4, pa je $\left(\frac{5}{37}\right) = -1$.

Slično, $\left(\frac{7}{37}\right)\left(\frac{37}{7}\right) = 1$, pa je $\left(\frac{7}{37}\right) = \left(\frac{37}{7}\right) = \left(\frac{2}{7}\right) = 1$. (Da je $\left(\frac{2}{7}\right) = 1$ smo videli u primeru). Prema tome, $\left(\frac{7}{37}\right) = 1$

Dakle, $\left(\frac{35}{37}\right) = (-1) \cdot 1 = -1$, pa kongruencija $2x^2 + 5x + 8 \equiv 0 \pmod{37}$ nema rešenja.

2. b) Ima li $9x^2 + 11x - 2 \equiv 0 \pmod{41}$ rešenja?

3. Neka su x i y uzajamno prosti prirodni brojevi. Dokazati da je svaki prost delilac p od $x^2 + y^2$ ili jednak 2, ili mora biti oblika $p = 4k + 1$, za neki prirodan broj k.

Ako p deli $x^2 + y^2$, to možemo zapisati i kao $x^2 \equiv -y^2 \pmod{p}$. Recimo da je $p \neq 2$. Tada, pošto važi ova kongruencija, imamo da je

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

zbog čega p mora biti oblika $p = 4k + 1$.

4. Neka su a i b celi brojevi, i p prost broj koji ne deli a. Dokazati da je

$$\sum_{k=0}^{p-1}\left(\frac{ak+b}{p}\right) = 0.$$

5. Neka je $p = 4k + 1$ prost broj, i $p' = \frac{p-1}{2}$. Dokazati da je $x = p'!$ jedno rešenje za $x^2 + 1 \equiv 0 \pmod{p}$

Za svaki ceo broj i važi $i \equiv -(p - i) \pmod{p}$, pa imamo da je $p'! = (-1)^{p'}(p' + 1)(p' + 2)\ldots(p - 2)(p - 1)$. Tada, pošto je p' parno, imamo po Vilsonovoj teoremi da je $x^2 = (p'!)^2 = (-1)^{p'}(p - 1)! \equiv (-1)^{p'+1} = -1 \pmod{p}$.