



Diofantske jednadžbe

Okvirna razina: JBMO / SŠ A var. državno

1. Teorija i primjeri

U prošlim lekcijama o diofantskim jednažbama prošli smo elementarne strategije rješavanja, te najčešće izolirane (u svakom zadatku primijenili bismo samo jednu metodu). U ovoj lekciji pokazat ćemo kako kompleksnije zadatke rješavamo kombiniranjem svih naučenih metoda. Na kraju ćemo pokazati i neke napredne rezultate iz teorije brojeva.

Počnimo s uvodnim primjerom koji se pojavio kao treći zadatak na županijskom natjecanju iz matematike 2024. za treći razred (A varijanta).

Primjer 1

Odredi sve prirodne brojeve a, b, c takve da je $2^a + 2^b + 2^c + 3$ potpun kvadrat.

Rješenje. Bez smanjenja općenitosti ćemo pretpostaviti da je $a \leq b \leq c$, budući da je izraz simetričan u varijablama a, b i c .

Promotrimo prvo izraz modulo 4. Ako je $a \geq 2$, tada su sve potencije broja 2 dijeljive s 4, pa izraz $2^a + 2^b + 2^c + 3$ daje ostatak 3 pri dijeljenju s 4 i stoga ne može biti kvadrat prirodnog broja. Dakle, mora biti $a = 1$.

Promotrimo sada izraz modulo 8. Slično zaključujemo da ako su b i c veći ili jednaki 3, tada izraz $2^a + 2^b + 2^c + 3 = 2^b + 2^c + 5$ daje ostatak 5 pri dijeljenju s 8 pa zbog toga ne može biti kvadrat prirodnog broja. Dakle, zaključujemo da je $b = 1$ ili $b = 2$. Provjerimo svaki od tih slučajeva zasebno.

Ako je $b = 1$, tada $2^a + 2^b + 2^c + 3 = 2^c + 7$ mora biti potpuni kvadrat. Promatrajući izraz modulo 4, zaključujemo da je nužno $c = 1$, jer bi inače izraz davao ostatak 3 pri dijeljenju s 4. Direktnom provjerom vidimo da za $c = 1$ dobivamo rješenje: $2^1 + 2^1 + 2^1 + 3 = 9$.

Ako je $b = 2$, tada $2^a + 2^b + 2^c + 3 = 2^c + 9$ mora biti potpuni kvadrat, tj. $2^c + 9 = m^2$ za neki prirodni broj m . Koristeći razliku kvadata, jednadžbu zapišimo kao

$$2^c = k^2 - 9 = (m - 3)(m + 3).$$

Iz gornje jednakosti slijedi da su $m - 3$ i $m + 3$ potencije od 2, tj. $m - 3 = 2^{c_1}$ i $m + 3 = 2^{c_2}$ pri čemu su c_1 i c_2 neki nenegativni cijeli brojevi.

Oduzimanjem dobivenih jednakosti slijedi

$$6 = 2^{c_2} - 2^{c_1} = 2^{c_1}(2^{c_2 - c_1} - 1)$$

iz čega zaključujemo da je $c_1 = 1$ i $c_2 = 3$, odnosno $c = 4$ i $m = 5$.

Dakle, uz pretpostavku $a \leq b \leq c$ imamo da su rješenja $(a, b, c) = (1, 1, 1), (1, 2, 4)$.

Sve moguće trojke brojeva (a, b, c) dobivamo permutiranjem dobivenih rješenja:

$$(a, b, c) = (1, 1, 1), (1, 2, 4), (1, 4, 2), (2, 1, 4), (2, 4, 1), (4, 1, 2), (4, 2, 1). \quad \square$$

Tehnika rješavanja koju smo primijenili u ovom zadatku nije rijetkost. Prvo smo promotрили jednadžbu modulo neki konkretni prirodan broj M (nekoliko puta) kako bismo saznali više informacija o nepoznanicama u zadatku, a u nekom trenutku to smo iskoristili kako bismo jednadžbu faktorizirali i napravili analizu faktora. Analiza faktora često vodi na provjeru nekoliko slučajeva, kojih može biti mnogo ako nismo pažljivi, te koji mogu ponovno biti podjednako kompleksni kao i originalni zadatak s kojim smo krenuli. Primijenili smo dvije metode: modularna aritmetika i faktorizacija.

Napomena: Kako birati module?

Kako bismo ubrzali proces ili uopće došli do zaključaka koji bi nam bili korisni za rješavanje zadataka, treba znati koje module uopće izabrati, tj. koje ostatke prilikom dijeljenja kojim brojem M treba promatrati. Postoje neka nepisana pravila:

- Brojevi koji se već pojavljuju u jednadžbama – ako već imamo neki broj u jednadžbi, ili ako vidimo da će nekoliko sumanada zbog tog broja biti djeljivo nekim brojem M , to za preostale članove u jednadžbi znači da imamo manje slučajeva za gledati ako gledamo jednadžbu modulo M .
- Ako u jednadžbi imamo izraze oblika $2^a, 3^b, \dots$ – u tim slučajevima, može biti korisno jednadžbu modulo 2 ili 3 redom, u vidu prošle natuknice, a možemo gledati i modulo 4 ili 8, te 9 redom, nadajući se da ćemo moći zaključiti da za a veće od 2 ili 3, odnosno za b veće od 2 jednadžba nema rješenja.
- Ako u jednadžbi imamo potpun kvadrat – u tim slučajevima korisni su moduli 3, 4, a onda i 5 i 8 (znaš li koji su kvadratni ostatci modulo 3, 4, 5 i 8, te kako se traže svi mogući kvadratni ostatci modulo M ?).
- Ako u jednadžbi imamo potpun kub – u tim slučajevima može biti korisno gledati jednadžbu modulo 7. To je posljedica malog Fermatovog teorema. Općenito, ako se u jednadžbi pojavljuje potencija a^k za neki fiksni broj k , ima smisla pogledati jednadžbu modulo $k + 1$ (ako je $k + 1$ prost) ili $2k + 1$ (ako je $2k + 1$ prost broj), jer će u tim slučajevima izraz a^k davati mali skup ostataka prilikom dijeljenja tim brojem. Recimo, ako se u jednadžbi pojavljuju devete potencije, isplati se gledati modulo $2 \cdot 9 + 1 = 19$.

Napomena: Što raditi nakon faktorizacije

Kada faktoriziramo neki izraz (najčešće koristeći razliku kvadrata ili nekih drugih potencija), dobivamo da je umnožak dviju zagrada koje su nam i dalje nepoznate jer ovise o nepoznicama jednak nekoj vrijednosti K . Najčešće situacije su sljedeće:

- Ta vrijednost K je neki fiksni prirodni broj (recimo $(2^a - 3)(2^a + 3) = 65$ – takva situacija je najlakša. Koristimo rastav na proste faktore tog poznatog broja K (u ovom slučaju $65 = 5 \cdot 13$) te rastavljamo na sve moguće slučajeve kada je koji od faktora s lijeve strane jednak svakom mogućem djelitelju broja K . Ne smijemo zaboraviti i mogućnost da izrazi na lijevoj strani možda mogu biti i negativni. U ograničavanju broja slučajeva korisno je pokušati dokazati da je jedan od nepoznatih faktora uvijek veći od drugog. Konkrentno, u ovoj situaciji znamo da je $2^a + 3 > 2^a - 3$ za sve a , te $2^a + 3 > 0$, pa je potrebno gledati rastave broja 65 na pozitivne faktore, pri čemu je prvi manji od drugog, odnosno slučajeve $(2^a - 3, 2^a + 3) = (1, 65)$ ili $(5, 13)$.
- Ta vrijednost K nepoznata je potencija poznatog broja (ili neki slični umnožak takvih izraza) – to je situacija iz prošlog primjera kada smo imali $2^c = k^2 - 9 = (m - 3)(m + 3)$. Tada je svaki od faktora jednak potenciji istog broja. Ponekad je korisno gledati i najveći zajednički djelitelj, o čemu više u sljedećoj natuknici.
- Ta vrijednost K nepoznata je potencija poznatog broja (ili neki slični umnožak takvih izraza) – to je jedna od najkompliciranijih situacija (recimo $(5^b - 4)(5^b + 4) = m^2$). Tada je ključno promatrati najveći zajednički djelitelj faktora s lijeve strane. U ovom primjeru, uvedimo $d = D(5^b - 4, 5^b + 4)$. Kako d dijeli oba izraza, dijeli i njihovu razliku $(5^b + 4) - (5^b - 4) = 8$. Međutim, izrazi u zagradama su očito neparni, pa je jedino moguće da je $d = 1$. U tom slučaju umnožak relativno prostih brojeva može biti potpun kvadrat samo ako je svaki od njih jednak potpunom kvadratu (vidjeti lemu u nastavku): $5^b + 4 = k^2$ i $5^b - 4 = l^2$. Sada bismo oduzeli te dvije jednakosti i dobili faktorizaciju s konstantnom desnom stranom, dakle nešto što smo komentirali u prvoj natuknici.

Zadatak 1. Riješi do kraja primjere zadataka iz gornje napomene.

Uputa. Postupi kao što je najavljeno u napomeni. □

Rješenje. Za jednadžbu $(2^a - 3)(2^a + 3) = 65$ već smo u tekstu napomene spomenuli sve moguće slučajeve. Za opciju $2^a - 3 = 1$, $2^a + 3 = 65$ oduzimanjem dobivamo $6 = 64$, što daje kontradikciju, dok za opciju $2^a - 3 = 5$, $2^a + 3 = 13$ rješavanjem svake od jednadžbi daje rješenje $a = 3$.

Za jednadžbu $(5^b - 4)(5^b + 4) = m^2$ smo zaključili da je nužno $5^b - 4 = l^2$, $5^b + 4 = k^2$, gdje su k i l prirodni brojevi. Oduzimanjem dobivamo $8 = k^2 - l^2 = (k - l)(k + l)$. Očito je $k + l > k - l$, pa je potrebno gledati faktorizacije oblika $k - l = 1$ i $k + l = 8$ (koja ne daje rješenje), te $k - l = 2$ i $k + l = 4$, odakle je $k = 3$, $l = 1$. Zato je $m = k \cdot l = 3$, $b = 1$. □

Lema 1

Ako za dva relativno prosta prirodna broja x, y vrijedi $x \cdot y = n^m$ (gdje su $n, m \in \mathbb{N}$), tada je svaki od tih brojeva m -ta potencija nekog prirodnog broja.

Zadatak 2. Dokaži ovu lemu.

Uputa. Pogledaj rastav na proste faktore broja n (pa onda i n^m). Može li neki prosti djelitelj od n sudjelovati u raspisu oba broja x i y ? □

Rješenje. Neka je $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. U jednakosti

$$x \cdot y = n^m = p_1^{m\alpha_1} \dots p_k^{m\alpha_k}$$

promotrimo djeljivost faktorom p_1 . Kada bi p_1 dijelio i x i y , tada oni ne bi bili relativno prosti. Zato je samo jedan od njih djeljiv s p_1 , pa zato u svom raspisu na proste faktore imaju cijeli $p_1^{m\alpha_1}$. Analogni zaključak ponavljamo za sve faktore.

Uz potencijalnu zamjenu indeksa prostih brojeva $p_1, \dots, p_k$ i njihovih eskponenata $\alpha_1, \dots, \alpha_k$, dokazali smo da postoji $l \in \{0, 1, \dots, k\}$ takav da je

$$x = p_1^{m\alpha_1} \dots p_l^{m\alpha_l} = (p_1^{\alpha_1} \dots p_l^{\alpha_l})^m, \quad y = p_{l+1}^{m\alpha_{l+1}} \dots p_k^{m\alpha_k} = (p_{l+1}^{\alpha_{l+1}} \dots p_k^{\alpha_k})^m,$$

odnosno x i y su m -ta potencija prirodnog broja, što je i trebalo dokazati. □

U vidu ovih napomena, promotrimo sljedeći primjer.

Primjer 2

Riješi jednadžbu $3^a + 4^b = 5^c$ u skupu prirodnih brojeva.

Rješenje. Motivirani gornjim napomenama, jednadžbu prvo napadamo promatrajući ju modulo neki M . Kako se pojavljuju potencije broja 3, 4 i 5, upravo su to moduli koji nam prvi padaju na pamet prilikom rješavanja.

Promotrimo jednadžbu modulo 3. Izraz 3^a djeljiv je s 3, 4^b uvijek daje ostatak 1, dok 5^c daje ostatak 1 ili 2. Jednadžba će imati rješenja tek ako $5^c \equiv 1 \pmod{3}$ što se ostvaruje za parne c . Dakle, $c = 2k$, za neki $k \in \mathbb{N}$.

Možemo dalje provoditi modularnu aritmetiku i zaista ćemo imati nove zaključke o varijablama a , b i c , međutim već ovaj zaključak dovoljan nam je za faktorizaciju. Primjećujemo da su 5^{2k} i $4^b = 2^{2b}$ potpuni kvadrati, pa ih možemo prebaciti na istu stranu i iskoristiti razliku kvadrata:

$$(5^k - 2^b)(5^k + 2^b) = 3^a.$$

Svaki od faktora na lijevoj strani mora biti potencija broja 3. Dakle, postoje nenegativni cijeli brojevi a_1 i a_2 takvi da je $5^k - 2^b = 3^{a_1}$ i $5^k + 2^b = 3^{a_2}$. U ovom trenutku najčešće se fokusiramo na jednu od tih jednakosti, ili ih oduzmemo/zbrojimo. Oduzimanjem ove dvije jednakosti dobivamo

$$2^{b+1} = (5^k + 2^b) - (5^k - 2^b) = 3^{a_2} - 3^{a_1} = 3^{a_1}(3^{a_2-a_1} - 1).$$

Izraz s lijeve strane nije djeljiv s 3, zbog čega je nužno $a_1 = 0$. Odavde dobivamo

$$2^{b+1} = 3^{a_2} - 1.$$

Ovu jednakost ponovno promatramo kao mali zadatak: ponovno primijenjujemo tehnike modularne aritmetike, a ako ne dobijemo sva rješenja ili kontradikciju, faktoriziramo i nastavljamo. Promotrimo jednadžbu modulo 4. Kako je b prirodan, lijeva strana djeljiva je s 4, pa mora biti

i desna, što je moguće samo ako je a_2 paran broj: $a_2 = 2l$, $l \in \mathbb{N}$. Ovo je ponovno dovoljno za faktorizaciju: na desnoj strani jednakosti nalazi se razlika kvadrata. Imamo

$$(3^l - 1)(3^l + 1) = 2^{b+1}.$$

Faktori s lijeve strane opet moraju biti potencije koja se pojavljuje na desnoj strani: $3^l - 1 = 2^{b_1}$ i $3^l + 1 = 2^{b_2}$ za neke nenegativne brojeve b_1 i b_2 . Oduzimanjem dobivamo

$$2 = (3^l + 1) - (3^l - 1) = 2^{b_1}(2^{b_2-b_1} - 1).$$

Kako na desnoj strani imamo umnožak potencije broja 2 i neparnog broja, jedina mogućnost je $2^{b_1} = 2^1$ i $2^{b_2-b_1} - 1 = 1$. To vodi na sljedeći niz zaključaka: $b_1 = 1$, $b_2 = 2$, $b = 2$, $l = 1$, $a_2 = 2$, $a = 2$, $k = 1$, $c = 2$.

Konačno, jedino rješenje u prirodnim brojevima je $(a, b, c) = (2, 2, 2)$. □

Kao što smo najavili da bi se moglo dogoditi, slučaj na koji smo sveli zadatak bila je jednadžba oblika

$$2^B = 3^A - 1$$

za neke prirodne brojeve A i B , što smo opet rješavali kao zasebni zadatak. Tu se očituje kompleksnost ovakvih zadataka: pored intuicije oko izbora odgovarajućih modula na početku, ograničavanje broja slučajeva i baratanje njima nakon faktorizacije, bitna je i upornost u rješavanju svakog od podslučaja, makar oni značili i rješavanje novih malih zadataka.

Na ovoj novodobivenoj jednadžbi pokazat ćemo i tri složenije metode rješavanja diofantskih jednadžbi. Kao što smo vidjeli, cijeli zadatak riješili smo samo elementarnim metodama, tako da nam metode koje ćemo pokazati nisu potrebne, ali je dobar trenutak za pokazati sve metode na jednom primjeru.

Teorem 2: Zsigmondyjev teorem

Neka su $a > b > 0$ relativno prosti prirodni brojevi. Tada za svaki prirodan broj $n > 1$ postoji barem jedan prost broj p koji dijeli izraz $a^n - b^n$, ali ne dijeli niti jedan izraz oblika $a^k - b^k$ za sve $1 \leq k < n$, uz sljedeće izuzetke:

- kada je $n = 2$ i $a + b$ je potencija broja 2;
- kada je $n = 6$, $a = 2$ i $b = 1$ (odnosno $2^6 - 1^6 = 63$).

Analogna tvrdnja vrijedi i u slučaju zbroya $a^n + b^n$. Ako su $a > b > 0$ relativno prosti, tada za svaki $n > 1$ postoji barem jedan prost broj p koji dijeli $a^n + b^n$, ali ne dijeli $a^k + b^k$ za sve $k < n$, uz jedini izuzetak: $2^3 + 1^3 = 9$.

Recimo, brojevi oblika $11^n - 8^n$ za svaki prirodni broj n imat će neki prosti faktor za koji nijedan drugi izraz $11^k - 8^k$ za $k < n$ nije imao. Posebno, $11^n - 8^n$ ne može biti potencija broja 3 za $n > 1$, jer će svaki put imati neki prosti faktor različit od 3. Slično vrijedi i za $a^n + b^n$.

Postoje iznimke koje su popisane u teoremu. Broj $a^2 - b^2 = (a - b)(a + b)$ nema novih prostih faktora u odnosu na $a - b$ ako je $a + b$ potencija broja 2, dok $2^6 - 1 = 63 = 3^2 \cdot 7$ ima proste faktore 3 koji već dijeli $2^2 - 1$ i 7 koji već dijeli $2^3 - 1$.

Primijenimo Zsigmondyjev teorem na jednadžbi $2^B = 3^A - 1$. Na desnoj strani jednadžbe nalazi se razlika A -tih potencija. Stoga, prema tom teoremu, za svaki $A > 1$ (do na moguće iznimke spomenute u teoremu) postoji neki prost p djelitelj koji ne dijeli $3^k - 1$ ni za koji $k < A$, pa posebno ni $3^1 - 1 = 2$. Dakle, za sve $A > 1$ izraz $3^A - 1$ ima neki neparni prosti djelitelj, pa ne može biti jednak potenciji broja 2. Jedina moguća iznimka je $A = 2$, jer je $3 + 1 = 4$ potencija broja 2, pa zato slučajeve $A = 1$ i $A = 2$ treba provjeriti zasebno. U tim slučajevim zaista i dobivamo rješenja: $(A, B) = (1, 1), (2, 3)$.

Pokažimo sada drugi jaki rezultat. Za to nam je potrebna sljedeća definicija:

Definicija 3

Neka je p prost broj i n cijeli broj različit od nule. Oznakom $v_p(n)$ definiramo najveći prirodni broj k za koji vrijedi da p^k dijeli n (posebno, p^{k+1} ne dijeli n). U tom slučaju često koristimo i zapis $p^k \parallel n$, što čitamo kao da p^k točno dijeli n .

Teorem 4: Lifting The Exponent Lemma - LTE

Neka je p prost broj te neka su a i b cijeli brojevi takvi da p ne dijeli niti a niti b .

- Ako $p \nmid n$ i $p \mid a - b$, tada za svaki prirodni broj n vrijedi

$$v_p(a^n + b^n) = v_p(a + b).$$

- Ako $p \nmid n$ i $p \mid a + b$, tada za svaki **neparni** prirodni broj n vrijedi

$$v_p(a^n + b^n) = v_p(a + b).$$

- Ako $p \mid a + b$, tada za svaki **neparni** prirodni broj n vrijedi

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n).$$

- Ako je $p > 2$ i $p \mid a - b$, tada za svaki prirodni n vrijedi

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

- Ako je $p = 2$ i 4 dijeli $a - b$, tada za svaki prirodni n vrijedi:

$$v_2(a^n - b^n) = v_2(a - b) + v_2(n).$$

- Ako je $p = 2$ i 2 dijeli $a - b$, tada za svaki **parni** prirodni n vrijedi:

$$v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1.$$

Više o teoriji možeš pročitati u tekstu *Lifting The Exponent Lemma* Amira Hosseina Parvardija [1]. Iskaz je najlakše pamtljiv za $p > 2$, dok za $p = 2$ ima dosta specifičnih iskaza. Prilikom primjene ove teorije bitno je ne zaboraviti provjeriti uvjete: $p \mid a \pm b$, ali $p \nmid a$, $p \nmid b$.

Primijenimo LTE na jednadžbi $2^B = 3^A - 1$. Primijenjujemo ga za $p = 2$, $a = 3$, $b = 1$. Kako je $3 - 1$ djeljivo s 2, ali ne s 4, zaključujemo da za parne A vrijedi (zadnji slučaj)

$$B = v_2(2^B) = v_2(3^A - 1) = v_2(3 - 1) + v_2(3 + 1) + v_2(A) - 1 = v_2(A) + 2,$$

dok za neparne A vrijedi (prvi slučaj)

$$B = v_2(2^B) = v_2(3^A - 1) = v_2(3 - 1) = 1.$$

Ako je A neparan, moguće je samo $B = 1$, što vodi na rješenje $(A, B) = (1, 1)$. Ako je A paran, tada relacija $v_2(A) + 2 = B$, odnosno $v_2(A) = B - 2$ povlači da je A djeljiv s 2^{B-2} , odakle je posebno $A \geq 2^{B-2}$. Označimo $m := 2^{B-2}$. Imamo

$$4m = 2^B = 3^A - 1 \geq 3^{2^{B-A}} - 1 = 3^m - 1.$$

Međutim, indukcijom se lako pokaže da vrijedi $3^m > 4m + 1$ za sve prirodne brojeve $m \geq 3$. Stoga ova jednadžba može imati rješenja samo za $2^{B-2} = m \leq 2$, odnosno $B \leq 3$. Direktnom provjerom malih slučajeva, dobivamo ista rješenja kao kad smo rješavali zadatak drugačijim metodama.

Od tri napredne metode koje pokazujemo ova je najviše tehnička. Potrebno je pamtit i mnogo posebnih iskaza u svakom od slučajeva, te je potrebno ograničavati nepoznanice na netrivialan način. Prava moć ove tehnike ne očituje se u ovom zadatku, nego u zadacima u kojima nijedna druga tehnika osim ove u pravilu ne prolazi.

Zadnje, pokažimo najkraći, naspecifičniji i najjači teorem od ova tri.

Teorem 5: Mihăilescuov teorem / Catalanova slutnja

Neka su x, y, a, b prirodni brojevi takvi da su svi veći od 1. Jednadžba oblika

$$x^a - y^b = 1$$

ima točno jedno jedinstveno rješenje u skupu prirodnih brojeva. To rješenje je dano četvorkom $(x, a, y, b) = (3, 2, 2, 3)$, što odgovara jednakosti $3^2 - 2^3 = 9 - 8 = 1$.

Prema tom teoremu, jednadžba $2^A = 3^B - 1$ (odnosno $3^B - 2^A = 1$) može imati rješenja samo u iznimci navedenoj u teoremu ($9 - 8 = 1$) ili slučajevima kada je $B = 1$ ili $A = 1$. Direktno dobivamo rješenja kao i prije: $(A, B) = (1, 1), (2, 3)$.

Ovu je tvrdnju prvi postavio Eugène Charles Catalan 1844. godine, ali je ostala nedokazana više od stoljeća i pol. Tek ju je 2002. godine dokazao rumunjski matematičar Preda Mihăilescu. Zato ćeš u literaturi moći naći mnogo zadataka koji se mogu vrlo brzo svesti na ovaj teorem. Od kad je dokazan teorem, sastavljači zadataka postali su mnogo oprezniji pa se sada ovaj teorem u pravilu primjenjuje tek u ograničavanju jednog od više slučajeva na koji se zadatak grana.

Pokazali smo tri napredna teorema, međutim njih ne treba smatrati čarobnim štapićem koji mijenjaju način na koji inače rješavamo zadatke, nego samo nadogradnju elementarnih metoda. Vratimo se unazad, te pokažimo razmišljanja elementarnim metodama (modularna aritmetika i faktORIZACIJA) na još jednom primjeru. Radi se o četvrtom zadatku prvog dana Hrvatske matematičke olimpijade 2018. godine.

Primjer 3

Odredi sve prirodne brojeve a i m takve da je $2^m = 7n^2 + 1$.

Rješenje. Promatrajmo jednadžbu modulo 7. Ostatak desne strane pri dijeljenju sa 7 mora biti 1, a to se događa samo kada je m višekratnik broja 3. Dakle, postoji prirodan broj k takav da je $m = 3k$. Iskoristimo to tako da prebacimo 1 na lijevu stranu jednadžbe i faktoriziramo koristeći razliku kubova:

$$(2^k - 1)(2^{2k} + 2^k + 1) = 7n^2.$$

Najveća zajednička mjera faktora na lijevoj strani jednadžbe nužno je 1 ili 3. Da bismo to dokazali, uz pretpostavku da $d \mid 2^k - 1$ i $d \mid 2^{2k} + 2^k + 1$, dobivamo $2^k \equiv 1 \pmod{d}$, pa je $0 \equiv 2^{2k} + 2^k + 1 \equiv 3 \pmod{d}$. To je moguće samo ako $d \mid 3$.

Zastanimo na tren da vidimo kako bismo precizno iskoristili Lemu 1. Jednadžba koju smo dobili na apstraktan način kaže $A \cdot B = 7n^2$. Ako su faktori A i B relativno prosti, tada je točno jedan od njih djeljiv sa 7. Kada to iskoristimo, zaključujemo da imamo dva moguća rastava kvadrata broja n na umnožak dva faktora: $n^2 = (A/7) \cdot B$ ili $n^2 = A \cdot (B/7)$. Prema lemi, faktori s desne strane su potpuni kvadrati. Dobivamo prva dva slučaja: $A = 7x^2, B = y^2$ ili $A = x^2, B = 7y^2$. Ako je pak najveći zajednički djelitelj jednak 3, tada i $3 \mid n$, odnosno $n = 3n'$, pa iz zapisa $n'^2 = (A/21) \cdot (B/3)$ i $n'^2 = (A/3) \cdot (B/21)$ dolazimo do analognih zaključaka. Dobivamo 4 slučaja (rastav na te slučajeve inače nećemo ovako precizno dokazivati):

1. $2^k - 1 = 21a^2, 2^{2k} + 2^k + 1 = 3b^2$. Promatrajmo drugu jednadžbu modulo 4. Za $k \geq 2$, lijeva strana daje ostatak 1, dok je desna strana modulo 4 uvijek jednaka 0 ili 3. Stoga k mora biti 1. Međutim, za $k = 1$, prva jednadžba nema rješenja.
2. $2^k - 1 = a^2, 2^{2k} + 2^k + 1 = 7b^2$. Slično prethodnom slučaju, promatranjem ostatka pri dijeljenju sa 4 u drugoj jednadžbi, zaključujemo da je $k = 1$. To daje $b = 1$, a prva jednadžba povlači $a = 1$. Time dobivamo rješenje $(m, n) = (3, 1)$. Primijeti da smo slučaj mogli riješiti i primjenom Mihailescuovog teorema na prvu jednakost.
3. $2^k - 1 = 3a^2, 2^{2k} + 2^k + 1 = 21b^2$. Promatrajmo prvu jednadžbu modulo 3. Desna strana je djeljiva s 3, a lijeva strana je djeljiva s 3 samo ako je k paran. Dakle, postoji prirodan broj l takav da je $k = 2l$. Možemo iskoristiti razliku kvadrata: $(2^l - 1)(2^l + 1) = 3a^2$. Razlika između (neparnih) faktora na lijevoj strani je 2, pa oni moraju biti relativno prosti. Budući da je njihov umnožak jednak $3a^2$, imamo dva podslučaja: $2^l + 1 = x^2$ ili $2^l - 1 = x^2$. Svaki od njih možemo opet riješiti Mihailescuovim teoremom (jedino su moguća trivijalna rješenja za $l = 1$ ili $x = 1$), ili nastavljamo elementarnim metodama. U prvom slučaju možemo faktorizirati jednadžbu: $2^l = (x - 1)(x + 1)$. Faktori na desnoj strani su iste parnosti, oba su potencije broja 2 i razlikuju se za 2. To znači da je njihova najveća zajednička mjera 2, pa manji faktor nužno mora biti jednak 2. To daje rješenje $l = 3$, pa je $k = 6$. Međutim, ne postoji b koji zadovoljava jednadžbu $2^{2k} + 2^k + 1 = 21b^2$ za $k = 6$. U drugom slučaju ($2^l - 1 = x^2$), promatramo jednadžbu modulo 4 i zaključujemo da je jedina mogućnost $l = 1$. To daje $k = 2$ i rješenje $(m, n) = (6, 3)$.
4. $2^k - 1 = 7a^2, 2^{2k} + 2^k + 1 = b^2$. Posljednji slučaj može se riješiti na barem dva načina. Za prvi način se podsjećamo još jedne metode rješavanja diofantskih jednadžbi: smještanje

među kvadrate. Ako neki izraz za koji je nužno da je potpun kvadrat dokažemo da se nalazi između dva uzastopna potpuna kvadrata, tada ne može biti potpun kvadrat. Uočimo li da vrijedi

$$(2^k)^2 < 2^{2k} + 2^k + 1 < (2^k + 1)^2,$$

vidimo da se ovaj izraz nalazi između dva uzastopna potpuna kvadrata, te on ne može biti jednak potpunom kvadratu. Drugi način rješavanja je metoda beskonačnog spusta. U toj metodi prepoznavamo da nove nepoznanice zadovoljavaju istu jednadžbu kao onu s kojom smo krenuli, te ako dokažemo da su te nove nepoznanice manje od početnih, možemo doći do kontradikcije. Precizna primjena beskonačnog spusta na ovom primjeru glasi ovako: pretpostavimo da je (m, n) još neko rješenje početne jednadžbe različito od $(3, 1)$ i $(6, 3)$ (cilj nam je pokazati da takvo ne postoji), te ako ih ima više, pretpostavimo da je najmanje moguće, tj. među svim takvim potencijalnim uređenim parovima (m, n) uzmimo onaj za koji je vrijednost varijable m najmanja moguća. Dokazali smo da niti u jednom od preostala tri slučaja nema takvih rješenja (m, n) . Ako imamo rješenje u ovom slučaju, tada je par (k, a) također rješenje početne jednadžbe jer vrijedi $2^k - 1 = 7a^2$. Međutim, tada je $k = m/3 < m$, što znači da smo našli neko rješenje koje je manje od (m, n) . To je moguće samo ako je to jednako nekom već pronađenom rješenju, tj. ako je $(k, a) = (3, 1)$ ili $(6, 3)$. No u tim slučajevima direktno vidimo da druga jednadžba $2^{2k} + 2^k + 1 = b^2$ nema rješenja.

Dakle, sva rješenja za (m, n) su $(3, 1)$ i $(6, 3)$. □

Na kraju slijede mnogi zadatci za samostalnu vježbu. Do na par iznimaka, to su sve zadatci s državnih i županijskih natjecanja iz matematike, te se svi rješavaju na isti način kao što smo pokazali na primjerima iznad: prvo modularna aritmetika, pa faktORIZACIJA i analiza slučajeva. Iako je na natjecanju dozvoljeno koristiti jake teoreme navedene u ovoj lekciji, prilikom rješavanja pokušaj svaki put kada riješiš zadatak tim teoremima razmisliti kako bi riješio zadatak elementarnim metodama kako bi što više vježbao taj način razmišljanja.

Zadaci za samostalnu vježbu

1. Dokaži da ne postoje prirodni brojevi a i b koji zadovoljavaju jednakost

$$3^a - 2^b = 2021.$$

2. Odredi proste brojeve p , q , r i prirodni broj n za koje vrijedi

$$p^2 = q^2 + r^n.$$

Nađi sva rješenja.

3. Odredi najmanju vrijednost koju može poprimiti izraz

$$|8 \cdot 5^m - n^2|$$

pri čemu su m i n prirodni brojevi.

4. Od svih brojeva oblika $36^m - 5^n$, gdje su m i n prirodni brojevi, odredi najmanji po apsolutnoj vrijednosti.

5. Odredi sve trojke prirodnih brojeva (a, b, c) za koje vrijedi

$$2^a + 2021 = 3^b \cdot 25^c.$$

6. Odredi sve prirodne brojeve m i n za koje je $2^n + 5 \cdot 3^m$ kvadrat nekog prirodnog broja.

7. Odredi sve prirodne brojeve m za koje je $2^m - 63$ kub nekog cijelog broja.

8. Odredi sve cijele brojeve x takve da je $1 + 5 \cdot 2^x$ kvadrat racionalnog broja.

9. Odredi sve prirodne brojeve m i n za koje je $6^m + 2^n + 2$ potpun kvadrat.

10. Odredi sve parove prostih brojeva (p, q) za koje je $p^{q-1} + q^{p-1}$ kvadrat prirodnog broja.

11. Odredi sve trojke prirodnih brojeva (a, b, c) za koje vrijedi

$$2^a \cdot 5^b - 1 = 11 \cdot 3^c.$$

12. Postoje li prirodni brojevi k i m takvi da je $2022^k + 2022^m$ kvadrat prirodnog broja?

13. Odredi sve trojke prirodnih brojeva (p, m, n) takve da je p prost broj i da vrijedi

$$2^m p^2 + 1 = n^5.$$

14. Nađi sve trojke prirodnih brojeva (m, n, k) takve da vrijedi $3^m + 7^n = k^2$.

15. Odredi sve parove (n, k) prirodnih brojeva za koje vrijedi

$$3^n = 5k^2 + 1.$$

16. Odredi sve parove (m, n) prirodnih brojeva za koje vrijedi

$$5^n = 6m^2 + 1.$$

Upute za zadatke za samostalnu vježbu

1. Modularnom aritmetikom dokaži da su a i b parni, a onda nakon razlike kvadrata dokaži da ni u kojem slučaju ne dolazimo do rješenja.
2. Dokaži da je barem jedan od prostih brojeva jednak 2 i barem jedan od prostih brojeva jednak 3. Prođi sve slučajeve.
3. Pogodi najmanju vrijednost, promatraj izraz modulo 8, a preostalu vrijednost riješi faktorizacijom.
4. Pogodi rješenje, za sve manje opcije nađi odgovarajući modul s kojim ćeš dobiti kontradikciju, ili traži razliku kvadrata.
5. Dokazuj parnost brojeva a i b koristeći modulo 3 i 4. Napravi razliku kvadrata.
6. Analiziraj jednadžbu modulo 8 i modulo 3, dobit ćeš samo jednu vrijednost za a . Nakon toga razlika kvadrata.
7. Kubovi vole modulo 7. Nakon toga razlika kubova.
8. Razmatraj odvojeno jednadžbu za pozitivne x , negativne parne x i negativne neparne x . Za negativne x namjesti nazivnik izraza na neki broj za koji znaš da je potpuni kvadrat.
9. Proučavaj jednadžbu po modulu 4, tako ćeš dobiti dva glavna slučaja. Jedan svedi na razliku kvadrata, drugi riješi
10. Pokaži da jedan od prostih brojeva nužno mora biti paran analizirajući jednadžbu za slučaj da su oba prosta broja neparna. Posluži se modulom 4.
11. Promatraj jednadžbu po modulu 5, modulu 3 i modulu 8. Zaključi $a = 2$.
12. Izluči manju potenciju. Produkt dva relativno prosta broja može biti potpun kvadrat samo ako su oba potpun kvadrat.
13. Faktoriziraj s jedinicom, gledaj parnost velikog faktora. Za najteži slučaj gledaj modulo 8.
14. Proučavaj parnost brojeva m i n pomoću modula 4. Svaki od slučajeva slično riješi razlikom kvadrata.
15. Gledaj modulo 5 da zaključiš nešto o n , postupi slično kao u zadnjem primjeru iz glavnog dijela predavanja. Mnogo je slučajeva, napravi strategiju kako ćeš ih riješiti.
16. Promatraj jednadžbu po modulu 3 kako bi odredio parnost broja n . Zatim iskoristi razliku kvadrata. Neki od slučajeva riješi jakim teoremom.

Rješenja zadataka za samostalnu vježbu

1. Gledajmo jednadžbu modulo 4. Ako je $b = 1$, ne dobivamo rješenje jer ne postoji a takav da je $3^a = 2021 + 2$. Inače je 2^b djeljivo s 4. Desna strana daje ostatak 1, a i lijeva će tek ako a paran.

Gledajmo sada jednadžbu modulo 3. Desna strana daje ostatak 2 modulo 3. Kako je 3^b djeljivo s 3, lijeva strana će dati ostatak 2 modulo 3 tek ako je b paran.

Uvrštavanjem $a = 2a_1$ i $b = 2b_1$ te razlikom kvadrata dobivamo

$$(3^{a_1} - 2^{b_1})(3^{a_1} + 2^{b_1}) = 2021.$$

Rastav broja 2021 na proste faktore je $2021 = 43 \cdot 47$. Kako su faktori sustava očito pozitivni i $3^{a_1} - 2^{b_1} < 3^{a_1} + 2^{b_1}$, imamo dvije mogućnosti: manji faktor je jednak 1 ili 43. U prvom slučaju je $3^{a_1} - 2^{b_1} = 1$, ($3^{a_1} + 2^{b_1} = 2021$, odakle zbrajanjem dobivamo $2 \cdot 3^{a_1} = 2022$ što nema rješenja. U drugom slučaju je $3^{a_1} - 2^{b_1} = 43$, $3^{a_1} + 2^{b_1} = 47$, odakle zbrajanjem dobivamo $2 \cdot 3^{a_1} = 90$, što opet nema rješenja.

Zaključujemo da takvi prirodni brojevi ne postoje.

2. Pogledajmo jednadžbu modulo 2. Ne mogu svi prosti brojevi biti neparni jer bi tada strane jednakosti bile različite parnosti. Dakle, barem jedan od brojeva p, q, r je jednak 2. Pogledajmo jednadžbu modulo 3. Ako ni p ni q nisu djeljivi s 3, tada kvadrirani daju isti ostatak pri dijeljenju s 3, pa onda 3 mora dijeliti r^n , odakle je $r = 3$.

Ovime smo dokazali da je jedan od brojeva 2 i barem jedan od brojeva 3. Prvo provjerimo slučaj ako je p jednak nekoj od tih vrijednosti. Primijetimo da je $p^2 = q^2 + r^n > q^2$. Zato je trivijalno $p > q$. Iz toga zaključujemo da $p \neq 2$, te u slučaju $p = 3$ je nužno $q = 2$. Dobivamo rješenje $(p, q, r, n) = (3, 2, 5, 1)$.

Preostala su dva slučaja: $(q, r) = (2, 3)$ ili $(q, r) = (3, 2)$. U oba slučaja ćemo napraviti razliku kvadrata. U prvom imamo

$$(p - 2)(p + 2) = 3^n.$$

Razlika faktora s lijeve strane je jednaka 4 što je relativno prosto s 3. Zato manji od faktora mora biti jednak 1. Ali jednakost $p - 2 = 1$ vodi na $p = 3$, što ne daje rješenje. U drugom slučaju imamo

$$(p - 3)(p + 3) = 2^n.$$

Razlika faktora s lijeve strane je jednaka 6. Dakle iste su parnosti, pa da bi u umnošku dali paran broj, svaki od njih mora biti paran. Dodatno, broj 2 im mora biti najveći zajednički djelitelj, pa je nužno manji od faktora jednak 2: $p - 3 = 2$. Odavde je $p = 5$, što vodi rješenju $(p, q, r, n) = (5, 3, 2, 4)$.

Sva rješenja zadatka su četvorke $(p, q, r, n) = (5, 3, 2, 4)$ i $(3, 2, 5, 1)$.

3. Označimo $A = 8 \cdot 5^m - n^2$. Primijećujemo da je $A = 4$ za $m = 1, n = 6$. Dokažimo da ta vrijednost ne može biti manja. Očito ne može biti jednaka nuli (tada bi n^2 bio djeljiv s 8, ali ne i 16). Inače gledamo jednadžbu modulo 8. Desna strana daje ostatke 0, 7i4, stoga da bi postigli $|A| \leq 3$ jedina je mogućnost $A = -1$.

U slučaju $A = -1$ imamo

$$8 \cdot 5^m = n^2 - 1 = (n - 1)(n + 1).$$

Brojevi na desnoj strani razlikuju se za 2 pa svaki od njih mora biti paran kako bi im umnožak bio paran. Sada možemo pisati

$$2 \cdot 5^m = \frac{n-1}{2} \cdot \frac{n+1}{2}.$$

Faktori s desne strane sada su uzastopni prirodni brojevi, pa su relativno prosti. Zato 5^m dijeli jednog od njih, pa mora onog većeg. Za onog manjeg jedine mogućnosti su da je jednak 1 ili 2, no ni u kojem slučaju ne dobivamo rješenje.

Budući da smo eliminirali manje vrijednosti, najmanja moguća vrijednost koju izraz može poprimiti je upravo 4.

4. Za $m = 1$, $n = 2$ vrijednost izraza je 11. Dokažimo da jednačba $36^m - 5^n = A$ nema rješenja za $|A| \leq 10$.

Prvo primijetimo da je A relativno prost s 5 (inače 5 dijeli A i 5^n pa mora dijeliti i 36^m), ali je i iz sličnog razloga relativno prost sa 6. Jedine opcije koje su nam preostale su $A = \pm 1$ i $A = \pm 7$.

Pogledajmo pozornije modulo 5. Kako je $36^m - 5^n \equiv 1 \pmod{5}$, jedina preostala moguća opcija je $A = 1$. Dakle, treba dokazati da $36^m - 5^n = 1$ nema rješenja.

Jedan način je dokazati prema Mihaelescuovom teoremu. Drugi je koristeći razliku kvadrata:

$$5^n = (6^m - 1)(6^m + 1).$$

Faktori na desnoj strani su relativno prosti (jer se razlikuju za 2, a moraju biti neparni), pa je jedino moguće da je manji od njih jednak 1, ali $6^m - 1 = 1$ nema rješenja.

5. Gledajući jednačbu modulo 3, vidimo da je desna strana djeljiva s 3, a lijeva će postati samo ako je a paran. Posebno, $a \geq 2$, pa modulo 4 sada znamo da lijeva strana daje ostatak 1 pri dijeljenju s 4. Kako je $25^c \equiv 1 \pmod{4}$, nužno je b paran. Koristeći $a = 2k$ i $b = 2l$ ($k, l \in \mathbb{N}$), jednačba postaje:

$$2021 = (3^l \cdot 5^c - 2^k)(3^l \cdot 5^c + 2^k).$$

Znamo da je $2021 = 43 \cdot 47$. Kako su faktori s desne strane pozitivni i prva zagrada je manja od druge, postoje dva slučaja: $3^l \cdot 5^c - 2^k = 43$ i $3^l \cdot 5^c + 2^k = 47$, ili $3^l \cdot 5^c - 2^k = 1$ i $3^l \cdot 5^c + 2^k = 2021$. U oba slučaja zbrojimo jednakosti. U prvom slučaju dobivamo $2 \cdot 3^l \cdot 5^c = 90$ odakle je $l = 2$ i $c = 1$. Dobivamo rješenje $(a, b, c) = (2, 4, 1)$. U drugom slučaju zbrajanjem jednakosti dobivamo $2 \cdot 3^l \cdot 5^c = 2022$, što nema rješenja u prirodnim brojevima.

Rješenje je $(a, b, c) = (2, 4, 1)$.

6. Neka je zadana jednačba $2^n + 5 \cdot 3^m = k^2$. Gledajmo izraz modulo 8. Za $n \geq 3$, lijeva strana daje ostatak 7 ili 5, što nije kvadratni ostatak modulo 8, pa je zato $n \leq 2$.

Gledajmo jednačbu modulo 3. Lijeva strana daje ostatak 2 ili 1 modulo 3. Samo je 1 kvadratni ostatak, te će se on ostvariti kada je a paran, odnosno kada je $a = 2$.

Sada primijenimo razliku kvadrata:

$$5 \cdot 3^m = (k - 2)(k + 2).$$

Razlika faktora je 4, što je relativno prosto s lijevom stranom jednakosti, pa faktori moraju biti relativno prosti. To znači da cijela potencija 3^m dijeli neki faktor s desne strane, pa onda

zaključujemo da je onaj drugi faktor jednak 1 ili 5. Imamo 4 slučaja za provjeriti: $k - 2 = 1$, $k - 2 = 5$, $k + 2 = 1$, ili $k + 2 = 5$. Dobivamo vrijednosti $k = 3$ ili $k = 7$. Direktnim uvrštavanjem u početnu jednakost (znamo i $n = 2$) dobivamo jedno rješenje $(n, m) = (2, 2)$.

7. Neka je $2^m - 63 = k^3$, za neki cijeli broj k . Gledajmo izraz modulo 7. Kubovi daju ostatak $-1, 0, 1$ modulo 7 broj 63 djeljiv je sa 7, dok broj 2^m redom daje ostatke 2, 4, 1 modulo 7. Da bi jednakost vrijedila, jedina mogućnost je da svaka strana jednakosti daje ostatak 1 modulo 7, odakle zaključujemo da m mora biti višekratnik broja 3. Neka je stoga $m = 3a$, $a \in \mathbb{N}$. Tada je $2^{3a} - k^3 = 63$, pa koristimo formulu za razliku kubova:

$$(2^a - k)(2^{2a} + 2^a k + k^2) = 63.$$

Druga zagrada uvijek je pozitivna, čak i kad je k negativna, jer je oblika $A^2 + AB + B^2$, pa pozitivnost lako dokažemo koristeći A–G nejednakost. Zato i prvi faktor, $2^a - k$, mora biti strogo pozitivan, a oba faktora su pozitivni djelitelji broja 63. Također, drugi faktor veći je od prvog. Zato su jedine mogućnosti za $2^a - k$ jednake 1, 3 i 7.

Prije uvrštavanja tih slučajeva u drugi faktor, zapišimo ga na drugačiji način. Uvodeći $t = 2^a - k$, imamo $k = 2^a - t$, odakle je

$$2^{2a} + 2^a k + k^2 = 2^{2a} + 2^a(2^a - t) + (2^a - t)^2 = 3 \cdot 2^{2a} - 3 \cdot 2^a \cdot t + t^2.$$

U prvom slučaju je $t = 2^a - k = 1$, pa je $63 = 3 \cdot 2^{2a} - 3 \cdot 2^a + 1$, što nema rješenja (desna strana nije djeljiva s 3). U drugom slučaju je $t = 2^a - k = 3$, pa je $21 = 3 \cdot 2^{2a} - 3 \cdot 2^a \cdot 3 + 9$. Rješavanje kvadratne jednadžbe (gledamo samo pozitivna rješenja) daje $2^a = 4$, odakle je $m = 6$. U trećem slučaju je $t = 2^a - k = 7$, odakle je $9 = 3 \cdot 2^{2a} - 3 \cdot 2^a \cdot 7 + 49$, što opet nema rješenja zbog ostataka modulo 3.

Zato je jedino rješenje $m = 6$.

8. Neka je $1 + 5 \cdot 2^x = q^2$, gdje je q pozitivan racionalan broj. Lako vidimo da za $x = 0$ nema rješenja. Neka je prvo $x > 0$. Tada je q ustvari prirodan broj, pri čemu dodatno mora biti neparan (jer je lijeva strana jednadžbe neparna). Razlikom kvadrata dobivamo

$$5 \cdot 2^x = q^2 - 1 = (q - 1)(q + 1).$$

Kako je q neparan, na desnoj strani nalaze se dva parna prirodna broja, pa možemo pisati i

$$5 \cdot 2^{x-2} = \frac{q-1}{2} \cdot \frac{q+1}{2}.$$

Na desnoj strani sada je umnožak dva uzastopna prirodna broja, pa su oni relativno prosti [zaključak o njihovom najvećem zajedničkom djelitelju mogli smo provesti i bez dijeljenja jednadžbe s 4]. Kako je drugi faktor veći od prvog, imamo tri mogućnosti:

- $\frac{q-1}{2} = 1$, $\frac{q+1}{2} = 5 \cdot 2^{x-2}$: iz prve jednadžbe je $q = 2$, no ne dobivamo rješenje za x ;
- $\frac{q-1}{2} = 5$, $\frac{q+1}{2} = 2^{x-2}$: iz prve jednadžbe je $q = 11$, no opet ne dobivamo rješenje za x ;
- $\frac{q-1}{2} = 2^{x-2}$, $\frac{q+1}{2} = 5$: iz druge jednadžbe je $q = 9$, što u prvoj jednadžbi daje $x = 4$.

Neka je sada x negativni neparni broj: $x = -2k + 1$, $k \in \mathbb{N}$. Tada je $1 + 5 \cdot 2^x = \frac{2^{2k} + 10}{2^{2k}}$ potpun kvadrat ako i samo ako je brojnik potpun kvadrat. Međutim, on daje ostatak 2 daje pri dijeljenju s 4, pa to nije moguće.

Konačno, ako je x negativni parni broj ($x = -2k$, $k \in \mathbb{N}$, tada je $1 + 5 \cdot 2^x = \frac{2^{2k} + 5}{2^{2k}}$ potpun kvadrat ako i samo ako je brojnik potpun kvadrat: $2^{2k} + 5 = m^2$ za neki prirodni broj m . Ovo možemo riješiti faktorizacijom (razlika kvadrata) ili modulo 8: kada je $k \geq 2$, desna strana daje ostatak 5 pri dijeljenju s 8, što je nemoguće za kvadrat prirodnog broja, odakle je nužno $k \leq 1$. To vodi na rješenje $x = -2$.

Sva rješenja su $x = 4, -2$.

9. Neka je zadana jednačba $6^m + 2^n + 2 = k^2$. Gledamo ostatke modulo 4. Kada bi bilo $m \geq 2$ i $n \geq 2$, tada lijeva strana daje ostatak 2 modulo 4 što nije kvadratni ostatak. Time smo dobili kontradikciju s početnom pretpostavkom, zato je nužno $m = 1$ ili $n = 1$.

Neka je prvo $m = 1$. Jednačba postaje $8 + 2^n = k^2$. Broj k je očito nužno paran jer je lijeva strana parna, pa uvedimo $k = 2l$, $l \in \mathbb{N}$ i podijelimo jednačbu s 4: $2 + 2^{n-2} = l^2$. Ponovno gledamo modulo 4. Za $n \geq 4$, desna strana daje ostatak 2 pri dijeljenju s 4, pa u tom slučaju nema rješenja. Direktna provjera za $n \leq 3$ daje jedno rješenje $(m, n) = (1, 3)$.

Neka je sada $n = 1$. Jednačba postaje $6^m + 4 = k^2$. Broj k je ponovno paran, pa uvođenjem $k = 2l$, $l \in \mathbb{N}$ dobivamo $3^m \cdot 2^{m-2} = (l-1)(l+1)$. Za $m = 2$ ne dobivamo rješenje. Inače je lijeva strana parna, pa mora biti i desna. To znači da su $l-1$ i $l+1$ uzastopni parni brojevi, pa im je najveća zajednička mjera jednaka 2. Drugačije zapisano:

$$3^m \cdot 2^{m-4} = \frac{l-1}{2} \cdot \frac{l+1}{2}.$$

Na desnoj strani se nalaze relativno prosti brojevi od kojih je prvi manji od drugog. Jedine mogućnosti su da je $\frac{l-1}{2} = 1$, $\frac{l+1}{2} = 3^m \cdot 2^{m-4}$ ili $\frac{l-1}{2} = 2^{m-4}$, $\frac{l+1}{2} = 3^m$. U prvom slučaju vidimo da za $l = 3$ ne dobivamo rješenje, dok u drugom mora vrijediti $l = 2^{m-3} + 1 = 2 \cdot 3^m - 1$, međutim drugi izraz uvijek je veći od prvog, pa ni ovdje ne dobivamo rješenje.

Jedino rješenje je $(m, n) = (1, 3)$.

10. Neka je $p^{q-1} + q^{p-1} = k^2$. Pretpostavimo da su oba prosta broja neparna. Tada su $p-1$ i $q-1$ parni brojevi, pa je na lijevoj strani zbroj kvadrata neparnih brojeva koji daje ostatak 2 pri dijeljenju s 4, što nije kvadratni ostatak. Dobili smo kontradikciju, stoga je barem jedan od prostih brojeva paran, odnosno jednak 2. Bez smanjenja općenitosti $p = 2$.

Naša jednačba tada postaje $2^{q-1} + q = k^2$. Za $q = 2$, dobivamo jedno rješenje $(p, q) = (2, 2)$. Inače je q neparan broj, pa je $q-1$ paran, pa možemo iskoristiti razliku kvadrata:

$$q = k^2 - (2^{\frac{q-1}{2}})^2 = (k - 2^{\frac{q-1}{2}})(k + 2^{\frac{q-1}{2}}).$$

S obzirom na to da je q prost broj i da je prva zagrada strogo manja od druge, nužno mora vrijediti da je prva zagrada jednaka 1, a druga q . Oduzimanjem jednakosti $k - 2^{\frac{q-1}{2}} = 1$ i $k + 2^{\frac{q-1}{2}} = q$ dobivamo $2^{\frac{q+1}{2}} = q - 1$. Indukcijom možemo dokazati da je za sve prirodne brojeve $q \geq 5$ lijeva strana strogo veća od desne. Zato potencijalno rješenje postoji za još samo $q = 3$, no direktnom provjerom vidimo da to nije rješenje.

Jedino rješenje zadatka je par $(p, q) = (2, 2)$.

11. Gledajući jednadžbu modulo 5, lijeva strana daje ostatak 4, a desna strana daje ostatak 3^c . Jednakost će se postići ako je $c = 4k + 2$ za neki $k \in \mathbb{N}_0$. Posebno c je paran. Gledajući jednadžbu modulo 3, vidimo da je $2^a \cdot 5^b \equiv 2^{a+b} \pmod{3}$, što znači da će taj član dati ostatak 1 pri dijeljenju s 3 tek ako su a i b iste parnosti. Gledajući modulo 8, kako je c paran, desna strana daje ostatak 3 modulo 8. Za $a \geq 3$ imamo da lijeva strana daje ostatak 7 pri dijeljenju s 8, pa ne dobivamo rješenja. Dakle, $a \leq 2$. Za $a = 1$, kako je b neparan (a $5^2 \equiv 1 \pmod{8}$), slijedi $2^a \cdot 5^b \equiv 2 \cdot 5 \equiv 2 \pmod{8}$, pa opet ne dobivamo rješenja. Dakle, nužno je $a = 2$.

Dakle, kako je a paran, paran je i b : $b = 2l$, $l \in \mathbb{N}$. Zato lijevu stranu možemo raspisati koristeći razliku kvadrata:

$$(2 \cdot 5^l - 1)(2 \cdot 5^l + 1) = 11 \cdot 3^c.$$

S lijeve strane imamo umnožak dva neparne broja koji se razlikuju za 2 pa su relativno prosti. Jedine mogućnosti su da je manji od njih jednak 1 (što je nemoguće jer je prvi faktor jednak barem 9) ili da je bilo koji od njih jednak 11. Samo drugi faktor daje ostatak 1 pri dijeljenju s 5 kao i 11, pa je $2 \cdot 5^l + 1 = 11$, odakle je $l = 1$. To vodi na jedino rješenje $(a, b, c) = (2, 2, 2)$.

12. Bez smanjenja općenitosti, pretpostavimo da je $k \leq m$. Jednadžbu pišemo kao:

$$2022^k(1 + 2022^{m-k}) = x^2.$$

Faktori su relativno prosti (pretpostavi da postoji prost broj p koji dijeli oba faktora – kako dijeli i 2022, dijeli i $2022^{m-k} + 1$, pa dijeli i 1). Posebno, vrijednost unutar zagrade je potpun kvadrat.

Uvedimo susptituciju $n = m - k$. Jednadžbu $2022^n = x^2 - 1$ možemo trivijalno riješiti Mihaeles-cuovim teoremom (ni u slučaju $n = 1$ nema rješenja), ili možemo napraviti razliku kvadrata:

$$2^n \cdot 3^n \cdot 337^n = (x - 1)(x + 1).$$

Prost broj 337 može dijeliti samo jednu od zagrada, pa je onda u potpunosti dijeli. Ako $337^n \mid x - 1$ ili $337^n \mid x + 1$, u oba slučaja dobivamo da je $x \geq 337^n - 1$, pa je $x^2 - 1 \geq (337^n - 1)^2 - 1 = 337^{2n} - 2 \cdot 337^n > 2022^n$, iz čega vidimo da nema rješenja.

13. Prebacimo jedinicu na desnu stranu i faktorizirajmo:

$$2^m p^2 = n^5 - 1 = (n - 1)(n^4 + n^3 + n^2 + n + 1).$$

U ovom trenutku prirodno je gledati najveći zajednički djelitelj faktora na desnoj strani, ali to neće biti potrebno. Naime, pogledajmo prvo parnost izraza $n^4 + n^3 + n^2 + n + 1$. U njemu sudjeluje četiri izraza iste parnosti i neparan broj, pa je sigurno neparan broj. Zato ne može biti djeljiv s 2^m . Nadalje, taj izraz je sigurno veći od $n - 1$. Zato, kako bi u umnošku ta dva faktora bila jednaka $2^m p^2$, nužno je

$$n - 1 = 2^m, \quad n^4 + n^3 + n^2 + n + 1 = p^2$$

(slučajevi kada je druga zagrada jednaka p ili 1 otpadaju jer bi tada taj izraz bio manji od prve zagrade). Pogledajmo sada ostatke modulo 8 u drugoj zagradi. Ako je $m \geq 3$, tada je $n = 2^m + 1 \equiv 1 \pmod{3}$, pa je $n^4 + n^3 + n^2 + n + 1 \equiv 5 \pmod{8}$. Međutim, to nije kvadratni ostatak modulo 8. Zato je nužno $m \leq 2$. Direktno provjerimo ta dva slučaja, te dobivamo jedino rješenje $m = 2$, $n = 3$, $p = 11$.

14. Pogledajmo jednadžbu po modulu 4. Kako je $3^a \equiv 7^a \equiv (-1)^a \pmod{4}$ možemo zaključiti da su m i n različite parnosti, jer kad bi bili iste, lijeva strana davala bi ostatak 2 pri dijeljenju s 4. Dakle, točno jedan od m i n je paran.

Neka je prvo m paran: $m = 2m_1$. Razlikom kvadrata dobivamo

$$7^n = k^2 - 3^m = (k - 3^{m_1})(k + 3^{m_1}).$$

Najveći zajednički djelitelj faktora na desnoj strani dijeli i njihovu razliku $2 \cdot 3^{m_1}$, koja je relativno prosta sa 7. Zato da bi njihov umnožak bio potencija broja 7, manji od njih mora biti jednak 7. Oduzimanjem $k - 3^{m_1} = 1$ i $k + 3^{m_1} = 7^n$ dobivamo $2 \cdot 3^{m_1} = 7^n - 1$.

Prije nego nastavimo rješavati ovu jednadžbu, primijetimo da će drugi slučaj potpuno analogno se svesti na jednadžbu $2 \cdot 7^{n_1} = 3^m - 1$. Te dvije jednadžbe sličnog su tipa. Iako se mogu riješiti modulima (pokušaj modulo 9 i modulo 7) te se jedan od slučajeva može riješiti s LTE, oba slučaja riješit ćemo na isti način pomoću Zsigmondyjevog teorema.

Pokažimo ideju na prvoj jednakosti: $2 \cdot 3^{m_1} = 7^n - 1$. Desno imamo razliku n -tih potencija, kao u Zsigmondyjevom teoremu, a lijevo samo faktore 2 i 3. Ideja je sljedeća: ili ćemo dokazati da desna strana nikad nije djeljiva sa 6 ni za koji n_0 , ili ćemo dokazati pomoću Zsigmondyjevog teorema da za sve $n > n_0$ ne može biti oblika $2 \cdot 3^{m_1}$ jer će imati još neke proste djelitelje.

U ovoj jednakosti stvari su direktnije jer postoji takav n_0 i to je već $n_0 = 1$. U tom slučaju dobivamo rješenje $n = 1$, $m = 2$, $k = 4$. Za sve $n > 1$, prema Zsigmondyjevom teoremu $7^n - 1$ ima neki prosti faktor koji se ne pojavljuje u raspisu broja $7^1 - 1^1$ na proste faktore, dakle postoji neki $p > 3$ koji dijeli desnu stranu, a ne dijeli lijevu.

Za drugu jednakost ($2 \cdot 7^{n_1} = 3^m - 1$) malo ćemo duže tražiti odgovarajući m_0 . Tek za $m_0 = 6$ imamo da je $3^{m_0} - 1$ djeljivo sa 7 (a uvijek je djeljivo s 2). Zato za svaku od vrijednosti $m \leq 6$ se zasebno uvjerimo da ne vodi rješenju, dok za $m > 6$ prema Zsigmondyjevom teoremu $3^m - 1$ ima neki prosti djelitelj koji se ne pojavljuje u raspisu $3^6 - 1$ na proste faktore, posebno, postoji za svaki $m > 6$ postoji neki prosti $p \neq 2, 7$ koji dijeli desnu stranu, a ne dijeli lijevu, pa zato nema rješenja.

Jedino rješenje je $(m, n, k) = (2, 1, 4)$.

15. Gledamo zadanu jednadžbu modulo 5. Desna strana daje ostatak 1, a lijeva će davati taj ostatak samo ako je n djeljiv s 4. Zato možemo pisati $n = 4m$, $m \in \mathbb{N}$, te nakon primjene dvije razlike kvadrata imamo

$$(3^m - 1)(3^m + 1)(3^{2m} + 1) = 5k^2.$$

Na desnoj nalaze se tri parna broja, pa je k nužno djeljiv s 4: $k = 4l$, $l \in \mathbb{N}$. Također, prva dva faktora razlikuju se za 2, a zadnji faktor jednak je umnošku prva dva faktora uvećan za 2 pa je zato najveći zajednički djelitelj svaka dva faktora jednak 2. Nakon dijeljenja s 8 slijedi

$$\frac{3^m - 1}{2} \cdot \frac{3^m + 1}{2} \cdot \frac{3^{2m} + 1}{2} = 10l^2,$$

gdje su na lijevoj strani u parovima relativno prosti faktori. Zato je svaki od njih jednak nekom potpunom kvadratu pomnožen s faktorom 1, 2, 5 ili 10. To vodi na potencijalno mnogo slučajeva koje treba iskontrolirati.

Jedan način za kontrolu broja slučajeva je pogledati dodatno parnost broja m . Ako je m paran, tada $3^m + 1$ nije djeljiv ni s 5 ni s 4, pa je nužno $3^{2m} + 1 = 2x^2$ što nema rješenja kada se jednadžba

promotri modulo 3. Ako je m neparan, tada je $3^m \not\equiv \pm 1 \pmod{5}$, pa zato samo zadnji faktor može biti djeljiv s 5. Također, $3^m \equiv 3 \pmod{4}$, pa samo drugi faktor može biti djeljiv s 4. Zato je jedina mogućnost

$$\frac{3^m - 1}{2} = x^2, \quad \frac{3^m + 1}{2} = 2y^2, \quad \frac{3^{2m} + 1}{2} = 5z^2.$$

Drugu jednadžbu riješimo rastavom na razliku kvadrata: $3^m = (2y - 1)(2y + 1)$, faktori nužno moraju biti relativno prosti, pa je $y = 1$, $m = 1$, što vodi na jedino rješenje $(n, k) = (4, 4)$.

Drugi način kontrole slučaja je koristeći Mihaelescuv teorem: nikoji od faktora ne može biti jednak $2x^2$ jer bi to vodilo na jednadžbe $3^m - 1 = 4x^2$, $3^m + 1 = 4x^2$ i $3^{2m} - 1 = 4x^2$ koje nemaju rješenja (ili imaju trivijalna rješenja). Preostalo je provjeriti slučaj kada je jedan od faktora oblika $10x^2$, a druga dva potpun kvadrat. U tom slučaju imamo $3^m + 1 = 2 \cdot x^2$ ili $3^m + 1 = 2 \cdot 10x^2$. U oba slučaja desna strana jednadžbe daje ostatak 0 ili 2 pri dijeljenju s 3, a lijeva strana 1, pa ne dobivamo nova rješenja.

Jedino rješenje zadatka je par $(n, k) = (4, 4)$.

- 16.** Gledamo jednadžbu modulo 3. Desna strana daje ostatak 1 pri dijeljenju s 3, a lijeva će tek ako je n paran: $n = 2k$, $k \in \mathbb{N}$. Koristeći razliku kvadrata, dobivamo

$$(5^k - 1)(5^k + 1) = 6m^2.$$

Na lijevoj strani imamo umnožak dva uzastopna parna broja. Implicitno to znači i da je m paran: $m = 2p$, $p \in \mathbb{N}$. Podijelimo li jednadžbu s 4, dobivamo:

$$\frac{5^k - 1}{2} \cdot \frac{5^k + 1}{2} = 6p^2.$$

Faktori na lijevoj strani su relativno prosti prirodni brojevi, pa je svaki od njih jednak potpunom kvadratu pomnoženom s faktorom 1, 2, 3 ili 6. Dodatno, $5^k \equiv 1 \pmod{4}$, tako da u stvari imamo dva slučaja: $5^k - 1 = 4x^2$, $5^k + 1 = 6y^2$ ili $5^k - 1 = 12x^2$, $5^k + 1 = 2y^2$. Prvi slučaj se inače može riješiti tek nekim naprednim tehnikama (Pellova jednadžba, [2]) ili Mihaelescuvim teoremom: $5^k - 1 = 4x^2$ može imati rješenje samo u trivijalnom slučaju $k = 1$, što vidi na rješenje $(m, n) = (2, 2)$. Drugi slučaj nema rješenja modulo 5: u jednakosti $5^k + 1 = 2y^2$ lijeva strana daje ostatak 1, a desna može davati ostatke 0, 2, 3, pa zato nema rješenja.

Jedino rješenje je $(m, n) = (2, 2)$.

Izvori i dodatna literatura

- [1] A. H. Parvardi, *Lifting The Exponent Lemma* (verzija 3), [Art of Problem Solving](#), pristupljeno 2026.
- [2] *Pellova jednadžba*, [Školjka](#), pristupljeno 2026.
- [3] E. Macić, *Diofantske jednadžbe* (2. tjedan), [MetaMath 2023](#).