Princíp matematickej indukcie

Uvažujme súčty za prvých n sebou idúcich nepárnych čísel. Platí:

$$1 = 1 = 1^2$$

$$1 + 3 = 4 = 2^2$$

$$1 + 3 + 5 = 9 = 3^2$$

$$1 + 3 + 5 + 7 = 16 = 4^2$$

$$\dots$$

Z toho by sme mohli dedukovať, že

$$1 + 3 + \cdots + (2n - 1) = n^2$$

? Ako dokázať platnosť tohto vzťahu ?

Definícia

Množina $\mathbb{N}$ prirodzených čísel je taká podmnožina množiny $\mathbb{R}$, ktorá spĺňa:

1. $0 \in \mathbb{N}$
2. $x \in \mathbb{N} \Rightarrow x + 1 \in \mathbb{N}$
3. $(\forall A \subseteq \mathbb{R})\ ((0 \in A) \wedge (x \in A \Rightarrow x + 1 \in A)) \Rightarrow \mathbb{N} \subseteq A$

Podmienka 3) hovorí, že $\mathbb{N}$ je minimálna podmnožina $\mathbb{R}$ spĺňajúca prvé dve podmienky.

Veta (princíp matematickej indukcie)

Nech $V(x)$ je výroková funkcia definovaná na $\mathbb{N}$, spĺňajúca nasledovné podmienky:

1. $V(0)$ *platí*
2. $V(k) \Rightarrow V(k+1)$.

Potom $V(x)$ platí pre všetky $x \in \mathbb{N}$.

Výrok $V(0)$ sa nazýva *základ indukcie*, výrok $V(k)$ z predpokladu implikácie sa nazýva *indukčný predpoklad*.

Dôkaz: Nech $A = \{x \in \mathbb{N} : \ V(x) \text{ platí } \}$. Zrejme platí $A \subseteq \mathbb{N}$.

Z predpokladov vety máme, že $0 \in A$ a ak $x \in A$, tak aj $x + 1 \in A$.

Na základe tretej vlastnosti z definície množiny $\mathbb{N}$ potom musí platiť $\mathbb{N} \subseteq A$.

Teda $A = \mathbb{N}$, čiže $V(x)$ platí pre všetky $x \in \mathbb{N}$.

Modifikácia: základ indukcie môže byť aj rôzny od nuly:

Veta

Nech $V(x)$ je výroková funkcia definovaná pre $x \in \mathbb{N}, x \geq k_0$, spĺňajúca nasledovné podmienky:

1. $V(k_0)$ *platí*
2. $V(k) \Rightarrow V(k+1)$.

Potom $V(x)$ platí pre všetky $x \in \mathbb{N}, x \geq k_0$.

Príklad

Dokážte, že $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

1° : tvrdenie platí pre $n = 1$: $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$.

2° : nech tvrdenie platí pre $n = k$, t.j. nech $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Pre $n = k + 1$ dostávame

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) \overset{i.p.}{=} \frac{k(k+1)}{2} + k + 1 =$$

$$\frac{(k+1)(k+2)}{2} = \frac{n(n+1)}{2},$$

teda tvrdenie platí aj pre $n = k + 1$.

Veta (princíp úplnej indukcie)

Nech $V(x)$ je výroková funkcia definovaná na $\mathbb{N}$, spĺňajúca podmienku:

- $(\forall k < n)\ V(k)) \Rightarrow V(n)$

Potom $V(x)$ platí pre všetky $x \in \mathbb{N}$.

Dôkaz: Nech $A = \{x \in \mathbb{N} :\ V(x)$ platí $\}$ a nech $B = \mathbb{N} \setminus A$. Chceme ukázať, že $B = \emptyset$.

Sporom: nech $B \neq \emptyset$. Potom (keďže $B \subseteq \mathbb{N}$) B má najmenší prvok; označme ho n.

Keďže $n \notin A$, tak platí $\neg V(n)$. Avšak, pre každé $m < n$ platí $V(m)$ (pretože m je menšie ako najmenší prvok B, a teda $m \notin B$).

Podľa predpokladu vety potom dostávame, že $V(n)$ platí, čo je spor.

Príklad

Dokážte, že n priamok v rovine delí danú rovinu na najviac $\frac{n^2+n+2}{2}$ častí.

Označme dané priamky v rovine $p_1, \ldots, p_n$. Ak budeme uvažovať $n-1$ priamok $p_1, \ldots, p_{n-1}$, tak podľa indukčného predpokladu tieto priamky delia rovinu na najviac $\frac{(n-1)^2+(n-1)+2}{2} = \frac{n^2-n+2}{2}$ častí. Priamka p_n má s priamkami $p_1, \ldots, p_{n-1}$ najviac $n-1$ priesečníkov, ktoré ju rozdeľujú na najviac n častí (dve z nich sú polpriamky, ostatné úsečky). Každá z týchto polpriamok resp. úsečiek rozdeľuje časť roviny, v ktorej leží, na dve nové časti. Týmto spôsobom pribudne najviac n častí roviny; spolu teda priamky $p_1, \ldots, p_n$ delia rovinu na najviac $\frac{n^2-n+2}{2} + n = \frac{n^2+n+2}{2}$ častí.

Dirichletov princíp

Typická formulácia ("holubníkový princíp"): ak sa v k holubníkoch nachádza viac ako k holubov, tak v aspoň jednom holubníku sú aspoň dva holuby.

Veta (Dirichletov princíp)

Nech $A = \{a_1, \ldots, a_n\}, B = \{b_1, \ldots, b_m\}$ sú konečné množiny a $n > m$. Potom neexistuje žiadne prosté zobrazenie $f : A \to B$.

Dôkaz: Nech
$S = \{n \in \mathbb{N} : \ (\exists f) \ f : \ A \stackrel{1-1}{\to} B$ pre nejaké $m < n\}$. Chceme ukázať, že $S = \emptyset$.

Sporom: nech $S \neq \emptyset$. Potom S má najmenší prvok n_0, t.j. n_0 je najmenšie prirodzené číslo, pre ktoré existuje prosté zobrazenie $g : \ A \stackrel{1-1}{\to} B$ pre nejakú množinu $A, |A| = n_0$ a pre nejaké $m < n_0$.

Zrejme $m > 1$ (inak by bolo $m = 1$ a pre $n_0 > 1 = m$ by všetky zobrazenia z A do B boli konštantné, teda nie prosté).

Nech $g(a_{n_0}) = b_r, 1 \leq r \leq m$.

Ak žiaden z prvkov $g(a_1), \ldots, g(a_{n_0-1})$ nie je rovný b_m, tak zobrazenie $g' : \ A \setminus \{a_{n_0}\} \to B \setminus \{b_m\}$, ktoré je zúžením zobrazenia g na množinu $A \setminus \{a_{n_0}\}$ je prosté (keďže zúženie prostého zobrazenia je samo prosté). To je však v spore s definíciou čísla n_0 (pretože $|A \setminus \{a_{n_0}\}| < n_0$).

Dôkaz (pokr.): Teda existuje $j, 1 \leq j \leq n_0 - 1$ také, že $g(a_j) = b_m$. Keďže g je prosté, tak $g(a_{n_0}) \neq b_m$, čiže $r \leq m - 1$.

Definujme zobrazenie $h: \ A \setminus \{a_{n_0}\} \to B \setminus \{b_m\}$ predpisom

$$h(a_j) = b_r$$

$$h(a_i) = g(a_i) \text{ pre } i \neq j$$

Platí, že h je prosté, to je však spor s definíciou čísla n_0.

Modifikácia: ak je viac ako $m \cdot n$ objektov rozdelených do n skupín, tak v aspoň jednej skupine sa nachádza aspoň $m + 1$ objektov.

Príklad

Ukážte, že spomedzi n celých čísel možno vždy vybrať niekoľko (možno i jediné) tak, že ich súčet je deliteľný n.

Nech uvažované čísla sú $a_1, a_2, \ldots, a_n$. Uvažujme súčty $a_1, a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n$.

Ak niektorý z nich je deliteľný n, tak tvrdenie platí. Inak sú zvyšky po ich delení číslom n z množiny $\{1, 2, \ldots, n-1\}$.

Z toho vyplýva, že existujú dva súčty $a_1 + \cdots + a_i, a_1 + \cdots + a_j$, ktoré po delení n dávajú rovnaký zvyšok; BUNV nech $j > i$. Potom rozdiel $a_1 + \cdots + a_j - (a_1 + \cdots + a_i) = a_{i+1} + \cdots + a_j$ je deliteľný n. Teda podmienkam úlohy vyhovuje čísla $a_{i+1}, \ldots, a_j$.

Príklad

V desiatkovom zápise ľubovoľného racionálneho čísla sa vždy vyskytuje opakujúca sa postupnosť cifier (pričom tieto môžu byť nuly).

Nech je dané racionálne číslo $\frac{m}{n}$ (bez ujmy na všeobecnosti kladné). Vydeľme "ručne" m číslom n, pokiaľ nevyčerpáme všetky cifry m; týmto spôsobom dostaneme celú časť daného čísla (pred desatinnou čiarkou). Ďalej vykonajme $n+1$ delení číslom n (opäť "ručne" postupným pripisovaním 0). Takto dostaneme $n+1$ zvyškov. Keďže roznych zvyškov po delení n je práve n, podľa Dirichletovho princípu sa niektorý zvyšok vyskytol dvakrát. Potom postupnosť zvyškov, ktoré sa vyskytujú medzi týmito dvomi opakujúcimi sa zvyškami, sa pri ďalšom delení stále opakuje.

Príklad (Erdös, Szekeres, 1935)

Dokážte, že každá postupnosť n^2+1 reálnych čísel vždy obsahuje rýdzomonotónnu $(n+1)$-prvkovú vybranú postupnosť.

Nech členy uvažovanej postupnosti sú $a_1, a_2, \ldots, a_{n^2+1}$. Každému členu a_j priraďme usporiadanú dvojicu (r_j, k_j), kde r_j je dĺžka najdlhšej rastúcej vybranej postupnosti začínajúcej členom a_j a k_j je dĺžka najdlhšej klesajúcej vybranej postupnosti začínajúcej a_j.

Sporom: predpokladajme, že neexistuje vybraná rýdzomonotónna $(n+1)$-prvková postupnosť. Potom pre každé $j = 1, \ldots, n^2+1$ platí $r_j \leq n, k_j \leq n$. Možných usporiadaných dvojíc (r_j, k_j) je teda $n \cdot n = n^2$. Podľa Dirichletovho princípu teda dve z n^2+1 existujúcich usporiadaných dvojíc musia byť rovnaké, t.j. existujú čísla $s, t \in \{1, \ldots, n^2+1\}, s < t$ také, že $r_s = r_t$ a $k_s = k_t$.

Príklad (pokr.)

Ak $a_s < a_t$, tak pridaním člena a_s pred členy rastúcej vybranej podpostupnosti začínajúcej a_t získame rastúcu vybranú postupnosť s $r_s + 1$ členmi, čo je spor.

Ak $a_s > a_t$, tak rovnakým spôsobom dostaneme klesajúcu vybranú postupnosť s $k_s + 1$ členmi, čo je opäť spor.

Príklad (BYTE Magazine 17 (6):45, June 1992)

Predstavitelia firmy WEB Technologies tvrdili, že ich kompresný program DataFiles/16 komprimuje všetky typy súborov na cca jednu šestnástinu ich pôvodnej veľkosti a že pre súbory veľkosti aspoň 64 kB je táto kompresia bezstratová.

Uvažujme súbor dĺžky $16n$ bitov. Takýchto súborov je 2^{16n}.

Ľubovoľný z týchto súborov sa má dať skomprimovať na súbor dĺžky najviac n bitov. Počet rôznych súborov dĺžky najviac n bitov je $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.

Pretože $2^{n+1} - 1 < 2^{16n}$, podľa Dirichletovho princípu musia existovať dva súbory dĺžky $16n$ bitov, ktoré po skomprimovaní dajú ten istý súbor. Teda kompresia nemôže byť bezstratová.

(ďalšie informácie napr. na http://www.faqs.org/faqs/compression-faq/part1/)