Poglavlje 3

Kvadratni ostaci

Neka je p prost broj i $a \in \mathbb{Z}$ relativno prost s p. Kažemo da je a kvadratni ostatak mod p ako postoji $x \in \mathbb{Z}$ takav da je $a \equiv x^2 \pmod{p}$.

Teorem: *Neka je $p > 2$ prost broj. Tada u skupu $\{1, 2, \ldots, p-1\}$ postoji točno $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ neostataka mod p.*

Neka je $p > 2$ prost broj i $a \in \mathbb{Z}$. Legendreov simbol $\left(\frac{a}{p}\right)$ definira se na sljedeći način:

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

Teorem: *Legendreov simbol ima sljedeća svojstva:*

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

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ ako } a \equiv b \pmod{p}$$

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & : p \equiv \pm 1 \pmod{8}, \\ -1 & : p \equiv \pm 3 \pmod{8}, \end{cases},$$

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \text{ za različite neparne proste } p, q.$$

$$= \begin{cases} -\left(\frac{p}{q}\right) & : p, q \equiv -1 \pmod{4}, \\ \left(\frac{p}{q}\right) & : \text{inače.} \end{cases}$$

Zadnja tvrdnja se zove Gaussov kvadratni zakon reciprociteta.

Direktno iz definicije Legendreovih simbola vidimo da -1 nije kvadratni ostatak mod $p = 4k + 3$. Sljedeća važna tvrdnja lagano slijedi iz te činjenice.

Teorem: *Neka je $p = 4k + 3$ prost broj. Ako za neke $x, y \in \mathbb{Z}$ vrijedi $p \mid x^2 + y^2$, tada $p \mid x, y$.*

Neka je $Q = q_1 \dots q_s \in \mathbb{N}$ neparan (prosti brojevi q_i ne moraju biti različiti). Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira se preko Legendreovih simbola na sljedeći način.

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1}\right) \dots \left(\frac{a}{q_s}\right).$$

Ako je Q prost broj, tada se Jacobijev i Legendreov simbol podudaraju.

Teorem: *Jacobijev simbol ima sljedeća svojstva:*

$$\left(\frac{a}{Q}\right) = -1 \implies a \text{ nije kvadratni ostatak mod } Q,$$
$$\left(\frac{a}{QQ'}\right) = \left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right),$$
$$\left(\frac{aa'}{Q}\right) = \left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right),$$
$$\left(\frac{a}{Q}\right) = \left(\frac{a'}{Q}\right) \text{ ako } a \equiv a' \pmod{Q},$$
$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}},$$
$$\left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right)(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} \text{za relativno proste neparne } P, Q \in \mathbb{N}.$$

Primijetite da, ako je $\left(\frac{a}{Q}\right) = 1$, ne možemo samo iz Jacobijevog simbola odrediti je li a kvadratni ostatak mod Q, već moramo to provjeravati zasebno za svaki prost djelitelj $q_i \mid Q$.

Zadatak 3.1. Izračunajte Legendreove simbole $\left(\frac{-558}{733}\right), \left(\frac{237}{457}\right)$.

Rješenje.

$$\begin{aligned}\left(\frac{-558}{733}\right) &= \left(\frac{9}{733}\right)\cdot\left(\frac{2}{733}\right)\cdot\left(\frac{-1}{733}\right)\cdot\left(\frac{31}{733}\right) = \\ &= 1\cdot(-1)\cdot 1\cdot\left(\frac{31}{733}\right) = -\left(\frac{31}{733}\right) = \\ &= -\left(\frac{733}{31}\right) = -\left(\frac{20}{31}\right) = -\left(\frac{4}{31}\right)\cdot\left(\frac{5}{31}\right) = \\ &= -\left(\frac{5}{31}\right) = -\left(\frac{31}{5}\right) = -\left(\frac{1}{5}\right) = -1,\end{aligned}$$

$$\begin{aligned}\left(\frac{237}{457}\right) &= \left(\frac{457}{237}\right) = \left(\frac{220}{237}\right) = \left(\frac{4}{237}\right)\cdot\left(\frac{55}{237}\right) = \\ &= \left(\frac{55}{237}\right) = \left(\frac{237}{55}\right) = \left(\frac{17}{55}\right) = \\ &= \left(\frac{55}{17}\right) = \left(\frac{4}{17}\right) = 1.\end{aligned}$$

Primijetite da smo u drugom nizu jednakosti pojednostavili račun korištenjem Jacobijevih simbola. Naime, Jacobijevi simboli su proširenje Legendreovih simbola i za njih vrijedi isti Gaussov zakon reciprociteta pa ne moramo svaki put faktorizirati brojeve prije okretanja (osim dvojke koju moramo izvući van jer zakon reciprociteta vrijedi samo za neparne brojeve).

Zadatak 3.2. Izračunajte $\left(\frac{65}{231}\right)$. Je li 65 kvadratni ostatak mod 231?

Rješenje. Vrijedi

$$\left(\frac{65}{231}\right) = \left(\frac{65}{3}\right) \cdot \left(\frac{65}{7}\right) \cdot \left(\frac{65}{11}\right) = (-1) \cdot 1 \cdot (-1) = 1.$$

Međutim, iz računa vidimo da 65 nije kvadratni ostatak mod 231 jer nije kvadratni ostatak mod 3 i mod 11.

Zadatak 3.3. Odredite sve proste brojeve p takve da je je a kvadratni ostatak mod p za

(a) $a = -3$.

(b) $a = -2$.

(c) $a = 5$.

Rješenje. (a) $p = 2$ je očito rješenje. Neka je sada $p \geq 5$. Vrijedi

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = \begin{cases} 1 & : p = 3k+1, \\ -1 & : p = 3k+2. \end{cases}$$

Dakle, sva rješenja su $p = 2$ i prosti brojevi oblika $3k + 1$.

(b) Vrijedi

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{p^2-1}{8}} = \begin{cases} 1 & : p = 8k+1 \text{ or } p = 8k+3, \\ -1 & : p = 8k+5 \text{ or } p = 8k+7. \end{cases}$$

Dakle, sva rješenja su prosti brojevi oblika $8k + 1$ i $8k + 3$.

(c) $p = 2$ je očito rješenje i vidimo da $p = 3$ nije. Neka je sada $p \geq 7$. Tada je

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & : p = 5k \pm 1, \\ -1 & : p = 5k \pm 2. \end{cases}$$

Dakle, sva rješenja su $p = 2$ i prosti brojevi oblika $5k \pm 1$.

Zadatak 3.4. Neka je p prost broj i $k \in \mathbb{Z}$. Dokažite da postoje $a, b \in \mathbb{Z}$ takvi da $p \mid a^2 + b^2 + k$.

Rješenje. Skupovi

$$A = \{x^2 \bmod p : x \in \{0, 1, \ldots, p-1\}\},\ B = \{(-k-y^2) \bmod p : x \in \{0, 1, \ldots, p-1\}\}$$

imaju po $\frac{p+1}{2}$ elemenata ($\frac{p-1}{2}$ kvadratnih ostataka i nula). Stoga je $A \cap B \neq \emptyset$ pa postoje x, y takvi da je $x^2 \equiv -k - y^2 \pmod{p} \iff p \mid x^2 + y^2 + k$.

Zadatak 3.5. Dokažite da suma kvadrata 5 uzastopnih prirodnih brojeva ne može biti potpun kvadrat.

Rješenje. Pretpostavimo da je $(x-2)^2 + (x-1)^2 + x^2 + (x+1)^2 + (x+2)^2 = y^2$. Nakon pojednostavljivanja dobivamo jednadžbu $5(x^2+2) = y^2$. Stoga mora vrijediti $5 \mid x^2 + 2$, međutim $x^2 \equiv 0, 1, 4 \pmod{5}$ i dobili smo kontradikciju.

Zadatak 3.6. Odredite sve $n, k \in \mathbb{N}_0$ takve da je $n^6 - 1 = 63 \cdot 85^k$.

Rješenje. Primijetimo da je

$$n^6 - 1 = (n-1)(n+1)(n^2 - n + 1)(n^2 + n + 1).$$

Također, ako $p \mid n^2 \pm n + 1$, tada $p \mid 4n^2 \pm 4n + 4 = (2n \pm 1)^2 + 3$ što znači da je $\left(\frac{-3}{p}\right) = 1$. Gaussov zakon reciprociteta nam kaže da je $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Zaključujemo da su brojevi $n^2 \pm n + 1$ nemaju djelitelja oblika $3k + 2$.

Kako $5, 17 \equiv 2 \pmod{3}$, to znači da $85^k \mid (n-1)(n+1)$. Onda mora vrijediti da $n^4 + n^2 + 1 = (n^2 - n + 1)(n^2 + n + 1) \mid 63$. To znači da je $n^4 + n^2 + 1 \leq 63$ pa je $n \leq 2$. Lako se provjeri da je $n = 2, k = 0$ jedino rješenje.

Zadatak 3.7. Odredite sve $n, a, b, c, d \in \mathbb{N}_0$ takve da je $n^4 + 1 = 2^a 5^b 11^c 43^d$.

Rješenje. Ako $p \mid n^4 + 1$, tada mora vrijediti $\left(\frac{-1}{p}\right) = 1$, tj. $p \equiv 1 \pmod{4}$. To znači da je $c = d = 0$.

Primijetimo također da $n^4 + 1$ ne može biti djeljivo s 4 pa je $a \leq 1$. Po Malom Fermatovom teoremu je $n^4 \equiv 0, 1 \pmod{5}$ pa je i $b = 0$. Stoga su jedina rješenja $n = 0, a = 0$ i $n = 1, a = 1$.

Zadatak 3.8. Dokažite da za $x, y \in \mathbb{Z}$ vrijedi tvrdnja $7 \mid x^2 + 2y^2 \implies 7^2 \mid x^2 + 2y^2$.

Rješenje. Kako je $\left(\frac{-2}{7}\right) = 1$, dobivamo da vrijedi sljedeće: ako $7 \mid x^2 + 2y^2$, tada $7 \mid x, y$. Sada sigurno vrijedi $7^2 \mid x^2 + 2y^2$.

Zadatak 3.9. Dokažite da za $n \geq 2$ svaki prost djelitelj broja $2^{2^n} + 1$ daje ostatak 1 mod 2^{n+2}.

Rješenje. Neka $p \mid 2^{2^n} + 1$. Tada $p \mid 2^{2^{n+1}} - 1$ i $p \nmid 2^{2^n} - 1$ pa je $\mathrm{ord}_p(2) = 2^{n+1}$. Zaključujemo da $2^{n+1} \mid \varphi(p) = p - 1$.

Kako je $n \geq 2$, vidimo da je $p \equiv 1 \pmod{8}$ pa je $\left(\frac{2}{p}\right) = 1$. To po definiciji Legendreovog simbola znači da je

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Stoga $2^{n+1} \mid \frac{p-1}{2} \implies p \equiv 1 \pmod{2^{n+2}}$.

Zadatak 3.10. Dokažite da $p \nmid 2^n + 3$ za sve $n \in \mathbb{N}$ i proste brojeve $p \equiv 17 \pmod{24}$.

Rješenje. Ako $2 \mid n$, tada $p \mid x^2 + 3$ pa je $\left(\frac{-3}{p}\right) = 1$ pa je $p \equiv 1 \pmod 3$ što je u suprotnosti s $p \equiv 11 \pmod{24}$.

Ako $2 \nmid n$, tada $p \mid 2x^2 + 3 \implies p \mid 4x^2 + 6$ pa je $\left(\frac{-6}{p}\right) = 1$. Međutim, zbog uvjeta $p \equiv 17 \pmod{24}$ dobivamo da je

$$\left(\frac{-6}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{2}{p}\right) = (-1) \cdot 1 = -1,$$

kontradikcija.

Zadatak 3.11. Dokažite da ne postoji $n \in \mathbb{N}$ takav da $101 \mid 9^n + 7$.

Rješenje. Ako $101 \mid 9^n + 7 = x^2 + 7$, tada je -7 kvadratni ostatak mod 101. Međutim, $\left(\frac{-7}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1$.

Zadatak 3.12. Dokažite da je 3 primitivni korijen za sve Mersenneove proste brojeve $p = 2^k + 1$ veće od 3.

Rješenje. Primijetimo prvo da je k potencija broja 2. Kako je $\varphi(p) = p - 1 = 2^k$, dovoljno je provjeriti da je $3^{2^{k-1}} \neq 1 \pmod p$. Međutim,

$$3^{2^{k-1}} = 3^{\frac{p-1}{2}} = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2^k + 1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

što dokazuje da je 3 primitivni korijen.

Zadatak 3.13. Neka je $p = 4n + 1$ prost broj. Odredite ostatak pri dijeljenju broja n^n s p.

Rješenje. Koristit ćemo jednakost $(4n)^n = 2^{2n} \cdot n^n$. Znamo da je $(4n)^n \equiv (-1)^n \pmod p$ i

$$2^{2n} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2n^2+n} = (-1)^n \pmod p.$$

Stoga je $n^n \equiv 1 \pmod p$.

Zadatak 3.14. Dokažite da jednadžba $4ab - a - b = x^2$ nema rješenja u $\mathbb{N}$.

Rješenje. Kad obje strane pomnožimo s 4 i dodamo 1, dobivamo $(4a-1)(4b-1) = 4x^2 + 1$. Međutim, izraz $4x^2 + 1$ nema prostih djelitelja oblika $4k + 3$.

Zadatak 3.15. Neka je $p > 2$ prost broj. Dokažite da postoji prirodni broj manji od $\sqrt{p} + 1$ koji nije kvadratni ostatak mod p.

Rješenje. Neka je $0 < a < p$ najmanji kvadratni neostatak mod p. Tada je $\left(\frac{ak}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{k}{p}\right) = -1$ za sve $0 < k < a$. Pretpostavimo da je $a > \sqrt{p}+1$. Za $k = \lfloor \frac{p}{a} \rfloor + 1 \leq \sqrt{p} + 1 < a$ vrijedi $p < ak < p + a$, tj. $0 < ak - p < a$. Stoga bi moralo biti

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

što nije moguće. Dobili smo kontradikciju pa mora vrijediti $a < \sqrt{p} + 1$.

Zadatak 3.16. Neka je p prost broj. Dokažite ekvivalenciju

$$\exists x \in \mathbb{Z}, p \mid x^2 - x + 3 \iff \exists y \in \mathbb{Z}, p \mid y^2 - y + 25.$$

Rješenje. Primijetimo da su brojevi $x^2 - x + 3, y^2 - y + 25$ neparni što automatski rješava slučaj $p = 2$. Neka je sada $p \geq 3$. Vrijedi

$$p \mid x^2 - x + 3 \iff p \mid 4x^2 - 4x + 12 = (2x-1)^2 + 11.$$

Takav x postoji ako i samo ako je $\left(\frac{-11}{p}\right) = 1$. Slično je

$$p \mid y^2 - y + 25 \iff p \mid 4y^2 - 4y + 100 = (2y-1)^2 + 99.$$

Takav y postoji ako i samo ako je $\left(\frac{-99}{p}\right) = 1$. Ekvivalencija slijedi jer je $\left(\frac{-99}{p}\right) = \left(\frac{-11}{p}\right)\left(\frac{3}{p}\right)^2 = \left(\frac{-11}{p}\right)$.

Zadatak 3.17. Odredite sve $x, y \in \mathbb{N}$ takve da vrijedi $y^2 - 5 \mid x^2 + 1$.

Rješenje. Izraz $x^2 + 1$ ne može biti djeljiv s 4 pa y mora biti paran. Međutim, sada je izraz $y^2 - 5$ oblika $4k + 3$. Ako je $y^2 - 5 > 0$, tada $y^2 - 5 \nmid x^2 + 1$ jer $x^2 + 1$ nema prostih djelitelja oblika $4k + 3$.

Jedina preostala mogućnost je $y = 2$ i vidimo da su svi parovi $(x, y) = (x, 2)$ rješenje zadatka.

Zadatak 3.18. Dokažite da za svaki prost broj p postoji $n \in \mathbb{N}$ takav da $p \mid (n^2 - 3)(n^2 - 5)(n^2 - 15)$.

Rješenje. Ako je $p = 3, 5$, možemo uzeti $n = p$. Ako je $p = 2$, možemo uzeti $n = 1$. Neka je sada $p \neq 2, 3, 5$. Tada znamo da vrijedi

$$\left(\frac{3}{p}\right) \cdot \left(\frac{5}{p}\right) = \left(\frac{15}{p}\right).$$

Zbog multiplikativnosti Legendreovih simbola bar jedan od brojeva $\left(\frac{3}{p}\right), \left(\frac{5}{p}\right), \left(\frac{15}{p}\right)$ je jednak 1.

Zadatak 3.19. Odredite sve $n \in \mathbb{N}$ za koje vrijedi $12n^2 + 3 \mid 2^n + 1$.

Rješenje. Kako $3 \mid 2^n+1$, n mora biti neparan. Neka $p \mid 4n^2+1$. Tada $p \mid 2^n+1 = 2x^2+1$ pa je $\left(\frac{-2}{p}\right) = 1$. Stoga je $p \equiv 1,3 \pmod 8$. Međutim, $4n^2+1 \equiv 4+1 = 5 \pmod 8$ sigurno ima prost djelitelj oblika $8k+5$ ili $8k+7$ što je kontradikcija. Dakle, ne postoji takav n.

Zadatak 3.20. Odredite sve proste brojeve p koji dijele neki od brojeva oblika x^2+5x+7.

Rješenje. Broj x^2+5x+7 je uvijek neparan pa je $p \neq 2$. Sada vrijedi

$$p \mid x^2+5x+7 \iff p \mid 4x^2+20x+28 = (2x+5)^2+3.$$

Takav x postoji ako i samo ako je $1 = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Stoga su rješenje svi p oblika $3k+1$.

Zadatak 3.21. Odredite sve $a, b \in \mathbb{N}$ takve da $2^b-1 \mid 2^a+1$.

Rješenje. Ako je $b = 1$, tada je svaki a rješenje. Ako je $b = 2$, tada je svaki $2 \nmid a$ rješenje. Neka je sada $b \geq 3$.

Pretpostavimo da $2 \mid a$. Tada $2^a+1 = x^2+1$ nema prostih djelitelja oblika $4k+3$, ali 2^b-1 je oblika $4k+3$ pa imamo kontradikciju.

Pretpostavimo da $2 \nmid a$. Tada $2^a+1 = 2x^2+1$ i za svaki prost $p \mid 2^a+1$ vrijedi $\left(\frac{-2}{p}\right) = 1 \implies p \equiv 1,3 \pmod 8$. Međutim, $2^b-1 \equiv -1 \pmod 8$ sigurno ima prost djelielj oblika $8k+5$ ili $8k+7$, kontradikcija.

Dakle, sva rješenja su $(a,b) = (n,1), (2n-1,2)$ za neki $n \in \mathbb{N}$.

Zadatak 3.22. Dokažite da svaki neparni djelitelj broja $5x^2+1$ ima parnu znamenku desetica.

Rješenje. Ako $p \mid 5x^2+1$, tada je $1 = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$. Dakle, imamo 2 slučaja:

$$\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = 1 \implies p \equiv 1 \pmod 4, p \equiv \pm 1 \pmod 5 \implies p \equiv 1,9 \pmod{20},$$

$$\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = -1 \implies p \equiv -1 \pmod 4, p \equiv \pm 2 \pmod 5 \implies p \equiv 3,7 \pmod{20}.$$

Nije teško provjeriti da umnožak prostih brojeva koji daju ostatke $1,3,7,9 \bmod 20$ također daje ostatak $1,3,7,9 \bmod 20$ pa ima parnu znamenku desetica.

Zadatak 3.23. (*) Odredite sve $n \in \mathbb{N}$ za koje vrijedi $2^n+1 \mid 5^n-1$.

Rješenje. Ako je n neparan, broj 2^n+1 je djeljiv s 3, ali 5^n-1 nije. Stoga $2 \mid n$. Također $n \neq 4k+2$ jer u tom slučaju $5 \mid 2^n+1$.

Neka je $n = 2^a b$ za $2 \nmid b$ i $a \geq 2$. Neka $p \mid 2^n+1$, tada jednog od prošlih zadataka znamo da je $p \equiv 1 \pmod{2^{a+2}}$. Međutim, također vrijedi i $p \mid 5^n-1$ te $5^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. Ako je $5^{\frac{p-1}{2}} \equiv -1 \pmod p$, tada je

$$5^{\frac{p-1}{2}b} \equiv -1 \pmod p,\ 5^n \equiv 1 \pmod p,$$

što je nemoguće. Naime, $n = 2^a b \mid \frac{p-1}{2} b$ jer $p \equiv 1 \pmod{2^{a+2}} \iff 2^{a+1} \mid \frac{p-1}{2}$.

Zaključujemo da je $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = 5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ iz čega slijedi da je $p \equiv \pm 1 \pmod 5$. Dakle, svi prosti djelitelji broja $2^n + 1$ moraju biti oblika $5k \pm 1$, ali $2^n + 1 \equiv 1 + 1 = 2 \pmod 5$ pa on nužno ima djelitelj oblika $5k \pm 2$, kontradikcija. Stoga ne postoji takav $n \in \mathbb{N}$.

Zadatak 3.24. (*) Ako su $m, n \in \mathbb{N}$ takvi da je $\sqrt{7} > \frac{m}{n}$, dokažite da je $\sqrt{7} > \frac{m}{n} + \frac{1}{mn}$.

Rješenje. Vrijedi

$$7n^2 > m^2 \implies 7n^2 \geq m^2 + 1.$$

Međutim, jednadžba $7n^2 = m^2 + 1$ nema rješenja u $\mathbb{Z}$ jer je $\left(\frac{-1}{7}\right) = -1$. Stoga je $7n^2 \geq m^2 + 2$.

Međutim, ni jednadžba $7n^2 = m^2 + 2$ nema rješenja u $\mathbb{Z}$ zbog $\left(\frac{-2}{7}\right) = -1$ pa je $7n^2 \geq m^2 + 3$. Sada je

$$7 \geq \frac{m^2}{n^2} + \frac{3}{n^2} \geq \frac{m^2}{n^2} + \frac{2}{n^2} + \frac{1}{m^2 n^2} = \left(\frac{m}{n} + \frac{1}{mn}\right)^2 \implies \sqrt{7} \geq \frac{m}{n} + \frac{1}{mn}.$$

Štoviše, mora vrijediti stroga nejednakost jer je $\sqrt{7}$ iracionalan broj.

Zadatak 3.25. (*) Dokažite da ne postoje $a, b, c \in \mathbb{N}$ takvi da je $\frac{a^2+b^2+c^2}{3(ab+bc+ca)} \in \mathbb{Z}$.

Rješenje. Možemo pretpostaviti da je $(a, b, c) = 1$, inače sva tri broja podijelimo s njihovim najvećim zajedničkim djeliteljem. Pretpostavimo da je $a^2 + b^2 + c^2 = 3n(ab + bc + ca)$ za neki $n \in \mathbb{N}$. Tada je

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

pa postoji prost broj $p = 3k + 2$ koji dijeli $3n + 2$ neparno puta. Za taj broj p onda mora vrijediti i

$$p \mid a + b + c, ab + bc + ca \implies p \mid ab + (a + b)(-a - b) \implies p \mid a^2 + ab + b^2.$$

Ako je $p = 2$, lako vidimo da mora biti $2 \mid a, b \implies 2 \mid c$. To je kontradikcija jer smo pretpostavili $(a, b, c) = 1$.

Ako je $p > 2$, tada vrijedi $p \mid 4(a^2 + ab + b^2) = (2a + b)^2 + 3b^2$. Međutim, $\left(\frac{-3}{p}\right) = -1$ pa imamo $p \mid 2a + b, b \implies p \mid a, b \implies p \mid c$ što opet daje kontradikciju zbog $(a, b, c) = 1$.

Zadatak 3.26. (*) Odredite sve proste brojeve p takve da je $p! + p$ potpun kvadrat.

Rješenje. Brojevi $p = 2, 3$ su rješenje jer je $2! + 2 = 2^2, 3! + 3 = 3^2$, a $p = 5$ nije rješenje jer je $5! + 5 = 125$. Neka je sada $p \geq 7$ i pretpostavimo da je $p! + p = x^2$.

Neka je $2 \leq q < p$ prost broj. Kako je $p! + p = x^2$, mora vrijediti $x^2 \equiv p \pmod q$ pa je $\left(\frac{p}{q}\right) = 1$. Budući da je $p \geq 7$, imamo da je $x^2 = p! + p \equiv p \pmod 8$ iz čega slijedi da je $p \equiv 1 \pmod 8$. Stoga je $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. Također je i $\left(\frac{2}{p}\right) = 1$.

Iz ovoga možemo zaključiti da je $\left(\frac{n}{p}\right) = 1$ za sve $1 \leq n < p$ zbog multiplikativnosti Legendreovih simbola. To je kontradikcija jer postoji točno $\frac{p-1}{2}$ kvadratnih ostataka i neostataka mod p.

Zadatak 3.27. (*) Neka je $k \in \mathbb{N}$ kvadratni ostatak za sve dovoljno velike proste brojeve. Dokažite da je k potpun kvadrat.

Rješenje. Neka je $k = x^2 \cdot p_1 \dots p_n$, gdje je $p_1 < \dots < p_n$. Tada je i $p_1 \dots p_n$ kvadratni ostatak za sve dovoljno velike proste brojeve p, odnosno

$$\left(\frac{p_1 \cdots p_n}{p}\right) = \left(\frac{p_1}{p}\right) \dots \left(\frac{p_n}{p}\right) = 1.$$

Lako vidimo da nije moguć slučaj $p_1 \dots p_n = 2$ pa je $p_n > 2$. Sada ćemo naći prost broj p sa sljedećim svojstvima:

$$p \equiv 1 \pmod 8,\ \left(\frac{p}{p_1}\right) = 1,\ \dots,\ \left(\frac{p}{p_{n-1}}\right) = 1,\ \left(\frac{p}{p_n}\right) = -1.$$

Po CRT-u postoji beskonačno mnogo rješenja $n \equiv a \pmod{8p_1 \dots p_n}$ tog sustava kongruencija (ako je $p_1 = 2$, kongruenciju mod p_1 možemo zanemariti i gledamo mod $8p_2 \dots p_n$). Dirichletov teorem garantira da postoji beskonačno mnogo prostih brojeva $p \equiv a \pmod{8p_1 \dots p_n}$. Sada je

$$\left(\frac{p_1 \cdots p_n}{p}\right) = \left(\frac{p_1}{p}\right) \dots \left(\frac{p_n}{p}\right) = \left(\frac{p}{p_1}\right) \dots \left(\frac{p}{p_n}\right) = 1 \cdot \ldots \cdot 1 \cdot (-1) = -1$$

što je kontradikcija (pri okretanju Legendreovih simbola znak se ne mijenja jer je $p \equiv 1 \pmod 4$). Dakle, mora biti $k = x^2$.

Napomena: Kao što smo vidjeli na ovim zadacima, kvadratni ostaci imaju široku primjenu u teoriji brojeva. Osim njih, postoje i npr. kubni ostaci za proste brojeve $p = 3k + 1$. Ako je $p = 3k + 2$, tada taj pojam nema smisla jer jednadžba $x^3 \equiv a \pmod p$ ima rješenje za svaki $a \in \mathbb{Z}$ (Zašto?) pa je svaki a kubni ostatak.

Ako želimo definirati kubni simbol sa sličnim svojstvima kao Legendreov simbol (multiplikativnost, reciprocitet, ...), moramo izaći iz prstena $\mathbb{Z}$. Naime, nultočke polinoma $x^3 - 1$ su $1, \omega, \omega^2$, gdje je $\omega = e^{\frac{2\pi i}{3}}$. Stoga je prirodan prsten ovdje prsten Eisensteinovih cijelih brojeva $\mathbb{Z}[\omega]$.

Pomoću ovih kubnih simbola se može npr. dokazati da su prosti brojevi oblika $p = a^2 + 27b^2$ točno prosti brojevi $p = 3k + 1$ takvi da kongruencija $x^3 \equiv 2 \pmod p$ ima cjelobrojno rješenje. Više o kubnim ostacima može se pronaći u [1, 2, 3].

Bibliografija

[1] D. A. Cox: *Primes of the form $x^2 + ny^2$*, Wiley, New York (2013.) 3

Svečilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike, Osijek (2023,)

[2] K. Ireland, M. I. Rosen: *A Classical Introduction to Modern Number Theory*, Springer Science & Business Media (1990.) 3

[3] M. C. Relyea: *On Finite Fields and Higher Reciprocity*, `https://arxiv.org/abs/2407.03559` 3