Друштво математичара Србије
РЕШЕЊА ЗАДАТАКА - 18. СМО, Београд 2024.

Први дан

1. (ПРВО РЕШЕЊЕ) Доказаћемо да је број n решење задатка акко је $n = p^{k-1}$, за ма који прост број p.
Нека је неки природан број n решење задатка. Делилац d_2 је прост број, те нека је $d_2 = p$. За сваки природан број n важи $d_i \cdot d_{k+1-i} = n,\ i = \overline{1,k}$, те је, специјално, $d_{k-1} = \frac{n}{p}$. Највећи од посматраних бројева је број $d_k - d_{k-1}$, пошто је $d_k - d_{k-1} \geqslant n - \frac{n}{2} \geqslant d_{k-1} > d_{i+1} - d_i$, за свако $i = \overline{1,k-2}$. Без умањења општости можемо претпоставити да су посматрани бројеви поређани у строго растућем поретку и нека је $c > 1$ количник геометријске прогресије (број c је као количник два природна броја рационалан, али не нужно и природан). За неко $i \in \mathbb{N}$ важи $c^i = \frac{d_k - d_{k-1}}{d_2 - d_1} = \frac{n - \frac{n}{p}}{p-1} = \frac{n}{p} \in \mathbb{N}$. Дакле, неки степен рационалног броја c једнак је природном броју, те и број c мора бити природан (пошто је $i-$ти корен природног броја или ирационалан број или природан број). Сада знамо да је $c > 1$ неки делилац броја n, пошто $c \mid c^i \mid \frac{n}{p} \mid n$, те је $c \geqslant p$. Отуда је најмања од посматраних разлика баш $d_2 - d_1 = p - 1$ (уколико не би била, онда међу разликама постоји и $\frac{d_2 - d_1}{c} < 1$, што није цео број). Дакле, највећа разлика је $d_k - d_{k-1}$, док је најмања $d_2 - d_1$, те је

$$c^{k-2} = \frac{d_k - d_{k-1}}{d_2 - d_1} = \frac{n}{p}. \qquad (\diamondsuit)$$

Збир свих посматраних разлика, изузев највеће $d_k - d_{k-1}$, са једне стране једнак је $d_{k-1} - d_1 = \frac{n}{p} - 1$, док је са друге стране (као геометријска прогресија са првим чланом $d_2 - d_1$ и количником c) једнак $(p-1) \cdot \frac{c^{k-2}-1}{c-1}$. Зато сада, користећи $(\diamondsuit)$, добијамо $\frac{n}{p} - 1 = (p-1) \cdot \frac{c^{k-2}-1}{c-1} = (p-1) \cdot \frac{\frac{n}{p}-1}{c-1}$, те је $c = p$. Овим смо доказали да су једини кандидати за решења задатка бројеви облика $n = p^{k-1}$. Докажимо да су овакви бројеви n заиста решења задатка. Заиста, ако је $n = p^{k-1}$, тада је $d_i = p^{i-1},\ i = \overline{1,k}$, те је $\frac{d_{i+2} - d_{i+1}}{d_{i+1} - d_i} = \frac{p^{i+1} - p^i}{p^i - p^{i-1}} = p$, за свако $i = \overline{1,k-2}$. Ово сведочи да за $n = p^{k-1}$ постоји пермутација бројева $d_2 - d_1, d_3 - d_2, d_4 - d_3, ..., d_k - d_{k-1}$ тако да они чине коначну геометријску прогресију.
(ДРУГО РЕШЕЊЕ) Делилац d_2 броја n је прост број, те нека је $d_2 = p$. За сваки природан број n важи $d_i \cdot d_{k+1-i} = n,\ i = \overline{1,k}$, те је, специјално, $d_{k-1} = \frac{n}{p}$ и $d_{k-2} = \frac{n}{d_3}$. Највећи од посматраних бројева је број $d_k - d_{k-1}$, пошто је $d_k - d_{k-1} \geqslant n - \frac{n}{2} \geqslant d_{k-1} > d_{i+1} - d_i$, за свако $i = \overline{1,k-2}$. Без умањења општости можемо претпоставити да су посматрани бројеви поређани у строго растућем поретку и нека је $c > 1$ количник геометријске прогресије (број c је као количник два природна броја рационалан, али не нужно и природан). За неко $i \in \mathbb{N}$ важи $c^i = \frac{d_k - d_{k-1}}{d_2 - d_1} = \frac{n - \frac{n}{p}}{p-1} = \frac{n}{p} \in \mathbb{N}$. Дакле, неки степен рационалног броја c једнак је природном броју, те и број c мора бити природан (пошто је $i-$ти корен природног броја или ирационалан број или природан број). За неко $j \in \mathbb{Z}$ важи $c^j = \frac{d_{k-1} - d_{k-2}}{d_3 - d_2} = \frac{\frac{n}{p} - \frac{n}{d_3}}{d_3 - p} = \frac{n}{pd_3}$ (може се доказати и да је $j \in \mathbb{N}_0$, али то није важно за решење). Сада је $c^{i-j} = \frac{\frac{n}{p}}{\frac{n}{pd_3}} = d_3$, те како је $c > 1$, то је d_3 степен природног броја c. Сада разликујемо следеће случајеве:
1° d_3 је прост број. Нека је $d_3 = q > p$. Тада из $c^{i-j} = q$ имамо да је $c = q$. Међу посматраним бројевима најмањи је број $d_2 - d_1 = p - 1$. Заиста, уколико то не би био случај, онда би број $\frac{d_2 - d_1}{c} = \frac{p-1}{q} < 1$ био неки од посматраних бројева, што није могуће (сви посматрани бројеви су природни). Зато сада једнакост $c^i = \frac{n}{p}$ постаје једнакост

$q^{k-2} = \frac{n}{p}$, те је $n = p \cdot q^{k-2}$. Међутим, сада је $k = \tau(n) = 2(k-1) = 2k-2 \Leftrightarrow k = 2$. Контрадикција.
2° d_3 је сложен број. Сви делиоци броја d_3, мањи од d_3, деле број n и припадају скупу $\{1, p\}$. Зато је $d_3 = p^2$. Сада једнакост $c^{i-j} = d_3$ постаје једнакост $c^{i-j} = p^2$, те је $c \in \{p, p^2\}$. На идентичан начин као у 1° закључујемо да је и сада међу посматраним бројевима најмањи број $d_2 - d_1 = p - 1$. Зато сада једнакост $c^i = \frac{n}{p}$ постаје једнакост $c^{k-2} = \frac{n}{p}$, па је $n = p^{k-1}$ или $n = p^{2k-3}$. Друга могућност отпада јер би тада важило $k = \tau(n) = 2k-2 \geqslant k+2$. Овим смо доказали да су једини кандидати за решења задатка бројеви облика $n = p^{k-1}$. Докажимо да су овакви бројеви n заиста решења задатка. Заиста, ако је $n = p^{k-1}$, тада је $d_i = p^{i-1}$, $i = \overline{1,k}$, те је $\frac{d_{i+2}-d_{i+1}}{d_{i+1}-d_i} = \frac{p^{i+1}-p^i}{p^i-p^{i-1}} = p$, за свако $i = \overline{1,k-2}$. Ово сведочи да за $n = p^{k-1}$ постоји пермутација бројева $d_2-d_1, d_3-d_2, d_4-d_3, ..., d_k-d_{k-1}$ тако да чине коначну геометријску прогресију.

2. Одговор: $n! \cdot 2^n$. Ставимо да је $[n] = \{1, 2, \ldots, n\}$. Фиксирајмо индекс победника турнира $1 \leqslant x \leqslant 2^n$. Доказаћемо да постоји $n!$ турнира у којима он побеђује. Означимо са A_i скуп људи који су остали на турниру после i кола. Тада је $A_n = \{x\}$ и $A_0 = \{1, 2, \ldots, 2^n\}$. Тврђење задатка нам каже да за свако $i \in \{1, 2, \ldots, n\}$ постоји број x_i тако да је $A_{i-1} = A_i \cup (x_i - A_i)$ (односно, ако је сума индекса у сваком двобоју x_i, тада, ако је $a \in A_i$, мора бити и $\{a, x_i - a\} \subset A_{i-1}$). Кључно тврђење у решењу ће нам бити да за свако $i \in \{1, 2, \ldots, n\}$ постоји a_i тако да је $A_{i-1} = A_i \cup (a_i + A_i)$. За $i = n$ је ово очигледно, тако да нас интересују само преостали случајеви. Приметимо да је $A_i = x_{i+1} - A_i$, те је $A_{i-1} = A_i \cup (x_i - A_i) = A_i \cup (x_i - x_{i+1} + A_i)$, те, стога, можемо узети да је $a_i = x_i - x_{i+1}$. Отуда, n-торке које формирају x_i, који одговарају валидним решењима, као и n-торке формиране од a_i, који исто одговарају валидним решењима, су бијективно еквивалентне. Одавде следи да морамо да избројимо колико постоји избора n-торки $(a_1, a_2, \ldots, a_n)$, тако да кад дефинишемо $A_n = \{x\}$ и $A_{i-1} = A_i \cup (a_i + A_i)$, да је тада $A_0 = \{1, 2, \cdots, 2^n\}$. Није тешко показати (принципом математичке индукције) да ће скуп A_0 бити облика

$$A_0 = \{x + \sum_{i \in I} a_i | I \subset [n]\},$$

где се празна сума дефинише као 0. Ово значи да $a_1, a_2, \ldots, a_n$ треба да буду такви цели бројеви тако да је сваки број од $-x+1$ до $2^n - x$ представљив на јединствен начин као сума неких a_i (јединственост следи јер је сума исто 2^n). Доказаћемо да је избор оваквих бројева јединствен (до на пермутацију), те је одговор заиста $n!$, за свако x, односно $n! \cdot 2^n$ укупно, чиме је доказ завршен.

Докажимо претходно случају када је $x = 1$. Потребно је да докажемо да постоје јединствени бројеви $b_1 < b_2 < \ldots < b_n$, такви да се сваки број од 1 до $2^n - 1$ може добити као сума неколико њих. Приметимо да ниједан од b_i није негативан, јер ниједна сума није негативна. Докажимо индукцијом да је $b_k = 2^{k-1}$, за свако k. Заиста, ако је $b_i = 2^{i-1}$, за свако $i < k$, тада преко првих k бројева можемо добити све бројеве од 1 до $2^k - 1$, тако што га напишемо у бинарном запису, те тада ниједан други број мањи од 2^k не може бити међу b_i, због јединствености, а ако су преостали b_i већи од 2^k, онда се 2^k неће никако моћи представити као сума неких b_i. Овиме је индукција завршена.

Сада, за генерално x, мора да постоји неки подскуп $C \subset \{a_1, \ldots, a_n\}$, такав да је $\sum_{c \in C} c = -x + 1$. Посматрајмо, затим, скуп B, који формирамо на следећи начин: $\{a_1, a_2, \ldots, a_n\} \setminus C \subset B$, као и ако је $c \in C$, тада је $-c \in B$. Ако је $B = \{b_1, b_2, \ldots, b_n\}$, знамо да је тада $-x + 1 + \sum_{i \in I} b_i$, за $I \subset [n]$, узима све вредности између $-x+1$ и $2^n - x$ (јер "избацивање" неког сабирка $c \in C$, почевши од 0, је исто као додавање $-c$, почевши од $-x + 1$). Међутим, по претходном случају је тада $B = \{1, 2, 4, \ldots, 2^{n-1}\}$, а оне које треба претворити у негативне су управо они који учествују у бинарном запису броја $x - 1$ (јер је у питању највећи негативан број, те је сума свих негативних бројева).

3. Лема: Нека је $f(x)$ функција облика $f(x) = \sum_{i=1}^{n} |x - x_i|$ за неке $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. Тада она минимум достиже у медијани низа x_i (у случају непарног n, свакако, док за парно n минимум се постиже у свакој тачки интервала $[x_{\lfloor \frac{n+1}{2} \rfloor}, x_{\lceil \frac{n+1}{2} \rceil}]$, а у том случају је мадијана заправо аритметичка средина крајева претходно наведеног интервала, која припада том интервалу). Заиста, ако је $x < x_1$, тада је $f(x) > f(x_1)$, док за $x > x_n$ је $f(x) > f(x_n)$, као и да за $x \in [x_i, x_{i+1}]$ важи $f(x) \geqslant \min(f(x_i), f(x_{i+1}))$, јер је на овим интервалима функција линеарна. Стога, видимо да фунцкија f, на $[x_i, x_{i+1}]$, достиже минимум у једној од крајњих тачака тог интервала. Такође, јасно је да је нагиб те линеарне фунцкије на интервалу $[x_i, x_{i+1}]$ заправо $i - (n - i) = 2i - n$, па за $i \leqslant \frac{n}{2}$ важи $f(x_i) \geqslant f(x_{i+1})$, а за $i \geqslant \frac{n}{2}$ је $f(x_i) \leqslant f(x_{i+1})$. Из овога следи да се минимум, заиста, достиже у $x_{\lfloor \frac{n+1}{2} \rfloor}$, за n непарно, односно у било којој тачки интервала $[x_{\lfloor \frac{n+1}{2} \rfloor}, x_{\lceil \frac{n+1}{2} \rceil}]$, за парне n.

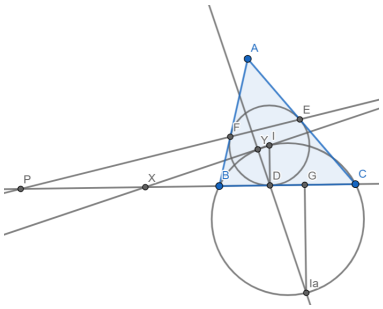
Без умањења општости препоставимо да је $\alpha^2 + \beta^2 = 1$ (скалирањем се ништа не мења). Посматрајмо дате у пару, тј. као n тачака у координатном систему: (a_1, b_1), (a_2, b_2), $\cdots$, (a_n, b_n). Нека је ℓ права која пролази кроз координатни почетак, тј. тачку $O = (0, 0)$, и тачку $M = (\alpha, \beta)$ и нека је c_i растојање од координатног почетка до пројекције из тачке (a_i, b_i) на ℓ (посматрамо оријентисане дужине, што значи да могу бити и негативне, тј. узећемо да дужина c_i иде са негативним предзнаком ако је вектор $\overrightarrow{OP_i}$ супротног смера од вектора $\overrightarrow{OM}$, где је P_i одговарајућа пројекција. Сада, кључно је приметити да је $\alpha a_i + \beta b_i = \frac{(\alpha,\beta)\cdot(a_i,b_i)}{||(\alpha,\beta)||} = c_i$, при чему прва једнакост следи из дефиниције скаларног производа и тога што је $\alpha^2 + \beta^2 = 1$, а друга је познати начин за рачунање дужине пројекције на основу скаларног производа. Сада $p_j = \sum_{i=1}^{n} |c_i - c_j|$, па нам треба да је c_m медијана у низу $c_1, c_2, \cdots, c_n$. Приметимо да је ово еквивалентно са тиме да, ако повучемо нормалу на ℓ у тачки (a_m, b_m), да има највише $\lceil \frac{n}{2} \rceil$ тачака са обе стране те праве.

Стога, свакој правој кроз (a_m, b_m) можемо приписати праву ℓ нормалну на њу кроз координатни почетак и одговарајуће α и β, тако да нам је задатак еквивалентан са тиме да кроз (a_m, b_m) постоји највише $\lceil \frac{n}{2} \rceil$ тачака са обе стране те праве (тачке на самој правој нам нису проблем, јер је медијана једнака c_m ако је испуњен овај услов). Повуцимо произвољну праву кроз (a_m, b_m) која не садржи ниједну другу тачку из скупа. Са једне стране је више од пола осталих тачака, а са друге мање од пола. Тада, постепено ротирамо праву користећи дискретну непрекидност. Нека је са леве стране l тачака, а са десне те праве d тачака. Зарад лакшег завршетка, замишљајмо да кад нам права пролази кроз више тачака одједном, да те тачке додајемо једну по једну из једне области у другу (ако нам се негде на пола овог додавања догоди $|l - d| \leqslant 1$, онда ће нам бити сигурно добра права, јер те тачке на самој правој се не рачунају, па није битно којој половини их приписујемо, јер ће свакако бити мање од пола). С обзиром да је на почетку $l \geqslant d$, а на крају $l \leqslant d$ или обрнуто, те у сваком тренутку се разлика $l - d$ мења за највише 2, постојаће тренутак где има највише пола са обе стране ове праве, што нам завршава доказ.

Друштво математичара Србије
РЕШЕЊА - 18. СМО, Београд 2024.

Други дан

4. (ПРВО РЕШЕЊЕ) Нека је Y други пресек праве XI са кружницом описаном око троугла BIC. Доказаћемо да је Y тачка тражене нормалности. Прво, знамо да је, по Менелајевој теореми, испуњено $\frac{PB}{PC}\frac{EC}{EA}\frac{AF}{FB} = 1 \implies \frac{PB}{PC} = \frac{DB}{DC}$, па је $(B, C; D, P)$ хармонијски прамен. Сада, познатно да је да се инверзијом у односу на Аполонијеву кружницу тачке хармонијске четворке сликају једне у друге, одакле произилази да је $XB \cdot XC = XD^2$. Међутим, сада је $XD^2 = XB \cdot XC = XI \cdot XY$, па, како је $\sphericalangle XDI = 90°$, знамо да је $\sphericalangle IYD = 90°$. Међутим, како знамо да је I_a такође на кружници описаној око троугла BIC (дијаметрално супротна тачка од тачке I), тада је $\sphericalangle IYI_a = 90°$, те су тачке Y, I_a, D колинеарне, из чега следи тврђење.



(ДРУГО РЕШЕЊЕ) Нека је G подножје висине из тачке I_a на праву BC. Доказаћемо да су троуглови $\triangle I_aGD$ и $\triangle XDI$ слични, из чега ће нам решење директно следити. Заиста, ако је Y пресек XI и I_aD, онда би важило $\sphericalangle XYD = \sphericalangle YXD + \sphericalangle XDY = \sphericalangle DI_aG + \sphericalangle I_aDG = 90°$. Сада нам је потребно да докажемо $\frac{I_aG}{DG} = \frac{XD}{ID} \iff \frac{r_a}{b-c} = \frac{XD}{r}$. Дужину $XD = \frac{1}{2}PD$ рачунамо преко Менелајеве теореме, као и у претходном решењу. Јасно је да важи $\frac{PB}{PC} = \frac{DB}{DC} = \frac{a+c-b}{a+b-c}$, а како је $PC - PB = a$, то је

$$PC(1 - \frac{a+c-b}{a+b-c}) = a \implies PC = \frac{a(a+b-c)}{2(b-c)},$$

те је, коначно,

$$PD = PC - CD = \frac{a(a+b-c)}{2(b-c)} - \frac{a+b-c}{2} = \frac{(a+c-b)(a+b-c)}{2(b-c)}.$$

Сада нам се сличност своди на то да је $rr_a = \frac{a+b-c}{2}\frac{a+c-b}{2}$, што и није тешко видети да је тачно, јер је $\triangle BID \sim \triangle I_aGB$, што се тривијално добија на основу рачунања одговарајућих углова.

(ТРЕЋЕ РЕШЕЊЕ) Нека су N и M средишта FD и FE редом. Пошто инверзија у односу на уписани круг, шаље N и M у B и C редом, онда су поларе тачака N и M редом заправо спољне симетрале углова ABC код B и C. Међутим, то значи да, с обзиром да тачка I_a лежи на обе ове спољне симетрале, да је права NM заправо полара тачке I_a. Због хомотетије, знамо да су тачке X, N, M колинеарне. Такође, BC је полара тачке D. Са друге стране, тачка X лежи у пресеку полара тачака D и I_a, па је DI_a полара тачке X, из чега одмах следи тврђење задатка.

(ЧЕТВРТО РЕШЕЊЕ) У овом случају ћемо задатак решити уз помоћ комплексних бројева. Нека је уписана кружница троугла ABC јединичнна кружница равни и нека тачкама A, B, C, D, E и F одговарају, редом, комплексни бројеви a, b, c, d, e и f. Користићемо познате формуле:

- $I_a = \frac{4def}{(d+e)(d+f)}$
- $P = \frac{d^2(e+f)-2def}{d^2-ef}$.

Следи, $X = \frac{d^2(d+e+f)-3def}{2(d^2-ef)}$ и $I_a - d = \frac{3def-d^2(d+e+f)}{(d+e)(d+f)}$. Дакле, како је ортогоналност еквивалентна са тим да је $\frac{I_a-d}{X} = -\frac{2(d^2-ef)}{(d+e)(d+f)}$ чисто имагинаран комплексан број, доказ је завршен.

5. Ако је $w \in \mathbb{C}$ и важи $|w| = 1$, онда је $Re(w) = \frac{w+\overline{w}}{2} \cdot \frac{w}{w} = \frac{w^2+1}{2w}$.(∗) Нека је $z = e^{ix}$, $\varepsilon = e^{i\frac{2\pi}{n}}$ и K јединична кружница у комплексној равни чији је центар у 0. Посматрајмо функцију $g : K \to \mathbb{R}$, дефинисану са

$$g(z) = (z + \frac{1}{z})^k + (z\varepsilon + \frac{1}{z\varepsilon})^k + (z\varepsilon^2 + \frac{1}{z\varepsilon^2})^k + ... + (z\varepsilon^{n-1} + \frac{1}{z\varepsilon^{n-1}})^k, \quad \text{за свако} \quad z \in K. \quad (\dagger)$$

Због (∗) је очигледно да је функција f константна акко је функција g константна. Користећи биномну формулу имамо да је $g(z) = a_k z^k + a_{k-1} z^{k-1} + ... + a_1 z + a_0 + a_1 z^{-1} + ... + a_{k-1} z^{-(k-1)} + a_k z^{-k}$. Функција g је константна акко за неку константу c важи једнакост

$$P(z) = a_k z^{2k} + a_{k-1} z^{2k-1} + ... + a_1 z^{k+1} + (a_0 - c) z^k + a_1 z^{k-1} + ... + a_{k-1} z^{1)} + a_k = 0, \text{ за свако } z \in K.$$

Ако је $P(z) = 0$, за свако $z \in K$, онда $P(z)$ има бесконачно много нула, па је идентички једнак нула полиному. Како обрат очигледно важи, добијамо да је g константна акко важи $a_k = a_{k-1} = ... = a_1 = 0$. Нека је сада $0 < t \leqslant k$. Примењујући биномну формулу у (†) имамо да је $a_t = 0$ ако је $t \not\equiv_2 k$, док за $t \equiv_2 k$ важи

$$a_t = \binom{k}{\frac{k+t}{2}} (1 + \varepsilon^t + \varepsilon^{2t} + ... + \varepsilon^{(n-1)t}). \quad (\heartsuit)$$

Уколико је $\varepsilon^t = 1$, што је еквивалентно са $n \mid t$, онда из (♡) имамо да је $a_t \neq 0$. Са друге стране, за све t за које је $\varepsilon^t \neq 1$, односно када $n \nmid t$, имамо да је $1 + \varepsilon^t + \varepsilon^{2t} + ... + \varepsilon^{(n-1)t} = \frac{1-\varepsilon^{nt}}{1-\varepsilon^t} = 0$, те је $a_t = 0$. Из свега наведеног закључујемо да је број k решење акко сваки број t, $0 < t \leqslant k$, који је исте парности са k, није дељив са n. (!) Зато коначно имамо следећа два случаја:
1° n је паран: Парни бројеви k за које важи $k \geqslant n$, нису решења, пошто $t = n$ не задовољава наведени услов (!). Сви непарни бројеви k, $k > n$, као и сви бројеви $k < n$ задовољавају услов (!), те јесу решења.
2° n је непаран: Непарни бројеви k за које важи $k \geqslant n$, нису решења, пошто $t = n$ не задовољава наведени услов (!). Такође, ако је k паран и важи $k \geqslant 2n$, он није решење, пошто $t = 2n$ не задовољава наведени услов (!). У овом случају су решења сви бројеви k за које је $k < n$, као и сви парни бројеви k већи од n и мањи од $2n$.

6. Уколико је $P(x) - x = c$ константан полином, број $m^2 + 2mnc + n^2$ је квадрат за све природне бројеве m и n, одакле је $1 + 2nc + n^2 = (n+c)^2 + 1 - c^2$ увек потпун квадрат. Како је онда константан број $1 - c^2$ разлика квадрата бесконачно много парова целих бројева, он мора бити 0 (имао би бесконачно много целих делилаца). Дакле, у овом случају су једина решења $P(x) = x \pm 1$, која очито исуњавају услов, јер $P^{2mn}(m^2) + n^2 = (m \pm n)^2$ у тим случајевима. Докажимо да других решења нема.

Ако полином $P(x)-x$ није константан, то очито није ни $Q(x)=P(x^2)-x^2$, па на основу Шурове теореме закључујемо да полином Q има бесконачно много простих делилаца. Дакле, постоји бесконачно простих бројева p за које постоји природан број m такав да важи $p \mid Q(m)$. Посматрајмо ове парове. Како је $P(m^2) \equiv m^2 \pmod{p}$, једноставном индукцијом (због $P(a) \equiv P(b) \pmod{a-b}$, за све целе бројеве a и b) закључујемо $P^l(m^2) \equiv P^{l-1}(m^2) \equiv ...P(m^2) \equiv m^2 \pmod{p}$, за свако $l \in \mathbb{N}$, одакле је $P^{2mn}(m^2)+n^2 \equiv m^2+n^2 \pmod{p}$. Закључили смо да ако $p \mid Q(m)$, онда је $a+m^2$ квадратни остатак по модулу p за сваки квадратни остатак (0 сматрамо квадратним остатком у овом случају) $a \pmod{p}$, одакле се, индукцијом, закључује да је $a+tm^2$ квадратни остатак по модулу p, за сваки природан број t. Почетним узимањем $a=0$, закључујемо да је tm^2 увек квадратни остатак по модулу p, одакле је $p=2$ или $p \mid m$ (уколико друго не важи, tm^2 може постићи све остатке по модулу p, а квадратних је тачно $1+\frac{p-1}{2}=\frac{p+1}{2}<p$ када је $p>2$). Дакле, доказали смо својство: ако $p \mid Q(m)$, онда је $p=2$ или $p \mid m$. Назовимо ово својство s.

Нека је, сада, $Q(x)=x^tR(x)$, $t \geqslant 0$ $R(0) \neq 0$. Како се својство s очигледно преноси и на полином R ($p \mid R(m) \implies p \mid Q(m) \implies s$), он мора бити константан. Заиста, у супротном би, по Шуровој теореми, R имао произвољно велике просте делиоце. Када би било $p>|R(0)|$, $p>2$ и $p \mid R(m)$, не може бити $p \mid m$, јер би тада важило $R(m) \equiv R(0) \not\equiv 0 \pmod{p}$, што је у контрадикцији са својством s. Дакле, $R(x)=u$ је константан полином, одакле, на основу својства s, u мора бити степен двојке, $u=\pm 2^k$, $k \in \mathbb{N} \cup \{0\}$. Дакле, важи $P(x^2)-x^2=Q(x)=\pm 2^k x^t$, одакле је $t=2r$ паран ненегативан број, тј. добијамо полиномски идентитет, те је $P(x)-x=\pm 2^k x^r$, $P(x)=x \pm 2^k x^r$. Приметимо да овде, под претпоставком $P(x)-x \neq const$, имамо $r \geqslant 1$, па је, на основу позитивности водећег коефицијента полинома P, $P(x)=x+2^k x^r$. Ако је $k \geqslant 2$, важи $P(v) \equiv v \pmod{4}$ $\forall v \in \mathbb{N}$, $P^l(v) \equiv v \pmod{4}$, за свако $l \in \mathbb{N}$. За $m=n=1$, важи $P^2(1)+1 \equiv 1+1=2 \pmod{4}$, па он не може бити потпун квадрат.

Дакле, на основу свега претходног, може бити $k=0$ или $k=1$, односно $P(x)=x+x^r$ или $P(x)=x+2x^r$. Степен r ћемо одредити на основу чињенице да је $P^2(1)+1$ потпун квадрат. У првом случају је $P(1)=2$, па је $P^2(1)+1=P(2)+1=2^r+3$, што не може бити потпун квадрат ни за један природан број r, јер за $r \geqslant 2$ важи $2^r+3 \equiv 3 \pmod{4}$, а $r=1$ не испуњава услов. У другом случају је $P^2(1)+1=P(3)+1=2 \cdot 3^r+4 \equiv 2 \pmod{4}$, па ни у овом случају нема решења. Дакле, тврђење је у потпуности доказано.