

2. Dôkazy v matematike

Matematika je jediná exaktná veda. To znamená, že všetky tvrdenia, ktoré sa v matematike nazývajú *vety*, sa musia dokazovať pomocou nástrojov matematickej logiky a jazyka príslušnej teórie¹. Takéto dokázané tvrdenia, vety, potom majú v medziach svojej teórie univerzálnu platnosť. Medzi najznámejšie matematické vety, s ktorými sme sa už určite stretli, patria napríklad Pythagorova veta a Euklidova veta, ktoré obe postulujú tvrdenia o pravouhlom trojuholníku. Dokázali ich už starí Gréci a my sme sa s nimi stretli najneskôr na strednej škole. Inou známou vetou, s ktorou sme sa mohli stretnúť v rámci matematickej analýzy, je napríklad Newtonova-Leibnizova veta o určitom integráli.

Pri budovaní matematickej teórie sa vždy vychádza z *axióm*. Axióma je nejaké základné tvrdenie, ktoré sa považuje za platné a nedokazuje sa. Prvou podmienkou pri výbere axióm je obmedziť ich počet na nevyhnutné minimum. Nie je totiž žiaduce stavať teóriu na veľkom počte nedokázaných tvrdení. Snažíme sa preto vybrať vždy len minimálny počet axióm, ktoré nám umožnia odvodiť pravdivé tvrdenia príslušnej teórie. Druhou podmienkou pri výbere axióm je brať za axiómy len jednoduché tvrdenia, ktoré si vieme overiť nástrojmi mimo príslušnej teórie a o ktorých platnosti málokto pochybuje a väčšina ľudí ich považuje za samozrejmé. Tretou a veľmi dôležitou podmienkou pri výbere axióm je to, že vybrané axiómy nesmú byť sporné, t. j. nedá sa z nich odvodiť výrok a zároveň jeho negácia. Ak by totiž nejaká teória obsahovala sporné axiómy, tak potom v tejto teórii sú dokázateľné (pravdivé) všetky tvrdenia.

Ako prvý príklad si môžeme uviesť výrokovú logiku. Tam nám na dokázanie všetkých možných pravdivých výrokov stačia 3 axiómy (pozri [9], str. 14). Jednou z nich je napr. výrok $A \Rightarrow (B \Rightarrow A)$, o ktorého pravdivosti sa môžeme presvedčiť napr. pravdivostnou tabuľkou, čo sa však nepovažuje za dôkaz v jazyku výrokovej logiky. V prípade výrokovej logiky existujú aj iné axiomatické systémy, než je ten, ktorý je uvedený v [9]. Všetky tieto axiomatické systémy sú navzájom ekvivalentné a v [9] boli uvedené tri axiómy zvolené z toho dôvodu, že sa pomocou nich pomerne ľahko dokazujú pravdivé výroky.

¹matematická logika, teória množín, matematická analýza, geometria...

Druhým príkladom môže byť teória množín, ktorá sa axiomaticky začala budovať koncom 19. a začiatkom 20. storočia. V tejto teórii taktiež existuje viacero rôznych axiomatických systémov, napríklad Zermelov, Zermel-Frankelov . . . Na vybudovanie celej teórie množín nám stačí 9 axióm (pozri [2], str. 35). Prvou z týchto axióm je axióma existencie množín, ktorá hovorí $(\exists x)(x = x)$. Písmeno x tu označuje množinu a s tým, že existuje nejaká množina, ktorá sa rovná sama sebe, bude zrejme súhlasiť väčšina ľudí.

Posledným príkladom, ktorý si tu uvedieme, je Euklidovská geometria. Je to najstaršia matematická teória postavená a budovaná na axiomatických základoch. Táto teória používa 5 axióm, ktoré sformuloval Euklides v prvej knihe svojich *Základov*. Prvá z axióm Euklidovskej geometrie hovorí: *Lubovoľné dva body sa dajú spojiť úsečkou*. To je triviálne tvrdenie, s ktorého platnosťou bude zrejme súhlasiť väčšina ľudí. Až v 19. storočí vznikli aj iné než euklidovské geometrie, s konzistentnými axiomatickými systémami. Sú to napríklad Lobačevského (hyperbolická) geometria, Riemannova geometria a ďalšie. Tieto neeuklidovské geometrie sa využívajú napr. v Einsteinovej teórii relativity, kozmológii, kartografii, pri navigácii . . .

Komplexnejšie pojmy sa v matematických teóriách zavádzajú pomocou *definícií*. V definícii popisujeme nový pojem pomocou už známych pojmov. Definícia presne vymedzuje obsah definovaného pojmu.

Tvrdenie v matematickej teórii je pravdivé len vtedy, pokiaľ sa dá dokázať vychádzajúc z axióm, už predtým dokázaných tvrdení a pomocou nástrojov matematickej logiky a jazyka príslušnej teórie. Čiže tvrdenie sa stáva vetou až potom, keď existuje jeho dôkaz. Dovtedy je to len *hypotéza*, ktorá môže, ale nemusí, byť pravdivá. V matematike existuje viacero základných typov dôkazov. Niektoré z nich si tu preberieme a ilustrujeme na príkladoch.

2.1 Priamy dôkaz

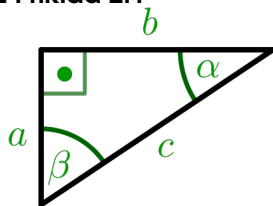
Priamy dôkaz je postup, pri ktorom je dokazované tvrdenie odvodené priamou aplikáciou predpokladov, axióm, definícií a už dokázaných viet. V priamych dôkazoch sa často využíva pravidlo *modus ponens*, postavené na implikácii.

Definícia 2.1.1 — Modus ponens. Majme dve tvrdenia A a B . Pravidlo modus ponens hovorí, že ak platia tvrdenia A a $A \Rightarrow B$, tak potom platí aj tvrdenie B .

Logická pravdivosť pravidla modus ponens sa dá dokázať pomocou pravdivostných tabuliek a toto pravidlo je súčasťou jazyka výrokovej logiky. V skutočnosti je to jediné odvodzovacie pravidlo jazyka výrokovej logiky a pomocou neho sa z axióm dokazujú a dajú dokázať všetky pravdivé výrokové formuly výrokovej logiky. Ako však bolo spomenuté, pravidlo modus ponens sa v priamych dôkazoch, najmä komplexnejších tvrdení, často, ale nie vždy, využíva.

Na úvod si uvedieme priamy geometrický dôkaz Pythagorovej vety. Takéto „geometrické“ dôkazy obľubovali starí Gréci.

■ Príklad 2.1



V pravouhlom trojuholníku sa plocha štvorca zostrojeného nad preponou rovná súčtu plôch štvorcov zostrojených nad odvesnami. Dokážte!

Dôkaz: Vieme, že súčet uhlov trojuholníka je 180° . To znamená, že v pravouhlom trojuholníku bude súčet uhlov $\alpha + \beta = 90^\circ$. Nakreslíme si teraz daný pravouhlý trojuholník štyrikrát nasledovným spôsobom.

Prepony štyroch kópií daného trojuholníka tvoria vnútorný štvorec a jeho odvesny tvoria vonkajší štvorec. To, že útvar tvorený odvesnami je tiež štvorec, vyplýva z faktu, že $\alpha + \beta = 90^\circ$. Poďme teraz spočítať plochu vonkajšieho štvorca. Tú môžeme vypočítať dvoma spôsobmi. Najskôr ako druhú mocnina strany štvorca

$$P = (a + b)^2 = a^2 + 2ab + b^2$$

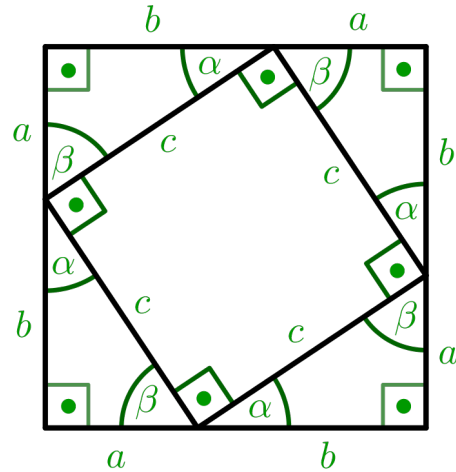
a potom ako súčet štyroch pravouhlých trojuholníkov a vnútorného štvorca

$$P = 4 \cdot \frac{ab}{2} + c^2 = 2ab + c^2.$$

Keďže sa tieto plochy musia rovnať, platí

$$a^2 + 2ab + b^2 = 2ab + c^2 \iff a^2 + b^2 = c^2.$$

Tým sme ukázali, že súčet obsahov štvorcov nad odvesnami pravouhlého trojuholníka sa rovná obsahu štvorca nad preponou tohto trojuholníka. Q.E.D.² ■



Ďalej si ukážeme tri príklady priamych dôkazov z oblasti teórie čísel.

■ **Príklad 2.2** Ak $m, n \in \mathbb{Z}$, m je párne a n je nepárne, tak potom číslo $m + n$ je nepárne. Dokážte!

Dôkaz: Číslo m je celé a párne. To znamená, že existuje číslo $k \in \mathbb{Z}$ také, že $m = 2k$. Číslo n je celé a nepárne, čo znamená, že musí existovať číslo $l \in \mathbb{Z}$ také, že $n = 2l + 1$. Potom platí

$$m + n = (2k) + (2l + 1) = 2(k + l) + 1.$$

Číslo $k + l$ je celé, čo znamená, že číslo $2(k + l)$ je párne číslo a číslo $m + n = 2(k + l) + 1$ je nepárne číslo. Tým je dokázané, že súčet párneho a nepárneho čísla je nepárne číslo. Q.E.D. ■

■ **Príklad 2.3** Druhá mocnina párneho čísla n je párne číslo. Dokážte!

Dôkaz: Číslo n je párne (a teda samozrejme aj celé), čiže existuje číslo $k \in \mathbb{Z}$ také, že $n = 2k$. Potom platí

$$n^2 = (2k)^2 = 4k^2.$$

Číslo $4k^2$ je párne, čiže druhá mocnina párneho čísla je párne číslo. Q.E.D. ■

■ **Príklad 2.4** Štvorec súčtu dvoch nepárnych čísel $m, n \in \mathbb{Z}$ je párne číslo. Dokážte!

Dôkaz: budeme robiť postupne.

- Najskôr ukážeme, že súčet dvoch nepárnych čísel je párne číslo. Ak čísla $m, n \in \mathbb{Z}$ sú nepárne, tak musia existovať čísla $k, l \in \mathbb{Z}$ také, že platí $m = 2k + 1$ a $n = 2l + 1$. Potom platí

$$m + n = (2k + 1) + (2l + 1) = 2(k + l) + 2 = 2(k + l + 1).$$

Číslo $2(k + l + 1)$ je párne a tým sme dokázali, že súčet dvoch nepárnych čísel je párne číslo.

² Q.E.D. = *quod erat demonstrandum* = „čo bolo treba dokázať“

- V príklade 2.3 sme dokázali, že druhá mocnina párneho čísla je párne číslo. Označme si tvrdenie „ $\underbrace{\text{Ak číslo je párne}}_A, \text{ tak jeho druhá mocnina je párna} \underbrace{\text{}}_B$ “ (skrátene $A \Rightarrow B$).
- V prvom kroku sme ukázali, že súčet dvoch nepárnych čísel je párny. Čiže súčtom dvoch nepárnych čísel dostaneme číslo x a označme si tvrdenie „Číslo x je párne.“ pomocou A .
- Teraz už vieme, že platí tvrdenie A a platí tvrdenie $A \Rightarrow B$. Podľa pravidla modus ponens potom platí aj tvrdenie B . Q.E.D. ■

P Treba však priznať, že vo vyššie uvedenom postupe sme trochu „švindľovali“. V tvrdení A , z tretieho bodu, je totiž ukrytá implikácia. Je to implikácia hovoriaca: „Ak sú dve čísla nepárne, tak ich súčet je párny.“ Ak by sme túto implikáciu neskryli do jedného tvrdenia A , ale nechali ju v pôvodnom tvare, tak by nešlo o pravidlo modus ponens, ale o pravidlo sylogizmu.

Veta 2.1.1 — Pravidlo sylogizmu. Majme tri tvrdenia A , B a C . Pravidlo sylogizmu hovorí, že ak platia tvrdenia $A \Rightarrow B$ a $B \Rightarrow C$, tak potom platí aj tvrdenie $A \Rightarrow C$.

P Pravidlo sylogizmu sme neuviedli ako definíciu, ako v prípade pravidla modus ponens, preto, lebo to je odvodené pravidlo. Znamená to, že samotné pravidlo sylogizmu sa vo výrokovej logike dá dokázať z axióm len pomocou pravidla modus ponens. Keďže ide o tvrdenie matematickej logiky a je mimo rámca tohto kurzu, dokazovať ho tu nebudeme. Dôkaz pravidla sylogizmu môžete nájsť v skriptách [9].

Teraz si ukážeme priamy dôkaz jedného tvrdenia z teórie množín.

■ **Príklad 2.5** Pre ľubovoľné dve množiny A a B platí $A \cup (B \setminus A) = A \cup B$. Dokážte!

Dôkaz: Z definície 1.1.3 vieme, že dve množiny X a Y sa rovnajú ($X = Y$), ak majú rovnaké prvky. Potrebujeme preto dokázať ekvivalenciu $(x \in X) \Leftrightarrow (x \in Y)$, čo je to isté, ako dokázať dve implikácie $(x \in X) \Rightarrow (x \in Y)$ a $(x \in Y) \Rightarrow (x \in X)$. Konkrétne, v zadanej úlohe, to musíme dokázať pre $X = A \cup (B \setminus A)$ a $Y = A \cup B$.

1. $(x \in X) \Rightarrow (x \in Y)$ – Nech je $x \in X$. Z definície zjednotenia vyplýva, že musí platiť $x \in A$ alebo $x \in B \setminus A$. Ak ale $x \in B \setminus A$, tak z definície rozdielu množín vyplýva, že $x \in B$. Platí teda, že $x \in A$, alebo $x \in B$. Potom však z definície zjednotenia platí, že $x \in A \cup B$.
2. $(x \in Y) \Rightarrow (x \in X)$ – Nech je $x \in Y$. Z definície zjednotenia vyplýva, že musí platiť $x \in A$ alebo $x \in B$. Ak je $x \in A$, tak musí platiť aj $x \in A \cup (B \setminus A)$. Ak ale $x \notin A$, tak potom musí platiť $x \in B$ a súčasne $x \in B \setminus A$. Z toho opäť dostávame $x \in A \cup (B \setminus A)$.

Tým je dokázané tvrdenie $A \cup (B \setminus A) = A \cup B$. Q.E.D. ■

V matematike málokedy existuje len jediný spôsob, ako možno vyriešiť danú úlohu, alebo dokázať nejaké tvrdenie. Takmer vždy existuje viacero ciest k správne riešeniu. Ukážeme si to na predošlom príklade. Tvrdenie z príkladu 2.5 si dokážeme ešte aj iným spôsobom.

■ **Príklad 2.6** Pre ľubovoľné dve množiny A a B platí $A \cup (B \setminus A) = A \cup B$. Dokážte!

Dôkaz: Nech $\mathcal{U}$ je univerzum množín A a B , čiže $A, B \subseteq \mathcal{U}$. Potom, podľa definície rozdielu množín, platí $B \setminus A = B \cap \bar{A}$. Takže

$$A \cup (B \setminus A) = A \cup (B \cap \bar{A}) = (A \cup B) \cap (A \cup \bar{A}) = (A \cup B) \cap \mathcal{U} = A \cup B. \quad \text{Q.E.D.} \quad \blacksquare$$

Na záver časti o priamom dôkaze si ešte ukážeme dôkaz jedného triviálneho tvrdenia, využijúci tranzitívnosť relácie „ $\leq$ “. O reláciách sa potom dozvieme viac v 6. kapitole.

■ **Príklad 2.7** Definujeme si funkciu „*minimum z dvoch čísel*“ takto

$$\min(a, b) = \begin{cases} a, & \text{ak } a < b \\ a, & \text{ak } a = b \\ b, & \text{ak } b < a. \end{cases}$$

Nech $d_1, d_2 \in \mathbb{R}$. Ak $d = \min(d_1, d_2)$ a $x \leq d$, tak $x \leq d_1$ a $x \leq d_2$.

Dôkaz: Najskôr ukážeme, že platí $d \leq d_1$ a $d \leq d_2$. To vyplýva priamo z definície funkcie *minimum*. Vieme, že $d = \min(d_1, d_2)$. Čiže $d = d_1$ ak $d_1 \leq d_2$ alebo $d = d_2$ ak $d_2 < d_1$. V oboch prípadoch platí $d \leq d_1$ a $d \leq d_2$. Ak máme $x \in \mathbb{R}$ a platí $x \leq d \leq d_1$ a $x \leq d \leq d_2$, tak musí platiť aj $x \leq d_1$ a $x \leq d_2$. Q.E.D. ■

2.2 Nepriamy dôkaz

Niekedy sa stáva, že tvrdenie v tvare „*Ak platí ... , tak platí ...*“ nevieme dokázať priamo, t.j. odvodiť ho jednoduchým spôsobom z axióm a už dokázaných tvrdení. Uvedený tvar tvrdenia je implikácia $A \Rightarrow B$. Podľa vety o obmenenej (obrátenej) implikácii ([9], str. 18) platí, že výrokové formuly $A \Rightarrow B$ a $\neg A \Rightarrow \neg B$ sú tautologicky ekvivalentné, čiže pre rovnaké ohodnotenia prvotných formúl A a B budú mať rovnaké pravdivostné hodnoty. Na tejto tautologickej ekvivalencii je postavený *nepriamy dôkaz*.

Ak tvrdenie v tvare $A \Rightarrow B$ nevieme jednoduchým spôsobom dokázať priamo, ale vieme priamo dokázať jemu tautologicky ekvivalentné tvrdenie $\neg B \Rightarrow \neg A$, tak takýto dôkaz sa nazýva *nepriamy dôkaz* tvrdenia $A \Rightarrow B$.

■ **Príklad 2.8** Pre každé $n \in \mathbb{N}$ platí, že ak 9 nedelí n^2 , tak 3 nedelí n . Dokážte!

Dôkaz: Uvedené tvrdenie nevieme jednoduchým spôsobom dokázať priamo. Problém sa ukrýva v slovíčku „nedelí“. Negatívne tvrdenia sa obvykle dokazujú ťažšie, než ich pozitívne modifikácie. Napríklad je ťažšie dokázať, že číslo a nedelí číslo b , než dokázať, že číslo a delí číslo b . Takže pomôžeme si nepriamym dôkazom. Obmenená implikácia ku tvrdeniu zo zadania úlohy je nasledovná

$$\text{Pre každé } n \in \mathbb{N} \text{ platí, že ak } 3 \text{ delí } n, \text{ tak } 9 \text{ delí } n^2.$$

Toto tvrdenie je tautologicky ekvivalentné s pôvodným a jeho priamy dôkaz je triviálny.

Ak 3 delí prirodzené číslo n , tak existuje $k \in \mathbb{N}$ také, že $n = 3k$. Potom $n^2 = 9k^2$ a z toho je zrejmé, že 9 delí číslo n^2 . Q.E.D. ■

Podobne jednoducho sa dá dokázať ďalšie tvrdenie z teórie čísel.

■ **Príklad 2.9** Pre každé $n \in \mathbb{N}$ platí, že ak n^2 je párne, tak n je párne. Dokážte!

Dôkaz: Obmenená implikácia ku tvrdeniu zo zadania úlohy je nasledovná

$$\forall n \in \mathbb{N} \text{ platí, že ak } n \text{ je nepárne, tak } n^2 \text{ je nepárne.}$$

Toto tvrdenie je tautologicky ekvivalentné s pôvodným a jeho priamy dôkaz je triviálny.

Ak prirodzené číslo n je nepárne, tak to znamená, že existuje $k \in \mathbb{N}$ také, že $n = 2k + 1$. Potom $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, čo je zjavne nepárne číslo. Q.E.D. ■

Nasledujúce tvrdenie, ktoré dokážeme nepriamo, bude hovoriť o racionálnych číslach.

■ **Príklad 2.10** Pre každé $x \in \mathbb{R}$ platí, že ak $x^2 \notin \mathbb{Q}$, tak aj $x \notin \mathbb{Q}$. Dokážte!

Dôkaz: Obmenená implikácia ku tvrdeniu zo zadania úlohy je nasledovná

$$\forall x \in \mathbb{R} \text{ platí, že ak } x \in \mathbb{Q}, \text{ tak aj } x^2 \in \mathbb{Q}.$$

Toto tvrdenie je tautologicky ekvivalentné s pôvodným a jeho priamy dôkaz je triviálny.

Ak reálne číslo $x \in \mathbb{Q}$, tak to znamená, že existujú čísla $a, b \in \mathbb{Z}$ také, že $x = \frac{a}{b}$. Potom $x^2 = \frac{a^2}{b^2}$, čo je zjavne racionálne číslo, a preto $x^2 \in \mathbb{Q}$. Q.E.D. ■

Posledný príklad nepriameho dôkazu bude znova z teórie čísel.

■ **Príklad 2.11** Pre každé $(x \in \mathbb{R}), (\forall y \in \mathbb{R}) : (x + y \geq 2) \Rightarrow (x \geq 1 \vee y \geq 1)$. Dokážte!

Dôkaz: Obmenená implikácia ku tvrdeniu zo zadania úlohy je nasledovná

$$(\forall x \in \mathbb{R}), (\forall y \in \mathbb{R}) : (x < 1 \wedge y < 1) \Rightarrow (x + y < 2).$$

Toto tvrdenie je tautologicky ekvivalentné s pôvodným a jeho priamy dôkaz je viac než triviálny.

Ak máme reálne čísla $x < 1$ a $y < 1$, tak platí $x + y < 1 + 1 = 2$. Q.E.D. ■

2.3 Dôkaz sporom

Niektoré tvrdenia nevieme jednoduchým spôsobom dokázať ani priamo, ani nepriamo. V takom prípade nám môže pomôcť *dôkaz sporom* nazývaný aj *reductio ad absurdum*. Dôkaz sporom je založený na tom, že namiesto dokazovaného tvrdenia predpokladáme platnosť jeho negácie a odvodzujeme dôsledky, ktoré z toho vyplývajú. Táto naša snaha nás dovedie ku sporu, čiže k nejakému tvrdeniu, ktoré je v rozpore s už známymi a dokázanými tvrdeniami, alebo predpokladmi. Z toho vyplýva, že negácia pôvodného tvrdenia je nepravdivá, a preto musí byť pôvodné tvrdenie pravdivé.

Ako príklad si uvidíme dôkaz tvrdenia, že číslo $\sqrt{2}$ nie je racionálne. Ako už bolo spomenuté pri racionálnych číslach, na strane 15, starí Gréci sa dlho domnievali, že všetky čísla sú buď celé, alebo sa dajú vyjadriť ako zlomok. Až v 5. storočí pred n. l. sa Hippasovi podarilo zistiť, že existujú aj čísla, ktoré sa nedajú vyjadriť ako zlomok. K tomuto svojmu objavu dospel nechtiac a úplnou náhodou, keď sa snažil presne vyjadriť dĺžku uhlopriečky štvorca so stranou dĺžky 1. Hippasos bol členom sekty pytagorejcov a na zverejnenie svojho objavu kruto doplatil, pretože tvrdenie, že všetky čísla sa dajú zapísať ako zlomok, bol jeden z ústredných bodov ich učenia. Dôkaz sporom toho, že $\sqrt{2}$ nie je racionálne číslo, si tu teraz uvidíme.

■ **Príklad 2.12** Číslo $\sqrt{2}$ nie je racionálne. Dokážte!

Dôkaz: Takéto tvrdenie nevieme dokázať priamo, ani nepriamo. Skúsme preto na chvíľu predpokladať, že uvedené tvrdenie neplatí a odvodíme dôsledky, ktoré z toho vyplývajú. Negácia tvrdenia zo zadania úlohy bude

Číslo $\sqrt{2}$ je racionálne.

Ak $\sqrt{2} \in \mathbb{Q}$, tak musia existovať čísla $p, q \in \mathbb{Z}$ také, že $\sqrt{2} = \frac{p}{q}$. Bez straty na všeobecnosti môžeme predpokladať, že čísla p a q sú nesúdeliteľné, čo znamená, že zlomok $\frac{p}{q}$ je vo vykrátenom tvare. Ak by totiž čísla p a q neboli nesúdeliteľné, tak ich vykrátíme ich najväčším spoločným deliteľom, dostaneme čísla $p', q' \in \mathbb{Z}$ a platilo by $\sqrt{2} = \frac{p'}{q'} = \frac{p}{q}$. Takže máme nesúdeliteľné čísla $p, q \in \mathbb{Z}$ a platí

$$\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2} \implies 2q^2 = p^2.$$

Z poslednej rovnosti a príkladu 2.9 (str. 35) vyplýva, že číslo p je párne. Čiže existuje $m \in \mathbb{Z}$ také, že $p = 2m$. Potom ale $p^2 = 4m^2$ a poslednú rovnosť si môžeme upraviť

$$2q^2 = p^2 \implies 2q^2 = 4m^2 \implies q^2 = 2m^2.$$

Opäť z poslednej rovnosti a z príkladu 2.9 vyplýva, že číslo q je párne. Takže sme ukázali, že obe čísla p a q sú párne. Tieto čísla potom nie sú nesúdeliteľné, pretože sú obe deliteľné číslom 2, čo je v spore s predpokladom na začiatku dôkazu. Takže z predpokladu, že tvrdenie zo zadania úlohy neplatí, sme dospeli k sporu. Z toho vyplýva, že tvrdenie zo zadania úlohy musí platiť. Q.E.D. ■

Uvedieme si ešte jeden príklad dôkazu sporom. Tento dôkaz tiež pochádza od starých Grékov, rovnako ako Hippasov dôkaz z predošlého príkladu. Ide o klasický Euklidov dôkaz neexistencie najväčšieho prvočísla.

■ **Príklad 2.13** Neexistuje najväčšie prvočíсло. Dokážte!

Dôkaz: priamy ani nepriamy dôkaz tohto tvrdenia spraviť nevieme. Na priamy dôkaz by sme museli vymenovať všetky prvočísla, ktorých je nekonečne mnoho a o nepriamom dôkaze vôbec nemôžeme uvažovať, pretože tvrdenie zo zadania úlohy nie je implikácia. Takže ideme sa pokúsiť o dôkaz sporom. Negácia uvedeného tvrdenia je

Existuje najväčšie prvočíсло.

Budeme teda predpokladať, že existuje najväčšie prvočíсло a označíme si ho p_n . Všetky existujúce prvočísla potom môžeme zoradiť podľa veľkosti do konečnej postupnosti $\{p_1, p_2, \dots, p_n\}$. Zostrojme si teraz číslo N ako súčin všetkých existujúcich prvočísel, zväčšený o 1

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

Základná veta aritmetiky hovorí, že každé prirodzené číslo väčšie než 1 sa dá jednoznačne zapísať ako súčin mocnín prvočísel, t.j. napríklad $168 = 2^3 \cdot 3 \cdot 7$. Preto, podľa základnej vety aritmetiky, aj číslo N sa musí dať zapísať ako súčin mocnín prvočísel. Ale akých prvočísel? Číslo N sme predsa zostrojili ako súčin všetkých existujúcich prvočísel zväčšený o 1. Takže ak ho budeme deliť ľubovoľným prvočíslom z množiny $\{p_1, p_2, \dots, p_n\}$, tak dostaneme zvyšok 1 a predpokladali sme, že iné prvočísla už neexistujú. Preto N nie je deliteľné žiadnym prvočíslom, a teda sa ani nedá zapísať ako súčin mocnín prvočísel, čo je spor so základnou vetou aritmetiky. Predpokladom, že existuje najväčšie prvočíсло sme sa, ako vidíme, dostali ku sporu. Takže tento predpoklad je nesprávny a platí jeho negácia, t.j. neexistuje najväčšie prvočíсло. Q.E.D. ■

2.4 Dôkaz matematickou indukciou

Matematická indukcia je metóda, pomocou ktorej sa dokazujú tvrdenia platiace pre prirodzené čísla, alebo pre spočítateľné (nekonečné) množiny. *Spočítateľné množiny* sú také množiny, ktorých všetky prvky sa dajú očíslovať pomocou navzájom rôznych prirodzených čísel. Princíp matematickej indukcie sa dá ilustrovať nasledovným spôsobom.

1. Na nekonečnej tabuli majme postupnosť kruhov, očíslovaných číslami $1, 2, 3, \dots, n, \dots$
2. Nech je 1. kruh zafarbený.
3. Pre každé $n \in \mathbb{N}$ nech platí, že ak je n . kruh zafarbený, tak je aj $(n + 1)$. kruh zafarbený.

Asi každý bude súhlasiť s tým, že z uvedených troch bodov vyplýva, že všetky kruhy sú zafarbené. A toto je práve princíp matematickej indukcie a veľmi významná vlastnosť prirodzených čísel. Tento princíp sa používa pri dokazovaní pravdivosti výrokov, závisiacich od parametra $n \in \mathbb{N}$.

■ **Príklad 2.14** Nech $S_n = 1 + 2 + \dots + n$. Potom pre každé $n \in \mathbb{N}$ platí $S_n = \frac{n(n+1)}{2}$. Dokážte!

Dôkaz: budeme robiť v dvoch krokoch.

1. Najskôr si platnosť tvrdenia overíme pre malé hodnoty n .

$$\begin{aligned} S_1 = 1 &= 1 = \frac{1 \cdot 2}{2} \\ S_2 = 1 + 2 &= 3 = \frac{2 \cdot 3}{2} \\ S_3 = 1 + 2 + 3 &= 6 = \frac{3 \cdot 4}{2} \\ &\dots \text{ atď.} \end{aligned}$$

Vo všeobecnosti nie je potrebné overovať tvrdenie pre viacero hodnôt. Nám by úplne stačilo overiť tvrdenie pre S_1 . Toto sa nazýva *prvý krok matematickej indukcie*.

2. V ďalšom kroku dokážeme, že ak tvrdenie platí pre nejaké číslo $n \in \mathbb{N}$, tak platí aj pre číslo $(n+1) \in \mathbb{N}$. Predpoklad, že tvrdenie platí pre nejaké $n \in \mathbb{N}$, sa nazýva *indukčný predpoklad*. Dôkaz, že z platnosti tvrdenia pre číslo n vyplýva platnosť tvrdenia pre číslo $(n+1)$, sa nazýva *indukčný krok*. V našom prípade musíme dokázať, že

$$\text{ak } S_n = 1 + 2 + \dots + n = \frac{n \cdot (n+1)}{2}, \text{ tak platí } S_{n+1} = \frac{(n+1)(n+1+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

V bode č. 1 sme overili, že tvrdenie platí pre S_1 a ak teraz ukážeme, že z platnosti tvrdenia pre S_n vyplýva platnosť tvrdenia pre S_{n+1} , tak podľa princípu matematickej indukcie tvrdenie platí pre všetky prirodzené čísla n . Ideme teda dokázať, že z platnosti tvrdenia pre S_n vyplýva platnosť tvrdenia pre S_{n+1} .

$$S_{n+1} = \underbrace{1 + 2 + \dots + n}_{S_n} + (n+1) = \frac{n \cdot (n+1)}{2} + (n+1) = \frac{n \cdot (n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Tým je dokázané, že ak platí tvrdenie pre S_n , tak platí aj pre S_{n+1} a potom, podľa princípu matematickej indukcie, platí aj $\forall n \in \mathbb{N}$. Q.E.D. ■

P Tvrdenie z predošlého príkladu dokázal Carl Friedrich Gauss už ako 9 ročný školák. Nerobil to však matematickou indukciou, ale priamym dôkazom. Tento geniálny matematik z prelomu 18. a 19. storočia bol už ako malý chlapec veľmi bystrý. Učiteľ v škole, do ktorej chodil, sa raz chcel venovať nejakej svojej práci a aby ho žiaci nejaký čas nerušili, potreboval ich „zabaviť“. Prikázal im preto vypočítať súčet čísel od 1 po 100 mysliať si, že im sčítavanie 100 čísel potrvá dosť dlho. Gauss si však všimol nasledovnú vec

$$\begin{array}{cccccccc} 1 & + & 2 & + & 3 & + \dots + & (n-2) & + & (n-1) & + & n \\ + & n & + & (n-1) & + & (n-2) & + \dots + & 3 & + & 2 & + & 1 \\ \hline (n+1) & + & (n+1) & + & (n+1) & + \dots + & (n+1) & + & (n+1) & + & (n+1) \end{array}$$

t. j. ak v súčte prvých n prirodzených čísel sčíta prvé s posledným, druhé s predposledným atď., tak vždy dostane výsledok $(n+1)$. Keď takto spáruje každé z daných n čísel a spočíta súčet všetkých párov, dostane hodnotu $n \cdot (n+1)$. V tejto hodnote je ale každé číslo pôvodného súčtu zarátané dvakrát (napr. $1 + n$ a $n + 1$), takže výsledok ešte treba vydeliť dvoma. A Gaussov učiteľ bol veľmi prekvapený, keď správny výsledok súčtu čísel od 1 po 100 dostal už po pár sekundách.

Sformulujeme teraz princípu matematickej indukcie ako vetu.

Veta 2.4.1 — Matematická indukcia. Nech pre každé $n \in \mathbb{N}$ je $V(n)$ výrok. Nech

1. *Prvý krok* – Výrok $V(1)$ je pravdivý.
2. *Indukčný krok* – Nech pre každé $n \in \mathbb{N}$: $V(n) \implies V(n+1)$.

Potom $\forall n \in \mathbb{N}$ je výrok $V(n)$ pravdivý.

S faktoriálom sa skoro určite všetci stretli už na strednej škole, napr. pri kombinatorike. Avšak pre úplnosť si tu uvedieme jeho formálnu definíciu.

Definícia 2.4.1 — Faktoriál. Nech $n \in \mathbb{N}$. Faktoriál čísla n , označujeme $n!$, vypočítame ako

$$n! = \begin{cases} 1, & \text{ak } n = 0 \\ n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1, & \text{ak } n \geq 1. \end{cases}$$

■ **Príklad 2.15** Napr. $0! = 1$, $3! = 3 \cdot 2 \cdot 1 = 6$, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ atď. ■

Teraz si pomocou matematickej indukcie dokážeme ďalšie tvrdenie.

■ **Príklad 2.16** Pre každé $n \in \mathbb{N}$: $n \geq 1$ platí $n! \geq 2^{n-1}$. Dokážte!

Dôkaz: Toto tvrdenie, na rozdiel od príkladu 2.14, hovorí o nerovnosti. Rovnako ho však budeme dokazovať matematickou indukciou.

1. Prvý krok indukcie – overíme si tvrdenie pre $n = 1$

$$1! = 1 \geq 1 = 2^{1-1}.$$

2. Indukčný krok – z predpokladu, že platí $n! \geq 2^{n-1}$ musíme dokázať, že platí $(n+1)! \geq 2^n$.

$$(n+1)! = (n+1) \cdot n! \geq (n+1) \cdot 2^{n-1}. \quad (2.1)$$

Keďže $n \geq 1$, platí $(n+1) \geq 2$ a z nerovnosti (2.1) potom dostávame $(n+1)! \geq 2^n$. Q.E.D. ■

Niekedy pomocou matematickej indukcie dokazujeme platnosť výrokov

$$V(n_0), V(n_0+1), V(n_0+2), \dots, \text{ kde } n_0 \neq 1.$$

V takom prípade bude prvý krok indukcie dôkaz pravdivosti výroku $V(n_0)$ a indukčným krokom bude dôkaz, že pre každé $n \in \mathbb{N}$: $n \geq n_0$ z pravdivosti výroku $V(n)$ vyplýva pravdivosť výroku $V(n+1)$.

■ **Príklad 2.17 [Súčet prvých n členov geometrickej postupnosti.]**

Majme $a \in \mathbb{R}$ a $q \in \mathbb{R}$, $q \neq 1$. Potom pre všetky prirodzené čísla $n \geq 0$ platí

$$\text{Nech } S_n = a + aq + aq^2 + \dots + aq^n, \text{ potom } S_n = \frac{a(q^{n+1} - 1)}{q - 1}. \text{ Dokážte!}$$

Dôkaz: budeme robiť matematickou indukciou, pričom prvý krok spravíme pre $n = 0$.

1. Prvý krok – overenie pre $n = 0$.

$$\text{Rovnosť } S_0 = a = \frac{a(q^{0+1} - 1)}{q - 1} \text{ platí.}$$

2. Indukčný krok – ukážeme, že z platnosti rovnosti pre n vyplýva platnosť rovnosti pre $(n+1)$.

$$\begin{aligned} S_{n+1} &= \underbrace{a + aq^1 + aq^2 + \dots + aq^n}_{S_n} + aq^{n+1} = \frac{a(q^{n+1} - 1)}{q - 1} + aq^{n+1} = \\ &= \frac{aq^{n+1} - a + aq^{n+2} - aq^{n+1}}{q - 1} = \frac{a(q^{n+2} - 1)}{q - 1}. \quad \text{Q.E.D.} \end{aligned}$$

P Špeciálne pre $a = 1$ a $q = 2$ podľa predošlého príkladu dostávame

$$1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1.$$

■ **Príklad 2.18** Pre každé $n \in \mathbb{N}$ 4 delí číslo $5^n - 1$. Dokážte!

Dôkaz: budeme opäť robiť matematickou indukciou.

1. Prvý krok – pre $n = 1$: 4 delí číslo $5^1 - 1 = 4$.
2. Indukčný krok – nech 4 delí číslo $5^n - 1$ (zapisuje sa to $4 \mid (5^n - 1)$). Ukážeme, že z toho vyplýva, že $4 \mid (5^{n+1} - 1)$. Ak $4 \mid (5^n - 1)$, tak musí existovať $k \in \mathbb{Z}$ také, že $5^n - 1 = 4k$. Potom

$$5^{n+1} - 1 = 5^{n+1} - 5^n + 5^n - 1 = 5^n(5 - 1) + 4k = 4(5^n + k).$$

Keďže $4 \mid [4(5^n + k)]$, je pôvodné tvrdenie dokázané. Q.E.D. ■

P Tvrdenie z predošlého príkladu sa dá ľahko dokázať aj priamym výpočtom – pozri cvičenie 2.7.

Nech $\mathbb{X}$ je množina. Pripomeňme si, že $\mathcal{P}(\mathbb{X})$ označuje potenčnú množinu množiny $\mathbb{X}$. Podľa definície 1.1.10 je to množina všetkých podmnožín množiny $\mathbb{X}$. Napríklad

$$\begin{aligned} \mathcal{P}(\{a, b\}) &= \{\emptyset, \{a\}, \{b\}, \{a, b\}\}, \\ \mathcal{P}(\{a, b, c\}) &= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}. \end{aligned}$$

Dokážeme teraz vetu

Veta 2.4.2 — O potenčnej množine. Nech $n \in \mathbb{N}$, $n \geq 0$. Ak $\mathbb{X}$ je množina, $|\mathbb{X}| = n$, potom platí $|\mathcal{P}(\mathbb{X})| = 2^n$.

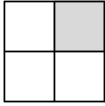
Dôkaz: sa dá spraviť priamo, alebo matematickou indukciou. My tu samozrejme spravíme dôkaz indukciou.

1. Prvý krok – Pre $n = 0$ musí byť $\mathbb{X} = \emptyset$ a jediná podmnožina $\mathbb{X}$ je $\emptyset$. Takže $\mathcal{P}(\mathbb{X}) = \{\emptyset\}$ a $|\mathcal{P}(\mathbb{X})| = 1 = 2^0$.
2. Indukčný krok – Nech tvrdenie platí pre n a množina $\mathbb{X}$ má $(n+1)$ prvkov. Zvoľme si nejaký prvok $x \in \mathbb{X}$. Podmnožín množiny $\mathbb{X}$, ktoré obsahujú prvok x , je presne toľko ako podmnožín množiny $\mathbb{X}$, ktoré neobsahujú prvok x . Každú podmnožinu $\mathbb{X}$ obsahujúcu prvok x totiž vieme jednoznačne priradiť podmnožinu neobsahujúcu prvok x tak, že prvok x z nej vynecháme. Opačne to platí tiež (pridáme prvok x).
Vynechaním prvku x z množiny $\mathbb{X}$ dostaneme množinu $\mathbb{Y} = \mathbb{X} \setminus \{x\}$, pre ktorú platí $|\mathbb{Y}| = n$ a $|\mathcal{P}(\mathbb{Y})| = 2^n$. Takže podmnožín množiny $\mathbb{X}$, ktoré neobsahujú prvok x je, podľa indukčného predpokladu, 2^n a presne toľko isto je aj podmnožín množiny $\mathbb{X}$, ktoré obsahujú prvok x . Platí teda $|\mathcal{P}(\mathbb{X})| = 2^n + 2^n = 2^{n+1}$. Q.E.D.

■ **Príklad 2.19** Tromino je plošný útvar zložený z troch štvorcov so stranou jednotkovej dĺžky . Ak zo šachovnice s rozmermi $2^k \times 2^k$ odstránime ľubovoľné políčko, tak zvyšok šachovnice sa bude dať pokryť trominami tak, aby sa neprekrývali. Dokážte!

Dôkaz: budeme robiť matematickou indukciou vzhľadom na k .

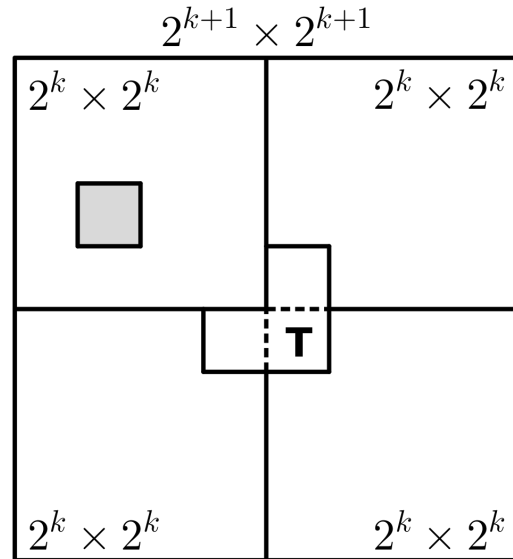
1. Prvý krok – Ukážeme, že tvrdenie platí pre $k = 1$.



Ak zo šachovnice s rozmermi $2^1 \times 2^1$ odstránime ľubovoľné políčko, tak to, čo nám zostane, je tromino. Takže po odstránení ľubovoľného políčka sa zvyšok šachovnice určite bude dať pokryť trominom.

2. Indukčný krok – Predpokladajme, že tvrdenie platí pre k a ukážeme, že potom musí platiť aj pre $(k + 1)$.

Šachovnicu s rozmermi $2^{k+1} \times 2^{k+1}$ si rozdělíme na 4 šachovnice rozmerov $2^k \times 2^k$. Zo šachovnice odstránime ľubovoľné políčko. Na obrázku je toto vyznačené šedou farbou. Do stredu šachovnice potom umiestnime jedno tromino tak, aby pokrývalo práve jedno políčko v každej zo zvyšných troch štvrtín šachovnice. Teraz v každej štvrtine šachovnice chýba, alebo je pokryté, práve jedno políčko. Podľa indukčného predpokladu môžeme zvyšok každej zo štvrtín šachovnice pokryť trominami, čiže šachovnica $2^{k+1} \times 2^{k+1}$ sa, po odstránení ľubovoľného políčka, dá pokryť trominami. Tým je tvrdenie dokázané. Q.E.D. ■



Predtým, ako sa pustíme do cvičení, si zadefinujeme funkciu *modulo* a funkciu *symetrickej diferencie dvoch množín*. Pomôže nám to zostručniť zápis niektorých úloh.

Definícia 2.4.2 — Modulo – zvyšok po delení. Majme čísla $a \in \mathbb{Z}$ a $0 \neq p \in \mathbb{N}$. Potom funkcia „ a modulo p “, označujeme ju $a \pmod{p}$, je zvyšok, ktorý dáva číslo a po delení číslom p . Platí

$$r = a \pmod{p} \iff ((0 \leq r < p) \wedge (\exists k \in \mathbb{Z}: a = k \cdot p + r)).$$

Definícia 2.4.3 — Symetrická diferencia množín. Majme dve množiny $\mathbb{A}$ a $\mathbb{B}$. Potom ich symetrická diferencia, označujeme ju $\mathbb{A} \triangle \mathbb{B}$, sa definuje ako

$$\mathbb{A} \triangle \mathbb{B} = (\mathbb{A} \cup \mathbb{B}) \setminus (\mathbb{A} \cap \mathbb{B}).$$

2.5 Cvičenia

Priamy dôkaz

Cvičenie 2.1 Dokážte, že uvedená postupnosť je klesajúca

(a) $\left\{ \frac{n+2}{2n+1} \right\}_{n=1}^{\infty}$

(b) $\left\{ \frac{1}{n(n+1)} \right\}_{n=1}^{\infty}$

■

Cvičenie 2.2 Dokážte, že uvedená postupnosť je ohraničená

(a) $\left\{ \frac{2n}{n+1} + \frac{n+1}{3n} \right\}_{n=1}^{\infty}$

(b) $\left\{ 3 + \frac{1}{2n} \right\}_{n=1}^{\infty}$

(c) $\left\{ \frac{n^2}{n^2+2n+1} \right\}_{n=1}^{\infty}$

■

Cvičenie 2.3 Dokážte, že pre každú aritmetickú postupnosť platí vzťah

$$a_{k-1}^2 + 8a_k \cdot a_{k+1} = (2a_k + a_{k+1})^2.$$

■

Cvičenie 2.4 Dokážte, že ak čísla a, b, c sú tri po sebe idúce členy aritmetickej postupnosti, tak platí vzťah $(a+b+c)^2 - 3(a^2+b^2+c^2) + 6(a-b)^2 = 0$.

■

Cvičenie 2.5 Dokážte, že $\forall x \in \mathbb{Z}$ platí: buď $x^2 \pmod{4} = 0$, alebo $x^2 \pmod{4} = 1$. Inak povedané, štvorec ľubovoľného celého čísla dáva po delení 4 zvyšok buď 0, alebo 1.

■

Cvičenie 2.6 Dokážte, že $\forall x \in \mathbb{Z}$ platí: $(3 \mid x^2) \Rightarrow (3 \mid x)$.

■

Cvičenie 2.7 Dokážte, že platí $\forall n \in \mathbb{N} : 4 \mid (5^n - 1)$.

■

Cvičenie 2.8 Dokážte, že $\forall m, n \in \mathbb{Z}$ platí(a) ak m, n sú párne, tak $m+n$ je párne(d) $(2 \nmid m \wedge 2 \nmid n) \Rightarrow (2 \mid (m+n))$ (b) $(2 \mid m \wedge 2 \mid n) \Rightarrow (2 \mid m \cdot n)$ (e) $(2 \nmid m \wedge 2 \nmid n) \Rightarrow (2 \nmid m \cdot n)$ (c) $(2 \nmid m \wedge 2 \mid n) \Rightarrow (2 \mid m \cdot n)$ (f) $(2 \mid m \wedge 2 \mid (m+n)) \Rightarrow (2 \mid n)$

■

Cvičenie 2.9 Dokážte, že $\forall x \in \mathbb{Q}$ platí $(x \neq 0) \Rightarrow (\frac{1}{x} \in \mathbb{Q})$.

■

Cvičenie 2.10 Dokážte, že $\forall x, y \in \mathbb{Q}$ platí(a) $x \cdot y \in \mathbb{Q}$ (b) $(x+y) \in \mathbb{Q}$

■

Cvičenie 2.11 Nech $\mathbb{X}$ a $\mathbb{Y}$ sú neprázdne množiny, pre ktoré platí $\mathbb{X} \times \mathbb{Y} = \mathbb{Y} \times \mathbb{X}$. Čo vieme povedať o množinách $\mathbb{X}$ a $\mathbb{Y}$? Dokážte to!

■

Cvičenie 2.12 Dokážte, že pre ľubovoľné dve množiny X a Y platí

- (a) $X \cap Y \subseteq X$ (b) $X \subseteq (X \cup Y)$

Cvičenie 2.13 Dokážte, že pre ľubovoľné dve množiny X a Y platí

- (a) $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$ (c) $(\mathcal{P}(X) \subseteq \mathcal{P}(Y)) \Rightarrow (X \subseteq Y)$
 (b) $\mathcal{P}(X \cap Y) = \mathcal{P}(X) \cap \mathcal{P}(Y)$

Cvičenie 2.14 Dokážte, že pre ľubovoľné dve množiny A a B platí

- (a) $A \triangle B = (A \setminus B) \cup (B \setminus A)$ (b) $(A \triangle B) \triangle A = B$

Cvičenie 2.15 Dokážte, že pre ľubovoľné tri množiny X , Y a Z platí

- (a) $(X \subseteq Y) \Rightarrow (X \cup Z \subseteq Y \cup Z)$ (c) $(X \subseteq Y) \Rightarrow (Z \setminus Y \subseteq Z \setminus X)$
 (b) $(X \subseteq Y) \Rightarrow (X \cap Z \subseteq Y \cap Z)$ (d) $(X \subseteq Y) \Rightarrow (Y \setminus (Y \setminus X) = X)$
 (e) $((X \cap Y = X \cap Z) \wedge (X \cup Y = X \cup Z)) \Rightarrow (Y = Z)$

Cvičenie 2.16 Nech X , Y a Z sú tri množiny z univerza $\mathcal{U}$ a univerzum pre kartézky súčin je $\mathcal{U} \times \mathcal{U}$. Dokážte nasledujúce tvrdenia, ak sú pravdivé. Inak nájdite kontrapríklad.

- (a) $\forall X, Y \in \mathcal{U} : (X \subseteq Y) \vee (Y \subseteq X)$ (d) $\forall X, Y \in \mathcal{U} : \overline{X \cap Y} \subseteq \overline{X} \cap \overline{Y}$
 (b) $\forall X, Y \in \mathcal{U} : \overline{Y \setminus X} = X \cup \overline{Y}$ (e) $\forall X, Y \in \mathcal{U} : \overline{X} \times \overline{Y} = \overline{X \times Y}$
 (c) $\forall X, Y \in \mathcal{U} : \overline{X \setminus Y} = \overline{Y} \setminus \overline{X}$ (f) $\forall X, Y \in \mathcal{U} : (X \cap Y) \cup (Y \setminus X) = Y$
 (g) $\forall X, Y, Z \in \mathcal{U} : X \times (Y \setminus Z) = (X \times Y) \setminus (X \times Z)$
 (h) $\forall X, Y, Z \in \mathcal{U} : X \cap (Y \times Z) = (X \cap Y) \times (X \cap Z)$
 (i) $\forall X, Y, Z \in \mathcal{U} : X \cup (Y \setminus Z) = (X \cup Y) \setminus (X \cap Z)$
 (j) $\forall X, Y, Z \in \mathcal{U} : Y \setminus Z = (X \cup Y) \setminus (X \cup Z)$
 (k) $\forall X, Y, Z \in \mathcal{U} : X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$
 (l) $\forall X, Y, Z \in \mathcal{U} : (X \times Y) \cup (X \times Z) = X \times (Y \cup Z)$
 (m) $\forall X, Y, Z \in \mathcal{U} : X \setminus (Y \times Z) = (X \setminus Y) \times (X \setminus Z)$

Cvičenie 2.17 Pre ľubovoľné tri množiny A , B a C dokážte, alebo vyvráťte tvrdenia

- (a) $\star (A \triangle C = B \triangle C) \Rightarrow (A = B)$ (e) $A \triangle (B \cup C) = (A \triangle B) \cup (A \triangle C)$
 (b) $\star (A \triangle B) \triangle C = A \triangle (B \triangle C)$ (f) $A \cup (B \triangle C) = (A \cup B) \triangle (A \cup C)$
 (c) $A \triangle (B \cap C) = (A \triangle B) \cap (A \triangle C)$ (g) $A \triangle B = B \triangle A$
 (d) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

Cvičenie 2.18 Dokážte, že pre ľubovoľné množiny A a B_i platí

$$A \cup (B_1 \cap B_2 \cap \dots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \dots \cap (A \cup B_n).$$

Nepriamy dôkaz

Cvičenie 2.19 Dokážte: $\forall x \in \mathbb{R} : (x^2 \notin \mathbb{Q}) \Rightarrow (x \notin \mathbb{Q})$. ■

Cvičenie 2.20 Dokážte: $\forall x \in \mathbb{R} : (x^3 \notin \mathbb{Q}) \Rightarrow (x \notin \mathbb{Q})$. ■

Cvičenie 2.21 Dokážte tvrdenia

- (a) $\forall n \in \mathbb{Z} : (2 \nmid n^2) \Rightarrow (2 \nmid n)$
- (b) $\forall x, y, z \in \mathbb{R} : (x + y + z \geq 3) \Rightarrow (x \geq 1 \vee y \geq 1 \vee z \geq 1)$
- (c) $\forall x, y \in \mathbb{R} : (x \cdot y \leq 2) \Rightarrow (x \leq \sqrt{2} \vee y \leq \sqrt{2})$ ■

Dôkaz sporom

Cvičenie 2.22 Dokážte, že $\sqrt[3]{2}$ nie je racionálne číslo. ■

Cvičenie 2.23 Dokážte, že $\sqrt{3}$ nie je racionálne číslo.
(Pomôcka: najskôr vyriešte cvičenia 2.5 a 2.6.) ■

Cvičenie 2.24 Dokážte, že nasledujúce čísla nie sú racionálne

- (a) $\log 2$ (b) $\log 5$ (c) $\log 15$ (d) $\log 21$ ■

Cvičenie 2.25 Dokážte, že pre ľubovoľné dve množiny $\mathbb{A}$ a $\mathbb{B}$ platí $(\mathbb{A} \setminus \mathbb{B}) \cap (\mathbb{B} \setminus \mathbb{A}) = \emptyset$. ■

Cvičenie 2.26 Dokážte, že pre ľubovoľnú množinu $\mathbb{A}$ platí $\mathbb{A} \times \emptyset = \emptyset$. ■

Cvičenie 2.27 Dokážte, že prvočísel je nekonečne veľa. ■

Cvičenie 2.28 Dokážte, že ak 100 lôpt rozmiestnime do 9 krabíc, tak v aspoň jednej krabici bude aspoň 12 lôpt. ■

Cvičenie 2.29 Dokážte, že ak 40 lôpt rozmiestnime do 9 krabíc, pričom v každej krabici bude aspoň 1 lopta, tak aspoň dve krabice budú obsahovať rovnaký počet lôpt. ■

Cvičenie 2.30 Nech $A = \frac{s_1 + s_2 + \dots + s_n}{n}$ je aritmetický priemer čísel $s_1, s_2, \dots, s_n \in \mathbb{R}$. Dokážte

- (a) $\exists i \in \mathbb{N} : s_i \leq A$ (b) $\exists i \in \mathbb{N} : s_i \geq A$ ■

Cvičenie 2.31 Dokážte tvrdenia

- (a) $\forall x, y \in \mathbb{R} : (x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \Rightarrow (x + y) \notin \mathbb{Q}$
- (b) $\forall x, y \in \mathbb{R} : (x \in \mathbb{Q} \wedge y \notin \mathbb{Q} \wedge x \neq 0) \Rightarrow (x \cdot y) \notin \mathbb{Q}$
- (c) $(\forall x, y \in \mathbb{R}) : ((\forall \varepsilon > 0) : x - y \leq \varepsilon) \Rightarrow (x \leq y)$ ■

Dôkaz matematickou indukciou

Cvičenie 2.32 Dokážte, že každé celé číslo väčšie než 1 vieme zapísať ako súčin mocnín prvočísel. ■

Cvičenie 2.33 Dokážte, že n bodov v rovine, z ktorých žiadne tri nie sú kolineárne, vieme spojiť práve $\frac{n(n-1)}{2}$ priamkami, ak každý bod spájame s každým práve jednou priamkou. ■

Cvičenie 2.34 Dokážte, že $\forall n \in \mathbb{N}$ platí

- | | | |
|--|------------------------------------|-------------------------------------|
| (a) $6 \mid (7^n - 1)$ | (c) $31 \mid (5^{n+1} + 6^{2n-1})$ | (e) $11 \mid (2^{2n-1} + 3^{4n-2})$ |
| (b) $4 \mid (6 \cdot 7^n - 2 \cdot 3^n)$ | (d) $5 \mid (11^n - 1)$ | (f) $30 \mid (7^{4n+1} - 7)$ |

Cvičenie 2.35 Dokážte, že $\forall n \in \mathbb{N}$ platí nerovnosť $\frac{1}{2n} \leq \frac{1 \cdot 3 \cdot 5 \dots (2n-1)}{2 \cdot 4 \cdot 6 \dots 2n}$. ■

Cvičenie 2.36 Pre každé $n \in \mathbb{N}$ dokážte rovnosti

- | | |
|--|--|
| (a) $\sum_{i=1}^n (2i-1) = n^2$ | (g) $\sum_{i=1}^n (2i-1)^2 = \frac{n \cdot (2n-1)(2n+1)}{3}$ |
| (b) $\sum_{i=1}^n i \cdot (i+1) = \frac{n \cdot (n+1) \cdot (n+2)}{3}$ | (h) $\sum_{i=1}^n i^3 = \left(\frac{n \cdot (n+1)}{2} \right)^2$ |
| (c) $\sum_{i=1}^n i \cdot (i+1) \cdot (i+2) = \frac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4}$ | (i) $\sum_{i=1}^n \frac{1}{i \cdot (i+1)} = 1 - \frac{1}{n+1}$ |
| (d) $\sum_{i=1}^n i \cdot (i!) = (n+1)! - 1$ | (j) $\sum_{i=1}^n \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$ |
| (e) $\sum_{i=1}^n i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$ | (k) $\sum_{i=1}^n \frac{i^2}{(2i-1)(2i+1)} = \frac{n(n+1)}{2(2n+1)}$ |
| (f) $\sum_{i=1}^n (-1)^{i+1} i^2 = (-1)^{n+1} \cdot \frac{n \cdot (n+1)}{2}$ | (l) $\sum_{i=1}^n \frac{i}{(i+1)!} = 1 - \frac{1}{(n+1)!}$ |
| (m) $\sum_{i=1}^n \frac{1}{(i+1)^2 - 1} = \frac{3}{4} - \frac{1}{2(n+1)} - \frac{1}{2(n+2)}$ | |

Cvičenie 2.37 Dokážte, že pre $2 \leq n \in \mathbb{N}$ platí nerovnosť $\frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \dots + \frac{n}{n+1} < \frac{n^2}{n+1}$. ■

Cvičenie 2.38 Dokážte, že pre $n \in \mathbb{N}$ platia nerovnosti

- | | | |
|--------------------------------|-----------------------------------|----------------------------------|
| (a) pre $n \geq 0$: $2^n > n$ | (b) pre $n \geq 3$: $2^n > 2n+1$ | (c) pre $n \geq 5$: $2^n > n^2$ |
|--------------------------------|-----------------------------------|----------------------------------|

Cvičenie 2.39 Nech $A, B_1, B_2, \dots, B_n$ sú ľubovoľné množiny. Dokážte, že platí

- | | |
|---|--|
| (a) $A \cap (B_1 \cup B_2 \cup \dots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \dots \cup (A \cap B_n)$ | |
| (b) $\overline{B_1 \cap B_2 \cap \dots \cap B_n} = \overline{B_1} \cup \overline{B_2} \cup \dots \cup \overline{B_n}$ | (c) $ B_1 \times B_2 \times \dots \times B_n = B_1 \cdot B_2 \cdot \dots \cdot B_n $ |

Cvičenie 2.40 Dokážte, že nasledujúce logické výroky sú tautológie

(a) $\left(\dots \underbrace{((A \Rightarrow A) \Rightarrow A) \Rightarrow \dots}_{2k \text{ } A\text{-čiek}} \Rightarrow A \right)$

(b) $\left(\dots \underbrace{((\neg A \Rightarrow A) \Rightarrow A) \Rightarrow \dots}_{2k \text{ } A\text{-čiek}} \Rightarrow A \right)$





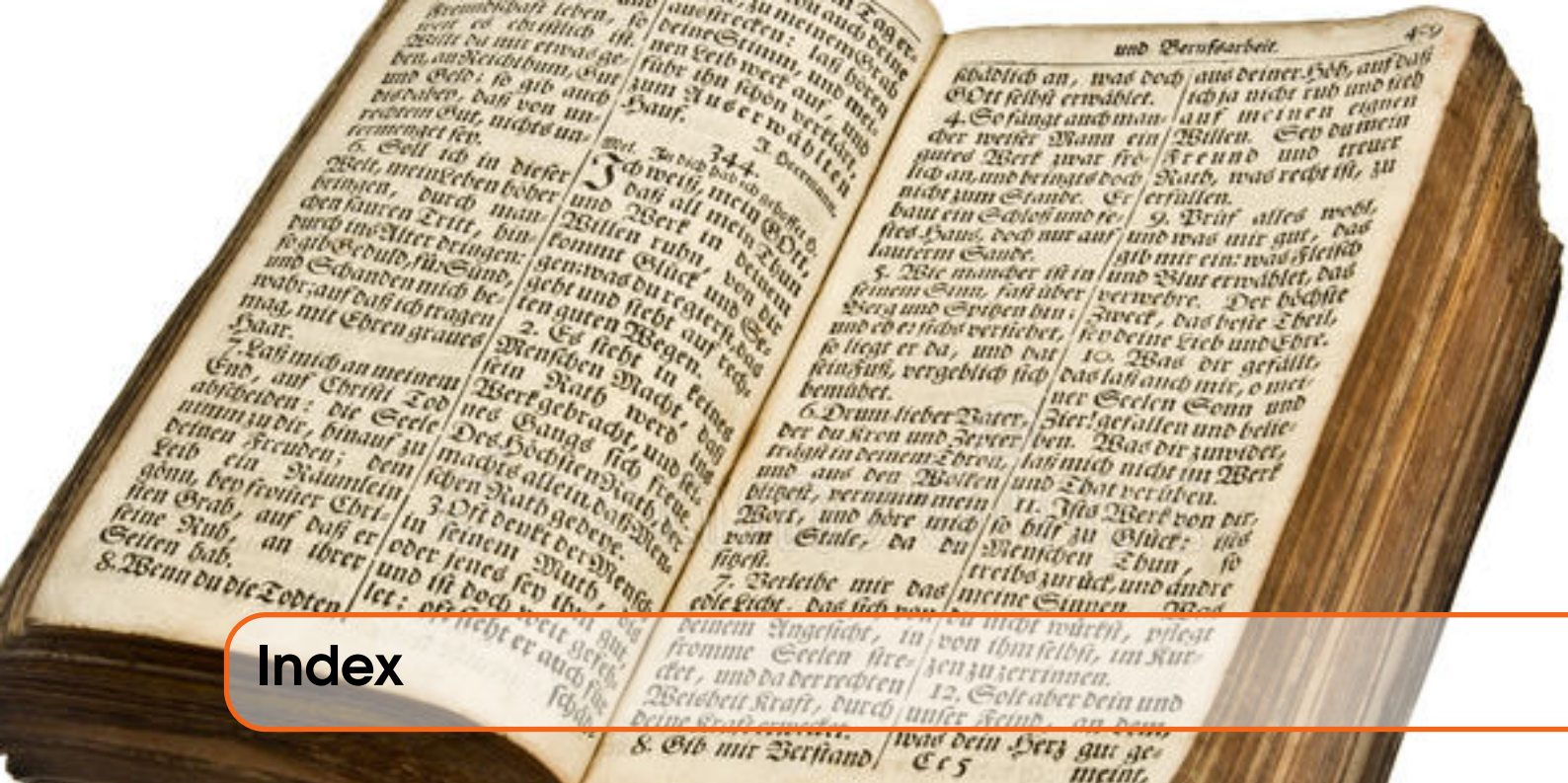
Použitá a odporúčaná literatúra

- [1] Martin Aigner: **Combinatorial Theory**, SPRINGER VERLAG, HEIDELBERG 1979.
- [2] Bohuslav Balcar, Petr Štěpánek: **Teorie množin**, ACADEMIA, PRAHA 1986.
- [3] Berežný, Draženská, Kravcová: **Zbierka úloh z diskrétnej matematiky**, FEI TU, KOŠICE 2005. <http://web.tuke.sk/fei-km/sites/default/files/prilohy/10/Zbierka-DM.pdf>
- [4] J. A. Bondy, U. S. Murty: **Graph Theory With Applications**, NORTH-HOLLAND 1976.
- [5] Reinhard Diestel: **Graph Theory**, SPRINGER 2000.
- [6] Harary, Frank: **Graph theory**, ADDISON-WESLEY 1969.
- [7] Richard Johnsonbaugh: **Discrete Mathematics**, PEARSON 2017.
- [8] Josef Kaucký: **Kombinatorické identity**, VEDA, VYDAVATELSTVO SAV, BRATISLAVA 1975.
- [9] Martin Knor: **Úvod do matematickej logiky**, FIIT STU, BRATISLAVA 2016.
<http://www.math.sk/jmkollar/literatura/Knor-Uvod.do.matematickej.logiky.pdf>
- [10] Martin Knor: **Teória grafov**, SVF STU, BRATISLAVA 2008.
<http://www.svf.stuba.sk/docs/dokumenty/skripta/teoria-grafov.martin.knor.pdf>
- [11] Martin Knor, Jozef Kollár: **Matematika pre architektov**, STU BRATISLAVA, 2002.
- [12] Donald E. Knuth: **The Art of Computer Programming, Volume 1**, ADDISON-WESLEY, 1997.
- [13] Sergei K. Lando: **Lectures on Generating Functions**, AMERICAN MATHEMATICAL SOCIETY, STUDENT MATHEMATICAL LIBRARY 2003.
- [14] Milan Mareš: **Příběhy matematiky**, PISTORIUS & OLŠANSKÁ, PŘÍBRAM 2011.
- [15] J. Matoušek, J. Nešetřil: **Kapitoly z diskrétní matematiky**, KAROLINUM, PRAHA 2002.

- [16] М. В. Меньшиков, А. М. Ревякин, А. Н. Копылова, Ю. Н. Макаров, Б. С. Стечкин: **Комбинаторный Анализ – Задачи и упражнения**, ИЗДАТЕЛЬСТВО »НАУКА«, МОСКВА 1982.
- [17] В. А. Носов: **Комбинаторика и теория графов**, МОСКВА 1999.
<http://intsys.msu.ru/staff/vnosov/combgraph.htm> (PDF verzia)
- [18] Stanislav Palúch: **Algoritmická teória grafov**, ŽILINSKÁ UNIVERZITA, 2008.
<http://frcatel.fri.uniza.sk/users/paluch/grafy.pdf>
- [19] Ján Plesník: **Grafové algoritmy**, VEDA, BRATISLAVA 1983.
- [20] Franco P. Preparata, Raymond T. Yeh: **Úvod do teórie diskretných matematických štruktúr**, ALFA, BRATISLAVA 1982.
- [21] Edward M. Reingold, Jurg Nievergelt, Narsingh Deo: **Combinatorial Algorithms – Theory and Practice**, PRENTICE-HALL, NEW JERSEY 1977.
- [22] Beloslav Riečan a kol.: **Úlohy z matematiky pre 4. ročník gymnázia**, SPN, BRATISLAVA 1976.
- [23] Beloslav Riečan a kol.: **Matematika pre 4. ročník gymnázia**, SPN, BRATISLAVA 1987.
- [24] Beloslav Riečan a kol.: **Zbierka úloh z matematiky pre 4. ročník gymnázia**, SPN, BRATISLAVA 1991.
- [25] Karol Rován a kol.: **Zbierka riešených úloh z algebry pre SVŠ a odborné školy**, SPN, BRATISLAVA 1969.
- [26] К. А. Рыбников: **Введение в Комбинаторный Анализ**, ИЗДАТЕЛЬСТВО МОСКОВСКОГО УНИВЕРСИТЕТА, МОСКВА 1985.
- [27] Raymond M. Smullyan: **A Beginner's Guide to Mathematical Logic**, DOVER PUBLICATIONS, NEW YORK 2014.
- [28] František Vejsada, František Talafous: **Zbierka úloh z matematiky pre SVŠ a gymnázia**, SPN, BRATISLAVA 1973.
- [29] Naum J. Vilenkin: **Rozhovory o množinách**, SPN, BRATISLAVA 1972.
- [30] Herbert S. Wilf: **generatingfunctionology**, ACADEMIC PRESS, INC. 1994.
<https://www.math.upenn.edu/~wilf/DownldGF.html>
- [31] Niklaus Wirth: **Algoritmy a štruktúry údajov**, ALFA, BRATISLAVA 1989.
- [32] Štefan Znáň: **Kombinatorika a teória grafov**, PF UK, BRATISLAVA 1978.

IV

Index



Index

Symboly

∈ operátor „patrí do množiny“	11
∉ operátor „nepatrí do množiny“	11
⊂ operátor vlastnej podmnožiny	12
⊆ operátor nevlastnej podmnožiny	12
⋃ operátor zjednotenia množín	12
⋂ operátor prieniku množín	13
∖ operátor rozdielu množín	13
Ā komplement množiny Ā	14
¬ operátor logickej negácie	20
∨ operátor disjunkcie	20
∧ operátor konjunkcie	20
⇔ operátor ekvivalencie	20
⇒ operátor implikácie	20
∃ existenčný kvantifikátor	23
∀ všeobecný kvantifikátor	23
operátor „a delí b“ (a b)	40
Δ operátor symetrickej diferencie	41

A

acyklický graf	62
algoritmus	
Borůvkov	203
Dijkstrov	229–231
hľadania kostry grafy	179
Jarníkov (Primov)	197
konštrukcie očíslovaného stromu z Prüfe- rovho kódu	241

B

konštrukcie optimálneho Huffmanovho kódu	206
konštrukcie Prüferovho kódu z očíslova- ného stromu	235
konštrukcie prehľadávacieho binárneho stromu	215
Kruskalov	201, 202
pažravý	201
prehľadávania grafu do hĺbky	187
prehľadávania grafu do šírky	182
zostavovania identifikačného kódu binár- neho stromu	219
zostavovania identifikačného kódu kore- ňového stromu	222
antisymetrickosť (relácie)	125, 130
Appel Kenneth (1932–2013)	48
ASCII kód	204
atomická formula	20
axióma	31

backtracking	186
bijektivnosť	145
binárny strom	80
binomický koeficient	171
Borůvka Otakar (1899–1995)	196, 203
Bouton Charles Leonard (1869–1922)	224

C

Catalanovo číslo 174, 213
 Cayley Arthur (1821–1895) 16, 48, 241
 centrálny vrchol grafu 56
 centrum grafu 56
 cesta (v grafe) 55, 112
 cyklus (v grafe) 57, 112

Č

číslo

Catalanovo 174, 213
 celé $\mathbb{Z}$ 15
 iracionálne 15
 komplexné $\mathbb{C}$ 16
 kvaternion 16
 oktonion 16
 prirodzené $\mathbb{N}$ 14
 racionálne $\mathbb{Q}$ 15
 reálne $\mathbb{R}$ 15

D

dátová štruktúra

fronta 180
 zásobník 180

dôkaz

matematickou indukciou 37, 39
 nepriamy 35
 priamy 32
 sporom 36

de Moivre Abraham (1667–1754) 155

de Morgan Augustus (1806–1871) 48

definícia 32

Dijkstra Edsger Wybe (1930–2002) . 197, 230

Dijkstrov algoritmus 229, 231

disjunkcia ($\vee$) 21

disjunktné množiny 13

E

ekvivalencia ($\Leftrightarrow$) 22

ekvivalencia (relácie) 140

entropický kód 204

Euklides Alexandrijský (~3. stor. pred n.l.) 15

Euklidovský priestor 108

Euler Leonhard (1707–1783) 47, 84, 109, 156

F

faktor grafu 62

faktoriál 39

dvojný 172

Fano Roberto Mario (1917–2016) 204

Fibonacci Leonardo (~1170 – ~1240) ... 167

Fibonacciho postupnosť 167

formula

atomická 20

prvotná 20

výroková 20, 22

formuly

ekvivalentné 22

fronta 180

funkcia 143

bijektívna 145

charakteristická funkcia množiny 149

definičný obor 143

injektívna 144

inverzná 145

koobor 143

obor hodnôt 143

parciálna 143

surjektívna 144

vytvárajúca

exponenciálna, 175

obyčajná, 160

zložená 146

G

Gauss Carl Friedrich (1777-1855) 38

geometrická postupnosť

súčet prvých n členov 39

Gonthier Georges 48

graf

acyklický 62

artikulácia 61

bipartitný 53

kompletný ($K_{m,n}$), 54, 112

centrum 56

cesta 55, 112

cesta (P_n) 112

cyklus 57, 112

hamiltonovský, 95

cyklus (C_n) 112

digraf 50

dĺžka ťahu 55

dĺžka cesty 55

graf

dĺžka cyklu	57
dĺžka sledu	54
dokonalé párovanie	89
Eulerova veta o rovinných grafoch	110
eulerovský	87
eulerovský ťah	85
otvorený, 85, 87	
uzavretý, 85, 86	
excentricita vrcholu	56
faktor	62
hodnota	196
hodnota hrany	195
hodnota sledu	229
homeomorfné grafy	112
hrana	49
ohodnotená, 195	
hranica oblasti	108
húsenica	113
hviezda (S_n)	113
incidencia (vrchol–hrana)	50
invariant	101
izomorfizmus	
binárnych stromov, 106	
koreňových stromov, 105	
izomorfizmus grafov	98, 99
izomorfné grafy	99
jadro	225
jednoduchý (obyčajný)	51
Knight graph	98
koleso (W_n)	113
komplementárny	53
kompletný (K_n)	52, 112
kompletný bipartitný ($K_{m,n}$)	54, 112
komponent súvislosti	57, 60
konečný	49
koreňový strom	77
dieťa vrcholu, 78	
koncový vrchol, 78	
list, 78	
otec vrcholu, 78	
podstrom, 78	
potomok vrcholu, 78	
predkovia vrcholu, 78	
súrodenci (vrcholy), 78	
úroveň vrcholu, 77	
vnútorný vrchol, 78	
výška, 77	

graf

kostra	62
minimálna, 196	
Kuratowského veta	112
ľavý podstrom	213
les	77
list	77
matica incidencie	72
matica susednosti	69
minimálna kostra	196
množina vrcholov	
nezávislá, 225	
stabilná, 225	
most	61
najlacnejšia cesta	230
najlacnejšia kostra	196
násobné hrany	50
nekonečný	49
neorientovaný	49
nesúvislý	57
nezávislá množina vrcholov	225
oblasť	108
obyčajný (jednoduchý)	51
ohodnotený	195
ohodnotenie hrany	195
orientovaná hrana	49, 50
orientovaný	49, 50
otvorený sled	55
párovanie	89
maximálne, 89	
perfektné párovanie	89
podgraf	58
polomer	56
pravý podstrom	213
pravidelný	52
prázdny	49, 80
prehľadávanie do šírky	182
prehľadávanie do hĺbky	187
priemer	56
problém obchodného cestujúceho	234
rovinné nakreslenie	108
rovinný	108
sled	54
otvorený, 55	
uzavretý, 55	
slučka (hrana)	50
stabilná množina vrcholov	225

graf
 strom 73
 binárny, 80
 binárny úplný, 81
 binárny dokonalý, 82
 binárny prehľadavací, 214
 binárny vyvážený, 81
 koreň, 77, 105
 očíslovaný, 234
 prehľadavací binárny, 213
 stupeň vrcholu 51
 subdivízia hrany 111
 susedné oblasti 108
 susednosť (vrchol–vrchol) 50
 súvislý 57
 ťah 55
 uzavretý sled 55
 vrchol 49, 50
 centrálny, 56
 izolovaný, 50
 stupeň, 51
 vzdialenosť vrcholov 56
 Graves John Thomas (1806–1870) 16
 Guthrie Francis (1831–1899) 48

H

Haken Wolfgang (1928–...) 48
 Hamilton William R. (1805–1865) . 16, 48, 95
 harmonická postupnosť 166
 Herón Alexandrijský (10–75) 15
 Hippasos (~530–~450 pred n. l.) 15
 hodnota grafu 196
 hrana
 koncový vrchol 181
 počiatočný vrchol 181
 Huffman David Albert (1925–1999) 204
 Huffmanov kód 80, 204, 206
 húsenica (graf) 113
 hviezda (graf) 113
 hypotéza 32

I

implikácia ($\Rightarrow$) 21
 indukčný
 krok 38
 predpoklad 38
 injektívnosť 144
 inverzná funkcia 145

inverzná relácia 127

J

jadro grafu 225
 Jarník Vojtěch (1897–1970) 196, 197
 Jarníkov (Primov) algoritmus 197
 jazyk 1. rádu 23
 jednotka
 imaginárna 16
 kvaternionová 16
 oktonionová 16

K

kartézsky súčin 19
 Kempe Alfred Bray (1849–1922) 48
 kód
 ASCII 204
 Huffmanov 80, 204, 206
 Prüferov 234
 koeficient
 binomický 171
 Newtonov, 171
 multinomický 177
 koleso (graf) 113
 komplementárna množina 14
 komponent súvislosti (grafu) 60
 konjunkcia ($\wedge$) 21
 kontradikcia 20
 koreň 77
 koreňový strom 77
 kostra grafu 62
 Kőnig Dénes (1884–1944) 48
 Kruskal Joseph B. (1928–2010) 196, 201
 Kruskalov algoritmus 202
 Kuratowski Kazimierz (1896–1980) 111
 kvantifikátor
 existenčný 23
 všeobecný 23

L

Laplace Pierre-Simon (1749–1827) 156
 lema 62
 les 77
 list 77
 logická
 hodnota 19
 premenná 19

logická	
spojka	19, 20
logický	
operátor	19
výrok	19
logika	
predikátová	23
výroková	22

M

matematická indukcia	37, 39
matica	
incidencie grafu	72
relácie	128
susednosti grafu	69
maximálne párovanie grafu	89
množina	11
charakteristická funkcia	149
kartézsky súčin množín	19
komplementárna	14
konečná	12
mohutnosť	12
nekonečná	12
podmnožina	12
potenčná	13
prázdna	11
rozklad	138
spočítateľná	37
systém množín	138
univerzálna	14
univerzum	13, 14
množiny	
disjunktné	13
prienik množín	13
rovnosť množín	11
rozdiel množín	13
symetrická diferencia množín	41
zjednotenie množín	12
mocninový rad	156
modulo (zvyšok po delení)	41
modulo $a \pmod{b}$	41
modus ponens	32
mohutnosť množiny	12
Moskovský papyrus	16
multinomická veta	177
multinomický koeficient	177

N

negácia ($\neg$)	20
Newton Isaac (1642–1727)	171
Newtonov binomický koeficient	171

P

P-kód (prefixový kód)	204
párovanie grafu	89
perfektné párovanie	89
podgraf grafu	58
podmnožina	
vlastná	12
postupnosť	
Fibonacciho	167
harmonická	166
potenčná množina	13
pravdivostná hodnota	19
pravdivostná tabuľka	20
prázdna množina	11
prázdny graf	80
prefixový kód	204
prehľadavací binárny strom	213, 214
prehľadávanie grafu	
do hĺbky	186, 187
do šírky	181, 182
prienik množín	13
Prim Robert Clay (1921–...)	197
princíp zapojenia-vypojenia	18
problém	
NP-úplný	96
obchodného cestujúceho	47, 234
štyroch farieb	48
Prüfer Ernst Paul Heinz (1896–1934)	241
Prüferov kód	234
prvky	
porovnateľné	137
neporovnateľné	137
prvotná formula	20
pseudokód	
Dijkstrovho algoritmu	231
hľadania kostry grafu	179
Jarníkovho algoritmu	197
konštrukcie očíslovaného stromu z Prüferovho kódu	241
konštrukcie optimálneho Huffmanovho kódu	206
konštrukcie prehľadávacieho binárneho stromu	215

konštrukcie Prüferovho kódu z očíslovaného stromu 235
 Kruskalovho algoritmu 202
 prehľadávania grafu do hĺbky 187
 prehľadávania grafu do šírky 182
 zostavovania identifikačného kódu binárneho stromu 219
 zostavovania identifikačného kódu koreňového stromu 222
 pytagorejci 15

R

rad
 formálny mocninový 156
 Maclaurinov 156
 mocninový 156
 Taylorov 156
 reflexívnosť (relácie) 124, 129
 relácia
 n -árna 123
 antisymetrická 125, 130
 binárna 123, 124
 čiasťočné usporiadanie 137
 ekvivalencie 140
 inverzná 127
 maticová reprezentácia 128
 na množine 124
 reflexívna 124, 129
 symetrická 125, 129
 tranzitívna 126
 zložená 128
 rovnosť množín 11
 rozdiel množín 13
 rozklad množiny 138
 triedy ekvivalencie 141
 triedy rozkladu 138

S

semifaktoriál 172
 skladanie funkcií 146
 skladanie relácií 128
 sled (v grafe) 54
 slučka (graf) 50
 spočítateľná množina 37
 Stirling James (1692–1770) 156
 strom (graf) 73
 vyvážený binárny 81
 subdivízia hrany 111

súčin
 kartézsky 19
 surjektívnosť 144
 sylogizmus 34
 symetrická diferencia množín (Δ) 41
 symetrickosť (relácie) 125, 129
 systém množín 138

T

tabuľka
 pravdivostná 20
 Tait Peter Guthrie (1831–1901) 48
 tautológia 20
 tautologicky ekvivalentné formuly 22
 tranzitívnosť (relácie) 126
 trieda
 rozkladu 138
 zvyšková 142
 trieda ekvivalencie 141

Ť

ťah (v grafe) 55

U

univerzum množín 13, 14
 usporiadaná dvojica 18
 usporiadanie
 čiasťočné 137
 neporovnateľnosť, 137
 porovnateľnosť, 137
 lineárne 138

Ú

úplný binárny strom 81

V

Vennove diagramy 16
 veta
 Cayleyho 242
 Eulerova o rovinných grafoch 110
 Kuratowského 112
 multinomická 177
 o centre stromu 224
 o cykloch 58
 o existencii cesty v grafe 56
 o existencii jadra grafu 226

veta	
o existencii kostry grafu	63
o explicitnom vyjadrení rekurentných postupností	170
o invariantnosti cyklu C_n	102
o invariantnosti stupňov vrcholov	101
o inverznej funkcii	145
o komponentoch grafu	61
o korektnosti prehľ. algoritmov	191
o matematickej indukcii	39
o matici susednosti	71
o matici zloženej relácie	131
o maticiach susednosti izomorfných grafov	100
o mohutnosti kartézskeho súčinu	19
o optimálnej lokalizácii v prehľadávacom binárnom strome	217
o otvorenom eulerovskom ťahu	87
o počte koncových vrcholov úplných binárnych stromov	81
o potenčnej množine	40
o relácii danej rozkladom množiny	139
o rozklade danom rel. ekvivalencie	141
o správnosti Jarníkovho algoritmu	199
o stromoch	76
o stupňoch vrcholov rovinného grafu	111
o súčte stupňov vrcholov grafu	52
o súvislosti výšky a počtu koncových vrcholov binárnych stromov	82
o tranzitívnosti relácie na množine	132
o uzavretom eulerovskom ťahu	86
o vrchoch stromov	76
pravidlo sylogizmu	34
základná algebry	16
základná aritmetiky	37
veta (matematická)	31
vrchol	
dieťa	78
koncový	50, 78
list	77
otec	78
počiatočný	50
potomok	78
predkovia	78
rodič	78
súrodenci	78
syn	78
vnútorný	78
výroková formula	20, 22

vytvárajúca funkcia	
exponenciálna	175
obyčajná	160
súčet	161
súčin	162
vyvážený binárny strom	81

W

Werner Benjamin	48
-----------------	----

Z

základná veta algebry	16
základná veta aritmetiky	37
zásobník	180
zjednotenie množín	12
zložená funkcia	146
zvyšková trieda	142
zvyšok po delení (modulo)	41