O indirektnom dokazu u matematici

Šefket Arslanagić[1]

Matematičke tvrdnje, u pravilu, imaju oblik univerzalnog suda (iskaza) „svi *P* su *Q*". Ovaj sud najčešće ima kondicionalni (pogodbeni) oblik:

Ako je P, onda je Q. (I)

To obilježavamo s $P \Rightarrow Q$, a čita se još i „iz *P* slijedi *Q*", npr. „Ako je zbroj znamenaka cijelog broja djeljiv brojem 3, onda je taj broj djeljiv brojem 3". Često se tvrdnja koja nije u kondicionalnom obliku može dovesti na taj oblik. Evo nekoliko primjera.

Primjer 1. Zbroj veličina unutarnjih kutova α, β, γ trokuta ΔABC iznosi 180°.

Kondicionalni oblik: Ako su α, β, γ veličine unutarnjih kutova trokuta ΔABC, onda je $\alpha + \beta + \gamma = 180°$.

Primjer 2. Dijagonale paralelograma se raspolavljaju.

Kondicionalni oblik: Ako je četverokut paralelogram, onda se njegove dijagonale raspolavljaju.

Vidimo da matematička tvrdnja (I) sadrži dva dijela. Prvi dio *P* zove se pretpostavka ili hipoteza (*antecedens*), a drugi dio *Q* zaključak (tvrdnja) ili teza (*konsekvens*).

Sudovima (iskazima) pripisuje se kvaliteta *istinit* (točan, vrijedi) ili *neistinit* (lažan, ne vrijedi). Pri tome se pretpostavlja da vrijedi logički *princip proturječnosti* po kojemu svaki sud (iskaz) ne može istodobno biti istinit i lažan, te logički *princip isključenja trećeg* po kojemu svaki sud (iskaz) mora imati jednu od tih kvaliteta istinit ili lažan, jer treće ne postoji (*tertium non datur*).

Kod dokaza tvrdnji (teorema) treba strogo razlikovati ono što se dokazuje od onog na temelju čega se dokazuje. Prije dokaza neke tvrdnje imamo jedan sustav *S* već utvrđenih tvrdnji: aksioma, dokazanih teorema i definicija, što nam čini argumente dokaza (baza dokaza). Za dokazivanje tvrdnji obično koristimo direktan i indirektan dokaz. Kod direktnog dokaza oblika (I) „Ako je *P*, onda je *Q*" polazimo od hipoteze *P* (koja je točna) i koristeći spomenute argumente iz *S* (uvedene aksiome i definicije te ranije dokazane teoreme) dolazimo do teze (tvrdnje ili zaključka) teorema.

[1]Šefket Arslanagić, Odsjek za matematiku Prirodno-matematičkog fakulteta Univerziteta u Sarajevu, BiH

Indirektan dokaz (*reductio ad absurdum*) tvrdnje (teorema) oslanja se na logičke principe proturječnosti i isključenja trećeg. Ukratko, indirektan dokaz sastoji se u pobijanju antiteze dane tvrdnje, dovodeći pretpostavku o točnosti antiteze u proturječnost s nekom utvrđenom tvrdnjom (iz *S*), ili sa samom hipotezom (pretpostavkom) antiteze.

U ovom ćemo radu upravo indirektan dokaz tvrdnje (teorema) koristiti za dokaze više raznih tvrdnji iz različitih područja matematike.

Primjer 3. Dokažimo da skup *P* svih prostih brojeva nije konačan.

Dokaz:

Teza: Skup *P* svih prostih brojeva je beskonačan (nije konačan). (X)

Antiteza: Skup *P* svih prostih brojeva je konačan. $(\overline{X})$

Pretpostavimo da je tvrdnja $\overline{X}$ istinita. Tada možemo odrediti umožak svih prostih brojeva 2, 3, 5, …, *p* pa postoji broj

$$k=(2\cdot 3\cdot 5\cdot \ldots \cdot p)+1 .$$

Broj *k* je neparan pa može biti prost ili složen.

1° Neka je *k* prost broj. On je svakako veći od svakog od prostih brojeva iz skupa *P*, dakle različit je od njih, pa ako je on prost, to znači da izvan skupa *P* ima bar još jedan prost broj, suprotno pretpostavci da je *P* skup **svih** prostih brojeva. Dakle, broj *k* nije prost.

2° Neka je *k* složen broj. On nije djeljiv ni s jednim od prostih brojeva iz skupa *P* (ostatak dijeljenja uvijek je 1). Budući da je *k* složen broj, on se može napisati kao umnožak dvaju brojeva od kojih je jedan prost, što znači da je djeljiv nekim drugim prostim brojem koji je izvan skupa *P*. Dakle, opet postoji bar jedan prost broj koji je izvan skupa *P*, što je opet u kontradikciji s pretpostavkom. Prema tome, tvrdnja $\overline{X}$ je neistinita, pa je, dakle, istinita tvrdnja *X*.

Napomena: Ovaj se dokaz pripisuje velikom starogrčkom matematičaru **Euklidu** (oko 340. - oko 287. prije Krista), autoru čuvene knjige „Elementi" u 13 svezaka.

Primjer 4. Dokažimo da jednadžba $x^2+y^2+z^2=2012$ nema rješenja ako su *x*, *y* i *z* prosti brojevi.

Dokaz: Pretpostavimo obrnuto, tj. da ta jednadžba ima rješenja *x*, *y*, *z* koji su prosti brojevi. Budući da je jednadžba simetrična, možemo pretpostaviti da je $x\le y\le z$, a da se pri tome ne naruši uopćenost. Ako je $x\neq 2$, tj. *x*, *y*, *z* su neparni prosti brojevi, onda je $x^2+y^2+z^2$ također neparan broj, pa jednadžba nema rješenja.

Ako je $x=2$, onda je $y^2+z^2=2008$. Ako je $y=3$, tada dobivamo da je $z^2=1999$, pa *z* ne postoji. Svaki prosti broj veći od 3 može se napisati u obliku $6k\pm 1$; $(k\in\mathbb{N})$.

Tada je $y^2 = (6k \pm 1)^2 = 36k^2 \pm 12k + 1 = 12\left(3k^2 \pm k\right) + 1 = 12M + 1$,
gdje je $M = 3k^2 \pm k$ i, analogno,

$$z^2 = 12M + 1, \text{ te } y^2 + z^2 = 12 \cdot 2M + 2 = 2008 \Rightarrow 12 \cdot 2M = 2006,$$

a broj 2006 nije djeljiv brojem 12, pa jednadžba nema rješenja u skupu prostih brojeva.

Primjer 5. Dokažimo da jednadžba $x^2 - y^2 = 4z + 2$ nema rješenja u skupu cijelih brojeva.

Dokaz: Pretpostavimo da postoje *x*, *y*, *z* koji zadovoljavaju danu jednadžbu:

$$x^2 - y^2 = 4z + 2 \Leftrightarrow (x - y)(x + y) = 2(2z + 1).$$

Desna strana jednadžbe je paran broj, pa je i lijeva strana, tj. $(x - y)(x + y)$, također paran broj. To znači da je bar jedan od brojeva $x - y$ i $x + y$ paran. Ako je $x - y$ paran broj, tada je i broj $x + y$ paran (i obrnuto), pa je broj $(x - y)(x + y)$ djeljiv brojem 4. Ali, broj na desnoj strani jednadžbe $2(2z + 1) = 4z + 2$ nije djeljiv brojem 4. Dobili smo kontradikciju pa ne postoje $x, y, z \in \mathbb{Z}$ koji bi bili rješenja jednadžbe.

Primjer 6. Dokažimo da

$$n = 1 + \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} + \ldots + \frac{1}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2012}$$

nije cijeli broj.

Dokaz: Pretpostavimo da je $n \in \mathbb{Z}$. Tada, nakon množenja dane jednadžbe brojem 2011!, dobivamo:

$$n \cdot 2011! = 2011! + \ldots + 1 + \frac{1}{2012} \notin \mathbb{N}.$$

Opet smo dobili kontradikciju jer je na lijevoj strani cijeli broj, a na desnoj strani nije cijeli broj. Dakle, $n \notin \mathbb{Z}$, što je trebalo dokazati.

Primjer 7. Dokažimo da sustav jednadžbi

$$x^2 + y^2 + z^2 = 1$$
$$x + 2y + 3z = 4,$$

nema rješenja u skupu $\mathbb{R}$.

Dokaz: Neka postoji rješenje (x, y, z) danog sustava jednadžbi. Na osnovi nejednakosti **Cauchy-Bunyakovski-Schwartza** imamo:

$$(x \cdot 1 + y \cdot 2 + z \cdot 3)^2 \leq 2\ (x^2 + y^2 + z^2)\ (1^2 + 2^2 + 3^2),$$

odnosno

$$4^2 \leq 1 \cdot 14, \text{ tj.}$$
$$16 \leq 14,$$

a ovo je apsurd. Dakle, dana jednadžba nema rješenja u skupu $\mathbb{R}$.

Primjer 8. Dokažimo da za bilo koje $n \in \mathbb{N}$ vrijedi $\sqrt{n+\sqrt{n}} \notin \mathbb{N}$.

Dokaz: Pretpostavimo suprotno, tj. da $\sqrt{n+\sqrt{n}} \in \mathbb{N}$, odnosno da $\sqrt{n+\sqrt{n}} = a \in \mathbb{N}$. Nakon kvadriranja ove jednadžbe slijedi:

$$\sqrt{n} = a^2 - n \in \mathbb{N}.$$

Odavde zaključujemo da mora biti $n = m^2$, $m \in \mathbb{N}$. Sada dobivamo:

$$m = a^2 - m^2, \text{ tj.}$$
$$m^2 + m = a^2,$$

a odavde

$$4m^2 + 4m = 4a^2$$
$$4m^2 + 4m + 1 = 4a^2 + 1$$
$$\Leftrightarrow (2m+1)^2 - 4a^2 = 1$$
$$\Leftrightarrow (2m+1-2a)(2m+1+2a) = 1,$$

odakle slijedi:

$$2m+1-2a = 1 \ \wedge \ 2m+1+2a = 1, \text{ tj.}$$
$$2m+1-2a = 2m+1+2a,$$

odnosno

$$4a = 0 \Rightarrow a = 0,$$

što je kontradikcija jer $a \in \mathbb{N}$.

Dakle, $\sqrt{n+\sqrt{n}} \notin \mathbb{N}$; ($n \in \mathbb{N}$), što je trebalo dokazati.

Primjer 9. Dan je polinom

$$P(x) = x^{1997} - x^{1995} + x^2 - 3kx + 3k + 1; \ (k \in \mathbb{Z}).$$

Dokažimo da:

a) polinom $P(x)$ nema cjelobrojnih nultočaka;
b) brojevi $P(n)$ i $P(n) + 3$ su relativno prosti za bilo koji broj $n \in \mathbb{Z}$.

Dokaz: a) Pretpostavimo suprotno, tj. neka dani polinom ima jednu cjelobrojnu nultočku $x = \alpha$. Tada slijedi:

$$P(x) = (x-\alpha) \cdot Q(x),$$

gdje je $Q(x)$ polinom stupnja 1996 s cjelobrojnim koeficijentima. Sada imamo:

$$P(-1)P(0)P(1) = (-1-\alpha)(-\alpha)(1-\alpha)Q(-1)Q(0)Q(1).$$

Cijeli brojevi $-1-\alpha, -\alpha, 1-\alpha$ su uzastopni pa je njihov umnožak djeljiv brojem 3. Ali, $P(-1) = 6k+2$, $P(0) = 3k+1$ i $P(1) = 2$ pa je: $P(-1)P(0)P(1) = 4(3k+1)^2$, a ovaj broj nije djeljiv brojem 3. Dakle, dani polinom nema cjelobrojnih nultočaka.

b) Pretpostavimo opet suprotno, tj. neka postoji jedan prirodan broj za koji brojevi $P(n)$ i $P(n)+3$ nisu relativno prosti. Neka je d najmanji zajednički djelitelj ovih brojeva. Tada je $d \mid P(n)+3-P(n) \Rightarrow d \mid 3 \Rightarrow d=3$. Sada imamo:

$$P(n)=(n-1)n(n+1)n^{1994}-3k(n-1)+n^2+1 .$$

Budući da vrijedi $3 \mid P(n) \wedge 3 \mid (n-1)n(n+1) \wedge 3 \mid 3k(n-1)$, slijedi da mora biti i $3 \mid n^2+1$, što nije točno (uzeti $n=3k$ $n=3k\pm 1;\ k\in\mathbb{Z}$). Dakle, brojevi $P(n)$ i $P(n)+3$ su relativno prosti za bilo koji broj $n\in\mathbb{Z}$.

Primjer 10. Dokažimo: ako su a, b, c različiti realni brojevi, tada jednadžbe

$$ax^2+2bx+1=0,$$

$$bx^2+2cx+1=0,$$

$$cx^2+2ax+1=0,$$

nemaju niti jedno zajedničko rješenje.

Dokaz: Pretpostavimo suprotno, tj. neka dane jednadžbe imaju zajednički korijen x_0, tj. neka vrijedi $ax_0^2+2bx_0+1=0$ i $bx_0^2+2cx_0+1=0$, gdje je $x_0\neq 0$. Sada dobivamo da je:

$$ax_0^2+2bx_0+1=bx_0^2+2x_0+1$$

$$\Leftrightarrow (a-b)x_0^2=2(c-b)x_0 \quad \Big/ : x_0,\ x_0\neq 0$$

$$\Leftrightarrow (a-b)x_0=2(c-b), \text{ tj.}$$

$$x_0=\frac{2(c-b)}{a-b};\ \ (a\neq b). \tag{1}$$

Analogno, iz druge i treće jednadžbe dobivamo:

$$x_0=\frac{2(a-c)}{b-c};\quad (b\neq c). \tag{2}$$

Sada iz (1) i (2) dobivamo:

$$\frac{2(c-b)}{a-b}=\frac{2(a-c)}{b-c} \Big/ :2$$

$$\Leftrightarrow (c-b)(b-c)=(a-c)(a-b)$$

$$\Leftrightarrow a^2+b^2+c^2-ab-bc-ac=0$$

$$\Leftrightarrow \frac{1}{2}\left[(a-b)^2+(b-c)^2+(a-c)^2\right]=0,$$

a odavde

$$a=b=c,$$

što je suprotno pretpostavci da su a, b, c različiti realni brojevi.

Primjer 11. Dokažimo da brojevi:

a) $\sqrt{2}+\sqrt{3}+\sqrt{5}$ i b) $\sqrt{2}+\sqrt[3]{5}$ nisu racionalni.

Dokaz: a) Pretpostavimo suprotno, tj. da je $\sqrt{2}+\sqrt{3}+\sqrt{5}\in\mathbb{Q}$. Neka je $\sqrt{2}+\sqrt{3}+\sqrt{5}=a\in\mathbb{Q}$. Sada imamo:

$$a-\sqrt{5}=\sqrt{2}+\sqrt{3}$$

$$\Leftrightarrow (a-\sqrt{5})^2=(\sqrt{2}+\sqrt{3})^2$$

$$\Leftrightarrow a^2-2a\sqrt{5}+5=2+2\sqrt{6}+3$$

$$\Leftrightarrow a^2-2a\sqrt{5}=2\sqrt{6}\,/^2$$

$$\Leftrightarrow a^4-4a^3\sqrt{5}+20a^2=24$$

$$\Leftrightarrow \sqrt{5}=\frac{a^4+20a^2-24}{4a^3}\in\mathbb{Q},$$

što nije točno jer je $\sqrt{5}\notin\mathbb{Q}$ (što se lako dokaže indirektnim dokazom). Dakle, $\sqrt{2}+\sqrt{3}+\sqrt{5}\notin\mathbb{Q}$, što je trebalo dokazati.

b) Pretpostavimo suprotno, tj. da je $\sqrt{2}+\sqrt[3]{5}\in\mathbb{Q}$ i neka je $\sqrt{2}+\sqrt[3]{5}=b\in\mathbb{Q}$. Sada imamo:

$$\sqrt[3]{5}=b-\sqrt{2}$$

$$\Leftrightarrow 5=\left(b-\sqrt{2}\right)^3$$

$$\Leftrightarrow 5=b^3-3\sqrt{2}b^2+6b-2\sqrt{2}$$

$$\Leftrightarrow \sqrt{2}=\frac{b^3+6b-5}{3b^2+2}\in\mathbb{Q},$$

što opet nije točno jer je $\sqrt{2}\notin\mathbb{Q}$ (što se također lako dokaže pomoću indirektnog dokaza). Dakle, $\sqrt{2}+\sqrt[3]{5}\notin\mathbb{Q}$, što je trebalo dokazati.

Primjer 12. Dokažimo da za realne brojeve $a,b,c\in(0,1)$ vrijedi nejednakost:

$$\min\left\{ab(1-c)^2,bc(1-a)^2,ca(1-b)^2\right\}\le\frac{1}{16}.$$

Dokaz: Poslužit ćemo se indirektnim dokazom, tj. pretpostavit ćemo da je

$$\min\left\{ab(1-c)^2,bc(1-a)^2,ca(1-b)^2\right\}>\frac{1}{16}.$$

Tada slijedi da je:

$$ab(1-c)^2 > \frac{1}{16},\ bc(1-a)^2 > \frac{1}{16}\ \text{ i }\ ca(1-b)^2 > \frac{1}{16}.$$

Koristeći nejednakost između aritmetičke i geometrijske sredine četiriju pozitivnih brojeva, imamo:

$$\frac{a+b+(1-c)+(1-c)}{4} \geq \sqrt[4]{ab(1-c)^2}\text{ , tj.}$$

$$a+b-2c+2 \geq 4\sqrt[4]{ab(1-c)^2}\ ,$$

a odavde, zbog $ab(1-c)^2 > \frac{1}{16}$ slijedi:

$$a+b-2c+2 > 4\sqrt[4]{\frac{1}{16}}\text{ , tj.}$$

$$a+b-2c > 0$$

ili

$$a+b > 2c\ . \tag{1}$$

Analogno dobivamo i ove nejednakosti:

$$b+c > 2a \tag{2}$$

i

$$a+c > 2b. \tag{3}$$

Nakon zbrajanja nejednakosti (1), (2) i (3), dobivamo da je:

$$a+b+c > a+b+c,$$

što nije točno, tj. predstavlja kontradikciju. Dakle, tvrdnja zadatka je točna.

Literatura

[1] Arslanagić, Š., *Matematika za nadarene*, Bosanska riječ, Sarajevo, 2004.

[2] Klašnja, S., *Elementarna matematika I, Algebra*, Univerzitet u Sarajevu, 1963.

[3] Niculescu, L., *Metoda reducerii la absurd*, Editura GIL, Zalau, 2007.