Pellova jednadžba

13.3.2016.

Uvod

Pellova jednadžba je jednadžba oblika

$$x^2 - dy^2 = 1,$$

gdje je $d \in \mathbb{N}$ dani prirodni broj koji nije djeljiv ni s jednim kvadratom prirodnog broja većeg od 1. Pokazuje se da ta jednadžba ima beskonačno rješenja, koja zadovoljavaju jednu linearnu rekurziju. Kako u zadatcima iz teorije brojeva najčešće nailazimo na jednadžbe s konačno mnogo rješenja (često i bez rješenja), ova jednadžba je zato jedna zanimljiva iznimka.

Pellova jednadžba

Definicija 1. *Jednadžbu*

$$x^2 - dy^2 = 1,$$

*gdje su d, x, y prirodni brojevi, i d je kvadratno slobodan (tj., ne postoji kvadrat prirodnog broja veći od jedan koji je djelitelj od d) nazivamo **Pellovom jednadžbom**. Jednadžbu*

$$x^2 - dy^2 = N$$

*(uz iste uvjete na x, y, d, te N cijeli broj) nazivamo **pellovskom jednadžbom**.*

Napomena 1. *Ovdje ćemo se baviti samo Pellovom jednadžbom i pellovskom za $N = -1$. Ostali primjeri gotovo da se ni ne pojavljuju na natjecanjima.*

Fokusirajmo se zasada samo na Pellovu jednadžbu. Na broj d postavlja se jedan čudan uvjet, stoga idemo pojasniti njegovu pozadinu. Kao prvo, pogledajmo Pellovu jednadžbu za $d = 1$:

$$x^2 - y^2 = 1 \iff x^2 = y^2 + 1.$$

Intuitivno je jasno da ne postoji baš mnogo uzastopnih brojeva koji su ujedno i kvadrati. Jedan način kako to pokazati je faktorizirati lijevu stranu. Također, postoji i jedna druga metoda, sa širom primjenom. Iako to nije tema ovog predavanja, pokazat ćemo ju. Ona se naziva *smještanje među kvadrate.*

Pogledajmo broj $y^2 + 1$, za neki prirodan y. Ono što ćete se zasigurno složiti je da je on strogo veći od broja y^2. Također, on je i strogo manji od broja $y^2 + 2y + 1$. Dakle, imamo

$$y^2 < y^2 + 1 < y^2 + 2y + 1 = (y + 1)^2.$$

Tu dolazimo do interesantne kontradikcije: želimo da je broj $y^2 + 1$ kvadrat prirodnog broja, no on se nalazi između dva uzastopna kvadrata: y^2 i $(y+1)^2$. Kažemo da smo taj izraz smjestili između dva uzastopna kvadrata, odakle i ime metodi. Dakle, za prirodan y, izraz $y^2 + 1$ ne može biti potpun kvadrat.

U primjeru koji smo zajedno riješili, broj smo smjestili između dva kvadrata i pokazali da on ne može biti potpun kvadrat. Slično, možemo broj smjestiti između dva kuba (ili neke više potencije) i pokazati da taj broj ne može biti potpun kub (ili neka viša potencija).

Zadatak 1.
Pokažite da jednadžba $x^2 = y^2 + 1$ ima samo dva rješenja u cijelim brojevima: $x = \pm 1, y = 0$.

Zadatak 2.
Pokažite da broj $x^2 + x + 1$ nije potpun kvadrat ni za jedan prirodan broj x.

Zadatak 3.
Pokažite da brojevi $x^2 + x + 1$ i $x + 1$ ne mogu istodobno biti potpuni kubovi prirodnih brojeva, ni za koji prirodan x.

Dakle, složili smo se da Pellovu jednadžbu za $d = 1$ nije zanimljivo gledati. Također, ako je d potpun kvadrat ($d = k^2$), tada bismo imali

$$1 = x^2 - dy^2 = x^2 - (ky)^2,$$

pa kao i prije, ne bismo imali rješenja.

Konačno, pretpostavimo da znamo riješiti Pellovu jednadžbu za sve kvadratno slobodne d. Neka je d_1 broj koji nije kvadratno slobodan. Tada postoje $k, n \in \mathbb{N}$ takvi da je $d_1 = kn^2$ i k je kvadratno slobodan (kad k ne bi bio kvadratno slobodan, njegov kvadratni djelitelj mogli bismo "strpati" u n^2). Tada bismo imali jednadžbu

$$1 = x^2 - dy^2 = x^2 - k(ny)^2,$$

za koju znamo sva rješenja.

Sada pokažimo najvažniji rezultat, koji nećemo dokazivati:

Teorem 1. *Neka je d kvadratno slobodan prirodan broj. Pellova jednadžba (za taj d) tada ima beskonačno rješenja. Nadalje, neka je (x_1, y_1) njeno najmanje rješenje. Tada su sva ostala rješenja dana s*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{1}$$

Napomena 2.
- *Netko bi se mogao zapitati po kojem kriteriju je neko rješenje najmanje. Kako usporediti dva rješenja (x, y) i (x', y')? Ideje koje padaju na pamet su primjerice provjeriti je li $x < x$ ili $y < y'$ ili $x + y < x' + y'$ ili udaljenost od ishodišta u ravnini: $\sqrt{x^2 + y^2} < \sqrt{x'^2 + y'^2}$. Lako je pokazati da su svi ti kriteriji ekvivalentni. Primjerice: Ako je $x < x'$, imamo*

  $$x^2 - dy^2 = 1 \text{ i } x'^2 - dy'^2 = 1 \implies dy^2 + 1 = x^2 < x'^2 = dy'^2 + 1 \implies y < y'.$$

  Lako je pokazati i drugi smjer. Pozivamo čitatelja da se uvjeri i u ekvivalentnost svih kriterija.

- *Jednadžba 1 možda nije jasna na prvi pogled, pa ju pojasnimo. Ona se zasniva na tome da se za sve prirodne brojeve a, b, n i d broj $(a + b\sqrt{d})^n$ opet može prikazati u obliku $A + B\sqrt{d}$. Primjerice*

  $$(2 + \sqrt{3})^3 = (2 + \sqrt{3})^2(2 + \sqrt{3}) = (4 + 2\sqrt{3} + 3)(2 + \sqrt{3})$$
  $$= (7 + 4\sqrt{3})(2 + \sqrt{3}) = (14 + 7\sqrt{3} + 8\sqrt{3} + 12) = 26 + 15\sqrt{3}.$$

  Koliko god je taj način zadavanja rješenja lako pamtljiv, ipak se čini da se s njime ne može mnogo toga dalje napraviti (ukoliko nam je u zadatku rečeno da trebamo nešto dokazati za skup rješenja). Uskoro ćemo dati alternativne načine zadavanja rješenja.

- *Prema teoremu, za nalaženje svih rješenja trebamo samo naći najmanje rješenje, a dalje imamo formulu. U nekim slučajevima, riječ "samo" ima smisla. Primjerice, najmanje rješenje jednadžbe $x^2 - 2y^2 = 1$ je $(x, y) = (3, 2)$. No, za broj $d = 61$, najmanje rješenje je*

  $$(x_1, y_1) = (1766319049, 226153980).$$

  Srećom, u našim primjerima, i općenito u primjerima na natjecanjima, najmanje rješenje bit će skoro uvijek par sastavljen od jednoznamenkastih brojeva.

Sljedećom propozicijom dat ćemo korisniju formulu za rješenja.

Propozicija 1. *Rješenja (x_n, y_n) Pellove jednadžbe zadovoljavaju sljedeću rekurziju:*

$$x_{n+1} = x_1x_n + dy_1y_n, \; y_{n+1} = y_1x_n + x_1y_n.$$

Dokaz. Koristimo relaciju iz teorema:

$$(x_{n+1} + y_{n+1}\sqrt{d}) = (x_1 + y_1\sqrt{d})^{n+1} = (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d})^n = (x_nx_1 + dy_ny_1) + (y_nx_1 + x_ny_1)\sqrt{d}.$$

Dakle, kad nađemo najmanje rješenje (x_1, y_1), ono što ostaje je sustav linearnih rekurzija za nizove x_n i y_n. U toj rekurziji isprepliću se formule za niz x_n i niz y_n. Te formule možemo "rasplesti".

Propozicija 2. *Rješenja (x_n, y_n) Pellove jednadžbe zadovoljavaju sljedeću rekurziju:*

$$x_{n+2} = 2x_1x_{n+1} - x_n, \; y_{n+2} = 2x_1y_{n+1} - y_n.$$

Dokaz. Koristimo rekurzije iz prošlog teorema. Ideja je da iz jedne jednadžbe izrazimo jednu varijablu i uvrstimo je u drugu jednadžbu. Poznata metoda u rješavanju sustava linearnih jednadžbi, ovdje je samo u novom ruhu:

$$y_{n+1} = y_nx_1 + x_ny_1 \implies x_n = \frac{1}{y_1}(y_{n+1} - y_nx_1).$$

Dobiveni izraz vrijedi za sve prirodne brojeve n. Zato imamo i

$$x_{n+1} = \frac{1}{y_1}(y_{n+2} - y_{n+1}x_1).$$

To uvrštavamo u jednadžbu koju još nismo iskoristili (pomnožit ćemo je i s y_1, da nam bude lakše):

$$y_1x_{n+1} = y_1(x_1x_n + dy_1y_n) \implies y_{n+2} - y_{n+1}x_1 = x_1(y_{n+1} - y_nx_1) + dy_1y_n$$

$$\implies y_{n+2} = (x_1 + x_1)y_{n+1} + (-x_1^2 + dy_1^2)y_n = 2x_1y_{n+1} - y_n.$$

Slično dobijemo i formulu za x_n.

Riješimo sada jedan zadatak:

Zadatak 4.
Neka prirodni brojevi x, y zadovoljavaju $x^2 - 2y^2 = 1$. Dokažite $6|xy$.

Rješenje.
Za ovaj zadatak nije nužno poznavanje svojstava Pellove jednadžbe, možemo direktno gledati samo neke ostatke (pozivamo čitatelja da izvede i takav dokaz). Ali, mi ćemo za potrebe ovog predavanja iskoristiti dokaz preko izvedenih svojstava. Lako provjerimo da je najmanje rješenje jednadžbe $(x_1, y_1) = (3, 2)$. Koristeći formule iz propozicija, imamo da je sljedeće rješenje $(x_2, y_2) = (17, 12)$, te rekurziju $x_{n+2} = 6x_{n+1} - x_n, y_{n+2} = 6y_{n+1} - y_n \implies x_{n+2}y_{n+2} \equiv x_ny_n \ (mod\, 6)$. Kako za prva dva rješenja vrijedi da im je umnožak djeljiv sa 6, trivijalnom indukcijom vrijedi i za sve ostale n.

Ako se dogodi slučaj da se ne možete sjetiti ide li u Teoremu 1 u formuli znak plus ili minus, imamo rješenje za to:

Propozicija 3. *Neka je (x_1, y_1) najmanje rješenje Pellove jednadžbe. Tada su sva ostala rješenja dana s*

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n. \tag{2}$$

Dokaz. Uzmemo recipročni izraz za $x_n + y_n\sqrt{d}$ i racionalizirajmo ga:

$$\frac{1}{x_n + y_n\sqrt{d}} = \frac{1}{x_n + y_n\sqrt{d}}\frac{x_n - y_n\sqrt{d}}{x_n - y_n\sqrt{d}} = \frac{x_n - y_n\sqrt{d}}{x_n^2 - dy_n^2} = x_n - y_n\sqrt{d}.$$

Slično napravimo i za $(x_1 + y_1\sqrt{d})^n$. Dobijemo:

$$x_n - y_n\sqrt{d} = \frac{1}{x_n + y_n\sqrt{d}} = \frac{1}{(x_1 + y_1\sqrt{d})^n} = (x_1 - y_1\sqrt{d})^n.$$

Zbog zadnjeg rezultata, možemo na još jedan način zapisati rješenje:

$$x_n = \frac{1}{2}((x_n + \sqrt{d}y_n) + (x_n - \sqrt{d}y_n)) = \frac{1}{2}((x_1 + \sqrt{d}y_1)^n + (x_1 - \sqrt{d}y_1)^n),$$

$$y_n = \frac{1}{2\sqrt{d}}((x_n + \sqrt{d}y_n) - (x_n - \sqrt{d}y_n)) = \frac{1}{2\sqrt{d}}((x_1 + \sqrt{d}y_1)^n - (x_1 - \sqrt{d}y_1)^n).$$

Iako su brojevi $\alpha_{1,2} = (x_1 \pm y_1\sqrt{d})$ koji se pojavljuju u formulama realni i nimalo cijeli, njihov zbroj $(2x_1)$ i produkt (1) jesu cijeli brojevi. Zato ipak s njima možemo raditi neke stvari kao i s cijelim brojevima.

Zadatak 5.
Dokažite da rješenja Pellove jednadžbe (x_n, y_n) i (x_m, y_m) zadovoljavaju $x_n|x_m$, kad god su m i n neparni, te $n|m$.

Rješenje.
Na trenutak zamislimo da su brojevi $\alpha_{1,2}$ prirodni i riješimo ovaj zadatak s tom pretpostavkom. Neka $n|m$. Tada trebamo dokazati

$$x_n|x_m \iff \frac{1}{2}(\alpha_1^n + \alpha_2^n)\Big|\frac{1}{2}(\alpha_1^m + \alpha_2^m) \iff \alpha_1^n + \alpha_2^n\Big|\alpha_1^m + \alpha_2^m.$$

$$(A_1 := \alpha_1^n, A_2 := \alpha_2^n, k = \frac{m}{n}) \text{ (odavde je } k \text{ neparan)}$$

$$\iff A_1 + A_2|A_1^k + A_2^k = (A_1 + A_2)(A_1^{k-1} + A_1^{k-2}A_2 + \cdots A_1^1 A_2^{k-2} + A_2^{k-1}).$$

U slučaju da su $\alpha_{1,2}$ prirodni, zadatak bi bio gotov. No, ovako trebamo provjeriti svaki korak. Svi koraci koje smo ispisali vrijede neovisno o tome jesu li brojevi cijeli ili realni, samo je zadnji zaključak možda drukčiji. No, budući da je umnožak brojeva $A_1A_2 = (\alpha_1\alpha_2)^n$ prirodan i budući da je suma svake dvije potencije $A_1^l + A_2^l = \alpha_1^{nl} + \alpha_2^{nl} = 2x_{nl}$ prirodna, tada su i svi faktori u izrazu

$$A_1 + A_2|A_1^k + A_2^k = (A_1 + A_2)(A_1^{k-1} + A_1^{k-2}A_2 + \cdots A_1^1 A_2^{k-2} + A_2^{k-1})$$

prirodni. Izraze u ovoj velikoj zagradi uparujemo: uz npr $l \leqslant k-l-1$ imamo $A_1^l A_2^{k-l-1} + A_1^{k-l-1}A_2^l = (A_1A_2)^l(A_1^{k-2l-1} + A_2^{k-2l} + 1)$. Dakle, svi brojevi u gornjem raspisu su prirodni, i sav račun je valjan.

Za kraj, pogledajmo poseban slučaj pellovske jednadžbe, za $N = -1$. Za razliku od Pellove jednadžbe, iako naoko nismo mnogo toga promijenili, ova jednadžba ne mora uvijek imati rješenje.

Zadatak 6.
Neka je n prirodan broj takav da je $n + 1$ djeljivo s 4. Dokažite da jednadžba $x^2 - ny^2 = -1$ nema rješenja.

Rješenje.
U jednadžbi $x^2 + 1 = ny^2$ lijeva strana ne smije imati prosti faktor oblika $4k + 3$ (jedna od posljedica Fermatovog teorema, ako čitatelj ne zna za to, preporučamo istoimeno online predavanje), dok desna strana očito ima takav djelitelj. Kontradikcija.

Našli smo veliku klasu jednadžbi kada ova pellovska jednadžba nema rješenje. Inače, bez nekog velikog dodatnog znanja nema jednostavnog kriterija za d kada jednadžba ima rješenja. Nudimo utjehu sa sljedeća dva rezultata:

Teorem 2. *Neka je d kvadratno slobodan prirodan broj. Pretpostavimo da postoji rješenje pellovske jednadžbe. Tada ih postoji beskonačno. Nadalje, neka je (x_1, y_1) njeno najmanje rješenje. Tada su u nizovima (x_n, y_n) zadanima rekurzijom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{3}$$

na neparnim mjestima dana sva rješenja pellovske jednadžbe $x^2 - dy^2 = -1$, a na parnim mjestima sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$.

Korolar 1. *Neka je (x', y') neko rješenje Pellove jednadžbe $x^2 - dy^2 = 1$. Ako ne postoji rješenje pellovske jednadžbe $x^2 - dy^2 = -1$ koje je manje od (x', y'), tada ta pellovska jednadžba uopće nema rješenja.*

Zadatak 7.
Koristeći trik kao u jednoj od propozicija u ovom predavanju, "raspletite rekurziju" iz teorema o postojanju rješenja pellovske jednadžbe i nađite rekurziju samo za ta rješenja, bez rješenja odgovarajuće Pellove jednadžbe.

Rješenje.

$$x_{n+2} = (x_1^2 + dy_1^2)x_n + (2dx_1y_1)y_n, \ \ y_{n+2} = (2x_1y_1)x_n + (x_1^2 + dy_1^2)y_n.$$

Primjeri

Zadatak 8.
Dokažite da jednadžba $a(a-1) = 2b(b-1)$ ima beskonačno rješenja u prirodnim brojevima. Opišite ih.

Rješenje.
Pomnožimo li jednadžbu s 4, dodamo sa svake strane 2, dobit ćemo kvadrate binoma:

$$(2a-1)^2 + 1 = 2(2b-1)^2 \iff x^2 - 2y^2 = -1, \text{ gdje je } x = 2a-1, \ y = 2b-1.$$

Najmanje rješenje je $(x,y) = (1,1)$. Znamo da su sva rješenja dana (prema zadatku 7) s (gledamo samo neparne članove)

$$x_{n+2} = 3x_n + 4y_n, \ y_{n+2} = 2x_n + 3y_n.$$

Trivijalnom indukcijom zaključujemo da su svi članovi s neparnim indeksom u nizu neparni. Zato su sva rješenja početne zadaće dana s

$$\left(\frac{x_k+1}{2}, \frac{y_k+1}{2}\right), \text{ gdje je } k \text{ neparan broj.}$$

Zadatak 9.
Dokažite da jednadžba $x^2 + y^2 - 4xy + 2 = 0$ ima beskonačno rješenja u prirodnim brojevima. Opišite ih.

Rješenje.
Početna jednadžba ekvivalentna je s

$$(x+y)^2 - 3(x-y)^2 = 4.$$

Lijeva strana jednadžbe može davati ostatke $0, 1, 2$ pri dijeljenju s 4. Davat će ostatak nula samo ako su oba broja koja kvadriramo parna. Dakle, $x + y = 2a, x - y = 2b \iff x = a + b, y = a - b$. Kad podijelimo s 4 dobijemo

$$a^2 - 3b^2 = 1.$$

Znamo kako glasi rekurzija za sva rješenja ove Pellove jednadžbe. Preko relacija $x = a + b, y = a - b$ zadali smo sva moguća rješenja početne jednadžbe.

Zadatak 10.
Dokažite da sustav jednadžbi

$$\begin{cases} x^2 - 2y^2 = 1 \\ x^2 - 3z^2 = 1 \\ x^2 - 5t^2 = 1 \end{cases}$$

nema rješenja.

Rješenje.
Ovo je jedan mali uljez među zadatcima. Sada kada znate rješavati Pellovu jednadžbu, ponekad trebate uočiti da ne morate sve zadatke riješiti koristeći stečeno znanje.
Oduzimanjem prvih dviju relacija dobivamo

$$2y^2 = 3z^3 \iff \frac{y}{z} = \pm\sqrt{\frac{3}{2}}.$$

Dakle, dobili smo da je broj s desne strane racionalan broj, a dobro znamo da nije. Kontradikcija. Ovaj sustav nema rješenja.

Zadatci

Zadatak 11.
Dokažite da za svaki prirodan broj $\mathbb{N}$ postoje prirodni $a, b > 1$ takvi da je $a^2 + 1 = 2b^2$ i da je $n \mid a - b$.

Zadatak 12.
Za prirodan broj n, broj $2 + 2\sqrt{28n^2+1}$ je prirodan. Dokažite da je tada potpun kvadrat.

Zadatak 13.
Dokažite da brojevi $2a^2 + 1, 2b^2 + 1, 2a^2b^2 + 1$ ne mogu istodobno biti potpuni kvadrati, za prirodne a, b.

Zadatak 14.

(a) Dokažite da za prost broj p oblika $4k + 1$ pellovska jednadžba $x^2 - py^2 = -1$ uvijek ima rješenja.

(b) Dokažite da za prost broj p oblika $4k + 1$ pellovska jednadžba $x^2 - p^{2n-1}y^2 = -1$ uvijek ima rješenja, gdje je n dani prirodan broj.

Hint: (tekst hinta napisan je bijelom bojom nakon ovog komentara u zagradi; označite ga mišem i kopirajte u neki editor teksta kako biste ga pročitali)

Zadatak 15.
Nađite sva prirodna rješenja jednadžbe $5^n = 6m^2 + 1$.

Rješenja

Rješenje zadatka 10.

Kao u zadatku 11 izvedemo rekurziju za rješenje. Znamo da gledamo samo neparne članove u rekurziji iz Teorema 2, pa ćemo onda samo i ta rješenja gledati:

$$a_1 = 1, b_1 = 1, a_{k+1} = 3a_k + 4b_k,\ b_{k+1} = 2a_k + 3b_k.$$

Primijetimo da niz ima beskonačno članova, ali samo konačno mnogo ostataka modulo n. Sada primijenimo Dirichletov princip: postoje neki $k_0, N \in \mathbb{N}$ takvi da je $a_{k_0} \equiv a_{k_0+N}$, $a_{k_0+1} \equiv a_{k_0+N+1}$ te $b_{k_0} \equiv b_{k_0+N}$, $b_{k_0+1} \equiv b_{k_0+N+1}$ (sve kongruencije su modulo n). Zbog toga što smo htjeli namjestiti dva uzastopna člana u nizovima, zaključujemo da će i svi članovi nakon spomenutih mjesta davati jednake ostatke, dakle dobili smo da su od nekog mjesta nizovi (što se tiče ostataka) periodični s periodom N. Trebamo dokazati da to ne vrijedi samo počevši od nekog mjesta, nego za cijele nizove. To ćemo dokazati tako da dokažemo da je $a_{k-1} \equiv a_{k+N-1}$ i $b_{k-1} \equiv b_{k+N-1}$, koristeći gornje znanje. Ali to je zato što iz izraza za rekurziju imamo da je

$$a_{k-1} = 3a_k - 4b_k,\ b_{k-1} = -2a_k + 3b_k,$$

tj. ukoliko znamo ostatke dva uzastopna člana nizova, znamo i ostatke njihovih prethodnika na jedinstven način odrediti. Dakle, nizovi a_k i b_k su u potpunosti periodični modulo N. Zato to vrijedi i za niz $c_k := a_k - b_k$. Kako je $c_1 = 0$, znamo da je $c_{N+1} \equiv 0$, čime je zadatak gotov.

Rješenje zadatka 12. Ako je zadani izraz prirodan broj, nužno je da je dio pod korijenom potpun kvadrat. Neka je $a = \sqrt{28n^2+1} \implies a^2 - 28n^2 = 1$. Odavde je i $a^2 - 7(2n)^2 = 1$. Najmanje rješenje Pellove jednadžbe $x^2 - 7y^2 = 1$ je $(8, 3)$, a rekurzija

$$x_{k+1} = 8x_k + 21y_k,\ y_{k+1} = 3x_k + 8y_k.$$

Nas zanima samo slučaj kada je y_n paran. Lako je vidjeti da je to kada je k paran.

Vratimo se na tekst zadatka. Nama je cilj dokazati da je za sve k broj $2 + 2x_{2k}$ potpun kvadrat.

Sada koristimo Propoziciju 3. Neka je $\alpha_{1,2} = (8 \pm 3\sqrt{7})$. Imamo:

$$2 + 2x_{2k} = 2 + \alpha_1^{2k} + \alpha_2^{2k} = (\alpha_1^k + \alpha_2^k)^2 = (2x_k)^2,$$

što je i trebalo pokazati.

Rješenje zadatka 13. Postoji rješenje preko Pellove jednadžbe (preko Propozicije 3 i ograničavanja), no ovdje prikazujemo jedno elegantno rješenje koristeći smještanje među kvadrate.

Neka je BSO $a \geqslant b > 1$. Tada za broj

$$c := 4(2a^2+1)(2a^2b^2+1),$$

koji mora biti kvadrat, vrijedi

$$(4a^2b + b)^2 < c < (4a^2b + b + 1)^2,$$

kontradikcija.

Rješenje zadatka 14. Riješimo prvo $a)$ dio. Pretpostavimo da je (a, b) minimalno rješenje Pellove jednadžbe $x^2 - py^2 = 1$. Imamo

$$a^2 - pb^2 = 1 \implies (a-1)(a+1) = pb^2.$$

Gledajući početnu jednadžbu modulo 4, vidimo da b ne može biti neparan, jer bi tada bilo $a^2 \equiv 2 \pmod 4$. Dakle, b je paran, a a neparan. To znači da faktoriziranu jednadžbu možemo podijeliti s 4 (sve će ostati prirodno):

$$\frac{a+1}{2} \cdot \frac{a-1}{2} = p\left(\frac{b}{2}\right).$$

Faktori na lijevoj strani su uzastopni prirodni brojevi, dakle relativno su prosti. S desne strane imamo umnožak prostog broja i kvadrata, što ne ostavlja mnogo mogućnosti za faktorizaciju s dva relativno prosta faktora:

- *Prvi slučaj:* $\frac{a+1}{2} = \alpha^2$, $\frac{a-1}{2} = p\beta^2$. Tada je $\alpha^2 - p\beta^2 = 1$, što je kontradikcija s time da je (a, b) najmanje rješenje.
- *Prvi slučaj:* $\frac{a+1}{2} = p\alpha^2$, $\frac{a-1}{2} = \beta^2$. Tada je $\beta^2 - p\alpha^2 = -1$, čime smo dobili rješenje pellovske jednadžbe.

Riješimo sada b) dio. Opet gledamo Pellovu jednadžbu $x^2 - py^2 = 1$. Znamo da ona ima beskonačno rješenja, s rekurzivnom relacijom

$$x_{n+1} = x_1x_n + dy_1y_n,\ y_{n+1} = y_1x_n + x_1y_n.$$

Kao u zadatku 10 zaključimo da su ostatci modulo bilo koji $n \in \mathbb{N}$ periodični s nekim periodom M. Tada iz relacije za prethodne članove

$$x_{n-1} = x_1x_n - dy_1y_n,\ y_{n-1} = -y_1x_n + x_1y_n$$

možemo vidjeti da za rješenje (x_M, y_M) vrijedi (računi su modulo m)

$$x_M \equiv x_1^2 - dy_1^2 = 1,\ y_M \equiv -y_1x_1 + x_1y_1 = 0.$$

Dakle, za svaki m postoji rješenje (x_M, y_M) takvo da je y_M djeljiv s m. Uzmimo najmanje takvo rješenje za $m = p^{2n-1}$ iz zadatka. Sada napravimo postupak sličan kao u a) zadatku. To ćemo ostaviti čitatelju.

Rješenje zadatka 15.

Jasno je da je $(2, 2)$ jedno takvo rješenje. Gledajući mod 3 dobijemo da je n nužno paran: $n = 2k$. Uvedimo supstituciju $x = 5^l$, pa dobijemo Pellovu jednadžbu $x^2 - 6m^2 = 1$. Minimalno rješenje je $(5, 2)$ (koje odgovara već pronađenom rješenju), a ostala izrazimo preko propozicije 3:

$$x_k = \frac{1}{2}((5 + 2\sqrt{6})^k + (5 - 2\sqrt{6})^k).$$

Pogledajmo ostatak pri dijeljenju s 25. To dobijemo iz binomnih formula za $(5 \pm 2\sqrt{6})^k$, uz to da imamo na umu da članove oblika $\sqrt{6}$ na neparnu potenciju ne gledamo jer se pokrate, te da je 5^l djeljivo s 25 za $l \geqslant 2$. Tada dobijemo

$$k \equiv 1 \pmod 2 \implies 2x_k \equiv 10k(2\sqrt{6})^{k-1},$$
$$k \equiv 0 \pmod 2 \implies 2x_k \equiv 2(2\sqrt{6})^k,$$

odnosno da je $25 \mid 2x_l \iff k \equiv 5 \pmod{10}$. (Napomenimo da se do tog zaključka moglo doći i tako da smo gledali samo rekurziju za x_k modulo 25 i čekali da ostatci postanu periodični modulo 10). No, tada, prema zadatku 5 vrijedi

$$2 \cdot 5^2 \cdot 1901 = 2x_5 \mid 2x_k.$$

Dakle, ako je x_k djeljiv s 25, nije potencija broja 5, pa je $(5, 2)$ jedino rješenje početne jednadžbe.