S2	Seniorska grupa

Predavanja subotom
Osijek, sezona 2022./23.

Kvadratni ostaci

Jakov Cigrovski

29.10.2022.

Mladi nadareni matematičari
"Marin Getaldić"

1. Uvod

Važna je činjenica da, za dani prirodan broj m, kvadrati cijelih brojeva ne daju sve moguće ostatke pri dijeljenju s m.

Na primjer, za $m = 10$ kvadrati završavaju znamenkama $0, 1, 4, 5, 6, 9$, dok se znamenke $2, 3, 7, 8$ ne pojavljuju.

U ovom predavanju ćemo pokazati kako odrediti je li broj kvadratni ostatak.

Definicija 1.1: Kvadratni ostatak

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

Definicija 1.2: Legendreov simbol

Za cijeli broj a i neparan prost broj p, Legendreov simbol $\left(\frac{a}{p}\right)$ definiramo na sljedeći način:

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

Teorem 1.3: Svojstva Legendreovog simbola

(a, b su proizvoljni cijeli brojevi, a p proizvoljan neparan prost broj):

- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- $\left(\frac{a+bp}{p}\right) = \left(\frac{a}{p}\right)$
- (Eulerov kriterij) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Teorem 1.4: Gaussov zakon reciprociteta

Neka su p i q različiti neparni prosti brojevi. Tada vrijedi Gaussov zakon reciprociteta:

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

I njegov suplement

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ako je } p \text{ oblika } 8k \pm 1 \\ -1, & \text{inače.} \end{cases}$$

Zadaci

1. Ako je p prost broj pokažite da je $x^2 \equiv 1 \pmod{p}$ ako i samo ako je $x \equiv \pm 1 \pmod{p}$.

2. Dokaži da neparni potpuni kvadrati uvijek daju ostatak 1 pri dijeljenju s 8.

3. Izračuajte:

a) $\left(\frac{-1}{37}\right)$

b) $\left(\frac{18}{23}\right)$

c) $\left(\frac{-3}{29}\right)$

d) $\left(\frac{814}{2003}\right)$.

4. Odredite sve prirodne brojeve n za koje je broj $N_n = 1! + 2! + \ldots n!$ kvadrat.

5. Neka su $a, b \in \mathbb{N}$ pokažite da ako $7 \mid a^2 + b^2$ onda $7 \mid a$ i $7 \mid b$.

6. Postoji li prirodan broj x takav da je $x^2 - 31x + 34$ djeljiv s 37?

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

8. Prosti brojevi p i q zovu se prosti brojevi blizanci ako je $q = p + 2$. Dokažite da postoji $a \in \mathbb{Z}$ takav da $p \mid (a^2 - q)$ ako i samo ako postoji $b \in \mathbb{Z}$ takav da $q \mid (b^2 - p)$.

9. Pokažite da $2^n + 1$ nema prost faktor oblika $8k + 7$:

a) kada je n paran.

b) kada je n neparan.

10. Neka je p neparan prost broj, skup $\{1, 2, \ldots, p-1\}$ sadrži jednako kvadratnih ostatak i neostataka.

11. Neka je p prost broj oblika $4k + 1$ dokažite da postoji točno k parnih kvadratnih ostataka.

Teži zadaci

12. Neka je $p > 5$ prost broj. Pokažite da postoje dva prirodna uzastopna broja koja su oba kvadratni ostaci modulo p.

13. Neka je p neparni prost broj, te q najmanji pozitivni kvadratni neostatak modulo p.

a) Dokažite da je q prost broj.

b) * Dokažite da vrijedi $q < \sqrt{p} + 1$.

Hintovi

1. Prebacite 1 na lijevu stranu.

2. Ispišite sve kvadrate svih ostataka.

3. a) Eulerov kriterij

b) 1. svojstvo iz 1.3

c) Kombinacija prva 2 plus Gaussov zakon

d) isto kao pod c)

4. Promatrajmo modulo 5.

5. Koji su sve kvadratni ostaci modulo 7 i kakav može biti zbroj.

6. Namjestimo da izraz oblika $(x+a)^2+b$ pa moramo provjeriti je li $-b$ kvadratni ostatak.

7. Opet primjena svojstava u 1.3.

8. Primjetimo da postoji $a \in \mathbb{Z}$ takav da je $p \mid (a^2 - q)$ ako i samo ako je q kvadratni ostatak modulo p, slično i za $b +$ još Gauss.

9. kada je n paran je pitanje je li -1 kvadrati ostatak, a kada je paran odumemo p i podijelimo sve s 2.

10. primjetimo da su x i $-x$ različiti ostaci modulo p no njihov kvadrat je isti pa moramo pokazati da su $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ različiti ostaci.

11. Pokažite da ima jednako parnih i neparnih uspostavljanjem bijekcije ("uparivanjem")

12. Kvadrati su uvijek kvadratni ostaci pa pokažimo da abrem neki kvadrat od 1, 4, 9 ima "susjeda" koji je kvadratni ostatak također.

13. a) Pretpostavite da nije.

b) Uzmimo k takav da je kq najmanji višekratnik od q za koji je $kq > p$.

Rješenja

1. Jednakost $x^2 \equiv 1 \pmod{p}$ je ekvivalentna s $(x-1)(x+1) \equiv 0 \pmod{p}$, pa zaključujemo da p dijeli $x-1$ ili $x+1$ te je $x \equiv \pm 1 \pmod{p}$.

2. Neparni brojevi mogu davati ostatke $1, 3, 5, 7$ pri dijeljenju s 8. Njihovi su kvadrati redom $1, 9, 25, 49$ i svi oni daju ostatak 1 pri dijeljenju s 8.
Alternativno, možemo dokazati da ako je a neparan, tada je $a^2 - 1$ djeljiv s 8. Primijetimo da su $a-1$ i $a+1$ 2 uzastopna parna broja, dakle barem 1 od njih je djeljiv s 4, a time je njihov umnožak djeljiv s 8.

3. a)

$$\left(\frac{-1}{37}\right) = (-1)^{\frac{37-1}{2}} = (-1)^{18} = 1$$

b)

$$\left(\frac{18}{23}\right) = \left(\frac{9}{23}\right)\left(\frac{2}{23}\right) = \left(\frac{2}{23}\right) = -1$$

c)

$$\left(\frac{-3}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{3}{31}\right) = -\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right) = 1$$

d)

$$\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right)\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right) = \left(\frac{2003}{11}\right)\left(\frac{2003}{37}\right) = \left(\frac{1}{11}\right)\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = -1$$

4. Očito su brojevi $N_1 = 1$ i $N_3 = 9$ kvadrati, dok $N_2 = 3$ nije kvadrat. Za $n \geq 4$ vrijedi $N_n \equiv 1! + 2! + 3! + 4! \equiv 33 \equiv 35$, pa N_n ne može biti kvadrat (jer 3 nije kvadratni ostatak modulo 5).

5. **Prvo rješenje**
Pretpostavimo da 7 ne dijeli a, onda ne dijeli niti b. Kvadratni ostaci pri dijeljenju s 7 su $1, 2, 4$, znači a^2 i b^2 daju neki od tih ostataka pa zbrajanjem dobivamo neki od idućih ostataka $1, 2, 3, 4, 5, 6$. U tom slučaju vidimo da 7 ne dijeli $a^2 + b^2$ pa slijedi tvrdnja zadatka.

Drugo rješenje
U ovom rješenje je jedino bitno da je 7 oblika $4k+3$ pa zapravo isto ovako bi se dokazala tvrdnja za svaki prost broj oblika $4k+3$. Primjetimo da je -1 kvadratni neostatak modlulo 7 pa slijedi $\left(\frac{x}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{-x}{7}\right) = -\left(\frac{-x}{7}\right)$ to jest nemoguće je da su x i $-x$ oboje kvadratni ostaci modulo 7 pa zaključujemo da mora vrijediti $a^2 \equiv -b^2 \equiv 0 \pmod{7}$ te slijedi tražena tvrdnja.

6. $x^2 - 31x + 34$ daje isti ostatak pri dijeljenju s 37 kao i $x^2 + 6x + 34 = (x+3)^2 + 25$, što daje isti ostatak pri dijeljenju s 37 kao i $(x+3)^2 - 12$. Ostaje provjeriti postoji li broj čiji kvadrat daje ostatak 12 pri dijeljenju s 37, međutim $37 + 12 = 49 = 7^2$. Dakle, takav broj postoji.

7. Trebamo naći sve proste brojeve za koje vrijedi $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$. Imamo dvije mogućnosti:

a) $\left(\frac{-1}{p}\right) = 1$ i $\left(\frac{2}{p}\right) = 1$. Prvi uvjet je ekvivalentan s $p \equiv 1 \pmod{4}$, a drugi s $p \equiv 1, 7 \pmod{8}$, što zajedno daje $p \equiv 1 \pmod{8}$.

b) $\left(\frac{-1}{p}\right) = -1$ i $\left(\frac{2}{p}\right) = -1$. Prvi uvjet je ekvivalentan s $p \equiv 3 \pmod{4}$, a drugi s $p \equiv 3, 5 \pmod{8}$, što zajedno daje $p \equiv 3 \pmod{8}$.

8. Uočimo da jedan od brojeva p, q ima oblik $4k+1$, a drugi $4k+3$. Stoga vrijedi

$$\begin{aligned} \exists a \in \mathbb{Z}, a^2 \equiv q \pmod{p} &\iff \left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right) = 1 \\ &\iff \exists b \in \mathbb{Z}, b^2 \equiv p \pmod{q}. \end{aligned}$$

9. a) Primjetimo da -1 nije kvadratni ostatak modulo p kada je p oblika $8k+7$, te za n paran 2^n je kvadrat pa 2^n+1 nije djeljivo s p.

b) Neka je $n=2k+1$.

$$2^n+1 \equiv 2\cdot 2^{2k}+1 \equiv 2\cdot(2^{2k}+\frac{-p+1}{2}) \pmod p$$

Vidimo da ako p dijeli 2^n+1 onda p dijeli $2^{2k}+\frac{-p+1}{2}$ pa je $\frac{p-1}{2}$ kvadratni ostatak modulo p. No,

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

pa je $(\frac{\frac{p-1}{2}}{p})=-1$ kontradikcija.

10. Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od brojeva

$$-\frac{p-1}{2},\dots,-1,1,\dots,\frac{p-1}{2},$$

tj. kongruentan je nekom od brojeva $1^2,2^2,\dots,(\frac{p-1}{2})^2$. Preostaje pokazati da je ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentno modulo p. Pretpostavimo da je $k^2\equiv l^2 \pmod p$, gdje je $1\le k<l\le \frac{p-1}{2}$. Tada je $(l-k)(l+k)\equiv 0 \pmod p$, što nije moguće jer je $0<l-k<l+k<p$.

11. Prvo prema tvrdnji prošlog zadatka znamo da imamo $2k$ kvadratnih ostataka modulo p. Pa pokažimo da imamo jednako parnih i neparnih ostataka. Primjetimo da je -1 kvadratni ostatak modulo p pa imamo tvrdnju $(\frac{x}{p})=(\frac{-x}{p})=(\frac{p-x}{p})$. Iz toga slijedi da x parni kvadratni ostatak modulo p, onda je $p-x$ neparni kvadratni ostatak te iz tog sparivanja vidimo da mora biti jednako parnih i neparnih kvadratnih ostataka pa parnih ima točno k.

12. Kako je $p>5$ brojevi $2,5,10$ su nekongruentni modulo p te barem jedan od njih je kvadratni ostatak modulo p jer vrijedi $(\frac{2}{p})(\frac{5}{p})=(\frac{10}{p})$. Također, $1,4,9$ su uvijek kvadratni ostaci pa vidimo da onda sigurno imamo 2 uzastopna kvadratna ostatka.

13. a) Pretpostavimo da q nije prost. Onda se može napisati kao $q=ab$, $a,b>1$. Iz $(\frac{a}{p})(\frac{b}{p})=(\frac{q}{p})=1$ dobivamo da je jedan od a,b kvadratni neostatak modulo p što je nemoguće zbog minimalnosti od q.

b) Neka je kq najmanji višekratnik broja q koji je veći od p, tj. $(k-1)q<p<kq$. Neka je $r=kq-p<q$. Stoga je r kvadratni ostatak modulo p, pa je kq kvadratni ostatk (jer je $kq\equiv r \pmod p$). Vidimo da k mora biti kvadratni neostatak, pa je $k\ge q$. Dobili smo da je $(q-1)q<p$ odakle slijedi tražena nejednakost.