Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

ŠTÁTNY PEDAGOGICKÝ ÚSTAV
NATIONAL INSTITUTE FOR EDUCATION

Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

# Matematika pre učiteľov informatiky 2

Predmet: Matematika pre učiteľov informatiky

**Línia: Vlastný odborový kontext informatiky a informatickej výchovy**

Operačný program VZDELÁVANIE

EURÓPSKA ÚNIA
Európsky sociálny fond

Európska únia
Európsky sociálny fond

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je spolufinancovaný zo zdrojov ES

# Matematika pre učiteľov informatiky 2

## Identifikácia modulu

| | |
|---|---|
| **Aktivita projektu:** | 1.2 Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ |
| **Línia aktivity:** | Vlastný odborový kontext informatiky a informatickej výchovy |
| **Predmet:** | Matematika pre učiteľov informatiky 2 |

**Garant predmetu:**

RNDr. Katarína Bachratá, PhD., KIS FRI ZU, Žilina
bachrata@kis.fri.uniza.sk

**Autori:**

RNDr. Katarína Bachratá, PhD., KIS FRI ZU, Žilina
RNDr. Hynek Bachratý, PhD., KST FRI ZU, Žilina
Mgr. Peter Czimmermann, PhD., KMM FRI ZU, Žilina
Mgr. Juliana Šišková, KZVI FMFI Bratislava
RNDr. Michal Winczer, PhD., KZVI FMFI Bratislava, Bratislava

## Zaradenie modulu


Modul *Matematika pre učiteľov informatiky 2* je zaradený do vzdelávania v rámci aktivity 1.2, na začiatok druhého semestra. Modul slúži ako prerekvizita nasledujúcim informatickým a programátorským modulom, kde sa používa matematika. V tomto semestri sú to najmä moduly programovania a digitálnej gramotnosti. Ďalej modul slúži ako prerekvizita modulu *Matematika pre učiteľov informatiky 3*.

Modul má e-learningovú podporu

## Abstrakt modulu

V druhej časti predmetu *Matematika pre učiteľov informatiky* ukážeme niektoré matematické myšlienky, postupy a spôsoby uvažovania, ktorých úroveň pochopenia a osvojenia má významný dosah na prácu informatika. To, v ako presne a jasne definovaných pojmoch vie človek myslieť, ovplyvní jeho prácu ako programátora vytvárajúceho alebo ladiaceho algoritmus, ako analytika modelujúceho problémovú situáciu, ako človeka využívajúceho IK technológie, alebo ako informatika vedca, ktorý buduje niektorú z teoretických informatických disciplín. Vo väčšine prípadov pritom pôjde o spracovanie dát, z ktorých najpoužívanejšie sú asi stále tie číselné. V tomto module sú preto rozpracované dve témy, a to *teória čísel* a *logika*.

# Obsah


Matematika pre učiteľov informatiky 2 .......... 1
Identifikácia modulu .......... 1
Zaradenie modulu .......... 1
Abstrakt modulu .......... 1
Obsah .......... 2
Úvod .......... 3
Cieľ modulu .......... 3
Vstupné vedomosti .......... 5
Požadované prerekvizity .......... 5
Predpokladané vstupné vedomosti a zručnosti .......... 5
Preverenie vstupných vedomostí .......... 5
1. Ľahký úvod do teórie čísel .......... 6
1.1 Veľkosť čísla – počet bitov .......... 6
1.2 Čísla v počítači .......... 7
1.3 Delitele a násobky .......... 9
1.4 Zvyšok .......... 11
1.5 Modulárna aritmetika .......... 11
1.6 Prvočísla .......... 12
1.7 Algoritmy a problémy z teórie čísel .......... 15
2. Logika .......... 17
2.1 Jazyk, jeho funkcie, presný a vedecký jazyk .......... 17
2.2 Definície a axiómy .......... 22
2.3 Jednoduché a zložené tvrdenia .......... 25
2.4 Čo platí pre niekoho, pre nikoho a čo pre všetkých? .......... 29
2.5 Kto musí a kto potrebuje dokazovať? .......... 34
2.6 Logické spojky v informatike .......... 35
Čo sme sa naučili v tomto module .......... 39
Preverenie výstupných vedomostí .......... 39
Celkové hodnotenie predmetu .......... 39
Literatúra a použité zdroje .......... 39

# Úvod

V prvej časti predmetu *Matematika pre učiteľov informatiky* sme si zopakovali vedomosti na úrovni strednej školy. Venovali sme sa takým témam a oblastiam, ktorých výsledky a z nich odvodené pravidlá a vzorce sa objavia (alebo už objavili) v moduloch venovaných programovaniu. Naším cieľom však nebolo naučiť účastníkov vzdelávania nové vedomosti. Chceli sme ukázať a ponúknuť formy a metódy práce, ktorými je možné študentov základných a stredných škôl priviesť k tomu, aby sa prvoradou potrebou na hodinách matematiky nestalo zvládnutie postupu, vzorca, či algoritmu. Dôležitejším je podľa nás postoj študentov k duševnej práci, ich ochota riešiť problémy, či hrať sa s myslením. Preto boli v prvej časti tohto predmetu zaradené témy, ktoré nevyžadovali vedomosti a schopnosti prevyšujúce úroveň myslenia maturantov. Veríme, že rovnako ako niektorí poslucháči na školení, aj ich študenti sú schopní prekonať možno získanú nechuť k matematike a dokážu riešiť úlohy, ktoré sú vhodné pre ich matematický rozvoj.

Okrem pochopenia konkrétnych faktov a techník, bude hlavným prínosom tohto modulu možnosť prekonať v danej oblasti celú cestu od vytvorenia pojmov a vlastností na intuitívnej úrovni, cez manipuláciu s nimi, ich použitie vo výpočtoch a rôzne formulovaných úlohách, cez presnú formalizáciu až po využitie uvedených poznatkov v informatickej praxi.

Pokúsime sa poslucháčom ukázať nielen to, že logika a teória čísel sú veľmi dôležité pre informatiku, ale sú zaujímavé aj z historického hľadiska. Je fascinujúce sledovať cestu, akou sa poznatky objavené Grékmi (o ktorých vieme, že svoje úvahy písali do piesku a len objavy, ktoré považovali za hodnotné, zaznamenávali na drahý papyrus) prepracovali do dnešnej informatiky, kryptografie a mnohých ďalších oblastí. Zoznámenie sa s touto cestou je dôležité aj preto, že niekde na nej, v závislosti od veku a skúseností, sa nachádzajú aj študenti, ktorých učíme. Sme presvedčení, že úlohou učiteľov je robiť im na tejto ceste sprievodcov, a nie len kontrolórov na jej konci.

Naše školstvo vychádza z tradície vojenských škôl Rakúska-Uhorska. Jedným z viditeľných prejavov zachovaných z týchto škôl až do dnešných čias je zvyk podriadených vstať pri vstupe nadriadeného do miestnosti. *Je to pravda?*

# Cieľ modulu

Učiteľ má robiť študentovi spoločníka na ceste jeho objavovania. Na to musí sám zažiť radosť z vlastného objavu alebo z vytvoreného programu. Nemal by mať z vlastného vzdelávania skúsenosť, ktorá by ho presvedčila, že úlohou učiteľa je tréning, represia a kontrola. Doterajší spôsob výchovy budúcich učiteľov na našich vysokých školách, vychádzajúci z tradícií nášho regiónu, za vzdelávanie považuje skôr tvrdú a náročnú prácu a dril, než zábavu a tvorivú hru. Preto naši budúci učitelia základných a stredných škôl absolvujú kurzy matematickej analýzy, algebry, či teórie množín a formálnej logiky. Kurzy tak náročné, že v ich rámci sotva zvládnu pochopiť logické súvislosti medzi jednotlivými krokmi. Do priebehu vyučovania nie je v ich silách zasiahnuť. Na prednáškach pre študentov vedeckého zamerania je menší objem preberanej látky a možno aj trochu vyhranenejší záujem o daný odbor. Navyše títo študenti neštudujú dva obory ako budúci učitelia. Preto budúci vedci občas nájdu v prednáške chybu, či dokonca sa začnú priečiť s vyučujúcim. Študenti „vedci“ si z vysokej školy odnášajú informáciu, že je v ich silách podieľať sa na vymýšľaní. Študenti „pedagógovia“ majú pocit, že matematika spočíva v schopnosti pochopiť cudzie postupy a dôkazy, a potom sa naučiť ich predvádzať. „Vedci“ sa dokážu s matematikou hrať, vedia si ju užívať. „Pedagógovia“ sú tak zahltení rozsahom, ktorý majú naštudovať, že sa snažia byť efektívni a príliš sa nezdržovať hľadaním iných než vychodených cestičiek. To je napríklad dôvod, prečo sa paradoxne do dobrovoľníckej práce s talentovanými žiakmi zapájajú študenti „vedci“ a nie „pedagógovia“, ktorí sa pôvodne rozhodli venovať práci s deťmi aj profesionálne. Problémom je, že absolventi prichádzajú do školskej praxe nepripravení na svoju profesiu, nepoznajú súčasné osnovy a učebnice, podľa vyhlášok musia viesť hodinu podľa nachystaných príprav, ale skúste do učebného plánu naplánovať spontánne reakcie detí! Vojenský dril sa robil takto, ale už aj vojaci zistili, že to treba zmeniť.

Pán profesor Kolibiar zvykol rozprávať o prvákovi, ktorý mu skoro na každej prednáške z prvej rady oznámil, že na tabuli je „blbosť“. O tom študentovi rozprával rád.

Pán profesor Brunovský nám hovoril o študentovi, ktorý mu našiel v prednáške chybu. Štyri roky si ju študenti nevšimli, až teraz ju jeden objavil. Pán profesor sa nehanbil, neospravedlňoval za svoju chybu, nevyhováral sa, že má kopu papierovačiek a nemá čas sa poriadne pripraviť, vôbec sa neobával, že by sa jeho vedecká reputácia pošramotila, keď by svoj omyl prezradil iným matematikom. On bol len ľudsky rád, že má študenta, ktorý je taký múdry!

Začínajúci pedagóg musí byť naozaj kúzelník, aby dokázal vyhovieť všetkým požiadavkám a neurobil zo svojej práce otravnú rutinu. Krátkodobo sa ako jednoduchšia cesta v takejto situácii učiteľovi vidí ukázať deťom pár návodných úloh, vysvetliť na nich základné postupy a požadovať od detí, aby sa naučili naspamäť tvrdenia v rámčekoch. Niekedy začínajúci učiteľ ani netuší, že žiak, ktorý vie odrapkať všetky poučky zo žltých rámčekov, pamätá si násobilku a vie bezpečne použiť všetky algoritmy preberané v jeho ročníku, nemusí byť vôbec dobrý v matematike.

Z vyjazdených koľají sa vychádza ťažko. Chcieť od detí, aby chápali matematiku ako zábavnú zbierku hlavolamov, a nie nezmyselný dril o neznámych, nejasných, a tým aj vcelku zbytočných matematických objektoch, je veľmi ťažké. V tomto module by sme chceli ukázať, ako sa dá s matematikou hrať. Budeme sa venovať dvom témam, ktoré majú významný vplyv na prácu pri tvorbe modelov, algoritmov a programov, ako aj pri hľadaní motivačných úloh pre žiakov.


5+3/2

Vyskúšajte si to!

A čo Váš mobil? Používa vedeckú alebo štandardnú kalkulačku?

Častým omylom pri vyučovaní matematiky a zrejme aj iných vied je poskytnutie informácií v ich najpresnejšej, najčistejšej, definitívnej a bezchybnej forme. Študent má potom dojem, že všetko poznanie je už hotové a vybudované a nie je dôvod zamýšľať sa nad predkladanými faktami. Môže vzniknúť situácia, že študent, ktorý sa niektorý fakt naučil bez znalosti súvislostí, bez vymedzenia tvrdenia spomedzi viacerých nesprávnych alebo nepresných hypotéz, nie je schopný v prípade potreby dohodnúť sa na zmene pravidiel, neštandardnej definícii, či novom postupe. Pamätá si totiž, že *nulou sa deliť nesmie*, *od 5 zaokrúhľujeme nahor*, *násobenie má prednosť pred sčítaním* a *pri úprave rovníc píšeme neznámu vždy na ľavú stranu*. Netuší však, čo by sa stalo, keby sme nulou delili, že niekedy môže byť výhodnejšie zaokrúhľovať nadol, že ak do kalkulačky dáme príkaz 5+3/2, tak niekedy bude výsledok 6,5 (vedecká kalkulačka vo Windows) a niekedy 4 (štandardná kalkulačka vo Windows), že rovnaké riešenie rovnice dostaneme, aj keď necháme neznámu na pravej strane rovnice.

Pre vývoj kvalitného myslenia u detí je niekedy dôležitejšie tvoriť pojmy, ktoré spočiatku nebudú presné, hovoriť s nimi jednoduchším jazykom a ukázať, prečo je niekedy vhodné veci formalizovať až neskôr. Keď svoje dôvody nevieme vysvetliť ich jazykom, na úrovni ich potrieb, skúseností a pochopenia, nebudú deti o nič múdrejšie, ak sa naučia memorovať slová, ktorým nerozumejú. S kolegami, ktorí sa dôsledne, ale iba formálne, nekriticky a bez porozumenia naučili niektoré pravidlá, sa ťažko dohodneme na ich zmene. Budú argumentovať, že by sme žiakov zbytočne poplietli. Že deťom treba vysvetliť veci čo najpresnejšie a jediným spôsobom, aby si ich dobre zapamätali a mohli používať. Predstava, že pravidlá musia byť presné, aby deti nerobili chyby, vedie k umelým, neživým tvrdeniam, ktoré sú síce formálne presné, ale s ktorými žiak nemôže urobiť nič iné, iba sa ich naučiť.

Učitelia informatiky asi najviac spomedzi všetkých učiteľov musia čeliť zmenám vo svojom predmete. Veríme preto, že ich ochota meniť zaužívané a naučené postupy bude väčšia ako u učiteľov iných predmetov. Majú výhodu, že sú na neustále pokusy a omyly trénovaní. A tak ako sa žiadne dieťa nenaučilo chodiť bez toho, aby pri tom učení veľakrát spadlo, tak ako sa žiadna vedná disciplína nevybudovala bez teórií, ktoré sa neskôr ukázali nesprávne, tak ani vývoj myslenia jedného človeka nemôže preskočiť pády, omyly a naprávanie vlastných chýb. Bez nich sa môže vyvinúť iba ploché uvažovanie, ktoré bez výhrad akceptuje autority a ich výsledky. A také (poslušné a podriadené) by nemalo byť myslenie, aké chceme u našich detí vychovávať. Ukážeme poslucháčom, ako pripravovať problémy, ako sa nebáť robiť chyby pri ich riešení a ako na základe predošlých chýb hľadať lepšie riešenia. Chceli by sme poslucháčov presvedčiť, že aj matematika na elementárnej úrovni môže mať veľa slabých miest, ktoré by sme pred študentmi nemali skrývať, ale skôr na ne poukázať a inšpirovať sa nimi k hlbším úvahám.

V časti o *teórii čísel* poslucháčom okrem základných poznatkov priblížime aj zaujímavé aplikácie v informatike. Je to zároveň príležitosť poukázať na dôležitosť základného výskumu, pretože pojmy ako prvočíslo, deliteľ a ďalšie, ktoré boli bez zjavných aplikácií objavené a skúmané už v staroveku nachádzajú dôležité uplatnenie po tisíckach rokov v informatike. Navyše sú to pojmy, ktorých osvojenie si nevyžaduje náročné a zdĺhavé štúdium. Taktiež sa pozrieme trochu detailnejšie na reprezentáciu celých čísel v počítači. Zameriame sa na najtypickejšie reprezentácie, ktoré sa používajú, a ukážeme, aké obmedzenia ich používanie prináša a aké sú pri tom možné chyby. Koľko miesta v pamäti potrebujeme na uloženie čísla? Ako súvisí nevyhnutne potrebné miesto s veľkosťou čísla, ktoré si chceme zapamätať? Sú v počítači zapamätané len celé čísla? Ako je to s reálnymi číslami? Niečo sme naznačili už v závere predchádzajúcej časti, teraz si všimneme „reálne" čísla detailnejšie. Na aké problémy môžeme natrafiť pri ich používaní?

Časť *logika* obsahuje niekoľko tém, ktorých úlohou je vyprovokovať poslucháčov k polemike a ku kultivovaniu svojho vyjadrovania. Ukážeme rôzne úrovne argumentácie a vysvetlíme, prečo sú dobre vedené slovné súboje pre rozvoj logického myslenia nepostrádateľné. Problémom súčasnej didaktiky je totiž predpoklad, že naučíme študentov používať logické spojky, keď ich pomenujeme, presne zadefinujeme a naučíme študentov, ako zostavovať a vypĺňať tabuľky pravdivostných hodnôt pomocou nich vytvorených výrokov. Ale človeku, ktorý zložitý zložený výrok sám nikdy nevytvoril alebo nepotreboval analyzovať, je takýto poznatok nanič. Bude si myslieť, že vypĺňanie tabuliek je dôležitejšie, ako zmysluplné a presné používanie takýchto výrokov tam, kde je to ozaj potrebné. Učiteľ s týmto presvedčením bude namiesto kultivovania jazyka, vyjadrovania a myslenia v diskusiách učiť vypĺňanie tabuliek. Žiaci sa určite o logických spojkách dozvedia viac, keď budú potrebovať analyzovať napínavú a zložitú situáciu, než keď budú vypisovať 0 a 1. Podobnú chybu vo vyučovaní robíme neskôr, keď predpokladáme, že naučíme študentov robiť dôkazy, ak pomenujeme spôsoby dokazovania a roztriedime ich do skupín. Pokiaľ študent predtým sám žiadny dôkaz neurobil, ani nepocítil jeho potrebu, bude si myslieť, že triedenie dôkazov (na priamy, nepriamy, sporom, konštruktívny dôkaz, dôkaz indukciou) je dôležitejšie, než dokazovanie samotné. Žiaci sa naučia viac, keď budú mať rozhodnúť, ktorá z troch odlišných úvah je správna, než keď budú zaraďovať dôkaz do príslušnej skupiny. Pre úplnosť ešte treba pripomenúť, že v okamihoch „vymýšľania" matematiky nie je presnosť tým najdôležitejším nástrojom. Predstavy matematika sú v týchto momentoch niekedy viac umelecké ako exaktné. Podobne komunikácia viacerých matematikov pri riešení spoločného problému je často veľmi expresívna. Spresnenie takto vznikajúcich nápadov prichádza vtedy, keď sa chceme ubezpečiť o ich správnosti a sprístupniť ich ďalším záujemcom. To, že matematici vo svojich knihách a článkoch vynechávajú opis cesty k objavu a obmedzia sa len na formálny zápis dosiahnutých výsledkov, je ich zvykom a možno až zlozvykom.

Aj keď sa diskutujúci na konci dohodnú na nesprávnom riešení, je to pre rozvoj ich myslenia lepšie, než keď sa iba naučia správne riešenie.

# Vstupné vedomosti

## Požadované prerekvizity

Účastník vzdelávania má mať absolvovaný modul *Matematika pre učiteľov informatiky 1*. Účastník dokáže otvoriť, vypracovať a odovzdať zadanie v LMS Moodle a dokáže spolupracovať na riešení úlohy aspoň s jedným kolegom.

## Predpokladané vstupné vedomosti a zručnosti

Účastník vzdelávania sa nezľakne neznámeho zadania. Dokáže analyzovať problém a pozrieť sa na zadanie z viacerých uhlov pohľadu. V prípade potreby dokáže formulovať zadanie tak, aby mu rozumel matematik a mohol mu pomôcť. Spolupráca pri riešení problémov nie je podvádzanie, ale jedna z pracovných metód.

## Preverenie vstupných vedomostí

Súťaž skupín v riešení úloh, ktorých zadania budú k dispozícii na internete pred začiatkom školení.

# 1. Ľahký úvod do teórie čísel

Už sme sa zoznámili s číselnými sústavami, ktoré sa používajú v súvislosti s počítačmi. Zopakovali sme si základné aritmetické operácie s celými číslami v desiatkovej sústave a poukázali sme na ich podobnosť s operáciami v dvojkovej sústave. Operácia odčítania nás prinútila zamyslieť sa nad reprezentáciou záporných čísel. V tejto časti sa budeme zaoberať tým, koľko miesta (akú veľkú pamäť) potrebujeme na zapamätanie si čísla veľkosti $n$. Ako sú v počítači reprezentované reálne čísla a čo z toho vyplýva pre presnosť aritmetických operácií.

## 1.1 Veľkosť čísla – počet bitov

Koľko miesta v pamäti potrebujeme na uloženie čísla? Ako súvisí nevyhnutne potrebné miesto s veľkosťou čísla a číselnou sústavou, v ktorej si ho chceme zapamätať?

| **Zadanie 1** | Zopakujte si zápis celých čísiel v číselných sústavách s rôznym základom. 1) V dvojkovej sústave zapíšte dnešný deň, rok. 2) Prepíšte výsledok z bodu 1) do osmičkovej a šestnástkovej sústavy. 3) Zapíšte čísla z bodu 1) v trojkovej a jedenástkovej sústave. |
|---|---|

Všetci máme nejaké skúsenosti zo zápisom čísiel v desiatkovej sústave. Nevyhnutne potrebné miesto je vlastne počet cifier na zápis čísla. Pokúsme sa zistiť, ako závisí počet cifier čísla $n$ (chápeme ho v desiatkovej sústave), keď ho chceme zapísať v sústave so základom $b$. Skúsme najprv užitočný a overený spôsob: *„začni s malými hodnotami $b$, napr. $0,1,2, \ldots$ a uvidíš, či sa ukáže niečo zaujímavé a výsledky sa budú dať zovšeobecniť“*.

Číslo $n$ v sústave so základom $b$ zapisujeme $(n)_b$

Toto sa asi oplatí zapamätať a skúsiť použiť aj v iných situáciách.

V našom prípade zoberieme ako najmenšiu hodnotu $b = 1$. Podľa našej definície pozičnej sústavy to síce nie je celkom korektné, lebo by malo byť $b > 1$. Tento prípad budeme chápať ako jednotkovú sústavu. Zapíšme napríklad číslo $(7)_{10} = (|||||||)_1$. Každý vidí, že dĺžka zápisu je priamo úmerná veľkosti čísla, pre číslo $n$ je dĺžka zápisu $n$.

Jednoducho „paličkový“ zápis, skoro ako v krčme.

Skúsme teraz $b = 2$. Teda dvojkovú sústavu. Opäť použijeme techniku „začni s malými hodnotami“. Ako vidíme z tabuľky na okraji, dĺžka zápisu čísla $n$ rastie s veľkosťou čísla $n$. Tiež vidíme, že tento nárast je pomalší než lineárny, ako bol pri jednotkovej sústave. Skúsme si zobrať na pomoc spôsob zápisu, aký sme používali v minulej časti. Zoberme napríklad číslo $45$:

Hovoríme, že $y$ rastie vzhľadom na $x$ lineárne, keď platí, že $y = kx + q$, pre nejaké $k, q \in \mathbb{R}$.

| $n$ | binárne |
|---|---|
| $1$ | $1$ |
| $2$ | $10$ |
| $3$ | $11$ |
| $4$ | $100$ |
| $\ldots$ | |
| $2010$ | $11111011010$ |
| $\ldots$ | |

| | | | | | |
|---|---|---|---|---|---|
| $1$ | $0$ | $1$ | $1$ | $0$ | $1$ |
| $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |

Keď číslo $45$ vidíme rozpísané ako súčet mocnín základu, v tomto prípade dvojky, ľahko si všimneme, že číslo má približne toľko cifier, koľko je najväčšia mocnina základu v ňom obsiahnutá. Približne preto, lebo mocniny sú „číslované“ od $0$, a teda je to o jedna viac. Ako zistíme maximálnu mocninu základu obsiahnutú v nejakom čísle? Na to máme predsa funkciu logaritmus. Napríklad, $\log_2 45 \cong 5.4918 \ldots$. Maximálna mocnina je celá časť tejto hodnoty, presnejšie dolná celá časť, označujeme ju $\lfloor \ \rfloor$. Teda pre číslo $45$, potrebujeme v dvojkovej sústave $\lfloor \log_2 45 \rfloor + 1 = 6$ cifier. Vo všeobecnosti číslo $n$ zapíšeme v dvojkovej sústave $\lfloor \log_2 n \rfloor + 1$ ciframi.

$\log_b y = x$ práve vtedy, keď $b^x = y$

Funguje to aj v desiatkovej sústave? Vyskúšajte si to! Samozrejme, že to funguje. Nikde sme špeciálne nevyužívali, že základ sústavy je $2$ alebo, že číslo, ktoré chceme zapísať, je $45$. Boli to len príklady, takže nie je žiaden dôvod, aby rovnaký postup nefungoval aj s inou sústavou. Pokojne môžeme dvojku v základe nahradiť za $10$. Zistíme, že $\lfloor \log_{10} 45 \rfloor + 1 = 2$. A naozaj, na zápis čísla $45$ v desiatkovej sústave potrebujeme $2$ cifry. Vo všeobecnosti môžeme použiť číslo $n$, na jeho zápis v sústave so základom $b$ potrebujeme $\lfloor \log_b n \rfloor + 1$ cifier.

Niekedy je užitočný aj iný postup, ako skúšať malé prípady. V niektorých situáciách je šikovné úlohu najprv zovšeobecniť, vyriešiť ju všeobecne a na záver dosadiť do všeobecného riešenia hodnotu, ktorá nás zaujíma. Tento postup je však pokročilejší.

| | |
|---|---|
| **Zadanie 2** | Napíšte program, ktorý nájde a) všetky $5$-ciferné čísla, ktorých ciferný súčet je deliteľný $13$; b) všetky štvorciferné štvorce, ktorých prvé dve cifry a aj druhé dve cifry sa rovnajú; c) všetky šesťciferné čísla, ktorých ciferný súčet cifier na párnych pozíciách bude väčší než ciferný súčet cifier na nepárnych pozíciách. |
| **Zadanie 3** | Využitím vzťahu $log\,x + log\,y = log\,xy$, skúste zistiť koľko cifier má v desiatkovej sústave $10!$. Vedeli by ste napísať program, ktorý zistí koľko cifier má v desiatkovej sústave $n!$? |
| **Zadanie 4** | V desiatkovej sústave navrhnite postup sčítania čísiel s „veľa“ ciframi. Vedeli by ste navrhnúť aj postup pre násobenie? |
| **Zadanie 5** | Vedeli by ste odhadnúť koľko operácií s jednocifernými číslami musíme vykonať, keď chceme sčítať $c$-ciferné s $d$-ciferným číslom? A koľko operácií by to bolo pri ich vynásobení? |
| **Zadanie 6** | (Náročné) Ako sa zmení riešenie zadania 4 a 5, ak by sme chceli reprezentovať čísla v inej ako desiatkovej sústave? Skúste dvojkovú. Vyskúšajte aj sústavu so základom $256$, resp. $2^{16}$. |

Pomôcka:
$log_b\, x = log_a\, x / log_a\, b$

Toto sú, ak sa nemýlime, cvičenia na vymyslenie celočíselnej aritmetiky veľkých čísiel, ale to je predsa dosť ťažké, však? Alebo nie je? Ak máte chuť, naprogramujte si to, je to celkom krátky program na pár desiatok riadkov.

## 1.2 Čísla v počítači

V tejto časti sa ešte raz pozrieme na reprezentáciu celých čísiel v dvojkovej sústave. Zameriame sa na najtypickejšie reprezentácie, Byte, Word, Integer. V počítači si pamätáme aj reálne čísla. Uvedieme, ako ich reprezentujeme. Nebudeme zachádzať do technických detailov, skôr nám pôjde o ozrejmenie princípov, na základe ktorých pochopíme limity narábania s číslami a potenciálne zdroje chýb. Podrobnosti záujemca môže nájsť napr. v [14].

Príklady rozsahov niektorých celočíselných typov

| typ | počet bitov | hodnoty |
|---|---|---|
| Byte | 8 | 0 až 255 |
| Word | 16 | 0 až 65535 |
| Shortint | 8 | -128 až 127 |
| Integer | 32 | -2147483648 2147483647 |

Asi najdôležitejšie je uvedomiť si, že nech používame na zapamätanie si celých čísiel premenné ktoréhokoľvek základného typu, napr. Byte, Word, Integer a pod., vždy ide o reprezentáciu, ktorá má na uloženie čísla vyhradený určitý fixný priestor. Inak povedané v premennej toho-ktorého typu môžu byť uložené iba hodnoty z istého intervalu. Z toho vyplýva, že keď chceme do premennej napr. typu Byte uložiť číslo väčšie, než je jej rozsah, mala by nastať chyba. To, čo sa ozaj stane, však závisí od konkrétnych nastavení v danom programovacom jazyku, jednoznačná odpoveď nie je. Operácie s celými číslami sa dajú totiž v princípe vykonať vždy, ale záleží na tom, ako interpretujeme (alebo sa v danom programovacom jazyku interpretujú) výsledky.

Napríklad hodnota $255$ je v premennej Byte reprezentovaná $(11111111)_2$. Keď k nej pripočítame $1$ dostaneme výsledok $0$ a nie $256$, ako by sme možno očakávali. Ešte kurióznejšia situácia nastane, keď je v premennej typu Byte uložená hodnota $127$, reprezentovaná ako $(01111111)_2$. Ak k nej pripočítame $1$, dostaneme hodnotu $128$, reprezentovanú ako $(10000000)_2$. Tú ak interpretujeme ako hodnotu Shortint, dostaneme $-128$. Takže v programovacom jazyku treba dávať pozor, akého typu sú jednotlivé premenné, lebo hoci môžu byť v premenných zapísané identické hodnoty, môžu sa podľa typu premennej interpretovať rôzne. Najčastejšie chyby vznikajú, keď sa miešajú premenné tzv. neznamienkových (obsahujú len nezáporné hodnoty) a znamienkových (obsahujú aj kladné aj záporné hodnoty) typov.

Tzv. *signed* a *unsigned* typy.

V neznamienkových typoch je to vlastne aritmetika modulo príslušná mocnina dvojky ($2^8$, $2^{16}$, a pod.)

Rovnako nepríjemná situácia môže nastať, keď chceme priradiť hodnotu premennej typu Word do premennej typu Byte. Teda hodnotu premennej s väčším rozsahom do premennej s menším rozsahom. To sa v princípe tiež dá urobiť vždy, a preto nesmieme byť prekvapení, ak sa namiesto chybového hlásenia operácia vykoná. Ale čo sa vlastne stane? Môžu nastať rôzne situácie, ale najčastejšie je, že do premennej s menším rozsahom sa prenesie len časť z premennej s väčším rozsahom. Napríklad premennú X typu Word s hodnotou $(\mathrm{ABCD})_{16}$ priradíme do premennej typu Byte a jej hodnota bude len „dolná časť" premennej X, t.j. $(CD)_{16}$.

Ešte si pamätáte šestnástkovú sústavu?

Situácia s reprezentáciou reálnych čísiel v počítači je o čosi zložitejšia. Priblížime si, pomocou desiatkovej sústavy, ako sa v počítači chápu „reálne" čísla. Nazývame tak čísla v tvare $m \cdot 10^e$, $m$ sa nazýva mantisa a $e$ exponent. Graficky sa to dá znázorniť takto:

| znamienko | Mantisa | exponent |
|---|---|---|
| + | 12345678901234567890 | 13 |

Takto by bolo reprezentované, číslo $123456789012345678900000000000000.0$. Vidíme, že to nie je nič iné, iba posunutie desatinnej čiarky o $e$ miest doprava. V praxi sa používa $0 \leq m < 1$, takže desatinná čiarka je vždy pred prvou cifrou mantisy. Všimnite si, že mantisa má vždy nejaký pevný počet cifier, čo znamená, že takto reprezentované číslo nemôže mať viac platných nenulových cifier. Nemá zmysel, aby mantisa začínala nulami, vždy vieme upraviť exponent (posunúť desatinnú čiarku) tak, aby bola prvá cifra nenulová. Napríklad $0{,}00123 \cdot 10^5 = 0{,}123 \cdot 10^3$, $123{,}456 \cdot 10^{-5} = 0{,}123456 \cdot 10^{-2}$. Úprava čísla do takéhoto tvaru sa nazýva *normalizácia*. Keď sa chvíľu zamyslíme nad tým, ako sa dajú robiť základné aritmetické operácie s takto reprezentovanými číslami, ihneď prídeme na potenciálne ťažkosti.

V našom príklade bola mantisa celé číslo, takže vynásobenie s $10^{13}$ bolo len pripísanie 13 núl.

To vlastne znamená, že to vôbec nie sú všetky reálne čísla, aké poznáme z matematiky, dokonca to nie sú ani všetky racionálne čísla! Vlastne to nie je až také prekvapujúce. Keď čísla reprezentujeme len veľmi obmedzenou pamäťou, tak nemôžeme očakávať, že budeme vedieť reprezentovať nekonečne veľa hodnôt.

**Zadanie 7**

Rozmyslite si, ako sa násobia a delia čísla zapísané v tvare $m \cdot 10^e$, kde $0 \leq m < 1$ a $e$ je z nejakého intervalu, napríklad $-128$ až $127$.

Ak ste vyriešili zadanie 7, určite Vám nerobí problém vymyslieť, ako by sa realizovalo sčítanie a odčítanie čísiel v uvedenom tvare. Označme si čísla $X$ a $Y$. Nech je $X = m \cdot 10^e$ a $Y = n \cdot 10^f$, sčítať resp. odčítať ich vieme len v prípade, keď $e = f$. Ak $e \neq f$, musíme upraviť buď $e$, alebo $f$ tak, aby boli rovnaké. Predpokladajme, že $e < f$, Upravíme menšie číslo, teda $X$ takto:

$$X = m \cdot 10^e = m \cdot 10^e \cdot 10^{f-e} \cdot 10^{e-f} = m \cdot 10^f \cdot 10^{e-f} = (m \cdot 10^{e-f}) \cdot 10^f.$$

Vidíme, že mantisu $X$ musíme vynásobiť $10^{e-f}$. Kedže $e - f < 0$, znamená to, že $m$ musíme posunúť doprava o $e - f$ miest, alebo napísať pred $m$ $e - f$ núl. Ale $m$ má pevný počet miest, takže pri tejto operácii môžeme nenávratne prísť o platné cifry $m$, a teda aj čísla $X$. Inak povedané, strácame presnosť čísla $X$. Teraz môžeme konečne $X$ a $Y$ sčítať alebo odčítať, napr.:

Urobte si samostatne všetky úpravy!

Posun $m$ o jedno miesto doprava, zodpovedá posunu desatinnej čiarky v čísle $X$ o jedno miesto doľava.

$$X + Y = m \cdot 10^e + n \cdot 10^f = (m \cdot 10^{e-f}) \cdot 10^f + n \cdot 10^f = (m \cdot 10^{e-f} + n) \cdot 10^f$$

Aha! Preto treba sčitovať a odčitovať približne rovnako veľké čísla, a nikdy nie také dve, ktoré sa veľkosťou veľmi líšia, lebo inak sa nám môžu strácať cifry, čím klesá aj presnosť výsledku.

Doteraz sme sa venovali zápisu „reálnych“ čísiel v desiatkovej sústave. Nič nám však nebráni nahradiť základ $10$ v uvedených zápisoch všade za základ $2$. Pri použití dvojkovej sústavy reprezentujeme znamienko napr. takto: $0$ bude $+$ a $1$ bude $-$. Mantisa bude mať určitý počet bitov (cifier v dvojkovej sústave) a exponent bude celé číslo v dvojkovej sústave.

V praxi používané reálne čísla majú takúto veľkosť mantisy a exponentu (v bitoch):

| mantisa | exponent |
|---|---|
| 23 | 8 |
| 52 | 11 |

**Zadanie 8**

Napíšte program na sčítanie prvých $n$ členov *harmonického radu*: $H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. Skúste sčítať zlomky $\frac{1}{j}$, pre $j$ od $1$ po $n$ a pre $j$ od $n$ po $1$. Vypíšte a porovnajte výsledky pre $n =$ $100$, $10000$, $1000000$.

Používanie reálnych čísiel v sebe skrýva mnohé nástrahy. Uvedieme pár z nich. Porovnávanie dvoch reálnych čísiel na rovnosť je asi najbežnejšia z nich. Prvá nástraha je neporovnávanie dvoch reálnych hodnôt testom $=$. Rovnosť dvoch reálnych čísiel sa vždy testuje len približne. V prípade, že chceme porovnať, či sa $X$ rovná $Y$, musíme to zapísať $\mathrm{abs}(X - Y) < \varepsilon$, kde $\varepsilon$ je nami zvolená presnosť, napríklad $10^{-6}$. Ďalšia nástraha je zaokrúhľovanie. Jeho dôsledkom je, že v počítačovej aritmetike nemusí vždy platiť komutatívny zákon, teda $X + Y$ sa nemusí rovnať $Y + X$.

Pravidlá pre prácu s reálnymi číslami:

Neporovnávajte dve reálne hodnoty testom = !

Dávajte pozor, aby nenastali chyby zaokrúhľovaním!

**Zadanie 9**

(Náročné) V zvolenej presnosti reálnych čísiel si napíšte dve po sebe idúce reálne čísla v dvojkovej sústave. Aká je ich hodnota v desiatkovej sústave? Aký je ich rozdiel? Skúste viac takýchto po sebe idúcich dvojíc.

## 1.3 Delitele a násobky

V tejto časti, ktorá je určená predovšetkým pre nematematikov, si povieme niečo o násobkoch a deliteľoch prirodzených čísel. Čitatelia zbehlejší v matematike môžu začať až najväčším spoločným deliteľom - zadaním 4.

### Deliteľ a násobok prirodzeného čísla

Začnime jednoduchou úlohou, pred ktorú bol postavený nejeden rodič. Koľko hrušiek (jahôd, sliviek alebo iného ovocia) potrebujeme, aby sme ich vedeli rozdeliť medzi $3$ deti (ale počet detí by mohol byť aj iný, preto ho budeme neskôr označovať všeobecnejšie písmenom $k$) tak, aby každé dieťa dostalo rovnaký počet kusov ovocia? Je jasné, že počet kusov ovocia môže byť $0$ (tá sa obzvlášť dobre delí a nestojí to peniaze), $3$, $6$, $9$, $12$, atď. Tieto čísla sú násobkami čísla $3$. Pozrime sa na to všeobecnejšie. Prirodzené číslo $n$ je násobkom čísla $3$, ak existuje také prirodzené číslo (označme ho $q$), že $n$ môžeme napísať ako súčin čísel $3$ a $q$. Čiže $n = 3 \cdot q$. Násobky čísla $3$ sú teda čísla, ktoré môžeme zapísať ako súčin $3$ a prirodzeného čísla. Napríklad $3 \cdot 1$, $3 \cdot 2$, $3 \cdot 3$, atď. (ak by sme pracovali s množinou celých čísel, môžeme zvoliť samozrejme aj záporné násobky, napríklad $3 \cdot (-1)$, $3 \cdot (-2)$ a iné). Miesto čísla $3$ zvoľme prirodzené číslo $k$. Násobky čísla $k$ dostaneme tak, že toto číslo násobíme číslami $1$, $2$, $3$ a ďalšími. Všeobecne môžeme povedať, že prirodzené číslo $n$ je násobkom čísla $k$, ak existuje prirodzené číslo $q$ také, že $n = k \cdot q$.

Až po koniec tejto kapitoly budeme pracovať s prirodzenými číslami a občas si požičiame $0$ (ktorú podľa dohody nepovažujeme za prirodzené číslo).

Položme si teraz otázku, ktorá síce znie podobne ako predchádzajúca, ale je trochu absurdnejšia. Máme $24$ jabĺk. Koľko detí potrebujeme, aby sme im vedeli tie jablká rozdeliť spravodlivo? Je jasné, že počet detí môže byť $1$, $2$, $3$, $4$, $6$, $8$, $12$, $24$. Hľadáme delitele čísla $24$. Napríklad, ak delíme jablká trom deťom, tak každé by malo dostať práve osem a teda číslo $3$ je deliteľom $24$, pretože existuje celé číslo $q$ (v tomto prípade $q = 8$) také, že $24 = 3 \cdot q$. Všeobecne hovoríme, že celé číslo $k$ je deliteľom celého čísla $n$, ak existuje celé číslo $q$ také, že $n = k \cdot q$.

## Najmenší spoločný násobok

Začnime príkladom zo základnej školy. Sčítajme zlomky $\frac{3}{4}$ a $\frac{5}{6}$. Musíme ich oba rozšíriť tak, aby mali spoločného menovateľa. Je ľahké zistiť, že spoločný menovateľ musí byť násobkom trojky aj štvorky. Hľadáme teda spoločný násobok čísel $3$ a $4$. Sú to čísla $12$, $24$, $36$, atď. Najmenší spoločný násobok čísel $3$ a $4$ je najmenšie z týchto čísel, čiže $12$. Číslo $n$ je spoločným násobkom čísel $a$, $b$, ak je násobkom $a$ aj $b$. Číslo $a \cdot b$ je vždy spoločným násobkom čísel $a$, $b$. Každé dve prirodzené čísla teda majú spoločný násobok. Najmenší spomedzi spoločných násobkov sa nazýva najmenší spoločný násobok – označíme ho nsn$(a, b)$. Z príkladu v úvode vidíme, že nsn$(4,6) = 12$, a teda $\frac{3}{4} + \frac{5}{6} = \frac{9}{12} + \frac{10}{12} = \frac{19}{12}$.

Takto to v matematike funguje často. Ak nevieme odpovedať na nejakú otázku, hľadáme prepojenia na iné matematické oblasti a pojmy, ktoré by nám to umožnili.

| | |
|---|---|
| **Zadanie 1** | Najmenší spoločný násobok dvoch čísel je buď rovný ich súčinu, alebo je menší ako ich súčin. Vedeli by ste povedať, kedy nastáva ktorá situácia? |
| **Návod 1** | Ak neviete na otázku zatiaľ odpovedať, čítajte ďalej, o chvíľu narazíte na pojmy, ktoré vám pomôžu odpovedať na ňu. |
| **Zadanie 2** | Navrhnite postup na hľadanie najmenšieho spoločného násobku dvoch prirodzených čísel.<br><br>Skúste tento postup rozšíriť na hľadanie najmenšieho spoločného násobku troch, respektíve štyroch prirodzených čísel. |
| **Návod 2** | Hľadáme najmenší spoločný násobok čísel $a,b$. Najjednoduchší postup je taký, že vypisujeme násobky čísla $a$: $a, 2a, 3a, \cdots, ba$ a násobky čísla $b$: $b, 2b, 3b, \cdots, ab$. Nájdeme najmenšie spoločné číslo z tohto zoznamu. To musí byť najmenší spoločný násobok. |

## Najväčší spoločný deliteľ

Delitele čísla $20$ sú čísla $1$, $2$, $4$, $5$, $10$, $20$ a delitele čísla $24$ sú $1$, $2$, $3$, $4$, $6$, $8$, $12$, $24$. Čísla $20$ a $24$ majú tri spoločné delitele: $1$, $2$, $4$. Ak máme dve prirodzené čísla $a, b$, tak číslo $k$ je ich spoločným deliteľom, ak $k$ delí $a$ aj $b$. Jednotka je deliteľom každého prirodzeného čísla, takže každé dve prirodzené čísla majú aspoň jedného spoločného deliteľa. Najväčšie číslo spomedzi spoločných deliteľov čísel $a, b$ sa nazýva najväčší spoločný deliteľ – budeme ho označovať NSD$(a, b)$. V prípade čísel $20$ a $24$ vidíme, že NSD$(20,24) = 4$. Existujú dvojice čísel, napríklad $4$ a $9$, ktoré majú len jedného spoločného deliteľa, čiže NSD$(4,9) = 1$. Takéto čísla nazývame nesúdeliteľné.

| | |
|---|---|
| **Zadanie 3** | V zadaní 1 sme sa pýtali, kedy je najmenší spoločný násobok dvoch čísel rovný ich súčinu a kedy je menší ako ich súčin. Ak ste vtedy nevedeli na túto otázku zodpovedať, pokúste sa o to teraz – už by ste mali mať všetko, čo potrebujete na jej zodpovedanie. |
| **Návod 3** | Najmenší spoločný násobok čísel $a, b$ je rovný súčinu $a \cdot b$ práve vtedy, keď sú tieto čísla nesúdeliteľné. |

| **Zadanie 4** | Navrhnite postup na hľadanie najväčšieho spoločného deliteľa dvoch prirodzených čísel.<br><br>V dostupnej literatúre, alebo na internete nájdite informácie o Euklidovom algoritme na hľadanie najväčšieho spoločného deliteľa a porovnajte ho s vaším postupom. Testovaním na niektorých dvojiciach prirodzených čísel zistite, ktorý postup vyžaduje pri týchto dvojiciach viac aritmetických operácií! |
|---|---|
| **Návod 4** | Na začiatku tejto časti je uvedený jednoduchý postup. |

## 1.4 Zvyšok

Vráťme sa k úlohe z úvodu o hruškách. Ak chceme rozdeliť napríklad $14$ hrušiek trom deťom, nie je to možné urobiť tak, aby sme im dali všetky hrušky a každé dieťa dostalo rovnako. Väčšina „rozdeľovačov“ ovocia postupuje tak, že nájde násobok trojky, ktorý je menší ako $14$ a rozdelí tento počet hrušiek. Zostávajúce hrušky (teda zvyšok) väčšina „rozdeľovačov“ zje. Asi ťažko nájdeme niekoho, kto by deťom nedoprial a pri delení si väčšina z nás dáva ešte podmienku, že počet hrušiek, ktoré zostanú nám po rozdelení musí byť menší, ako počet, ktorý sme dali každému z detí (v najhoršom prípade nám nič nezostane). Nie je ťažké zistiť, že pri tejto dodatočnej podmienke existuje len jeden spôsob delenia hrušiek: deťom rozdelíme $12$ hrušiek, každé dieťa dostane štyri hrušky a nám zostane zvyšok – dve hrušky. Čo môžeme formálne zapísať $14 = 3 \cdot 4 + 2$. Číslo $2$ predstavuje zvyšok po delení čísla $14$ číslom $3$.

Tento fakt môžeme zovšeobecniť a každé prirodzené číslo $n$ môžeme jediným spôsobom napísať v tvare $n = 3 \cdot q + r$, kde $q$ je vhodné prirodzené číslo alebo nula a $r$ môže nadobudnúť niektorú z hodnôt $0$, $1$, $2$. Číslo $r$ nazývame zvyšok.

Tieto úvahy môžeme ďalej zovšeobecniť, ak miesto čísla $3$ vezmeme ľubovoľné prirodzené číslo $k$. Pre každé prirodzené číslo $n$ existuje práve jedna dvojica čísel $q$,$r$ taká, že $q$ je prirodzené číslo alebo nula, číslo $r$ (nazvané zvyšok) nadobúda niektorú z hodnôt $0,\ 1,\ \dots,\ k-1$ a platí rovnosť $n = k \cdot q + r$. Uveďme niekoľko príkladov: nech $k = 5$, potom $7 = 5 \cdot 1 + 2$, $23 = 5 \cdot 4 + 3$, $4 = 5 \cdot 0 + 4$.

## 1.5 Modulárna aritmetika

Venujme sa teraz otázke, ako vyzerá zvyšok po delení číslom $k$ súčtu a súčinu dvoch prirodzených čísel. Začnime prípadom, keď $k = 2$. Čísla dávajúce zvyšok $0$ sú párne čísla, čísla dávajúce zvyšok $1$ sú nepárne. Určite si každý rýchlo uvedomí, že keď sčitujeme dve párne čísla, výsledok je vždy párny, nepárne číslo s párnym má súčet nepárny, atď. Nie je ťažké si uvedomiť, že to, či bude súčet a súčin dvoch čísel párny alebo nepárny, závisí len od toho, aký zvyšok podelení dvojkou tie dve čísla dávajú. Prehľadnejšie je to v nasledujúcej tabuľke (zápis je už pomocou zvyškov):

| $\oplus$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

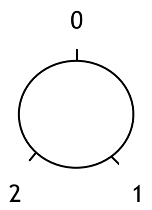
| $\odot$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ |

To, čo vidíme v tabuľkách, sa veľmi podobá na operácie s bitmi z predchádzajúcej kapitoly. V týchto tabuľkách je vlastne definovaná aritmetika zvyškov po delení číslom $2$. Hovorí sa jej aj *modulárna aritmetika* alebo aritmetika modulo $2$.

Vezmime si teraz všeobecný prípad. Majme dve prirodzené čísla $n_1$ a $n_2$ a ich zvyšky po delení číslom $k$. Ako sa mení zvyšok ich súčtu a súčinu? Nech sa tieto čísla dajú zapísať nasledovne: $n_1 = k \cdot q_1 + r_1$ a $n_2 = k \cdot q_2 + r_2$. Potom $n_1 + n_2 = (k \cdot q_1 + r_1) + (k \cdot q_2 + r_2) = k \cdot (q_1 + q_2) + r_1 + r_2$. Číslo $k \cdot (q_1 + q_2)$ je deliteľné číslom $k$, takže k výslednému zvyšku neprispeje ničím. Zvyšok výsledku závisí len od súčtu zvyškov $r_1 + r_2$. Podobne to platí pre súčin: $n_1 \cdot n_2 = (k \cdot q_1 + r_1) \cdot (k \cdot q_2 + r_2) = k^2 \cdot q_1 \cdot q_2 + k \cdot q_1 \cdot r_2 + k \cdot q_2 \cdot r_1 + r_1 \cdot r_2 = k \cdot (k \cdot q_1 \cdot q_2 + q_1 \cdot r_2 + q_2 \cdot r_1) + r_1 \cdot r_2$. Podobne, ako pri súčte, zvyšok súčinu závisí len od súčinu zvyškov $r_1 \cdot r_2$. Pre $k = 3$ máme zvyšky $0$, $1$, $2$ a situácia je priblížená v nasledujúcich tabuľkách:

| $\oplus$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ |
| $1$ | $1$ | $2$ | $0$ |
| $2$ | $2$ | $0$ | $1$ |

| $\odot$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ |
| $2$ | $0$ | $2$ | $1$ |




Napríklad $2 \oplus 1 = 0$ znamená: ak sčítame číslo, ktoré dáva zvyšok $2$ (po delení trojkou) s číslom, ktoré dáva zvyšok $1$, výsledný súčet dáva zvyšok $0$. Podobne $2 \odot 2 = 1$ znamená, že vynásobením dvoch čísel dávajúcich zvyšok $2$ (po delení tromi) dostávame číslo, ktoré dáva zvyšok $1$. Takéto sčitovanie a násobenie nazývame sčitovanie (respektíve násobenie) modulo $3$. Vo všeobecnom prípade modulo $k$ a hovoríme o modulárnej aritmetike. Je to vlastne aritmetika, v ktorej sa pohybujeme na kružnici. V bežnej aritmetike prirodzených čísel sa pohybujeme na číselnej osi. Súčet $2 + 2$ si môžeme na nej predstaviť aj tak, že zastavíme na čísle $2$ a posunieme sa o dva dieliky doprava na číslo $4$. Modulárnu aritmetiku (napríklad modulo $3$) si môžeme predstaviť na kružnici, na ktorej vyznačíme tri rovnaké dieliky a očíslujeme ich v smere hodinových ručičiek hodnotami $0$, $1$, $2$. Súčet $2 \oplus 2$ znamená, že zastavíme na čísle $2$ a posunieme sa o dva dieliky v smere hodinových ručičiek – zastavíme na čísle $1$. V časti 1.2 o reprezentácii čísel ste mali možnosť sa stretnúť s takouto aritmetikou. Je tam príklad na aritmetiku modulo $256$ (sčítaním $255 \oplus 1$ dostávame výsledok $0$). Avšak s modulárnou aritmetikou sa stretávame aj v bežnom živote. Hodiny predstavujú aritmetiku modulo $12$ alebo $24$ a hodinový ciferník kružnicu s dvanástimi dielikmi (číslo $12$ treba nahradiť číslom $0$). Dni v týždni predstavujú aritmetiku modulo $7$. Ak nám niekto o desiatej doobeda povie, že príde o tri hodiny, vieme, že ho máme čakať o jednej (na kružnici sme sa posunuli o tri dieliky v smere hodinových ručičiek).

**Zadanie 5**

Zostavte podobné tabuľky pre sčitovanie a násobenie modulo $5$, $6$ a $7$.

## 1.6 Prvočísla

V predchádzajúcej časti ste si určite všimli, že existujú prirodzené čísla, ktoré majú práve dvoch deliteľov (z množiny prirodzených čísel): jednotku a samého seba (sú to napríklad $2$, $3$, $5$, $7$). Takéto čísla nazývame prvočísla. Prirodzené číslo $1$ má len jedného deliteľa a nepovažujeme ho za prvočíslo. Ďalej vieme, že existujú prirodzené čísla (napríklad $4$, $6$, $8$), ktoré majú viac ako dvoch deliteľov. Tieto čísla nazývame zložené čísla. V zadaní 6 nájdeme jednu vlastnosť zložených čísel.

| | |
|---|---|
| **Zadanie 6** | Premyslite si a pokúste sa dokázať pravdivosť nasledujúceho tvrdenia: Každé zložené číslo je deliteľné prvočíslom. |
| **Riešenie 6** | Predpokladajme, že toto tvrdenie nie je pravdivé a existujú zložené čísla, ktoré nie sú deliteľné žiadnym prvočíslom. Najmenšie takéto číslo označme $x$. Keďže $x$ je zložené číslo, musí byť deliteľné číslom (označme ho $y$) rôznym od $x$ aj $1$. Číslo $y$ musí byť zložené číslo a keďže $y$ je menšie ako $x$, tak je deliteľné nejakým prvočíslom $p$. Potom je prvočíslom $p$ deliteľné aj číslo $x$, čo je v spore s tvrdením, že $x$ nie je deliteľné prvočíslom. |

Je známe, že o prvočísla sa zaujímali už Gréci v staroveku. V Euklidových Základoch možno napríklad nájsť dôkaz tvrdenia, že prvočísel je nekonečne veľa. Vzhľadom na to, že dôkaz tohto tvrdenia nie je náročný (bol publikovaný dokonca v jednom slovenskom obrázkovom týždenníku [12]), tak ho tu uvedieme.

***Prvočísel je nekonečne veľa.***

***Ako to dokázať?*** Predpokladajme, že toto tvrdenie neplatí. Potom by prvočísel muselo byť len konečne veľa (nech ich je $k$). Označme ich $p_1, p_2, \dots, p_k$. Vynásobme tieto prvočísla a výsledok označme $P$ (čiže $P = p_1 \cdot p_2 \cdot \dots \cdot p_k$). Potom číslo $P$ je deliteľné každým z prvočísel $p_1, p_2, \dots, p_k$ a číslo $P + 1$ dáva po delení každým z týchto prvočísel zvyšok $1$. Čiže $P + 1$ nie je deliteľné žiadnym prvočíslom z nášho zoznamu. To však znamená, že musí byť prvočíslom (ako sme spomenuli v zadaní 6, každé zložené číslo je deliteľné nejakým prvočíslom menším ako to zložené číslo). Číslo $P + 1$ sa však nemôže nachádzať v konečnom zozname $p_1, p_2, \dots, p_k$ všetkých prvočísel, pretože je väčšie, ako ktorékoľvek z uvedených čísel. Dospeli sme k logickému sporu. Keď si náš postup ešte raz premyslíme, zistíme, že jediná nesprávna logická úvaha bola hneď na začiatku, keď sme predpokladali, že prvočísel je konečne veľa (a vieme z nich vytvoriť konečný zoznam). Musí platiť opak tohto tvrdenia: prvočísel je nekonečne veľa.

Za zmienku stojí, že v čase, keď Euklides uviedol tento dôkaz, matematická symbolika nebola na takej úrovni ako dnes. Napríklad nepoznali takéto označovanie premenných a ich indexovanie (nepoužívali dokonca ani pozičnú číselnú sústavu).

| | |
|---|---|
| **Zadanie 7** | Predchádzajúci odsek môže budiť zdanie, že máme nasledujúci postup na vytváranie prvočísel. Vezmeme prvých $k$ prvočísel $p_1, p_2, \dots, p_k$, vynásobíme ich a pripočítame k nim jednotku. Zdá sa, že takto vzniknuté číslo by malo byť prvočíslom (napríklad výsledky $2 \cdot 3 + 1 = 7$, $2 \cdot 3 \cdot 5 + 1 = 31$, $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ sú prvočísla). Zistite, koľko prvočísel nám stačí zobrať, aby výsledné číslo nebolo prvočíslo. Prečo výsledné číslo nemusí byť prvočíslo a v predchádzajúcom odseku sme tvrdili, že $P + 1$ musí byť prvočíslo? |
| **Riešenie 7** | Stačí zobrať prvých šesť prvočísel: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. V dôkaze v predchádzajúcom odseku sme najprv nesprávne predpokladali, že prvočísel je len konečne veľa, a z tohto predpokladu nám vyšlo, že aj $P + 1$ musí byť prvočíslo. Medzi číslami $13$ a $30031$ však existuje množstvo ďalších prvočísel a môže sa stať, že niektoré z nich (napríklad $59$) bude deliteľom $30031$. |

## Zisťovanie prvočíselnosti

V tejto časti sa pozrime na dva postupy na zisťovanie, či dané číslo je prvočíslo. Prvý postup, známy už v staroveku, sa nazýva Eratosthenovo sito. Chceme zistiť, či prirodzené číslo $n$ je prvočíslo. Postup môžeme opísať nasledovne:

1. Vytvoríme (vypíšeme) zoznam všetkých prirodzených čísel od $2$ do $n$.
2. Zakrúžkujeme prvé číslo v zozname, ktoré ešte nie je zakrúžkované ani zaškrtnuté.
3. Ak sme zakrúžkovali $n$, môžeme skončiť – $n$ je prvočíslo. Inak pokračujeme ďalej.
4. Vyškrtáme všetky násobky tohto čísla zo zoznamu.
5. Ak sme vyškrtli $n$, môžeme skončiť - $n$ je zložené číslo. Inak sa vrátime na krok 2 a pokračujeme ďalej.

| | |
|---|---|
| **Zadanie 8** | Zistite pomocou tohto postupu, či sú čísla $31$, $93$ a $97$ prvočísla. |

Pomocou tohto postupu nezistíme len, či je dané číslo $n$ prvočíslom, ale nájdeme všetky prvočísla menšie alebo rovné ako $n$. Ak by sme však mali rozhodnúť o nejakom veľkom čísle, či je prvočíslo, tento postup je veľmi neefektívny.

Uveďme iný postup, pomocou ktorého môžeme zisťovať, či je dané číslo $n$ prvočíslom. Ukážme si ho na čísle $31$. Najprv vypočítame odmocninu z $31$, čo je približne $5{,}57$. Teraz nám stačí pre každé prirodzené číslo od $2$ po $5$ vyskúšať, či je deliteľom čísla $31$. Zistíme, že $2$, $3$, $4$, $5$ nie sú deliteľmi $31$. Takže toto číslo je prvočíslom. Podobne možno postupovať aj vo všeobecnom prípade. Ak chceme zistiť o nejakom prirodzenom čísle $n$, či je prvočíslom, preveríme prirodzené čísla od $2$ po $\sqrt{n}$, či niektoré z nich nie je deliteľom $n$. Ak nájdeme deliteľa, $n$ je zložené číslo, ak sme deliteľa medzi nimi nenašli, $n$ je prvočíslo.

| | |
|---|---|
| **Zadanie 9** | Premyslite si a zdôvodnite, prečo stačí overovať deliteľnosť len po $\sqrt{n}$? |
| **Zadanie 10** | Vezmime si prirodzené číslo $n$, na ktorého zápis potrebujeme $256$ bitov. Chceme zistiť, či je $n$ prvočíslo.<br>1. Ak použijeme algoritmus hľadajúci deliteľov čísla $n$ až po $\sqrt{n}$, koľko čísel musíme v najhoršom prípade preveriť?<br>2. Ak by náš počítač dokázal preveriť miliardu čísel za sekundu, ako dlho by mu preverovanie trvalo v najhoršom prípade?<br>3. Ak by sme zvýšili výkon nášho počítača desaťnásobne, stonásobne, ako by sa znížila celková doba výpočtu?<br>*Pre jednoduchosť predpokladáme, že na overenie každého čísla potrebujeme približne rovnaký čas, čo pri praktickej realizácii neplatí.* |
| **Riešenie 10** | Prirodzené číslo, na ktorého zápis potrebujeme $256$ bitov môže mať hodnotu až $2^{256}-1$. Aby sa nám lepšie odmocňovalo, pracujme s číslom $2^{256}$. Jeho odmocnina je $2^{128}$. Čiže v najhoršom prípade by sme museli testovať deliteľnosť čísel od $2$ po $2^{128}$. To je približne $3 \cdot 10^{38}$ čísel. Ak by sme mali počítač s programom, ktorý otestuje miliardu čísel za sekundu, zistíme, že by nám to trvalo približne $3 \cdot 10^{29}$ sekúnd, čo je okolo $10^{22}$ rokov. Ak by sme chceli zvýšiť rýchlosť výpočtu desaťnásobne alebo stonásobne, doba výpočtu by sa znížila len na $10^{21}$, respektíve $10^{20}$ rokov. Žiaľ, ani tie najlepšie počítače v súčasnosti na tom nebudú oveľa lepšie. |

Skúste povedať, ako sme sa dopracovali k číslu $3 \cdot 10^{38}$.

### Rozklad čísla na súčin prvočísel

Ak by sme tvrdenie zo zadania 6 rozvíjali ďalej (na čo v tomto texte nie je priestor), pravdepodobne by sme sa dopracovali k záveru, že každé zložené číslo možno jediným spôsobom (až na poradie prvočísel) napísať ako súčin prvočísel. Napríklad $10 = 2 \cdot 5, 12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$. Tento zápis nazývame ***rozklad*** (alebo ***faktorizácia***) čísla na súčin prvočísel.

| | |
|---|---|
| **Zadanie 11** | Navrhnite postup na hľadanie rozkladu čísla na súčin prvočísel. Využite postupy opísané v časti o prvočíslach. |
| **Riešenie 11** | Jedno riešenie, ktoré nás môže napadnúť, je nasledujúce: Máme číslo $n$ a skúšame všetky prvočísla (môžeme ich generovať napríklad pomocou Eratosthenovho sita) od $2$. Ak číslo $2$ je deliteľom $n$, potom $n = 2 \cdot n_1$ a pokračujeme ďalej. Ak $2$ delí skúsime, či $2$ je deliteľom $n_1$. Ak je $2$ deliteľom $n_1$, potom $n_1 = 2 \cdot n_2$, $n = 2^2 \cdot n_2$ a opakujeme to isté pre $2$ a $n_2$. Ak $2$ nie je deliteľom $n_1$, skúšame ďalšie prvočíslo v poradí, v tomto prípade $3$. Pokračujeme, pokiaľ nenastane situácia, že $n_k = 1$ pre nejaké $k$. |
| **Zadanie 12** | Podobnými úvahami, ako v časti o prvočíslach sa pokúste dopracovať k záveru, že pre veľké čísla je tento postup neefektívny. |
| **Návod 12** | Napríklad si vezmime zložené číslo $n = p^2$, kde $p$ je prvočíslo, na ktorého zápis potrebujeme $256$ bitov. Dopracovať sa k číslu $p$ je veľmi problematické a dôvody sú tie isté, ako sme opísali v riešení 10. |

## 1.7 Algoritmy a problémy z teórie čísel

### Problém prvočíselnosti a rozklad čísla na súčin prvočísel

Už sme si priblížili niektoré postupy na zisťovanie prvočíselnosti a rozkladu čísla na súčin prvočísel. Tiež sme si povedali, že tieto postupy sú neefektívne a v praxi sú nepoužiteľné. Avšak problém prvočíselnosti sa matematikom podarilo rozlúsknuť a dnes existujú efektívne algoritmy schopné zistiť, či je dané číslo prvočíslom. Matematika využívaná v týchto algoritmoch je však už nad rámec tohto textu. Podobne aj presné vysvetlenie, čo si predstavujeme pod pojmom efektívny algoritmus. Iná situácia je v prípade hľadania rozkladu na súčin prvočísel. V tomto prípade nepoznáme efektívny algoritmus na riešenie tohto problému a nevieme, či existuje.

Niekto by si mohol položiť otázku, prečo je dobré poznať algoritmy na riešenie týchto problémov. V nasledujúcej časti si ukážeme šifrovací algoritmus RSA, ktorý sa používa na šifrovanie a využíva aj poznatky z teórie čísel, o ktorých sme tu hovorili.

### Algoritmus RSA

Algoritmus RSA je peknou ukážkou využitia poznatkov teórie čísel v praxi. Naším cieľom nie je priniesť podrobný opis tohto algoritmu, ani dôkaz, že funguje korektne. Na toto nie je v týchto učebných textoch priestor. Našou snahou je ukázať, že existuje algoritmus používaný v praxi, v ktorom sú využité aj pojmy a poznatky teoretickej matematiky, s ktorými sa majú možnosť oboznámiť už žiaci na základných a stredných školách. Kto by chcel viac informácií o tomto algoritme aj s dôkazmi jeho korektnosti, môže skúsiť napríklad učebné texty [7].

Tento algoritmus sa používa na šifrovanie pomocou verejného kľúča. Princíp tohto šifrovania spočíva v tom, že ten, kto chce prijať zašifrovanú správu, zverejní kľúč na jej zašifrovanie. V podstate každý, kto má záujem, mu môže poslať zašifrovanú správu. Vtip je v tom, že keď chceme správu dešifrovať, potrebujeme ešte tajný kľúč. Na to, aby sme ho získali, potrebujeme poznať rozklad čísla na súčin prvočísel. Ako sme spomenuli v predchádzajúcej časti, zatiaľ nepoznáme rýchly algoritmus na hľadanie rozkladu na súčin prvočísel.

**Popis algoritmu RSA:**

Príjemca vytvorí verejný a tajný kľúč nasledovne:

1. Vygeneruje dve rôzne (dostatočne veľké) prvočísla $p$ a $q$.
2. Vynásobí ich: $n = pq$.
3. Vyberie celé číslo $e$ také, že $\text{NSD}\big(e, (p-1)(q-1)\big) = 1$. Dvojica $(e, n)$ predstavuje verejný kľúč.
4. Vypočíta číslo $d$ také, že súčin $de$ dáva po vydelení číslom $(p-1)(q-1)$ zvyšok $1$ (čiže pracuje s aritmetikou modulo $(p-1)(q-1)$ a v tejto aritmetike musí platiť $d \odot e = 1$). Dvojica $(d, n)$ je tajný kľúč.

Posielajúci pomocou verejného kľúča zašifruje správu $m$ na $m'$: $m' = \text{zvy}(m^e, n)$.

Príjemca dešifruje pomocou tajného kľúča správu $m'$ na $m$: $m = \text{zvy}((m')^d, n)$.

Skúste napríklad vynásobiť na kalkulačke prvočísla $9419$ a $1993$. Potom skúste nájsť pomocou kalkulačky rozklad čísla $18206927$ na súčin prvočísel. Koľko vám trvali tieto výpočty?

Pod označením $\text{zvy}(m^e, n)$ myslíme zvyšok $r$ zo zápisu $m^e = n \cdot q + r$ (je to vlastne výpočet mocniny $m^e$ v aritmetike modulo $n$). Ako sme spomenuli vyššie, dôležitú úlohu v tomto algoritme zohráva fakt, že pre dostatočne veľké $p,q$ nie sme schopní nájsť rozklad $n$ na súčin prvočísel. Na druhej strane, nájsť dve veľké prvočísla a vynásobiť ich nepredstavuje pre dnešné počítače problém.

Ak si chcete overiť tieto výpočty, zvyšok čísla $x$ po delení číslom $y$ môžete vypočítať na vedeckej kalkulačke vo Windows, pomocou funkcie Mod.

Uveďme príklad s malými číslami. Nech $p = 5$ a $q = 11$. Potom $n = 55$. Číslo $e$ volíme tak, aby bolo nesúdeliteľné s číslom $40 = 4 \cdot 10$, napríklad $e = 3$. Dvojica $(3{,}55)$ predstavuje verejný kľúč. Vypočítame $d = 27$, je to číslo, pre ktoré v aritmetike modulo 40 platí $d \odot e = 1$ (dá sa dokázať, že toto číslo je určené jednoznačne). Dvojica $(27{,}55)$ predstavuje tajný kľúč. Ak odosielateľ chce poslať správu $m$, zapíše ju ako postupnosť núl a jednotiek. Tejto postupnosti zodpovedá v dvojkovej sústave prirodzené číslo (označme ho tiež $m$). Nech je teda správa reprezentovaná číslom $m = 25$ (pre jednoduchosť ho uvádzame v desiatkovej sústave). Ten, kto nám chce poslať správu, ju zašifruje pomocou verejného kľúča na správu $m' = \text{zvy}(25^3, 55) = 5$ (čiže bolo treba vypočítať $25 \odot 25 \odot 25$ v aritmetike modulo $55$). Na dešifrovanie správy použijeme postup $m = \text{zvy}(5^{27}, 55)$ (čiže vypočítame mocninu $m = 5^{27}$ v aritmetike modulo $55$). Teda $m = 25$.

Tento algoritmus sa využíva napríklad aj pri internet bankingu a elektronickom podpise, avšak výpočty, ktoré sme tu popísali, urobí za nás počítač. Koho zaujala problematika šifrovania a chcel by si rozšíriť poznatky v tejto oblasti (na populárno-náučnej úrovni), tomu odporúčame knihu [8].

## Niekoľko nevyriešených problémov z teórie čísel

Na záver uveďme ešte niekoľko otvorených problémov z teórie čísel, ktoré možno jednoducho sformulovať, ale ich riešenie zatiaľ matematikom odoláva. Kto by mal záujem ďalej si rozšíriť poznatky z teórie čísel, tomu odporúčame knihu [13].

**Goldbachova domnienka:** Každé párne číslo väčšie alebo rovné ako $4$ je súčtom dvoch prvočísel. Napríklad to platí pre $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$. Nevieme však, či to platí pre všetky párne prirodzené čísla.

**Prvočíselné dvojčatá:** Existuje nekonečne veľa prvočíselných dvojčiat? Prvočíselné dvojčatá sú dvojice prvočísel takých, že druhé je o $2$ väčšie ako prvé. Napríklad $11$ a $13$, $3$ a $5$, $5$ a $7$. Nie je známe, či existuje konečný, alebo nekonečný počet takýchto dvojíc.

# 2. Logika

## 2.1 Jazyk, jeho funkcie, presný a vedecký jazyk

### Vhodná úroveň presnosti a formalizácie

Jazyk matematiky pripadá nematematikom zbytočne komplikovaný. Niekedy takéto pozorovanie zvonka vedie k mylnému záveru, že vedeckosť alebo závažnosť tvrdení spočíva práve v nezrozumiteľnosti a komplikovanosti jazyka, v ktorom bolo tvrdenie vyslovené. V matematike, samozrejme, to tak nie je. Každé slovo a výraz majú v definícii alebo vete svoj význam. Keď však používajú takto jazyk nematematici, je často na mieste jeho zjednodušenie. Nasledujúca aktivita vtipne ukazuje, ako možno jednoduché slovenské príslovia povedať nezrozumiteľne vďaka tomu, že používame pseudovedecký jazyk.

| | |
|---|---|
| **Zadanie** | V nasledujúcom texte je pseudovedeckým jazykom vyslovené slovenské príslovie. Zistite, o aké príslovie ide! |
| **Úloha 1** | Kto odoláva pokušeniu podľahnúť túžbe nechať driemať vlastnú energiu, býva obklopený chlorofylom. (*Komu sa nelení, tomu sa zelení*.) |
| **Úloha 2** | Kinetická energia eroticky motivovaného bilaterálneho, spravidla heterosexuálneho vzťahu, môže byť použitá k transferu vysokých geologických útvarov. |
| **Úloha 3** | Viac než raz, ale menej než trikrát, urči veľkosť fyzickej či chemickej veličiny, a menej než dvakrát, ale viac než nula krát použi spôsob spracovania, ktorým sa časti materiálu od seba oddeľujú. |
| **Úloha 4** | Číslo, ktorým môžeš vyjadriť svoju lingvistickú potenciu, sa rovná číslu, ktorým znásobuješ svoje ego. |
| **Úloha 5** | Pri poklese produktivity práce na nulu prejaví sa totálny nedostatok kruhového pečiva, spôsobujúceho obezitu obyvateľstva. |
| **Úloha 6** | Prenos informácie od jedinca s kalorickým deficitom k jedincovi s kalorickou potrebou už saturovanou je blokovaný. |
| **Úloha 7** | Pri zistení zámerného transportu časti horniny od občana *A* k občanovi *B* je posledne menovaný povinný uskutočniť spätný presun po rovnakej dráhe v opačnom smere, avšak s použitím žitného pečiva. |
| **Úloha 8** | Pri závodoch na spracovanie obilia, riadených mytologickou bytosťou, je pomerne nízka produktivita práce vyvážená úplnou spoľahlivosťou. |
| **Úloha 9** | Prognózu optimálneho okamžiku pre svoju akciu vykonaj podľa modelového vzťahu domestikovaného vodného operenca k plodu kultúrnych tráv. |
| **Úloha 10** | Chemická zlúčenina vodíka s kyslíkom, ktorá produkuje minimum belov, pôsobí eróziou na vrstvy hornín, uložených pozdĺž jej trajektórie. |
| **Úloha 11** | Na mieste, nachádzajúcom sa v bezprostrednej blízkosti zariadenia slúžiaceho k inštalácii svetelného zdroja, dopadá minimálny počet lúčov zo zdroja sa šíriacich. |

| | |
|---|---|
| **Úloha 12** | Pri nadmernom zvyšovaní pohybu dolných končatín v značnom časovom rozpätí za účelom dosiahnutia naplnenia zlúčeninou kyslíka a vodíka krivuľu s držadlom, dôjde jedného dňa k uvoľneniu molekúl spájajúcich túto krivuľu s oným držadlom, čím sa menovaný predmet rozdelí na dva segmenty. |

Ak ste vyriešili predchádzajúcu úlohu, môžete si skontrolovať svoje výsledky s našimi, ktoré sa nachádzajú v časti *Čo sme sa naučili*.

| | |
|---|---|
| **Zadanie** | Nájdite na internete stránku so slovenskými prísloviami a porekadlami a prepíšte niektoré z nich do pseudovedeckého jazyka, tak ako sme to urobili v zadaní 1. (Napríklad http://www.juko56.allforum.sk/prislovia.htm) |

## Čo sme sa naučili

Laskahoryprenasadvakratmerajarazrezkolkoreciviestolkokratsiclovekombezpraceniesukolacesytyhladnemuneveriktodotebakamenomtydonehochlebomboziemlynymelupomalyaleistodockajcasuakohusaklasutichavodabrehymyjepodlampoujenajväcsiatmatakdlhosachodisdzbanompovodukymsauchoodtrhne

## Interpretácie zadania úlohy, ktoré učiteľ neočakáva

V nasledujúcej aktivite si ukážeme, ako je dôležité, aby bola úloha pochopená a interpretovaná správne. Presnejšie, chceli by sme ukázať, že nepresne zadaná úloha môže mať viacero interpretácií, a preto aj viacero riešení. Úloha o včele nie je zaradená preto, aby sme sa naučili formulovať čo najpresnejšie zadania. Také zadania sú totiž nezrozumiteľné. Omnoho dôležitejší efekt je, že sa poslucháči naučia počúvať cudzie riešenia a argumenty. A akceptovať aj inú interpretáciu zadania, než tú svoju.

| | |
|---|---|
| **Zadanie** | Do miestnosti jedným z 5 okien vletela včela. Potom niekto jedno okno zavrel a včela jedným zo 4 otvorených okien vyletela von. Koľko bolo možností, ako to mohla urobiť? |

Vyberte si z nasledujúcich „riešení“ to, ktoré považujete za správne. Vytvorte skupiny, ktoré budú obhajovať jednotlivé riešenia. Dohodnite sa medzi skupinami, ktoré riešenie je správne. Lektori podporia svojimi argumentmi početne najslabšiu skupinu. Cieľom tejto aktivity je naučiť sa vnímať aj postupy a argumenty, ktoré neočakávame. Len ak pochopíme cudzie riešenie, tak sme schopní v ňom nájsť chybu, alebo naopak, nájsť chybu vo vlastnom riešení.

| | |
|---|---|
| **Riešenie 1** | *Možností je* 20. Pre vletenie do miestnosti má včela 5 možností a ku každej z tých piatich možností má 4 rôzne možnosti, ako z miestnosti odletieť. To je spolu 20. To, čo robí niekto iný (človek, ktorý zavrel okno), nie je pre včelu možnosťou, a preto sa do počtu všetkých možností nezapočítava. |

| | |
|---|---|
| **Riešenie 2** | *Možností je* 100. Tu berieme do úvahy aj možnosť, ako človek okno zavrie. Keby sme to totiž nebrali do úvahy a nezapočítali do počtu možností, tak napr. pri zavretom druhom okne vylúčime možnosť, že ním včela vyletí, ale medzi celkový počet možností túto zarátať treba, lebo niekedy nastať môže. Teda je 5 možností pre vletenie, 5 možností pre zavretie okna a 4 možnosti pre odlet. |
| **Riešenie 3** | *Možností je* 25. Riešenie uvádza práve raz každú z možností vletenia a odletu, ktorá môže nastať, a tých je 25. Vôbec nás nemusí zaujímať, ktoré okno je pri tom zavreté, lebo to, že včela vletí oknom 1 a vyletí oknom 2, je jediná možnosť, nech už je zavreté ktorékoľvek okno. |
| **Riešenie 4** | *Možnosť je* 1. Ak neberieme do úvahy rôzne dráhy letu cez rovnaké okno, je len jeden spôsob, ako mohla včela preletieť. Všetko sa už totiž stalo v minulosti, a keď vieme, že včela prišla oknom jedna a odišla oknom 5, tak žiadnu inú možnosť, ako sa to stalo, už uvažovať nemôžeme. |

Korešpondenčné semináre a matematická olympiáda na Slovensku pomáhajú učiteľom a rodičom v starostlivosti o talentovaných žiakov. Kým olympiáda je zameraná na vyhľadanie talentovaného žiaka, a potom v rámci súťaže na určenie veľkosti jeho talentu, korešpondenčné semináre venujú veľkú časť svojej činnosti motivácii a budovaniu záujmu o matematiku, fyziku alebo informatiku. Pretože prvoradým záujmom je motivácia detí na riešenie úloh, organizátori sa snažia napísať zadania čo najatraktívnejšie. Vďaka tomu sa občas stane, že zadanie nie je jednoznačné a možno ho chápať viacerými spôsobmi. Deti väčšinou nemajú problém pochopiť organizátorov a nájdu očakávané riešenie. Ale to často nie je jediné. Preto so stredoškolákmi občas hráme hru, v ktorej majú hľadať také interpretácie zadania, a tým aj riešenia, ktoré zadávateľ nečakal. To je podstata nasledujúcej aktivity.

www.sezam.sk

| | |
|---|---|
| **Zadanie** | Vyriešte v skupinách úlohy korešpondenčného seminára Sezamko tak, aby ste našli čo najoriginálnejšie riešenia. |
| **Hodnotenie** | • Za každé správne riešenie úlohy dostane skupina 1 bod.<br>• V prípade, že úlohu vyriešila iba jedna skupina, dostane táto skupina za každé riešenie 2 body.<br>• V prípade, že úlohu vyrieši iba jedna skupina a zároveň riešenie nebolo očakávané, teda organizátori nemali uvedené príslušné vzorové riešenie, dostane za riešenie skupina 3 body. |

Zadania úloh korešpondenčných matematických seminárov, ktoré na Slovensku organizujú študenti vysokých, prípadne stredných škôl a ich učitelia, možno nájsť na internetových stránkach týchto seminárov. Väčšina korešpondenčných seminárov sa orientuje na základné školy: V Bratislave sú to Pikomat a Riešky, v Žiline Sezam a Sezamko, v Košiciach Malynár a Matik. Hoci väčšina z týchto seminárov pôsobí prioritne vo vlastnom regióne, riešia ich deti z celého Slovenska, prípadne aj zo zahraničia.
Na stredné školy sa orientuje celoslovenský seminár KMS a na východnom Slovensku aj Strom.

## Čo sme sa naučili

Niekedy úloha skutočne môže mať „dve rôzne riešenia“. Stáva sa to hlavne vtedy, keď sa zadávateľ úlohy pokúsi formálne presné zadanie formulovať v reálnej situácii, v konkrétnom kontexte. Ten, kto pozná riešenie úlohy, väčšinou vie, čo ním autor myslel. Žiaci si však môžu predstaviť úplne iné zadanie a riešiť inú úlohu, ktorá formálne zadaniu tiež vyhovuje. Ak neštandardné riešenie učiteľ nepochopí a nástojí na očakávanom riešení, musí sa žiak podrobiť autorite sily, a nie autorite argumentov. V tom okamihu je rozvoj jeho logického myslenia ohrozený!

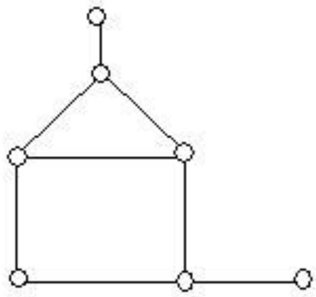
JSMF Žilina, Fakulta riadenia a informatiky ŽU,

S E Z A M K O, Školský rok 2004/2005, 1.zimná séria

## Čo Ste o Pipi nevedeli !

Ahoj kamaráti! Možno ste už o mne počuli, som ππ-Dlhá Pančucha.
Čudujete sa, prečo mám v mene tú čudnú značku π namiesto „pí“? To je preto, lebo som sa rozhodla prezradiť Vám veľké tajomstvo. Okrem toho, že som najsilnejšie a najbohatšie dievča na svete, som aj matematický génius. Už dávno som v jednej starej knihe na ockovej lodi našla symbol π, ktorý sa číta ako „pí“. Je to akési zvláštne číslo týkajúce sa obvodu a obsahu kruhu, alebo kružnice (alebo tak nejak). Najväčší mudrci staroveku dokonca zistili, že toto číslo je o čosi viac ako 3. Ja som si sama vypočítala, koľko je to číslo presne. Vám ho určite prezradia v škole. Toľko o mojom skutočnom tajnom mene.
Teraz sa chcem s Vami podeliť o niektoré zaujímavé matematické problémy, s ktorými sme sa stretli ja a moji kamaráti Tomi, Anika, Kôň, pán Galán, námorník Fridolf a otecko Efraim.

**1.úloha:** Minulý týždeň som sa u nás rozhodla zaviesť konskú dopravu. Môj Kôň s tým súhlasil. Naše mestečko nie je veľmi veľké, takže stačilo urobiť len sedem zastávok. Prvý deň sme prešli 6 zastávok v takomto poradí:
Pri Fridolfovi –Pri Cukrárni – Pri Anike – Pri Efraimovi – Pri Bazéne – Pri Galantérii. Mojim kamarátom sa hromadná konská doprava veľmi páčila. Ďalší deň sme si vybrali inú trasu. Teraz sme prešli 6 zastávok v tomto poradí:
Pri Doktorovi – Pri Fridolfovi – Pri Anike – Pri Cukrárni – Pri Bazéne – Pri Efraimovi.

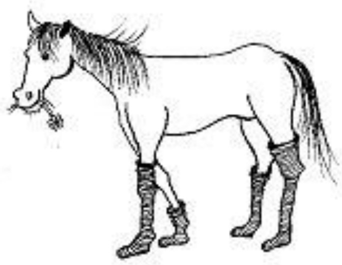


Ďalší deň sme chceli ísť zasa. Môj Kôň však povedal: „Kým nebudem presne vedieť, kde je ktorá zastávka, nejdem nikam!“ Tak som si zobrala plánik mesta, ktorý vidíte na obrázku a k jednotlivým zastávkam som dopísala ich názvy. Dokážete to aj Vy?
**Napíšte názvy zastávok do plánika ak viete, že pri našich cestách kôň vždy zastal na každej zastávke okolo ktorej sme išli!**

**2.úloha:** Ďalší deň som sa zobudila skoro ráno. Keďže som nemala čo robiť, tak som si začala počítať zlaté dukáty od otca. Chcela som totiž vedieť, koľko kíl cukríkov si za ne môžem kúpiť. Keď som dukáty spočítala, bola som strašne rada. Potom som si napísala list:

*Milá ππ !*
*Vieš koľko máš dukátov? Nemáš ich 3501210210.*
*Ale keď toto číslo rozšifruješ, zistíš, koľko ich máš.*
*Na noc si vždy zas3 !*
*Môj Kôň zjedol 100h slamy.*
*Dúfam, že aj Tvoj.*

*Pozdravuje sa ππ*



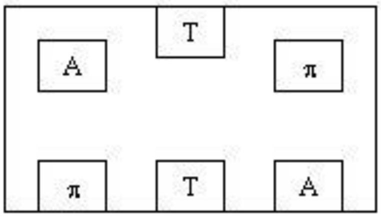
V liste som si napísala, koľko mám dukátov. Aby nemohol každý prečítať, koľko mám peňazí, počet dukátov som zašifrovala. Šifrou, ktorú som použila, sa šifrujú len tie desaťciferné čísla, ktoré obsahujú všetky cifry od 0 po 9 (každú presne raz). Našťastie počet mojich dukátov taký bol. Šifruje sa tak, že postupne zľava doprava namiesto každej cifry napíšeme počet cifier, ktoré sú napravo od nej a sú od nej menšie. Takže napríklad číslo 4658237019 by som zašifrovala ako 4545222000. Rozumiete?

**Vedeli by ste vypočítať, koľko mám dukátov? Rozšifrujte číslo 3501210210!**

Poriadne svoj postup zdôvodnite! Chcem si ísť kúpiť cukríky!

**3.úloha:** Po obede prišli na návštevu Tomi s Anikou. Hrali sme sa takúto hru. Každý z nás si vybral dve skrine (pozri obrázok). Skrine, ktoré si vybral Tomi, sú označené T . Tie, ktoré si vybrala Anika, sú označené A. Moje sú označené π. Skrine sa nedajú posúvať a poza tie, ktoré sú nakreslené pri stene sa nedá chodiť. Potom pán Galán navrhol: „Nakreslite si každý od jednej svojej skrine k druhej svojej skrini po zemi čiaru.“ Tento nápad nás veľmi nadchol a ja som hneď zašla po vedrá s farbou. Skôr ako som ich stihla nájsť, prišiel Kôň. Ten nespokojne povedal: „ Keď už chcete počmárať podlahu, tak to urobte tak, aby sa žiadne dve čiary nekrižovali!“ Kým som hľadala farbu, rozmýšľali sme, ako to urobiť. Porozmýšľajte nad tým aj vy.

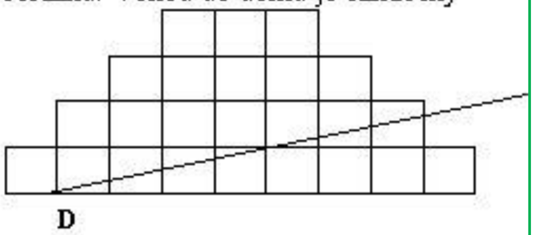
**Napíšte a nakreslite nám, ako máme na podlahu nakresliť čiary spájajúce skrine tak, aby sa žiadne dve nekrižovali a naviac, žiadna z čiar nešla poza skrine, ktoré sú pri stene!**




**4.úloha:** Dnes večer som sa rozhodla, že budem pestovať kvety. Ale môj Kôň prehlásil: „Pol záhrady chcem mať pre seba, aby som mal čo jesť. A ak mi necháš voľný prístup k domu, tak nebudem chodiť do tvojej polovice.“ Viem, že môj Kôň má rád rovné cestičky a chcela som mu spraviť radosť. Preto som sa rozhodla záhradu rozdeliť jednou rovnou cestičkou začínajúcou pri vchode do domu. Moja záhrada je už rozdelená na rovnako veľké štvorcové záhony a má tvar ako na obrázku. Vchod do domu je označený písmenkom D. Je tam aj prvý pokus o rozdelenie záhrady, ale ten sa Koňovi nepáči, lebo ešte nesplňa jeho požiadavky. Tu sú:

**Chodník má byť rovná čiara, má začínať v bode D a plochu záhrady má rozdeliť na dve časti s rovnakým obsahom!**

**Skúste mi poradiť, ako mám záhradu rozdeliť!**




A poriadne mne a Koňovi zdôvodnite, prečo obe časti záhrady vo Vašom riešení majú rovnaký obsah.

**5.úloha:** V sobotu sa môj otecko Efraim Pančušisko vrátil z dlhej plavby. Na druhý deň zobral mňa, Tomiho a Aniku na výlet vlakom. Od radosti sme začali s Tomim a Anikou behať po všetkých vagónoch. Pri príchode do ďalšej stanice sme preto sedeli každý v inom vagóne. Na nástupišti bolo niekoľko lavičiek. Každý z nás spočítal, okolo koľkých lavičiek prešiel, kým vlak zastavil. Vyšli nám čísla 7, 12 a 15. Celý čas, kým stál vlak v stanici, sme slušne sedeli na svojich miestach. Keď sa vlak pohol a vychádzal zo stanice, opäť sme každý spočítali lavičky, okolo ktorých sme prešli pri odjazde. Anike teraz vyšlo číslo trikrát väčšie ako mne. Tomi však zabudol, koľko lavičiek napočítal pri odchode on. Skúste nám to pomôcť zistiť.

**Koľko lavičiek napočítal pri odchode vlaku zo stanice Tomi?**

*Na Vaše riešenia sa spolu s ππ tešíme aj my, opravovatelia úloh a organizátori korešpodenčného seminára SEZAMKO. Nájdete nás na* **www.sezam.sk**

Riešenia, napísané na **samostatných a podpísaných** papieroch (spolu **s obálkou** veľkosti A5, na ktorej bude napísaná Tvoja spätná adresa a nalepená známka 13 Sk), posielajte najneskôr do **11.októbra 2004** na adresu:

**SEZAMKO**
Fakulta riadenia a informatiky
Žilinská univerzita
Ulica Univerzitná 1
010 26 Žilina

## 2.2 Definície a axiómy

### Čo spôsobí čiarka vo vete?

Nielen v technických vedách, ale aj v našej každodennej komunikácii dochádza k mnohým nedorozumeniam. Niektoré z nich majú dôvod, ktorý je relatívne ľahko odstrániteľný - nepresné vyjadrovanie. Poďme sa spoločne pozrieť na možné príčiny týchto problémov.

| | |
|---|---|
| **Príklad** | Ambiciózny politik chcel predniesť plamenný prejav pod transparentom s heslom: „***Napred, nemožno ísť nazad!***“ Keď zistil, že sa nedostavili žiadni poslucháči, skontroloval si text na transparente. Stálo na ňom: „ ***Napred nemožno ísť, nazad!***“ |
| **Zadanie** | Vysvetlite rozdiel vo význame viet (výňatok zo sprievodcu Prahou): „***Praha je mesto, kde sa stretávajú turisti s množstvom pamätihodností.***“ Predstavme si, že nejaký turista si zapísal podobnú vetu: „***Praha je mesto, kde sa stretávajú turisti, s množstvom pamätihodností.***“<br><br>Ktorá z predošlých viet má rovnaký zmysel, ako nasledovná veta? ***„Praha je mesto s množstvom pamätihodností, kde sa stretávajú turisti.***“ |

V obchodoch, podnikoch a rôznych iných inštitúciách sa môžeme často stretnúť na dverách s nápisom „*Nezamestnaným vstup zakázaný.*“ Myslí sa ním, že do uvedených dverí nesmú vojsť len nezamestnaní obyvatelia Slovenska? Pravdepodobne nie. I keď som zamestnaný, vstupovať by som do týchto dverí nemal (ak nie som zamestnaný priamo v tejto inštitúcii).

| | |
|---|---|
| **Zadanie** | Preformulujte oznam „***Nezamestnaným vstup zakázaný!***“ tak, aby vyjadroval presne to, čo ním bolo myslené! |
| **Riešenie** | „***Osobám nezamestnaným v tomto podniku je vstup zakázaný!***“ Je už tento oznam presný? Nie je presnejší nasledujúci oznam? „***Osobám nezamestnaným v tomto podniku je vstup do týchto dverí zakázaný!***“ Alebo ešte presnejšie: „***Osobám v tejto chvíli nezamestnaným v tomto podniku je vstup do týchto dverí zakázaný!***“ Zdá sa vám to kostrbaté? Máte pravdu. Kostrbaté, ale postupne omnoho presnejšie. A vôbec, nemyslia sa tým len nezamestnaní v oddelení, do ktorého vedú tieto dvere? Na druhej strane, môže do nich vstúpiť požiarnik alebo aj Vy, keď Vás pozve sám pán riaditeľ podniku? |
| **Zadanie** | ***Cestujúci sú počas jazdy povinní sa držať!***<br><br>Porušujú pokyn deti, ktoré<br><br>a) sa po nastúpení do autobusu navzájom pochytajú,<br>b) si sadnú a ničoho sa nedržia?<br><br>Pokúste sa tento text naformulovať presne. |

## Ako definujeme nové pojmy?

Pri komunikácii medzi ľuďmi je potrebné, aby rovnaké slová a pojmy chápali rovnako. Ak by pod pojmom kôň chápal každý niečo iné, mali by problém sa dohodnúť. Čo je to vlastne kôň, sa môžeme dočítať vo výkladovom slovníku. Dozvieme sa tam:

| Opis pojmu | 1. ***Kôň:*** domáce zviera používané na ťahanie alebo jazdenie; jeho samec<br>2. ***Byt:*** miestnosti na bývanie tvoriace celok<br>3. ***Koleso:*** kruhový predmet, ktorý otáčaním umožňuje pohyb iných predmetov<br>4. ***Rektor:*** najvyšší akademický funkcionár vysokej školy |
|---|---|

Zamyslime sa teraz nad vysvetlením jednotlivých slov.

1. Existuje iné zviera, ktoré spĺňa uvedená definíciu? Ak áno, viete definíciu slova kôň upraviť tak, aby nájdené iné zviera tejto definícii nevyhovovalo?
2. Je WC a kúpeľňa súčasťou bytu? Sú to miestnosti určené na bývanie? Ako by ste definovali slovo dom tak, aby sa táto definícia odlišovala od definície slova byt?
3. Poznáte iný predmet, ktorý spĺňa definíciu kolesa z výkladového slovníka?
4. Ak viete, že jeden z akademických funkcionárov meria 190 cm, môže byť rektorom funkcionár s výškou 180 cm? Ako by ste upravili vyššie uvedenú definíciu tak, aby sa predchádzajúca otázka stala nezmyselnou?

| Aktivita | Vyberte si nejaký pojem, označme ho *X*. Prvý hráč sa pokúsi vysvetliť pojem *X* bez použitia slova, ktoré označuje *X*. Druhý hráč sa potom snaží nájsť iný pojem, označme ho *Y*, ktorý tiež spĺňa opis pojmu *X* prvého hráča. Prvý hráč sa potom snaží vylepšiť vysvetlenie pojmu *X* tak, aby ho nespĺňal pojem *Y*. Na to sa snaží druhý hráč nájsť nový pojem *Y*, ktorý spĺňa tento vylepšený opis pojmu *X*. |
|---|---|

Pojem *X* „tiger“ popíšeme ako „cicavec, ktorý má na tele pruhy“.
Súper vyberie objekt *Y* „zebra“.

Vylepšíme popis pojmu *X*.

Pojmy, ktoré patria do hovorovej reči a poznáme ich už dávno, nemusíme nanovo násilne definovať. Aktivity a príklady v tejto časti nám však ukázali, že nie je jednoduché nový pojem presne vymedziť. Aby sme mohli v príslušnej vedeckej disciplíne používať presné pojmy, je ich potrebné čo najskôr presne vysvetliť, definovať. Prípadne tak presne, ako je to potrebné, alebo aspoň tak presne, ako je to najlepšie možné.

## Príbuzní

V prípade, že chceme do logických úvah a polemík motivovať spôsobom, ktorý je deťom blízky, môžeme siahnuť k osvedčenej tematike príbuzenských vzťahov. Niektoré deti sa v tejto problematike nielen dobre orientujú, ale sú ochotné tému ďalej rozvíjať. Uvádzame dve aktivity, ktoré sa dajú meniť v závislosti od skupiny, s ktorou pracujeme.

Úvahou o rozvoji logického myslenia a argumentácie v prostredí, ktoré je pre žiaka blízke, sa začína článok Z. Kubáčka [6], z ktorého sme čerpali inšpiráciu pre nasledujúce aktivity.

| Aktivita 1 | V cudzom jazyku máte pomerne dobrú slovnú zásobu, no neovládate pojmy pre komplikovanejšie príbuzenské vzťahy. Ovládate iba slová, ktoré označujú pojmy: ***mama***, ***otec***, ***syn***, ***dcéra***, ***sestra***, ***brat***, manžel<br><br>Vysvetlite pomocou vymenovaných pojmov nasledujúce pojmy: ***teta***, ***bratranec***, ***nevesta***, ***švagriná***, ***svokor***. |
|---|---|

| Aktivita 2 | Doplňte v texte chýbajúce slová:<br><br>Oženil som sa so ženou, ktorá už mala dospelú dcéru. Môj otec sa zamiloval do mojej nevlastnej dcéry a zobral si ju za ženu. Tým sa stal mojím ......... a moja nevlastná dcéra mojou ......... . Moja nevlastná dcéra sa stala ......... mojej manželky. |
|---|---|

## Koľko krokov treba na dôkaz, že 2+2=4?

Zermelov-Fraenkelov systém axióm pozostáva z axióm:

- extenzionality
- dvojice
- zjednotenia
- nekonečna
- podmnožiny
- potenčnej množiny
- nahradenia
- fundovanosti
- výberu

Presný popis uvedených axióm sa nachádza v materiáloch [7].

Matematika ako vedná disciplína rieši svoje odborné problémy a kráča vpred v abstraktných oblastiach svojho záujmu a výskumu. Zároveň poskytuje množstvo aplikácií, výsledkov a postupov ostatným vedeckým a technickým oborom. Slúži im aj ako nástroj pre vyjadrovanie problémov a formulovanie výsledkov. Matematika je jednou z najabstraktnejších vied. Väčšina pojmov, s ktorými pracuje, nemá svoje priame vzory v realite. Hlavnou náplňou práce matematikov je vytváranie rôznych imaginárnych objektov a skúmanie ich vlastností a vzájomných vzťahov. Obsahom a podstatou matematiky sú potom takto vzniknuté myšlienkové konštrukcie. Ich osvojenie si spočíva v pochopení písaných alebo vyslovených myšlienok a predstáv iných ľudí. Význam presného a zároveň zmysluplného vyjadrovania sa je preto v matematike obzvlášť veľký. Matematici sú si toho veľmi dobre vedomí a matematická logika, ktorá skúma jazyk matematiky, je jedným z jej samostatných a veľmi významných oborov.

Prejavom tejto presnosti je aj značná štruktúrovanosť matematických textov. Obsahujú veľmi málo „voľného“, nezáväzného rozprávania. Omnoho častejšie majú jednotlivé odseky a časti textu špeciálny význam, formu a dokonca aj názov. V matematických textoch nachádzame definície, v ktorých sa zavádzajú nové pojmy. K vysvetleniu neznámych pojmov je pochopiteľne potrebné použiť už známe, predtým definované pojmy. Dobré definície by mali byť nielen správne, ale aj zrozumiteľné a mali by sa nimi zavádzať naozaj dôležité a kľúčové pojmy. Aké ťažkosti môžu pri definovaní nového pojmu nastať, sme si ukázali v predošlej časti.

Zložitým definíciám zložitých pojmov by mali predchádzať stále jednoduchšie a jednoduchšie definície jednoduchších pojmov. Tento proces však niekde musí mať začiatok. V matematike takýto začiatok predstavuje súbor základných definícií, vlastností a pojmov príslušnej matematickej teórie, ktorý sa nazýva systém axióm. Pre každú oblasť matematiky sú tieto prvotné pravdy dohodnuté inak. Celý systém musí mať samozrejme rozumné vlastnosti, napríklad axiómy by nemali viesť k sporu, nemalo by ich byť zbytočne veľa, ale mala by sa z nich dať príslušná časť matematiky vybudovať. Aj keď sa to dá, neznamená to, že každé tvrdenie a pojem budujeme od axióm (rovnako, ako nepíšeme každý program v strojovom kóde.)

V literatúre [7] je napríklad uvedené, že dôkaz rovnosti 2+2=4 vychádzajúci zo systému axióm teórie množín (Zermelo-Fraenkel) má viac ako 20 tisíc krokov. Keby sme pri každej úlohe na sčítanie mali urobiť všetky tie kroky, ďalej ako po „sčítalku“ do 10 by sme sa v matematike nedostali. To neznamená, že systémy axióm nie sú pre matematiku dôležité. Len si je potrebné uvedomiť, že ani matematici väčšinou nedokazujú svoje tvrdenia zo základných axióm, ale z tvrdení, ktoré niekto odvodil pred nimi.

## Čo sme sa naučili

Prílišná presnosť jazyka a dôraz na jeho formálnu stránku ubíja u detí tvorivosť. Prílišná voľnosť jazyka spôsobuje nepresnosti a nedorozumenia. Preto úroveň presnosti jazyka volíme podľa toho, na čo ho používame. Formálne presné texty (poučky v učebniciach), ktoré sa majú učiť žiaci naspamäť bez porozumenia, škodia vývoju ich kauzálneho myslenia!

## 2.3 Jednoduché a zložené tvrdenia

Prvým krokom pri vedeckom skúmaní a budovaní pravidiel logického uvažovania a vyjadrovania je tzv. výrokový počet. V tejto časti pristúpime na dohodu, že výrok je „základným stavebným kameňom“ zložitejších tvrdení a vyjadrení, ktoré budeme ďalej skúmať. Pre naše potreby bude tiež postačovať definícia, že výrokom je každé tvrdenie, o ktorom je možné jednoznačne rozhodnúť, či je pravdivé, alebo nepravdivé. (Pri hlbšej úrovni budovania a formalizácie matematickej logiky sa podrobnejšie skúma aj štruktúra výroku, spôsob jeho vytvárania z používanej abecedy znakov atď. Pre nás takýto detailný prístup nie je potrebný. Tak isto zostaneme pri klasickej logike, ktorá používa len dve pravdivostné hodnoty. Skúmajú a používajú sa aj viachodnotové logiky, dnes asi najznámejšia z nich je tzv. fuzzy logika.) Výroky je možné vzájomne spájať do zložitejších pomocou tzv. logických spojok. Opäť je možné skúmať vlastnosti a vzájomné súvislosti spojok, hľadať ich minimálny potrebný počet alebo vymýšľať ďalšie. Pomocou spojok a jednoduchších výrokov sa dajú vytvoriť zložitejšie výroky.

| | |
|---|---|
| **Spojky** | V bežnom matematickom, ale aj informatickom jazyku sa ustálilo používanie nasledujúcich spojok: |
| **a** | „...*a*...“ nazývané „*konjunkcia*“, „logický súčin“, „platí súčasne“. Značenie: $\wedge$, prípadne &. |
| **alebo** | „...*alebo*...“ nazývané „*disjunkcia*“, „logický súčet“, „platí aspoň jeden z výrokov“. Značenie: $\vee$. |
| **ak, potom** | „*ak*...*tak*...“ , „*ak*... *potom*...“ nazývané „*implikácia*“, ak je splnený predpoklad, musí platiť záver“. Značenie: $\Rightarrow$. |
| **práve vtedy** | „...*práve vtedy*...“ nazývané „*ekvivalencia*“, oba výroky súčasne buď platia alebo neplatia“. Značenie: $\Leftrightarrow$. |
| **nie je pravda** | „*nie je pravda, že*...“, „*neplatí*...“ nazývané „*negácia*“, ktorá znamená nahradenie výroku jeho opačným tvrdením. Značenie: $\neg$ pred výrokom, prípadne apostrofom za, alebo čiarou nad negovaným výrokom. |

Pomocou spojok môžeme výroky nielen spájať, ale aj naopak, ak vo výroku nájdeme niektorú spojku, môžeme výrok rozložiť na jednoduchšie. Výroky, ktoré už takto rozdeliť nemôžeme, sa nazývajú jednoduché, tie ostatné výroky sú zložené. Jednou z „hlavných disciplín“ výrokového počtu je skúmanie pravidiel, ako sa pri vytváraní zložených výrokov z jednoduchších prenášajú ich pravdivostné hodnoty.

| | |
|---|---|
| **Príklad** | Keď pomocou spojky „*a*“ vytvoríme nový výrok z dvoch jednoduchších, ich konjunkcia bude pravdivá len v prípade, že boli pravdivé aj oba pôvodné výroky. V tomto prípade panuje zásadná zhoda medzi používaním spojky v logike a v bežnom jazyku. Veta „*Basketbalisti a basketbalistky potrebujú väčšie postele.*“ však ukazuje, že aj o tejto spojke je možné viesť hlbšiu diskusiu. V tomto prípade však problém spočíva v neodlíšení logického „*a*“ spájajúceho výroky a množinového „*a*“, kombinujúceho dva súbory objektov. |

U najmladších žiakov (pre niektorých učiteľov prekvapujúco) spôsobuje najväčšie problémy spojka „*alebo*“. Príčina nie je v prílišnej obťažnosti použitia tejto spojky v matematickej logike, ale v rozdiele medzi jej používaním v bežnom (slovenskom) jazyku a v logike.

Možnosť určenia pravdivosti chápeme ako potenciálnu. Preto aj vety „*Na Marse je voda.*“ alebo „*Existuje nekonečne veľa prvočíselných dvojčiat.*“ považujeme za výroky, aj keď na jednoznačné určenie ich pravdivostí si budeme ešte musieť počkať.

Výrokmi nie sú vety, ktorým tomu bráni ich gramatická stavba a účel: „*Ach jaj!*“ „*Nevyrušuj na hodine!*“

Výrokmi nie sú ani tvrdenia, ktoré na prvý pohľad výrokmi môžu byť, ale bránia im v tom omnoho hlbšie príčiny: „*Vždy klamem.*“ „*Toto tvrdenie je nepravdivé.*“

Pravidlá o určovaní pravdivosti výrokov vytvorených pomocou základných logických spojok sú v podstate súčasťou ich definície. Tieto potom ďalej využívame pri určovaní pravdivosti omnoho zložitejšie a rafinovanejšie „poskladaných“ výrokov.

Je smutné, že vyučovanie schopnosti určiť pravdivostnú hodnotu, často zdegraduje na mechanické vypĺňanie známych tabuliek pravdivostných hodnôt.

V našom texte namiesto upratených tabuliek ponúkame úlohy, ktoré sú podľa našich skúseností na získanie schopnosti práce so zloženými výrokmi a ich pravdivostnými hodnotami omnoho vhodnejšie. Ich samostatné preriešenie preto odporúčame nielen čitateľom tohto materiálu, ale tiež ako aktivitu pre prácu so žiakmi v rámci školského vyučovania.

Takáto ilustrácia implikácie (zo života) je celkom prijateľná: *„Ak sa budeš dobre učiť, dostaneš bicykel!“* Dokonca aj keď sa dobre neučím, mám šancu dostať bicykel a zachovať pravdivostnú hodnotu implikácie.

Ťažšie už by sme intuitívne vysvetľovali všetky situácie, kedy je podľa pravidiel logiky pravdivá implikácia: *„Ak prinesieš päťku, dostaneš výprask!“*

*„Ak je 2 nepárne číslo, potom je 6 druhou mocninou“* je pravdivá, ale podozrivo znejúca implikácia.

Pravdivosť ekvivalentného tvrdenia *„Číslo 2 je párne alebo 6 je druhá mocnina“* je už očividnejšia.

*„Alebo“* je v našej reči používané niekedy vo vylučovacom a inokedy v nevylučovacom zmysle. Vo vetách *„Večer pôjdem do kina alebo do divadla.“* alebo *„K obleku si dám kravatu alebo motýlik.“* vcelku oprávnene predpokladáme, že nenastanú súčasne obe možnosti. V predchádzajúcej vete alebo vo vete *„Na koncerte musí byť prítomný lekár alebo zdravotník.“* nám naopak neprekáža, že je pravdivá vtedy, ak je pravdivá prvá, druhá alebo aj obidve jej časti.

Naopak sa zdá, že známe problémy s implikáciou (jej pravdivosť pri nesplnení predpokladu, zámena „smeru“ implikácie ) sa objavia až potom, ako začneme žiakov „učiť logiku“. K pochopeniu implikácie sa väčšinou vedia dostať uvedomením si významu jej opaku, t.j. negácie. Implikácia neplatí len vtedy, keď je pravdivý jej predpoklad a nepravdivý jej záver. Opakovanou negáciou sa dostaneme k tvrdeniu logicky zhodnému (teda ekvivalentnému) s pôvodnou implikáciou: neplatí predpoklad alebo platí záver. V formálnom zápise to vyzerá takto: $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$ . Viac ako tomuto zápisu však odporúčame poriadne sa venovať jeho zmyslu. Vyskúšajte si ho na príkladoch implikácií z bežného jazyka a z jednoduchých matematických pravidiel.

Sme presvedčení, že zvládnutie matematickej logiky sa priamo prejavuje vo viacerých typických činnostiach informatiky. Bezprostredne napríklad pri potrebe vytvárania podmienok v *„IF“* častiach podmienených príkazov. Ďalšou oblasťou je analýza a tvorba algoritmov. Algoritmus v podobe vývojového diagramu sa dá v určitom zmysle interpretovať ako úvahami programátora vytvorený zložený výrok. Veľmi podobná a dôležitá je aj analýza práce alebo zlyhania algoritmu, kde sa snažíme určiť, aká (logická) kombinácia hodnôt parametrov a premenných vedie k rôznym stavom a činnostiam programu.

## Tigre a princezné

Výrokový počet je východiskom pri budovaní logiky aj z historického hľadiska. Aristotelova práca *O sofistických dôkazoch* je prvou (známou) z tejto oblasti. Vychádza z analýzy postupov používaných sofistami pri dokazovaní rôznych paradoxných tvrdení a pri ich spôsobe dokazovania pravdivosti tvrdení všeobecne. Samotní sofisti pritom Aristotela predišli a svojimi službami sa dobre živili už o približne jedno storočie skôr. Dá sa preto povedať, že snaha a schopnosť upresňovať význam dôležitých slov a určovať súvislosti a pravdivostné hodnoty výrokov a ich sústav je stará viac ako 2500 rokov. Pre uvažujúcich ľudí bola už vtedy zaujímavá, atraktívna a zvládnuteľná.

Nasledujúcu kaskádu úloh, odporúčame „vlastnoručne“ vyriešiť. Môžete si viesť evidenciu svojich úspechov a neúspechov.

Výsledky uvádzame hlavne s cieľom ukázať rôzne metódy riešenia úloh.

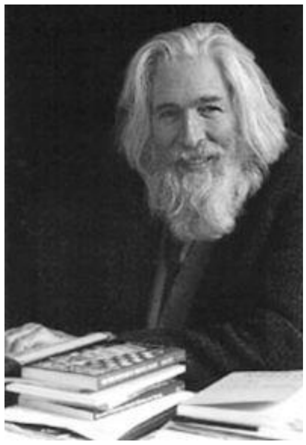
Vzhľadom na paralelu historického a osobnostného vývoja kognitívnych schopností (potvrdenú mnohými skúsenosťami z vyučovania) je preto táto téma schopná zaujať uvažujúcich žiakov a študentov už od veku 2. stupňa základnej školy. Dôležité ale je, aby sa (aspoň spočiatku) neskúmala formálne, na papieri, ale pri riešení zaujímavých a atraktívnych úloh v živých diskusiách pred angažovaným publikom. V prípade použitia pri vyučovaní preto jednoznačne odporúčame skupinovú organizáciu práce. Osvedčila sa nám metóda práce v 3- až 4-členných skupinách, v ktorých si musia žiaci najskôr vydiskutovať a dohodnúť jedno spoločné riešenie. Zástupcovia jednotlivých skupiniek ho potom prezentujú plenárne, pričom sa snažíme, aby slovo počas hodiny postupne dostalo čo najviac študentov.

Teoreticky mohol pytač v úlohe 1 čeliť dvom miestnostiam s princeznami, alebo dvom miestnostiam s tigrami.

**Motivácia 1**

Nasledujúca skupina úloh rozpráva o kráľovi, ktorého sídlo je preplnené tigrami (tie už dnes chová kdekto aj na Slovensku) a princeznami. Kráľ sa rozhodol pozvať na zámok zástupy pytačov a pripraviť pre nich test inteligencie. Na základe výsledku testu získajú buď doživotnú spoločnosť niektorej princeznej, alebo tigra. Test spočíva v nutnosti otvoriť dvere jednej z miestností, pričom v každej sa vždy skrýva *jedna bytosť*: buď princezná, alebo tiger. O obsahu miestností hovoria nápisy na ich dverách. Nápisy, spolu s informáciou o ich pravdivosti, umožňujú pytačovi správne rozhodnutie.

Inšpiráciu pre úlohy v tejto časti sme našli v knihách amerického matematika, logika a klaviristu Raymoda Smullyana [9], [10], [11].



| Úloha 1 | Kráľ ukázal prvému nápadníkovi dvoje dverí. V každej miestnosti za nimi mohol byť buď tiger, alebo princezná. Na ľavých dverách bol nápis „***V tejto miestnosti je princezná a v susednej tiger***“. Na pravých dverách bol nápis „***V jednej z miestností je princezná a v jednej z miestnosti je tiger***“. Pytač sa už chcel rozbehnúť k jedným z dverí, ale pre istotu sa ešte spýtal kráľa: „Sú nápisy pravdivé?“ Kráľ odpovedal: „***Jeden z nápisov je pravdivý a jeden nepravdivý***“. |
|---|---|

Predpokladáme, že v tomto okamžiku čitateľ už pozná riešenie a môže porovnať svoj postup s naším. Ten vychádza z myšlienky, že druhá veta vyplýva z prvej. Preto pokiaľ by bola pravdivá prvá veta, musí byť pravdivá aj veta druhá, a teda obidve. To však odporuje kráľovým informáciám o pravdivosti nápisov. (Tie budeme považovať za vždy pravdivé. Pokiaľ by kráľ nechcel v testoch postupovať poctivo, mohol prideľovať nápadníkom princezné alebo tigre priamo.) Preto je jedinou možnosťou, že pravdivá je druhá veta a nepravdivá prvá. Dve rozdielne bytosti do dvoch miestností, navyše v rozpore s prvou vetou, môžeme umiestniť len tak, že v prvej je tiger a v druhej princezná. Odporúčame preto vstúpiť do pravej miestnosti.

Uvádzame úlohy, na ktorých sa žiaci môžu naučiť rozmýšľať, logicky uvažovať a argumentovať. Takéto úlohy sme riešili už s žiakmi 5. ročníka základnej školy. Ich odvaha argumentovať a experimentovať bola často výrazne väčšia ako u našich vysokoškolákov.

| Úloha 2 | Druhý nápadník má na ľavých dverách nápis „***Aspoň v jednej z miestností je princezná***“ a na pravých „***V susednej miestnosti je tiger***“. Kráľ dodal, že buď sú oba výroky súčasne pravdivé, alebo sú oba súčasne nepravdivé. Kam treba ísť? |
|---|---|

Aj v tejto úlohe môžeme nájsť súvislosť tvrdení, ktorá nás privedie k výsledku. Skúsime však aj iný postup. Predpokladajme, že prvý nápis je pravdivý. Potom podľa kráľových podmienok musí byť pravdivý aj druhý. V ľavej miestnosti je preto tiger, a ak máme mať aspoň jednu princeznú, musí byť v pravej miestnosti. Ale skôr než do nej vstúpime, musíme overiť aj druhú možnosť. Ak by bol prvý nápis nepravdivý, musí byť nepravdivý aj druhý. Platia preto opaky, negácie oboch tvrdení. Podľa prvého preto v žiadnej izbe nie je princezná, a podľa druhého vo vedľajšej miestnosti nie je tiger, a teda tam musí byť princezná. Tieto dve požiadavky sa však očividne vzájomne vylučujú. Nie je preto možné, aby oba nadpisy boli nepravdivé, a máme preto len prvé riešenie. Na jeho základe by mal nápadník vstúpiť do pravej miestnosti.

Pri riešení prvých troch úloh sme videli tri možné (aj keď prelínajúce sa) prístupy k riešeniu:

- hľadanie zaujímavej súvislosti nápisov, ktorá nám uľahčí riešenie
- môžeme vyjsť z predpokladu pravdivosti jednotlivých nápisov
- môžeme predpokladať, aká bytosť sa nachádza v miestnostiach

| Úloha 3 | Aj tretí pytač mal pred sebou buď dva pravdivé, alebo dva nepravdivé nápisy. Ten na ľavých dverách znel „***V tejto miestnosti je tiger alebo je vedľa princezná***“ a na pravých „***V susednej miestnosti je princezná***“. Ktorú miestnosť si má vybrať? |
|---|---|

Skúsime ešte trochu iný prístup.

- Čo by sa stalo, ak by v ľavej miestnosti bol tiger? Tvrdenie na nej je potom pravdivé, a podľa kráľa potom musí byť pravdivý aj pravý nápis. Ten ale tvrdí, že v ľavej miestnosti je princezná. To je ale v spore s podmienkami, že v každej miestnosti je len jedna bytosť. Tiger v ľavej miestnosti preto vedie k sporu a určite v nej nie je. Ak budeme veriť, že úlohy sú zadané korektne, už teraz vieme, že v ľavej miestnosti je princezná. Túto dôveru však netreba preháňať. Navyše si chceme precvičiť tento postup riešenia, preto pokračujeme.

- Preveríme preto možnosť, že v ľavej miestnosti je princezná. O nápise na nej ešte nevieme veľa povedať, ale nápis na pravej miestnosti je teraz očividne pravdivý. Preto musí byť pravdivý aj ľavý nápis. Ide o disjunkciu, ktorej prvá časť je nepravdivá. Pravdivá preto musí byť jej druhá časť, a teda princezná je aj v pravej miestnosti. Nápadníkovi teda teraz nejde o život a môže si vybrať ľubovoľnú miestnosť.

Odporúčame čitateľovi, aby úlohy riešil všetkými tromi spôsobmi (čím si aj overí správnosť riešenia) a aby pozoroval rozdiely v jasnosti, dĺžke a zrozumiteľnosti argumentácie. Odporúčame podobne postupovať aj pri ďalších úlohách, v ktorých si ešte ukážeme ďalšie dva prístupy.

Pokiaľ pracujeme so žiakmi, môžeme ich vždy vyzvať, či niekto našiel aj iný postup riešenia. Po čase žiaci väčšinou objavia všetky možné spôsoby.

| | |
|---|---|
| **Motivácia 2** | V ďalších úlohách sa kráľ rozhodol zvýšiť náročnosť a dať tak väčšiu šancu tigrom. Zachované ostalo pravidlo, že v každej miestnosti je len jedna bytosť, princezná alebo tiger. (Môžu byť aj v oboch miestnostiach rovnaké.) Zmenil sa však spôsob určenia pravdivosti nápisov. Na ľavých dverách je pravdivý nápis práve vtedy, ak je za nimi princezná, a nepravdivý, ak je za nimi tiger. Pravý nápis funguje naopak. Ak je v pravej miestnosti tiger, je pravdivý, a ak princezná, je nepravdivý. |
| **Úloha 4** | Štvrtý pytač našiel na ľavých aj pravých dverách rovnaký nápis: „*V oboch miestnostiach je princezná*“.<br><br>Aké bytosti sú v miestnostiach? |

Ako sme sľúbili, ponúkneme ďalší, aj keď nie úplne nový postup. Bude ale viac „mechanický“. V princípe totiž máme len štyri možnosti, ako môžu byť miestnosti obsadené: P/P, P/T, T/P a T/T. Analyzujme každú z nich na zhodu s podmienkami zadania.

- Pokiaľ je v oboch miestnostiach princezná, ľavý nápis má byť pravdivý (a je), ale prvý nápis má byť nepravdivý, a to nie je. Takéto obsadenie miestností je v spore so zadaním a môžeme ho vylúčiť.
- Pri obsadení P/T je v ľavej miestnosti princezná a nápis na nej by mal byť pravdivý. To ale očividne nie je. (Sporný je aj nápis na pravej miestnosti, lebo ak v nej je tiger, mal by byť pravdivý.) Ani toto riešenie teda nie je správne, resp. prípustné.
- Obsadenie T/P vyžaduje, aby nápis na ľavej aj pravej miestnosti bol nepravdivý. A to naozaj je, lebo dve princezné v miestnostiach nie sú. Toto obsadenie miestností je možné, musíme však zistiť, či aj jediné.
- Obsadenie oboch miestností tigrami však vedie k sporu v prípade pravého nápisu, ktorý by mal byť pravdivý, a nie je.

Jediná možnosť teda je, že v ľavej miestnosti je tiger a v pravej princezná.

| | |
|---|---|
| **Úloha 5** | Piateho nápadníka na ľavých dverách čakal nápis „*Aspoň v jednej miestnosti je princezná*“ a na pravých „*Princezná je vo vedľajšej miestnosti*“. Aké bytosti sú v miestnostiach? |

Ukážeme tu posledný možný postup. Preberieme všetky možnosti pravdivosti nápisov. Pri bežnom značení vyzerajú takto: 0/0, 0/1, 1/0, 1/1.

- Ak sú oba nápisy nepravdivé, má byť podľa podmienok v ľavej miestnosti tiger a v pravej princezná. Potom je aspoň v jednej miestnosti princezná, a ľavý nápis je pravdivý. Tým sme dostali spor, a takéto hodnoty pravdivosti

nápisov nie sú možné.
- Ak je ľavý nápis nepravdivý a pravý pravdivý, v oboch by mal byť tiger. Potom ale pravý nápis nie je pravdivý, a opäť máme spor.
- Ak je pravdivý ľavý a nepravdivý pravý nápis, v oboch miestnostiach by mala byť princezná. Pravý nápis je ale potom pravdivý, čo je tiež spor.
- Ak sú oba nápisy pravdivé, v ľavej miestnosti by mala byť princezná a v pravej tiger. Oba nápisy v tomto prípade súhlasia s obsadením miestností, a máme teda jediné riešenie.

Ďalej už uvedieme len zadania úloh. V prípade, ak by ste chceli ako učitelia použiť túto tému pri vyučovaní, odporúčame predtým prerieširť úlohy všetkými uvedenými postupmi, aby ste vedeli pochopiť možné prístupy žiakov.

| | |
|---|---|
| **Úloha 6** | Nápis na ľavých dverách znie „*Vyber si ľubovoľnú miestnosť, je to jedno*“ a na pravých „*Princezná je vo vedľajšej miestnosti*“. |
| **Úloha 7** | Na ľavých dverách je nápis „*Poriadne sa zamysli, nie je jedno kam vstúpiš*“ a na pravých „*Lepšie je vojsť do susednej miestnosti*“. |
| **Úloha 8** | Ďalší nápadník bol veľmi netrpezlivý a vošiel v okamžiku, keď nápisy ešte len ležali pred kráľom a neboli umiestnené na dverách. Jeden znel „*V tejto miestnosti je tiger*“ a druhý „*V oboch miestnostiach je tiger*“. Nápadník chcel počkať, kým nápisy zavesia na správne dvere. Kráľ sa ale zamyslel a povedal, že úloha sa dá vlastne riešiť aj bez toho a nech svoju netrpezlivosť vykúpi väčšou náročnosťou úlohy. |

Tretí deň nápadníci vyberali z troch miestností.

| | |
|---|---|
| **Úloha 9** | V jednej z miestností je teraz princezná a v dvoch tiger. Z troch nápisov je najviac jeden pravdivý. Na ľavej miestnosti znel „*V tejto miestnosti je tiger*“, na prostrednej „*V tejto miestnosti je princezná*“ a na pravej „*Tiger je v prostrednej miestnosti*“. |
| **Úloha 10** | Aj teraz je v jednej z miestností princezná a v dvoch tiger. Nápis na miestnosti s princeznou je pravdivý, a z druhých dvoch je aspoň jeden nepravdivý. Na ľavých dverách stojí „*Tiger je v prostrednej miestnosti*“, na prostredných „*Tiger je v tejto miestnosti*“ a na ľavých „*Tiger je v ľavej miestnosti*“. |

Pri používaní logiky a jej pravidiel sa samozrejme nezaobídeme bez presných definícií, opisov a tvrdení. Už vyše 20 rokov so žiakmi základných škôl overujeme možnosti kultivovania argumentácie a hľadania správnych pravidiel logiky pomocou aktivít podobných tým, ktoré vymyslel pán Raymond Smullyan.

Máme skúsenosť, že študenti, ktorí prešli fázou tvorby vlastných teórií, sú neskôr schopní pracovať aj s náročnými textami, v ktorých nájdu logiku v omnoho abstraktnejšej forme. Ak by mal čitateľ potrebu pozrieť si tému logika spracovanú presnejšie a navyše so zameraním pre študentov informatiky, odporúčame mu text [4].

Veríme, že Vás (a možno aj Vašich žiakov) úlohy zaujali a zároveň ste si osviežili vedomosti o výrokoch. Koľkokrát ste našli princeznú a koľko krát ste boli zožratí tigrom?

## 2.4 Čo platí pre niekoho, pre nikoho a čo pre všetkých?

Pokiaľ sa od výrokového počtu posunieme na nasledujúcu hlbšiu úroveň skúmania matematickej logiky (alebo presného vyjadrovania o matematických objektoch a štruktúrach všeobecne), ocitneme sa v oblasti tzv. predikátového počtu. V ňom sa už podrobnejšie skúma štruktúra výroku, ktorý tu zvykneme nazývať formulou. Jej hlavnou úlohou je popisovať vlastnosti objektov z určitej množiny alebo súboru, ktorý nás zaujíma. Môže ísť o vlastnosť jedného objektu (číslo je deliteľné tromi, štvoruholník je štvorec, funkcia je párna), ich dvojice (číslo $n$ delí číslo $m$, strany sú rovnobežné, funkcie sú vzájomne inverzné), trojice (3 čísla sú strany pravouhlého trojuholníka) atď. Pre presné určenie významu formuly je potrebné určiť rozsah objektov, pre ktoré majú v nej uvedené vlastnosti platiť. K tomu sa vo formulách používajú tzv. ***kvantifikátory***. Prvý z nich, tzv. ***všeobecný*** a označovaný ∀, vyjadruje, že vlastnosť platí pre všetky objekty z uvažovaného súboru. Zápis $\forall x \in \mathrm{N}$ … čítame „***Pre každé x z N...***“, „***pre všetky prirodzené čísla x...***“ Druhý základný kvantifikátor označujeme znakom ∃ a nazývame ho ***existenčný***. Tento kvantifikátor vyjadruje, že existuje (aspoň jeden) objekt danej vlastnosti. Písmená, ktorými označujeme objekty a ktoré sú viazané kvantifikátormi, nazývame premenné. V zložitejších formulách sa premenných a aj potrebných kvantifikátorov nachádza veľa. Pre pochopenie významu formuly je dôležité aj poradie, v akom sú kvantifikátory uvedené.

**Úloha 1**

Dohodnime sa, že pre dvojicu prirodzených čísel $x, y$ budeme vlastnosť „***x je menšie ako y***“ označovať $x < y$.

Určte pravdivostnú hodnotu nasledujúcich formúl, líšiacich sa kvantifikátormi a ich poradím:

1. $(\forall x \in \mathrm{N})(\forall y \in \mathrm{N})\; x < y$
2. $(\forall x \in \mathrm{N})(\exists y \in \mathrm{N})\; x < y$
3. $(\exists x \in \mathrm{N})(\forall y \in \mathrm{N})\; x < y$
4. $(\exists x \in \mathrm{N})(\exists y \in \mathrm{N})\; x < y$
5. $(\forall y \in \mathrm{N})(\forall x \in \mathrm{N})\; x < y$
6. $(\forall y \in \mathrm{N})(\exists x \in \mathrm{N})\; x < y$
7. $(\exists y \in \mathrm{N})(\forall x \in \mathrm{N})\; x < y$
8. $(\exists y \in \mathrm{N})(\exists x \in \mathrm{N})\; x < y$

- V prvom a piatom tvrdení je iba zmenené poradie rovnakých kvantifikátorov. Táto zmena nespôsobí zmenu významu. Obe tvrdenia sú nepravdivé: dve prirodzené čísla sa môžu aj rovnať alebo môže prvé z nich byť väčšie. Preto nie je pravda, že pre všetky prirodzené $x$ a $y$ platí, že $x < y$.
- Podobne rovnocenné sú štvrté a ôsme tvrdenie, ktoré očividne platia. Nájsť dve prirodzené čísla, z ktorých prvé je menšie ako druhé, nie je problém.
- Druhé tvrdenie je pravdivé a hovorí, že ku každému prirodzenému číslu je možné nájsť od neho väčšie.
- Tretie tvrdenie naopak hovorí, že existuje prirodzené číslo, od ktorého sú všetky väčšie. Na prvý pohľad by túto vlastnosť mohla spĺňať $0$, ale, žiaľ, nie je menšia ako ona sama. Ak by vo formule bola ešte podmienka $x \neq y$, tvrdenie by platilo v tvare: $(\exists x \in \mathrm{N})(\forall y \in \mathrm{N})\; x \neq y \Rightarrow x < y$.
- Šieste tvrdenie hovorí, že ku každému prirodzenému číslu nájdeme menšie. To nie je pravda, lebo pre najmenšie číslo $0$ už menšie neexistuje.
- Neplatí ani siedme tvrdenie, podľa ktorého existuje prirodzené číslo, od ktorého sú všetky menšie.

**Úloha 2**

Odporúčame čitateľovi, aby určil pravdivostnú hodnotu formúl z úlohy 1 v prípade, keď ostrú nerovnosť „<“ nahradíme neostrou „≤“ a namiesto prirodzených čísiel budeme uvažovať množinu reálnych čísiel alebo uzavretý interval $\langle 0,1 \rangle$.

Pre jednoduchšie pochopenie významu formúl a skrátenie zápisu sa často definuje a používa aj kvantifikátor „***existuje práve jeden***“, značený ∃!.

Pri menej formálnom vyjadrovaní sa používajú aj spojenia „***platí pre najviac 3***“ alebo „***existuje aspoň 6***“.

Pre značne zjednodušenú, ale nám postačujúcu definíciu predikátového počtu ešte treba doplniť, že okrem pravdivostnej hodnoty formúl sa skúma ich vzájomná previazanosť, a to najmä možnosť odvodiť (dokázať) platnosť jednej zo súboru iných. Presne je opísaná aj „gramatika“ vytvárania formúl, ktorá znemožňuje vytvárať nezmyselné zhluky znakov.

## Chlapci a dievčatá

Viac či menej rigorózne formuly predikátového počtu sú jazykom, v ktorom sa zvyknú písomne vyjadrovať matematici a ich knihy. Prevod formúl do „ľudskejšieho“, menej formálneho jazyka a pochopenie ich obsahu je preto dôležitou schopnosťou pre tých, ktorí ich musia alebo potrebujú čítať. (Ako v tomto prípade chápeme spojku „alebo“?) K tejto skupine ľudí určite patria aj informatici. Navyše zovšeobecnením schopnosti čítať formuly sa dostaneme k univerzálnejšej schopnosti osvojenia si a pochopenia obsahu textu, písaného v umelom, štruktúrovanom a formálnom jazyku. Tomu (napriek snahám zaviesť konvencie o písaní komentárov atď.) zodpovedá štúdium zdrojových textov vytvorených programov, štruktúr databáz atď. Tu sme už plne v oblasti informatiky a jej vyučovania.

Ponúkame preto nasledujúcu sadu úloh na tréning tejto schopnosti. Ich formulácia je podľa našich skúseností dostatočne motivujúca a atraktívna, aby sa dala (po prispôsobení veku žiakov) použiť aj pri vyučovaní.

<table>
<tr><td>Motivácia<br><br>aPb</td><td>Písmenom $D$ označíme množinu dievčat, písmenom $C$ množinu chlapcov. Zápisom $d \in D, c \in C$ značíme, že $d$ je dievča a $c$ je chlapec.<br><br>Ďalej definujeme vlastnosť „a sa páči b“, ktorú budeme označovať „aPb“.<br><br>Chápeme ju ako „objektu a sa páči objekt b“, teda táto vlastnosť nie je symetrická.<br><br>Prvý objekt v nej vystupuje aktívne, druhý nemusí túto náklonnosť opätovať, prípadne o nej ani nevie.</td></tr>
<tr><td>Úloha 1</td><td>Prečítajte a potom skúste neformálne vysvetliť význam nasledujúcich formúl. Pokúste sa presne si uvedomiť rozdiely vo význame formúl (aj pri ich len drobných zmenách).<br><br>Určte, či sú uvedené tvrdenia pravdivé. Pokúste sa o to, aj keď na rozdiel od matematiky vo svete medziľudských vzťahov nie je vždy možné určiť pravdivostnú hodnotu jednoznačne.<br><br>1. $(\forall d \in D)(\exists c \in C)\ cPd$<br>2. $(\exists c \in C)(\forall d \in D)\ cPd$<br>3. $(\exists c \in C)(\forall d \in D)\ \neg cPd$<br>4. $(\exists d \in D)(\forall c \in C)\ cPd$<br><br>5. $(\exists d \in D)(\exists c \in C)\ (dPc \wedge cPd)$<br>6. $(\exists d \in D)(\forall c \in C)\ (dPc \wedge cPd)$<br>7. $(\exists d \in D)(\forall c \in C)\ (dPc \Rightarrow cPd)$<br>8. $(\exists d \in D)(\forall c \in C)\ (cPd \Rightarrow dPc)$<br>9. $(\exists c \in C)(\forall d \in D)\ (cPd \Rightarrow \neg dPc)$<br>10. $(\exists c \in C)(\forall d \in D)\ (dPc \wedge \neg cPd)$<br>11. $(\exists c \in C)(\forall d \in D)\ (dPc \Rightarrow \neg cPd)$<br>12. $(\exists d_1 \in D)(\forall c \in C)\ (\exists d_2 \in D)\ \big((d_1 \neq d_2) \wedge (d_1Pc \Rightarrow d_2Pc)\big)$</td></tr>
</table>

| | |
|---|---|
| | 13. $(\exists d_1 \in D)(\forall c \in C)(\exists d_2 \in D)\left((d_1 \neq d_2) \wedge (d_1 Pc \Rightarrow cPd_2)\right)$<br>14. $(\forall d_1 \in D)(\exists c \in C)(\forall d_2 \in D)\left((d_1 \neq d_2) \wedge (d_1 Pc \Rightarrow cPd_2)\right)$ |

Uvedieme len veľmi stručné formulácie riešení.

1: Každé dievča sa páči nejakému chlapcovi. 2: Niektorému chlapcovi sa páčia všetky dievčatá. 3: Niektorému žiadne. 4: Sú dievčatá, ktoré sa páčia všetkým chlapcom. 5: Existuje aspoň jedna dvojica, ktorá sa páči sebe navzájom. 6: Existuje dievča s dobrým odhadom: ak sa jej páči chlapec, páči sa aj ona jemu. 7: Existuje dievča, ktoré záujem je vždy opätovaný. 8: Existuje dievča, ktoré vždy opätuje záujem. 9: Existuje chlapec, ktorého záujem odradí každé dievča. 10: Existujú pekní chlapci, ktorým sa vôbec nepáčia dievčatá. 11: Existujú chlapci, ktorí (naschvál?) neopätujú záujem. 12: Existuje dievča, ktoré si vždy „vykoleduje“ súperku.13: Existuje úplná smoliarka, keď sa je niekto zapáči, jemu sa páči iná. 14: Každé dievča môže „netrafiť“, páči sa jej chlapec, ktorému sa páčia všetky ostatné.

**Úloha 2**

Skúste teraz naopak formulou zapísať nasledujúce tvrdenia (rozdelenie úloh medzi dievčatá a chlapcov necháme na vás).

1. Kde sa dvaja bijú, môže zvíťaziť tretí.
2. Vždy keď sa dvaja bijú, zvíťazí tretí.
3. Niektorí si miesto súperenia radšej nájdu niekoho iného.
4. Sú takí, ktorí sa zľaknú opätovaného záujmu a radšej „vycúvajú“.
5. Existujú „prehodené“ dvojice.
6. Miesto každého neopätovaného záujmu je možné nájsť vzťah vzájomný.

**Úloha 3**

Definujme ďalšiu vlastnosť „***aRb***“, ktorá znamená „***a chodí na rande s b***“. O tejto vlastnosti už budeme predpokladať, že je symetrická.

Navrhnite pre svojich žiakov (s použitím oboch vlastností) úlohy na pochopenie a vytváranie zaujímavých formúl.

## Logická polícia

Táto skupina úloh slúži na osvojenie si menej formálnych kvantifikátorov „***práve***“, „***aspoň***“ a „***najviac***“, a hlavne na skúmanie súvislostí celej skupiny výrokov, resp. formúl.

V úlohách budeme určovať pravdivosť a nepravdivosť navzájom súvisiacich a autoreferujúcich tvrdení, uvedených na spoločnom formulári. Ukážeme tiež, že pre niektoré formuláre nie je možné určiť, či sú tvrdenia pravdivé, alebo nie. Vety na takýchto formulároch nemožno pokladať za výroky.

Motivácia, uvedená v texte, bola vyskúšaná so žiakmi druhého stupňa základnej školy.

**Motivácia**

V meste Logikovo si obyvatelia zvykli zdobiť svoje domy tabuľami s rafinovanými sústavami výrokov. Chceli nimi upútať pozornosť okoloidúcich. Po čase však pri niektorých tabuliach dochádzalo k zápcham, hádkam, a vyskytli sa dokonca aj logické nešťastia. Mesto preto zriadilo logickú políciu, ktorá kontrolovala pravdivosť a korektnosť tvrdení na tabuliach.

Vašou úlohou bude pomáhať logickej polícii a určiť pre každú z tabuliek, ktoré výroky na nej sú (môžu byť) pravdivé a ktoré nie.

| Úloha 1 | Tabuľka obsahuje nasledujúcich 5 tvrdení:<br><br>1. <u>Na tejto tabuľke je práve jedno pravdivé tvrdenie.</u><br>2. <u>Na tejto tabuľke sú práve dve pravdivé tvrdenia.</u><br>3. <u>Na tejto tabuľke sú práve tri pravdivé tvrdenia.</u><br>4. <u>Na tejto tabuľke sú práve štyri pravdivé tvrdenia.</u><br>5. <u>Na tejto tabuľke je práve päť pravdivých tvrdení.</u><br><br>Zistite, ktoré z týchto tvrdení môžu byť pravdivé a ktoré nepravdivé! Ako tvrdenia spolu navzájom súvisia? |
|---|---|

Ako pomôcku uvedieme, že princíp riešenia sa nezmení, ak by tvrdenia pokračovali do iného celkového počtu, napr. 10. Zmena by však nastala, ak by tabuľka neobsahovala prvé tvrdenie, alebo naopak pred prvé tvrdenie by pribudlo ešte nulté „Na tejto tabuľke je práve nula pravdivých tvrdení."

Pokiaľ ste si premysleli aj tieto varianty tabuľky s iným počtom riadkov, porovnajte svoj postup s naším. Kľúčom k elegantnému riešeniu je uvedomenie si súvislosti tvrdení. Keďže hovoria o presnom počte pravdivých tvrdení, každé dva z nich sa vzájomne vylučujú. Ak by ľubovoľné z nich platilo, ostatné už musia byť nepravdivé. Z toho vyplýva, že na tabuľke môže byť najviac jedno pravdivé tvrdenie. Ak by bolo pravdivé práve jedno, bude to očividne prvé tvrdenie (lebo hovorí, že pravdivé je jedno tvrdenie), ostatné sú nepravdivé.

Druhé riešenie je, že všetky tvrdenia sú nepravdivé. Treba si vždy overiť, že tieto (jediné možné) riešenia sú naozaj korektné, teda určená pravdivosť tvrdení zodpovedá aj ich obsahu a skutočnému stavu. Varianty zadania s odobratým prvým, resp. pridaným nultým tvrdením vždy „pokazia" jedno z riešení. Čitateľovi ešte odporúčame premyslieť si varianty zadania, ak slovo „pravdivé" zameníme za „nepravdivé".

| Úloha 2 | Význam a dôležitosť logickej polície si uvedomíme pri analýze pravdivosti tvrdenia na nasledujúcej, na prvý pohľad jednoduchej tabuľke: <u>Na tejto tabuľke je práve jedno nepravdivé tvrdenie.</u> |
|---|---|

Predpoklad o pravdivosti aj predpoklad nepravdivosti tvrdenia na tabuľke z úlohy 2 vedie vždy k sporu. Tvrdenie na tabuľke preto nie je výrokom. V meste Logikovo je vyvesenie tabúľ obsahujúcich tvrdenia, ktoré nie sú výroky, obyvateľom mesta úradne zakázané. Polícia musí takéto tabule odstraňovať.

| Úloha 3 | Teraz treba určiť pravdivosť výrokov na nasledujúcej tabuľke:<br><br>1. <u>Na tejto tabuľke je aspoň jedno pravdivé tvrdenie.</u><br>2. <u>Na tejto tabuľke sú aspoň dve pravdivé tvrdenia.</u><br>3. <u>Na tejto tabuľke sú aspoň tri pravdivé tvrdenia.</u><br>4. <u>Na tejto tabuľke sú aspoň štyri pravdivé tvrdenia.</u><br>5. <u>Na tejto tabuľke je aspoň päť pravdivých tvrdení.</u><br><br>Aká je v tomto prípade kľúčová súvislosť tvrdení? |
|---|---|

Použitie slova „aspoň" mení spôsob previazania tvrdení. Pokiaľ niektoré z nich platí, platia aj všetky predchádzajúce. Naopak, ak je niektoré nepravdivé, nepravdivé sú aj všetky nasledujúce. Všetky riešenia teda musia mať rovnaký „tvar": po určitom počte (iba) pravdivých tvrdení pokračuje súvislý úsek nepravdivých tvrdení. Overením zistíme, že ***všetkých 6*** takýchto riešení je korektných. Môžu teda byť nepravdivé všetky tvrdenia, pravdivé len prvé tvrdenie, pravdivé len prvé dve atď., až po prípad pravdivosti všetkých piatich tvrdení.

Opäť veľmi zaujímavý variant zadania dostaneme, keď pridáme nultú vetu „Na tejto tabuľke je aspoň nula pravdivých tvrdení“. Táto veta je určite pravdivá a vyplýva z nej riešenie, ktoré študenti nazvali „logické domino“. Pokiaľ naopak zo zadania odstránime poslednú vetu, podobné „domino“ môžeme spustiť od posledného tvrdenia.

| | |
|---|---|
| **Úloha 4** | Na otestovanie bdelosti logickej polície ponúkame teraz na určenie pravdivostí tabuľku s nasledujúcimi dvomi tvrdeniami:<br><br>1. Na tejto tabuľke sú všetky tvrdenia nepravdivé.<br>2. Na tejto tabuľke sú všetky tvrdenia pravdivé.<br><br>Ide o povolenú tabuľku? Ak nie, ktorá veta z nej je „hlavný páchateľ“? |
| **Úloha 5** | Ďalšia tabuľka je nám už určite povedomá, zmenil sa však typ kvantifikátora:<br><br>1. Na tejto tabuľke je najviac jedno pravdivé tvrdenie.<br>2. Na tejto tabuľke sú najviac dve pravdivé tvrdenia.<br>3. Na tejto tabuľke sú najviac tri pravdivé tvrdenia.<br>4. Na tejto tabuľke sú najviac štyri pravdivé tvrdenia.<br>5. Na tejto tabuľke je najviac päť pravdivých tvrdení.<br><br>Ako je to s pravdivosťou týchto viet? |

Aj keď drobná zmena z „aspoň“ na „najviac“ sa nezdá zásadná, úloha je ťažšia a má len jedno riešenie. Súvis tvrdení je podobný (ale opačný) ako v úlohe 3. Preto musí riešenie obsahovať najskôr (aj prázdny) úsek nepravdivých tvrdení a potom (aj prázdny) súvislý úsek pravdivých tvrdení. Ak začneme preberať jednotlivé možnosti a zisťovať súlad pravdivosti tvrdení s ich obsahom a skutočnou situáciou, väčšina sa ukáže ako nekorektných. Pokiaľ by sme dokonca zo zadania ubrali poslednú vetu (alebo pridali ďalšie do ľubovoľného párneho počtu), získame zakázané tabuľky!

V tomto okamžiku veríme, že ste schopní vymýšľať a riešiť ďalšie obdobné tabuľkové úlohy. Ponúkame ešte jeden námet na zamyslenie. „Zakázané tvrdenia“, ktorým nemožno určiť pravdivostnú hodnotu, nazveme spornými a povolíme ich používanie.

| | |
|---|---|
| **Úloha 6** | Ako by ste teraz vyhodnotili tvrdenia z nasledujúcej tabuľky?<br><br>1. Na tejto tabuľke sú všetky tvrdenia nepravdivé.<br>2. Na tejto tabuľke sú všetky tvrdenia pravdivé.<br>3. Na tejto tabuľke je aspoň jedno tvrdenie sporné. |

## 2.5 Kto musí a kto potrebuje dokazovať?

Dôvod, prečo robiť dôkaz, môže byť snaha presvedčiť sa o správnosti tvrdenia, ak to nie je úplne jasné. Táto potreba rastie, ak sme už zažili pár vážnych omylov alebo narazíme na problém, ktorý nemá riešenie. Podozrenie, že hľadaný matematický objekt neexistuje (napríklad euklidovská konštrukcia rozdelenia uhla na tretiny), sa dá potvrdiť len všeobecnou úvahou, dôkazom. Ďalším dôvodom môže byť snaha vysvetliť a objasniť tvrdenie, ukázať, ako vyplýva z iných tvrdení a ako navzájom súvisia. Dôkaz slúži na lepšie pochopenie tvrdenia a budovanej teórie. Konštruktívny dôkaz dáva návod, ako niečo vyrobiť, vypočítať. Existenčný dôkaz nám tento návod nedáva, ale zato máme istotu o existencii určitého objektu a zmysluplnosti jeho ďalšieho skúmania. (Samozrejme, pre matematikov nutnosť dokazovania vyplýva aj z mnohých ďalších profesných a vnútorných dôvodov.)

### Súboj, hádka, polemika, diskusia, argumentácia

Malé deti sa postupne učia, ako získať hračku, ktorú má niekto iný. Najprv ju jednoducho vytrhnú druhému z ruky. Po pár skúsenostiach už berú hračky iba slabším. Potom prídu na rad výchovné zásahy rodičov a sociálneho prostredia, v ktorom vyrastajú. Po čase sa deti už dokážu pohádať, neskôr dokonca dohodnúť. Asi najvyššie štádium je schopnosť argumentovať a počúvať argumenty iných. V školskej praxi by sme mali kultivovať hlavne dve posledne menované schopnosti.

Túto úlohu sme vybrali zo zbierky [1], ktorú pripravili doktorandi MFF v Bratislave.

| Úloha | |
|---|---|
| | Slávny učiteľ rétoriky a umenia argumentácie Protagoras vyučoval žiaka menom Euatlos. Dohodli sa, že Euatlos zaplatí Protagorovi polovicu peňazí za vyučovanie hneď a druhú až potom, keď vyhrá prvý súdny spor. Avšak po vyučení Euatlos žiadny súdny spor neviedol a Protagorovi nič nezaplatil.<br><br>Protagoras ho zažaloval, usudzujúc takto: Euatlos mi musí zaplatiť, či spor prehrá alebo vyhrá. Ak prehrá, donúti ho súd, ak vyhrá, tak bude musieť splniť našu dohodu. Euatlos zase uvažoval takto: Či spor vyhrám alebo prehrám, nebudem musieť zaplatiť. Ak vyhrám, tak súd rozhodol, že platiť nemám, ak prehrám, tak podľa našej dohody platiť nemusím. |

Na koho stranu by ste sa priklonili vy? Ako mali sudcovia rozhodnúť?

V informatike o správnosti algoritmov a programov vo veľkej miere rozhodujú ich používatelia. Reklamáciami pomáhajú pri hľadaní a odstraňovaní chýb, sťažnosťami a pripomienkami odhaľujú nepresné funkcie. Pri programoch pre dispečerov železničnej dopravy, riadenie raketoplánu alebo finančné operácie veľkej banky sa správnosť algoritmov, samozrejme, overuje oveľa dôkladnejšie a vopred. Korektnosť takýchto algoritmov sa najskôr snažia dosiahnuť a dokázať ich tvorcovia. Nasleduje dlhodobé testovanie v simulovaných podmienkach. Zároveň zdrojové texty analyzujú a kontrolujú nezávislí experti, ktorí im nakoniec udelia svoj certifikát. Iný význam slova správnosť hodnotí, či algoritmus naozaj vykonáva to, čo chcel jeho zadávateľ.

## 2.6 Logické spojky v informatike

Predpoklady matematických tvrdení a viet sú vlastne podmienky, ktoré musia byť splnené, aby tvrdenie platilo. V programoch sa takéto podmienky vyskytujú v rozhodovacích príkazoch. Program potom vykonáva nasledujúce príkazy len v prípade, že sú podmienky splnené.

| Príklad 1 | |
|---|---|
| | Nasledujúca časť programu vykoná `Prikaz` , iba ak je číslo `x` väčšie ako 3.<br><br>`Ak x > 3 potom Prikaz;` |

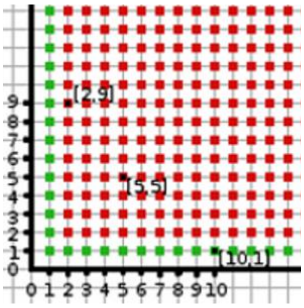
Rovnako, ako sa vo výrokovej logike často používajú zložené výroky, pri programovaní sa často používajú zložené podmienky. Ukážeme si základné logické spojky v podmienenom príkaze.

| Príklad 2 | `if ( x > 3 ) and ( x < 8 ) then Prikaz;` |
|---|---|
| **Úloha 1** | Pre aké `x` by sa vykonal `Prikaz` , ak by sme v predchádzajúcom príklade nahradili `and` za `or`? |

| | |
|---|---|
| **Príklad 3** | `if ( x > 3 ) or ( x = 3 ) then Prikaz;` |
| **Úloha 1** | Pre aké `x` by sa vykonal `Prikaz` , ak by sme v predchádzajúcom príklade nahradili `or` za `and`? |

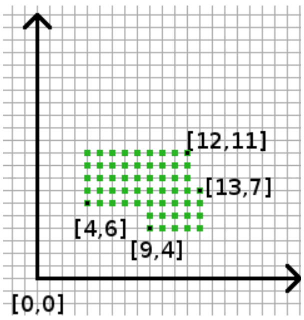
## Vymedzenie skupiny stromov danej vlastnosti v nekonečnom sade

V téme nekonečný sad v prvom module sme mrežové body v prvom kvadrante nazvali stromami.



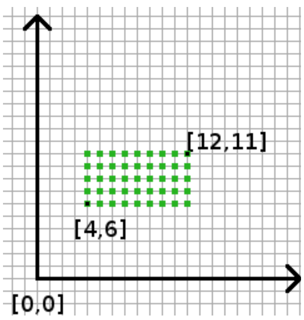

| | |
|---|---|
| **Úloha 2** | V ovocnom sade vyznačte krajné stromy zelenou farbičkou a vnútorné stromy červenou farbičkou.<br><br>Napíšte podmienku, ktorá pre dané súradnice stromu zistí, či je strom zelený (či je na kraji).<br><br>Napíšte podmienku, ktorá pre dané súradnice stromu zistí, či je strom červený (či je mimo kraja). |

Ak ste podmienky napísali tak, ako sme predpokladali, práve sa vám podarilo vyrobiť negáciu podmienky, pretože červené stromy sú všetky tie, ktoré nie sú zelené.




| | |
|---|---|
| **Aktivita 1** | Na obrázku sadu vyznačte náhodne tri stromy. Napíšte *podmienku* pre `if podmienka then prikaz;` tak, aby ste vybrali práve tieto stromy. Pravdepodobne budete potrebovať použiť logické spojky `and` a `or`. |
| **Aktivita 2** | V predchádzajúcej aktivite si skúste vybrať približne sto stromov v rôznych ľahko opísateľných útvaroch, akými sú štvorec, obdĺžnik, či pás. Skúste podmieneným príkazom opísať aj viac obdĺžnikov naraz.<br><br>Ak sa Vám to zdá ľahké, skúste príkazom opísať aj kružnicu s daným stredom a polomerom, či trojuholníky. |

Pre lepšie pochopenie spájania podmienok logickými spojkami si vyriešime jednu úlohu z Aktivity 2.




| | |
|---|---|
| **Zadanie** | Na obrázku vyznačte všetky tie stromy, ktoré spadajú do zadaného obdĺžnika. Nech ľavý dolný roh obdĺžnika je v bode [4,6] a pravý horný roh v bode [12,11].<br><br>Napíšte *podmienku* pre `if podmienka then prikaz;` tak, aby sa `príkaz` vykonal práve pre tieto stromy. |

| | |
|---|---|
| **Riešenie** | V danom obdĺžniku sa strom nachádza, ak jeho $x$-ová súradnica je v obdĺžnikovom rozpätí $x$-ových súradníc, **a** tiež $y$-ová súradnica je v obdĺžnikovom rozpätí $y$-ových súradníc.<br><br>To, že je súradnica $x$ v rozpätí $x$-ových súradníc znamená, že je medzi dvoma hodnotami - menšou a väčšou. V našom prípade je teda $x$ väčšie či rovné ako $4$ **a** menšie či rovné ako $12$. Obdobne to platí pre súradnicu $y$.<br><br>`if ((x >= 4) and (x <= 12)) and`<br>`((y >= 6) and (y <= 11)) then prikaz;` |

Uvedomme si, že podmienka väčšie alebo rovné sa vo veľa jazykoch zapisuje ako <=. V skutočnosti je to skrátený tvar pre 2 podmienky spojené spojkou **or**. Takže x <= y sa dá zapísať aj ako (x < y) **or** (x = y).

V riešení sú pre programovací jazyk dva páry zátvoriek zbytočné, nie sú však na škodu. Zvyšujú čitateľnosť tým, že obsah prvej zátvorky sa vzťahuje na súradnicu $x$ a obsah druhej na súradnicu $y$.

## Podmienky a predpoklady v algoritmoch

Vráťme sa k programovaniu algoritmov. Väčšinou má proces programovania podmienky dve fázy - sformulovanie si podmienky vo svojom jazyku a prepis do reči programovacieho jazyka. V prvej fáze často nastáva zámena logických spojok alebo zlé znegovanie podmienky. V druhej fáze okrem iného študenti nerozmýšľajú nad *prioritou operátorov* (poradie vyhodnotenia operácií), takže nesprávne uzátvorkujú podmienku. Samozrejme, chyby závisia od úlohy. Spomenuté chyby však patria k tým častým.

Pri zistení chyby študenti často bezmyšlienkovite prepisujú všetky logické spojky a relačné znamienka.

| | |
|---|---|
| **Úloha 3** | Na číselnej osi vyznačte interval $\langle -5, 11 \rangle$. Napíšte časť programu, ktorá pre zadané číslo $c$ zistí, či sa $c$ nachádza vnútri alebo mimo daného intervalu.<br><br>To isté spravte aj pre nie pevný interval. Hranice intervalu tento krát nebudú $-5$ a $11$, ale premenné $x$ a $y$. Môžete predpokladať, že $x \leq y$. |
| **Úloha 4** | Na číselnej osi máme dva intervaly $\langle a, b \rangle$ a $\langle c, d \rangle$. Napíšte program, ktorý zistí vzájomnú polohu týchto intervalov, t. j. či majú spoločný prienik, a ak áno, či sa jeden z nich nachádza celý v druhom. |

Teraz sme si skúsili podmienky v jednorozmernom súradnicovom systéme - číselnej osi. Podmienky v dvojrozmernom súradnicovom systéme budú zložitejšie, pretože sa budeme musieť pýtať na oba rozmery a podmienky znova spájať logickými spojkami.

| | |
|---|---|
| **Úloha 5** | Majme obdĺžnik so stranami rovnobežnými s osami súradnicového systému. Jeho ľavý horný roh má súradnice $[-1, 7]$ a pravý dolný roh súradnice $[8, 4]$. Napíšte program, ktorý pre zadané súradnice $[x, y]$ zistí, či sa bod nachádza vnútri alebo vonku z obdĺžnika. |

Zložitejší príklad si teraz ukážkovo vyriešime.

| Zadanie | Majme obdĺžnik so stranami rovnobežnými s osami súradnicového systému. Jeho ľavý horný roh má súradnice $[-1,7]$ a pravý dolný roh súradnice $[8,4]$. Majme úsečku, rovnobežnú s niektorou súradnicovou osou, s krajnými bodmi $[x_1,y_1]$ a $[x_2,y_2]$. Napíšte program, ktorý zistí, či sa úsečka nachádza vnútri obdĺžnika, vonku, alebo ho pretína. |
|---|---|

Naozaj platí, že aby bola celá úsečka zo zadania mimo obdĺžnika, tak musí byť celá vľavo, vpravo, pod alebo nad obdĺžnikom? Skúste si nakresliť obdĺžnik s rôznymi polohami úsečky.

**Riešenie**

Ak sú oba krajné body úsečky v obdĺžniku, potom je celá úsečka v obdĺžniku. Ak je úsečka celá pod obdĺžnikom, nad obdĺžnikom, vľavo od neho alebo vpravo od neho, úsečka je mimo obdĺžnika. Ak neplatí ani jedna z možností, úsečka obdĺžnik pretína.

```
if (je_v_obdlzniku(bod1) and
    je_v_obdlzniku(bod2)) then
  vnutri()
else
  if (oba_body_vlavo() or
      oba_body_vpravo() or
      oba_body_pod() or
      oba_body_nad()) then
    vonku()
  else
    pretina();
```

Po rozpísaní máme nasledovný výsledok:

```
if (((x1 >= -1) and (x1 <= 8)) and
     ((y1 >= 4) and (y1 <= 7))) and
   (((x2 >= -1) and (x2 <= 8)) and
     ((y2 >= 4) and (y2 <= 7))) then
  vnutri()
else
  if ((x1 < -1) and (x2 < -1)) or
     ((x1 > 8) and (x2 > 8)) or
     ((y1 < 4) and (y2 < 4)) or
     ((y1 > 7) and (y2 > 7)) then
  vonku()
else
  pretina();
```

Na precvičenie si skúste vyriešiť nasledujúce príklady.

Pomôcka: Pre aké hodnoty z je splnená podmienka `(z>='a') and (z<='z')`?

| | |
|---|---|
| **Úloha 6** | V poli `P` sú znaky. Od `P[0]` po `P[k]`. Napíšte program, ktorý v ňom zamení malé písmená za veľké a naopak. |
| **Úloha 7** | Napíšte program, ktorý zistí, či sa bod nachádza v štvorci so stranou veľkosti $4$ a ľavým rohom v bode [2,7]. Úlohu vyriešte aj všeobecne pre stranu veľkosti $d$ a ľavý roh v bode $[x,y]$. |
| **Úloha 8** | Napíšte program, ktorý zistí, či sa bod nachádza v kružnici s polomerom $3$ a stredom v bode $[1,-6]$. Úlohu vyriešte aj všeobecne pre polomer $r$ a stred v bode $[x,y]$. |
| **Úloha 9** | Napíšte program, ktorý zistí, či sa bod $[x,y]$ nachádza pod alebo nad grafom funkcie $6x^2+11x-7$ , teda pod alebo nad bodom $[x,6x^2+\ 11x-7]$. |

# Čo sme sa naučili v tomto module

## Zhrnutie

Študijný materiál obsahuje kapitoly z teórie čísel, ktoré sú použiteľné pre učiteľov informatiky ako zdroj motivačných úloh pre programovanie. V tejto časti je ukázané, ako s číslami pracujú počítače a sú predvedené algoritmy na vyhľadávanie špeciálnych čísel. Ďalej je tu zahrnuté učivo o deliteľoch a násobkoch. Jedna časť je venovaná zvyškom a modulárnej aritmetike. Ďalej sa venujeme prvočíslam a rozkladu čísiel na súčin prvočísel. Záver kapitoly je venovaný praktickému využitiu uvedených pojmov a spomenuté sú tu niektoré otvorené problémy z teórie čísel. V časti logika sú zaradené aktivity, ktoré napomáhajú rozvoju logického myslenia a upozornenie na nezmyselnosť vyučovania matematiky ako zbierky faktov a pravidiel bez toho, aby im študenti porozumeli najskôr na konkrétnych úlohách. Na príkladoch v poslednej časti je ilustrované využitie logiky v informatike.

## Preverenie výstupných vedomostí

Poslucháči vytvoria skupiny po dvoch alebo troch účastníkoch a vypracujú spoločne zadanie problému, o ktorom si myslia, že by jeho riešenie vedeli ako informatici využiť. Tento problém by mal byť taký, že poslucháči, teda zadávatelia problému, nepoznajú jeho riešenie, alebo majú niekoľko rôznych hypotéz o možnom riešení úlohy.

## Celkové hodnotenie predmetu

Toto je druhý z troch modulov predmetu. V prvom účastníci za riešenie zadania mohli získať 10 bodov, v tomto module to bude 50 bodov, v treťom, poslednom to bude 40 bodov. Na absolvovanie celého predmetu bude potrebných aspoň 51 bodov.

# Literatúra a použité zdroje


[1] Bálint, V., Bálintová, M., Bednářová, S., Višňovská, J., Závadová, I., Žabka, J., (2000), *Logika I*, KZDM MFF UK Bratislava: TEMPUS AC_JEP-13101-98

[2] Graham,R.L., Knuth,D.E., Patashnik,O. (1994), *Concrete Mathematics*, Massachusetts: Addison-Wesley, ISBN 0-201-55802-5

[3] Černek, P., Kubáček, Z., Žabka, J. (2006), *Návrhy učebných textov pre stredné školy* (nevyužité časti)

[4] Krajči, S. (2008), *Symbolická logika*, UPJŠ Košice, 2008, ISBN: 978-80-7097-707-1 *http://ics.upjs.sk/~krajci/skola/vyucba/ucebneTexty/logika.pdf*

[5] Kubáček, Z., Černek, P., Žabka, J. a kol.(2008), *Matematika a svet okolo nás* (Zbierka úloh), Bratislava: ISBN 978-80-969950-1-1

[6] Kubáček, Z., (2008), *Príbuzenské vzťahy a logika,* Setkání učitelů matematiky všech typů a stupňů škol, Srní na Šumavě, ISBN 978-80-86843-22-3

[7] Meyer, A., R. (2007) *Mathematics for Computer Science*, Massachusetts Institute of Technology, Lecture notes, *http://people.csail.mit.edu/meyer/6042-notes-spring08.pdf*

[8] Singh, S. (2002) *Kniha kódů a šifer*, Argo Dokořán, Praha, ISBN 80-86569-18-7

[9] Smullyan, R. (2003) *Navěky nerozhodnuto*, ACADEMIA, Praha: ISBN 80-200-1068-8

[10] Smullyan, R., M. (1986) *Jak se jmenuje tahle knížka?*, MLADÁ FRONTA, Praha

[11] Smullyan, R. (1985) *Princessa ili tigr?*, MIR, Moskva

[12] Mojžiš, M. (2006), *Koľko je prvočísel?,* Týždeň, č.7, str. 57, ISSN 1336-653X

[13] Znám, Š. (1977), Teória čísel, Alfa, Bratislava

[14] Foríšek, M. (2005) *Representation of Integers and Reals*, Algorithm competition tutorial published by TopCoder, Inc. http://www.topcoder.com/tc?module=Static&d1=tutorials&d2=integersReals

[15] Tarski, A. (1966) *Úvod do logiky a metodologie deduktivních věd*, Academia Praha

[16] Kršák, E. (2001) *Elektronický podpis*, konferencia Systémová integrácia 2001, Žilina, ISBN 80-7100-880-X

Tento študijný materiál vznikol ako súčasť národného projektu Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika v rámci Aktivity „Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ“.

Autori © RNDr. Katarína Bachratá, PhD.
RNDr. Hynek Bachratý, PhD.
Mgr. Peter Cimmermann, PhD.
Mgr. Júlia Šišková
RNDr. Michal Winczer, PhD.

Názov Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

Podnázov Matematika pre učiteľov informatiky 2

Študijný materiál prešiel recenzným pokračovaním.

Recenzenti doc. RNDr. Stanislav Krajči, PhD.
doc. RNDr. Zbyněk Kubáček, CSc.

Počet strán 40

Náklad 300 ks

**Prvé vydanie, Bratislava 2009**



Vydal Štátny pedagogický ústav, Pluhová 8, 830 00 Bratislava, v súčinnosti s Univerzitou Pavla Jozefa Šafárika v Košiciach, Univerzitou Komenského v Bratislave, Univerzitou Konštantína Filozofa v Nitre, Univerzitou Mateja Bela v Banskej Bystrici a Žilinskou univerzitou v Žiline

Vytlačil BRATIA SABOVCI, s r.o., Zvolen

**ISBN 978-80-89225-97-2**