



Prosti brojevi i kanonski zapis

Okvirna razina: HJMO / SŠ A var. županijsko

1. Teorija i primjeri

Definicija 1

Kažemo da je prirodan broj prost ako ima točno 2 pozitivna djelitelja: 1 i samog sebe. Nadalje, kažemo da je broj složen ako ima više od 2 pozitivna djelitelja. Broj 1 nije ni prost ni složen jer ima samo jednog djelitelja - samog sebe.

Prosti brojevi su iznimno važni u teoriji brojeva. Jedini paran prost broj je 2. Ova tvrdnja, iako naizgled trivijalna, je često korisna u zadacima. U nastavku iznosimo još nekoliko bitnih rezultata o prostim brojevima.

Primjer 1

Svi prosti brojevi $p \geq 3$ su oblika $4k \pm 1$ jer su brojevi $4k$ i $4k \pm 2$ parni. Posebno, broj p^2 je oblika $8k + 1$ jer je $(4k \pm 1)^2 = 8(2k^2 \pm k) + 1$.

Svi prosti brojevi $p \geq 5$ su oblika $6k \pm 1$ jer su brojevi $6k, 6k \pm 2, 6k \pm 4$ parni, a brojevi $6k \pm 3$ djeljivi s 3. Posebno, broj p^2 je oblika $3k + 1$.

Propozicija 2: Euklidova lema

Neka je p prost broj i $a, b \in \mathbb{Z}$. Ako $p \mid ab$, tada $p \mid a$ ili $p \mid b$.

Teorem 3: Osnovni teorem aritmetike

Neka je $n > 1$ prirodan broj. Tada postoje jedinstveni prosti brojevi $p_1 < \dots < p_k$ i eksponenti $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ takvi da je

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Drugim riječima, svaki prirodni broj ima jedinstveni rastav na proste faktore.

Dokaz. Jakom indukcijom ćemo dokazati da svaki broj ima barem jedan rastav na proste faktore. Ako je n prost, tvrdnja trivijalno vrijedi. Ako je n složen, tada postoje brojevi $n_1, n_2 > 1$ takvi da je $n = n_1 n_2$. Brojevi n_1, n_2 imaju rastav na proste faktore po pretpostavci indukcije pa ga onda ima i n .

Jakom indukcijom ćemo dokazati i da je rastav jedinstven. Ako je n prost, tvrdnja trivijalno vrijedi zbog definicije prostih brojeva. Pretpostavimo da je n složen i

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

Po Euklidovoj lemi p_1 mora dijeliti neki od brojeva q_i pa je $p_1 = q_i$ za neki i . Broj $\frac{n}{p_1}$ ima jedinstven rastav po pretpostavci indukcije pa ga onda mora imati i n . $\square$

Iz ovog teorema lako slijedi da je n kvadratno slobodan ako i samo su svi eksponenti α_i jednaki 1. Također, n je potpuna m -ta potencija ako i samo ako su svi eksponenti djeljivi s m .

Definicija 4

Kažemo da su prirodni brojevi relativno prosti ako im je najveći zajednički djelitelj jednak 1, odnosno ako nisu istovremeno djeljivi s istim prostim brojem.

Propozicija 5: Euklidov algoritam

$\text{nzd}(a, b) = \text{nzd}(a, b + ka)$ za svaki $k \in \mathbb{Z}$.

Dokaz. Ako $d \mid a$ i $d \mid b$, tada vrijedi i $d \mid b + ka$. Također, ako $d \mid a$ i $d \mid b + ka$, tada vrijedi i $d \mid (b + ka) - k \cdot a = b$. Tvrdnja sada slijedi iz definicije najvećeg zajedničkog djelitelja. $\square$

Primjer 2: Međunarodna matematička olimpijada 1959.

Razlomak $\frac{21n+4}{14n+3}$ je do kraja skraćen za svaki $n \in \mathbb{N}$. Naime, vrijedi

$$\text{nzd}(21n + 4, 14n + 3) = \text{nzd}(7n + 1, 14n + 3) = \text{nzd}(7n + 1, 1) = 1.$$

Propozicija 6

Za prirodne brojeve a, b vrijedi $\text{nzd}(a, b) \cdot \text{nzv}(a, b) = ab$.

Dokaz. Neka su $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ i $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ (zbog jednostavnosti dopuštamo da su neki eksponenti α_i, β_j jednaki 0). Tada je

$$\begin{aligned} \text{nzd}(a, b) &= p_1^{\min(\alpha_1, \beta_1)} \dots p_k^{\min(\alpha_k, \beta_k)}, \\ \text{nzv}(a, b) &= p_1^{\max(\alpha_1, \beta_1)} \dots p_k^{\max(\alpha_k, \beta_k)}, \\ ab &= p_1^{\alpha_1 + \beta_1} \dots p_k^{\alpha_k + \beta_k}. \end{aligned}$$

Naime, $\text{nzd}(a, b)$ dijeli a i b pa mu eksponent uz svaki p_i može biti najviše α_i i najviše β_i . Analogno zaključujemo za $\text{nzv}(a, b)$.

Tvrdnja zadatka slijedi jer je $\min(x, y) + \max(x, y) = x + y$ za sve brojeve x, y . $\square$

Oprez

Slična tvrdnja ne vrijedi za 3 ili više brojeva. Npr, neka je $a = b = c = 2$. Tada je $\text{nzd}(a, b, c) \cdot \text{nzv}(a, b, c) = 2 \cdot 2 = 4 \neq 8 = abc$.

Primjer 3

Ako su a, b relativno prosti prirodni brojevi čiji je umnožak potpun kvadrat, dokaži da su i brojevi a, b potpuni kvadrati.

Rješenje. Neka su kao u prethodnom dokazu brojevi $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ i $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ (zbog jednostavnosti dopuštamo da su neki eksponenti α_i, β_j jednaki 0). Tada vrijedi

$$2 \mid \alpha_i + \beta_i, \min(\alpha_i, \beta_i) = 0 \implies \alpha_i = 0 \text{ ili } \beta_i = 0.$$

Oдавде vidimo da vrijedi $2 \mid \alpha_i$ i $2 \mid \beta_i$ za svaki i pa su brojevi a, b potpuni kvadrati. □

Teorem 7: Euklid

Prostih brojeva ima beskonačno mnogo.

Dokaz. Pretpostavimo suprotno i neka su $p_1, \dots, p_k$ svi prosti brojevi. Promotrimo broj

$$N = p_1 \dots p_k + 1.$$

On ima rastav na proste faktore, ali nije djeljiv s nijednim brojem p_i jer je

$$\text{nzd}(N, p_i) = \text{nzd}(p_1 \dots p_k + 1, p_i) = \text{nzd}(1, p_i) = 1.$$

Dakle, mora postojati još prostih brojeva, kontradikcija. □

Napomena 8

Bez obzira što ima beskonačno mnogo prostih brojeva, oni su rijetki u skupu $\mathbb{N}$. Npr. za svaki n postoji n uzastopnih složenih brojeva

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n + 1.$$

Oni su očito složeni jer je prvi broj djeljiv s 2, drugi s 3, ..., a zadnji s $n+1$.

S druge strane, postoji mnogo otvorenih problema o distribuciji prostih brojeva. Poznata Goldbachova slutnja kaže da postoji beskonačno mnogo parova blizanaca prostih brojeva (tj. prostih brojeva koji se razlikuju za 2).

1.1. Riješeni primjeri

Primjer 4

Odredi sve proste brojeve p takve da su brojevi $p + 2$ i $p + 4$ 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 $p = 3$. $\square$

Primjer 5

Dokaži da za svaki prost broj $p \geq 5$ vrijedi $24 \mid p^2 - 1$.

Rješenje. p je oblika $6k \pm 1$ pa je

$$p^2 - 1 = (6k \pm 1)^2 - 1 = 36k^2 \pm 12k = 12k(3k \pm 1).$$

Broj $k(3k \pm 1)$ je uvijek paran jer je barem jedan od brojeva $k, 3k + 1$ paran. Stoga je $p^2 - 1$ djeljivo s 24. $\square$

Primjer 6

Dokaži da ima beskonačno mnogo prostih brojeva oblika $4k + 3$.

Rješenje. Pretpostavimo suprotno i neka su $p_1, \dots, p_k$ svi prosti brojevi oblika $4k + 3$. Ključna tvrdnja ovdje je da je produkt brojeva oblika $4k + 1$ također tog oblika jer je

$$(4k + 1)(4l + 1) = 4(4kl + k + l) + 1.$$

Promotrimo broj

$$N = 4p_1 \dots p_k - 1.$$

On je oblika $4k + 3$ pa zbog gore navedenog ima barem jedan prost djeliteľ tog oblika, ali nije djeljiv s nijednim brojem p_i jer je

$$\text{nzd}(N, p_i) = \text{nzd}(4p_1 \dots p_k - 1, p_i) = \text{nzd}(1, p_i) = 1.$$

Dakle, mora postojati još prostih brojeva oblika $4k + 3$, kontradikcija. $\square$

Primjer 7: Fermatovi prosti brojevi

Ako je broj $2^k + 1$ prost, dokaži da je $k = 0$ ili je k potencija broja 2.

Rješenje. Pretpostavimo da k nije potencija broja 2. Tada k možemo napisati u obliku $k = pa$, gdje je $p \geq 3$ prost. Sada je

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

Faktor $2^a + 1$ to je očito veći od 1, a drugi je veći od 1 jer je $2^{ap} + 1 > 2^a + 1$. Dakle, $2^k + 1$ se može rastaviti na produkt 2 faktora veća od 1 pa je složen, kontradikcija. $\square$

Primjer 8: Mersenneovi prosti brojevi

Ako je broj $2^k - 1$ prost, dokaži da je i k prost.

Rješenje. Pretpostavimo da je k složen. Tada k možemo zapisati u obliku $k = ab$, gdje su $a, b > 1$. Sada je

$$2^k - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1).$$

Oba faktora su veća od 1 pa je broj $2^k - 1$ složen, kontradikcija. □

Zadaci za samostalnu vježbu

1. Odredi prirodni broj n takav da mu je suma dva najmanja djelitelja 6, a suma dva najveća djelitelja 1122.
2. Dokaži da svaki složen broj n ima prost faktor $p \leq \sqrt{n}$.
3. Odredi sve prirodne brojeve n takve da su brojevi $3n - 4, 4n - 5, 5n - 3$ prosti.
4. Ako su brojevi p i $p^2 + 2$ prosti, dokaži da je i $p^3 + 4$ prost.
5. Odredi sve proste brojeve p takve da je $21p + 1$ potpun kvadrat.
6. Odredi sve prirodne brojeve n takve da su brojevi $2^n - 1, 2^n + 1$ prosti.
7. Odredi sve parove prostih brojeva (p, q) takve da je $p^2 - 2q^2 = 1$.
8. Dokaži da $360 \mid p^4 - 5p^2 + 4$ za sve proste brojeve $p \geq 7$.
9. Za koje proste brojeve je i $2^p + p^2$ prost broj?
10. Odredi sve proste brojeve p, q takve da je $p + q = (p - q)^3$.
11. Odredi sve proste brojeve p za koje postoje $m, n \in \mathbb{N}$ takvi da je $p^{2n+1} = 2^m + 1$.
12. Neka je $n \geq 3$ prirodan broj i neka su p, q prosti brojevi takvi da $p \mid n!, q \mid n! - 1$. Dokaži da je $p < q$.
13. Odredi sve proste brojeve p, q takve da je $p^3 - q^5 = (p + q)^2$.
14. Odredi sve prirodne brojeve x, y za koje je $\frac{xy^2}{x+y}$ prost broj.
15. Nađi sve proste brojeve p, q za koje je $p^{q-1} + q^{p-1}$ potpun kvadrat.
16. Iz skupa $\{1, 2, 3, \dots, 2n\}$ odabrano je $n + 1$ brojeva. Dokaži da među njima postoje 2 koji su relativno prosti.
17. Neka su $f_n = 2^{2^n} + 1$. Dokaži da za $m \neq n$ vrijedi $\text{nzd}(f_m, f_n) = 1$.
18. Odredi sve cijele brojeve x takve da je $2x^2 - x - 36$ kvadrat prostog broja.

- 19.** Neka su $a, b, c \in \mathbb{N}$ takvi da su brojevi ab, ac, bc potpuni kubovi. Dokažite da su i a, b, c potpuni kubovi. Vrijedi li ista tvrdnja za kvadrate?
- 20.** Odredi sve uređene trojke (x, y, p) , gdje je p prost, a x i y prirodni brojevi za koje vrijedi
- $$p^x - 1 = y^3.$$
- 21.** Dokažite da su elementi skupa $S = \{n! \cdot i + 1 : i \in \{1, \dots, n\}\}$ u parovima relativno prosti.
- 22.** 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.

Upute za zadatke za samostalnu vježbu

1. Odredi najmanji prosti djeljitelj broja n .
2. $n = ab$ za $a, b > 1$.
3. mod 2.
4. mod 3.
5. Razlika kvadrata.
6. mod 2 i mod 3.
7. mod 8.
8. Faktoriziraj izraz.
9. mod 2 i mod 3.
10. mod 3.
11. Faktoriziraj izraz.
12. $p \mid n! \iff p \leq n$.
13. mod 3.
14. Dokaži da $p \mid x$ ili $p \mid y$.
15. mod 3.
16. Dokaži da su odabrana 2 uzastopna broja.
17. Primijeti da $f_n \mid f_{n+1} - 2, f_{n+2} - 2, \dots$
18. Faktoriziraj izraz.
19. Pomnoži te brojeve.
20. Faktoriziraj izraz.
21. Euklidov algoritam.
22. Prikaži jednakost u obliku u kojem su s jedne strane traženi izrazi, a s druge potpun kvadrat.

Rješenja zadataka za samostalnu vježbu

1. Neka je p najmanji prosti djelitelj broja n . Tada je $1 + p = 6 \implies p = 5$. Također, suma dva najveća djelitelja je $n + \frac{n}{p} = n + \frac{n}{5} = \frac{6n}{5} = 1122$ iz čega slijedi da je $n = 935$.
2. Postoje prirodni brojevi $a, b > 1$ takvi da je $n = ab$. Neka je bez smanjenja općenitosti $a \leq b$. Broj a je veći od 1 pa postoji prost broj $p \mid a$. Sada je $p \leq a$ i $n = ab \geq a^2$ iz čega slijedi $n \geq p^2 \implies p \leq \sqrt{n}$.
3. Brojevi $3n - 4$ i $5n - 3$ su različite parnosti pa je barem jedan od njih jednak 2. Sada lako vidimo da mora biti $n = 2$ i da je to rješenje zadatka.
4. Ako je $p \neq 3$, tada je p^2 oblika $3k + 1$ pa $3 \mid p^2 + 2$, kontradikcija. Dakle, mora biti $p = 3$ i u tom slučaju je $p^3 + 4 = 31$.

5. 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 $p = 3, 19, 23$.

6. 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.

7. Broj p mora biti neparan pa je p^2 oblika $8k + 1$. Stoga $8 \mid 2q^2$ iz čega slijedi $q = 2$ i $p = 3$.

8. Vrijedi

$$p^4 - 5p^2 + 4 = (p^2 - 4)(p^2 - 1).$$

Znamo da je p^2 oblika $8k + 1$ i $3k + 1$ pa $8 \mid p^2 - 1$ i $3 \mid p^2 - 4, p^2 - 1$. Također, p je veći od 5 pa imamo 2 slučaja.

- $p = 5k \pm 1 \implies 5 \mid p^2 - 1$
- $p = 5k \pm 2 \implies 5 \mid p^2 - 4$

U svakom slučaju smo dokazali da je izraz $(p^2 - 4)(p^2 - 1)$ djeljiv s 8, 9 i 5 pa je djeljiv s $8 \cdot 9 \cdot 5 = 360$.

9. Ako je $p \geq 5$, tada je p^2 oblika $3k + 1$, a 2^p je oblika $3k + 2$ pa $3 \mid 2^p + p^2$, kontradikcija. Za $p = 2$ je $2^p + p^2 = 8$, a za $p = 3$ je $2^p + p^2 = 17$. Dakle, jedino rješenje je $p = 3$.

10. Ako nijedan od brojeva p, q nije jednak 3, onda je točno jedan od brojeva $p \pm q$ djeljiv s 3 što nije moguće.

Ako je $p = 3$, tada je $q + 3 = (3 - q)^3$ pa mora biti $q < 3$. Lako vidimo da u ovom slučaju nema rješenja.

Ako je $q = 3$, tada je

$$p + 3 = (p - 3)^3 \iff p^3 - 9p^2 + 26p - 30 = 0.$$

Gledajući male slučajeve primjećujemo da je $p = 5$ rješenje, stoga se ovaj polinom može faktorizirati kao

$$(p - 5)(p^2 - 4p + 6) = 0.$$

Nije teško provjeriti da jednačba $p^2 - 4p + 6 = 0$ nema realnih rješenja pa je jedino rješenje $(p, q) = (5, 3)$.

11. 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 .

12. 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 $p < q$.

13. Ako nijedan od brojeva p, q nije jednak 3, tada gledanjem po slučajevima nije teško dobiti da je točno jedan od brojeva $p^3 - q^5$ i $p + q$ djeljiv s 3 što nije moguće.

Ako je $p = 3$, tada je $27 - q^5 = (q + 3)^2$. Kako mora biti $q^5 < 27$, lako vidimo da u ovom slučaju nema rješenja.

Ako je $q = 3$, tada je

$$p^3 - 243 = (p + 3)^2 \iff p^3 - p^2 - 6p - 252 = 0.$$

Gledajući male slučajeve primjećujemo da je $p = 7$ rješenje, stoga se ovaj polinom može faktorizirati kao

$$(p - 7)(p^2 + 6p + 36) = 0.$$

Nije teško provjeriti da jednačba $p^2 + 6p + 36 = 0$ nema realnih rješenja pa je jedino rješenje $(p, q) = (7, 3)$.

14. Neka je $xy^2 = p(x + y)$. Stoga je barem jedan od brojeva x, y djeljiv s p .

Ako je $y = pb$, tada jednačba postaje

$$p^2b^2x = p(x + pb) \implies p \mid x.$$

Dakle, svakako je x djeljiv s p i možemo pisati $x = pa$. Sada jednačba postaje

$$pay^2 = p(pa + y) \implies ay^2 = pa + y \implies pa = y(ay - 1).$$

Brojevi $a, ay + 1$ su relativno prosti pa mora vrijediti $a \mid y$, tj. $y = ak$ pa je $p = k(a^2k - 1)$. Kako je p prost, jedan od faktora mora biti jednak 1.

Ako je $k = 1$, tada je $a = y$ i $p = a^2 - 1 = (a - 1)(a + 1)$. Lako vidimo da mora biti $a = 2, p = 3$ i dobivamo rješenje $x = 6, y = 2$.

Ako je $a^2k - 1 = 1$, tada je $a^2k = 2$ pa je $a = 1$ i $k = 2$. Stoga je $p = 2$ pa dobivamo rješenje $x = 2, y = 2$.

15. Ako su $p, q \geq 5$, tada su brojevi p^{q-1} i q^{p-1} oblika $3k + 1$ pa je $p^{q-1} + q^{p-1}$ oblika $3k + 2$. Međutim, nijedan potpun kvadrat ne može biti tog oblika, kontradikcija.

Ako je $q = 2$, lako vidimo da je $p = 2$ rješenje, a inače dobivamo jednačbu

$$p + 2^{p-1} = x^2 \iff p = (x - 2^{\frac{p-1}{2}})(x + 2^{\frac{p-1}{2}}).$$

Kako je p prost, jedan od ovih brojeva mora biti jednak 1 pa je $x - 2^{\frac{p-1}{2}} = 1$ i $x + 2^{\frac{p-1}{2}} = p$. Iz ovoga možemo zaključiti da je $p = 2^{\frac{p+1}{2}} + 1$. Dakle, p je Fermatov prosti broj. Sada dobivamo kontradikciju mod 4 jer je $p = 2^{\frac{p+1}{2}} + 1$ oblika $4k + 1$, a $\frac{p+1}{2}$ mora biti potencija od 2.

Ako je $q = 3$, lako vidimo da je $p \geq 3$ i dobivamo jednačbu

$$p^2 + 3^{p-1} = x^2.$$

Brojevi p^2 i 3^{p-1} su oblika $4k + 1$ pa x^2 mora biti oblika $4k + 2$, kontradikcija.

Dakle, jedino rješenje je $p = q = 2$.

16. Podijelimo brojeve u parove

$$\{1, 2\}, \{3, 4\}, \dots, \{2n - 1, 2n\}.$$

Po Dirichletovom principu smo iz barem jednog para odabrali oba broja. Oni su uzastopni pa su relativno prosti jer je $\text{nzd}(n, n + 1) = \text{nzd}(n, 1) = 1$.

17. Neka je bez smanjenja općenitosti $m > n$. Primijetimo da vrijedi

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

Zaključujemo da $f_n \mid f_{n+1} - 2$ i $f_n - 2 \mid f_{n+1} - 2$ pa

$$f_n \mid f_{n+1} - 2 \mid f_{n+2} - 2 \mid \dots \mid f_m - 2.$$

Sada po Euklidovom algoritmu vrijedi $\text{nzd}(f_m, f_n) = \text{nzd}(2, f_n) = 1$.

18. Imamo jednadžbu

$$2x^2 - x - 36 = (x + 4)(2x - 9) = p^2.$$

Sada imamo 6 slučajeva:

- $x + 4 = 1, 2x - 9 = p^2$: ovdje nema rješenja.
- $x + 4 = p, 2x - 9 = p$: iz $x + 4 = 2x - 9$ dobivamo $x = 13$ i $p = 17$.
- $x + 4 = p^2, 2x - 9 = 1$: dobivamo $x = 5$ i $p = 3$.
- $x + 4 = -1, 2x - 9 = -p^2$: ovdje nema rješenja.
- $x + 4 = -p, 2x - 9 = -p$: iz $x + 4 = 2x - 9$ dobivamo $x = 13$, međutim ovdje nema rješenja.
- $x + 4 = -p^2, 2x - 9 = -1$: ovdje nema rješenja.

Dakle, sva rješenja su $x = 5, 13$.

19. 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 $a = b = c = 2$.

20. 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 $(x, y, p) = (1, 1, 2), (2, 2, 3)$.

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

22. 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.