

Poglavlje 1

Djeljivost

Teorem (o dijeljenju s ostatkom): *Neka je $a \in \mathbb{N}$ i $b \in \mathbb{Z}$. Tada postoje jedinstveni cijeli brojevi q, r takvi da je $b = qa + r$ i $0 \leq r < a$.*

Euklidov algoritam

Teorem (Euklidov algoritam): *Neka su $b, c \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema o dijeljenju s ostatkom dobiven niz jednakosti*

$$\begin{aligned}b &= cq_1 + r_1, & 0 < r_1 < c \\c &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\&\dots \\r_{j-2} &= r_{j-1}q_{j-1} + r_j, & 0 < r_j < r_{j-1} \\r_{j-1} &= r_jq_{j+1}.\end{aligned}$$

Tada je $(b, c) = r_j$ i vrijedi jednakost $(b, c) = bx_0 + cy_0$, pri čemu se koeficijenti $x_0, y_0 \in \mathbb{Z}$ mogu dobiti iz algoritma izražavanjem svakog broja r_i kao linearne kombinacije b i c .

Zadatak 1.1. Odredite sve parove cijelih brojeva (a, b) za koje vrijedi $732a + 288b = (a, b)$.

Rješenje. Uzastopno primjenjujemo Euklidov algoritam.

$$\begin{aligned}732 &= 288 \cdot 2 + 156 \\288 &= 156 \cdot 1 + 132 \\156 &= 132 \cdot 1 + 24 \\132 &= 24 \cdot 5 + 12 \\24 &= 12 \cdot 2 + 0\end{aligned}$$

Dakle, $(732, 288) = 12$. Još samo trebamo rekonstruirati koeficijente a, b .

$$\begin{aligned} 12 &= 132 - 24 \cdot 5 = 132 - (156 - 132 \cdot 1) \cdot 5 \\ &= 132 \cdot 6 - 156 \cdot 5 = (288 - 156 \cdot 1) \cdot 6 - 156 \cdot 5 \\ &= 288 \cdot 6 - 156 \cdot 11 = 288 \cdot 6 - (732 - 288 \cdot 2) \cdot 11 \\ &= 288 \cdot 28 - 732 \cdot 11 \end{aligned}$$

Dakle, našli smo jedan traženi par. Nadalje, ako vrijedi $732a + 288b = 732a' + 288b' = 12$, tada mora biti

$$732(a - a') = 288(b' - b) \iff 61(a - a') = 24(b' - b) \iff a - a' = 24k, b' - b = 61k.$$

Stoga su svi traženi parovi oblika $(a, b) = (24k - 11, 61k + 28)$ za neki $k \in \mathbb{Z}$.

Zadatak 1.2. Odredite sve $n \in \mathbb{N}$ za koje $n + 5 \mid n^3 + 100$.

Rješenje. Uzastopno primjenjujemo Euklidov algoritam.

$$\begin{aligned} n + 5 \mid n^3 + 100 &= (n + 5)n^2 - 5n^2 + 100 \iff \\ \iff n + 5 \mid 5n^2 - 100 &= 5(n + 5)n - 25n - 100 \iff \\ \iff n + 5 \mid 25n + 100 &= 25(n + 5) - 125 + 100 \iff \\ \iff n + 5 \mid 25 \end{aligned}$$

Dakle, jedino rješenje je $n = 20$.

Zadatak 1.3. Odredite sve $n \in \mathbb{N}$ za koje $2n^2 + 1 \mid n^3 - 8$.

Rješenje. Kako je $2n^2 + 1$ neparan, vrijedi $2n^2 + 1 \mid n^3 - 8 \iff 2n^2 + 1 \mid 2n^3 + 16$. Ovdje smo množili desnu stranu s 2 da bismo u koraku Euklidovog algoritma imali cijele brojeve. Sada imamo

$$\begin{aligned} 2n^2 + 1 \mid 2n^3 - 16 &= (2n^2 + 1)n - n - 16 \iff \\ 2n^2 + 1 \mid n + 16 \end{aligned}$$

Primijetimo da je lijeva strana kvadratni, a desna linearni polinom i da su obje strane pozitivne. Stoga lijeva strana raste brže od desne pa će za dovoljno velike n vrijediti $2n^2 + 1 > n + 16$ (preciznije, za $n \geq 4$) i djeljivost ne može vrijediti. Provjerom se utvrdi da $n = 1$ nije rješenje, a $n = 2, 3$ jesu.

Zadatak 1.4. Koliki ostatak daje broj $2025^{2026} + 2026$ pri dijeljenju s $2025^2 + 2026$?

Rješenje. Neka je $a := 2025$. Tada nas zanima koliki je ostatak $a^{2026} + a + 1 \bmod a^2 + a + 1$. Primijetimo da je $a^2 + a + 1 = \frac{a^3 - 1}{a - 1}$ pa imamo

$$a^{2026} + a + 1 = (a^3 - 1) \cdot (a^{2023} + a^{2020} + \dots + a^4 + a) + 2a + 1.$$

Kako je $2 \cdot 2025 + 1 = 2a + 1 < a^2 + a + 1$, dobivamo da broj $2025^{2026} + 2026$ daje ostatak 4051 pri dijeljenju s $2025^2 + 2026$.

Prosti brojevi

Teorem (Osnovni teorem aritmetike): *Svaki prirodni broj n se može jedinstveno faktorizirati na proste faktore do na njihov poredak. Drugim riječima, postoje jedinstveni prosti brojevi $p_1 < \dots < p_k$ i eksponenti $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ takvi da vrijedi $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.*

Teorem (Euklid): *Prostih brojeva ima beskonačno mnogo.*

Proste brojeve oblika $2^p - 1$, gdje je p prost, zovemo Mersenneovi prosti brojevi, a proste brojeve oblika $2^{2^n} + 1$ zovemo Fermatovi prosti brojevi. Otvoren je problem postoji li beskonačno Mersenneovih i Fermatovih prostih brojeva.

Teorem: *Neka je $n \in \mathbb{N}$ i p prost broj. Broj $k \in \mathbb{N}$ takav da $p^k \parallel n!$ (tj. $p^k \mid n!$, $p^{k+1} \nmid n!$) se označava s $v_p(n!)$. Ako s $\lfloor x \rfloor$ označimo najveći cijeli broj manji ili jednak x , tada vrijedi*

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Ova suma je konačna jer je $p^m > n$ za sve dovoljno velike brojeve m .

Zadatak 1.5. Odredite sve proste brojeve p takve da su brojevi $p+2, p+4$ također prosti.

Rješenje. Bar jedan od brojeva $p, p+2, p+4$ je djeljiv s 3. Dakle, jedan od njih mora biti jednak 3. Sad se lako vidi da je jedino rješenje $p = 3$.

Zadatak 1.6. Odredite sve proste brojeve p za koje postoje $m, n \in \mathbb{N}$ takvi da je $p^{2n+1} = 2^m + 1$.

Rješenje. Vrijedi

$$p^{2n+1} - 1 = (p - 1)(p^{2n} + p^{2n-1} + \dots + p + 1).$$

Izraz $p^{2n} + \dots + 1$ je neparan i veći od 1. Stoga ne može biti potencija broja 2 pa ne postoji takav p .

Zadatak 1.7. Odredite sve proste brojeve p takve da je $21p + 1$ potpun kvadrat.

Rješenje. Diofantsku jednadžbu $21p + 1 = x^2$ zapišimo u obliku $21p = (x - 1)(x + 1)$. Sada imamo 8 slučajeva.

- $x - 1 = 1, x + 1 = 21p \implies x = 2$, nema rješenja
- $x - 1 = 3, x + 1 = 7p \implies x = 4$, nema rješenja
- $x - 1 = 7, x + 1 = 3p \implies x = 8, p = 3$
- $x - 1 = 21, x + 1 = p \implies x = 22, p = 23$
- $x - 1 = p, x + 1 = 21 \implies x = 20, p = 19$

- $x - 1 = 3p, x + 1 = 7 \implies x = 6$, nema rješenja
- $x - 1 = 7p, x + 1 = 3 \implies x = 2$, nema rješenja
- $x - 1 = 21p, x + 1 = 1 \implies x = 0$, nema rješenja

Dakle, sva rješenja su $p = 3, 19, 23$.

Zadatak 1.8. Odredite sve $n \in \mathbb{N}$ takve da su $2^n - 1, 2^n + 1$ prosti brojevi.

Prvo rješenje. Broj $2^n - 1$ može biti prost samo ako je n prost, a broj $2^n + 1$ može biti prost samo ako je n potencija broja 2. Stoga je jedini kandidat $n = 2$ i lako se vidi da je to jedino rješenje. $\square$

Drugo rješenje. Ako $2 \mid n$, tada $3 \mid 2^n - 1$. Ako $2 \nmid n$, tada $3 \mid 2^n + 1$. Dakle, jedan od brojeva $2^n \pm 1$ je djeljiv s 3 pa, ako je prost, mora biti jednak 3. Stoga su jedini kandidati $n = 1, 2$ i lako se vidi da je $n = 2$ jedino rješenje. $\square$

Zadatak 1.9. Neka je $n \geq 3$ prirodan broj i neka su p, q prosti brojevi takvi da $p \mid n!, q \mid n! - 1$. Dokažite da je $p < q$.

Rješenje. Iz $p \mid n!$ slijedi da je $p \leq n$. Kad bi bilo $q \leq p$, tada bi vrijedilo $q \mid n!$. Međutim, znamo da je $(n!, n! - 1) = 1$ što nam daje kontradikciju. Dakle, mora biti $p < q$.

Zadatak 1.10. S koliko nula završavaju brojevi $100!$ i $\binom{100}{20}$?

Rješenje. Prvo riješimo broj $100!$. Treba izračunati brojeve $v_2(100!)$ i $v_5(100!)$. Broj nula će tada biti jednak $\min(v_2(100!), v_5(100!))$. Međutim, iz formule je jasno da će vrijediti $v_2(100!) \geq v_5(100!)$ jer je $\lfloor \frac{100}{2^k} \rfloor \geq \lfloor \frac{100}{5^k} \rfloor$ za svaki $k \in \mathbb{N}$. Zato je broj nula s kojima završava $100!$ jednak

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 24.$$

Sada ćemo riješiti broj $n := \binom{100}{20} = \frac{100!}{20!80!}$. Nije teško izračunati da je

$$v_2(n) = v_2(100!) - v_2(20!) - v_2(80!) = 97 - 18 - 78 = 1,$$

$$v_5(n) = v_5(100!) - v_5(20!) - v_5(80!) = 24 - 4 - 19 = 1.$$

Zato broj $\binom{100}{20}$ završava s jednom nulom.

Zadatak 1.11. (*) Dokažite da postoji 1000 uzastopnih prirodnih brojeva među kojima je točno 10 prostih brojeva.

Rješenje. Među prvih 1000 brojeva je sigurno više od 10 prostih brojeva, a postoji i 1000 uzastopnih složenih brojeva (npr. $1001! + 2, 1001! + 3, \dots, 1001! + 1001$). Definirajmo

$$s(n) = \text{broj prostih brojeva u skupu } \{n, n + 1, \dots, n + 999\}.$$

Dakle, $s(1) > 10$, $s(1001! + 2) = 0$. Također,

$$s(n+1) - s(n) = \begin{cases} -1 & : n \text{ prost, } n+1000 \text{ složen,} \\ 1 & : n \text{ složen, } n+1000 \text{ prost,} \\ 0 & : \text{inače.} \end{cases}$$

Stoga je $|s(n+1) - s(n)| \leq 1$ za sve $n \in \mathbb{N}$ pa sigurno postoji $n \in \mathbb{N}$ za koji je $s(n) = 10$.

Zadatak 1.12 (Hrvatska matematička olimpijada za djevojke 2025., 1. dan *). Ako za proste brojeve p, q i $n \in \mathbb{N}$ vrijedi

$$p + q^2 = (n^2 + 1)p^2 + q,$$

dokažite da je $q = p^2 - p + 1$.

Rješenje. Ako je $p = q$, tada mora biti $n = 0$ što nije prirodan broj. Pretpostavimo sada da je $p \neq q$. Jednadžbu možemo zapisati kao

$$q(q-1) = ((n^2 + 1)p - 1)p.$$

Slijedi da $p \mid q(q-1)$. Kako $p \neq q$, imamo $p \mid q-1$, odnosno postoji $k \in \mathbb{N}$ takav da je $q = kp + 1$. Sada jednadžba postaje

$$k(kp + 1) = (n^2 + 1)p - 1 \iff k + 1 = (n^2 + 1 - k^2)p.$$

Stoga postoji $a \in \mathbb{N}$ takav da je $k = ap - 1$ i jednadžba postaje

$$n^2 = (ap - 1)^2 + a - 1.$$

Dakle, izraz $(ap - 1)^2 + a - 1$ mora biti potpun kvadrat. Znamo da vrijedi $(ap - 1)^2 + a - 1 \geq (ap - 1)^2$, a također je $(ap - 1)^2 + a - 1 = a^2p^2 - 2ap - a < (ap)^2$. Zaključujemo da mora biti $(ap - 1)^2 + a - 1 = (ap - 1)^2$ i $a = 1$. Iz toga slijedi da je $k = p - 1$ i $q = p^2 - p + 1$.

Napomena: Bunyakovskyjeva slutnja kaže sljedeće: ako je $P \in \mathbb{Z}[x]$ ireducibilan polinom kojemu je vodeći koeficijent pozitivan i $(P(1), P(2), P(3), \dots) = 1$, tada postoji beskonačno mnogo prostih brojeva p prikazivih u obliku $p = P(x)$ za neki $x \in \mathbb{N}$. Slutnja je dokazana samo za polinome stupnja 1 (Dirichletov teorem). Tako je npr. otvoren problem postoji li beskonačno mnogo prostih brojeva oblika $x^2 + 1$.

Teorem (Dirichlet *): Neka su a, b relativno prosti prirodni brojevi. Tada u aritmetičkom nizu $an + b$, $n \in \mathbb{N}$ postoji beskonačno mnogo prostih brojeva.

Teorem (Bertrandov postulat *): Za svaki prirodan broj $n \geq 2$ postoji prost broj $n < p < 2n$.

Najveći zajednički djelitelj

Zadatak 1.13. Neka su $a, b, c \in \mathbb{N}$ takvi da su brojevi ab, ac, bc potpuni kubovi. Dokažite su i a, b, c potpuni kubovi. Vrijedi li ista tvrdnja za kvadrate?

Rješenje. Broj $(abc)^2 = ab \cdot ac \cdot bc$ je potpun kub jer je umnožak potpunih kubova. Stoga je $(abc)^2$ šesta potencija nekog prirodnog broja pa je abc potpun kub. Sada su i $a = \frac{abc}{bc}, b = \frac{abc}{ac}, c = \frac{abc}{ab}$ potpuni kubovi jer su kvocijenti potpunih kubova.

Za kvadrate ovakva tvrdnja ne vrijedi. Protuprimjer je $a = b = c = 2$.

Zadatak 1.14. Ako su a, b relativno prosti prirodni brojevi, odredite sve moguće vrijednosti broja $(a + b, a - b)$.

Rješenje. Vrijedi $(a + b, a - b) = (a + b, 2a) = (a + b, 2)$. Stoga je $(a + b, a - b) = 1$ ako su a, b različite parnosti i $(a + b, a - b) = 2$ ako su iste parnosti.

Zadatak 1.15. Ako su $a, b \in \mathbb{N}$ takvi da je $(a, b) = 10$, odredite sve moguće vrijednosti (a^3, b^4) .

Rješenje. Neka je $a = 10x, b = 10y$. Tada je $(x, y) = 1$ i

$$(a^3, b^4) = (10^3 x^3, 10^4 y^4) = 10^3 \cdot (x^3, 10y^4) = 10^3 \cdot (x^3, 10).$$

Stoga je $(a^3, b^4) \in \{10^3, 2 \cdot 10^3, 5 \cdot 10^3, 10^4\}$, ovisno o tome je li x djeljiv s 2 i 5.

Zadatak 1.16. Ako za prirodne brojeve a, b, c, d vrijedi $ab = cd$, dokažite da postoje $x, y, z, w \in \mathbb{N}$ takvi da je $a = xy, b = zw, c = xz, d = yw$.

Rješenje. Neka je $x = (a, c)$ i $w = (b, d)$. Tada je

$$\frac{a}{x} \cdot \frac{b}{w} = \frac{c}{x} \cdot \frac{d}{w}.$$

Zbog $(\frac{a}{x}, \frac{c}{x}) = 1$ mora vrijediti $\frac{a}{x} \mid \frac{d}{w}$. Analogno se dobiju djeljivosti $\frac{b}{w} \mid \frac{c}{x}, \frac{c}{x} \mid \frac{b}{w}, \frac{d}{w} \mid \frac{a}{x}$. Kako su svi ovi brojevi pozitivni, zaključujemo da je $y := \frac{a}{x} = \frac{d}{w}$ i $z := \frac{b}{w} = \frac{c}{x}$ pa smo dobili tražene brojeve x, y, z, w .

Zadatak 1.17 (Hrvatska juniorska matematička olimpijada 2025., 2. dan). Odredite sve $a, b \in \mathbb{N}$ za koje $3ab + a \mid 3a^2 + b$.

Rješenje. Vrijedi $a(3b + 1) \mid 3a^2 + b \implies a \mid 3a^2 + b \implies a \mid b$. Dakle, postoji $k \in \mathbb{N}$ takav da je $b = ka$ i jednadžba postaje

$$3ak + 1 \mid 3a + k.$$

Primijetimo da je lijeva strana veća od desne jer je

$$3ak + 1 - 3a - k = (3a - 1)(k - 1) \geq 0$$

te da su obje strane pozitivne. Stoga mora biti $3ak + 1 = 3a + k$ što je moguće samo za $k = 1$, tj. $a = b$. Lako se vidi da je $a = b$ zaista rješenje.

Zadatak 1.18 (Školsko natjecanje 2023., 4. razred, A varijanta). Odredite sve uređene trojke (x, y, p) , gdje je p prost, a x i y prirodni brojevi za koje vrijedi

$$p^x - 1 = y^3.$$

Rješenje. Zapišimo jednadžbu u obliku

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

Primijetimo da vrijedi $(y + 1, y^2 - y + 1) = (y + 1, 1 + 1 + 1) = (y + 1, 3) \mid 3$. Sada imamo 2 slučaja.

- $3 \mid y + 1$. Tada je $p = 3$ i brojevi $y + 1, y^2 - y + 1$ su oba potencije broja 3, s tim da je barem jedan od njih jednak 3. Nije teško dobiti da onda mora biti $y = 2$ i $x = 2$.
- $3 \nmid y + 1$. Tada su brojevi $y + 1, y^2 - y + 1$ oba potencije broja p i relativno prosti. Zato je jedan od njih jednak 1. Nije teško dobiti da onda mora biti $y = 1, p = 2, x = 1$.

Dakle, sva rješenja su $(x, y, p) = (1, 1, 2), (2, 2, 3)$.

Zadatak 1.19. Odredite sve $x, y, z \in \mathbb{N}$ za koje vrijedi $x! + y! = z!$.

Rješenje. Za početak, očito vrijedi $x, y < z$. Nadalje,

$$y! \mid z! = x! + y! \implies y! \mid x! \implies y \leq x.$$

Analogno se dobije $x \leq y$ pa zaključujemo $x = y$. Sada rješavamo jednadžbu $2x! = z!$. Međutim, $z! \geq (x + 1)! = (x + 1) \cdot x!$ iz čega slijedi da mora biti $x = y = 1, z = 2$. Lako se vidi da je to zaista rješenje zadatka.

Zadatak 1.20. Dokažite da su elementi skupa $S = \{n! \cdot i + 1 : i \in \{1, \dots, n\}\}$ u parovima relativno prosti.

Rješenje. Neka su $1 \leq i < j \leq n$. Vrijedi

$$(n! \cdot i + 1, n! \cdot j + 1) = (n! \cdot i + 1, n! \cdot (j - i)) = (n! \cdot i + 1, j - i).$$

Kako je $0 < j - i \leq n$, vrijedi $j - i \mid n!$ pa je $(n! \cdot i + 1, j - i) = 1$.

Zadatak 1.21. Neka su $a, b, c \in \mathbb{N}$ takvi da vrijedi $(a, b, c) = 1$ i $c = \frac{ab}{a-b}$. Dokažite da je $a - b$ potpun kvadrat.

Rješenje. Neka je $d = (a, b)$ i $a = da', b = db'$. Tada zbog uvjeta zadatka vrijedi $(c, d) = 1$. Nadalje,

$$c = \frac{ab}{a-b} = \frac{da'b'}{a' - b'} \implies a' - b' \mid da'b' \implies a' - b' \mid d.$$

Zadnja implikacija vrijedi jer je $(a' - b', a') = (a' - b', b') = (a', b') = 1$. Stoga je $c = \frac{d}{a' - b'} \cdot a'b'$. Iz ovoga možemo zaključiti

$$\frac{d}{a' - b'} \mid c, d \implies d = a' - b'$$

pa je $a - b = d(a' - b') = d^2$ potpun kvadrat.

Zadatak 1.22. (*) Neka su $a, b, c \in \mathbb{N}$. Dokažite da vrijedi nejednakost

$$(a, b-1) \cdot (b, c-1) \cdot (c, a-1) < ab + bc + ca.$$

Rješenje. Pretpostavimo prvo da je neki od brojeva jednak 1. Zbog simetričnosti nejednakosti možemo BSO pretpostaviti $c = 1$. U tom slučaju imamo

$$(a, b-1) \cdot (b, c-1) \cdot (c, a-1) = (a, b-1) \cdot b \cdot 1 \leq ab < ab + bc + ca.$$

Neka su sada svi brojevi veći od 1. Tada vrijedi

$$\begin{aligned} (a, b-1) \cdot (b, c-1) \cdot (c, a-1) &| a \cdot b \cdot c \\ (a, b-1) \cdot (b, c-1) \cdot (c, a-1) &| (b-1) \cdot (c-1) \cdot (a-1). \end{aligned}$$

Zato vrijedi i

$$(a, b-1) \cdot (b, c-1) \cdot (c, a-1) | abc - (a-1)(b-1)(c-1) = ab + ac + bc - a - b - c + 1.$$

Međutim, lako se vidi da je $0 \leq ab + ac + bc - a - b - c + 1 < ab + ac + bc$ što dokazuje nejednakost i u ovom slučaju.

Zadatak 1.23. (*) Odredite sve $a, b \in \mathbb{N}$ za koje vrijedi $a | b-1$, $b^2 | a^3-1$.

Prvo rješenje. Svi parovi $(a, 1)$, $(1, b)$ su očita rješenja. Pretpostavimo sada $a, b \geq 2$.

Neka je $(a, b) = d$. Tada imamo $d | b-1 \implies d | 1$ pa su a, b relativno prosti. Također, iz prve djeljivosti slijedi da je $b \geq a+1$. Sada ćemo dvije zadane djeljivosti spojiti u jednu ekvivalentnu njima. Vrijedi

$$a | b-1 | b^2-1 \implies a | b^2+a^3-1,$$

$$b^2 | a^3-1 \implies b^2 | a^2+b^2-1.$$

Zaključujemo da $ab^2 | a^3+b^2-1$. Kako je $a^3+b^2-1 > 0$, nužno vrijedi $ab^2 \leq a^3+b^2-1$. Međutim,

$$ab^2 - b^2 = (a-1)b^2 \geq (a-1)(a+1)^2 = a^3 + a^2 - a - 1 > a^3 - 1$$

i dobili smo kontradikciju. Dakle, sva rješenja su $(a, b) = (a, 1), (1, b)$. $\square$

Drugo rješenje. Svi parovi $(a, 1), (1, b)$ su očita rješenja. Pretpostavimo sada $a, b \geq 2$. Iz prve jednakosti dobivamo da postoji $k \in \mathbb{N}$ takav da je $b = ak + 1$. Druga djeljivost sada postaje

$$a^2k^2 + 2ak + 1 = (ak + 1)^2 | a^3 - 1.$$

Sada ćemo pomnožiti desnu stranu s k^2 i primijeniti Euklidov algoritam.

$$a^2k^2 + 2ak + 1 | a^3k^2 - k^2 \implies a^2k^2 + 2ak + 1 | -2a^2k - a - k^2.$$

Stoga nužno vrijedi $a^2k^2 + 2ak + 1 \leq 2a^2k + a + k^2 \iff a^2k(k-2) \leq k(k-2a) + a - 1$. Sada imamo 2 slučaja,

- $a \geq k \geq 2$: tada je $a^2k^2 + 2ak + 1 = a^2k^2 + ak + ak + 1 > 2a^2k + a + k^2$, kontradikcija.
- $k \geq a \geq 2$: tada je $a^2k(k-2) \geq 4k(k-2) > k(k-4) + k - 1 \geq k(k-2a) + a - 1$, kontradikcija.

Dakle, sva rješenja su $(a, b) = (a, 1), (1, b)$. □

Zadatak 1.24. (*) Neka su $x, y \in \mathbb{N}$ takvi da vrijedi $2x^2 + x = 3y^2 + y$. Dokažite da su $x - y, 2x + 2y + 1, 3x + 3y + 1$ potpuni kvadrati.

Rješenje. Glavna ideja ovdje je prikazati zadanu jednakost u obliku u kojem su s jedne strane traženi izrazi, a s druge potpun kvadrat. Primijetimo da vrijedi

$$2x^2 + x - 2y^2 - y = y^2 \implies (x - y)(2x + 2y + 1) = y^2.$$

Nadalje, ako za neki prosti broj p vrijedi $p \mid x - y, 2x + 2y + 1$, tada nužno i $p \mid y$ pa $p \mid (x - y) + y = x$. Međutim, sada dobivamo kontradikciju jer bi moralo vrijediti $p \mid x, y, 2x + 2y + 1 \implies p \mid (2x + 2y + 1) - 2x - 2y = 1$. Dakle, $(x - y, 2x + 2y + 1) = 1$ što znači da $x - y$ i $2x + 2y + 1$ moraju biti potpuni kvadrati (jer im je produkt potpun kvadrat).

Početnu jednakost možemo zapisati i u obliku

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

Analognim argumentom možemo dokazati da je $(x - y, 3x + 3y + 1) = 1$ što znači da $x - y$ i $3x + 3y + 1$ moraju biti potpuni kvadrati.