



Uvod

Diofantske jednadžbe su jednadžbe koje rješavamo u skupu prirodnih ili cijelih brojeva. Obično se sastoje od poznatih potencija nepoznanica npr. $x^2, y^3, x, y \in \mathbb{Z}$, nepoznatih potencija poznatih brojeva npr. $3^a, 10^b, a, b \in \mathbb{N}$ ili/i nepoznatih potencija $x^a, x, a \in \mathbb{N}$. Ne postoji univerzalni način kako riješiti svaku diofantsku jednadžbu koja se može pojaviti na natjecanju, no postoje brojne tvrdnje i ideje koje možemo koristiti pri rješavanju.

Korisne tvrdnje i ideje

1 Djeljivost

Po definiciji, $a, b \in \mathbb{Z}, a \neq 0$ a dijeli b i pišemo $a|b$, ako i samo ako postoji cijeli broj k takav da vrijedi $b = k \cdot a$. Ponekad je u zadatku potrebno uvesti količnik kada znamo da neki broj dijeli neki drugi.

Ako za $a, b, c \in \mathbb{Z}$ $a|b$ i $a|c$ Onda vrijedi

- $a|(b+c)$
- $a|(b-c)$
- $\forall k \in \mathbb{Z}, a|b \cdot k$

Teorem o djeljenju s ostatkom: Ako je $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da vrijedi $a = q \cdot b + r$ i $0 \leq r < b$.

2 Najveći zajednički djelitelj

Za $a, b \in \mathbb{Z}$ definiramo najveći zajednički djelitelj $M(a, b)$ ili $\gcd(a, b)$ kao:

- $M(0, 0) = 0$
- $M(a, b)$ je najveći prirodni broj koji dijeli a i b za $a \neq 0$ ili $b \neq 0$.

Vrijedi Euklidov algoritam: $M(a, b) = M(a, a-b)$ te se može proširiti koristeći teorem o djeljenju s ostatkom u $M(a, b) = M(b, r)$, gdje je $a = b \cdot q + r$.

Ako za $a, b, c \in \mathbb{Z}$ vrijedi $a|b \cdot c$ i $M(a, c) = 1$ onda vrijedi $a|b$.

Ako za $b, c, p \in \mathbb{Z}$ gdje je p prost, vrijedi $p|bc$ onda vrijedi $p|b$ ili $p|c$.

Ako za $a, b, x \in \mathbb{Z}$, $M(a, b) = 1$ i $n \in \mathbb{N}$ vrijedi $a \cdot b = x^n$ onda vrijedi da postoje $k, t \in \mathbb{N} \cup \{0\}$ takvi da je $a = x^k$, $b = x^t$ i $k+t = n$.

Ponekad je korisno promotriti najveći zajednički djelitelj od nepoznanica iz zadatka i zapisati nepoznanice pomoću njih. Npr. $x, y \in \mathbb{Z}$, kažemo da je $M(x, y) = d$, $d \in \mathbb{N} \cup \{0\}$ i onda vrijedi $x = d \cdot a$ i $y = d \cdot b$ za neke $a, b \in \mathbb{Z}$, te znamo da je $M(a, b) = 1$ što može biti dosta korisno u daljnjem rješavanju zadatka.

3 Kongruencije

Kongruencije su ostatci pri djeljenu nekog cijelog broja s nekim prirodnim brojem. Zapis $a \equiv r \pmod{n}$ (čitamo a je kongruentno r modulo n) znači da je ostatak pri djeljenu broja a s n jednak ostatku pri djeljenu broja r s n, tj. da im je razlika djeljiva s n.

$$k \in \mathbb{Z}, a \equiv a + kn \pmod{n}$$

$$a, b, c, d \in \mathbb{Z}, a \equiv b \pmod{n}, c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$$

$$a, b, c, d \in \mathbb{Z}, a \equiv b \pmod{n}, c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$$

$$c \in \mathbb{N}, M(c, n) = d, a \equiv b \pmod{n} \implies \frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{n}{d}}$$

$$k \in \mathbb{N}, a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$$

Mali fermatov teorem: Ako je p prost broj i a cijeli takav da je $M(a, p) = 1$ onda $a^{p-1} \equiv 1 \pmod{p}$

Iz tog teorema slijedi još jedna tvrdnja koja može biti korisna u diofantskim jednačabama a to je da broj oblika $y^2 + 1$, gdje je y prirodan broj, ne može imati prostih faktora p oblika $p = 4k - 1, k \in \mathbb{N}$ tj. ne može imati prostih faktora koji pri djeljenu s 4 daju ostatak 3.

Pri djeljenu sa nekim prostim brojevima, poznate potencije nepoznatih brojeva, ili nepoznate potencije poznatih brojeva, često ne poprimaju sve ostatke pri djeljenu s tim prostim brojem, pa je korisno promatrati koje ostatke mogu dati iz čega možemo zaključiti neke korisne informacije za rješavanje diofantske jednačbe.

Ako želimo utvrditi koje ostatke pri djeljenu može poprimiti poznata potencija, naprosto možemo isprobati sve moguće kombinacije baze potencije.

Na primjer. Koje sve ostatke daje kvadrat prije djeljenu s 4?

x	0	1	2	3
$x^2 \pmod{4}$	0	1	0	1

Za određivanje ostatka pri djeljenu potencija poznate baze a s brojem n koji je relativno prost s bazom, dovoljno je pronaći prvu prirodnu potenciju d koja daje ostatak 1 pri djeljenu s traženim brojem i onda ostatak pri djeljenu svake potencije a^m s n ovisi samo o ostatku pri djeljenu m s d. Na primjer ako promatramo ostatke koje potencije od 7 daju pri djeljenu s 5:

n	1	2	3	4
$7^n \pmod{5}$	2	4	3	1

Sada znamo da ostatak ovisi samo o ostatku pri djeljenu s 4 od n.

Npr. za svaki broj koji je oblika $m = 4k + 2, k \in \mathbb{N} \cup \{0\}$, $7^{4k+2} \equiv 7^2 \equiv 4 \pmod{5}$

Ako baza a nije relativno prosta s n kojim djelimo, obično ćemo promatrati samo ostatke modulo potencija prostog broja, tj. $n = p^k$, gdje je p prost i k prirodan, pa će za dovoljno velike eksponente potencija biti djeljiva s n. Npr. ako promatramo ostatke pri djeljenu s 8 od 2^m , za sve $m \geq 3$ će on biti 0.

Promatranjem koje ostatke daju izrazi u diofantskoj jednačbi nam može dati korisne informacije za eksponente potencija: odrediti koji ostatak daju pri djeljenu s nekim drugim brojem, ili broj od kojeg eksponent ne smije biti veći. Također, ako izrazi u jednačbi nikada ne daju ostatke pri djeljenu s nekim brojem n tako da lijeva i desna strana daju isti ostatak, onda jednačba nema rješenja.

Ako želimo pronaći povoljan prost broj p za promatranje ostataka, onda je generalno dobro promatrati takve p, da je $p - 1$ djeljiv s najvećim zajedničkim višekratnikom od eksponentenata koji se pojavljuju u jednačbi.

Ako želimo pronaći potenciju prostog broja, onda promatramo p^k takve da je $p^k - p^{k-1}$ djeljiv s višekratnikom ekponenata iz jednačbe.

4 Faktorizacije

Često je u diofantskim jednačbama korisno faktorizirati izraze koji se pojavljuju kako bi se dobile nove tvrdnje o tome koji izraz dijeli koji, kako bi primijenili neku od korisnih tvrdnji za najveći zajednički djelitelj, te ako znamo točan rastav na proste faktore umnoška s jedne strane jednačbe i s druge je neki umnožak onda znamo da možemo posebno promatrati sve slučajeve ovisno o tome koliko puta koji prosti faktor od broja dijeli koji od tih izraza. U tome nam također može pomoći najveći zajednički djelitelj jer npr. ako znamo da je najveći zajednički djelitelj dva faktora 3 i njihov umnožak je 3^k onda je jedan jednak 3^{k-1} , a drugi 3.

Popis korisnih formula i tvrdnji:

- Razlika kvadrata: $a^2 - b^2 = (a + b) \cdot (a - b)$
- Kvadrat binoma: $(a \pm b)^2 = a^2 \pm 2ab + b^2$
- Zbroj i razlika kubova: $a^3 \pm b^3 = (a \pm b) \cdot (a^2 \mp ab + b^2)$
- Kub zbroja $(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3$
- $a^n - b^n$ gdje je n prirodan broj se može faktorizirati kao $(a - b) \cdot (a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$
- $a^n + b^n$ gdje je n neparan prirodan broj se može faktorizirati kao $(a + b) \cdot (a^{n-1} - a^{n-2}b + a^{n-3}b^2 - a^{n-4}b^3 + \dots + a^2b^{n-3} - ab^{n-2} + b^{n-1})$
- Izraz oblika $x^a + x^b + x^c$, gdje su $a, b, i c$ prirodni brojevi ili nula koji daju međusobno različite ostatke pri djeljenju s 3, može se faktorizirati i jedan od faktora će biti $x^2 + x + 1$, drugi faktor će biti pozitivnog stupnja, ako je početni izraz različit od $x^2 + x + 1$.
- Diofantsku jednadžbu ponekad možemo promatrati kao kvadratnu jednažbu po nekoj nepoznanici i zapisati vrijednost te nepoznanice prema formuli za kvadratnu i gledali kada je taj izraz cijeli/prirodan broj. $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
Najčešće je dovoljno samo promatrati kada je diskriminanta $b^2 - 4ac$ kvadrat cijelog broja.

5 Ograničavanje

- $a, b \in \mathbb{Z}$, ako $a \mid b$ i $b \neq 0$ onda vrijedi $|a| \leq |b|$.
Također ako znamo da je $|b| < 2 \cdot |a|$ onda je $|a| = |b|$.
- Ponekad je korisno promatrati koji izrazi brže rastu od drugih npr. x^3 će biti veći od $4x^2$ za sve x veće jednake 5. Pomoću takvih ograda možemo zaključiti da će neka strana jednakosti biti veća od druge za sve brojeve veće od nekog, što naravno nije moguće, pa nam ostaje provjeriti samo one koji su manji jednaki tom broju.

Generalno polinomi većeg stupnja će rasti brže od onih manjih stupnjeva.

Izrazi u kojima je x eksponent će rasti brže od polinoma od x .

Ako uspoređujemo dva izraza u kojima je x eksponent, onaj s većom bazom će rasti brže.

- Nekad možemo potenciju nekog broja ograničiti s dvije potencije s istim eksponentom kao ova, pa onda znamo da i baza potencije mora biti između baza potencija. Npr. ako znamo da za neke $x, y \in \mathbb{N}$ $x^2 < y^2 < (x+1)^2$ onda za y treba vrijediti $x < y < x+1$ što nije moguće.

6 Beskonačni spust

Ponekad nam se tijekom rješavanja i promatranja djeljivosti može dogoditi da pomoću nekog rješenja jednadžbe možemo dobiti jednadžbu koja je ista ili dosta slična kao početna, a ima u sebi nepoznanice koje su po apsolutnoj vrijednosti strogo manje od nepoznanica iz početne jednadžbe. Ako isti postupak možemo primijeniti i na tu novu dobivenu jednadžbu i svaku daljnju koju dobijemo istim postupkom onda početna jednadžba nema rješenja jer ne postoji proizvoljno mali cijeli broj, gledajući apsolutnu vrijednost. Najčešće će jednadžba imati rješenje kada su svi brojevi 0, a ako nisu svi 0 će biti moguće dobiti manje rješenje za koje nisu svi brojevi 0, što će nas opet dovesti u kontradikciju.

Na primjer: Odredimo sva rješenja jednadžbe $3x^2 = y^2$, pri čemu su $x, y \in \mathbb{Z}$.

Ako je jedan od brojeva 0, onda je i drugi 0, te je (0,0) rješenje jednadžbe. Sada pretpostavimo da niti jedan od njih nije 0. Budući da $3|y^2$ slijedi $3|y$ tj. $y = 3y_1$, $y_1 \in \mathbb{Z}$. Sada je $3x^2 = 9 \cdot y_1^2$ tj. $x^2 = 3y_1^2$. Sada vidimo da $3|x^2$, pa $3|x$ tj. $x = 3x_1$, $x_1 \in \mathbb{Z}$. Sada je jednadžba oblika $9x_1^2 = 3y_1^2$ tj. $3x_1^2 = y_1^2$.

Uočavamo da smo dobili jednadžbu koja je istog oblika kao početna, vrijednosti su duplo manje, pa strogo manje apsolutno, te niti jedan od x_1 i y_1 nije 0 jer bi onda x ili y bio 0. Očito ovakav postupak možemo ponavljati u beskonačnost, pa ako postoji rješenje gdje brojevi nisu 0, onda postoji proizvoljno mali cijeli broj po apsolutnoj

vrijednosti što nije moguće.

U nekim slučajevima se formuliranje beskonačnog spusta može izbjeći tako da samo uzmemo najveći zajednički djelitelj brojeva iz zadatka, no nekad to nije moguće. Primjer kada to jest moguće je ovaj gornji primjer:

Kao i gore pretpostavimo da je $x \neq 0$ i $y \neq 0$. Ako uzmemo da je $M(x, y) = d$ onda je $d \in \mathbb{N}$ i $x = d \cdot a$, $y = d \cdot b$; $a, b \in \mathbb{Z}$.

Sada je jednačba oblika $3 \cdot d^2 \cdot a^2 = d^2 \cdot b^2 \iff 3a^2 = b^2$. Isto kao gore možemo zaključiti da 3 dijeli b, i onda da 3 dijeli a, no onda a i b imaju zajednički djelitelj pa je 3d zajednički djelitelj od a i b što je u kontradikciji s tim da je d najveći, pa slijedi da jednačba nema rješenja kada je $x \neq 0$.

Lakši zadaci

1. Riješi u skupu prirodnih brojeva $x^2 - y! = 2001$.
2. Riješi u skupu cijelih brojeva $x^6 + 3x^3 + 1 = y^4$.
3. Odredi sve uređene trojke prostih brojeva (p, q, r) za koje vrijedi $3p^4 - 5q^4 - 4r^2 = 26$.
4. Odredi za koje sve proste brojeve p postoji prirodni brojevi x i y takvi da je $x \cdot (y^2 - p) + y \cdot (x^2 - p) = 5p$.
5. Odredi sve prirodne brojeve n za koje je $n \cdot 2^{n+1} + 1$ potpuni kvadrat.
6. Riješi jednačbu u skupu cijelih brojeva $x^4 + y^4 + z^4 = 9u^4$.
7. Odredi sve uređene trojke nenegativnih brojeva (a, b, c) za koje vrijedi $2^a \cdot 3^b + 9 = c^2$

Umjereni zadaci

8. Riješi jednačbu $4xy - x - y = z^2$ u skupu cijelih brojeva.
9. Riješi jednačbu $5^x \cdot 7^y + 4 = 3^z$ u skupu nenegativnih brojeva.
10. Riješi jednačbu $p^2 - p + 1 = x^3$ gdje je p prost broj, a x prirodan broj.
11. Riješi jednačbu $5^x = 1 + 4y + y^4$ u skupu cijelih brojeva.
12. Odredi sva rješenja jednačbe $x^5 + x^4 + 1 = p^y$ gdje su x i y prirodni brojevi, a p prost.
13. Riješi jednačbu $x^3 + y^3 = x^2 + 42xy + y^2$ gdje su x i y prirodni brojevi.
14. Riješi jednačbu $y^2 = x^3 + 7$, gdje su x i y prirodni brojevi.
15. Riješi jednačbu $p^q - q^p = p \cdot q^2 - 19$ gdje su p i q prosti brojevi.

Teži zadaci

16. Riješi u skupu prostih brojeva sustav jednačbi $x^2 + yu = (x + u)^v$ i $x^2 + yz = u^4$.
17. Odredi sva rješenja jednačbe $(m^3 + n) \cdot (n^3 + m) = p^3$ gdje su n i m prirodni brojevi, a p prost.
18. Odredi sva rješenja jednačbe $3^k - 1 = x^n$, gdje su k, x i n prirodni brojevi.

Više zadataka možete pronaći na www.skoljka.org.

Hintovi

1. Promotri kada su brojevi djeljivi s 3 i s 9.
2. Raspiši kvadratnu po $t = x^3$ i pogledaj kada je diskriminanta kvadrat cijelog broja.
3. Protromotri ostatke pri djeljenju s brojevima koji se pojavljuju u zadatku.
4. Faktoriziraj izraz i promotri slučajeve u ovisnosti raspisa 5p na faktore.
5. Faktoriziraj, promotri kolika potencija od 2 može dijeliti faktore, te primijeni tvrdnju $a \mid b, b \neq 0 \implies |a| \leq |b|$.
6. Uvedi najveći zajednički djelitelj brojeva svih brojeva iz zadatka.
7. Promotri najveći zajednički djelitelj od $c + 3$ i $c - 3$, te promatraj slučajeve ovisno o tome kojeg dijele potencije od 2, a kojeg potencije od 3.
8. $y^2 + 1$ nema djelitelja oblika $4k - 1, k \in \mathbb{Z}$.
9. Koristi ostatke pri djeljenju kako bi dobio parnost eksponenata, te pomoći toga faktoriziraj izraz.
10. Gledaj slučajeve ovisno o tome koji faktor od $x^3 - 1$ je djeljiv s p , te uvedi količnik.
11. Promatraj ostatak pri djeljenju s 8, faktoriziraj i ograniči y .
12. Faktoriziraj lijevu stranu i promotri najveći zajednički djelitelj faktora.
13. Uvedi najveći zajednički djelitelj te koristi tvrdnje da faktori s lijeve strane dijele desnu.
14. $y^2 + 1$ nema djelitelja oblika $4k - 1, k \in \mathbb{Z}$.
15. Mali Fermatov teorem i uvođenje količnika.
16. Uvrsti y iz druge u prvu da ograničiš v . Faktoriziranje i ograničavanje.
17. Rastavi p^3 na faktore s desne strane, promatraj $M(m, n)$. Pomoću jednadžbi pokušaj dobiti neki relativno mali broj djeljiv s p .
18. $y^2 + 1$ nema djelitelja oblika $4k - 1, k \in \mathbb{Z}$. Faktoriziranje i ograničavanje.

Rješenja

1. Promatramo koje ostatke može poprimiti jednačba pri djeljenu s 9. $6!$ je djeljiv s 9, pa je za svaki $y \geq 6$, $y!$ djeljiv s 9. 2001 je djeljiv s 3, što znači da i x^2 mora biti djeljiv s 3, no onda je i x djeljiv s 3 što znači da je x^2 djeljiv s 9. Onda znamo da je desna strana djeljiva s 9, no lijeva je djeljiva samo s 3, što nije moguće. Zaključujemo da je $y \leq 5$. Direktnim uvrštavanjem zaključujemo da je jedino $2001 + 4! = 2025$ kvadrat prirodnog broja, pa je jedino rješenje (25, 4).

2. Primijetimo da je uz supstituciju $t = x^3$, dobivena jednačba $t^2 + 3t + 1 = y^4 \equiv t^2 + 3t + 1 - y^4 = 0$ kvadratna jednačba u varijabli t pa možemo primijeniti formulu za kvadratnu jednačbu $t_{1,2} = \frac{-3t \pm \sqrt{9 + 4(y^4 - 1)}}{2}$. Diskriminanta treba biti kvadrat nekog cijelog broja $\implies 4y^2 + 5 = c^2, c \in \mathbb{Z}$. Prepostavimo da je $y \geq 0$ jer ako je neki negativan broj a rješenje jednačbe onda je $-a$ isto rješenje i $-a \geq 0$, pa će sva rješenja biti pozitivna rješenja i njihovi suprotni brojevi.

Sljedeći kvadrat veći od $4y^2$ je $(2y + 1)^2 = 4y^2 + 4y + 1$ što je za $y \geq 2$ strogo veće od $4y^2 + 5$ koji se nalazi između dva susjedna kvadrata, pa ne može i sam biti kvadrat. Došli smo do kontradikcije pa y mora biti 0 ili 1.

Za $y = 0$, diskriminanta je jednaka 5 što nije kvadrat pa t neće biti racionalan.

Za $y = 1$, diskriminanta je jednaka 9 pa je $t_{1,2} = \frac{-3 \pm 3}{2}$, tj. $t_1 = 0$, i $t_2 = -3$. $x^3 = -3$ nema rješenja u cijelim brojevima, pa je jedino rješenje $x^3 = 0 \implies x = 0$ i $y = \pm 1$.

3. Isprobavanjem svih mogućnosti u tablici zaključujemo da x^2 poprima samo ostatke 0 i 1 pri djeljenu s 3, te x^4 isto poprima samo ostatke 0 i 1. Kada promatramo jednačbu modulo 3 i isprobamo sve mogućnosti ostataka za q^4 i r^2 , dobivamo da je jedina mogućnost kada je $q \equiv 0 \pmod{3}$. Budući da je q prost to je moguće samo za $q = 3$. Sada ponovimo isti postupak za ostatke pri djeljenu s 5. Te zaključujemo da x^4 poprima samo ostatke 0 i 1, a x^2 0, 1 i 4, te iz toga isprobavanjem svih mogućnosti zaključujemo da $3p^4 \equiv (\text{mod } 5)$, tj. da je p djeljiv s 5, tj. $p = 5$. Uvrštavanjem toga u jednačbu dobivamo $4r^2 = 1444$, tj. $r = 19$ što nam daje jedino rješenje $(p, q, r) = (5, 3, 19)$.

Link: JBM0 2014 P1

4. $x \cdot (y^2 - p) + y \cdot (x^2 - p) = 5p \iff xy^2 - px + yx^2 - py = 5p \iff xy(x+y) - p(x+y) = 5 \iff (x+y)(xy-p) = 5p$
Desna strana je umnožak dva prosta broja pa faktori s lijeve strane mogu biti jednaki 1, jedan od ta dva prosta ili umnošku oba prosta. $x + y \geq 2$, pa on ne može biti jednak 1, te nam ostaju 3 slučaja, $xy - p = 1$, $xy - p = p$ i $xy - p = 5$.

1. Slučaj: $x + y = 5p$, $xy - p = 1$, pomnožimo drugu jednačbu s 5 i uvrstimo u prvu umjesto $5p$: $x + y = 5(xy - 1) \iff 5xy - x - y - 5 = 0 \iff x(5y - 1) = y + 5$. Znamo da je x prirodan pa $x \geq 1$. Za $y \geq 2$ je lijeva strana veća jednaka $5y - 1 \geq y + 8 - 1 = y + 7$ što je veće od desne strane. Dobili smo kontradikciju pa $y = 1$, no uvrštavanjem dobivamo $4x = 6$ što nema rješenja. 2. Slučaj: $x + y = 5$, $xy - p = p \implies xy = 2p$. xy je umnožak dva prosta broja pa ili je jedna jednak 1, a drugi cijelom umnošku ili je svaki jedan jednom od prostih. Ako je jedan od njih jednak 1, bez smanjenja općenitosti $y = 1$, onda je $x = 2p$, i $x + y = 2p + 1 = 5$, tj. $p = 2$, tj. tvrdnja vrijedi za 2. Ako je jedan jednak 2, a drugi p , bez smanjenja općenitosti $x = 2, y = p$, $x + y = p + 2 = 5$, tj. $p = 3$ i za njega vrijedi tvrdnja. 3. Slučaj: $x + y = p$, $xy - p = 5$, Uvrstimo prvu jednačbu u drugu $xy - x - y = 5 \iff x(y - 1) = y + 5 \implies y - 1 \mid y + 5$, tj. $y - 16$ iz čega slijedi $y - 1 \in \{1, 2, 3, 6\}$, tj. $y \in \{2, 3, 4, 6\}$. Uvrštavanjem dobivamo da je jedino rješenje ovog slučaja $p = 7$.

Rješenje zadatka su prosti brojevi 2, 3 i 7.

Link: JBM0 2011 P2

5. $n \cdot 2^{n+1} + 1 = x^2 \iff (x+1)(x-1) = n \cdot 2^{n+1}$ $M(x+1, x-1) = M(x-1, 2)$, Znamo da je $(x+1)(x-1)$ paran, pa je x sigurno neparan, pa je $x-1$ paran, $M(x+1, x-1) = 2$. Onda je točno jedan od brojeva $(x+1)$ i $(x-1)$ djeljiv samo s 2, a drugi s 2^n . Ako je x jednak 1, onda bi n trebao biti 0 što nije moguće, pa je $x-1 > 0$. Sada $2^n \mid x+1 \implies x \geq 2^n - 1$ ili $2^n \mid x-1 \implies x \geq 2^n + 1 \geq 2^n - 1$. U oba slučaja je $x \geq 2^n - 1$. Znači $n \cdot 2^{n+1} + 1 \geq x^2 = 2^{2n} - 2^{n+1} + 1 \implies 2^{n+1}(n+1) \geq 2^{2n} \implies 2(n+1) \geq 2^n$. Za $n = 4$ $10 \geq 16$ ne vrijedi, a za veće n 2^n raste brže od $2(n+1)$ pa izrazi ne mogu biti jednaki. Iz toga slijedi $n \leq 3$. Uvrštavanjem dobivamo jedino rješenje za $n = 3$, i to $x = 7$. Znači jedini broj za koji vrijedi tvrdnja zadatka je 3.

Link: JBM0 2010 P2

6. Uočavamo da je $(0, 0, 0, 0)$ sigurno rješenje zadane jednačbe $x^4 + y^4 + z^4 = 9u^4$. Prepostavimo da neki od njih nije jednak 0, iz toga slijedi da postoji najveći zajednički djelitelj brojeva x, y, z i u , koji nije jednak 0. $d = M(x, y, z, u)$, $x = d \cdot x_1, y = d \cdot y_1, z = d \cdot z_1, u = d \cdot u_1$.

Uvrštavanjem tih jednakosti u početnu jednačbu i djeljenjem s d^4 dobivamo $x_1^4 + y_1^4 + z_1^4 = u_1^4$. Ako promotrimo

sve ostatke od koje a^4 popriva pri djeljenju sa 16, dobivamo da je moguće samo za 0 i 1.

1. Slučaj: $u_1^4 \equiv 0 \pmod{16}$, tj. u_1 je paran. Sada zbroj ostalih ostataka mora biti 0, no ako je neki od njih jednak jedan, onda je maksimalni zbroj ostataka 3 što je manje od sljedećeg broja djeljivog s 16, tj. 16. Zaključujemo da sve ostale 4. potencije isto daju ostatak 0 pri djeljenju s 16, tj. da su x_1, y_1 i z_1 svi parni. No, onda 2 dijeli sva 4 broja, no onda je 2d njihov zajednički djelitelj, a najveći zajednički je d, što nije moguće. Znači u ovom slučaju jednadžba nema rješenja. 2. Slučaj: $u_1^4 \equiv 0 \pmod{16}$. Sada desna strana daje ostatak 9 pri djeljenju s 16, no na lijevo strani su 3 broja koji daju ostatak 0 ili 1, pa njihov zbroj može biti samo 0, 1, 2 ili 3. Znači da ni ovaj slučaj nema rješenja.

Jedino rješenje zadatka je (0, 0, 0, 0);

7. $2^a 3^b + 9 = c^2 \iff 2^a 3^b = (c+3)(c-3)$. $M(c+3, c-3) = M(c+3, 6)$ Sada rastavljamo zadatak na slučajeve. Prva dva će pokriti one gdje lijeva strana nije djeljiva s 6, tj $a = 0$ ili $b = 0$.

1. Slučaj: $a = 0$: $3^b = (c+3)(c-3)$. Lijeva strana je pozitivna pa $c-3 > 0$, ako je $b = 0$, onda je lijeva strana 1, a desna barem 4 što nije moguće. znači $b \geq 1$, tj 3 dijeli $c+3$ ili $c-3$, a ako dijeli jednog dijeli i drugog. Također, znamo da najviše 3 može dijeliti oba, pa je jedan jednak 3, a drugi 3^{b-1} . Znamo da su oba djeljiva s 3, pa je b barem 2, pa je 3 sigurno manji jednak od 3^{b-1} , tj. manji od njih $c-3$ je jednak 3. $c-3 = 3 \implies c = 6 \implies 3^b = 27 \implies b = 3$. Rješenje (0, 3, 6).

2. Slučaj: $b = 0$: $2^a = (c+3)(c-3)$, Iz prvog slučaja znamo da je $a > 0$, pa $2 \mid (c+3)(c-3)$, tj. c je neparan. Isto kao i u prvom slučaju $c-3 > 1$, i 2 dijeli i $c+3$ i $c-3$ pa je faktor 2^{a-1} veći od faktora 2, pa je manji od faktora $c-3 = 2 \implies c = 5 \implies 2^a = 16 \implies a = 4$. Rješenje (4, 0, 5).

Sada znamo da 6 dijeli barem jednog od $c+3$ i $c-3$, pa dijeli oba. A osim te šestice, brojevi su relativno prosti, pa su svi ostali faktori 2 u jednom od njih i svi ostali faktori 3 u drugom od njih.

3. Slučaj: $c-3 = 6$ i $c+3 = 2^{a-1}3^{b-1}$. Znači $c = 9 \implies 12 = 2^{a-1}3^{b-1}$, tj. $2^2 \cdot 3 = 2^{a-1}3^{b-1}$, Znači $a-1 = 2 \implies a = 3$ i $b-1 = 1 \implies b = 2$. Rješenje (3, 2, 9).

4. Slučaj: $c-3 = 6 \cdot 2^{a-2}$ i $c+3 = 6 \cdot 3^{b-2}$. Uvrstimo jednu u drugu i podijelimo s 6. $2^{a-2} + 1 = 3^{b-2}$. Za $a-2 \geq 2$. Promatramo jednadžbu modulo 4, lijeva strana je kongruetna 1, pa i desna mora biti 1 tj. $b-2$ koji određuje $3^{b-2} \pmod{4}$ mora biti djeljiv s 2. $(3^{\frac{b-2}{2}} + 1)(3^{\frac{b-2}{2}} - 1) = 2^{a-2}$. Najveći zajednički djelitelj dva faktora je 1 i umnožak im djeljiv s 4, te su obojica potencije od dva, pa je manji od njih jednak 2. $\implies 3^{\frac{b-2}{2}} - 1 = 2 \implies b-2 = 2 \implies b = 4$. Rješenje (5, 4, 51).

Sada nam ostaje podslučaj gdje je $a-2$ manji od 2, Ako je $a-2 = 0$ onda je to isto kao slučaj 3 koji smo riješili, pa ostaje $a-2 = 1 \implies a = 3 \implies b-2 = 1 \implies b = 3$. Rješenje (3, 3, 15).

5. Slučaj: $c-3 = 6 \cdot 3^{b-2}$, $c+3 = 6 \cdot 2^{a-2}$ Uvrstimo jednu u drugu i podijelimo s 6. $3^{b-2} + 1 = 2^{a-2}$. Ako je $a-2 \geq 3$. Promotrimo jednadžbu modulo 8, 3^{b-2} daje samo ostatke 3, i 1, pa $3^{b-2} + 1$ daje samo 4 i 2, a desna strana ima ostatak 0, pa nema rješenja.

Ako je $a-2 \implies 3^{b-2} = 0$, nema rješenja.

Ako je $a-2 = 1 \implies a = 3 \implies b = 2$. Rješenje (3, 2, 9) koje smo već dobili.

Ako je $a-2 = 2 \implies a = 4 \implies b = 3$. Rješenje (4, 3, 21).

Pokrili smo sve slučajeve pa zaključujemo da zadatak ima 6 rješenja : (0, 3, 6), (4, 0, 5), (5, 4 51), (3, 3, 15), (3, 2, 9), (4, 3, 21).

[Link: JBMO 2009 P2](#)

8. $4xy - xx - y = z^2 \iff y(4x-1) = z^2 + x$. Znači da $4x-1 \mid z^2 + x$. Budući da je $M(4x-1, 4) = 1$ vrijedi da $4x-1 \mid 4 \cdot (z^2 + x) \implies 4x-1 \mid 4z^2 + 4x \implies 4x-1 \mid 4z^2 + 1$. Sada smo dobili da broj oblika $4x-1$ dijeli broj oblika $4z^2 + 1$ što nije moguće pa jednadžba nema rješenja.

9. $5^x \cdot 7^y + 4 = 3^z$

Ako promatramo ostatak pri djeljenju članova jednadžbe s 4, dobijemo $7^y \equiv 3^z \pmod{4} \implies 3^y \equiv 3^z \pmod{4}$ Ostatak od potencije od 3 će biti 3 ako je eksponent neparan i 1 ako je eksponent paran, pa su y i z iste parnosti.

Ako sada promatramo ostatak pri djeljenju s 8: 1. slučaj y i z su neparni. $5^x 7^y + 4 \equiv 3^z \pmod{8} \iff 5^x(-1) + 4 \equiv 3 \pmod{8} \iff 5^x \equiv 1 \pmod{8}$ Ostatak pri djeljenju s 8 od potencije od 5 ovisi samo o parnosti ekponenta pa je x paran. 2. slučaj y i z su parni $5^x 7^y + 4 \equiv 3^z \pmod{8} \iff 5^x(1) + 4 \equiv 1 \pmod{8} \iff 5^x \equiv 5 \pmod{8} \implies x$

je neparan.

Ako je $z = 0$ ili 1 desna strana je manja od lijeve pa je $z \geq 2$

Sada promatramo ostatak pri djeljivosti članova jednačbe s 3. Dobijemo $5^x + 4 \equiv 0 \pmod{3}$ Ostatak pri djeljivosti s 3 od potencije od 5 ovisi samo o parnosti eksponenta, pa je x neparan, iz čega znamo da su y i z parni. $\implies z = 2z_1, z_1 \in \mathbb{N}$

$5^{x7^y} = 3^{2z_1} - 4 \iff 5^{x7^y} = (3^{z_1} + 2)(3^{z_1} - 2), M(3^{z_1} + 2, 3^{z_1} - 2) = M(3^{z_1} + 2, 4)$ Budući da je $3^{z_1} + 2$ faktor od 5^{x7^y} nije djeljiv s 2 pa vrijedi $M(3^{z_1} + 2, 4) = 1$.

To znači da su faktori s desne strane relativno prosti pa cijela potencija od 5 mora biti dio samo jednog faktora, i cijela potencija od 7 mora biti dio samo jednog faktora. Također, $3^{z_1} + 2$ ne može biti 1 pa imamo 3 slučaja:

1. slučaj $5^{x7^y} = 3^{z_1} + 2, 3^{z_1} - 2 = 1 \implies z_1 = 1 \implies 5^{x7^y} = 5 \implies x = 1, y = 0$ Dobili smo rješenje $(1, 0, 2)$.

Rješili smo slučajeve kada je neki od faktora jednak 1, pa u ostalima možemo pretpostaviti da su eksponenti veći jednaki 1.

2. slučaj $5^x = 3^{z_1} + 2, 7^y = 3^{z_1} - 2$ Ako promatramo prvu jednačbu modulo 5 možemo dobiti da je z_1 neparan, a ako promatramo drugu modulo 7, možemo dobiti da je z_1 paran. Kontradikcija. 3. slučaj $5^x = 3^{z_1} - 2, 7^y = 3^{z_1} + 2 \implies 7^y - 5^x = 4$ Od prije znamo da je y paran pa vrijedi $y = 2y_1, y_1 \in \mathbb{N}$

$7^y - 5^x = 4 \iff (7^{y_1} + 2)(7^{y_1} - 2) = 5^x$ Faktori su relativno prosti, pa bi manji od njih trebao biti 1, ali on je uvijek različit od 1 pa nema rješenja.

Jedino rješenje je $(1, 0, 2)$.

10. $p^2 - p + 1 = x^3 \iff p(p - 1) = (x - 1)(x^2 + x + 1). x = 0 \implies p = 0$ ili 1, znači $x \geq 1$.

p dijeli desnu stranu pa dijeli jedan od faktora:

1. slučaj: $p \mid x - 1, x > 0 \implies x - 1 \geq p \implies x^2 + x + 1 > x - 1 > p > p - 1$, što ne može vrijediti jer je onda je onda desna strana strogo veća od lijeve. 2. slučaj: $p \mid x^2 + x + 1 \implies x^2 + x + 1 = p \cdot t, t \in \mathbb{N}$. $p(p - 1) = (x - 1)(x^2 + x + 1) \implies p(p - 1) = (x - 1)pt \implies p - 1 = (x - 1)t \implies p = xt - t + 1$

$pt = x^2 + x + 1 \implies (xt - t + 1)t = x^2 + x + 1 \implies xt^2 - t^2 + t = x^2 + x + 1 \implies x(t^2 - x - 1) = t^2 - t + 1 \implies x \mid t^2 - t + 1$. $t^2 - t + 1 > 0$ Ako je $t^2 - t + 1 \geq 2x \implies t^2 \geq 2x + t - 1, x^2 + x + 1 = t^2(x - 1) + t \geq (2x + t - 1)(x - 1) + t = 2x^2 - 2x + tx - t - x + 1 + t = 2x^2 - 3x + tx + 1$

$x^2 + x + 1 \geq 2x^2 - 3x + tx + 1 \implies 4x \geq tx + x^2 \implies 4 \geq t + x$

$t \geq 1 \implies x \leq 3$:

1. podslučaj: $x = 1$ nema rješenja

2. podslučaj: $x = 2 \implies p(p - 1) = 7$ nema rješenja

3. podslučaj: $x = 3 \implies p(p - 1) = 26$ nema rješenja

Rješili smo slučaj $t^2 - t + 1 \geq 2x$, pa ostaje $t^2 - t + 1 = x \implies t^2 = x + t - 1$.

$x^2 + x + 1 = (x - 1)t^2 + t \iff x^2 + x + 1 = (x - 1)(x + t - 1) + t \iff x^2 + x + 1 = x^2 + xt - x - x - t + 1 + t \iff 3x = tx \iff t = 3 \iff (p - 1) = 3(x - 1) \iff p = 3x - 2 \iff 9x - 6 = x^2 + x + 1 \iff x^2 - 8x - 7 = 0 \iff (x - 1)(x - 7) = 0$ Znači $x = 7$ je rješenje, onda je $p = 19$.

Link: BMO 2005 P2

11. Ako je x manji od 0, onda je desna strana cijeli broj, a lijeva nije, pa ne mogu biti jednake, znači $x \geq 0$.

Ako promatramo ostatak jednačbe $5^x = 1 + 4y + y^4$ pri djeljivosti s 8, lijeva strana je kongruetna 5 kad je x neparan i 1 kad je x paran, a desna strana je kongruetna 1 kad je y paran, te 6 kad je y neparan. Uočavamo da je jedini slučaj kad su jednaki kad je x paran i y paran. $x = 2x_1, x_1 \in \mathbb{Z}, x_1 \geq 0$.

$5^{2x_1} - y^4 = 4y + 1 \iff (5^{x_1} + y^2)(5^{x_1} - y^2) = 4y + 1$

$4y + 1 \neq 0 \implies |5^{x_1} - y^2| > 0 \implies |4y + 1| \geq |5^{x_1} + y^2| = 5^{x_1} + y^2$

3. slučaja: 1. $y = 0 \implies x = 0$ Jedno rješenje je $(0, 0)$. 2. $y > 0$, Ako je $y \geq 5, 4y + 1 \geq 5^{x_1} + y^2 > 5y > 4y + 1 \implies$ nema rješenja: Znači $y \leq 4$, Znamo da je y paran pa treba provjeriti samo 2 i 4.

$y = 2 \implies 5^x = 25 \implies x = 2$, Jedno rješenje je $(2, 2)$.

$y = 4 \implies 5^x = 273 \implies$ nema rješenja

3. $y < 0 \implies y = -a, a > 0, a \in \mathbb{Z}$ i a je paran. $|4a + 1| = |1 - 4a| = 4a - 1$

$4a - 1 \geq 5^{x_1} + a^2$ Za $a \geq 4$ vrijedi $5^{x_1} + a^2 > 4a > 4a - 1$, znači nema rješenja. Tj. $a < 4$ Znači da je $a = 2 \implies y = -2 \implies 5^x = 9 \implies$ nema rješenja

Jedina rješenja su $(0, 0)$ i $(2, 2)$. **Link: Turkey TST 2001**

12. Znamo da se $x^5 + x^4 + 1$ može faktorizirati tako da jedan od faktora bude $x^2 + x + 1$ koji je faktor od x^3 . $x^5 + x^4 + 1 = x^3(x^2 + x) + 1 = (x^3 - 1)(x^2 + x) + x^2 + x + 1 = (x - 1)(x^2 + x + 1)(x^2 + x) + x^2 + x + 1 = (x^3 - x^2 + x^2 - x)(x^2 + x + 1) + x^2 + x + 1 = (x^2 + x + 1)(x^3 - x + 1)$ $M(x^3 - x + 1, x^2 + x + 1) = (x^3 - x + 1 - x(x^2 + x + 1), x^2 + x + 1) = M(-x^2 - 2x + 1, x^2 + x + 1) = M(2 - x, x^2 + x + 1) =$

$$M(x-2, x^2+x+1) = M(x-2, x^2+x+1-x(x-2)) = M(x-2, 3x+1) = M(x-2, 7) \\ (x^3-x+1)(x^2+x+1) = p^y$$

1. slučaj Ako je $p \neq 7$ onda su faktori s lijeve strane relativno prosti pa je neki od njih sigurno 1. $x^2+x+1 \geq 3$ pa ne može biti jedan 1, pa je $x^3-x+1=1 \implies x=1 \implies p^y=3$. Dobili smo rješenje (1, 1, 3).

2. slučaj $p=7$, najveći zajednički djelitelj faktora je 1 ili 7, i oba faktora su potencije od 7 pa jedan od njih mora biti 1 ili 7.

Ako je $x^3+x+1=1 \implies x=1 \implies p=3$ ni rješenje u ovom slučaju. Ako je $x^3+x+1=7 \implies x^3-x=6$ Rješenje za $x=2$, dalje raste pa je strogo veće od 6. $x=2 \implies 7^y=49 \implies y=2$ Rješenje (2, 2, 7). Ako je $x^2+x+1=1$ nije moguće Ako je $x^2+x+1=7 \implies x^2+x=6$, Rješenje za $x=2$, dalje raste pa je strogo veće od 6. Isto rješenje kao u prošlom slučaju (2, 2, 7).

Rješenja zadatka su (1, 1, 3) i (2, 2, 7)

13. $x^3+y^3=x^2+42xy+y^2$ Uvedemo najveći zajednički djelitelj brojeva x i y . $d=M(x,y), x=d \cdot x_1, y=d \cdot y_1, M(x_1, y_1)=1$

$$x^3+y^3=x^2+42xy+y^2 \iff d^3x_1^3+d^3y_1^3=d^2x_1^2+d^2x_1x_1+d^2y_1^2 \iff d(x_1^3+y_1^3)=x_1^2+x_1y_1+y_1^2 \iff \\ d(x_1+y_1)(x_1^2-x_1y_1+y_1^2)=x_1^2+42x_1y_1+y_1^2$$

Sada znamo da $(x_1+y_1) \mid 40x_1y_1$, Također znamo da x_1 i y_1 nemaju zajedničkih prostih faktora, pa kad bi postojao prost broj p takav da p dijeli i x_1 i x_1+y_1 onda bi p dijelio y_1 što je kontradikcija s tim da nemaju zajedničkih djelitelja, znači da x_1 i x_1+y_1 nemaju zajedničkih djelitelja. Analogno se pokaže za y_1 , pa onda vrijedi $x_1+y_1 \mid 40$ Također, znamo da $x_1^2-x_1y_1+y_1^2 \mid x_1^2+42x_1y_1+y_1^2 \implies x_1^2-x_1y_1+y_1^2 \mid 43x_1y_1$ sada ako postoji neki prosti p koji bi dijelio x_1 i $x_1^2-x_1y_1+y_1^2$ onda bi on dijelio x_1 što nije moguće. Tako da je $M(x_1^2-x_1y_1+y_1^2, x_1)=1$ Analogno se dokaže za y_1 pa vrijedi $x_1^2-x_1y_1+y_1^2 \mid 43$

To nam daje dva slučaja jer 43 ima dva prirodna djelitelja 1 i 43:

1. slučaj $x_1^2-x_1y_1+y_1^2=1 \iff (x_1-y_1)^2+x_1y_1=1$ Znamo da je $(x_1-y_1)^2 \geq 0$, uz slučaj jednakosti $x_1=y_1$, te znamo da je $x_1y_1 \geq 1$, uz slučaj jednakosti $x_1=y_1=1$

To znači da je $1=(x_1-y_1)^2+x_1y_1 \geq 0+1=1$ Budući da vrijedi jednakost u nejednakosti moraju vrijediti svi slučajevi jednakosti tj. $x_1=y_1=1 \implies x=y$ Uvrštavanjem u početnu jednadžbu dobivamo $x^3+x^3=x^2+42x^2+x^2 \iff 2x^3=44x^2 \iff x=22$, pa je jedno rješenje jednadžbe (22,22).

2. slučaj $x_1^2-x_1y_1+y_1^2=43$, Sada će nam biti korisna tvrdnja $x_1+y_1 \mid 40$ koju smo ranije dokazali. Pomoću druge tvrdnje ćemo ograničiti x_1+y_1 za koji znamo da je djelitelj od 40. $x_1^2-x_1y_1+y_1^2=43 \iff x_1^2+2x_1y_1+y_1^2=43+3x_1y_1 \geq 43+3=46$. Znači $(x_1+y_1)^2 \geq 46 \implies x_1+y_1 \geq 7$.

Također, znamo da je $x_1^2+2x_1y_1+y_1^2 \geq 4x_1y_1$, pa je $\frac{3}{4}((x_1+y_1)^2) \geq 3x_1y_1$.

Od gore znamo da je $(x_1+y_1)^2=3x_1y_1+43 \leq \frac{3}{4}((x_1+y_1)^2)+43 \implies \frac{1}{4}((x_1+y_1)^2) \leq 43 \implies (x_1+y_1)^2 \leq 4 \cdot 43=172 \implies x_1+y_1 \leq 13$.

Sada znamo da je $7 \leq x_1+y_1 \leq 13$, a također da je to djelitelj od 40 pa može biti samo 8 ili 10.

1. podslučaj: $x_1+y_1=8 \implies 64=43+3x_1y_1 \implies 3x_1y_1=21 \implies x_1y_1=7$ Sada znamo da je jedan jednak 1, a drugi 7, jednadžba je simetrična pa možemo bez smanjenja općenitosti pretpostaviti $x_1=1, y_1=7 \implies y=7x \implies x^3+343x^3=x^2+42 \cdot 7x^2+49 \cdot x^2 \implies 344x=344 \implies x=1 \implies y=7$. Dobili smo rješenja (1, 7) i (7, 1).

2. podslučaj: $x_1+y_1=10 \implies 100=43+3x_1y_1 \implies 57=3x_1y_1 \implies x_1y_1=19$ Sada znamo da je jedan jednak 1, a drugi 19, pa bez smanjenja općenitosti $x_1=1, y_1=19$ tj. $y=19x$ Uvrštavanjem u početnu $x^3+19^3x^3=x^2+42 \cdot x^2+19^2 \cdot x^2 \implies x+19^3x=19(42+19) < 19 \cdot 19^2 < x+19^3x$ Dobili smo kontradikciju, znači nema rješenja.

Ukupno postoje 3 rješenja (1,7), (7, 1) i (22, 22). [Link: BMO 2017 P1](#)

14. $y^2=x^3+7 \iff y^2+1=x^3+8$ Znamo da vrijedi da y^2+1 ne može imati djelitelja oblika $4k-1, k \in \mathbb{N}$ pa ćemo dokazati da lijeva strana uvijek sadrži takav faktor.

Ako je x paran, promatramo koje strane jednadžbe daju pri djeljenu sa 4, desna strana je djeljiva, a y^2 daje ostatke 0 ili 1, pa y^2+1 daje 1 ili 2, što nije 0 koju daje desna strana, pa nema rješenja. Ako je x neparan on daje ili ostatak 1 ili ostatak 3 pri djeljenu s 4.

$$x^3+8=(x+2)(x^2-2x+4)$$

1. slučaj. $x \equiv 1 \pmod{4} \implies x+2 \equiv 3 \pmod{4}$ Znači $x+2$ je faktor od y^2+1 oblika $4k-1$ što nije moguće.

2. slučaj $x \equiv 3 \pmod{4} \implies x^2-2x+4 \equiv 1-2 \cdot 3+4 \equiv 3 \pmod{4}$ Znači x^2-2x+4 je faktor od y^2+1 oblika $4k-1$ što nije moguće, pa jednadžba nema rješenja.

Dobili smo da jednadžba nema rješenje u skupu prirodnih brojeva.

15. $x^y - y^x = xy^2 - 19$ Ako je $x = y$ onda je $x^3 = 19$ što nema rješenja, pa znamo da su x i y različiti, a budući da su prosti oni su i relativno prosti, tj. $M(x, y) = 1$.

Sada znamo da vrijedi MFT tj. $x^y \equiv x \pmod{y}$ i $y^x \equiv y \pmod{x}$

. Ako promatramo jednadžbu modulo x dobijemo $-y \equiv -19 \pmod{x}$ tj. da vrijedi $x \mid y - 19$.

Ako promatramo jednadžbu modulo y dobijemo $x \equiv -19 \pmod{y}$, tj. da vrijedi $y \mid x + 19$. Sada uvedemo količnik za ovu tvrdnju $x + 19 = y \cdot k, k \in \mathbb{N}$.

Kad bi $y = 19$ onda $19 \mid x + 19 \implies 19 \mid x \implies x = 19$ Kontradikcija jer su x i y različiti. Znači znamo $y \neq 19$. Znamo da vrijedi $x = yk - 19$, pa $yk - 19 \mid 19 - y \implies yk - 19 \mid 19 - y + yk - 19 \implies yk - 19 \mid y(k - 1)$. Kada bi postojao prosti p takav da $p \mid y$ i $p \mid yk - 19$ onda bi vrijedilo $p \mid 19$, pa bi $p = 19$ i onda $y = 19$, što smo dokazali da nije moguće, pa znamo da je $M(y, yk - 19) = 1$ iz čega slijedi $y \mid k - 1$.

Kada bi vrijedilo $k = 1$, onda $y = x + 19$, što znači da je ili x paran ili y paran, što znači da je neki od njih jednak 2, što je moguće samo za x , ali onda je $y = 21$, što nije prost broj.

Sada znamo da je $k > 1$, pa vrijedi $x = yk - 19 \leq k - 1 \implies yk - k \leq 18 \implies k(y - 1) \leq 18$. Znamo da je $k \geq 2$, pa onda $y - 1 \geq 9 \implies y \geq 10$. Znamo da je y prost pa može biti 2, 3, 5, ili 7.

1. Slučaj: $y = 2, x \mid y - 19 \implies x \mid 17 \implies x = 17$, Uvrštavanje u početnu $17^2 - 2^{17} = 17^2 - 19$ Uočavamo da je lijeva strana negativna, a desna pozitivna pa nema rješenja.

2. Slučaj: $y = 3, x \mid y - 19 \implies x \mid 16 \implies x = 2$. Uvrštavanjem u početnu $2^3 - 3^2 = 2 \cdot -19 \iff -1 = -1$ uviđamo da smo dobili rješenje (2, 3).

3. Slučaj: $y = 5, x \mid y - 19 \implies x \mid 14 \implies x = 2$ ili $x = 7$. Uvrštavanjem u početnu $2^5 = 2 \cdot 25 - 19 \iff 7 = 31$ i Korištenjem $y \mid x + 19 \iff 5 \mid 26$ zaključujemo da nema rješenja u ovom slučaju. 4. Slučaj: $y = 7, x \mid y - 19 \implies x \mid 12 \implies x = 2$ ili $x = 3$. Uvrštavanjem u početnu $2^7 - 7^2 = 2 \cdot 49 - 19 \iff 128 - 49 = 2 \cdot 49 - 19 \iff 128 = 3 \cdot 49 - 19 \iff 128 = 147 - 19$ Uočavamo da je (2, 7) rješenje jednadžbe. Za podslučaj $x = 3, y \mid x + 19 \iff 7 \mid 22$ pa nema rješenja.

Sva rješenja su (2, 3) i (2, 7).

16. Izrazimo y iz druge jednadžbe i uvrstimo u prvu: $y = \frac{u^4 - x^2}{z}, x^2 + u \cdot \frac{u^4 - x^2}{z} = (x + u)^v \iff x^2 + \frac{u^5 - ux^2}{z} = (x + u)^v$ Primijetimo da za $v \geq 5$ desna strana sadrži pribrojnik x^v i u^v što koji su veći jednaki $x^5 + u^5$ što je strogo veće od lijeve strane, pa u tom slučaju jednadžba nema rješenja. Sada znamo da je $v \leq 4$, a v je prost pa je 2 ili 3.

1. slučaj $v = 2$, Prva jednadžba je jednaka $x^2 + yu = x^2 + 2xu + u^2 \iff yu = 2xu + u^2 \iff y = 2x + u$.

Drugu jednadžbu možemo faktorizirati $yz = (u^2 - x)(u^2 + x)$, Znamo da su y i z prosti, pa postoje 4 moguća slučaja njihova rasporeda među faktorima, no $u^2 + x$ sigurno nije 1, pa ostaju 3 podslučaja.

1. podslučaj: $u^2 + x = yz, u^2 - x = 1 \implies u^2 - 1 = yz \implies u^2 - 1 = z(u + 2x) \implies u^2 - 1 = uz + z(2u^2 - 2) \implies u^2 - 1 = uz + u^2 2z - 2z \implies u^2(2z - 2) + z(u - 2) + 1 = 0$ Prosti brojevi su uvijek veći jednaki 2, pa je desna strana sigurno barem 1, pa ovaj slučaj nema rješenja.

2. podslučaj: $u^2 + x = y, u^2 - x = z, u^2 + x = y \iff u^2 + x = u + 2x \iff u^2 - u = x \iff u(u - 1) = x$, Za $u \geq 3$ je x umnožak dva broja veća od 1, pa ne može biti prost. Znači $u = 2 \implies x = 2 \implies y = 6$, nije moguće jer 6 nije prost.

3. podslučaj: $u^2 + x = z, u^2 - x = y, u^2 - x = y \iff u^2 - x = u + 2x \iff u^2 - u = 3x \iff u(u - 1) = 3x$. Ako je $u \geq 5$, onda su oba faktora s lijeve strane veća od 3, pa onaj količnik od onog koji je djeljiv s 3 će i dalje biti veći od 1, pa će x biti umnožak dva broja veća od 1, što nije moguće. Znači $u = 2$ ili $u = 3$. Za $u = 2 \implies 2 = 3x$, nema rješenja. Za $u = 3 \implies x = 2 \implies z = 11, y = 7$. Uvrstimo u početne jednadžbe $4 + 21 = (2 + 3)^2, 4 + 77 = 3^4$. Uviđamo da obje vrijede pa je to rješenje početne jednadžbe, uz $v = 2$.

2. slučaj $v = 3, izyz = (u^2 + x)(u^2 - x)$ kada se provjere sva 4 slučaja za raspored y i z među faktorima, slijedi da je y maksimalno $u^2 + x$, što znači da je $x^2 + yu$, maksimalno $x^2 + u^3 + ux$ što je strogo manje od $(x + u)^3 = x^3 + 3x^2u + 3xu^2 + u^3$ pa jednadžba nema rješenja u ovom slučaju.

Jedino rješenje je $x = 2, y = 7, z = 11, u = 3, v = 2$.

Izvor: BMO SHORTLIST 2005

17. $(m^3 + n)(n^3 + m) = p^3$ Imamo umnožak dva broja koji je jednak p^3 pa je ili jedan jednak 1, a drugi p^3 ili je jedan jednak p , a drugi p^2 . Oba broja su veća od 2, pa niti jedan ne može biti 1, pa je jedan jednak p , a drugi p^2 . Bez smanjenja općenitosti smijemo pretpostaviti da je $m^3 + n = p^2, n^3 + m = p$.

Kad bi $p \leq m$ vrijedilo bi $m^3 + n = p^2 \leq m^2$ Kontrakcija, pa znamo $p > m$.

Ako oduzmemo te dvije jednadžbe jednu od druge dobijemo $p^2 - p = m^3 - n^3 - m + n \iff p(p - 1) = (m - n)(m^2 + mn + n^2 - 1)$. Lijeva strana je pozitivna pa je sigurno $m > n$ Ako p dijeli $m - n$, onda je ili $n = m$, pa bi onda vrijedilo $p = p^2$, što nije moguće, ili je $m - n \geq p$ no onda je $m > p$ što nije moguće. Znači da p mora dijeliti drugi faktor, tj. $m^2 + mn + n^2 - 1$.

$p \mid m^2 + mn + n^2 - 1 \implies p \mid m^3 + nm^2 + n^2m - m$. Znamo da $p \mid m^3 + n$, pa vrijedi $p \mid m^3 + nm^2 + n^2m - m - m^3 - n \implies p \mid nm^2 + n^2m - m - n \implies p \mid mn(m + n) - (m + n) \implies p \mid (m + n)(mn - 1)$. Sada imamo dva slučaja u ovisnosti o tome koji faktor p dijeli:

1. slučaj $p \mid m + n \implies p \leq m + n \implies p \leq 2m - 1 \implies m^3 + n = p^2 \leq (2m - 1)^2 \implies m^3 + n \leq 4m^2 - 4m + 1 \implies m^3 - 4m^2 + 4m + n - 1 \leq 0$ Ovo očito ne vrijedi za $m \geq 4$, pa je $m \leq 3 \implies p \leq 5$

1. podslučaj: $p = 2 \implies n^3 + m = 2 \implies n = 1, m = 1 \implies 2 = m^3 + n = p^2 = 4$ Kontradikcija.

2. podslučaj $p = 3 \implies n^3 + m = 3 \implies n = 1 \implies m = 2$ Uvrstimo u $m^3 + n = 2^3 + 1 = 9$ Vrijedi tvrdnja zadatka, pa znamo da su $(1, 2, 3)$ i $(2, 1, 3)$ rješenja.

3. podslučaj $p = 5 \implies n^3 + m = 5 \implies n = 1 \implies m = 4 \implies 4^3 + 1 = 5^2$ Što ne vrijedi, pa ovaj slučaj nema rješenja.

2. Slučaj $p \mid nm - 1, n = m = 1$ nije rješenje pa vrijedi $p \leq nm - 1$.

$n^3 + m = p \leq nm - 1 \implies n^3 + m \leq nm - 1 \implies m \geq n^2 + 1$

$m^3 + n \geq m^2(n^2 + 1) + n = m^2n^2 + m^2 + n \leq mn - 1 \implies m^3 + n = p^2 \leq (nm - 1)^2 \implies m^3 + n \leq n^2m^2 - 2nm + 1$
 $m^2n^2 + m^2 + n \leq m^2n^2 - 2nm + 1 \implies m^2 + 2nm + n \leq 1$ što nije moguće, pa ovaj slučaj nema rješenja.

18. Ako je $n = 1$ onda za svaki k postoji rješenje $x = 3^k - 1$ pa su rješenja sve uređene trojke oblika $(k, 3^k - 1, 1), k \in \mathbb{N}$. U ostatku rješenja pretpostavljamo $n > 1$

Kad bi n bio paran $x^n + 1$ je broj oblika $y^2 + 1, y \in \mathbb{N}$, pa ne može biti djeljiv s brojem koji daje ostatak 3 pri djeljenju s 4, no to vrijedi za 3, pa onda jednačba nema rješenja. Znači n je neparan i veći od 1.

$x = 1 \implies 3^k = 2$, nije moguće, pa znamo da je $x \geq 2$

Sada možemo prebaciti 1 na desnu stranu i faktorizirati $3^k = (x + 1)(x^{(n-1)} - x^{n-2} + \dots - x + 1)$ Sada vidimo da faktori s desne strane oba moraju biti potencije od 3. Također, znamo da je desni faktor $\geq x^2 - x + 1 = x(x - 1) + 1 \geq x + 1$. Dva broja su potencije od 3, pa minimalni od njih sigurno mora dijeliti veći. Vrijedi

$$x + 1 \mid x^{(n-1)} - x^{n-2} + \dots - x + 1 = \sum_{i=0}^{n-1} (x^i \cdot (-1)^i)$$

Promatram ostatak koji suma daje pri djeljenju s $x + 1$: $\sum_{i=0}^{n-1} (x^i \cdot (-1)^i) \equiv \sum_{i=0}^{n-1} ((-1)^i \cdot (-1)^i) \equiv \sum_{i=0}^{n-1} ((-1)^{2i}) \equiv$

$$\sum_{i=0}^{n-1} (1) \equiv n \pmod{x + 1}$$

Znači suma daje isti ostatak pri djeljenju s $x + 1$ kao n , što znači da je n djeljiv s $x + 1$.

Znamo da $3 \mid (x + 1)$, pa onda $3 \mid n \implies n = 3a, a \in \mathbb{N}$.

Jednačba sada izgleda $3^k = x^{3a} + 1 \iff 3^k = (x^a + 1)(x^{2a} - x^a + 1)$ Znamo da je $x^a + 1$ potencija od 3, pa je $x^a + 1 = 3^t, t \in \mathbb{N}$. $x^{2a} - x^a + 1 = (3^t - 1)^2 - 3^t + 1 + 1 = 3^{2t} - 2 \cdot 3^t + 1 - 3^t + 1 + 1 = 3^{2t} - 3(t + 1) + 3$. Ovaj broj bi trebao biti potencija od 3, jer dijeli 3^k , no za $t \geq 2$ je veći od 3, ali daje ostatak 3, pri djeljenju s 9, pa ne može biti potencija broja 3.

Za $t = 1$ je $x^a = 2 \implies x = 2, a = 1 \implies 3^k = 3(4 - 2 + 1) \implies k = 2$ Uvrštavanjem u početnu uviđamo da $(2, 2, 3)$ stvarno je rješenje.