25. Bizonyítási módszerek bemutatása számelméleti problémák megoldásában

1. Direkt bizonyítás

Ismert tételeket és definíciókat alkalmazva megoldjuk az adott problémát.

Például:

1. Bizonyítsuk be, hogy végtelen sok olyan pozitív egész szám van, amely nem áll elő: a) 2 négyzetszám
   b) 2 köbszám összegeként

   Megoldás maradékok vizsgálatával:

   a) $x^2 + y^2 \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases} \pmod 4$

   $n = 4k + 3$, $k \in N$

   b) 9-es maradék

2. Adott a $p(x) = x^5 - 5x^3 + 4x$ polinom. Melyik az a legnagyobb pozitív egész szám, amellyel a polinom minden egész helyen vett helyettesítési értéke osztható?

   Megoldás:

   $p(x) = x(x^4 - 5x^2 + 4) = x(x^4 - x^2 - 4x^2 + 4) = x(x^2(x^2 - 1) - 4(x^2 - 1)) =$
   $= x(x^2 - 1)(x^2 - 4) = (x-2)(x-1)x(x+1)(x+2)$

   Ha $x \in Z$, akkor az 5 egymást követő egész szám szorzata, amelyek közül 1 osztható 5-tel, legalább 1 osztható 3-mal, 1 osztható 4-gyel, és azon kívül van köztük egy 2-vel osztható szám. Így a szorzat osztható $5 \cdot 3 \cdot 8 = 120$-szal.
   Mivel $p(3) = 120$, ezért ez a legnagyobb szám, amivel minden helyen osztható.

Oszthatóság tulajdonságai

Skatulyaelv: ha n skatulyába $n \cdot k$-nál több dolgot kell szétosztani, akkor lesz legalább 1 skatulya, amelybe legalább k+1 dolog kerül.

2. Indirekt bizonyítás

A bizonyítandó állítás ellentettjéről belátjuk, hogy hamis, ebből következik, hogy a bizonyítandó igaz.
A bizonyítandó állítás ellentettjéről feltesszük, hogy igaz, és ebből kiindulva ellentmondásra jutunk.

TÉTEL: $\sqrt{2}$ irracionális

TÉTEL: Végtelen sok prímszám van.

Bizonyítás:
Tegyük fel, hogy véges sok van! Legyenek ezek $p_1; p_2; \ldots; p_n$!
Legyen $A = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 > 1$ →van prímosztója
Legyen ez q!
Mivel p_i nem osztója A-nak ($i = 1, 2, \ldots, n$), ezért $q \ne p_i$ ($i = 1, 2, \ldots, n$).
Tehát találtunk a megadott prímektől különböző prímszámot.
Ellentmondás→Végtelen sok prímszám van.

3. Teljes indukció

P_n kijelentés, amelyben az $n \in N$, mint paraméter szerepel.

Ez a kijelentés igaz valamely $n_0 \in N$ -től kezdve minden természetes számra, ha

a) P_{n_0} igaz

b) valahányszor P_k igaz, mindannyiszor P_{k+1} is igaz.

Például:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$17 \mid 7 \cdot 5^{2n-1} + 2^{3n+1}$$

Olyan bizonyítási eljárás, amellyel egy a természetes számokra vonatkozó törvényszerűséget lehet bebizonyítani. Első lépésben belátjuk 1-re (vagy valamely konkrét természetes számra) a törvényszerűséget. Második lépésben azt mutatjuk meg, ha igaz n-re a törvényszerűség, akkor n+1-re is az. Vagyis azt látjuk be, hogy n-ről n+1-re öröklődik az állítás. Ezzel az eljárással megszámlálhatóan végtelen sok állítás igazságát lehet belátni.

Alkalmazás:

- számelméleti, oszthatósági példák megoldásánál
- kongruenciák alkalmazása titkosírásban
- legkisebb közös többszörös keresése
- titkosírás, diofantoszi egyenletek