MLADI NADARENI MATEMATIČARI
Marin Getaldić

Kvadratni ostatci

4.11.2017.

Uvod/teorijske osnove

Ovo predavanje podrazumijeva poznavanje osnovnih pojmova i rezultata iz djeljivosti i kongruencija. Za početak, uvedimo definiciju kvadratnih ostataka:

Definicija 1. *Za cijeli broj a kažemo da je kvadratni ostatak modulo n ako postoji cijeli broj x takav da je*

$$x^2 \equiv a \pmod{n}.$$

Drugim riječima, a je kvadratni ostatak modulo n ako postoji potpun kvadrat koji daje isti ostatak pri dijeljenju s n kao i a. Primjerice, 2 je kvadratni ostatak modulo 7 jer je $3^2 \equiv 2 \pmod{7}$, dok možemo vidjeti da 3 nije kvadratni ostatak modulo 5 jer niti jedan potpun kvadrat ne daje ostatak 3 pri dijeljenju s 5 (očito je potrebno provjeriti samo kvadrate brojeva 0, 1, 2, 3, 4).

U nastavku ovog predavanja posebno će nam biti zanimljivi kvadratni ostaci modulo prost broj p jer se pokazuje da imaju određena lijepa svojstva. Pojam kvadratnog ostatka u užem smislu koristit ćemo za brojeve iz skupa $\{0, 1, \ldots, p-1\}$, odnosno za brojeve koje smatramo ostacima pri dijeljenju s p. Imamo sljedeći teorem:

Teorem 1. *Ako je $p > 2$ prost broj, tada postoji $\frac{p+1}{2}$ različith kvadratnih ostataka modulo p.*

Dokaz teorema 1. Očito je 0 kvadratni ostatak modulo p, stoga ćemo dokazati da skup $\{1, 2, \ldots, p-1\}$ sadrži $\frac{p-1}{2}$ kvadratnih ostataka. Zapravo nas zanima koliko različitih ostataka pri dijeljenju s p postižu brojevi $1^2, 2^2, \ldots, (p-1)^2$. Tvrdimo da se svaki kvadratni ostatak različit od nule u tom nizu ostataka postiže točno dva puta. Zaista, ako se neki a postiže kao $a \equiv x^2 \pmod{p}$, gdje $x \in \{1, 2, \ldots, p-1\}$, tada se postiže i kao $a \equiv (p-x)^2 \pmod{p}$, gdje $p - x \neq x$ jer je p neparan. Također, ako se a postiže kao $a \equiv x^2 \equiv y^2 \pmod{p}$, tada je $x^2 \equiv y^2 \pmod{p}$ pa $p \mid x^2 - y^2$, odnosno $p \mid (x-y)(x+y)$. Kako je p prost broj, slijedi $p \mid x - y$ ili $p \mid x + y$, odnosno $x = y$ ili $x + y = p$ jer $x, y \in \{1, 2, \ldots, p-1\}$. To znači da se neki kvadratni ostatak ne može postići više od dva puta, zbog čega slijedi da se mora postići točno dva puta. Sada je jasno da skup $\{1, 2, \ldots, p-1\}$ sadrži $\frac{p-1}{2}$ kvadratnih ostataka.

Rad s kvadratnim ostacima modulo prost broj p olakšava nam tzv. *Legendreov simbol*, zato uvedimo i njegovu definiciju:

Definicija 2. (Legendreov simbol) *Za cijeli broj a i prost broj p definiramo:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{ako je } a \equiv 0 \pmod{p} \\ 1 & \text{ako je } a \not\equiv 0 \pmod{p} \text{ i } a \text{ je kvadratni ostatak modulo } p \\ -1 & \text{ako } a \text{ nije kvadratni ostatak modulo } p \end{cases}$$

Primjerice, po definiciji imamo $\left(\frac{6}{3}\right) = 0, \left(\frac{2}{7}\right) = 1$ te $\left(\frac{3}{5}\right) = -1$. Računanje Legendreovog simbola omogućuje nam sljedeći teorem:

Teorem 2 (Eulerov kriterij)**.** *Za cijeli broj a i prost broj p vrijedi $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Dokaz teorema 2. Ako je $a \equiv 0 \pmod{p}$, tada tvrdnja očito vrijedi, stoga promatrajmo slučaj kada a nije djeljiv s p. Ako je a kvadratni ostatak modulo p, postoji cijeli broj x takav da je $x^2 \equiv a \pmod{p}$ pa budući da x nije

djeljiv s p, zbog malog Fermatovog teorema slijedi $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ pa tvrdnja također vrijedi. Preostaje slučaj kada a nije kvadratni ostatak modulo p. Poznato je da za svaki $x \in \{1, 2, \ldots, p-1\}$ postoji jedinstven $y \in \{1, 2, \ldots, p-1\}$ takav da je $xy \equiv a \pmod{p}$. Kako a nije kvadratni ostatak modulo p, vrijedi $x \neq y$. Promotrimo li sve takve parove oblika (x, y), vidimo da smo skup $\{1, 2, \ldots, p-1\}$ podijelili na $\frac{p-1}{2}$ parova ostataka koji u umnošku daju a modulo p. Zaključujemo da vrijedi

$$a^{\frac{p-1}{2}} \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{p},$$

gdje smo u posljednjem koraku koristili Wilsonov teorem. Time je tvrdnja dokazana.

Napomena: Wilsonov teorem tvrdi da za svaki prost broj p vrijedi $(p-1)! \equiv -1 \pmod{p}$. Dokaz je sličan gornjem dokazu u slučaju kada a nije kvadratni ostatak modulo p, naime ideja je "upariti" ostatke koji u umnošku daju 1. Postoji i drugačiji dokaz ovog posljednjeg slučaja koji koristi Langrangeov teorem za polinome.

Korolar. Iz Teorema 2. direktno slijede neka svojstva Legendreovog simbola:

- Ako je $a \equiv b \pmod{p}$, tada je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- Vrijedi $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Drugim riječima, Legendreov simbol jest multiplikativan.
- Vrijedi $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{ako je } p \equiv 1 \pmod{4} \\ -1 & \text{ako je } p \equiv 3 \pmod{4} \end{cases}$.
  Posljedično, brojevi oblika $n^2 + 1$ nemaju prost faktor oblika $4k + 3$.

Konačno, dolazimo i do najtežeg teorema ovog predavanja, koji predstavlja vezu između kvadratnih ostataka modulo p i modulo q za različite neparne proste brojeve p i q. Izreći ćemo ga bez dokaza jer dokaz izlazi van granica ovog predavanja. Ako vas zanima dokaz, možete ga naći na `https://en.wikipedia.org/wiki/Proofs_of_quadratic_reciprocity`.

Teorem 3 (Gaussov zakon kvadratnog reciprociteta)**.** *Za različite neparne proste brojeve p i q vrijedi*

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

Napomena: Primijetite da Teorem 3. ne govori ništa o vrijednosti $\left(\frac{2}{p}\right)$ za neparan prost broj p. Zato postoji i dopuna ovog teorema koja glasi $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{ako } p \equiv 1 \text{ ili } 7 \pmod{8} \\ -1 & \text{ako } p \equiv 3 \text{ ili } 5 \pmod{8} \end{cases}$.

Primjer 1. U ovom ćemo primjeru pokazati kako možemo iskoristiti gornje teoreme za računanje nekih konkretnih vrijednosti Legendreovog simbola. Primjerice, odredimo vrijednost $\left(\frac{80}{59}\right)$. Vrijedi

$$\begin{aligned}
\left(\frac{80}{59}\right) &= \left(\frac{21}{59}\right) = \left(\frac{3}{59}\right)\left(\frac{7}{59}\right) \\
&= \left(\frac{59}{3}\right)(-1)^{\frac{59-1}{2}\frac{3-1}{2}}\left(\frac{59}{7}\right)(-1)^{\frac{59-1}{2}\frac{7-1}{2}} \\
&= \left(\frac{2}{3}\right)\left(\frac{3}{7}\right) = (-1)^{\frac{3^2-1}{8}}\left(\frac{7}{3}\right)(-1)^{\frac{3-1}{2}\frac{7-1}{2}} \\
&= \left(\frac{1}{3}\right) = 1.
\end{aligned}$$

Primjer 2. Dokaži da postoji beskonačno mnogo prostih brojeva p takvih da $p \equiv 1 \pmod{4}$.

Rješenje: Pretpostavimo suprotno, tj. da takvih brojeva ima konačno (znamo da postoji bar jedan takav, npr. $p = 5$). Neka su $p_1, p_2, \ldots, p_k$ svi prosti brojevi tog oblika. Promatrajmo broj $P = (2p_1p_2 \ldots p_k)^2 + 1$. Iz korolara drugog teorema slijedi da P nema prost faktor q takav da $q \equiv 3 \pmod{4}$. To znači da P ima prost faktor q takav da $q \equiv 1 \pmod{4}$ (jer je P neparan), no tada slijedi da $q = p_i$ za neki $i \in \{1, 2, \ldots, k\}$. Time dolazimo do kontradikcije jer nije moguće da $p_i \mid P$, čime je tvrdnja dokazana.

Zadatci i rješenja

Zadatak 1.
Dokaži da $x^2 - 17y^2 = 12$ nema rješenja u cijelim brojevima.

Rješenje.
Promatrajući ostatke pri dijeljenju sa 17, vrijedi $x^2 \equiv 12 \pmod{17}$, dok iz kvadratne recipročnosti imamo

$$\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{2^2}{17}\right) = \left(\frac{3}{17}\right)$$
$$= \left(\frac{17}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{2}{3}\right) = -1,$$

što je kontradikcija.

Zadatak 2.
Neka su p i q dva različita prosta broja, od kojih svaki daje ostatak 3 pri dijeljenju s 4. Onda jednadžba

$$x^2 - py^2 = q$$

nema rješenja u cijelim brojevima.

Rješenje.
Ako promatramo jednadžbu modulo p vidimo da q mora biti kvadratni ostatak, a ako je promatramo modulo q onda p mora biti kvadratni ostatak. Onda imamo

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

što je kontradikcija

Zadatak 3.
Dokaži da je svaki prost djeljitelj broja $n^4 - n^2 + 1$ oblika $12k + 1$.

Rješenje.
Želimo broj zapisati kao kombinacije nekih kvadrata da izvučemo što više informacija. Primjetimo da vrijedi

$$n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2$$
$$n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2.$$

Iz prve jednakosti slijedi

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

a iz druge

$$\left(\frac{3}{p}\right) = 1,$$

odakle skupa dobivamo $p \equiv 1 \pmod{12}$.

Zadatak 4.
Pokaži da svaki neparan djeljitelj broja $5x^2 + 1$ ima parnu znamenku desetica.

Rješenje.
Kako vrijedi $5x^2 \equiv -1 \pmod{p}$ onda $\left(\frac{-5}{p}\right) = 1$. Kvadratni reciprocitet daje

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$

Odavde se lako provjeri da p mora biti kogruentan $1, 3, 7$ ili 9 modulo 20.

Zadatak 5.
Dokaži da za svaki prost broj p postoje cijeli brojevi a, b takvi da je $a^2 + b^2 + 1$ višekratnik broja p.

Rješenje.
p dijeli $a^2 + b^2 + 1$ ako i samo ako vrijedi $a^2 \equiv -b^2 - 1 \pmod{p}$. Kako oba a^2 i $-b^2 - 1$ poprimaju točno $\frac{p+1}{2}$ vrijednosti modulo p, onda imaju i neku zajedničku koja zadovoljava uvjet zadatka.

Zadatak 6.
Ako su a i b relativno prosti prirodni brojevi i c prirodan broj, takvi da $a^2 - ab + b^2 = c^2$, dokaži da su svi prosti djeljitelji broja c oblika $6k + 1$.

Rješenje.
Uzmimo p takav da p dijeli c. Slijedi da p dijeli $a^2 - ab + b^2$, pa onda dijeli i $4a^2 - 4ab + 4b^2$. Onda redom imamo

$$(2a - b)^2 \equiv -3b^2 \pmod{p}$$
$$((2a - b)b^{-1})^2 \equiv -3 \pmod{p}$$
$$\left(\frac{-3}{p}\right) = 1,$$

odakle slijedi $p \equiv 1 \pmod{3}$. Ako pokažemo da $p \neq 2, 3$ onda znamo da $p \equiv \pm 1 \pmod{6}$ odakle, skupa sa $p \equiv 1 \pmod{3}$ dobivamo traženo.
Slučaj $p = 2$ se lako odbaci promatranjem parnosti uz uvjet $NZD(a, b) = 1$.
U drugom slučaju, 3 dijeli $2a - b$, dakle $b \equiv 2a \pmod{3}$. Supstitucijom $a = 3a' + 1$ i $b = 3b' + 2$ dobivamo

$$9a'^2 + 9b'^2 - 9a'b' + 9b' + 3 = c^2.$$

Kako vrijedi da je $LHS \equiv 3 \pmod{9}$, a $\left(\frac{3}{9}\right) = -1$, dobili smo kontradikciju, dakle $p \neq 3$, čime smo gotovi.

Zadatci za samostalan rad

Zadatak 7.
Dokaži da jednadžba $x^2 - 3y^2 = p$ nema rješenja u cijelim brojevima kad je $p = 2$ ili $p = 3$.

Zadatak 8.
Dokaži da $2^n + 1$ nema prostih djeljitelja oblika $8k + 7$.

Zadatak 9.
Ako neparan prost broj p dijeli $a^2 + b^2$ za neke relativno proste cijele brojeve a, b, onda $p \equiv 1 \pmod{4}$

Zadatak 10.
Ako neparan prost broj p dijeli $a^2 + 2b^2$ za neke cijele relativno proste brojeve a, b, onda $p \equiv 1 \pmod{8}$ ili $p \equiv 3 \pmod{3}$.

Zadatak 11.
Ako neparan prost broj p dijeli $a^2 - 2b^2$ za neke cijele relativno proste brojeve a, b, onda $p \equiv 1 \pmod{8}$ ili $p \equiv -1 \pmod{8}$.

Zadatak 12.
Dokaži da jednadžba

$$x^3 - 3 = 2y^2$$

nije rješiva u cijelim brojevima.

Zadatak 13.
Dokaži da jednadžba

$$8xy - (x + y) = z^2$$

nije rješiva u prirodnim brojevima.

Zadatak 14.
Dokaži da jednadžba $x^3 - x^2 + 8 = y^2$ nema rješenja u cijelim brojevima.

Zadatak 15.
Dokaži da $\frac{x^2+1}{y^2-5}$ ne može biti cijeli broj za prirodne brojeve x i y veće od 2.

Zadatak 16.
Dokaži da ne postoje prirodni brojevi x, y, z za koje je $4xyz - x - y$ potpun kvadrat.

Zadatak 17.
Za prirodan broj n, dokaži da su svi prosti djeljitelji broja $n^8 - n^4 + 1$ oblika $24k + 1$.

Zadatak 18.
Dokaži da ne postoje prirodni brojevi a, b, c takvi da je

$$\frac{a^2 + b^2 + c^2}{3(ab + bc + ca)}$$

cijeli broj.

Rješenja

Rješenje zadatka 7. Promatrajmo jednadžbu $x^2 - 3y^2 = 2$ modulo 3. Dobivamo $x^2 \equiv -1 \pmod 3$ što je kontradikcija.
U drugom slučaju, promatrajmo jednadžbu modulo 4. Dobivamo $x^2 + y^2 \equiv 3 \pmod 4$, što je također kontradikcija.

Rješenje zadatka 8. Pretpostavimo suprotno, tj. da $2^n \equiv -1 \pmod p$ za neki $p \equiv 3 \pmod 8$. Kako je $p \equiv 3 \pmod 4$, -1 nije kvadratni ostatak, odakle slijedi da je n neparan. Sad imamo $2^{n+1} \equiv -2 \pmod p$ pa je -2 kvadratni ostatak.
S druge strane,

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

što je kontradikcija.

Rješenje zadatka 9. Uzmimo $p \equiv 3 \pmod 4$ koji dijeli takav $a^2 + b^2$. Onda $a^2 \equiv -b^2 \pmod p$. Iz malog Fermatovog teorema imamo $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$. Sad vrijedi

$$1 = a^{p-1} = (a^2)^{\frac{p-1}{2}} = (-b^2)^{\frac{p-1}{2}} = -1$$

zbog naše pretpostavke.
Dakle imamo kontradikciju i zadatak je riješen.

Rješenje zadatka 10. Uzmimo neki prosti djeljitelj p za koji $a^2 \equiv -2b^2 \pmod p$. Kako su a i b relativno prosti, množenjem obje strane s inverzom od b dobivamo

$$(ab^{-1})^2 \equiv -2 \pmod p,$$

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

odakle lako slijedi $p \equiv 1 \pmod 8$ ili $p \equiv 3 \pmod 8$.

Rješenje zadatka 11. Rješenje je identično rješenju prošlog zadatka.

Rješenje zadatka 12. Jednadžba se može zapisati na ovakva dva načina:

$$x^3 - 1 = 2(y^2 + 1),$$
$$x^3 + 1 = 2(y^2 + 2).$$

Primjetimo prvo da su obje desne strane nedjeljive s 8. Dalje, kako je x neparan, dovoljno je pogledati slučajeve $x = 8k \pm 1$ i $x = 8k \pm 3$.
Ako je $x = 8k + 1$, onda je lijeva strana prve jednadžbe djeljiva s 8, kontradikcija. Analogno se pokaže i za $x = 8k - 1$.
Ako je $8k \pm 3$, onda je $x^2 - x + 1$ oblika $8m - 1$ ili $8m - 3$, i ima djeljitelja ovog oblika, što je u kontradikciji s desetim zadatkom.

Rješenje zadatka 13. Jednadžba se može zapisati kao

$$(8x - 1)(8y - 1) = 8z^2 + 1.$$

Kako je $8x - 1 \geqslant 7$, lijeva strana ima prostog djeljitelja oblika $8m - 1$ ili $8m - 3$, a kako ovo treba dijeliti i desnu stranu, imamo kontradikciju s jedanaestim zadatkom.

Rješenje zadatka 14. Jednadžba se može prikazati kao

$$(x + 2)(x^2 - 2x + 4) = x^2 + y^2.$$

Jasno je da su x i y relativno prosti. Ako je $x = 4k + 1$ onda $x + 2 = 4k + 3$ ima prostog djeljitelja ovog oblika koji dijeli $x^2 + y^2$, kontradikcija.
Ako $x = 4k + 3$, onda je $x^2 - 2x + 4$ oblika $4m + 3$, i sličnim argumentom ponovno dobivamo kontradikciju.
Za $x = 2u$, jednadžba postaje

$$2u^3 - u^2 + 2 = z^2.$$

Ako je u neparan, onda je lijeva strana kongruentna 3 modulo 4, pa ne može biti potpun kvadrat. Ako je u paran, onda je lijeva strana kongruentna 2 modulo 4 i također ne može biti kvadrat, čime smo gotovi.

Rješenje zadatka 15. Ako je y paran, onda je $y^2 - 5$ oblika $4k + 3$, pa ne može dijeliti $x^2 + 1$. Ako je y neparan, onda je $y^2 - 5$ djeljiv s 4, dok $x^2 + 1$ nikad nije višekratnik od 4.

Rješenje zadatka 16. Pretpostavimo suprotno. Onda imamo $4xyz - x - y = t^2$. Množeći sve s $4z$ dobivamo

$$(4xz - 1)(4yz - 1) = 4zt^2 + 1.$$

Dakle, $-z$ je kvadratni ostatak modulo $4xz - 1$. Dalje koristimo Jacobijev simbol. Ako je z neparan imamo

$$\left(\frac{-z}{4xz-1}\right) = \left(\frac{-1}{4xz-1}\right)\left(\frac{z}{4xz-1}\right) = (-1)\cdot(-1)^{\frac{z-1}{2}}\left(\frac{-1}{z}\right) = -1$$

Ako je z paran stavimo $z = 2^l z'$, pa imamo

$$\left(\frac{-z}{4xz-1}\right) = \left(\frac{2}{4xz-1}\right)^l\left(\frac{-z'}{4xz-1}\right) = 1^l \cdot (-1) = -1,$$

kontradikcija.

Rješenje zadatka 17. Imamo

$$n^8 - n^4 + 1 = (n^4 + n^2 + 1)^2 - 2(n^3 + n)^2$$

odakle dobivamo

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

a iz ovog slijedi $p \equiv \pm 13 \pmod{24}$.

Rješenje zadatka 18. Zapišimo uvjet u obliku

$$(a + b + c)^2 = (3n + 2)(ab + bc + ca).$$

Očito postoji prost broj $p \equiv 2 \pmod 3$ koji dijeli $3n+2$ neparno puta. Taj broj onda mora dijeliti i $ab+bc+ca$. Uvrštavanjem $c \equiv -a-b \pmod p$ u prošlu relaciju dobivamo da p dijeli a^2+ab+b^2, pa onda dijeli i $(2a+b)^2+3b^2$. Slijedi da je $\left(\frac{-3}{p}\right) = 1$, što je kontradikcija s $p \equiv 2 \pmod 3$.