Euklidov algoritam i kvadratni ostatci (MetaMath 2022 - 6. tjedan)

Josip Pupić

06.11.2022.

1 Primjeri

1. **Primjer:** Vrlo često je u zadacima iz teorije brojeva potrebno odrediti najveći zajednički djelitelj nekih dvaju cijelih brojeva. S konkretnim brojevima je postupak jasan, odredimo njihov rastav na proste faktore i točno sve ono što im je u presjeku je njihov najveći zajednički djelitelj. Recimo,

$$M(30, 105) = M(2 \cdot 3 \cdot 5, 3 \cdot 5 \cdot 7) = 3 \cdot 5 = 15.$$

(*Podsjetnik: najveći zajednički djelitelj brojeva a i b najčešće označavamo s $M(a, b)$. U stranoj literaturi obično se može vidjeti oznaku $GCD(a, b)$.*)

Ipak, u zadacima se češće susrećemo s određivanjem najvećeg zajedničkog djelitelja nekih algebarskih izraza. Primjerice, za relativno proste brojeve a i b, vrijedi $M(a^2b, ab^3) = M(a \cdot ab, b^2 \cdot ab) = ab$. Naime, a i b su relativno prosti pa nemaju zajedničkih djelitelja osim 1, a onda to vrijedi i za izraze a i b^2.

Međutim, ovakvi argumenti su dosta ograničeni. Primjerice, njima ne možemo reći ništa o $M(a, 2a+1)$ za proizvoljan a. Kao jedno od rješenja tog problema, nudi se takozvani **Euklidov algoritam**, koji kaže da za proizvoljne cijele brojeve a i b vrijedi

$$M(a, b) = M(a, b - a).$$

Dokažimo tu tvrdnju. Neka je $M(a, b) = x$ i $M(a, b-a) = y$. Tada vrijedi $x|a$ te $x|b$ pa je $a = cx$ i $b = dx$, za neke cijele brojeve c, d. Tada je $b - a = (d - c)x$ pa $x|(b - a)$. Znači da je x zajednički djelitelj brojeva a i $b - a$, a s obzirom da je y njihov najveći zajednički djelitelj, mora vrijediti $x \leq y$.

No, analognu argumentaciju možemo primijeniti i s druge strane. Kako $y|a$ i $y|(b - a)$, vrijedi $a = ey$, $b - a = fy$, za neke cijele brojeve e, f. Tada je $b = a + (b - a) = (e + f)y$ pa $y|b$. Dakle, y je zajednički djelitelj brojeva a i b, a x je po definiciji najveći takav pa mora biti $y \leq x$. Zato zaključujemo da je $x = y$.

2. **Primjer:** Koji je *kardinalitet* (broj članova) skupa svih cijelih brojeva n za koje je razlomak $\frac{40n+2}{15n-1}$ cijeli broj?

Rješenje: Napomenimo odmah na početku rješenja kako je iz tvrdnje i dokaza Euklidovog algoritma jasno da vrijedi i $M(a, b) = M(a, b - ka)$, za svaki cijeli broj k. Naime, za pozitivan k je to samo k uzastopnih primjena (osnovnog) Euklidovog algoritma:

$$M(a, b) = M(a, b - a) = M(a, (b - a) - a) = M(a, b - 2a) = ... = M(a, (b - (k - 1)a) - a) = M(a, b - ka).$$

Sada raspisujemo:

$$\begin{aligned} M(40n - 1, 15n - 1) &= M(40n - 1 - 2(15n - 1), 15n - 1) \\ &= M(10n + 1, 15n - 1) \\ &= M(10n + 1, 15n - 1 - (10n + 1)) \\ &= M(10n + 1, 5n - 2) \\ &= M(10n + 1 - 2(5n - 2), 5n - 2) \\ &= M(5, 5n - 2) = 1 \end{aligned}$$

U zadnjem koraku je najveći zajednički djelitelj 1 jer broj $5n - 2$ ne može biti djeljiv s 5. Dakle, brojnik i nazivnik početnog razlomka su relativno prosti pa su jedini n za koje taj razlomak može biti cijeli broj, oni za koje je vrijednost nazivnika 1 ili -1. Očito je da je jedini takav broj $n = 0$.

3. **Primjer:** Definirajmo cijeli broj m kao *kvadratni ostatak modulo n* ako postoji cijeli broj a takav da je $a^2 \equiv m(mod\, n)$.

   Dokažimo za neparan prosti broj p postoji točno $\frac{p+1}{2}$ kvadratnih ostataka modulo p.

   Rješenje: Najprije primijetimo da je 0 očito uvijek kvadratni ostatak jer je, primjerice, p^2 uvijek djeljiv s p.

   Neka je sada $1 \leq m \leq p-1$. Primijetimo da je $m^2 \equiv m^2 + p(p-2m) \equiv p^2 - 2pm + m^2 \equiv (p-m)^2(mod\, n)$. Dakle, kvadrati od m i $p-m$ daju jednake ostatke modulo p, za svaki promatrani m, što znači da možemo imati maksimalno $\frac{p-1}{2}$ kvadratnih ostataka u skupu $\{1, ..., p-1\}$.

   S druge strane, pretpostavimo da su $1 \leq m, n \leq p-1$ takvi da je $m^2 \equiv n^2(mod\, p)$. U tom je slučaju $(m-n)(m+n) \equiv 0(mod\, p)$, tj neki od brojeva $m-n$ i $m+n$ je djeljiv s p. To onda implicira da vrijedi ili $m \equiv n(mod\, p)$ ili $m \equiv p-n(modp)$. Dakle, svaki od $\frac{p-1}{2}$ parova ostataka $\{m, p-m\}$ iz skupa $\{1, ..., p-1\}$ daje različite kvadratne ostatke module p pa ih zaista ima točno $\frac{p-1}{2}$.

4. **Primjer:** Riješite jednadžbu $x^2 + 8y = 123$ u cijelim brojevima.

   Rješenje: Ideja koju ćemo primijeniti ovdje često se koristi u ovakvim zadacima. Cilj je promotriti jednadžbu modulo n, za neki n za kojeg ćemo moći eliminirati što više potencijalnih rješenja i svesti zadatak na jednostavniji problem. Primjerice, ovdje ćemo promotriti jednadžbu modulo 8, zato što time "nestaje" član $8y$ iz jednadžbe, budući da je taj izraz djeljiv s 8 neovisno o vrijednosti y. Dakle, svako potencijano rješenje promatrane jednadžbe mora zadovoljavati:

   $$x^2 \equiv 3(mod\, 8),$$

   jer je $123 \equiv 3(mod\, 8)$. Sada možemo samo uvrstiti sve moguće ostatke modulo 8 umjesto x i provjeriti daje li ijedan od njih nakon kvadriranja ostatak 3 pri dijeljenju s 8.

   Ipak, možemo i nešto pametnije pristupiti problemu i dodatno olakšati posao. Primijetimo da je kvadrat svakog parnog broja nužno djeljiv sa 4. No, ako je broj djeljiv s 4, jedini ostatci koje on može davati pri dijeljenju s 8 su 0 i 4. Dakle, x svakako ne može biti paran broj.

   Nadalje, ako se sjetimo **primjera 3**, ondje smo komentirali da kvadrati od x i $n-x$ uvijek daju jednake ostatke pri dijeljenju s n. Koristeći tu opservaciju, uz prethodnu koja nam govori da je x nužno neparan, preostaje nam samo provjeriti kakve ostatke modulo 8 daju 1^2 i 3^2. Odgovor je u oba slučaja očito 1, pa možemo zaključiti da ne postoji cijeli broj x čiji kvadrat daje ostatak 3 pri dijeljenju s 8, a samim time ne postoji niti jedno rješenje početne jednadžbe.

   Možda se ove napomene čine nepotrebne s obzirom da nije tako teško izračunati kvadrate 8 brojeva modulo 8, ali u praksi možemo imati puno veći broj potrebnih uvrštavanja i zato tu kompleksnost uvijek pokušavamo reducirati "pametnim" trikovima i opservacijama poput ovih ovdje.

2 Osnovni lanac

1. **Zadatak:** Ako je suma dvaju kvadrata prirodnih brojeva djeljiva s 11, dokažite da je onda djeljiva i sa 121.

   Rješenje: Imamo da je $a^2 + b^2 \equiv 0 \pmod{11}$. Uvrštavanjem svih ostataka od 0 do $\frac{11-1}{2} = 5$ (iz primjera znamo da se isti ostatci ponavljaju među kvadratima preostalih ostataka mod 11), zaključujemo da su svi kvadratni ostatci mod 11:

   $$0, 1, 3, 4, 5, 9.$$

   Provjerom svih mogućnosti, vidimo da je jedini slučaj kada $11 \mid a^2 + b^2$ onaj kada je $a^2 \equiv b^2 \equiv 0 \pmod{11}$. Kako $11 \mid a^2$, a 11 je prost broj, slijedi $11 \mid a$ pa i $121 \mid a^2$. Analogno dobijamo $121 \mid b^2$ pa je $a^2 + b^2 \equiv 0 \pmod{121}$.

2. **Zadatak:** Koji je najveći prirodan broj za koji je $n^3 + 100$ djeljivo s $n + 10$?

   Rješenje: Pomoću Euklidovog algoritma računamo:

   $$\begin{aligned} \mathrm{M}(n+10, n^3+100) &= \mathrm{M}(n+10, n^3+100-n^2(n+10)) \\ &= \mathrm{M}(n+10, 100-10n^2) \\ &= \mathrm{M}(n+10, 100-10n^2+10n(n+10)) \\ &= \mathrm{M}(n+10, 100n+100) \\ &= \mathrm{M}(n+10, 100n+100-100(n+10)) \\ &= \mathrm{M}(n+10, -900) \mid 900 \end{aligned}$$

   Želimo da $n+10 \mid n^3+100$ pa mora biti $n+10 = \mathrm{M}(n+10, n^3+100)$, a pokazali smo da je to neki djelitelj od 900. Najveći n se onda očito postiže upravo za najveći djelitelj od 900, odnosno kada je $n+10 = 900$, tj $n = \boxed{890}$.

3. **Zadatak:** Riješite u prirodnim brojevima jednadžbu $1! + 2! + 3! + ... + x! = y^2$.

   Rješenje: Pretpostavimo najprije da je $x \geq 4$. Promotrimo li jednažbu mod 5, zaključujemo da lijeva strana jednadžbe daje ostatak $1! + 2! + 3! + 4! \equiv 33 \equiv 3 \pmod 5$, jer su svi ostali pribrojnici na lijevoj strani djeljivi s 5. S druge strane, svi kvadratni ostatci pri dijeljenju s 5 su iz skupa $\{0, 1, 4\}$ pa za ovakve x nema rješenja početne jednadžbe.

   Dakle, nužno mora biti $x \leq 4$. Promotrimo preostale slučajeve:

   - $x = 1 \implies y = 1$
   - $x = 2 \implies y \notin \mathbb{N}$
   - $x = 3 \implies y = 3$
   - $x = 4 \implies y \notin \mathbb{N}$

   Stoga, jedina 2 rješenja su $\{(1, 1), (3, 3)\}$.

4. **Zadatak:** Dokažite da su svaka dva uzastopna člana Fibonaccijevog niza relativno prosti.

   (Napomena: Fibonaccijev niz je niz prirodnih brojeva definiran sa $F_0 = 0$, $F_1 = 1$ i $F_{n+1} = F_n + F_{n-1}$, za svaki prirodan broj n.)

   Prvo rješenje: Provedimo dokaz indukcijom. Baza indukcije očito vrijedi jer je $M(F_0, F_1) = M(0, 1) = 1$. Pretpostavimo sada da za neki n vrijedi $M(F_{n-1}, F_n) = 1$ i dokažimo da tada vrijedi i $M(F_n, F_{n+1}) = 1$. Po Euklidovom algoritmu imamo

   $$M(F_n, F_{n+1}) = M(F_n, F_n + F_{n-1}) = M(F_n, F_n + F_{n-1} - F_n) = M(F_n, F_n - 1) = 1,$$

   čime je dokaz indukcijom uspješno završen.

   Drugo rješenje: Pretpostavimo suprotno tvrdnji zadatka i neka je n najmanji prirodan broj takav da je $M(F_{n+1}, F_n) > 1$. Tada koristeći Euklidov algoritam dobivamo

   $$M(F_{n+1}, F_n) = M(F_n + F_{n-1}, F_n) = M(F_n + F_{n-1} - F_n, F_n) = M(F_{n-1}, F_n),$$

   čime smo pokazali da je i najveći zajednički djelitelj od F_n i F_{n-1} veći od 1. To je kontradikcija s pretpostavkom minimalnosti od n. Ovo je primjer korištenja principa ekstrema, čime smo zaobišli korištenje matematičke indukcije.

5. **Zadatak:** Nađite sve parove prirodnih brojeva x i y koji zadovoljavaju jednadžbu $x^5 = y^2 + 4$.

   Rješenje: Svi kvadratni ostatci $\pmod{11}$ su $0, 1, 3, 4, 5, 9$, kao što smo već rekli u rješenju prvog zadatka. S druge strane, svi ostatci petih potencija $\pmod{11}$ su $0, 1, 10$. Provjerom svih mogućnosti zaključujemo da ne postoje prirodni brojevi x, y koji zadovoljavaju $x^5 \equiv y^2 + 4 \pmod{11}$, a time ni oni koji zadovoljavaju $x^5 = y^2 + 4$.

   Često rješenja ovakvih zadataka izgledaju prilično jednostavno, ali ne čine se tako jednostavnima za smisliti. Razumno se pitati "Kako da znam koji mod je ispravan za promatrati? Trebam li samo isprobavati sve redom dok neki ne proradi?"

   Ne postoji "formula" kojom ćemo prepoznati postoje li mod-ovi koji će riješiti zadatak i koji su to, ali postoje principi koji nam mogu olakšati i ubrzati dolazak do rješenja.

   - Jedan od principa je svakako birati one mod-ove za koje "kompliciran" članovi u jednadžbi imaju što manje mogućih vrijednosti koje mogu poprimiti. Do njih pak dolazimo uz pomoću druge metode koju smo imali priliku naučiti ovaj tjedan - Eulerovog teorema. Naime, znamo da je $a^{\varphi(m)} \equiv 1 \pmod m$, u slučaju kada je $M(a, m) = 1$. Dakle, htjeli bismo birati takve m, da su njihovi pripadni $\varphi(m)$ jednaki "kompliciranim" eksponentima koji se javljaju u zadatku, ili su pak njihovi "bliski" višekratnici.

     Konkretno, u ovom zadatku je x^5 svakako najkompleksniji element jednadžbe, a vrijedi $\varphi(11) = 10$ pa je $x^{10} \equiv 0$ ili $1 \pmod{11}$, a time je x^5 iz skupa $\{0, 1, -1\}$ ostataka pri dijeljenju s 11.
   - Drugi princip je promatranje prostih mod-ova. Ovo svakako ne vrijedi uvijek, mod-ovi $4, 8, 9$ se znaju pokazati vrlo korisnima, ali često se većina "informacije" i "argumenata" može vidjeti već promatranjem prostih brojeva i stoga nema potrebe za promatranjem njihovih višekratnika.
   - S iskustvom se nauče neke "fore", koje se uglavnom baziraju na prvom principu. Primjerice, kada imamo jednadžbu s kubovima, često je korisno promatrati mod-ove 7 ili 9; kvadrati neparnih brojeva uvijek daju ostatak 1 pri dijeljenju s 8 i slično...

3 Ozbiljniji lanac

6. **Zadatak:** Promotrimo beskonačni niz prirodnih brojeva $(a_n)_n$ koji je zadan formulom $a_n = 100 + n^2$. Za svaki n, definirajmo d_n kao najveći zajednički djelitelj brojeva a_n i a_{n+1}, odnosno $d_n = M(a_n, a_{n+1})$. Koja je najveća vrijednost koju poprima neki od brojeva d_n?

   Rješenje: Pomoću Euklidovog algoritma dobivamo:

$$\begin{aligned} M(100+n^2, 100+(n+1)^2) &= M(100+n^2, 100+n^2+2n+1) \\ &= M(100+n^2, 100+n^2+2n+1-100-n^2) \\ &= M(100+n^2, 2n+1). \end{aligned}$$

   Budući da je $2n+1$ neparan, možemo prvi element u zadnjem izrazu pomnožiti s 2 i najveći zajednički djelitelj će ostati isti. Dalje vrijedi:

$$\begin{aligned} M(200+2n^2, 2n+1) &= M(200+2n^2-n(2n+1), 2n+1) \\ &= M(200-n, 2n+1) \\ &= M(200-n, 2n+1+2(200-n)) \\ &= M(200-n, 401). \end{aligned}$$

   Dakle, pokazali smo da je najveći zajednički djelitelj svaka 2 uzastopna člana niza uvijek neki djelitelj broja 401. Budući da se u slučaju $n = 200$ zaista postiže vrijednost 401, zaključujemo da je upravo to traženo rješenje.

7. **Zadatak:** Odredite sve cijele brojeve x za koje je razlomak $\frac{x^3-x^2-x-1}{3x-1}$ cijeli broj.

   Rješenje: Zahtjevom da promatrani razlomak bude cijeli broj zapravo tražimo da nazivnik bude djelitelj brojnika, odnosno da je $M(x^3-x^2-x-1, 3x-1) = 3x-1$.

   S druge strane, koristit ćemo Euklidov algoritam. Najprije primijetimo da $3x-1$ nije djeljivo s 3 ni za koji x pa možemo pomnožiti brojnik s 3 bez da promijenimo najveći zajednički djelitelj brojnika i nazivnika. Sada računamo:

$$\begin{aligned} M(3(x^3-x^2-x-1), 3x-1) &= M(3x^3-3x^2-3x-3-x^2(3x-1), 3x-1) \\ &= M(-2x^2-3x-3, 3x-1) \\ &= M(3(-2x^2-3x-3), 3x-1) \\ &= M(-6x^2-9x-9+2x(3x-1), 3x-1) \\ &= M(-11x-9, 3x-1) \\ &= M(3(-11x-9), 3x-1) \\ &= M(-33x-27+11(3x-1), 3x-1) \\ &= M(-38, 3x-1) \mid 38 \end{aligned}$$

   Pri raspisu smo još dvaput koristili ranije spomenuto svojstvo zbog kojeg smijemo lijevi član množiti s 3 bez promjene najvećeg zajedničkog djelitelja.

   Preostaje provjeriti za koje djelitelje od 38 ova jednadžba daje rješenja. Uvrštavanjem u $3x-1 \in \{\pm 1, \pm 2, \pm 19, \pm 38\}$ dobivamo da su sva cjelobrojna rješenja $x \in \{-6, 0, 1, 13\}$.

8. **Zadatak:** Neka su a, b, c, k prirodni brojevi takvi da vrijedi $a, b, c \geq 3$ i $abc = k^2 + 1$. Dokažite da je barem jedan od brojeva $a-1$, $b-1$ i $c-1$ složen.

   Rješenje: Pretpostavimo da su $a-1, b-1, c-1$ svi prosti. Neka je onda

$$\begin{aligned} a &= p+1 \\ b &= q+1 \\ c &= r+1, \end{aligned}$$

   gdje su p, q, r prosti brojevi. Bez smanjenja općenitosti možemo pretpostaviti $p \geq q \geq r$.

   Pretpostavimo najprije $q = 2$. Tada mora biti i $r = 2$. U tom je slučaju lijeva strana jednadžbe djeljiva s 3, dok desna to ne može biti jer 2 nije kvadratni ostatak modulo 3.

   Neka je sada $q > 2$. Promatranjem lijeve strane jednadžbe zaključujemo da je ona djeljiva s 4 (jer su p i q prosti brojevi veći od 2 pa su neparni), dok desna strana nikada nije djeljiva s 4 jer k^2 daje ostatke $0, 1$ pri dijeljenju s 4.

   U svakom slučaju dolazimo do kontradikcije pa je pretpostavka pogrešna i mora postojati barem 1 složen broj u skupu $\{a-1, b-1, c-1\}$.

9. **Zadatak:** Kod određivanja kvadratnih ostataka, korisno nam je definirati takozvani **Legendreov simbol**. Za prirodan broj a i prost broj p označavamo Legendreov simbol sa

$$\left(\frac{a}{p}\right)$$

i njegova je vrijednost 1 ukoliko je a kvadratni ostatak modulo p, 0 ukoliko p dijeli a te -1 inače.

(a) Dokažite svojstvo Legendreovog simbola koje se naziva *Eulerov kriterij*: ako je p neparan prost broj koji ne dijeli prirodan broj a, onda vrijedi

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

(b) Dokažite svojstvo Legendreovog simbola koje se naziva *Gaussov zakon reciprociteta*: ako su p i q različiti neparni prosti brojevi, onda vrijedi

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Rješenje: Za ovaj zadatak ne postoji baš elementaran dokaz. :)

Rješenje prvog dijela izvedivo je metodama koje se koriste u malo težim natjecateljskim zadacima i njegovo rješenje možete pronaći primjerice u TU. Rješenje drugog dijela je iznimno kompliciranо i nije izvedivo elementarnim metodama. Slobodno googlate malo na tu temu ako Vas zanima. :)

Ovaj zadatak je postavljen kao primjer "otvorenog problema", da malo simuliramo nešto manje slično natjecateljskim zadacima, a puno sličnije matematici kao znanosti. Uobičajeno je susresti nešto naoko rješivo, neko vrijeme neuspješno pokušavati rješavati, zatim se upustiti u googlanje i malo pomalo čitati o sve kompleksnijim metodama i razgranati se u puno smjerova...

Uglavnom, isprike ako je čitatelju uzelo puno vremena koje bi ipak radije utrošio na nešto natjecateljsko umjesto na simulaciju znanosti, ali ideja je bila pružiti i kratak drukčiji pogled na matematiku. :)

4 Teži lanac

10. **Zadatak:** Neka su a_n i b_n prirodni brojevi definirani tako da vrijedi

$$a_n + b_n\sqrt{2} = (1+\sqrt{2})^n,$$

za sve $n \geq 1$. Dokažite da za svaki n vrijedi $M(a_n, b_n) = 1$.

Rješenje: Vrijedi $a_1 = b_1 = 1$. Također, imamo

$$a_n + b_n\sqrt{2} = (a_{n-1} + b_{n-1}\sqrt{2})(1+\sqrt{2}) = a_{n-1} + 2b_{n-1} + \sqrt{2}(a_{n-1} + b_{n-1}),$$

odakle slijedi $a_n = a_{n-1} + 2b_{n-1}$ i $b_n = a_{n-1} + b_{n-1}$.

Sada možemo dokazati tvrdnju induktivno. Za bazu uzmimo $n = 1$ – tu tvrdnja očito vrijedi. Sada pretpostavimo da tvrdnja vrijedi za a_{n-1}, b_{n-1}, tj. da vrijedi $\mathrm{M}(a_{n-1}, b_{n-1}) = 1$. Pomoću Euklidovog algoritma dobivamo

$$\begin{aligned}
\mathrm{M}(a_n, b_n) &= \mathrm{M}(a_{n-1} + 2b_{n-1}, a_{n-1} + b_{n-1}) \\
&= \mathrm{M}(a_{n-1} + 2b_{n-1} - a_{n-1} - b_{n-1}, a_{n-1} + b_{n-1}) \\
&= \mathrm{M}(b_{n-1}, a_{n-1} + b_{n-1}) \\
&= \mathrm{M}(b_{n-1}, a_{n-1} + b_{n-1} - b_{n-1}) \\
&= \mathrm{M}(a_{n-1}, b_{n-1}) = 1,
\end{aligned}$$

čime je tvrdnja dokazana.

11. **Zadatak:** Nađite sve prirodne brojeve m, n te proste brojeve $p \geq 5$ takve da vrijedi

$$m(4m^2 + m + 12) = 3(p^n - 1).$$

Rješenje: Sređivanjem početne jednadžbe dobijamo

$$3p^n = 4m^3 + m^2 + 12m + 3 = (m^2 + 3)(4m + 1).$$

Nadalje, m je prirodan broj pa vrijedi $m^2+3 \geq 4$ i $4m+1 \geq 5$, što implicira da p dijeli oba ta izraza, jer ne mogu biti samo 1 ili 3. Iz tog razloga, p dijeli i najveći zajednički djelitelj od m^2+3 i $4m+1$. Iskoristimo sada Euklidov algoritam:

$$\begin{aligned} M(m^2+3, 4m+1) &= M(4m^2+12, 4m+1) \\ &= M(4m^2+12-m(4m+1), 4m+1) \\ &= M(12-m, 4m+1) \\ &= M(48-4m, 4m+1) \\ &= M(48-4m+4m+1, 4m+1) = M(49, 4m+1) \mid 49 \end{aligned}$$

Pritom smo u raspisu opet koristili svojstvo iz ranijih zadataka prema kojem smo smjeli množiti lijevi član s 4 bez da promijenimo vrijednost najvećeg zajedničkog djelitelja jer 4 ne dijeli $4m+1$ ni zakoji m. Zaključujemo da $p \mid 49$, što pak znači da je $p = 49$.

Budući da je raspisom dobiveno da je $M(m^2+3, 4m+1)$ djelitelj od 49, a pokazali smo ranije da ti brojevi nisu relativno prosti, jedine su mogućnosti 7 i 49. To znači da jedan od brojeva m^2+3 i $4m+1$ mora poprimati neku od vrijednosti iz skupa $\{7, 3\cdot 7, 49, 3\cdot 49\}$. Dobivamo slučajeve:

(a) $m^2+3 = 7 \implies m = 2 \implies 4m+1 = 9$, što nije oblika $3 \cdot 7^{n-1}$

(b) $m^2+3 = 3\cdot 7 \implies m^2 = 18 \implies m \notin \mathbb{N}$

(c) $m^2+3 = 49 \implies m \notin \mathbb{N}$

(d) $m^2+3 = 3\cdot 49 \implies m = 12 \implies 4m+1 = 49 = 7^{n-2} \implies n = 4$

(e) $4m+1 = 7 \implies n \notin \mathbb{N}$

(f) $4m+1 = 3\cdot 7 \implies m = 5 \implies m^2+3 = 28$, što nije oblika $3 \cdot 7^{n-1}$

(g) $4m+1 = 49 \implies$ slučaj (d)

(h) $4m+1 = 3\cdot 49 \implies m \notin \mathbb{N}$

Dakle, jedino rješenje je $(m, n, p) = (4, 12, 7)$.