

Univerzita Karlova v Praze  
Matematicko-fyzikální fakulta

## DIPLOMOVÁ PRÁCE



Mgr. Andrea Živčáková

## Dělitelnost pro nadané žáky středních škol

Katedra didaktiky matematiky

Vedoucí diplomové práce: doc. RNDr. Jarmila Robová, CSc.

Studijní program: Učitelství

Studijní obor: Učitelství matematiky pro SŠ v kombinaci s odbornou matematikou

Praha 2014

Rada by som na tomto mieste pod'akovala vedúcej diplomovej práce, doc. RNDr. Jarmile Robovej, CSc., za vypísanie témy, poskytnuté konzultácie, cenné rady a podnety, ktoré prispeli k vypracovaniu práce.

Ďakujem tiež svojim rodičom a súrodencom za podporu po celú dobu štúdia.

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne .....

Andrea Živčáková

Názov práce: Dělitelnost pro nadané žáky středních škol

Autor: Mgr. Andrea Živčáková

Katedra: Katedra didaktiky matematiky

Vedúci diplomovej práce: doc. RNDr. Jarmila Robová, CSc.

**Abstrakt:** Táto práca je výukový text určený žiakom stredných škôl. Jej cieľom je naučiť žiakov stredných škôl riešiť typické príklady o deliteľnosti, ktoré sa často vyskytujú v matematických korešpondenčných seminároch a v matematickej olympiáde. Čitateľ si v práci pripomene základné pojmy z deliteľnosti (napr. prvočíslo, deliteľ, násobok), zoznámi sa s kritériami deliteľnosti číslami 2 až 20, diofantickými rovnicami a tiež praktickými použitiami prvočísel v reálnom živote. Práca obsahuje jednú celú kapitolu príkladov a cvičení.

**Kľúčové slová:** deliteľnosť, prirodzené číslo, diofantické rovnice, prvočíslo

Title: Divisibility for talented students of secondary schools

Author: Mgr. Andrea Živčáková

Department: Department of Mathematics Education

Supervisor: doc. RNDr. Jarmila Robová, CSc.

**Abstract:** This thesis is an educational text for high school students. It aims to teach them how to solve typical problems concerning divisibility found in mathematical correspondence seminars and mathematical olympiads. Basic notions from the theory of divisibility are recalled (e.g. prime numbers, divisors, multiples). Criteria of divisibility by 2 to 20 are introduced, as well as diophantine equations and practical applications of prime numbers in real life. One whole chapter is dedicated to problems and exercises.

**Keywords:** divisibility, natural number, diophantine equations, prime number

# Obsah

<b>Zoznam použitých symbolov</b>	<b>3</b>
<b>Úvod</b>	<b>4</b>
<b>1 Základné pojmy a vety</b>	<b>5</b>
1.1 Značenie . . . . .	5
1.2 Logika . . . . .	6
1.2.1 Výroky . . . . .	6
1.2.2 Zložený výrok a logické spojky . . . . .	7
1.3 Typy dôkazov . . . . .	8
1.4 Číselné množiny . . . . .	10
1.5 Rozvinutý zápis prirodzeného čísla . . . . .	11
1.6 Mocniny a odmocniny . . . . .	11
1.7 Kombinačné čísla . . . . .	13
1.8 Základné pojmy deliteľnosti . . . . .	16
1.9 Euklidov algoritmus . . . . .	21
1.10 Rozklad zloženého čísla na súčin prvočísel . . . . .	22
<b>2 Kritéria deliteľnosti</b>	<b>26</b>
2.1 Úvod do problematiky . . . . .	26
2.2 Kritéria deliteľnosti číslami 2 až 10 . . . . .	27
2.3 Kritéria deliteľnosti prvočíslami 11 až 20 . . . . .	31
<b>3 Diofantické rovnice</b>	<b>35</b>
3.1 Lineárne diofantické rovnice . . . . .	35
3.1.1 Lineárne diofantické rovnice s dvoma neznámymi . . . . .	36
3.2 Diofantické rovnice druhého stupňa . . . . .	39
3.2.1 Kvadratické diofantické rovnice s dvoma neznámymi . . . . .	39
3.3 Slovné úlohy . . . . .	41
<b>4 Prvočísla a ich využitie v reálnom živote</b>	<b>42</b>
4.1 Prvočísla . . . . .	42
4.1.1 Eratosthenovo sito . . . . .	42
4.1.2 Ulamova špirála . . . . .	44
4.1.3 Euklidove vety . . . . .	45
4.1.4 Špeciálne typy prvočísel . . . . .	45
4.1.5 Kritéria prvočíselnosti . . . . .	47
4.2 Aplikácie prvočísel . . . . .	47
4.2.1 Prvočíslo 11 . . . . .	47

4.2.2	Metóda RSA . . . . .	48
<b>5</b>	<b>Príklady na deliteľnosť a prvočísla</b>	<b>50</b>
5.1	Test . . . . .	50
5.2	Príklady a cvičenia na deliteľnosť . . . . .	52
5.2.1	Príklady na deliteľnosť . . . . .	52
5.2.2	Dôkazové príklady . . . . .	59
5.3	Úlohy z olympiád a matematických korešpondenčných seminárov .	63
<b>Záver</b>		<b>68</b>

# Zoznam použitých symbolov

$\mathbb{N}$	množina všetkých prirodzených čísel
$\mathbb{N}_0$	množina všetkých prirodzených čísel s nulou
$\mathbb{Z}$	množina všetkých celých čísel
$\mathbb{Q}$	množina všetkých racionálnych čísel
$\mathbb{R}$	množina všetkých reálnych čísel
$=$	rovná sa
$\neq$	nerovná sa
$\doteq$	je po zaokruhlení rovné
$<$	menšie ako
$>$	väčšie ako
$\leq$	menšie alebo rovná sa
$\geq$	väčšie alebo rovná sa
$\sum$	sumačný znak
$\wedge$	konjunkcia
$\vee$	disjunkcia
$\Rightarrow$	implikácia
$\Leftrightarrow$	ekvivalencia
$A'$	negácia výroku $A$
$\exists$	existuje aspoň jeden (existenčný kvantifikátor)
$\forall$	pre každý, pre všetky (všeobecný kvantifikátor)
$\in$	je prvkom, patrí do
$\notin$	nie je prvkom, nepatrí do
$\cap$	priek množín
$\cup$	zjednotenie množín
$\subset$	je podmnožinou
$\setminus$	rozdiel množín
$n!$	$n$ faktoriál
$\binom{n}{k}$	kombináčné číslo ( $n$ nad $k$ )
$a^n$	$n$ -tá mocnina čísla $a$
$\sqrt[n]{a}$	$n$ -tá odmocnina z čísla $a$
$ $	delí ( $a   b$ znamená $a$ delí $b$ )
$\nmid$	nedelí ( $a \nmid b$ znamená $a$ nedelí $b$ )
$D(a, b)$	najväčší spoločný deliteľ čísel $a, b$
$n(a, b)$	najmenší spoločný násobok čísel $a, b$

# Úvod

Táto práca je výukový text pre nadaných žiakov stredných škôl na téma deliteľnosť. O čitateľovi sa predpokladá, že je žiakom strednej školy a je schopný upravovať algebraické výrazy, riešiť rovnice, nerovnice, pozná elementárnu výrokovú logiku a operácie s množinami, vie pracovať s mocninami, odmocninami a s kombinačným číslom.

Celá práca je rozdelená do niekoľkých častí. Tvrdenia, ktoré sú uvádzané ako vety, sú vždy v práci dokázané. Najdôležitejšou súčasťou je kapitola venovaná kritériám deliteľnosti. V práci sa tiež nachádza kapitola venovaná prvočíslam a ich využitiu v reálnom živote.

V prvej kapitole nazvanej „Základné pojmy a vety“ si čitateľ zopakuje, napríklad rozdiel medzi prvočíslom a zloženým číslom, čo sú súdeliteľné, nesúdeliteľné čísla, najmenší spoločný násobok, najväčší spoločný deliteľ, alebo tiež ako sa robí rozklad zloženého čísla na súčin prvočísel. Znalosť všetkých týchto pojmov si čitateľ vždy môže vyskúšať na rôznych cvičeniach, ktoré nasledujú za výkladom. V tejto kapitole sa čitateľ naučí hľadať najväčšieho spoločného deliteľa pomocou Euklidovho algoritmu.

Ďalšia kapitola je venovaná kritériám deliteľnosti číslami 2 až 20. Kritéria deliteľnosti slúžia k rozhodovaniu, či je dané číslo deliteľné daným prirodzeným číslom, a to tak, aby to bolo jednoduché aj bez použitia písomného delenia alebo kalkulačky. Existuje niekoľko spôsobov, napr. určovanie deliteľnosti pomocou posledných cifier čísla, pomocou celočíselnej lineárnej kombinácie jednotlivých cifier. Kritéria, ktoré tu budú uvedené, budú dokázané a tiež vysvetlené na príkladoch.

Nasleduje kapitola, ktorej obsahom sú diofantické rovnice, konkrétnie lineárne a kvadratické diofantické rovnice s dvoma neznámymi. Súčasťou tejto kapitoly sú slovné úlohy zamerané na diofantické rovnice.

V predposlednej kapitole nazvanej „Prvočísla a ich využitie v reálnom živote“ sa čitateľ zoznámi s Euklidovými vetami, kritériami prvočíselnosti a s rôznymi aplikáciami prvočísel, napr. v šifrovaní.

Posledná kapitola je zmes príkladov a cvičení. Začína jednoduchým testom na overenie znalostí o deliteľnosti, pokračuje príkladmi na deliteľnosť s riešeniami, medzi ktorými sú aj dôkazové príklady. Záver kapitoly tvoria zaujímavé úlohy z matematických olympiád a korešpondenčných seminárov.

V prílohe práce sa nachádza tabuľka prvočísel a odkazy na internetové stránky.

# Kapitola 1

## Základné pojmy a vety

V tejto kapitole uvedieme dôležité pojmy a tvrdenia, ktoré budeme v práci používať. Na začiatku vysvetlíme značenie, zopakujeme pojmy z výrokovej logiky, vysvetlíme typy dôkazov, ktoré budeme v práci používať. Tiež zopakujeme pojem mocnina, odmocnina, kombinačné číslo a ich základné vlastnosti. Potom definujeme pojmy z deliteľnosti, ako sú napríklad prvočíslo, zložené číslo, najmenší spoločný násobok, najväčší spoločný deliteľ. Pripomenieme, ako sa robí rozklad zloženého čísla na súčin prvočísel, a tiež sa naučíme hľadať najväčšieho spoločného deliteľa pomocou Euklidovho algoritmu.

### 1.1 Značenie

- Symbolom  $\in$  budeme zapisovať skutočnosť, že nejaký prvok **patrí do** istej množiny. Napríklad zápis  $a \in A$  značí, že prvok  $a$  patrí do množiny  $A$ .
- Symbol  $\exists$  (**existenčný**, resp. **malý kvantifikátor**) čítame ako „existuje“. Zápis  $\exists n \in A : V(n)$  má význam „Existuje aspoň jedno  $n \in A$ , pre ktoré platí  $V(n)$ .“
- Symbol  $\forall$  (**všeobecný**, resp. **veľký kvantifikátor**) čítame ako „pre všetky“ alebo „pre každé“. Zápis  $\forall n \in A : V(n)$  má význam „Pre každé  $n \in A$  platí  $V(n)$ .“

- Pre množiny  $A, B$  budeme používať nasledujúce symboly:

$\subset$  (čítame **je podmnožinou**)

Množina  $A$  je podmnožinou množiny  $B$  práve vtedy, keď každý prvok množiny  $A$  je prvkom množiny  $B$ , píšeme  $A \subset B$ .

$=$  (čítame **je rovná**)

Množina  $A$  je rovná množine  $B$  práve vtedy, keď množina  $A$  je podmnožinou  $B$  a  $B$  je podmnožinou  $A$ , tj.  $A = B$ .

$\cap$  (čítame **prienik**)

Prienik množín  $A \cap B$  je množina všetkých prvkov, ktoré patria do množiny  $A$  a súčasne aj do množiny  $B$ .

$\cup$  (čítame **zjednotenie**)

Zjednotenie množín  $A \cup B$  je množina všetkých prvkov, ktoré patria do množiny  $A$  alebo do množiny  $B$ .

$\setminus$  (čítame **rozdiel**)

Rozdiel množín  $A \setminus B$  je množina všetkých prvkov, ktoré patria do množiny  $A$ , ale nepatria do množiny  $B$ .

- V texte budeme používať symbol  $\sum$  (veľké grécke písmeno „sigma“). Symbol  $\sum$  (**sumačný znak**) sa používa na vyjadrenie zápisu súčtu čísel. To znamená, že pre prirodzené číslo  $n$  a pre reálne čísla  $a_i, i \in \{1, \dots, n\}$  platí

$$\sum_{i=1}^n a_i = a_1 + a_2 + a_3 + \dots + a_n.$$

### Vlastnosti sčítania/sumačného znaku

Pre prirodzené číslo  $n$ , pre reálne čísla  $a_i, b_i, i \in \{1, 2, \dots, n\}$  a reálnu konštantu  $c$  platí

$$\begin{aligned}\sum_{i=1}^n (a_i \pm b_i) &= \sum_{i=1}^n a_i \pm \sum_{i=1}^n b_i, \\ \sum_{i=1}^n (c \cdot a_i) &= c \cdot \sum_{i=1}^n a_i.\end{aligned}$$

## 1.2 Logika

Výroková logika (skr. logika) sa v matematike využíva v matematických úlohách, formuláciach, tvrdeniach. Pretože v texte sa budeme často stretávať s pojmi z logiky, je táto časť venovaná zopakovaniu základných pojmov (napr. zložený výrok, logické spojky – konjunkcia, disjunkcia, implikácia, ekvivalencia).

O čitateľovi sa predpokladá, že sa s touto problematikou už stretol, preto v tejto časti nájde len zhrnutie potrebných pojmov bez príkladov alebo cvičení. V prípade, že tomu tak nie je, odporúčame knihu [2], kap. 4, kde je tomuto okruhu matematiky venovaný väčší priestor.

### 1.2.1 Výroky

**Logický výrok** je každá oznamovacia veta, o ktorej má zmysel rozhodnúť, či je alebo nie je pravdivá. Výroky označujeme veľkými písmenami. Pravdivým výrokom priradujeme číslo 1 a nepravdivým výrokom priradujeme číslo 0. Tieto čísla nazývame **pravdivostná hodnota**.

**Negácia výroku** je výrok, ktorý vytvoríme popretím pravdivosti daného výroku pomocou logickej spojky „nie“ alebo „nie je pravda, že“. Pre výrok  $A$  značíme jeho negáciu ako  $A'$ .

**Hypotéza** je každá oznamovacia veta, u ktorej nevieme určiť pravdivostnú hodnotu, nie je známa.

Príklady jednoduchých výrokov:

- Bratislava je hlavné mesto Slovenska.
- Číslo 11 je prvočíslo.
- Dunaj je najdlhšia rieka na svete.
- $2 + 3 = 6$ .

### 1.2.2 Zložený výrok a logické spojky

**Zložený výrok** je každý výrok, ktorý vznikne spojením dvoch a viac jednoduchých výrokov.

Výroky spájame pomocou logických spojok – konjunkcia, disjunkcia, implikácia, ekvivalencia.

**Konjunkcia** výrokov  $A, B$  je výrok, ktorý vznikne spojením týchto dvoch výrokov spojkou „a“, resp. „a zároveň“. Konjunkcia je pravdivá práve vtedy, keď sú oba výroky pravdivé. Značíme:

$$A \wedge B.$$

Čítame: „Výrok  $A$  a zároveň výrok  $B$ .“

**Disjunkcia** výrokov  $A, B$  je výrok, ktorý vznikne spojením týchto dvoch výrokov spojkou „alebo“. Disjunkcia je pravdivá práve vtedy, keď aspoň jeden z výrokov je pravdivý. Značíme:

$$A \vee B.$$

Čítame: „Výrok  $A$  alebo výrok  $B$ .“

**Implikácia** výrokov  $A, B$  je výrok typu „Ak  $A$ , potom  $B$ “. **Predpokladom** nazývame výrok  $A$  a **záverom** výrok  $B$ . Implikácia nie je pravdivá pre pravdivý predpoklad a nepravdivý záver. Značíme:

$$A \Rightarrow B.$$

Čítame: „Ak výrok  $A$ , potom výrok  $B$ .“ Alebo tiež: „ $A$  implikuje  $B$ .“

**Obrátenou implikáciou** nazývame implikáciu  $B \Rightarrow A$ .

**Obmenenou implikáciou** k implikácii  $A \Rightarrow B$  nazývame výrok  $B' \Rightarrow A'$ .

Obmenená a pôvodná implikácia majú vždy rovnakú pravdivostnú hodnotu. Pre obrátenú implikáciu to neplatí, vid' Tab. 1.1.

**Ekvivalencia** výrokov  $A, B$  je konjunkcia implikácie  $A \Rightarrow B$  a knej obrátenej implikácie,  $B \Rightarrow A$ . Ekvivalencia je pravdivá práve vtedy, keď majú výroky  $A, B$  rovnakú pravdivostnú hodnotu. Značíme:

$$A \Leftrightarrow B.$$

Čítame: „Výrok  $A$  práve vtedy, keď výrok  $B$ .“ Alebo tiež: „ $A$  je ekvivalentné s  $B$ .“

$A$	$B$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$B \Rightarrow A$	$B' \Rightarrow A'$
1	1	1	1	1	1	1	1
1	0	0	1	0	0	1	0
0	1	0	1	1	0	0	1
0	0	0	0	1	1	1	1

Tabuľka 1.1: Tabuľka pravdivostných hodnôt.

**Výroková forma** (tiež **výroková formula**, **výrokový vzorec**, **výroková funkcia**)  $V(x)$ ,  $V(x, y)$ , kde  $x, y$  sú premenné, je výraz, ktorý sám nie je výrokom, ale obsahuje premenné, za ktoré ak dosadíme prípustné hodnoty, dostaneme výrok.

### 1.3 Typy dôkazov

Matematický dôkaz (skr. dôkaz) je postupnosť úvah, pomocou ktorých sa overuje pravdivosť, prípadne nepravdivosť daného výroku. V matematike existujú rôzne typy dôkazov. V prípade, že budeme chcieť dokázať pravdivosť výroku (tvrdenia), budeme používať jednu z nasledujúcich stratégií:

- Pokúsime sa dokázať výrok priamo.
- Utvoríme negáciu výroku, a tú sa pokúsime dovestiť k sporu.
- Utvoríme obmenu implikácie a túto implikáciu dokážeme priamo alebo sporom.
- Dôkaz vykonáme matematickou indukciou.

Ak výrok dokazujeme sporom alebo jeho obmenou, potom hovoríme o nepriamom dôkaze. Viac informácií o dôkazoch možno nájsť v [4] alebo [19].

**Priamy dôkaz** výroku  $B$  pozostáva z konečného reťazca implikácií

$$A \Rightarrow T_1 \Rightarrow T_2 \Rightarrow \dots \Rightarrow T_n \Rightarrow B,$$

ktorého prvý člen, výrok  $A$ , je axióm alebo už dokázané tvrdenie. Každý ďalší z výrokov  $T_1, T_2, \dots, T_n$  je vždy dôsledkom predchádzajúceho výroku. Posledným členom reťazca je dokazovaný výrok  $B$ .

**Nepriamy dôkaz (sporom)** výroku  $B$  vychádza z predpokladu, že platí výrok  $B'$ . Z neho potom odvodzujeme logické dôsledky tak dlho, až sa nám podarí odvodiť tvrdenie  $A$ , o ktorom vieme, že je nepravdivé. Hovoríme, že sme dospeli k sporu.

**Priamy dôkaz implikácie  $A \Rightarrow B$**  pozostáva z nájdenia postupnosti implikácií začínajúcich výrokom  $A$  a končiacich výrokom  $B$ , v ktorej každý člen je logickým dôsledkom predchádzajúcich výrokov.

**Nepriamy dôkaz implikácie  $A \Rightarrow B$  sporom** vychádza z predpokladu platnosti negácie dokazovanej implikácie, tj. prepokladáme, že platí  $A \wedge B'$ . Postupne odvodzujeme dôsledky tak dlho, pokiaľ nedôjdeme k sporu.

**Nepriamy dôkaz implikácie  $A \Rightarrow B$  pomocou obmeny** vychádza zo skutočnosti, že implikácia  $A \Rightarrow B$  a jej obmena  $B' \Rightarrow A'$  sú ekvivalentné (majú rovnakú pravdivostnú hodnotu). Nepriamym dôkazom implikácie  $A \Rightarrow B$  je teda reťazec implikácií

$$B' \Rightarrow T_1 \Rightarrow T_2 \Rightarrow \dots \Rightarrow T_n \Rightarrow A',$$

kde  $T_1, T_2, \dots, T_n$  sú výroky.

Dôkaz ekvivalencie  $A \Leftrightarrow B$  sa skladá z dôkazu implikácií  $A \Rightarrow B$  a  $B \Rightarrow A$ .

Pre výroky o prirodzených číslach sa používa metóda dôkazu matematickou indukciou.

**Dôkaz matematickou indukciou** sa skladá z týchto dvoch krokov:

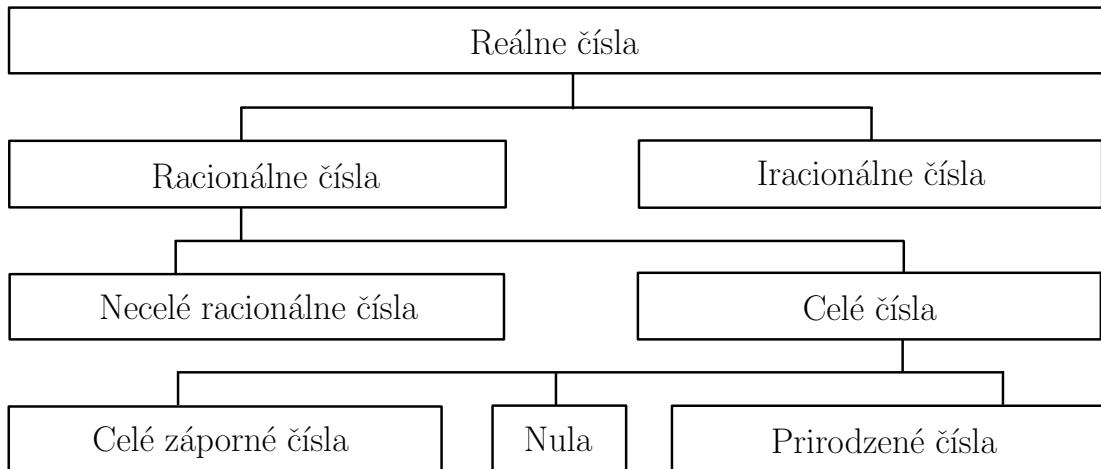
1. Pre  $n_0 \in \mathbb{N}$  overíme, že platí výrok  $V(n_0)$ .
2. Z platnosti predpokladu „Platí výrok  $V(k)$  pre každé prirodzené číslo  $k \geq n_0$ “, dokážeme, že platí výrok  $V(k+1)$ .

Potom výrok  $V(n)$  platí pre všetky prirodzené čísla  $n \geq n_0$ .

Predpoklad z druhého kroku nazývame **indukčný predpoklad**.

## 1.4 Číselné množiny

Množina je skupina (súbor, súhrn) navzájom rôznych objektov. Pod pojmom číselná množina rozumieme všetky množiny, ktorých prvkami sú čísla. Medzi dôležité číselné množiny patrí množina všetkých prirodzených, celých, racionálnych a tiež reálnych čísel.



Obr. 1.1: Vzťahy medzi číselnými množinami.

**Množina všetkých prirodzených čísel** je množina

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Prirodzené čísla vyjadrujú počet predmetov vnejakej skupine, počet prvkov konečných neprázdných množín.

**Množina všetkých prirodzených čísel s nulou** je množina

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}.$$

**Množina všetkých celých čísel** je množina

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Celé čísla vyjadrujú zmeny počtu prvkov, ich prírastok alebo úbytok. Do tejto množiny patria všetky prirodzené čísla, čísla k nim opačné (záporné) a nula.

**Množina všetkých racionálnych čísel** je množina

$$\mathbb{Q} = \left\{ \frac{a}{b}; a \in \mathbb{Z} \wedge b \in \mathbb{N} \right\},$$

tj. racionálne čísla sa dajú zapísat v tvare zlomku, v ktorom čitateľ je celé číslo a menovateľ je prirodzené číslo. Racionálne čísla vyjadrujú počty celkov a ich častí a zmeny týchto počtov.

Existujú aj čísla, ktoré nemožno zapísat v tvare  $\frac{a}{b}$ , kde  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}$ , napr. čísla  $\sqrt{2}$ ,  $\sqrt{3}$ , Ludolfov číslo  $\pi$ . Tieto čísla nazývame iracionálne čísla.

**Množina všetkých reálnych čísel** je množina, ktorá je tvorená všetkými racionálnymi a iracionálnymi číslami.

## 1.5 Rozvinutý zápis prirodzeného čísla

V deliteľnosti sa často používa rozvinutý zápis prirodzeného čísla v desiatkovej sústave (ďalej budeme hovoriť len rozvinutý zápis prirodzeného čísla). Čo to je, popisuje nasledujúca definícia.

**Rozvinutým zápisom** prirodzeného čísla  $x$  nazývame súčet

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10^1 + a_0 \cdot 10^0 = \sum_{i=0}^n (a_i \cdot 10^i) = x,$$

kde  $n \in \mathbb{N}_0$ ,  $a_i \in \{0, 1, 2, \dots, 9\}$  pre každé  $i \in \{0, 1, 2, \dots, n\}$  a  $a_n \neq 0$ .

Čísla  $a_i$ ,  $i \in \{0, 1, 2, \dots, n\}$  nazývame **cifry** čísla  $x$ .

**Ciferným súčtom** čísla  $x$  rozumieme súčet všetkých jeho cifier, tj.

$$a_0 + a_1 + \dots + a_n = \sum_{i=0}^n a_i.$$

Uvažujme napríklad číslo 25 016. Jeho zápis v desiatkovej sústave je

$$25 016 = 2 \cdot 10^4 + 5 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10^1 + 6 \cdot 10^0.$$

## 1.6 Mocniny a odmocniny

V tejto časti zhrnieme poznatky o mocninách a odmocninách. Najprv definujeme mocniny s prirodzeným mocniteľom.

Pre každé reálne číslo  $a$  a pre každé prirodzené číslo  $n$  platí:

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n-\text{krát}}.$$

Číslo  $a^n$  nazývame  **$n$ -tá mocnina**,  $a$  je **základ mocniny** a  $n$  je **mocniteľ (exponent)**.

Z definície mocniny vyplýva, že pre každé  $a, b \in \mathbb{R}$ ,  $n, m \in \mathbb{N}$  platí:

$$\begin{aligned} a^1 &= a, \\ 1^n &= 1, \\ 0^n &= 0, \\ a^m \cdot a^n &= a^{m+n}, \\ (a^n)^m &= a^{m \cdot n}, \\ \frac{a^m}{a^n} &= a^{m-n}, \quad a \neq 0, \quad m > n, \\ (a \cdot b)^n &= a^n \cdot b^n, \\ \left(\frac{a}{b}\right)^n &= \frac{a^n}{b^n}, \quad b \neq 0. \end{aligned}$$

Teraz definíciu mocniny zovšeobecníme pre celočíselný exponent.

Pre každé nenulové reálne číslo  $a$  a pre každé celé číslo  $k$  platí

$$a^{-k} = \frac{1}{a^k}.$$

Výraz  $a^{-k}$  nazývame **mocnina s celočíselným exponentom**.

Z tejto definície vyplýva, že  $\frac{a^r}{a^s} = a^{r-s}$  pre celé čísla  $r, s$  platí i v prípade, keď rozdiel  $r - s$  je záporné celé číslo.

Pre každé  $a, b \in \mathbb{R} \setminus \{0\}$ ,  $r, s \in \mathbb{Z}$  platia tieto vlastnosti:

$$\begin{aligned} a^0 &= 1, \quad (\text{POZOR! } 0^0 \text{ nie je definované}), \\ a^r \cdot a^s &= a^{r+s}, \\ (a^r)^s &= a^{r \cdot s}, \\ \frac{a^r}{a^s} &= a^{r-s}, \\ (a \cdot b)^r &= a^r \cdot b^r, \\ \left(\frac{a}{b}\right)^r &= \frac{a^r}{b^r}. \end{aligned}$$

Ďalej nasleduje definícia  $n$ -tej odmocniny.

Každé nezáporné reálne číslo  $a$  splňajúce vzťah

$$a^n = b,$$

kde  $b$  je nezáporné reálne číslo a  $n$  je prirodzené číslo, nazývame  **$n$ -tá odmocnina** z čísla  $b$ . Píšeme

$$\sqrt[n]{b} = a.$$

Špeciálne pre  $n = 2$  (druhá odmocnina) používame zápis  $\sqrt{b}$ .

Pre každé nezáporné reálne čísla  $a, b$ , pre každé prirodzené čísla  $m, n$  a pre každé celé číslo  $s$  platí

$$\begin{aligned}\sqrt[n]{a} \cdot \sqrt[n]{b} &= \sqrt[n]{a \cdot b}, \\ \frac{\sqrt[n]{a}}{\sqrt[n]{b}} &= \sqrt[n]{\frac{a}{b}}, \quad b \neq 0, \\ \sqrt[m]{\sqrt[n]{a}} &= \sqrt[m \cdot n]{a}, \\ (\sqrt[n]{a})^s &= \sqrt[n]{a^s}, \\ \sqrt[n]{a} &= \sqrt[n \cdot m]{a^m}, \quad a \neq 0, \\ \sqrt[m \cdot n]{a^{m \cdot s}} &= \sqrt[n]{a^s}, \quad a \neq 0.\end{aligned}$$

## 1.7 Kombinačné čísla

V práci sa stretнемe aj s pojmom kombinačné číslo.

**Kombinačné číslo** je číslo, ktoré udáva počet spôsobov (tzv. kombinácií), ako vybrať  $k$ -prvkovú podmnožinu z  $n$ -prvkovej množiny. Značí sa

$$\binom{n}{k}, \quad (\text{čítame „}n \text{ nad } k\text{“}).$$

Kombinačné číslo sa dá vyčísliť

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \quad (1.1)$$

Číslo  $n!$  nazývame **faktoriál** čísla  $n$ . Počítame ho ako  $n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$ . (Pre  $n = 0$  definujeme  $0! = 1$ .)

**Príklad 1.** Čomu sa rovná  $\binom{4}{3}$ ?

*Riešenie:* Kombinačné číslo  $\binom{4}{3}$  je rovné číslu 4. To je možné ukázať vypísaním všetkých 3-prvkových podmnožín zo 4-prvkovej množiny (na poradí prvkov nezáleží), tj. množín  $\{1, 2, 3\}$ ,  $\{1, 2, 4\}$ ,  $\{1, 3, 4\}$  a  $\{2, 3, 4\}$ .

Ďalšia možnosť ako obdržíme rovnaký výsledok je výpočet kombinačného čísla pomocou (1.1), tj.

$$\binom{4}{3} = \frac{4!}{3! \cdot (4-3)!} = \frac{24}{6 \cdot 1} = 4.$$

Môžeme si tiež uvedomiť, že počet možností výberu 3-prvkovej podmnožiny zo 4-prvkovej množiny je ekvivalentný počtu možností výberu 1-prvkovej podmnožiny (jedného prvku) zo 4-prvkovej množiny, a tých je zrejmé 4, tj.

$$\binom{4}{3} = \binom{4}{1} = 4.$$

## Vlastnosti kombinačných čísel

Pre každé nezáporné celé čísla  $n, k$  také, že  $k \leq n$  platí

$$\begin{aligned}\binom{n}{0} &= \binom{n}{n} = 1, \\ \binom{n}{k} &= \binom{n}{n-k}, \\ \binom{n}{1} &= n, \\ \binom{n}{k+1} &= \binom{n}{k} \cdot \frac{n-k}{k+1}, \\ \binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1}.\end{aligned}$$

## Pascalov trojuholník

Pascalov trojuholník je schéma, ktoré znázorňuje niektoré vlastnosti kombinačných čísel. Tento trojuholník je pomenovaný po francúzskom matematikovi Blaise Pascalovi. Existujú dva jeho tvary. Bud' sa zapisuje pomocou kombinačných čísel, alebo pomocou čísel, ktoré odpovedajú príslušným kombinačným číslam (vid' Obr. 1.2).

Konštrukcia Pascalovho trojuholníka sa riadi nasledovnými bodmi:

- Do prvého riadku sa zapisuje číslo  $\binom{0}{0}$ , ktoré je rovné číslu 1.
- V každom  $(n+1)$ -om riadku je prvé číslo rovné číslu  $\binom{n}{0}$  a posledné číslo číslu  $\binom{n}{n}$ . Obe tieto čísla sú rovné číslu 1.
- Ďalšie čísla  $\binom{n}{k}$  získame tým, že sčítame dve najbližšie čísla, ktoré sa nachádzajú o riadok vyššie, tj. riadime sa pravidlom

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

$n = 0$	$\binom{0}{0}$	1
$n = 1$	$\binom{1}{0} \quad \binom{1}{1}$	1 1
$n = 2$	$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$	1 2 1
$n = 3$	$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$	1 3 3 1
$n = 4$	$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$	1 4 6 4 1

Obr. 1.2: Pascalov trojuholník. Vľavo schéma s kombinačnými číslami, vpravo schéma, v ktorom sú kombinačné čísla vyčíslené.

Pascalov trojuholník je veľmi praktický pri počítaní rozvoja podľa binomickej vety (táto veta je uvedená nižšie, Veta 1).

**Príklad 2.** Vypočítajte

$$\binom{18}{1} + \binom{5}{2} + \binom{5}{3} - \binom{18}{18} - 3!.$$

Riešenie:

$$\underbrace{\binom{18}{1}}_{18} + \underbrace{\binom{5}{2} + \binom{5}{3}}_{\binom{6}{3} = \frac{6!}{3! \cdot 3!} = 20} - \underbrace{\binom{18}{18}}_{1} - \underbrace{3!}_{3 \cdot 2 \cdot 1 = 6} = 18 + 20 - 1 - 6 = 31.$$

Jedno z dôležitých tvrdení matematiky, v ktorom sa môžeme stretnúť s kombinačným číslom, je binomická veta. Vďaka tomuto tvrdeniu vieme napísat  $n$ -tú mocninu dvoch sčítancov ako súčet  $n+1$  istých sčítancov. Jej znenie je nasledovne:

**Veta 1. (Binomická veta)**

Pre každé prirodzené číslo  $n$  a pre každé dve reálne čísla  $a, b$  platí

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i. \quad (1.2)$$

*Poznámka.* Kombinačné čísla  $\binom{n}{i}$ ,  $i \in \{0, 1, 2, \dots, n\}$ , sa nazývajú binomické koeficienty (všetky sa nachádzajú v  $(n+1)$ -om riadku Pascalovho trojuholníka).

*Dôkaz.* Majme pevne zvolené čísla  $a, b \in \mathbb{R}$ . Vetu dokážeme pomocou matematickej indukcie.

Prvý krok matematickej indukcie požaduje, aby sme danú vlastnosť overili pre  $n = 1$ , teda

$$(a+b)^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b.$$

Je zrejmé, že pre  $n = 1$  tvrdenie platí.

V druhom kroku predpokladajme, že tvrdenie platí pre  $k \in \mathbb{N}$  (tentu predpoklad sa označujeme prívlastkom indukčný) a ukážeme, že potom tvrdenie platí i pre  $k+1$ . Náš indukčný predpoklad znie

$$(a+b)^k = \sum_{i=0}^k \binom{k}{i} a^{k-i} b^i,$$

Z neho dokážeme, že platí

$$(a+b)^{k+1} = \sum_{i=0}^{k+1} \binom{k+1}{i} a^{k+1-i} b^i.$$

K dôkazu využijeme nasledujúci vzťah medzi kombinačnými číslami

$$\binom{k+1}{i} = \binom{k}{i} + \binom{k}{i-1}.$$

Vďaka tejto identite môžeme písat' nasledujúce

$$\begin{aligned}
 \sum_{i=0}^{k+1} \binom{k+1}{i} a^{k+1-i} b^i &= a^{k+1} + \sum_{i=1}^k \binom{k+1}{i} a^{k+1-i} b^i + b^{k+1} \\
 &= a^{k+1} + \sum_{i=1}^k \left[ \binom{k}{i} + \binom{k}{i-1} \right] a^{k+1-i} b^i + b^{k+1} \\
 &= a^{k+1} + \sum_{i=1}^k \binom{k}{i} a^{k+1-i} b^i + \sum_{i=1}^k \binom{k}{i-1} a^{k+1-i} b^i + b^{k+1} \\
 &= a^{k+1} + [(a+b)^k - a^k] \cdot a + [(a+b)^k - b^k] \cdot b + b^{k+1} \\
 &= (a+b)^{k+1},
 \end{aligned}$$

čo sme chceli dokázať. Tým pádom sme pomocou matematickej indukcie dokázali platnosť binomickej vety.  $\square$

### Cvičenia

1. Vypočítajte

$$2! + (3^2) - 4! + 13.$$

2. Upravte na spoločného menovateľa

$$\frac{1}{8!} - \frac{90}{11!}.$$

3. Vypočítajte

$$\binom{13}{7}.$$

4. Vyjadrite jedným kombinačným číslom

$$\binom{15}{5} + \binom{15}{6}.$$

### Výsledky cvičení

1.  $2 + 9 - 24 + 13 = 0$ .

2.  $\frac{11 \cdot 10 \cdot 9 - 90}{11!} = \frac{900}{11!}$ .

3. 1716.

4.  $\binom{16}{6}$ .

## 1.8 Základné pojmy deliteľnosti

Táto časť obsahuje pojmy, ktoré súvisia s deliteľnosťou. Konkrétnie sa tu stretнемe s pojmi, ako sú napríklad deliteľ, násobok, zvyšok, prvočíslo, zložené číslo.

Pre ľubovoľné prirodzené čísla  $a, b$  existuje jediná dvojica  $q, r \in \mathbb{N}_0$  taká, že

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

Číslo  $q$  nazývame **podiel** čísel  $a, b$  a číslo  $r$  nazývame **zvyšok** po delení čísla  $a$  číslom  $b$ .

Hovoríme, že prirodzené číslo  $n$  je **deliteľné** prirodzeným číslom  $k$ , resp. „ $k$  delí  $n$  bez zvyšku“, ak existuje prirodzené číslo  $l$  také, že

$$k \cdot l = n.$$

Zapisujeme symbolom

$$k | n.$$

Číslo  $n$  nazývame **násobok** čísla  $k$  a číslo  $l$  nazývame **podiel** čísla  $n$  pri delení číslom  $k$ . Všetky čísla  $k$ , ktoré delia číslo  $n$ , nazývame **delitele** čísla  $n$ . Delitele 1 a  $n$  nazývame **triviálne delitele**. Ostatné delitele nazývame **netriviálne** alebo **vlastné delitele**.

**Nedeliteľnosť** čísla  $n$  číslom  $k$  (resp. vlastnosť „ $k$  nedelí  $n$ “) značíme symbolom

$$k \nmid n.$$

## Základné vlastnosti delenia

Pre ľubovoľné prirodzené čísla  $a, b, c, d$  platí:

$$\begin{aligned} 1 &\mid a, \\ a &\mid a, \\ a &\mid 0, \\ (a &\mid b \wedge a \mid c) \Rightarrow a \mid (b+c), \\ (a &\mid b \wedge b \mid c) \Rightarrow a \mid c, \\ (a &\mid b \wedge c \mid d) \Rightarrow (ac) \mid (bd). \end{aligned}$$

Prirodzené čísla podľa deliteľnosti číslom 2 rozdeľujeme na párne a nepárne čísla.

Hovoríme, že prirodzené číslo je **párne**, pokial' je deliteľné číslom 2 bez zvyšku, v opačnom prípade hovoríme o **nepárnom** číslе.

Všimnite si, že každé párne prirodzené číslo sa dá napísať ako súčin  $2 \cdot k$ , kde  $k \in \mathbb{N}$ . Nepárne číslo musí po delení číslom 2 dať nenulový zvyšok (to môže byť len číslo 1), a preto je rovné  $2 \cdot k + 1$ , kde  $k \in \mathbb{N}_0$ .

Podobne to platí i pri delení inými číslami. Napríklad prirodzené číslo deliteľné číslom 5 môžeme zapísať ako  $5 \cdot k$ , kde  $k \in \mathbb{N}$ . Všetky ostatné prirodzené čísla sú deliteľné jedným z týchto výrazov  $5 \cdot k + 1, 5 \cdot k + 2, 5 \cdot k + 3, 5 \cdot k + 4$ , kde  $k \in \mathbb{N}_0$ .

Každé prirodzené číslo sa dá zapísať pomocou prirodzeného čísla  $b > 1$  jedným z výrazov

$$b \cdot k, b \cdot k + 1, b \cdot k + 2, \dots, b \cdot k + (b - 1),$$

kde  $k \in \mathbb{N}_0$ .

**Príklad 3.** Zapíšte ľubovoľné prirodzené číslo, ktoré pri delení číslom 11 dáva zvyšok 3.

*Riešenie:* Nech  $n$  je ľubovoľné prirodzené číslo, ktoré pri delení číslom 11 dáva zvyšok 3. Potom číslo  $n = 11 \cdot k + 3$ , kde  $k \in \mathbb{N}_0$ .

Teraz vyplníme tabuľku o počte deliteľov pre  $n = 1, \dots, 10$ . Všímajte si, kolko z nich má len jedného deliteľa, dvoch alebo aspoň troch deliteľov.

$n$	Delitele	Počet deliteľov
1	1	1
2	1, 2	2
3	1, 3	2
4	1, 2, 4	3
5	1, 5	2
6	1, 2, 3, 6	4
7	1, 7	2
8	1, 2, 4, 8	4
9	1, 3, 9	3
10	1, 2, 5, 10	4

Tabuľka 1.2: Počet deliteľov prirodzeného čísla  $n \leq 10$ .

Z tabuľky vidíme, že prirodzené čísla môžu mať jedného, dvoch alebo viac deliteľov.

Jediné prirodzené číslo, ktoré má len jedného deliteľa, je číslo 1. Ostatné majú dva (1 a samé seba), resp. aspoň tri delitele.

**Prvocíslo** je každé prirodzené číslo, ktoré má práve dvoch rôznych deliteľov.

**Zložené číslo** je každé prirodzené číslo, ktoré má aspoň troch rôznych deliteľov.

Číslo 1 nie je ani zložené číslo, ani prvocíslo.

Ďalšie pojmy, s ktorými budeme pracovať je spoločný násobok, spoločný deliteľ, najväčší spoločný deliteľ a najmenší spoločný násobok.

**Spoločný deliteľ** dvoch prirodzených čísel  $a, b$  je prirodzené číslo, ktoré je deliteľom čísla  $a$  a zároveň deliteľom čísla  $b$ .

**Najväčší spoločný deliteľ** dvoch prirodzených čísel  $a, b$  je najväčší deliteľ zo všetkých spoločných deliteľov čísel  $a, b$ . Značíme ho ako  $D(a, b)$ .

**Spoločný násobok** dvoch prirodzených čísel  $a, b$  je prirodzené číslo, ktoré je násobkom čísel  $a$  a zároveň násobkom čísla  $b$ .

**Najmenší spoločný násobok** dvoch prirodzených čísel  $a, b$  je najmenší násobok zo všetkých spoločných násobkov čísel  $a, b$  (každý iný spoločný násobok je jeho násobkom). Značíme ho ako  $n(a, b)$ .

Ďalším dôležitým pojmom je súdeliteľnosť, resp. nesúdeliteľnosť.

Prirodzené čísla  $a, b$  nazývame **súdeliteľné**, ak majú aspoň jedného spoločného deliteľa  $d > 1$ . V opačnom prípade hovoríme o **nesúdeliteľných** číslach, tj. ich spoločný deliteľ je len číslo 1.

Napríklad čísla 24 a 6 sú súdeliteľné čísla, pretože existuje ich spoločný deliteľ (napr. číslo 2) väčší ako 1. Čísla 11 a 2 sú nesúdeliteľné, ich jediný spoločný deliteľ je číslo 1.

**Veta 2.** (*Deliteľnosť k po sebe idúcich prirodzených čísel*)

*Súčin k po sebe idúcich prirodzených čísel je deliteľný číslami  $1, 2, \dots, k!$ .*

*Dôkaz.* Predpokladajme, že máme súčin  $k$  po sebe idúcich prirodzených čísel. Najmenšie číslo z nich označme ako  $n$ . Potom platí, že

$$n \cdot (n+1) \cdot \dots \cdot (n+k-1) = \frac{(n+k-1)!}{(n-1)!} = k! \cdot \binom{n+k-1}{n-1}.$$

Pretože kombinačné číslo

$$\binom{n+k-1}{n-1} \in \mathbb{N},$$

musí tiež platiť

$$\frac{n \cdot (n+1) \cdot \dots \cdot (n+k-1)}{k!} \in \mathbb{N},$$

tj. súčin  $k$  po sebe idúcich prirodzených čísel musí byť deliteľný číslami  $1, 2, \dots, k!$ .

□

Predchádzajúce tvrdenie znamená napríklad toto: Ak budeme mať napríklad  $n \cdot (n+1) \cdot (n+2)$ , tj. súčin troch po sebe idúcich čísel, vieme určiť nejaké jeho delitele. Takýto súčin je deliteľný napr. číslom 1, 2, 3, aj číslom 3!.

## Cvičenia

1. Ktoré z nasledujúcich tvrdení je pravdivé:
  - a) Číslo 6 je násobok čísla 2.
  - b) Číslo 3 je násobok čísla 6.
  - c) Číslo 3 je deliteľ čísla 6.
  - d) Číslo 6 je deliteľ čísla 2.
2. Vyberte pravdivé tvrdenia:
  - a) Číslo 125 je násobok čísla 5.
  - b) Číslo 125 je násobok čísla 7.
  - c) Neexistuje číslo, ktoré je násobok čísla 5 a 7.
3. Doplňte nasledujúce tvrdenie tak, aby bolo pravdivé. Pre každé prirodzené čísla  $a, b$  je matematický výrok  $b \mid a$  ekvivalentný výroku:
  - a)  $a \mid b$ ,
  - b)  $a \nmid b$ ,
  - c)  $\forall c \in \mathbb{N} : a = cb$ ,
  - d)  $\exists c \in \mathbb{N} : a = cb$ .
4. Nájdite prirodzené číslo, ktoré pri delení 23 dáva zvyšok 7. Je toto číslo jediné?
5. Existuje prirodzené číslo, ktoré nie je prvočíslo ani zložené číslo?
6. Ktoré prirodzené číslo je najmenšie prvočíslo a zároveň jediné párne prvočíslo?
7. Ktoré prirodzené číslo je najmenšie zložené číslo? Kolko má deliteľov?

## Výsledky cvičení

1. Pravdivé odpovede sú a), c).
2. Správne je len a).
3. Správna odpoveď je d).
4. Jediné nie je. Všetky takéto čísla sú tvaru  $23 \cdot k + 7$ , kde  $k \in \mathbb{N}_0$ .
5. Číslo 1 má len jedného deliteľa, a to číslo 1.
6. Je to číslo 2. Každé iné párne číslo väčšie ako 2 je deliteľné číslami 1, 2 a samé sebou, a preto nemôže byť prvočíslo.
7. Číslo 4, má tri delitele.

## 1.9 Euklidov algoritmus

Veľmi užitočný nástroj na výpočet najväčšieho spoločného deliteľa dvoch prirodzených čísel je Euklidov algoritmus, ktorý teraz popíšeme.

**Euklidov algoritmus** pre určenie najväčšieho spoločného deliteľa  $D(a, b)$  prirodzených čísel  $a, b$ ,  $a \leq b$  pozostáva z nasledujúcich  $n$  krokov ( $n \in \mathbb{N}$ ):

1. Číslo  $b$  delíme číslom  $a$ . Zvyšok označíme ako  $z_1$ .
2. Ak  $z_1 \neq 0$ , potom číslo  $a$  delíme číslom  $z_1$ , zvyšok označíme ako  $z_2$ .
3. Ak  $z_2 \neq 0$ , potom číslo  $z_1$  delíme číslom  $z_2$ , zvyšok označíme ako  $z_3$ .
- ⋮
- $n$ . Ak  $z_n = 0$ , potom  $D(a, b) = z_{n-1}$ .

**Príklad 4.** Pomocou Euklidovho algoritmu určite najväčšieho spoločného deliteľa čísel 1 015 a 2 115.

*Riešenie:* Euklidovým algoritmom dostaneme tieto rovnosti

$$\begin{aligned} 2115 &= 2 \cdot 1015 + 85, \\ 1015 &= 11 \cdot 85 + 80, \\ 85 &= 1 \cdot 80 + 5, \\ 80 &= 40 \cdot 5 + 0. \end{aligned}$$

Ako postupujeme?

Najprv zavedieme značenie  $a = 1015$ ,  $b = 2115$  (označenie musí splňovať nerovnosť  $a \leq b$ ).

Pretože platí  $a \nmid b$ , musíme určiť číslo  $z_1$  tak, aby  $b = ak + z_1$ , kde  $k \in \mathbb{N}_0$ ,  $z_1 < a$ . Pretože  $b = 2a + z_1 = 2030 + 85$ , je naše hľadané číslo  $z_1 = 85$ .

V ďalšom kroku hľadáme  $z_2$  také, že  $a = z_1 \cdot k + z_2$ , kde  $k \in \mathbb{N}_0$  a  $z_2 < z_1$ . Dostaneme  $1015 = 11 \cdot 85 + 80$ . Odtiaľ máme  $z_2 = 80$ .

Podobne určíme číslo  $z_3$ . Platí  $85 = 1 \cdot 80 + 5$ . Číslo  $z_3$  je rovné číslu 5.

Číslo  $z_4$  dostaneme z rovnosti  $80 = 40 \cdot 5 + 0$ . Je to číslo 0, a preto najväčší spoločný deliteľ čísel 1 015, 2 115 je číslo  $z_3$ , tj. číslo 5.

### Cvičenia

1. Nájdite najväčšieho spoločného deliteľa čísel 25 a 35.
2. Pomocou Euklidovho algoritmu určte najväčšieho spoločného deliteľa čísel 1 222 a 3 520.

### Výsledky cvičení

1.  $D(25, 35) = 5$ .
2.  $D(1\,222, 3\,520) = 2$ .

## 1.10 Rozklad zloženého čísla na súčin prvočísel

Jedná zo zaujímavých vlastností zložených čísel je, že ich možno napísť ako súčin prvočísel.

Nech  $n$  je zložené prirodzené číslo, potom **prvočíselným rozkladom zloženého čísla** nazývame súčin

$$p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_k^{r_k},$$

kde  $k \in \mathbb{N}$ ,  $p_1, p_2, \dots, p_k$  sú prvočísla a  $r_1, r_2, \dots, r_k \in \mathbb{N}$ .

**Veta 3.** (*Existencia prvočíselného rozkladu zloženého čísla*)

Každé zložené číslo sa dá vyjadriť ako súčin prvočísel.

*Dôkaz.* Nech  $n$  je zložené číslo. Ak ho rozložíme na súčin dvoch prirodzených čísel  $a, b$  takých, že  $1 < a, b < n$ , tak potom sú buď obe čísla prvočísla, alebo aspoň jedno z nich je zložené číslo. Nové zložené číslo opäť rozložíme na súčin dvoch menších prirodzených čísel. Znova dostaneme bud' dve prvočísla, alebo aspoň jedno z nich zložené číslo. Postup rozkladu budeme opakovať dovtedy, kým nedostaneme len súčin prvočísel. Pretože prirodzených čísel menších ako číslo  $n$  existuje konečne mnoho, je tento rozklad konečný. Na konci tohto procesu dostaneme čísla, ktoré už nemožno rozložiť, tj. zložené číslo je zapísané ako súčin prvočísel.  $\square$

**Zápis/hľadanie prvočíselného rozkladu do/pomocou tabuľky**

Prvočíselný rozklad zloženého čísla môžeme hľadať pomocou tabuľky s dvoma riadkami a to takto: Do druhého riadku budeme zapisovať prvočíselné delitele (prvočísla) a do prvého podiely (tie budeme v každom ďalšom kroku rozkladať na súčin prvočísla a nového podielu).

Nasledujúca tabuľka znázorňuje prvočíselný rozklad čísla 210, podľa opísaného postupu.

210	105	35	7	1
	2	3	5	7

Tabuľka 1.3: Tabuľka určujúca prvočíselný rozklad čísla 210.

Ako vytvoríme takú tabuľku?

1. Na začiatku si vytvoríme tabuľku s dvoma riadkami, s piatimi stĺpcami (v tomto prípade počet stĺpcov poznáme, ale v prípade, že tomu tak nie je, si zaznačíme aspoň dva stĺpce a v prípade potreby dokresľujeme ďalsie).
2. Zapíšeme do ľavého horného rohu (prvý riadok, prvý stĺpec) číslo, ktorého prvočíselný rozklad hľadáme, tj. číslo 210.

3. Číslo 210 je párne – je deliteľné číslom 2 (to je jeho prvý prvočíselný deliteľ). Po vydelení čísla 210 číslom 2 dostaneme podiel 105. Pretože číslo 2 je prvočíselným deliteľom, zapíšeme ho do druhého stĺpca, do druhého riadku. Podiel, číslo 105, zapíšeme do prvého riadku toho istého stĺpca.
4. Teraz rozložíme na súčin číslo 105. Toto číslo je deliteľné číslom 3 (druhý prvočíselný deliteľ). Podiel po vydelení čísla 105 číslom 3 je číslo 35. Do nového stĺpca (tretí stĺpec) zapíšeme – prvý riadok číslo 35 a druhý riadok číslo 3.
5. Teraz rozložíme číslo 35 na súčin čísel 5 a 7. Do štvrtého stĺpca zapíšeme postupne 7, 5.
6. Nakoniec už zostane len rozložiť číslo 7, čo je už prvočíslo (tj. posledný hľadaný prvočíselný deliteľ). Číslo 7 rozložíme na súčin čísel 7 a 1. Tieto čísla zapíšeme do posledného stĺpca tabuľky.
7. Ak dostaneme číslo 1 (posledný podiel), tabuľka je hotová - číslo 210 sme rozložili na súčin prvočísel.

Prvočíselný rozklad čísla 210 teraz prečítame z druhého riadku, tj. je to súčin prvočísel 2, 3, 5 a 7.

Prvočíselný rozklad čísla zapisujeme pomocou mocnín prvočísel. Základy mocnín prvočísel zoradíme vždy vzostupne. Vďaka Základnej vety aritmetiky je tento rozklad vždy jednoznačný.

**Veta 4.** (Základná veta aritmetiky)

*Každé prirodzené číslo  $n > 1$  možno zapísať jednoznačne (jediným spôsobom) v tvare*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_k^{r_k},$$

kde  $k \in \mathbb{N}$ ,  $p_1 < p_2 < \dots < p_k$  sú prvočísla a  $r_1, r_2, \dots, r_k \in \mathbb{N}$  sú ich násobnosti.

*Dôkaz.* Dôkaz Základnej vety aritmetiky neuvádzame, možno ho nájsť napríklad v knihe [21], str. 51.  $\square$

Použitím prvočíselného rozkladu môžeme dokázať nasledujúci vzťah medzi najmenším spoločným násobkom a najväčším spoločným deliteľom.

**Veta 5.** Pre každé dve prirodzené čísla  $a, b$  platí

$$a \cdot b = n(a, b) \cdot D(a, b).$$

*Dôkaz.* Prvočíselné rozklady čísel  $a, b$  sú

$$\begin{aligned} a &= p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m}, \\ b &= p_1^{l_1} \cdot p_2^{l_2} \cdot \dots \cdot p_m^{l_m}, \end{aligned}$$

kde  $m \in \mathbb{N}$ ,  $p_1, p_2, \dots, p_m$  sú prvočísla,  $k_1, k_2, \dots, k_m, l_1, l_2, \dots, l_m \in \mathbb{N}_0$ .

Pre najväčší spoločný deliteľ  $D(a, b)$  čísel  $a, b$  platí

$$D(a, b) = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m},$$

kde  $s_i$  je najmenší spoločný mocniteľ u prvočísla  $p_i$ , resp. minimum z čísel  $k_i, l_i$ , pre každé  $i \in \{1, 2, \dots, m\}$ .

Pre najmenší spoločný násobok  $n(a, b)$  čísel  $a, b$  platí

$$n(a, b) = p_1^{r_1} \cdot p_2^{r_2} \cdots \cdot p_m^{r_m},$$

kde  $r_i$  je najväčší spoločný mocniteľ u prvočísla  $p_i$ , resp. maximum z čísel  $k_i, l_i$ , pre každé  $i \in \{1, 2, \dots, m\}$ .

Všimnite si, že platí  $k_i + l_i = r_i + s_i$  pre každé  $i \in \{1, 2, \dots, m\}$ , a preto

$$\begin{aligned} n(a, b) \cdot D(a, b) &= (p_1^{r_1} \cdot p_2^{r_2} \cdots \cdot p_m^{r_m}) \cdot (p_1^{s_1} \cdot p_2^{s_2} \cdots \cdot p_m^{s_m}) \\ &= p_1^{r_1+s_1} \cdot p_2^{r_2+s_2} \cdots \cdot p_m^{r_m+s_m} \\ &= p_1^{k_1+l_1} \cdot p_2^{k_2+l_2} \cdots \cdot p_m^{k_m+l_m} \\ &= (p_1^{k_1} \cdot p_2^{k_2} \cdots \cdot p_m^{k_m}) \cdot (p_1^{l_1} \cdot p_2^{l_2} \cdots \cdot p_m^{l_m}) \\ &= a \cdot b. \end{aligned}$$

□

**Príklad 5.** Nájdite  $b \in \mathbb{N}$ , ak viete, že platí:

$$a = 15, \quad D(a, b) = 3, \quad n(a, b) = 45.$$

*Riešenie:* Podľa predchádzajúceho tvrdenia vieme, že platí  $ab = n(a, b) \cdot D(a, b)$ . Preto číslo  $b$  určíme zo vzťahu

$$b = \frac{n(a, b) \cdot D(a, b)}{a} = \frac{45 \cdot 3}{15} = 9.$$

Na zefektívnenie hľadania prvočíselného rozkladu nám poslúží nasledujúce tvrdenie.

**Veta 6.** Každé zložené číslo  $n > 1$  je deliteľné aspoň jedným prvočíslom  $p$ , pre ktoré platí  $p \leq \sqrt{n}$ .

*Dôkaz.* Nech  $n$  je zložené číslo, tj. má aspoň 3 delitele.

Ak má číslo  $n$  práve 3 delitele ( $1, n$  a prvočíslo  $p$ ), musí platiť  $n = p^2$ . Preto platí  $p = \sqrt{n}$ .

Ak má číslo  $n$  viac ako 3 delitele, existujú aspoň dve prvočísla  $p_1$  a  $p_2$ , ktoré spĺňajú  $p_1 \leq p_2$  a súčasne  $p_1 \cdot p_2 \leq n$ . (Napríklad pre  $n = 6$  to je  $p_1 = 2, p_2 = 3$ , pre číslo  $n = 8$  je  $p_1 = p_2 = 2$ .) Pretože platí

$$p_1 \cdot p_1 \leq p_1 \cdot p_2 \leq n,$$

musí platiť nerovnosť  $p_1 \leq \sqrt{n}$ . To je presne to, čo sme chceli dokázať. □

**Príklad 6.** Určte prvočíselný rozklad čísla 3 103.

*Riešenie:* Na nájdenie jedného prvočíselného deliteľa čísla 3 103 nám podľa Vety 6 stačí overiť, či číslo 3 103 je deliteľné nejakým prvočíslom menším alebo rovným ako  $\sqrt{3 103} \doteq 55.7$ , tj. stačí hľadať medzi prvočíslami menšími ako číslo 56. Všetky uvažované prvočísla sú 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 a 53. Z týchto čísel vyhovuje jedine číslo 29. Podiel po vydelení čísla 3 103 prvočíslom 29 je 107. Číslo 107 je prvočíslo. Prvočíselný rozklad čísla 3 103 je súčin 29 · 107.

To, že 107 je prvočíslo sa dá overiť rovnakým postupom – stačí otestovať deliteľnosť prvočíslami, ktoré sú menšie ako  $\sqrt{107} \doteq 10.3$ , tj. číslami 2, 3, 5 a 7. Pretože žiadne z nich nedelí číslo 107, musí byť podľa Vety 6 číslo 107 prvočíslo.

## Cvičenia

1. Určte prvočíselný rozklad čísel 1 147 a 947.
2. Zapíšte prvočíselné rozklady týchto prirodzených čísel 24, 56, 200 a 321.
3. Pomocou prvočíselných rozkladov čísel 48 a 242 určte ich najväčšieho spoľného deliteľa a ich najmenší spoločný násobok.
4. Zistite, či niektoré z nasledujúcich čísel je prvočíslo:

557, 1 231, 2 419.

5. Po kol'kých pokusoch delenia čísla 1 001 prvočíslami 2, 3, 5, ... (v tomto poradí) budeme vedieť rozhodnúť, či toto číslo je prvočíslo?

## Výsledky cvičení

1.  $1 147 = 31 \cdot 37$ , 947 je prvočíslo.
2.  $24 = 2^3 \cdot 3$ ,  $56 = 2^3 \cdot 7$ ,  $200 = 2^3 \cdot 5^2$ ,  $321 = 3 \cdot 107$ .
3.  $48 = 2^4 \cdot 3$ ,  $242 = 2 \cdot 11^2$ ,  $n(48, 242) = 2^4 \cdot 3 \cdot 11^2$ ,  $D(48, 242) = 2$ .
4. Prvočísla sú čísla 557, 1 231.
5. Existuje 11 prvočísel menších alebo rovných ako číslo  $\sqrt{1\ 001}$ . Sú to čísla 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Číslo 1 001 nie je prvočíslo, pretože je deliteľné číslom 7. Stačia 4 pokusy.

# Kapitola 2

## Kritéria deliteľnosti

V tejto časti sa budeme venovať základným kritériám deliteľnosti. Kritéria deliteľnosti slúžia k rozhodovaniu, či je prirodzené číslo deliteľné určitým prirodzeným číslom a to tak, aby to bolo jednoduché aj bez použitia písomného delenia alebo kalkulačky. Zaoberať sa budeme kritériami deliteľnosti číslami 2 až 20.

### 2.1 Úvod do problematiky

Kritéria deliteľnosti sa určujú niekoľkými spôsobmi. Prvým spôsobom je určenie deliteľnosti pomocou posledných cifier čísla. Napríklad z poslednej cifry čísla môžeme určiť deliteľnosť číslom 2, 5 alebo 10. Z posledného dvojčísla môžeme rozhodnúť o deliteľnosti číslom 4. Pre deliteľnosť číslom 8 je rozhodujúce posledné trojčíslie.

Ďalšia možnosť je určiť deliteľnosť číslami zloženými z niekoľkých nesúdeliteľných deliteľov. Napríklad deliteľnosť číslom 6 zistíme pomocou deliteľnosti číslami 2 a 3, u čísla 10 pomocou čísel 2 a 5 a tiež u čísla 12 pomocou deliteľnosti číslami 3 a 4.

Univerzálnejšia metóda na určenie deliteľnosti nejakým číslom je pomocou nejakej celočíselnej lineárnej kombinácie jednotlivých cifier.

Nech  $n \in \mathbb{N}$  a jeho rozvinutý zápis je

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 = \sum_{i=0}^k (a_i \cdot 10^i),$$

kde  $k \in \mathbb{N}_0$ ,  $a_k \neq 0$ ,  $a_i \in \{0, 1, \dots, 9\}$  pre každé  $i \in \{0, 1, \dots, k\}$ . Potom **celočíselnou lineárnu kombináciou cifier** čísla  $n$  nazývame súčet

$$c_k \cdot a_k + c_{k-1} \cdot a_{k-1} + \dots + c_1 \cdot a_1 + c_0 \cdot a_0 = \sum_{i=0}^k (c_i \cdot a_i),$$

kde sú dané čísla  $c_i \in \mathbb{Z}$  pre každé  $i \in \{0, 1, \dots, k\}$ . Čísla  $c_i$  nazývame **koefficienty lineárnej kombinácie**.

Napríklad deliteľnosť číslom 3 máme zaručenú práve vtedy, keď ciferný súčet

je deliteľný troma (tj. všetky koeficienty lineárnej kombinácie cifier sú rovné číslu 1).

## 2.2 Kritéria deliteľnosti číslami 2 až 10

Na overovanie deliteľnosti číslami 2 až 10 nám poslúži nasledujúca veta:

**Veta 7.** (*Deliteľnosť číslom 2 až 10*)

*Prirodzené číslo  $n$  je deliteľné číslom:*

- a) 2 práve vtedy, keď je jeho posledná cifra 0, 2, 4, 6 alebo 8,
- b) 3 práve vtedy, keď je jeho ciferný súčet deliteľný 3,
- c) 4 práve vtedy, keď je jeho posledné dvojčíslo deliteľné 4,
- d) 5 práve vtedy, keď je jeho posledná cifra 0 alebo 5,
- e) 6 práve vtedy, keď je deliteľné 2 a 3,
- f) 7 práve vtedy, keď dvojnásobok počtu stoviek zväčšený o posledné dvojčíslo je deliteľný 7,
- g) 8 práve vtedy, keď je posledné trojčíslo deliteľné 8,
- h) 9 práve vtedy, keď je jeho ciferný súčet deliteľný 9,
- i) 10 práve vtedy, keď je posledná cifra 0.

*Poznámka.* Počet stoviek znamená číslo, ktoré dostaneme vyškrtnutím jeho posledných dvoch cifier. Napríklad číslo 1 234 567 má počet stoviek rovný číslu 12 345.

*Dôkaz.* Dôkaz rozdelíme do niekolkých častí. V prvej časti dokážeme kritéria na overovanie deliteľnosti číslami 2, 5 a 10. V druhej časti overíme tvrdenia pre deliteľnosť číslami 3, 9 a čísla 6. Potom v ďalšej časti dokážeme kritéria pre čísla 4 a 8. Nakoniec ukážeme platnosť overovacieho kritéria pre číslo 7.

*Čo budeme v dôkaze potrebovať/využívať*

- V celom dôkaze budeme rozvinutým zápisom čísla  $n$  označovať zápis

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

kde  $k \in \mathbb{N}_0$ ,  $a_k \neq 0$  a  $a_i \in \{0, 1, 2, \dots, 9\}$  pre každé  $i \in \{0, 1, 2, \dots, k\}$ .

- V dôkaze budeme využívať nasledovne pomocné tvrdenie.

*Pomocné tvrdenie.* Pre každé  $x, y, z \in \mathbb{N}$  platí

$$(z \mid x \wedge z \mid y) \Rightarrow z \mid (x + y), \quad (2.1)$$

$$(z \mid x \wedge z \mid y) \Rightarrow z \mid (x - y), \quad (2.2)$$

$$z \mid x \Rightarrow z \mid (xy), \quad (2.3)$$

$$(z \mid x \wedge y \mid x) \Leftrightarrow zy \mid x, \text{ kde } D(z, y) = 1. \quad (2.4)$$

*Dôkaz.* „Dôkaz tvrdení (2.1) a (2.2).“

Pretože  $z \mid x$  a  $z \mid y$  existujú čísla  $k, l \in \mathbb{N}$  také, že  $x = k \cdot z$  a  $y = l \cdot z$ .

Z toho vyplýva, že  $x + y = kz + lz = (k + l) \cdot z$ , tj.  $z \mid (x + y)$ . Súčasne platí  $x - y = kz - lz = (k - l) \cdot z$ , tj.  $z \mid (x - y)$ .

„Dôkaz tvrdenia (2.3).“

Z predpokladu  $z \mid x$  plynie existencia čísla  $k \in \mathbb{N}$  splňajúceho  $x = k \cdot z$ .

Ak vynásobíme obe strany rovnice  $x = k \cdot z$  číslom  $y$ , dostaneme  $xy = ky \cdot z$ . To znamená, že platí  $z \mid (xy)$ .

„Dôkaz tvrdenia (2.4).“

Pretože čísla  $y$  a  $z$  sú navzájom nesúdeliteľné a sú deliteľmi čísla  $x$ , musí byť aj číslo  $zy$  deliteľom čísla  $x$ , tj. musí platiť  $zy \mid x$ .

□

Teraz dokážeme vetu 7.

*1.časť* - Dôkaz tvrdení a), d) a i).

Úpravami rozvinutého zápisu prirodzeného čísla  $n$  dostaneme

$$n = \underbrace{a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10}_{10 \cdot \underbrace{(a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_2 \cdot 10^1 + a_1)}_A} + a_0 = 10 \cdot A + a_0.$$

Prípadne zápis predchádzajúceho pomocou sumičného znaku  $\sum$  je

$$n = \underbrace{\sum_{i=1}^k (a_i \cdot 10^i)}_{10 \cdot \underbrace{\sum_{i=1}^{k-1} (a_i \cdot 10^{i-1})}_A} + a_0 = 10 \cdot A + a_0.$$

Je zrejmé, že súčin  $10 \cdot A$  je vždy deliteľný číslami 2, 5 aj 10.

Miesto čísel 2, 5, 10 budeme ďalej používať symbol  $T$ , tj.  $T \in \{2, 5, 10\}$ .

Dokážeme ekvivalenciu „ $T \mid n \Leftrightarrow T \mid a_0$ “ pomocou priameho dôkazu (tj. dokážeme implikáciu „ $T \mid n \Rightarrow T \mid a_0$ “ a implikáciu „ $T \mid a_0 \Rightarrow T \mid n$ “).

*Dôkaz implikácie „ $T \mid n \Rightarrow T \mid a_0$ “:*

Nech platí  $T \mid n$ , tj.  $T \mid (10 \cdot A + a_0)$ . Vieme, že platí  $T \mid (10 \cdot A)$ . Potom podľa tvrdenia (2.2) musí platiť  $T \mid a_0$ .

*Dôkaz implikácie „ $T \mid a_0 \Rightarrow T \mid n$ “:*

Nech platí  $T \mid a_0$ . Súčasne vieme, že platí  $T \mid (10 \cdot A)$ . To znamená, že podľa tvrdenia (2.1) musí platiť  $T \mid (10 \cdot A + a_0)$ , tj.  $T \mid n$ .

V predchádzajúcim kroku sme dokázali ekvivalenciu „ $T \mid n \Leftrightarrow T \mid a_0$ “ pre  $T \in \{2, 5, 10\}$ , a tým aj tvrdenia a), d), i):

- $2 \mid n$  práve vtedy, keď  $2 \mid a_0$ , tj.  $a_0 \in \{0, 2, 4, 6, 8\}$ ,
- $5 \mid n$  práve vtedy, keď  $5 \mid a_0$ , tj.  $a_0 \in \{0, 5\}$ ,

- $10 \mid n$  práve vtedy, keď  $10 \mid a_0$ , tj.  $a_0 = 0$ .

*2.časť - Dôkaz tvrdení b), h) a e).*

Uvažujme teraz ciferný súčet čísla  $n$ , tj. súčet

$$s = a_k + a_{k-1} + \dots + a_1 + a_0 = \sum_{i=0}^k a_i.$$

Pre rozdiel čísla  $n$  a čísla  $s$  platí

$$\begin{aligned} n - s &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\quad - (a_k + a_{k-1} + \dots + a_1 + a_0) \\ &= a_k \cdot (10^k - 1) + a_{k-1} \cdot (10^{k-1} - 1) + \dots + a_2 \cdot 99 + a_1 \cdot 9. \end{aligned}$$

Zápis predchádzajúceho napísaný pomocou  $\sum$  je

$$\begin{aligned} n - s &= \sum_{i=0}^k 10^i a_i - \sum_{i=0}^k a_i = \sum_{i=0}^k (10^i a_i - a_i) \\ &= \sum_{i=2}^k (10^i a_i - a_i) + 10 \cdot a_1 - a_1 = \sum_{i=2}^k (10^i - 1) a_i + 9 a_1. \end{aligned}$$

Všimnite si, že pre každé prirodzené číslo  $i > 0$  číslo  $10^i - 1$  pozostáva zo samých deviatok, napríklad pre  $i = 1$  je to číslo 9, pre  $i = 2$  číslo 99, pre  $i = 3$  číslo 999 atď. Čísla, ktorých všetky cifry sú čísla 9, sú vždy deliteľné číslom 3 aj číslom 9. Preto platí  $3 \mid (n - s)$  a  $9 \mid (n - s)$ .

To isté môžeme vidieť, ak použijeme vzorec pre rozdiel  $i$ -tých mocnín, konkrétnie pre mocniny  $10^i$  a 1. Potom dostaneme

$$\begin{aligned} n - s &= \sum_{i=2}^k (10^i - 1) a_i + 9 a_1 \\ &= \sum_{i=2}^k (10 - 1) \cdot (10^{i-1} + \dots + 1) \cdot a_i + 9 a_1 = \sum_{i=2}^k 9 \cdot (10^{i-1} + \dots + 1) a_i + 9 a_1. \end{aligned}$$

Odtiaľ zrejme platí, že posledný výraz je deliteľný ako číslom 3, tak aj číslom 9, tj. platí  $3 \mid (n - s)$  a  $9 \mid (n - s)$ .

Pre  $T \in \{3, 9\}$  dokážeme, že platí „ $T \mid n \Leftrightarrow T \mid s$ “.

*Dôkaz implikácie „ $T \mid s \Rightarrow T \mid n$ “:*

Vieme, že platí  $T \mid (n - s)$  a predpokladáme, že  $T \mid s$ . Potom podľa tvrdenia (2.1) musí platiť  $T \mid n$ .

*Dôkaz implikácie „ $T \mid n \Rightarrow T \mid s$ “:*

Platí, že  $T \mid (n - s)$  a predpokladáme, že  $T \mid n$ . Potom podľa tvrdenia (2.2) musí platiť  $T \mid s$ .

Dôkazom ekvivalencie „ $T \mid n \Leftrightarrow T \mid s$ “ pre  $T \in \{3, 9\}$  sme dokázali platnosť tvrdení b), h):

- $3 \mid n$  práve vtedy, keď  $3 \mid s$ ,
- $9 \mid n$  práve vtedy, keď  $9 \mid s$ .

Pretože číslo 6 sa dá napísať ako súčin dvoch nesúdeliteľných čísel, súčin čísel 2 a 3, vďaka tvrdeniu (2.4) dostávame kritérium na deliteľnosť číslom 6. Platí tvrdenie e):

- $6 \mid n$  práve vtedy, keď  $2 \mid n$  a súčasne  $3 \mid n$ .

*3.časť - Dôkaz tvrdení c), g).*

Pre každé prirodzené číslo  $i > 1$  platí, že

$$10^i = 2^2 \cdot 5^2 \cdot 10^{i-2} = 4 \cdot 5^2 \cdot 10^{i-2}.$$

To znamená, že číslo  $10^i$  pre  $i > 1$  je vždy deliteľné číslom 4. Vďaka tejto deliteľnosti a toho, že platí

$$n = \underbrace{a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_2 \cdot 10^2}_{A} + a_1 \cdot 10 + a_0 = A + a_1 \cdot 10 + a_0,$$

musí platiť  $4 \mid A$ . Pre deliteľnosť číslom 4 je preto rozhodujúce posledné dvojčíslie.

Teraz dokážeme ekvivalenciu „ $4 \mid n \Leftrightarrow 4 \mid (a_1 \cdot 10 + a_0)$ “.

*Dôkaz implikácie „ $4 \mid (a_1 \cdot 10 + a_0) \Rightarrow 4 \mid n$ “:*

Vieme, že  $4 \mid A$  a predpokladáme, že  $4 \mid (a_1 \cdot 10 + a_0)$ . Podľa tvrdenia (2.1) je splnené  $4 \mid n$ .

*Dôkaz implikácie „ $4 \mid n \Rightarrow 4 \mid (a_1 \cdot 10 + a_0)$ “:*

Predpokladáme, že  $4 \mid n$  a vieme, že  $4 \mid A$ . Potom podľa tvrdenia (2.2) platí  $4 \mid (a_1 \cdot 10 + a_0)$ .

Dokázali sme tvrdenie c):

- $4 \mid n$  práve vtedy, keď  $4 \mid (a_1 \cdot 10 + a_0)$ .

Rovnako môžeme dokázať tvrdenie g). Stačí vychádzať z toho, že pre každé prirodzené číslo  $i > 2$  platí  $10^i = 8 \cdot 5^3 \cdot 10^{i-3}$ . Tvrdenie g) je:

- $8 \mid n$  práve vtedy, keď  $8 \mid (a_2 \cdot 100 + a_1 \cdot 10 + a_0)$ .

*4.časť - Dôkaz tvrdenia f).*

U deliteľnosti číslom 7 uvažujme číslo

$$m = 2 \cdot a_k \cdot 10^{k-2} + \dots + 2 \cdot a_2 + 10 \cdot a_1 + a_0 = \sum_{i=2}^k (2 \cdot 10^{k-2} \cdot a_i) + 10 \cdot a_1 + a_0,$$

kde  $k \in \mathbb{N}_0$  a čísla  $a_i \in \{0, 1, 2, \dots, 9\}$  pre  $i \in \{0, 1, 2, \dots, k\}$  sú cifry čísla  $n$ . Potom platí

$$\begin{aligned} n - m &= 10^k \cdot a_k + 10^{k-1} \cdot a_{k-1} + \dots + 10 \cdot a_1 + a_0 \\ &\quad - (2 \cdot a_k \cdot 10^{k-2} + \dots + 2 \cdot a_2 + 10 \cdot a_1 + a_0) \\ &= 98 \cdot a_k \cdot 10^{k-2} + \dots + 98 \cdot a_2. \end{aligned}$$

Pretože  $7 \mid 98$  je rozdiel  $n - m$  deliteľný číslom 7 (stačí použiť tvrdenie (2.3)). Podobne ako v predchádzajúcich častiach, využitím pomocných tvrdení (2.1) a (2.2) dostaneme:

- $7 \mid n$  práve vtedy, keď  $7 \mid m$ .

□

Najkomplikovanejšie kritérium máme pri deliteľnosti číslom 7. Preto si ukážeme použitie tohto kritéria na nasledujúcom príklade.

**Príklad 7.** Zistite, či číslo 3 584 je deliteľné číslom 7.

*Riešenie:* Podľa vety na overenie deliteľnosti číslom 7 musíme najprv vypočítať dvojnásobok počtu stoviek čísla 3 584, a potom k nemu pripočítať posledné dvojčíslo, tj.

$$2 \cdot 35 + 84 = 154.$$

Pretože je toto číslo deliteľné číslom 7, musí byť aj číslo 3 584 deliteľné číslom 7.

## 2.3 Kritéria deliteľnosti prvočíslami 11 až 20

**Veta 8.** (*Kritérium deliteľnosti číslom 11*)

Nech  $k \in \mathbb{N}_0$  a

$$n = \sum_{i=0}^k 10^i a_i \text{ pre } a_i \in \{0, 1, \dots, 9\}, \quad a_k \neq 0,$$

tj.  $a_k, \dots, a_0$  sú cifry prirodzeného čísla  $n$ . Potom

$$11 \mid n \iff 11 \mid \left( \sum_{i=0}^k (-1)^i a_i \right). \quad (2.5)$$

*Dôkaz.* Dokážeme najprv implikáciu „ $\Leftarrow$ “.

Označme

$$S = \left( \sum_{i=0}^k (-1)^i a_i \right).$$

Predpokladáme, že  $11 \mid S$ .

Platí, že

$$n - S = \sum_{i=0}^k (10^i a_i) - \sum_{i=0}^k (-1)^i a_i = \sum_{i=0}^k (10^i - (-1)^i) a_i.$$

Použitím vzorca pre rozdiel dvoch  $i$ -tých mocnín (rozdielu  $10^i - (-1)^i$ ) dostaneme

$$m = 10^i - (-1)^i = \underbrace{(10+1)}_{11} \cdot [10^{n-1} + 10^{n-2} \cdot (-1) + \dots + 10 \cdot (-1)^{n-2} + (-1)^{n-1}] .$$

Odtiaľ je zrejmé, že  $m$  je deliteľné číslom 11, a preto musí byť aj rozdiel  $n - S$  deliteľný číslom 11. Pomocou (2.1) a (2.2) a predpokladu  $11 \mid S$  dostávame  $11 \mid n$ .

Dôkaz obrátenej implikácie „ $\Rightarrow$ “.

Predpokladáme, že  $11 \mid n$ . Podobne ako v predchádzajúcim kroku  $m = n - S$  je deliteľné číslom 11. Preto opäť pomocou (2.1) a (2.2) platí  $11 \mid S$ . □

**Príklad 8.** Zistite, či číslo 5 082 je deliteľné číslom 11.

*Riešenie:* Najprv musíme vypočítať  $\sum_{i=0}^3 (-1)^i a_i$ , kde  $a_i$  sú cifry prirodzeného čísla 5 082. Pretože

$$S = \sum_{i=0}^3 (-1)^i a_i = (-1)^0 \cdot 2 + (-1)^1 \cdot 8 + (-1)^2 \cdot 0 + (-1)^3 \cdot 5 = 2 - 8 - 0 - 5 = -11$$

a  $11 \mid S$ , je číslo 5 082 deliteľné číslom 11 podľa kritéria z Vety 8.

Teraz nasledujú vety určujúce kritérium deliteľnosti číslom 13, 17 a 19. Dôkazy týchto viet neuvádzame, pretože sa urobia analogicky ako pre Vetu 7 a Vetu 8.

**Veta 9.** (Deliteľnosť číslom 13)

*Prirodzené číslo je deliteľné číslom 13, ak štvornásobok poslednej cifry pripočítaný k desiatkam je deliteľný 13.*

**Príklad 9.** Zistite, či číslo 1 105 je deliteľné číslom 13.

*Riešenie:* Podľa Vety 9 musíme zistiť, či štvornásobok poslednej cifry pripočítaný k desiatkam je deliteľný číslom 13. Platí

$$4 \cdot 5 + 110 = 130.$$

Číslo 130 je deliteľné číslom 13, a preto  $13 \mid 1105$ .

**Veta 10.** (Deliteľnosť číslom 17)

*Prirodzené číslo je deliteľné číslom 17, ak pätnásobok poslednej cifry odčítaný od desiatok je deliteľný 17.*

**Príklad 10.** Zistite, či číslo 16 371 je deliteľné číslom 17.

*Riešenie:* Využijeme Vetu 10. Pätnásobok poslednej cifry odčítaný od desiatok je rovný 1 632 ( $= 1637 - 5 \cdot 1$ ). Aplikujeme tento spôsob aj na číslo 1 632, dostaneme číslo 153 ( $= 163 - 5 \cdot 2$ ). Ak to zopakujeme ešte raz aj pre číslo 153, získame číslo 0 ( $= 15 - 5 \cdot 3$ ). Číslo 0 je deliteľné číslom 17, a preto aj čísla 153, 1 632 aj 16 371 sú deliteľné číslom 17.

**Veta 11.** (Deliteľnosť číslom 19)

*Prirodzené číslo je deliteľné číslom 19, ak dvojnásobok poslednej cifry pripočítaný k desiatkam je deliteľný 19.*

Pomocou súčtu celočíselných násobkov jednotlivých cifier môžeme určiť deliteľnosť číslami 12, 14, 15, 16, 18 a 20.

**Veta 12.** (Deliteľnosť číslami 12, 14, 15, 16, 18 a 20)

Nech  $n \in \mathbb{N}$  a nech

$$n = \sum_{i=0}^k 10^i a_i,$$

kde  $k \in \mathbb{N}_0$ ,  $a_i \in \{0, 1, \dots, 9\}$  a  $a_k \neq 0$ , je jeho rozvinutý zápis. Potom prirodzené číslo  $n$  je deliteľné číslom:

- a) 12 práve vtedy, keď je deliteľné tromi a štyrmi,
- b) 14 práve vtedy, keď je deliteľné dvomi a siedmimi,
- c) 15 práve vtedy, keď je deliteľné tromi a piatimi,
- d) 16 práve vtedy, keď posledné štvorčíslie čísla  $n$  je deliteľné šestnásťimi,
- e) 18 práve vtedy, keď je deliteľné dvomi a deviatimi,
- f) 20 práve vtedy, keď je deliteľné štyrmi a piatimi.

*Dôkaz.* Dôkaz Vety 12 sa spraví podobným spôsobom ako dôkaz Vety 7. K dôkazu sa využijú tvrdenie (2.4), tj. môžeme využiť fakt, že čísla 12, 14, 15, 18 a 20 možno napísť ako súčin dvoch nesúdeliteľných čísel. Platí, že

$$\begin{aligned} 12 &= 3 \cdot 4, & 14 &= 2 \cdot 7, & 15 &= 3 \cdot 5, \\ 18 &= 2 \cdot 9, & 20 &= 4 \cdot 5. \end{aligned}$$

Odtiaľ sú zrejmé tvrdenia a), b), c), e) a f).

Tvrdenie d) vychádza z faktu, že pre každé prirodzené číslo  $i > 3$  platí

$$10^i = 10^4 \cdot 10^{i-4} = 16 \cdot 625 \cdot 10^{i-4}.$$

□

*Poznámka.* Kritéria deliteľnosti môžu byť formulované aj inak.

Napríklad pre každé prirodzené číslo  $n$  platí:

- Číslo  $n$  je deliteľné číslom 7 práve vtedy, keď číslom 7 je deliteľný rozdiel súčtu jeho nepárnych a párných trojíc cifier.

$$\begin{aligned} 7 \mid 103\,671\,316 &\Leftrightarrow 7 \mid (316 - 671 + 103), \\ 7 \mid 25\,501\,007 &\Leftrightarrow 7 \mid (007 - 501 + 025). \end{aligned}$$

- Číslo  $n$  je deliteľné číslom 11 práve vtedy, keď číslom 11 je deliteľný súčet jednotlivých dvojčísel čísla  $n$ .

$$\begin{aligned} 11 \mid 6\,589 &\Leftrightarrow 11 \mid (89 + 65), \\ 11 \mid 74\,151 &\Leftrightarrow 11 \mid (51 + 41 + 07). \end{aligned}$$

## Cvičenia

1. Určte, ktoré z nasledujúcich čísel je deliteľné číslom 2, 3, 4, 5, 6, 7, 8, 9 alebo 10:  
123, 147, 263, 369, 1 000, 1 240.
2. Zistite, či číslo 332 211 je deliteľné číslom 11, 13, 17 alebo 19.

## Výsledky cvičení

1. Odpoveď je zapísaná do tabuľky.

Číslo	Delitele
123	3,
147	3, 7
263	
369	3, 9
1 000	2, 4, 5, 8, 10
1 240	2, 4, 5, 8, 10

2. Je deliteľné len číslom 11.

# Kapitola 3

## Diofantické rovnice

V tejto kapitole sa zoznámite s lineárnymi diofantickými rovnicami, ktorých názov je odvodený od mena gréckeho matematika Diofanta. Sú to rovnice, ktorých riešenie sa hľadá medzi celými číslami. Typicky sú tieto rovnice charakteristické tým, že máme väčší počet neznámych ako rovníc.

V prvej kapitole sme zaviedli dôležité pojmy týkajúce sa deliteľnosti prirodzených čísel. Analogicky môžeme definovať zavedené pojmy i pre celé čísla. Deliteľnosť celých čísel budeme využívať v tejto kapitole.

Viac o diofantických rovniciach sa môžete dočítať napr. v knihe [5].

*Poznámka.* Deliteľnosť celých čísel: Do množiny celých čísel patria všetky prirodzené čísla, čísla k nim opačné (záporné čísla) a nula. O deliteľnosti prirodzených čísel sme sa dozvedeli v kapitole 1. Nula je deliteľná každým nenulovým celým číslom. U deliteľnosti záporných čísel platí: Ak  $a \in \mathbb{Z}$  a  $a < 0$ , potom  $-a \in \mathbb{N}$ . Nech  $k_1, k_2, \dots, k_n$  sú všetky delitele čísla  $-a$ , potom všetky delitele čísla  $a$  sú čísla  $k_1, k_2, \dots, k_n$  a  $-k_1, -k_2, \dots, -k_n$ .

### 3.1 Lineárne diofantické rovnice

**Lineárnymi diofantickými rovnicami s  $n$  neznámymi**  $x_1, x_2, \dots, x_n \in \mathbb{Z}$  nazívame všetky rovnice s koeficientami  $a_1, a_2, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ ,  $c \in \mathbb{Z}$ , ktorých riešenie hľadáme medzi celými číslami. Sú to rovnice tvaru

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c.$$

Lineárne diofantické rovnice sú rovnice, ktorých existencia celočíselného riešenia vychádza zo znalosti najväčšieho spoločného deliteľa. Pokiaľ koeficienty tejto rovnice budú mať najväčšieho spoločného deliteľa, ktorý nedelí číslo na pravej strane, ihneď môžeme povedať, že daná rovnica nemá celočíselné riešenie. Pokiaľ ale najväčší spoločný deliteľ koeficientov bude deliť pravú stranu diofantickej rovnice, takáto rovnica bude mať nekonečne mnoho celočíselných riešení. Aby sme ich určili všetky, stačí nám nájsť jedno riešenie a všetky ostatné z neho jednoducho vypočítať.

Ďalej sa budeme venovať len lineárnym diofantickým rovniciam s dvoma neznámymi.

### 3.1.1 Lineárne diofantické rovnice s dvoma neznámymi

**Lineárna diofantická rovnica s dvoma neznámymi**  $x, y \in \mathbb{Z}$  je rovnicou tvaru

$$ax + by = c, \quad (3.1)$$

kde  $a, b \in \mathbb{Z} \setminus \{0\}$ ,  $c \in \mathbb{Z}$ .

Riešenia rovnice (3.1) budeme ďalej zapisovať ako usporiadanú dvojicu  $[x, y]$ .

V prípade, že pravá strana rovnice (3.1) je nulová, tj.  $c = 0$ , máme vždy zaručenú existenciu riešenia. Jedno z riešení je určite riešenie triviálne,  $x = y = 0$ . Predpokladajme ale, že existuje netriviálne riešenie  $x, y \neq 0$ , a upravme rovnicu na nasledujúci tvar

$$\frac{x}{y} = -\frac{b}{a}. \quad (3.2)$$

Ak označíme najväčšieho spoločného deliteľa čísel  $a, b$  ako  $D(a, b)$ , potom existujú čísla  $k, l \in \mathbb{Z}$  také, že

$$a = k \cdot D(a, b), \quad b = l \cdot D(a, b).$$

Dosadením týchto vzťahov do rovnice (3.2) dostaneme

$$\frac{x}{y} = -\frac{l}{k},$$

kde  $D(k, l) = 1$ . Čo zrejme naznačuje jedno netriviálne riešenie – usporiadanú dvojicu  $[x, y] = [l, -k]$ . Ostatné riešenia dostaneme vynásobením nejakým nenulovým celočíselným násobkom.

Všetky netriviálne riešenia lineárnej diofantickej rovnice s dvoma neznámymi (rovnica (3.1)) s  $c = 0$  sú tvaru

$$[x, y] = \left[ t \cdot \frac{b}{D(a, b)}, t \cdot \frac{-a}{D(a, b)} \right],$$

kde  $t \in \mathbb{Z} \setminus \{0\}$ . (V prípade triviálneho riešenia stačí položiť  $t = 0$ .)

**Príklad 11.** Nájdite všetky riešenia rovnice

$$11x + 2y = 0,$$

kde  $x, y \in \mathbb{Z}$ .

*Riešenie:* Pravá strana rovnice je číslo 0, preto je daná rovnica riešiteľná. Označme  $a = 11$ ,  $b = 2$ . Najväčší spoločný deliteľ  $D(a, b)$  čísel  $a, b$  je číslo 1. Podľa predchádzajúceho všetky riešenia rovnice  $11x + 2y = 0$  majú tvar

$$[x, y] = [2 \cdot t, -11 \cdot t],$$

kde  $t \in \mathbb{Z}$ .

V prípade, keď  $c \neq 0$  je situácia o niečo zložitejšia. Takéto rovnice nemusia byť vždy riešiteľné. Napríklad rovnica  $2x + 4y = 5$  nemá celočíselné riešenie. Spôsob ako určiť riešenia, popisuje nasledujúca veta.

**Veta 13.** (*Existencia riešenia lineárnej diofantickej rovnice s 2 neznámymi*)

Lineárna diofantická rovnica typu  $ax + by = c$ , kde  $a, b \in \mathbb{Z} \setminus \{0\}$ ,  $c \in \mathbb{Z}$ , má riešenie práve vtedy, keď  $D(a, b) \mid c$ .

*Dôkaz.* Najprv dokážeme implikáciu „Ak lineárna diofantická rovnica  $ax + by = c$  má riešenie, potom  $D(a, b) \mid c$ .“ Predpokladáme, že riešenie rovnice  $ax + by = c$  existuje, označujeme ho  $[u, v]$ , kde  $u, v \in \mathbb{Z}$ . Nech  $d$  označuje spoločného deliteľa čísel  $a, b$ . Po dosadení riešenia  $[u, v]$  do rovnice  $ax + by = c$  obdržíme  $au + bv = c$ . Ľavá strana tejto rovnosti je deliteľná číslom  $d$ , tj.  $d \mid (au + bv)$ . Aby platila rovnosť, to isté musí platiť aj pre pravú stranu, tj. musí platiť  $d \mid c$ . Toto odvodenie je splnené pre každého spoločného deliteľa čísel  $a, b$ , a preto platí  $D(a, b) \mid c$ .

Teraz dokážeme, implikáciu „Ak  $D(a, b) \mid c$ , potom lineárna diofantická rovnica má riešenie.“. Predpokladáme, že  $D(a, b) \mid c$ . Nech platí  $a = D(a, b) \cdot t$ ,  $b = D(a, b) \cdot s$ ,  $c = D(a, b) \cdot r$ , kde  $t, s, r \in \mathbb{Z}$ . Úpravami obdržíme

$$x = \frac{c - by}{a} = \frac{D(a, b) \cdot r}{D(a, b) \cdot t} - \frac{D(a, b) \cdot sy}{D(a, b) \cdot t} = \frac{r - sy}{t}.$$

Pretože čísla  $a, b, c$  sú pevne dané, tak máme pevne dané aj celé čísla  $r, s, t$ . Aby  $x \in \mathbb{Z}$  stačí, aby  $t \mid (r - sy)$ , čo je možné docieliť vhodnou voľbou  $y \in \mathbb{Z}$ . Znamená to, že za predpokladu  $D(a, b) \mid c$  je zaručená existencia celočíselné riešenie  $[x, y]$  rovnice  $ax + by = c$ .  $\square$

O počte a tvaru riešení hovorí nasledujúca veta. Pokial' je lineárna diofantická rovnica riešiteľná (je splnená podmienka  $D(a, b) \mid c$ ), tak riešení je nekonečne mnoho a na ich určenie nám stačí poznať jedno riešenie.

**Veta 14.** (*Riešenia lineárnej diofantickej rovnice*)

Ak je usporiadaná dvojica  $[x_0, y_0]$  jedno riešenie lineárnej diofantickej rovnice  $ax + by = c$ , kde  $a, b \in \mathbb{Z} \setminus \{0\}$ ,  $c \in \mathbb{Z}$ , potom všetky riešenia tejto rovnice sú

$$\left[ x_0 - \frac{b \cdot r}{D(a, b)}, y_0 + \frac{a \cdot r}{D(a, b)} \right],$$

kde  $r \in \mathbb{Z}$ .

*Dôkaz.* Nech  $a = D(a, b) \cdot t$ ,  $b = D(a, b) \cdot s$ , kde  $t, s$  sú nesúdeliteľné celé čísla, tj.  $D(t, s) = 1$ . Ďalej nech  $[x_0, y_0]$  a  $[x_1, y_1]$  sú dve riešenia rovnice  $ax + by = c$ . Potom platí

$$ax_0 + by_0 = ax_1 + by_1 = c.$$

Úpravami dostaneme

$$y_1 = \frac{a(x_0 - x_1)}{b} + y_0 = \frac{t(x_0 - x_1)}{s} + y_0.$$

Pretože  $D(t, s) = 1$  a  $y_1 \in \mathbb{Z}$ , musí platiť  $s \mid (x_0 - x_1)$ . Existuje preto  $r \in \mathbb{Z}$  také, že  $x_0 - x_1 = r \cdot s = r \cdot \frac{b}{D(a, b)}$ . Analogicky dostaneme  $y_1 - y_0 = r \cdot \frac{a}{D(a, b)}$ . Zo známeho riešenia  $[x_0, y_0]$  vypočítame ďalšie riešenie  $[x_1, y_1]$  nasledovne

$$\begin{aligned} x_1 &= x_0 - r \cdot \frac{b}{D(a, b)}, \\ y_1 &= y_0 + r \cdot \frac{a}{D(a, b)}, \end{aligned}$$

kde  $r \in \mathbb{Z}$ .  $\square$

**Príklad 12.** Riešte rovnicu  $2x + 3y = 1$ , kde  $x, y \in \mathbb{Z}$ .

*Riešenie:* Rovnica je lineárna diofantická rovnica s dvoma neznámymi a nenulovou pravou stranou. Označme  $a = 2, b = 3, c = 1$ . Najväčší spoločný deliteľ čísel  $a, b$  je  $D(a, b) = 1$ . Pretože platí  $D(a, b) \mid c$ , je táto rovница riešiteľná a riešení existuje nekonečne mnoho. Jedno riešenie je  $[x_0, y_0] = [-1, 1]$ . Všetky riešenia majú tvar  $[-1 - 3 \cdot r, 1 + 2 \cdot r]$ , kde  $r \in \mathbb{Z}$ .

**Príklad 13.** Vyjadrite číslo 3 v tvare  $21x + 15y$ , kde  $x, y \in \mathbb{Z}$ .

*Riešenie:* Úloha sa dá ekvivalentne formulovať i takto: Vyriešte diofantickú rovnicu  $21x + 15y = 3$ , kde  $x, y \in \mathbb{Z}$ .

Označme  $a = 21, b = 15, c = 3$ . Najväčší spoločný deliteľ čísel  $a, b$  je číslo  $D(a, b) = 3$ . Pretože platí  $D(a, b) \mid c$ , je táto úloha riešiteľná a riešení existuje nekonečne mnoho. Na vyjadrenie všetkých týchto riešení nám stačí určiť jedno. Na jeho nájdenie môžeme použiť Euklidov algoritmus pre čísla  $a = 21$  a  $b = 15$ . Pomocou Euklidovho algoritmu získame rovnosti

$$\begin{aligned} 21 &= 1 \cdot 15 + 6, \\ 15 &= 2 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Naším cieľom je vyjadriť číslo 3 (číslo na pravej strane diofantickej rovnice) pomocou čísel 21 a 15, čo sú koeficienty na ľavej strane diofantickej rovnice.

Ak číslo 3 vyjadríme z druhej rovnosti (dostaneme  $3 = 15 - 2 \cdot 6$ ) a číslo 6 vyjadríme z prvej rovnosti ( $6 = 21 - 1 \cdot 15$ ), môžeme číslo 3 napísat ako

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (21 - 1 \cdot 15) = -2 \cdot 21 + 3 \cdot 15.$$

To znamená, že jedno z možných riešení musí byť  $[x_0, y_0] = [-2, 3]$ . Všetky riešenia majú tvar  $[-2 - \frac{15r}{3}, 3 + \frac{21r}{3}]$ , kde  $r \in \mathbb{Z}$ .

### Cvičenia

- Zistite, či existujú celé čísla  $a, b$  splňajúce rovnicu

$$7a + 11b = 10.$$

- Nájdite všetky riešenia rovnice

$$3x - 5y = 1,$$

kde  $x, y \in \mathbb{Z}$ .

### Výsledky cvičení

- Existujú, pretože  $D(7, 11) \mid 10$ . Všetky riešenia sú tvaru  $[3 - 11r, -1 + 7r]$ , kde  $r \in \mathbb{Z}$ .
- $[2 + 5 \cdot r, 1 + 3 \cdot r]$ , kde  $r \in \mathbb{Z}$ .

## 3.2 Diofantické rovnice druhého stupňa

Medzi diofantické rovnice druhého stupňa zaraďujeme kvadratické diofantické rovnice, bilineárne diofantické rovnice, Pythagorejské rovnice alebo tiež Pellove rovnice, vid' Tab. 3.1.

Názov rovnice	Príklad rovnice	Zadané koeficienty	Neznáme
Kvadratická diofantická rovnica	$x^2 - y^2 = c$	$c \in \mathbb{N}$	$x, y \in \mathbb{Z}$
Bilineárna diofantická rovnica	$axy + bx + cy = d$	$a, b, c, d \in \mathbb{Z},$ $a, c$ nesúdeliteľné, $a, b, c \neq 0$	$x, y \in \mathbb{Z}$
Pythagorejské rovnice	$x^2 + y^2 = z^2$		$x, y, z \in \mathbb{N}$
Pellova rovnica	$x^2 + Dy^2 = 1$	$D \in \mathbb{N}$ , ktoré nie je druhou mocninou prirodzeného čísla	$x, y, z \in \mathbb{N}$

Tabuľka 3.1: Typy diofantických rovníc druhého stupňa.

My sa budeme v tejto práci venovať len kvadratickým diofantickým rovniciam s dvoma neznámymi.

### 3.2.1 Kvadratické diofantické rovnice s dvoma neznámymi

**Kvadratická diofantická rovnica s dvoma neznámymi**  $x, y \in \mathbb{Z}$  je rovnica tvaru

$$x^2 - y^2 = c, \quad (3.3)$$

kde  $c \in \mathbb{N}$ .

Nasledujúca veta hovorí o riešiteľnosti rovnice (3.3).

**Veta 15.** (*Existencia riešenia kvadratickej diofantickej rovnice s 2 neznámymi*) Rovnica (3.3) má celočíselné riešenie práve vtedy, keď číslo  $c$  je bud' nepárne, alebo deliteľné číslom 4.

**Dôkaz.** Ľavá strana rovnice (3.3) sa dá napísať ako súčin čísel  $x - y$  a  $x + y$ . Tie môžu byť obe párne, obe nepárne alebo jedno párne a druhé nepárne. V prvom prípade to znamená, že ich súčin musí byť deliteľný 4. V posledných prípadoch ich súčin môže byť len nepárne číslo.  $\square$

**Príklad 14.** Nájdite všetky celočíselné riešenia  $x, y \in \mathbb{Z}$  rovnice

$$x^2 - y^2 = 11.$$

**Riešenie:** Pravá strana je rovná číslu 11. To je nepárne číslo, preto je rovnica riešiteľná. Ľavá strana sa dá napísať ako súčin dvoch celých čísel  $x - y$  a  $x + y$ . My hľadáme celočíselné riešenie, a preto pravú stranu musíme napísať tiež ako súčin dvoch celých čísel. Pretože na pravej strane máme prvočíslo, existujú len

dva spôsoby ako to spraviť – musí to byť bud' súčin  $11 \cdot 1$ , alebo súčin  $-11 \cdot -1$ . Teraz budeme uvažovať, že  $11 = 11 \cdot 1$ :

Prvé riešenie dostaneme vyriešením sústavy rovníc

$$x + y = 11, \quad x - y = 1.$$

Je to dvojica  $[x, y] = [6, 5]$ .

Druhé riešenie získame so sústavy rovníc

$$x + y = 1, \quad x - y = 11,$$

tj. riešenie  $[x, y] = [6, -5]$ .

V prípade, kedy budeme uvažovať, že  $11 = -11 \cdot -1$ :

Prvé riešenie dostaneme vyriešením sústavy rovníc

$$x - y = -11, \quad x + y = -1.$$

Je to dvojica  $[x, y] = [-6, 5]$ .

Druhé riešenie získame so sústavy rovníc

$$x - y = -1, \quad x + y = -11,$$

tj. riešenie  $[x, y] = [-6, -5]$ .

Všetky riešenia rovnice  $x^2 - y^2 = 11$  sú dvojice  $[6, 5], [-6, 5], [6, -5], [-6, -5]$ .

## Cvičenia

1. Nájdite všetky celočíselné riešenia rovnice s neznámymi  $x, y \in \mathbb{Z}$ :

- a)  $x^2 - y^2 = 7$ ,
- b)  $x^2 - y^2 = 4$ ,
- c)  $x^2 - y^2 = 18$ .

2. Nájdite celočíselné riešenie  $[x, y]$  spĺňajúce nasledujúce dve rovnice:

$$\begin{aligned} x^2 - y^2 &= 5, \\ x + 3y &= 9. \end{aligned}$$

## Výsledky cvičení

1. a)  $[4, 3], [4, -3], [-4, -3], [-4, 3]$ .  
b)  $[2, 0], [-2, 0]$ .  
c) Nemá riešenie.
2. Riešením je dvojica  $[x, y] = [3, 2]$ .

### 3.3 Slovné úlohy

V tejto časti sa nachádzajú slovné úlohy na diofantické rovnice. Viac príkladov, resp. cvičení, na túto problematiku možno nájsť v Kapitole 5 tejto práce.

**Príklad 15.** Aké rozmery má obdlžník, ktorého obvod je 12 cm? (Rozmery obdlžníka sú prirodzené čísla.)

*Riešenie:* Obvod obdlžníka zo stranami  $a, b$  je  $2a + 2b$ . Naša úloha teda je: Nájsť všetky dvojice  $[a, b]$ , ktoré splňajú rovnicu  $2a + 2b = 12$ . Jedno z riešení rovnice je dvojica  $[a, b] = [6, 0]$ . Všetky celočíselné riešenia sú tvaru  $[a, b] = [6 - r, r]$ , kde  $r \in \mathbb{Z}$ . Pretože hľadáme  $a, b \in \mathbb{N}$  (vieme, že rozmery obdlžníka sú prirodzené čísla), pre  $r \in \mathbb{Z}$  musí platiť  $6 - r > 0$  a  $r > 0$ . To znamená, že  $r \in \{1, 2, 3, 4, 5\}$ . Všetky riešenia sú zapísané do nasledujúcej tabuľky.

$r$	$a$ (cm)	$b$ (cm)
1	5	1
2	4	2
3	3	3
4	2	4
5	1	5

**Príklad 16.** Zuzka má v peňaženke 6 dvadsaťkorunáčok a 3 päťdesiatkorunáčky. Koľkými spôsobmi môže zaplatiť 120 korún?

*Riešenie:* Zostavíme rovnicu  $20x + 50y = 120$ , kde  $x \in \mathbb{N}_0$  je počet dvadsaťkorunáčok a  $y \in \mathbb{N}_0$  je päťdesiatkorunáčok. Po vydelení oboch strán rovnice číslom 10, dostaneme novú rovnicu  $2x + 5y = 12$  (je ale ekvivalentná pôvodnej rovnici). Jedno z riešení tejto rovnice je  $[x_0, y_0] = [6, 0]$ . Všetky celočíselné riešenia sú tvaru  $[x, y] = [6 - 5r, 2r]$ , kde  $r \in \mathbb{Z}$ . Pretože chceme  $x, y \in \mathbb{N}_0$ , musí pre  $r \in \mathbb{Z}$  platiť  $6 - 5r \geq 0$  a  $2r \geq 0$ , tj.  $0 \leq r \leq 6/5$ . Číslo  $r$  teda môže byť len buď rovné 0, alebo 1. Preto existujú práve dve riešenia, a to  $[6, 0]$  a  $[1, 2]$ .

**Príklad 17.** Koľkými spôsobmi možno 21 litrov vody prelať do trojlitrových a šestlitrových nádob?

*Riešenie:* Označme  $x$  počet trojlitrových nádob,  $y$  počet šestlitrových nádob. Potom je našou úlohu nájsť všetky možné  $[x, y]$  spĺňajúce

$$3x + 6y = 21.$$

Pretože číslo 21 je deliteľné číslom  $D(3, 6) = 3$ , je rovnica riešiteľná. My ale nesmieme zabúdať na to, že potrebujeme nájsť nezáporné  $x, y$  (tieto hodnoty vyjadrujú počet, tj.  $x, y \in \mathbb{N}_0$ ). Jedno z riešení rovnice  $3x + 6y = 21$  je riešenie  $[x_0, y_0] = [7, 0]$ . Všetky celočíselné riešenia sú tvaru  $[x, y] = [7 - 2r, r]$ , kde  $r \in \mathbb{Z}$ . Chceme, aby platilo  $r \geq 0$  a  $7 - 2r \geq 0$ . Tomu vyhovuje len  $r \in \{0, 1, 2, 3\}$ . Existujú práve 4 riešenia a to dvojice  $[1, 3], [3, 2], [5, 1]$  a  $[7, 0]$ .

# Kapitola 4

## Prvočísla a ich využitie v reálnom živote

Prvočíslami nazývame všetky prirodzené čísla, ktoré majú práve dva rôzne delitele. Ich štúdiom sa matematici venujú už niekoľko tisícročí, avšak až od 20. storočia našli svoje uplatnenie v mnohých praktických aplikáciach. Možno si to ani neuvedomujeme, ale stretávame sa s nimi dennodenne. Napríklad všetky rodné čísla od roku 1986 sú volené tak, aby boli deliteľné prvočíslom 11. Podobne avšak viac komplikovanejšie sú volené čísla bankových účtov, identifikačné čísla organizácií, ISBN. Veľké prvočísla (prvočísla s veľkým počtom cifier – aspoň 100) používame v kryptológii, v algoritnoch na veľmi rýchle násobenie veľkých čísel.

V tejto kapitole sa naučíme, čo je Eratosthenovo sito, dozvieme sa nejaké kritéria na určenie, či dané prirodzené číslo je alebo nie je prvočíslo, ukážeme, že prvočísel je nekonečne veľa. Zoznámime sa tiež so špeciálnymi typmi prvočísel, napr. s Mersennovými prvočíslami. Nakoniec sa oboznámime aj s niekoľkými aplikáciami prvočísel v reálnom živote.

### 4.1 Prvočísla

V tejto časti popíšeme princíp hľadania prvočísel pomocou Eratosthenovho sita, uvedieme nejaké špeciálne typy prvočísel, napr. Mersennove prvočísla, Fermatove prvočísla. Ukážeme, ako sú prvočísla rozmiestnené na Ulamovej špirále. Zmienime tiež kritéria prvočíselnosti, tj. kritéria na určenie, či je dané prirodzené číslo prvočíslo, alebo nie je. Nakoniec dokážeme dve Euklidove vety o prvočíslach.

#### 4.1.1 Eratosthenovo sito

Hľadať prvočísla možno pomocou postupu/algoritmu nazývaného Eratosthenovo sito. Cieľom tohto algoritmu je nájsť všetky prvočísla menšie ako nejaké dané číslo.

**Eratosthenovo sito** je algoritmus, ktorý hľadá všetky prvočísla menšie ako je predom zadaná horná mez.

Nech číslo  $M \in \mathbb{N}$  označuje hornú mez. Algoritmus Eratosthenovho sita je nasledovný:

1. Na začiatku vypíšeme zoznam všetkých prirodzených čísel menších alebo rovných ako je číslo  $M$ . Začíname číslom 2, tj. zoznam tvoria čísla  $2, 3, 4, \dots, M - 1, M$ .
2. Zakrúžkujeme prvé číslo v zozname, tj. číslo 2 (to je prvočíslo).
3. Vyškrtneme všetky násobky čísla 2, tj. čísla  $4, 6, \dots$
4. Zakrúžkujeme prvé číslo v zozname, ktoré nie je zakrúžkované alebo vyškrtnuté. Toto číslo je prvočíslo.
5. Vyškrtneme všetky násobky zakrúžkovaného čísla, tj. prvočísla z predchádzajúceho kroku.
6. Posledné dva kroky (4. a 5.) opakujeme dovtedy, kým nie sú všetky čísla zoznamu rozdelené na čísla: zakrúžkované (to sú prvočísla) alebo preškrtnuté (to sú zložené čísla).
7. Všetky zakrúžkované čísla sú hľadané prvočísla medzi číslami 2 a  $M$ .

Teraz skúsime týmto spôsobom určiť všetky prvočísla, ktoré sú menšie ako číslo 21.

1. Napíšeme si zoznam všetkých prirodzených čísel od 2 do 21. (Všimnite si, že číslo 1 neuvažujeme, pretože nie je podľa definície ani prvočíslo, ani zložené číslo.)
2. Zakrúžkujeme prvé prvočíslo, tj. číslo 2.
3. Vyškrtneme všetky násobky čísla 2, tj. čísla  $4, 6, 8, 10, 12, 14, 16, 18, 20$ .

(2)	3	<del>4</del>	5	<del>6</del>
7	<del>8</del>	9	<del>10</del>	11
<del>12</del>	13	<del>14</del>	15	<del>16</del>
17	<del>18</del>	19	<del>20</del>	21

4. Najmenšie číslo, ktoré nie je preškrtnuté je číslo 3. Číslo 3 zakrúžkujeme a vyškrtneme všetky jeho nevyškrtnuté násobky, tj. čísla 9, 15, 21 (čísla 12 a 18 už preškrtnuté).
5. Ďalšie číslo zoznamu je číslo 5 (to je ďalšie prvočíslo). Žiadnen nepreškrtnutý násobok čísla 5 už nemáme. (Čísla 10, 15, 20 už už preškrtnuté.)

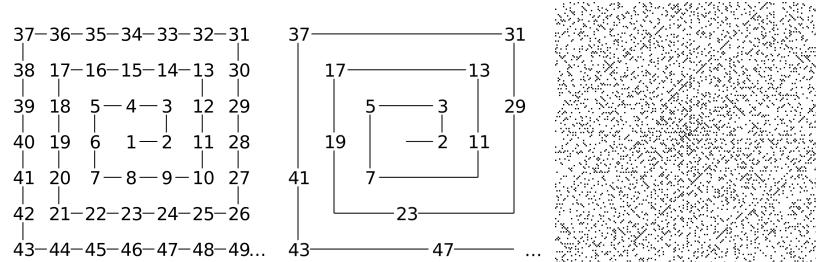
(2)	(3)	<del>4</del>	(5)	<del>6</del>
7	<del>8</del>	<del>9</del>	<del>10</del>	11
<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>
17	<del>18</del>	19	<del>20</del>	<del>21</del>

6. Nakoniec zakrúžkujeme aj zvyšné neoznačené čísla (ich násobky sa už v zo-zname nenachádzajú).
7. Zakrúžkované čísla, tj. prvočísla, sú čísla 2, 3, 5, 7, 11, 13, 17, 19.

(2)	(3)	<del>4</del>	(5)	<del>6</del>
(7)	<del>8</del>	<del>9</del>	<del>10</del>	(11)
<del>12</del>	(13)	<del>14</del>	<del>15</del>	<del>16</del>
(17)	<del>18</del>	(19)	<del>20</del>	<del>21</del>

### 4.1.2 Ulamova špirála

Zaujímavý obrázok, nazývaný Ulamová špirála, pozostávajúci z prvočísel objavil poľský matematik Stanisław Marcin Ulam. Ulamovú špirálu dostaneme napísaním prirodzených čísel do špirály a zakrúžkovaním všetkých prvočísel. Môžeme si všimnúť, že prvočísla vytvárajú diagonálne (dokonca i vodorovné a zvislé) čiary. Vid' Obr. 4.1.



Obr. 4.1: Postupne: Prirodzené čísla zapísané do špirály. Ulamová špirála. Ulamová špirála na sieti  $200 \times 200$ . (Obrázky z [http://cs.wikipedia.org/wiki/Ulamova\\_spirala](http://cs.wikipedia.org/wiki/Ulamova_spirala).)

### 4.1.3 Euklidove vety

Teraz uvedieme Prvú a Druhú Euklidovu vetu. Prvá Euklidova veta sa dosť často používa v príkladoch/úlohách na deliteľnosť. Druhá Euklidova veta hovorí o tom, že prvočísel je nekonečne mnoho.

**Veta 16.** (*Prvá Euklidova veta*)

Nech  $a, b$  sú prirodzené čísla. Ak je  $p$  prvočíslo a  $p \mid (a \cdot b)$ , potom platí bud'  $p \mid a$ , alebo  $p \mid b$ .

*Dôkaz.* Nech  $p$  je prvočíslo a  $a, b$  sú dve prirodzené čísla. Ak  $p$  delí  $a$ , veta platí. Preto predpokladajme, že tomu tak nie je, tj.  $p \nmid a$ . Chceme ukázať, že  $p \mid b$ . Využijeme na to Vetu 13 o lineárnych diofantických rovniciach. Tá hovorí, že pokial  $D(a, p) = 1$ , existujú celé čísla  $x, y$  splňajúce rovniciu  $ax + py = 1$ . Po vynásobení tejto rovnice číslom  $b$ , dostaneme rovniciu  $abx + pbx = b$ . Vieme, že  $p \mid (a \cdot b)$  a  $p \mid p$ . Aby riešenie  $x, y$  existovalo, musí platiť  $p \mid b$ , čo sme chceli dokázať.  $\square$

Dôsledkom Prvej Euklidovej vety je Základná veta aritmetiky, tj. Veta 4.

**Veta 17.** (*Druhá Euklidova veta*)

Prvočísel je nekonečne mnoho.

*Dôkaz.* Tvrdenie dokážeme sporom.

Predpokladáme, že platí výrok „Prvočísel je konečne mnoho.“. Všetky tieto prvočísla budeme označovať ako  $p_1, p_2, \dots, p_n$ .

Uvažujme teraz číslo

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

Žiadne z prvočísel  $p_1, p_2, \dots, p_n$  toto číslo nedelí bez zvyšku (zvyšok je vždy 1). To znamená, že číslo  $m$  musí byť podľa Základnej vety aritmetiky tiež prvočíslo. Avšak to je spor s naším predpokladom, že prvočísel je konečne mnoho.  $\square$

**Veta 18.** (*Dôsledok Druhej Euklidovej vety*)

Zlozených čísel je nekonečne mnoho.

### 4.1.4 Špeciálne typy prvočísel

Štúdiom čísel, ktoré sú o jedna menšie ako nejaká mocnina s prirodzeným mocniteľom z čísla 2, sa zaoberal francúzsky matematik M. Mersenne.

Prirodzené čísla tvaru

$$M_n = 2^n - 1,$$

kde  $n \in \mathbb{N}$ , nazývame **Mersennove čísla**. Ak je  $M_n$  prvočíslo, nazývame ho **Mersennovo prvočíslo**.

Prvé štyri Mersennove prvočísla dostaneme pre  $n = 2, 3, 5, 7$ , tj. sú to čísla 3, 7, 31 a 127. V prípade čísel  $n = 11$  alebo  $n = 23$  prvočísla nedostaneme, pretože číslo  $2^{11} - 1$  je deliteľné číslom 23 a číslo  $2^{23} - 1$  je deliteľné číslom 47.

Najväčšie známe Mersennovo prvočíslo má tvar  $2^{57\,885\,161} - 1$  (je to 48. Mersennovo prvočíslo). Predchádzajúce Mersennovo prvočíslo bolo číslo  $2^{43\,112\,609} - 1$ .

Hľadaniu Mersennových prvočísel sa venuje projekt GIMPS (Great Internet Mersenne Prime Search), bližšie informácie <http://www.mersenne.org>.

Ďalšie významné čísla sú Fermatove čísla, ktorími sa zaobral francúzsky matematik Pierre de Fermat.

Prirodzené čísla  $F_m = 2^{2^m} + 1$ , kde  $m \in \mathbb{N}_0$ , sa nazývajú **Fermatové čísla**. Ak je  $F_m$  prvočíslo, hovoríme o **Fermatovom prvočíslle**.

Prvé štyri Fermatove prvočísla sú čísla 3, 5, 17, 257. Pre  $m = 5$  prvočíslo nedostaneme, pretože  $F_5 = 641 \cdot 6700417$ . Najväčšie známe Fermatove prvočíslo je číslo  $F_4 = 65\,537$ .

Fermatove prvočísla sú dôležité najmä kvôli tomu, že súvisia s geometriou. Napríklad veľkým objavom bolo spojenie medzi Fermatovými prvočíslami a euklidovskou konštrukciou (tj. konštrukcia len pomocou kružidla a pravítka) pravidelných mnohouholníkov. Jeho objaviteľom je matematik Carl Friedrich Gauss. Gauss dokázal, že pravidelný  $n$ -uholník je možné skonštruovať euklidovsky práve vtedy, keď

$$n = 2^i \cdot F_{m_1} \cdot F_{m_2} \cdot \dots \cdot F_{m_j},$$

kde  $n \geq 3$ ,  $i, j \in \mathbb{N}_0$  a  $F_{m_1}, F_{m_2}, \dots, F_{m_j}$  sú navzájom rôzne Fermatove prvočísla.

Nasledujúce prvočísla sú pomenované po francúzskej matematicke Sophii Germainovej.

Nepárne prvočíslo  $p$ , pre ktoré  $2p+1$  je tiež prvočíslo, sa nazýva **prvočíslo Sophie Germainovej**.

Prvé štyri prvočísla Sophie Germainovej sú čísla 2, 3, 5, 11. Najväčšie doposiaľ známe (rok 2012) prvočíslo Sophie Germainovej je číslo  $18\,543\,637\,900\,515 \cdot 2^{666\,667} - 1$ , ktoré má 200 701 cifier.

Grécky matematik Euklides dokázal, že prvočísel je nekonečne mnoho. K dôkazu používal čísla, ktoré vznikli zo súčtu čísla 1 a súčinu prvých  $n$  prvočísel. Tieto čísla preto nazývame po ňom.

Nech  $p_1, p_2, \dots, p_n$  je prvých  $n$  prvočísel. Ak je číslo  $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$  prvočíslo, nazývame ho **Euklidove prvočíslo**.

Čísla 3, 7, 31, 211 sú Euklidove prvočísla. Prvočíslo nezískame napríklad pre 6 prvých prvočísel, pretože platí  $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$ .

#### 4.1.5 Kritéria prvočíselnosti

V tejto časti zmienime niekoľko kritérií na overenie, či je dané číslo prvočíslo, alebo nie je. Ako si môžete všimnúť, dôkazy neuvádzame, ale záujemcom odporúčame knihu [21], kde možno nájsť okrem dôkazov aj iné podrobnosti týkajúcich sa tejto problematiky.

**Tvrdenie 1.** *Prirodzené číslo  $n$  je prvočíslo práve vtedy, ked'  $n \mid \binom{n}{k}$  pre všetky  $k \in \{1, \dots, n-1\}$ .*

**Tvrdenie 2.** *Prirodzené číslo  $k$  je prvočíslo práve vtedy, ked'  $n \mid \binom{n}{k-2n}$  pre všetky  $n$  také, že  $\frac{k}{3} \leq n \leq \frac{k}{2}$ .*

**Tvrdenie 3.** *Ak  $2^p - 1$  je prvočíslo, potom  $p$  je tiež prvočíslo.*

## 4.2 Aplikácie prvočísel

### 4.2.1 Prvočíslo 11

Veta 8 dokázaná v Kapitole 2 nám určuje pravidlo deliteľnosti číslom 11. Pripomeňme si jej znenie:

Nech  $k \in \mathbb{N}_0$  a

$$n = \sum_{i=0}^k (a_i \cdot 10^i) \text{ pre } a_i \in \{0, 1, \dots, 9\}, \quad a_k \neq 0,$$

tj.  $a_k, \dots, a_0$  sú cifry prirodzeného čísla  $n$  v desiatkovej sústave. Potom

$$11 \mid n \iff 11 \mid \left( \sum_{i=0}^k (-1)^i a_i \right).$$

Existuje veľké množstvo aplikácií prvočísla 11 v praxi. Využívame ho napríklad pri tvorbe rodného čísla, kódu ISBN alebo tiež pri tvorbe čísel bankových účtov.

#### Tvorba rodného čísla

Prvočíslo 11 sa využíva napríklad na vytvorenie rodného čísla. To volíme tak, aby bolo deliteľné číslom 11.

Rodné číslo je desaťmiestne číslo, ktoré sa určuje podľa dátumu narodenia a súčasne pravidla deliteľnosti číslom 11. Ukážeme si, ako sa tvorí rodné číslo pre muža narodeného 22. 5. 1999 a ženu narodenú 13. 7. 1996.

Prvé dve číslice rodného čísla určuje posledné dvojčíslie roku narodenia, tj. muž bude mať 99 a žena 96. Nasleduje označenie muž alebo žena. Mužom sa dáva číslo 0 a ženám číslo 5. Potom je to už len mesiac a deň. V prípade dvojciferného čísla pre mesiac, napr. december (číslo 12), sa jednotka pripočíta k označeniu muž/žena (tj. 1/6). Nasleduje lomítka a štvorčíslie.

Od roku 2004 (zákon č. 53/2004 Sb.) sa zavádzajú možnosti, kedy v prípade, že sú v nejaký deň vyčerpané všetky platné štvorčísla, použiť alternatívne rodné číslo. Ženy majú vtedy označenie 7 a muži 2.

V našom prípade žena môže mať rodné číslo 965713/1110 a muž 990522/2591. Overiť, že takéto rodné číslo môže existovať, stačí podľa kritéria pre deliteľnosť číslom 11, tj.

$$-9 + 6 - 5 + 7 - 1 + 3 - 1 + 1 - 1 + 0 = 0,$$

$$-9 + 9 - 0 + 5 - 2 + 2 - 2 + 5 - 9 + 1 = 0.$$

Počítač by pri nesprávne zadanom rodnom čísle (zistil, že sme zadali číslo nedeliteľné 11) ohlásil chybu. Hovoríme vtedy, že číslo 11 detekovalo chybu. Kód nazývame jedenástkový kód samodetekujúceho kódu.

## Kód ISBN

Kód ISBN (International Standard Book Number) označuje knižné publikácie. Je zložený z 10 cifier  $x_1x_2\dots x_{10}$  rozdelených na 4 časti, medzi ktorými sú tri spojovníky. (Novo vydávané kódy sú trinásťmiestne začínajúce číslom 978.)

Tento kód má tvar: ISBN kód zeme (Česká aj Slovenská republika má kód 80) – nakladatelstvo – identifikačné číslo knihy – kontrolná cifra. Kontrolná cifra  $x_{10}$  sa volí tak, aby platilo:

$$11 \mid (x_1 + 2x_2 + 3x_3 + \dots + 10x_{10}).$$

**Príklad 18.** Kniha Zbierka úloh z matematiky (viď [3]) má tiež svoje ISBN. Skúste odhaliť posledné číslo (označujeme ho ako  $A$ ) pomocou znalosti prvých deviatich čísel. ISBN tejto knihy je 80-88792-16-A.

*Riešenie:* Podľa predchádzajúceho musíme nájsť také číslo  $A$ , tak aby platilo

$$11 \mid (x_1 + 2x_2 + 3x_3 + \dots + 10 \cdot A).$$

Pretože

$$x_1 + 2x_2 + 3x_3 + \dots + 9x_9 = 8 + 2 \cdot 0 + 3 \cdot 84 \cdot 85 \cdot 76 \cdot 97 \cdot 28 \cdot 19 \cdot 6 = 229 = \underbrace{220}_{11|220} + 9,$$

musí pre číslo  $A \in \{0, 1, 2, \dots, 9\}$  platiť  $11 \mid (9 + 10 \cdot A)$ . To bude splnené práve vtedy, keď  $A = 9$ .

## Čísla bankových účtov

Tak isto deliteľnosť číslom 11 využívajú aj banky. Napríklad Komerčná banka volí číslo účtu v tvare  $b_5b_4b_3b_2b_1b_0 - a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0$  tak, aby platilo

$$11 \mid \left( \sum_{i=0}^5 b_i 2^i \right), \quad 11 \mid \left( \sum_{i=0}^9 a_i 2^i \right).$$

### 4.2.2 Metóda RSA

Šifra pomáha odosielateľovi a adresátovi utajať obsah správy pred nepovolenou osobou. Pokiaľ na nejakú správu použijeme šifru, hovoríme, že sme správu zašifrovali. Opačným procesom k šifrovaniu nazývame dešifrovanie, ktoré robí ten, kto pozná všetky potrebné informácie k prevodu zašifrovaného textu na pôvodný

text, tj. ten, kto pozná dešifrovací klúč. Lúštenie robí kryptanalytik (neoprávnený príjemca), ktorý sa snaží získať informácie zo zašifrovej správy bez znalosti klúča a spôsobu šifrovania.

Sám Julius Caesar si uvedomoval dôležitosť šifrovania. Jeho šifra nahradzovala každé písmeno pôvodnej správy, písmenom, ktoré sa nachádzalo o tri miesta ďalej v abecede. Túto šifraciu metódu možno zovšeobecniť o ľubovoľný počet miest. Avšak problémom tejto šifry je to, že ju možno ľahko rýchlo rozlúštiť, a tým odhaliť skryté tajomstvo. Zachovať súkromie, zabezpečiť ochranu osobných údajov, bankových účtov vyžaduje oveľa lepšie spôsoby šifrovania.

Metóda RSA (autori L. Rivest (R), Adi Shamir (S), L. M. Adleman (A)), je metóda založená na tom, že ani zo znalosti šifrovacieho klúča, nie sme schopní odvodiť klúč dešifrovací. RSA prevádzza správu na reťazec číslic (prirodzené číslo). Trik metódy RSA spočíva v tom, že vynásobiť dve prvočísla, ktoré majú viac ako sto cifer, trvá na počítači veľmi krátky čas, ale rozložiť takto vzniknuté číslo na pôvodné prvočísla už nie je vôbec jednoduché, dokonca nemožné. Preto je táto metóda pri dostatočne dlhom klúči považovaná za veľmi bezpečnú.

Metóda RSA má veľmi veľké uplatnenie. Využíva sa najmä pri bankových transakciách, číslach PIN, pri prenosu tajných klúčov atď. Viac informácií o tejto metóde možno nájsť v knihách [21], [24].

# Kapitola 5

## Príklady na deliteľnosť a prvočísla

Táto kapitola obsahuje príklady, cvičenia na deliteľnosť a diofantické rovnice. Na začiatku kapitoly je pre čitateľa pripravený test na preverenie znalostí týkajúcich sa deliteľnosti a diofantických rovníc. Test pozostáva z 15 otázok. U niektorých otázkach môže byť viac správnych odpovedí. Kapitola potom pokračuje príkladmi a cvičeniami na deliteľnosť. Sú medzi nimi aj dôkazové príklady. Test aj väčšina príkladov bola vytvorená autorkou tejto práce. Záver kapitoly tvořia úlohy z matematických olympiád a korešpondenčných seminárov, konkrétnie PraSe (PRAŽSKÝ SEMINÁŘ), z korešpondenčnej súťaže z časopisu MATMIX a KMS (Korešpondenčný Matematický Seminár).

### 5.1 Test

1. Číslo 2 je
  - a) prvočíslo,
  - b) zložené číslo,
  - c) prvočíslo aj zložené číslo,
  - d) nie je prvočíslo ani zložené číslo.
2. Vzťah  $a \mid b$  znamená, že
  - a) číslo  $a$  je deliteľom čísla  $b$ ,
  - b) číslo  $b$  je deliteľom čísla  $a$ ,
  - c) číslo  $b$  delí číslo  $a$ ,
  - d) číslo  $a$  delí číslo  $b$ ,
  - e) číslo  $b$  nedelí číslo  $a$ .
3. Pre každé  $a, b \in \mathbb{N}$  a ich najmenší spoločný násobok  $n(a, b)$  a najväčší spoločný deliteľ  $D(a, b)$  platí
  - a)  $a \cdot b = \frac{D(a,b)}{n(a,b)}$ ,
  - b)  $a \cdot b = \frac{n(a,b)}{D(a,b)}$ ,
  - c)  $a \cdot b = n(a, b) \cdot D(a, b)$ ,
  - d)  $a \cdot b = n(a, b) + D(a, b)$ ,
  - e)  $\frac{a \cdot b}{D(a,b)} = n(a,b)$ .

4. Nesúdeliteľné čísla sú čísla, ktorých
- najmenší spoločný násobok je číslo 1,
  - najväčší spoločný deliteľ je číslo 1,
  - každý spoločný deliteľ je vždy väčší ako číslo 1,
  - každý spoločný násobok je menší ako najväčší spoločný deliteľ.
5. Prvočíselný rozklad čísla 30 je súčin
- $2 \cdot 15$ ,
  - $1 \cdot 5 \cdot 6$ ,
  - $1 \cdot 30$ ,
  - $2 \cdot 3 \cdot 5$ ,
  - $2^1 + 3^1 + 5^2$ .
6. Číslo  $4!$  je rovné
- súčinu ľubovoľných 4 po sebe idúcich čísel,
  - súčtu ľubovoľných 4 po sebe idúcich čísel,
  - súčinu najmenších po sebe idúcich 4 prirodzených čísel,
  - súčtu najmenších po sebe idúcich 4 prirodzených čísel,
  - číslu  $(5!)/5$ .
7. Kombinačné číslo  $\binom{n}{k}$  sa rovná číslu
- $\frac{n}{k}$ ,
  - $\frac{n!}{k!}$ ,
  - $\frac{n+k}{k}$ ,
  - $\frac{n!}{(n-k)!k!}$ ,
  - $\binom{n}{n-k}$ .
8. Euklidov algoritmus je algoritmus na
- hľadanie najmenšieho spoločného násobku dvoch čísel,
  - hľadanie najväčšieho spoločného deliteľa dvoch čísel,
  - hľadanie najväčšieho prvočísla,
  - hľadanie najmenšieho prvočísla.
9. Ktoré z nasledujúcich tvrdení je pravdivé?
- Prvočísel je konečne mnoho.
  - Prvočísel je nekonečne mnoho.
  - Prvočísel je menej ako zložených čísel.
  - Prvočísel je viac ako zložených čísel.
10. Súčin  $k$  po sebe idúcich prirodzených čísel je deliteľný číslom
- $k!$
  - $(k - 1)!$
  - $(k + 1)!$
  - $k$ ,
  - $k/2$ , ak  $k$  je párne číslo, alebo číslom  $(k + 1)/2$ , ak  $k$  je nepárne číslo.
11. Najväčší spoločný deliteľ čísel 15 a 35 je číslo
- 7,
  - 1,
  - 3,

- d) 5,  
e)  $3 \cdot 5 \cdot 7$ .
12. Najmenší spoločný násobok čísel 40 a 22 je číslo  
a) 220,  
b) 22,  
c) 440,  
d) 40,  
e) 2.
13. Každé párne prirodzené číslo môžeme zapísť v tvare  
a)  $2k$ , kde  $k \in \mathbb{N}$ ,  
b)  $2k + 1$  kde  $k \in \mathbb{N}$ ,  
c)  $2k - 1$ , kde  $k \in \mathbb{N}$ ,  
d)  $2k + 3$ , kde  $k \in \mathbb{N}$ ,  
e)  $2k + 2$ , kde  $k \in \mathbb{N}_0$ .
14. Lineárna diofantická rovnica s dvoma neznámymi  $x, y$  je rovnica tvaru  
a)  $ax + by = c$ , kde  $a, b \in \mathbb{Z} \setminus \{0\}, c \in \mathbb{Z}$ ,  
b)  $ax + by = c$ , kde  $a, b \in \mathbb{Z} \setminus \{0\}, c \in \mathbb{R}$ ,  
c)  $x^y = c$ , kde  $c \in \mathbb{N}$ ,  
d)  $xy = c$ , kde  $c \in \mathbb{N}$ ,  
e)  $ax + by = 0$ , kde  $a, b \in \mathbb{Z} \setminus \{0\}$ .
15. Kvadratická diofantická rovnica s dvoma neznámymi  $x, y$  je rovnica tvaru  
a)  $xy + yx + x^3 = c$ , kde  $c \in \mathbb{R}$ ,  
b)  $x^2 - y^2 = c$ , kde  $c \in \mathbb{Z}$ ,  
c)  $x + y = c$ , kde  $c \in \mathbb{N}$ ,  
d)  $x^y = c$ , kde  $c \in \mathbb{N}$ ,  
e)  $x^2 - y^2 = 2$ .

### Výsledky testu

Príklad	Výsledok	Príklad	Výsledok	Príklad	Výsledok
1.	a)	6.	c), e)	11.	d)
2.	a), d)	7.	d), e)	12.	c)
3.	c), e)	8.	b)	13.	a), e)
4.	b)	9.	b)	14.	a), e)
5.	d)	10.	a), b), d), e)	15.	b), e)

## 5.2 Príklady a cvičenia na deliteľnosť

### 5.2.1 Príklady na deliteľnosť

**Príklad 19.** Napíšte nasledujúce zlomky v základnom tvare

$$\frac{125}{520}, \frac{654}{456}, \frac{990}{1230}.$$

*Riešenie:* Úloha viedie na nájdenie najväčšieho spoločného deliteľa čitateľa a menovateľa zlomku. Platí

$$D(125, 520) = 5, \quad D(654, 456) = 6, \quad D(990, 1230) = 30.$$

Úpravami zlomkov dostaneme

$$\begin{aligned} \frac{125}{520} &= \frac{5 \cdot 25}{5 \cdot 104} = \frac{25}{104}, \\ \frac{654}{456} &= \frac{6 \cdot 109}{6 \cdot 76} = \frac{109}{76}, \\ \frac{990}{1230} &= \frac{30 \cdot 33}{30 \cdot 41} = \frac{33}{41}. \end{aligned}$$

**Príklad 20.** Určte všetky prvočísla, ktoré delia číslo 212 121.

*Riešenie:* Prvočíselný rozklad čísla 212 121 je  $3^2 \cdot 7^2 \cdot 13 \cdot 37$ . Všetky prvočísla, ktorými je číslo 212 121 deliteľné sú 3, 7, 13 a 37.

**Príklad 21.** Nájdite všetky prirodzené čísla  $n \leq 30$  splňajúce

$$2 \mid n \wedge 3 \mid (n^2 - 1).$$

*Riešenie:* Pretože číslo  $n$  je deliteľné číslom 2, hľadáme všetky párne prirodzené čísla, ktoré sú menšie alebo rovné ako číslo 30. Ďalej vieme, že číslo  $(n^2 - 1)$  je deliteľné číslom 3, a že platí  $n^2 - 1 = (n-1) \cdot (n+1)$ . To znamená, že hľadané číslo  $n$  nebude deliteľné číslom 3 (číslom 3 je deliteľné bud' číslo  $(n-1)$ , alebo číslo  $(n+1)$ ). Riešením sú všetky čísla, ktoré sú párne, menšie alebo rovné ako číslo 30 a nie sú deliteľné číslom 3, tj. riešením sú čísla 2, 4, 8, 10, 14, 16, 20, 22, 26, 28.

**Príklad 22.** Nech  $p, r$  sú dve rôzne prvočísla. Koľko deliteľov má číslo  $p^3 \cdot r$ ?

*Riešenie:* Číslo  $p^3 \cdot r$  má 8 deliteľov. Triviálne delitele sú čísla 1 a  $p^3 \cdot r$ . Netriviálne delitele sú čísla  $p, p^2, p^3, r, p \cdot r, p^2 \cdot r$ .

**Príklad 23.** Nájdite najväčšie prvočíslo, ktoré delí číslo 4 420.

*Riešenie:* Prvočíselný rozklad čísla 4 420 je súčin  $2^2 \cdot 5 \cdot 13 \cdot 17$ . Preto najväčšie prvočíslo, ktoré delí číslo 4 420 je prvočíslo 17.

**Príklad 24.** Nech  $a, b$  sú také dve rôzne prirodzené čísla, že číslo  $a^2$  má tri delitele a číslo  $b^4$  má päť deliteľov. Koľko deliteľov má číslo  $a \cdot b$ ?

*Riešenie:* Zo zadania plynie, že  $a$  aj  $b$  sú prvočísla. Z toho dôvodu môžu byť delitele čísla  $a \cdot b$  len čísla 1,  $a, b, a \cdot b$ . To znamená, že číslo  $a \cdot b$  má 4 delitele.

**Príklad 25.** Nech  $n$  je najmenší spoločný násobok čísel a  $D$  najväčší spoločný deliteľ čísel  $(3!)^2$  a  $(6! \cdot 3!)$ . Čomu sa potom rovná podiel  $n/D$ ?

*Riešenie:* Nech  $a = (3!)^2$  a  $b = 6! \cdot 3!$ . Platí

$$\begin{aligned} a &= (3!)^2 = 3! \cdot 3!, \\ b &= 6! \cdot 3! = 6 \cdot 5 \cdot 4 \cdot 3! \cdot 3!. \end{aligned}$$

Najmenší spoločný násobok je  $n(a, b) = 6 \cdot 5 \cdot 4 \cdot (3!)^2$ , najväčší spoločný deliteľ je  $D(a, b) = (3!)^2$ . Preto platí  $n/D = 6 \cdot 5 \cdot 4 = 120$ .

**Príklad 26.** Označme  $m_2$  najmenšie dvojciferné prirodzené číslo deliteľné číslom 9. Nech  $m_4$  označuje najmenšie štvorciferné prirodzené číslo, ktoré má ciferný súčet 2 a je deliteľné 4. A nakońec označme  $m_5$  najväčšie päťciferné prirodzené číslo, ktoré je deliteľné 3. Čomu sa rovná  $m_4 + m_5 - m_2$ ?

*Riešenie:* Najmenšie dvojciferné prirodzené číslo deliteľné číslom 9 je  $m_2 = 18$ . Najmenšie štvorciferné prirodzené číslo, ktoré má ciferný súčet 4 a je deliteľné číslom 4, je číslo  $m_4 = 1100$ . Najväčšie päťciferné prirodzené číslo, ktoré je deliteľné číslom 3, je číslo  $m_5 = 10\,002$ . Číslo  $m_4 + m_5 - m_2$  je rovné číslu 11 084.

**Príklad 27.** Koľkými spôsobmi môžeme rozpísať číslo 21 ako súčet troch prvočísel?

*Riešenie:* Všetky prvočísla, o ktorých má zmysel uvažovať musia byť menšie ako číslo 21, tj. uvažujeme čísla 2, 3, 5, 7, 11, 13, 17, 19.

Súčet troch párnych čísel alebo súčet dvoch nepárných čísel a čísla párnego je párne číslo. My chceme nepárne číslo – číslo 21. Preto musíme nájsť bud' súčet troch nepárných čísel, alebo súčet dvoch párných čísel a jedného nepárnego čísla.

Možnosť dve párne a jedno nepárne: Párne číslo môže byť len číslo 2. Preto nepárne musí byť 17, čo je prvočíslo. Prvá trojica je (2, 2, 17).

Možnosť tri nepárne: Pretože súčet dvoch nepárných najmenších prvočísel (dve trojky) je 6, stačí uvažovať len prvočísla menšie než 15. Dostaneme tieto trojice (3, 5, 13), (3, 7, 11), (5, 5, 11) a (7, 7, 7).

Existuje 5 spôsobov ako zapísať číslo 21 súčtom troch prvočísel, a to

$$21 = 2 + 2 + 17 = 3 + 5 + 13 = 3 + 7 + 11 = 5 + 5 + 11 = 7 + 7 + 7.$$

**Príklad 28.** Koľkými spôsobmi môžeme rozpísať číslo 60 ako súčin dvoch nesúdeliteľných čísel?

*Riešenie:* Nech  $60 = a \cdot b$ , kde  $a, b \in \mathbb{N}$ ,  $a \leq b$ . Potom platí nasledujúca tabuľka:

$a$	$b$	$D(a, b)$
1	60	1
2	30	2
3	20	1
4	25	1
5	12	1
6	10	2

Najväčší spoločný deliteľ nesúdeliteľných čísel je číslo 1. To znamená, že napísat číslo 60 ako súčin dvoch nesúdeliteľných čísel môžeme 4 spôsobmi. Sú to súčiny  $1 \cdot 60$ ,  $3 \cdot 20$ ,  $4 \cdot 15$ ,  $5 \cdot 12$ .

**Príklad 29.** Pre ktoré prirodzené čísla  $n$  sa zlomky

$$\frac{210}{2 \cdot n - 1}, \quad \frac{29}{n + 21}$$

rovnajú (oba súčasne) zasa prirodzeným číslam?

*Riešenie:* Zlomok sa rovná prirodzenému číslu práve vtedy, keď číslo v čitateli je deliteľné číslom v menovateli.

Číslo  $2 \cdot n - 1$  je nepárne číslo. Chceme aby toto číslo bolo deliteľom čísla 210. Nepárne čísla, ktoré sú deliteľmi čísla 210, sú čísla 1, 3, 5, 7, 15, 21, 35, 105. Tabuľka obsahuje všetky možné riešenia ( $2 \cdot n - 1 = (\text{deliteľ čísla } 210)$ ).

Deliteľ čísla 210	Číslo $n$	Deliteľ čísla 210	Číslo $n$
1	1	15	8
3	2	21	11
5	3	35	18
7	4	105	53

Dostávame, že  $n \in \{1, 2, 3, 4, 8, 11, 18, 53\}$ .

V druhom prípade, číslo 29 je prvočíslo, a preto uvažujeme len triviálne delitele, tj. čísla 1 a 29. Dostávame, že  $n \in \{8, 22\}$  (vid' tabuľka, kde platí  $n + 21 = (\text{deliteľ čísla } 29)$ ).

Deliteľ čísla 29	Číslo $n$
1	22
29	8

Zlomky  $\frac{210}{2 \cdot n - 1}$  a  $\frac{29}{n+21}$  sa rovnajú prirodzenému číslu práve vtedy, keď  $n = 8$ .

**Príklad 30.** Určte dve prirodzené čísla  $a, b$ , ktorých najväčší spoločný deliteľ  $D(a, b) = 2$  a najmenší spoločný násobok  $n(a, b) = 8$ .

*Riešenie:* Vieme, že platí  $a \cdot b = n(a, b) \cdot D(a, b) = 2 \cdot 8 = 16$ . Za daných predpokladov vyhovuje len dvojica  $[2, 8]$ , resp. dvojica  $[8, 2]$ .

**Príklad 31.** Určte všetky dvojice celých čísel  $x, y$  splňajúce rovnicu  $5x + 7y = 9$ .

*Riešenie:* Pretože  $D(7, 5) \mid 9$ , je uvedená rovnica riešiteľná. Platí, že

$$\begin{aligned} 9 &= 7 + 2, \\ 7 &= 5 + 2. \end{aligned}$$

Ak z každej rovnice vyjadríme číslo 2, dostaneme

$$\begin{aligned} 9 - 7 &= 7 - 5, \\ 9 &= 7 + 7 - 5 = 2 \cdot 7 - 1 \cdot 5. \end{aligned}$$

Jedno z riešení danej diofantickej rovnice je  $[x_0, y_0] = [-1, 2]$ . Riešením rovnice  $5x + 7y = 9$  je každá usporiadana dvojica  $[x, y] = [-1 - 7r, 2 + 5r]$ , kde  $r \in \mathbb{Z}$ .

**Príklad 32.** Určte všetky dvojice prirodzených čísel  $x, y$ , ktoré vyhovujú rovnici  $5x + 7y = 40$ .

*Riešenie:* Pretože  $D(5, 7) \mid 40$ , je rovnica riešiteľná a má nekonečne mnoho celočíselných riešení. Musíme dať pozor na to, že riešenie máme hľadať medzi prirodzenými číslami. Najprv však nájdeme všetky celočíselné riešenia.

Jedno z riešení danej diofantickej rovnice je  $[x_0, y_0] = [8, 0]$ . Všetky celočíselné riešenia sú tvaru  $[8 - 7r, 5r]$ , kde  $r \in \mathbb{Z}$ . Každé prirodzené číslo je väčšie alebo rovné ako číslo 1. Preto pre celé číslo  $r$  musí platiť

$$8 - 7r \geq 1, \quad 5r \geq 1.$$

Tomu vyhovuje jedine číslo  $r = 1$ . Jediná dvojica prirodzených čísel, ktorá je riešením rovnice  $5x + 7y = 40$ , je  $[x, y] = [1, 5]$ .

**Príklad 33.** Určte prirodzené číslo  $p$  tak, aby číslo  $p^2 - 1$  bolo prvočíslo.

*Riešenie:* Označme  $n = p^2 - 1$ . Chceme, aby  $n$  bolo prvočíslo. Jeho delitele musia byť len čísla 1 a  $n$ . Platí, že  $p^2 - 1 = (p-1)(p+1)$ , čo nie je nič iného ako prvočíselný rozklad čísla  $n$ . Preto musí platiť bud'  $p-1 = 1$ ,  $p+1 = n$ , alebo  $p-1 = n$ ,  $p+1 = 1$ . Riešením je prirodzené číslo  $p = 2$ .

**Príklad 34.** Nájdite dvojciferné číslo, ktoré po delení jeho ciferným súčtom dá číslo 6 a zvyšok 3.

*Riešenie:* Naše hľadané číslo zapísané v desiatkovej sústave má tvar  $10a + b$ , kde  $a \in \{1, 2, \dots, 9\}$ ,  $b \in \{0, 1, 2, \dots, 9\}$ . Rovnica úlohy je

$$10a + b = 6(a + b) + 3.$$

To vedie na lineárnu diofantickú rovnicu

$$4a - 5b = 3.$$

Riešením tejto rovnice sú usporiadane dvojice  $[a, b] = [2, 1]$  a  $[a, b] = [7, 5]$ . Hľadané dvojciferné čísla sú čísla 21 a 75.

**Príklad 35.** Koľko existuje prirodzených čísel  $m$  takých, že číslo  $11 - m^2$  je prvočíslo?

*Riešenie:* Zadanú úlohu vyriešime pre dva prípady –  $m$  párne a  $m$  nepárne číslo.

Nech  $m$  je nepárne číslo. Potom existuje  $k \in \mathbb{N}_0$  také, že  $m = 2k + 1$ . Rozdiel  $11 - m^2$  je párne číslo, pretože

$$11 - m^2 = 11 - (2k+1)^2 = 11 - 4k^2 - 4k - 1 = 10 - 4k^2 - 4k.$$

Jediná možnosť je, aby  $11 - m^2$  sa rovnalo číslu 2 (to je jediné párne prvočíslo). Preto  $m = 3$  je riešením.

Nech  $m$  je párne číslo. Potom existuje  $k \in \mathbb{N}$  také, že  $m = 2k$ . Rozdiel  $11 - m^2$  je

$$11 - m^2 = 11 - (2k)^2 = 11 - 4k^2.$$

Pre  $k \geq 2$  je rozdiel záporný. Pre  $k = 1$  je  $m = 2$ . Rozdiel  $11 - m^2$  je rovný číslu 7, čo je prvočíslo. Preto  $m = 2$  je riešením.

Existujú 2 riešenia,  $m = 2$  a  $m = 3$ .

**Príklad 36.** Dve ozubené kolesá s 24 a 40 zubami zapadajú do seba. Koľkokrát sa musí otočiť prvé koleso a koľkokrát druhé, aby určitý zub prvého kolesa zapadol opäť do tej istej medzery druhého kolesa?

*Riešenie:* Zapadnú vtedy, keď sa otočia o rovnaký násobok. Hľadáme preto najmenší spoločný násobok čísel 24 a 40. Ten je  $n(24, 40) = 120$ . Koleso s 24 zubami sa otočí  $(n(24, 40)/24)$ -krát, tj. 5-krát. Druhé koleso, koleso s 40 zubami sa otočí  $(n(24, 40)/40)$ -krát, tj. 3-krát.

**Príklad 37.** Rozmery kvádra sú prirodzené čísla  $a, a, b$  (v centimetroch). Číslo určujúce jeho povrch ( $\text{cm}^2$ ) sa rovná číslu, ktoré udáva jeho objem ( $\text{cm}^3$ ). Pre čísla  $a, b$  platí  $ab - b = 28$ . Určte rozmery kvádra.

*Riešenie:* Povrch kvádra je  $S = 2 \cdot (2 \cdot ab + a^2)$ . Objem kvádra je  $V = a^2 \cdot b$ . Platí

$$\begin{aligned} S &= V, \\ 2 \cdot (2 \cdot ab + a^2) &= a^2 \cdot b, \\ 2a^2 &= a^2 \cdot b - 4ab, \\ 2a^2 &= a \cdot (ab - 4b), \\ 2a &= (ab - b) - 3b, \\ 2a &= 28 - 3b, \\ 2a + 3b &= 28. \end{aligned}$$

Posledná rovnica je lineárna diofantická rovnica s dvoma neznámymi  $a, b$ . Jedno jej riešenie je  $[a, b] = [14, 0]$ . Všetky celočíselné riešenia sú usporiadane dvojice  $[a, b] = [14 - 3r, 2r]$ , kde  $r \in \mathbb{Z}$ . Pre riešenie pozostávajúce z prirodzených čísel musí platiť

$$(14 - 3r \geq 1, 2r \geq 1) \Rightarrow 1/2 \leq r \leq 13/3.$$

Všetky možnosti popisuje nasledujúca tabuľka

$r$	$a$	$b$	$ab - b$
1	11	2	20
2	8	4	28
3	5	6	24
4	2	8	32

Pretože má platiť  $ab - b = 28$ , riešením je len dvojica  $[a, b] = [8, 4]$ .

**Príklad 38.** Tri druhy plechoviek so súčiastkami dopravili v debne. Plechovky mali hmotnosť 2, 3 a 5 kg a objemy v poradí  $1 \text{ dm}^3$ ,  $4 \text{ dm}^3$  a  $6 \text{ dm}^3$ . Celá hmotnosť zásielky bez debny bola 81 kg, úhrnný objem plechoviek  $93 \text{ dm}^3$ . Vieme, že počet najťažších plechoviek bol najväčší. Koľko plechoviek každého druhu bolo v zásielke?

*Riešenie:*

Druh plechovky	Hmotnosť (kg)	Objem ( $\text{dm}^3$ )	Počet plechoviek
1. druh	2	1	$x$
2. druh	3	4	$y$
3. druh	5	6	$z$

Podľa zadania dostávame nasledujúce rovnice

$$\begin{aligned} 2x + 3y + 5z &= 81, \\ x + 4y + 6z &= 93. \end{aligned}$$

Ak z druhej rovnice vyjadríme  $x$  a dosadíme do prvej, dostaneme

$$\begin{aligned} 2 \cdot (93 - 4y - 6z) + 3y + 5z &= 81, \\ 186 - 8y - 12z + 3y + 5z &= 81, \\ 5y + 7z &= 105. \end{aligned}$$

Vieme, že počet najťažších plechoviek bol najväčší, tj. číslo  $z$  musí byť väčšie ako číslo  $x$  aj  $y$ .

Jedno z riešení rovnice  $5y + 7z = 105$  je  $[y, z] = [0, 15]$ . Všetky celočíselné riešenia sú tvaru  $[y, z] = [-7r, 15 + 5r]$ , kde  $r \in \mathbb{Z}$ . Hľadáme  $z \geq y \geq 0$  (neznáme  $y, z$  vyjadrujú počty plechoviek 2. a 3. druhu). Preto pre  $r \in \mathbb{Z}$  musí platiť

$$(15 + 5r \geq -7r \geq 0) \Rightarrow -15/12 \leq r \leq 0.$$

Nasledujúca tabuľka popisuje všetky možnosti, ktoré môžu nastat'.

$r$	$y$	$z$	$x = 93 - 4y - 6z$
-1	7	10	5
0	0	15	3

Riešením sú trojice  $[x, y, z] = [3, 0, 15]$  a  $[x, y, z] = [7, 10, 3]$ , kde  $x, y, z$  označujú počty plechoviek príslušného druhu (označenie vid' tabuľka).

## Cvičenia

- Nájdite prirodzené číslo  $n \leq 20$  deliteľné číslom 4 a spĺňajúce  $3 \mid n^2$ .
- Nájdite prirodzené číslo  $b$ , pre ktoré platí

$$D(3, b) = 1, \quad n(b, 3) = 12.$$

- Nech  $a, b$  sú prirodzené čísla, pre ktoré sú z podmienok
  - $a + 1$  je deliteľné číslom  $b$ ,
  - $a = 2b + 5$ ,
  - $a + b$  je deliteľné tromi,
  - $a + 7b$  je prvočíslo,

splnené práve tri. Nájdite všetky také dvojice  $a, b$ .

- Obsah obdĺžnika je  $S = 200 \text{ cm}^2$ . Aké veľké sú jeho rozmery, ked' sú vyjadrené prirodzenými číslami, a vieme, že jeho obvod je najmenší možný pre daný obsah?

## Výsledky cvičení

- Hľadané prirodzené číslo je číslo 12.
- Riešením je  $b = 4$ .
- Riešením sú dvojice  $[a, b] = [9, 2]$  a  $[a, b] = [17, 6]$ .
- Rozmery obdĺžnika sú 20 cm a 10 cm.

## 5.2.2 Dôkazové príklady

**Príklad 39.** Dokážte, že číslo  $17^{19} + 19^{17}$  je deliteľné číslom 36.

*Riešenie:* Platí

$$17^{19} + 19^{17} = (17 + 19) \cdot (17^{18} + \dots + 19^{16}) = 36 \cdot (17^{18} + \dots + 19^{16}).$$

Odtiaľ je zrejmá deliteľnosť číslom 36.

**Príklad 40.**

Dokážte, že pre každé prirodzené číslo  $n$  platí

$$5 \mid (n^2 + 1) \Rightarrow 5 \nmid n.$$

*Riešenie:* Využijeme nepriamy dôkaz. Obmenená implikácie k pôvodnej implikácii je  $5 \mid n \Rightarrow 5 \nmid (n^2 + 1)$ .

Z predpokladu  $5 \mid n$  vieme, že existuje  $k \in \mathbb{N}_0$  také, že  $5 \cdot k = n$ . Platí  $n^2 + 1 = 25k^2 + 1$ . Číslo  $25k^2 + 1$  nie je deliteľné číslom 5, a preto  $5 \nmid (n^2 + 1)$ . Dokázali sme, že  $5 \mid n \Rightarrow 5 \nmid (n^2 + 1)$ , čo je ekvivalentné tomu, že  $5 \mid (n^2 + 1) \Rightarrow 5 \nmid n$ .

**Príklad 41.**

Dokážte, že platí

$$\forall n \in \mathbb{N} : 6 \mid (n^3 + 5n).$$

*Riešenie:* Musíme dokázať, že číslo  $n^3 + 5n$  je deliteľné číslom 2 a číslom 3.

Najprv ukážeme deliteľnosť číslom 2.

Ak  $2 \mid n$ , potom  $2 \mid (n^3 + 5n)$ . To je zrejmé z toho, že  $n^3 + 5n = n \cdot (n^2 + 5)$ .

Ak  $2 \nmid n$ , potom  $n$  je nepárne číslo. Súčet  $n^2 + 5$  je párne číslo (súčet dvoch nepárných čísel je párne číslo). Preto  $2 \mid (n^2 + 5)$ , a teda i  $2 \mid (n^3 + 5n)$ .

Teraz dokážeme deliteľnosť číslom 3.

Ak  $3 \mid n$ , potom platí  $3 \mid (n^3 + 5n)$ .

Ak  $3 \nmid n$ , potom musíme ukázať, že  $3 \mid (n^2 + 5)$ . Prirodzené číslo, ktoré nie je deliteľné číslom 3, sa dá napísať bud' ako  $3k + 1$ , alebo  $3k + 2$ , kde  $k \in \mathbb{N}_0$ . Pre  $n = 3k + 1$  platí  $n^2 + 5 = (3k + 1)^2 + 5 = 9k^2 + 6k + 6$ . To je číslo deliteľné číslom 3, a preto  $3 \mid (n^2 + 5)$ . V druhom prípade, ked' predpokladáme, že  $n = 3k + 2$ , platí  $n^2 + 5 = (3k + 2)^2 + 5 = 9k^2 + 6k + 9$ , čo je opäť číslo deliteľné číslom 3, tj.  $3 \mid (n^2 + 5)$ .

Dokázali sme, že  $2 \mid (n^3 + 5n)$  a  $3 \mid (n^3 + 5n)$ , a teda aj  $6 \mid (n^3 + 5n)$ .

**Príklad 42.**

Dokážte, že platí

$$\forall n \in \mathbb{N} : 16 \mid (9^{n+1} - 8n - 9).$$

*Riešenie:* Dokážeme použitím matematickej indukcie. Nech  $n = 1$ . Potom

$$9^{n+1} - 8n - 9 = 9^2 - 8 - 9 = 64.$$

Číslo 64 je deliteľné číslom 16, a preto je tvrdenie pravdivé pre  $n = 1$ .

Teraz nech  $n > 1$  a predpokladajme, že tvrdenie platí pre všetky prirodzené čísla menšie alebo rovné ako číslo  $k - 1$ . Ukážeme, že tvrdenie platí pre  $k$ . Počítajme

$$\begin{aligned} 9^{k+1} - 8k - 9 &= 9 \cdot 9^k - 72k - 9 + 64k \\ &= 9 \cdot (9^k - 8k - 1) + 64k \\ &= 9 \cdot (9^{(k-1)+1} - 8(k-1) - 9) + 64k. \end{aligned}$$

Z indukčného predpokladu vieme, že

$$16 \mid (9^{(k-1)+1} - 8(k-1) - 9).$$

Súčasne platí  $16 \mid 64k$ . Preto platí  $16 \mid (9^{k+1} - 8k - 9)$ .

Matematickou indukciou sme ukázali, že pre každé prirodzené číslo  $n$  platí  $16 \mid (9^{n+1} - 8n - 9)$ .

**Príklad 43.** Dokážte, že číslo  $171^5 + 921^5$  je deliteľné číslom 84.

*Riešenie:* Platí  $171^5 + 921^5 = (171 + 921) \cdot (171^4 + \dots + 921^4) = 1092 \cdot (171^4 + \dots + 921^4)$ . Číslo 1092 je deliteľné číslom 84. To znamená, že číslom 84 je deliteľné aj číslo  $171^5 + 921^5$ .

**Príklad 44.** Dokážte, že súčet dvoch za sebou nasledujúcich nepárných prirodzených čísel je deliteľný štyrmi.

*Riešenie:* Označme prvé nepárne číslo ako  $2k + 1$ , kde  $k \in \mathbb{N}_0$ . Potom ďalšie nepárne číslo je  $2k + 3$ . Ich súčet je  $4k + 4 = 4 \cdot (k + 1)$ , čo je zrejme číslo deliteľné číslom 4.

**Príklad 45.** Dokážte, že výraz  $5n^4 + 10n^3 - 5n^2 - 10n$  je deliteľný číslom 120 pre každé prirodzené číslo  $n$ .

*Riešenie:* Deliteľnosť číslom 120 dokážeme tým, že dokážeme deliteľnosť číslami 24 a 5, pretože  $120 = 5 \cdot 24$  a čísla 5 a 24 sú nesúdeliteľné. Platí

$$5n^4 + 10n^3 - 5n^2 - 10n = 5 \cdot (n^4 + 2n^3 - n^2 - 2n).$$

Deliteľnosť číslom 5 je zrejmá. Preto nás zaujíma, či  $n^4 + 2n^3 - n^2 - 2n$  je deliteľné číslom 24. Výraz sa dá napísat ako súčin štyroch po sebe idúcich čísel

$$n^4 + 2n^3 - n^2 - 2n = (n^2 - 1) \cdot (n^2 + 2n) = (n - 1) \cdot n \cdot (n + 1) \cdot (n + 2).$$

Pre súčin štyroch po sebe idúcich čísel platí, že je deliteľný číslom  $4! = 24$ , preto platí  $24 \mid (n^4 + 2n^3 - n^2 - 2n)$ .

**Príklad 46.** Dokážte, že štvorec nepárnego prirodzeného čísla zmenšený o 1 je deliteľný štyrmi.

*Riešenie:* Nech nepárne číslo je  $n = 2k + 1$ , kde  $k \in \mathbb{N}_0$ . Potom jeho štvorec zmenšený o 1 je

$$n^2 - 1 = 4k^2 + 4k,$$

čo je číslo deliteľné číslom 4.

**Príklad 47.** Dokážte, že platí

$$\forall n \in \mathbb{N} : 24 \mid (25^n + 23).$$

*Riešenie:* Tento príklad môžete dokázať napríklad použitím matematickej indukcie. My ukážeme iný spôsob, pri ktorom použijeme binomickú vetu.

Použitím binomickej vety pre  $(24 + 1)^n$  dostaneme

$$25^n + 23 = (24 + 1)^n + 23 = \sum_{k=0}^n \binom{n}{k} \cdot 24^k \cdot \underbrace{1^{n-k}}_1 + 23.$$

Pre  $k > 1$  je časť výrazu s  $\binom{n}{k} \cdot 24^k$  vždy deliteľná číslom 24, pretože  $24 \mid 24^k$ . V prípade  $k = 0$ , dostaneme  $\binom{n}{0} \cdot 24^0 = 1$ . Jeho pripočítaním k číslu 23 obdržíme číslo 24, tj. číslo deliteľné číslom 24.

Predchádzajúca časť znamená, že

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} 24^k + 23 &= \underbrace{\binom{n}{0} \cdot 24^0}_1 + \sum_{k=1}^n \binom{n}{k} \cdot 24^k + 23 \\ &= 1 + 23 + \sum_{k=1}^n \binom{n}{k} \cdot 24^k \\ &= 24 + \sum_{k=1}^n \binom{n}{k} \cdot 24^k. \end{aligned}$$

Odtiaľ je zrejmé, že platí  $24 \mid (25^n + 23)$  pre každé prirodzené číslo  $n$ .

**Príklad 48.** Nech pre  $n \in \mathbb{N}$  je jeho rozvinutý zápis

$$\sum_{i=0}^k (10^i a_i),$$

kde  $k \in \mathbb{N}_0$ ,  $a_k \neq 0$ ,  $a_i \in \{0, 1, \dots, 9\}$  pre každé  $i \in \{0, 1, \dots, k\}$ .

Dokážte, že platí

$$\begin{aligned} \text{a)} \quad 6 \mid n &\Leftrightarrow 6 \mid \left( \sum_{i=1}^k (4a_i) + a_0 \right), \\ \text{b)} \quad 12 \mid n &\Leftrightarrow 12 \mid \left( \sum_{i=2}^k (4a_i) - 2a_1 + a_0 \right). \end{aligned}$$

*Riešenie:* K dôkazu použijeme skutočnosť, že pre každé  $n \in \mathbb{N}$ ,  $a \in \mathbb{N}$  a pre každé  $b \in \mathbb{Z} \setminus \{0\}$  platí

$$a \mid n \Leftrightarrow (ab) \mid (bn). \tag{5.1}$$

a) Kritérium pre deliteľnosť číslom 6 je

$$6 \mid n \Leftrightarrow (2 \mid n \wedge 3 \mid n).$$

Pre deliteľnosť číslom 2 a číslom 3 platí (druhá ekvivalencia v oboch prípadoch vychádza z (5.1))

$$2 \mid n \Leftrightarrow 2 \mid a_0 \Leftrightarrow 6 \mid (3a_0),$$

$$3 \mid n \Leftrightarrow 3 \mid \sum_{i=0}^k a_i \Leftrightarrow 6 \mid \sum_{i=0}^k (2a_i).$$

Označme

$$A = 3a_0, \quad B = \sum_{i=0}^k (2a_i), \quad C = \sum_{i=0}^k (6a_i),$$

kde  $C$  je vždy deliteľné číslom 6. Pre  $A, B, C$  platí

$$\begin{aligned} C - A - B &= \sum_{i=0}^k (6a_i) - \sum_{i=0}^k (2a_i) - 3a_0 \\ &= \sum_{i=1}^k (6a_i) + 6a_0 - \sum_{i=1}^k (2a_i) - 2a_0 - 3a_0 \\ &= \sum_{i=1}^k (6a_i - 2a_i) + (6a_0 - 2a_0 - 3a_0) \\ &= \sum_{i=1}^k (4a_i) + a_0. \end{aligned}$$

Z predchádzajúceho plynie

$$6 \mid n \Leftrightarrow (2 \mid n \wedge 3 \mid n) \Leftrightarrow (6 \mid A \wedge 6 \mid B) \Leftrightarrow 6 \mid (C - A - B),$$

čo sme chceli dokázať.

b) Teraz dokážeme kritérium pre číslo 12. Kritérium pre deliteľnosť číslom 12 je

$$12 \mid n \Leftrightarrow (3 \mid n \wedge 4 \mid n).$$

Pre deliteľnosť číslom 3 platí

$$3 \mid n \Leftrightarrow 3 \mid \sum_{i=0}^k a_i \Leftrightarrow 12 \mid \sum_{i=0}^k (4a_i).$$

Z deliteľnosti číslom 4 dostaneme

$$2 \mid n \Leftrightarrow 4 \mid (10a_1 + a_0) \Leftrightarrow 12 \mid (30a_1 + 3a_0).$$

Položme

$$A = \sum_{i=0}^k (4a_i), \quad B = 30a_1 + 3a_0, \quad C = 24a_1.$$

Je zrejmé, že je vždy splnené  $12 \mid C$ . Pre  $A, B, C$  platí

$$\begin{aligned}
A - B + C &= \sum_{i=0}^k (4a_i) - 30a_1 - 3a_0 + 24a_1 \\
&= \sum_{i=2}^k (4a_i) + 4a_1 + 4a_0 - 30a_1 - 3a_0 + 24a_1 \\
&= \sum_{i=2}^k (4a_i) + (4a_1 - 30a_1 + 24a_1) + (4a_0 - 3a_0) \\
&= \sum_{i=2}^k (4a_i) - 2a_1 + a_0.
\end{aligned}$$

Tvrdenie plynie z toho, že

$$12 \mid n \Leftrightarrow (3 \mid n \wedge 4 \mid n) \Leftrightarrow (12 \mid A \wedge 12 \mid B) \Leftrightarrow 12 \mid (A - B + C).$$

## Cvičenia

1. Dokážte, že pre každé prirodzené číslo  $a$  platí:

$$D(a, a+1) = 1, D(a, a+2) = D(a, 2), D(2a, 2a+1) = 1, n(a, a+1) = a \cdot (a+1).$$

2. Dokážte, že pre každé prirodzené číslo  $n$  platí

- a)  $5 \mid (n^5 + 4n)$ ,
- b)  $4 \mid (n^4 + 6n^3 + 11n^2 + 6n)$ ,
- c)  $3 \mid (4^n + 5)$ ,
- d)  $6 \mid (7^n - 6n - 1)$ ,
- e)  $5 \mid (8^{2n} - 3^{2n})$ ,
- f)  $5 \mid (2^{4n+2} - 3)$ ,
- g)  $7 \mid (n^7 - 8n)$ ,
- h)  $7 \mid (2^{n+2} + 3^{2n+1})$ .

## 5.3 Úlohy z olympiád a matematických korespondenčných seminárov

Nasledujúce úlohy pochádzajú z matematickej olympiády pre stredné školy a z korespondenčných seminárov, konkrétnie MATMIX, PraSe a KMS. Výsledky úloh možno nájsť na príslušných stránkach uvedených nižšie.

Matematická olympiáda je olympiáda pre žiakov základných a stredných škôl, v ktorej žiaci majú za úkol v niekoľkohodinovom limite vypočítať, resp. dokázať, niekoľko príkladov, bližšie informácie možno nájsť napríklad na stránke <http://mo.webcentrum.muni.cz/>.

MATMIX je časopis venovaný matematike, ktorý vydáva Ing. Mgr. Martin Hriňák v spolupráci s Jednotou slovenských matematikov a fyzikov, pobočka Bratislava 1. Jeho súčasťou je aj korešpondenčný seminár určený pre žiakov druhého stupňa základných a stredných škôl. Viac podrobností možno nájsť na <http://www.matmix.sk/>.

Matematický korešpondenčný seminár – seminár PraSe (PRAžský SEMinár) – je celoročná súťaž pre žiakov stredných škôl organizovaná študentmi Matematicko-fyzikálnej fakulty Univerzity Karlovej v Prahe. Informácie o tomto seminári nájdete na stránkach <https://mks.mff.cuni.cz/index.php>.

Seminár KMS (Korešpondenčný Matematický Seminár) je ďalšia matematická súťaž pre žiakov stredných škôl, ktorú organizujú študenti Univerzity Komenského v Bratislave, informácie možno nájsť na <http://www.kms.sk/>.

**Úloha 1.** (MO 47.ročník, kategória C, domáce kolo)

Pre ľubovoľné trojciferné číslo určíme jeho zvyšky pri delení číslami  $2, 3, 4, \dots, 10$  a získaných deväť čísel potom sčítame. Zistite najmenšiu možnú hodnotu takéhoto súčtu.

**Úloha 2.** (MO 47.ročník, kategória C, školské kolo)

Zistite najmenšie trojciferné číslo, ktoré je deliteľné práve polovicou z čísel

$$2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 36.$$

**Úloha 3.** (MO 49. ročník, kategória C, domáce kolo)

Pri delení istého prirodzeného čísla číslami 19 a 99 vyndú ako zvyšky dve prvočísla. Súčet oboch neúplných podielov sa rovná 1999. Určte delené číslo.

**Úloha 4.** (MO 48.ročník, kategória C, 2.kolo)

Najdite najväčšie trojmiestne číslo  $n$ , pre ktoré je súčet

$$1^2 + 2^3 + 3^4 + 4^5 + \dots + n^{n+1}$$

deliteľný troma.

**Úloha 5.** (MO 48.ročník, kategória A, 2.kolo)

Aritmetický priemer niekoľkých navzájom rôznych prvočísel sa rovná 27. Určte, aké najväčšie prvočíslo medzi nimi môže byť.

**Úloha 6.** (MO 48.ročník, kategória C, 1.kolo)

Určte najväčšie štvormiestne číslo  $n$ , pre ktoré je súčet  $n^{19} + 99^n$  deliteľný desiatimi.

**Úloha 7.** (MO 50.ročník, kategória C, domáce kolo)

Najdite všetky dvojice prirodzených čísel  $a, b$ , pre ktoré platí

$$n(a, b) + D(a, b) = 63,$$

kde  $n(a, b)$  značí najmenší spoločný násobok a  $D(a, b)$  najväčší spoločný deliteľ čísel  $a, b$ .

**Úloha 8.** (MO 48.ročník, kategória C, domáce kolo)

Zistite, či je číslo  $19^{1998} + 98^{1999}$  deliteľné deviatimi.

**Úloha 9.** (MO 50.ročník, kategória B, 1. kolo)

Nájdite všetky trojmiestne čísla  $n$ , ktorých druhá mocnina končí rovnakým trojčíslom ako druhá mocnina čísla  $3n - 2$ .

**Úloha 10.** (MO 50.ročník, kategória C, 1.kolo)

Nájdite všetky trojice  $a, b, c$  prirodzených čísel, pre ktoré súčasne platí

$$n(ab, c) = 2^8, \quad n(bc, a) = 2^9, \quad n(ca, b) = 2^{11},$$

kde  $n(a, b)$  značí najmenší spoločný násobok prirodzených čísel  $x$  a  $y$ .

**Úloha 11.** (MO 50.ročník, kategória C, 1.kolo)

Pre ktoré dvojmiestne čísla  $n$  je číslo  $n^3 - n$  deliteľné štomi?

**Úloha 12.** (MO 50.ročník, kategória C, 2.kolo)

Nájdite všetky dvojice prirodzených čísel  $a, b$ , pre ktoré platí

$$a + b + D(a, b) + n(a, b) = 50,$$

kde  $D(a, b)$  značí najväčší spoločný deliteľ a  $n(a, b)$  najmenší spoločný násobok prirodzených čísel  $a, b$ .

**Úloha 13.** (MO 51.ročník, kategória C, domáce kolo)

Dokážte, že existuje jediná číslica  $c$ , pre ktorú možno nájsť jediné prirodzené číslo  $n$  končiace číslicom  $c$  a majúca vlastnosť, že číslo  $2n + 1$  je druhou mocninou prvočísla.

**Úloha 14.** (MO 51.ročník, kategória C, 1. kolo)

Určte všetky dvojice prvočísel  $(p, q)$  také, že  $p > q$  a číslo  $p^2 - q^2$  má najviac štyri delitele.

**Úloha 15.** (MO 51.ročník, kategória A, 2. kolo)

Nájdite všetky dvojice prirodzených čísel  $x$  a  $y$ , pre ktoré platí

$$x^2 = 4y + 3 \cdot n(x, y),$$

kde  $n(a, b)$  značí najmenší spoločný násobok čísel  $x$  a  $y$ .

**Úloha 16.** (MO 51.ročník, kategória B, 2. kolo)

Nájdite všetky prirodzené čísla  $n$ , ktoré sú menšie ako 100 a majú tú vlastnosť, že druhé mocniny čísel  $7n + 5$  a  $4n + 3$  končia rovnakým dvojčíslom.

**Úloha 17.** (MO 51.ročník, kategória C, 2. kolo)

Určite počet dvojíc  $(a, b)$  prirodzených čísel ( $1 \geq a, a < b, b \geq 86$ ), pre ktoré je súčin  $ab$  deliteľný troma.

**Úloha 18.** (MO 51.ročník, kategória C, 2. kolo)

Nájdite všetky celé čísla  $x$ , pre ktoré sú obe čísla  $(x - 3)^2$ ,  $(x - 7)^2 + 1$  prvočísla.

**Úloha 19.** (MO 53.ročník, kategória B, domáce kolo)

Určite všetky prirodzené čísla  $M$  deliteľné 240, pre ktoré má rovnice

$$M = NSN(x, y)$$

s neznámymi  $x$  a  $y$  práve 1001 riešení v obore prirodzených čísel. (Symbol  $NSN(x, y)$  značí najmenší spoločný násobok čísel  $x, y$ .)

**Úloha 20.** (KMS, 1. séria letnej časti 2011/2012)

Snehulienka si myslí prvočíslo  $p > 7$ . Trpaslíci tvrdia, že  $p^2 - 1$  je deliteľné číslom 24. Dokážte, že majú pravdu.

**Úloha 21.** (KMS, 1. séria letnej časti 2012/2013)

Najdite všetky možnosti pre 21 po sebe idúcich čísel, z ktorých je aspoň 8 prvočísel.

**Úloha 22.** (KMS, 1. séria letnej časti 2012/2013)

Najdite prvočíslo  $p$ , pre ktoré platí, že  $2013 \cdot p + 1$  je druhou mocninou nejakého prirodzeného čísla.

**Úloha 23.** (KMS, 1. séria zimnej časti 2013/2014)

Po návštive indiánskej osady sa Monty vrátil späť do Oakvillu. Ihneď si všimol, že z miestnej banky stúpa kúdol čierneho dymu. Šerif, ktorý už bol na mieste činu, oboznámil Montyho s tým, že sa jedná o bankovú lúpež. Banditi ukradli z trezoru dve vrecia so zlatými tehličkami. V prvom vreci bolo  $a$  tehličiek a v druhom vreci  $b$  tehličiek. Navyše si bankár, väsnivý počtár, zapamätal, že číslo  $a + 11b$  je deliteľné číslom 13, a že číslo  $a + 13b$  je deliteľné číslom 11. Lúpež ho však natol'ko zaskočila, že zabudol na to, kolko tehličiek bolo v jednotlivých vreciach. Zaujímalo by ho, aký najmenší lup si mohli banditi odnieť. Pomôžte mu a zistite, akú najmenšiu hodnotu môže nadobúdať súčet  $a + b$ , ak viete, že čísla  $a$  a  $b$  sú kladné, celé a splňajú vzťah, ktorý si zapamätal bankár.

**Úloha 24.** (KMS, 2. séria zimnej časti 2013/2014)

Po nevydarenej lúpeži sa Krivozubý Tony nejakú dobu rozčuloval, no časom z neho hneď vyprchal. Rozhodol sa, že si zlepší náladu tým, že potrápi Waltyho hlavu. Dal mu nasledovnú úlohu. Na svojom tele má  $n$  jaziev. Toto číslo  $n$  je dvojciferné a navyše číslo  $n^3 - n$  je deliteľné číslom 100. Montyho úloha je zistiť, kolko jaziev môže mať Tony. Zistite aj vy, ktoré čísla  $n$  vychovujú zadaniu. Nezabudnite prísť na všetky riešenia.

**Úloha 25.** (Seminář PraSe, 2011/2012, 3. jarní série - Prvočísla)

Hovoríme, že prirodzené číslo je *ospalé*, pokiaľ sa v jeho prvočíselnom rozkladu vyskytujú len prvočísla 2 a 3. Martina našla ospalé čísla  $a$ ,  $b$  také, že  $a + b$  je tiež ospalé. Dokážte, že  $a$  je násobok  $b$  alebo naopak.

**Úloha 26.** (Seminář PraSe, 2011/2012, 3. jarní série - Prvočísla)

Anča má štvorcovú čokoládu ( $n \times n$  dielikov). Dostala chut', zjedla z nej prvočíselný počet dielikov a zvyšných 400 si schovala na neskôr. Kolko dielikov Anča zjedla? Najdite všetky možnosti.

**Úloha 27.** (Seminář PraSe, 2010/2011, 2. podzimní série - Dělitelnost)

Dokážte, že  $3^k \mid \underbrace{111 \dots 1}_{3^k}$  pre všetky  $k \in \mathbb{N}$ .

**Úloha 28.** (Seminář PraSe, 2010/2011, 2. podzimní série - Dělitelnost)

Najdite všetky prirodzené čísla, ktoré sa rovnajú druhej mocnine počtu svojich deliteľov.

**Úloha 29.** (Seminář PraSe, 2006/2007, 2. série - Diofantické rovnice)

Najdite všetky riešenia rovnice

$$\frac{a+1}{2} = \frac{3}{b+1}$$

v obore prirodzených čísel.

**Úloha 30.** (MATMIX, 2006/2007, 3. séria)

Najdite najmenšie prirodzené číslo  $n$ , pre ktoré vieme nájsť 15 rôznych prvkov  $a_1, a_2, \dots, a_{15}$  množiny  $\{16, 17, \dots, n\}$  takých, že prvok  $a_k$  je deliteľné číslom  $k$  pre  $k = 1, 2, \dots, 15$ .

**Úloha 31.** (MATMIX, 2009/2010, 1. séria)

Zistite, či existuje množina 4 004 takých prirodzených čísel, že súčet čísel ľubovoľnej 23-prvkovej podmnožiny tejto množiny nie je deliteľný číslom 2 003.

**Úloha 32.** (MATMIX, 2008/2009, 1. séria)

Najdite všetky také celé čísla  $y$  a prvočísla  $p, q$  menšie ako 100, pre ktoré platí

$$1999 = 86y + p - q.$$

**Úloha 33.** (MATMIX, 2005/2006, 2. séria)

Dokážte, že platí:

$$323 \mid (20^{2004} + 16^{2004} - 3^{2004} - 1).$$

**Úloha 34.** (MATMIX, 2007/2008, 3. séria)

Pre prirodzené číslo  $n$  platí, že číslo  $2n$  má 28 deliteľov a číslo  $3n$  má 30 prirodzených deliteľov. Určte, kolko prirodzených deliteľov môže mať číslo  $6n$ .

# Záver

Táto práca sa zaoberala vytvorením výukového materiálu na téma deliteľnosť pre nadaných žiakov stredných škôl.

Celá práca bola rozdelená do niekoľkých kapitol.

V prvej kapitole boli zhrnuté všetky potrebné pojmy a vety, ktoré čitateľ potreboval na pochopenie tejto problematiky. Za výkladmi k novým pojmom nasledovali cvičenia na precvičenie.

V ďalšej kapitole boli zhrnuté kritéria deliteľnosti číslami 2 až 20. Kritéria deliteľnosti slúžia k rozhodovaniu, či je dané číslo deliteľné určitým prirodzeným číslom, a to tak, aby to bolo jednoduché aj bez použitia písomného delenia alebo kalkulačky. Kritéria, ktoré tu boli uvedené, boli dokázané, a tiež vysvetlené na príkladoch.

Nasledovala kapitola venovaná diofantickým rovniciam, ktoré úzko súvisia s deliteľnosťou. Ukázali sme, že existencia riešenia takýchto rovníc závisí od zadaných celočíselných koeficientov a pravej strany. Pokial platila podmienka, že pravá strana je deliteľná najväčším spoločným deliteľom koeficientov na ľavej strane rovnice, mali sme zaručenú riešiteľnosť lineárnej diofantickej rovnice s dvoma neznámymi. Jedno riešenie takejto rovnice sme našli pomocou Euklidovho algoritmu. Pri kvadratických diofantických rovniciach bola opäť rozhodujúca podmienka na pravú stranu, aby bola zaručená existencia riešenia (muselo to byť buď nepárne číslo, alebo číslo deliteľné štyrmi). Riešenie týchto rovníc sa bez využitia deliteľnosti jednoducho nezaobišli.

Predposledná kapitola bola o prvočíslach a ich využití v praktickom živote. Čitateľ sa v nej mohol dozvedieť, že prvočíslo 11 sa využíva na vytvorenie rodného čísla alebo čísla bankových účtov, a tiež zo spôsobom šifrovania pomocou veľkých prvočísel (metóda RSA).

Posledná kapitola boli cvičenia a príklady na deliteľnosť. Niektoré z nich boli prevzaté z olympiád, matematických korešpondenčných seminárov, stredoškolských učebníc, ale časť z nich bola tiež vytvorená samotnou autorkou.

# Zoznam prvočísel menších ako číslo 3000

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999

# Odkazy na internetové stránky

## Deliteľnosť

- KMS – Knihovna: Dělitelnost a kongruence  
<https://mks.mff.cuni.cz/library/library.php?categ=44&supcats=7>
- Kritéria deliteľnosti  
[ftp://ftp.mgo.opava.cz/kav/matematika/prima/kr\\_delitelnosti\\_7\\_11-13.pdf](ftp://ftp.mgo.opava.cz/kav/matematika/prima/kr_delitelnosti_7_11-13.pdf)  
[http://class.pedf.cuni.cz/NewSUMA/Download/Volne/SUMA\\_44.pdf](http://class.pedf.cuni.cz/NewSUMA/Download/Volne/SUMA_44.pdf)

## Prvočísla

- Tabuľka všetkých 78 498 prvočísel do 1 000 000  
<http://www.beda.cz/~jirkaj/pr1e6.pdf>
- KMS – Knihovna: Prvočísla  
<https://mks.mff.cuni.cz/library/library.php?categ=58&supcats=7>
- Stránka o prvočíslach  
<http://primes.utm.edu/>

## Diofantické rovnice

- KMS - Knihovna: Diofantické rovnice  
<https://mks.mff.cuni.cz/library/library.php?categ=31&supcats=7>

## Matematické súťaže a korešpondenčné semináre

- Matematická olympiáda  
<http://mo.webcentrum.muni.cz/>
- Seminár PraSe (PRAžský SEMinář)  
<https://mks.mff.cuni.cz/index.php>
- KMS - korešpondenčný matematický seminár  
na <http://www.kms.sk/>
- Časopis MATMIX  
<http://matmix.sk/>

# Literatúra

- [1] KMS - korešpondenčný matematický seminár, archív. <http://www.kms.sk/archiv>. Navštívené dňa: 5.6.2014.
- [2] Bušek, I. a Calda, E. *Matematika pro gymnázia: Základní poznatky z matematiky*. Učebnice pro střední školy. Prometheus, 1999.
- [3] Olejár M., Olejárová I. a et al. *Zbierka vzorcov z matematiky*. Young Scientist, 2002.
- [4] Burjan V., Hrdina Ľ. a Maxian M. *Prehľad matematiky*. Slovenské pedagogické nakladatelstvo, Bratislava, 1977.
- [5] Ďuriš V. a Šovišová M. *Diofantické rovnice a metódy ich riešenia*. Fakulta prírodných vied UKF/Prírodovedec č. 452, Nitra, 2011.
- [6] Bálint V. et al. *53. ročník matematickej olympiády na stredných školách*. IUVENTA, 2005.
- [7] Horák K. et al. *47. ročník matematickej olympiády na stredných školách*. IUVENTA, 1999.
- [8] Horák K. et al. *48. ročník matematickej olympiády na stredných školách*. IUVENTA, 2000.
- [9] Horák K. et al. *49. ročník matematickej olympiády na stredných školách*. IUVENTA, 2001.
- [10] Horák K. et al. *50. ročník matematickej olympiády na stredných školách*. ŽSR, 2001.
- [11] Horák K. et al. *51. ročník matematickej olympiády na stredných školách*. IUVENTA, 2004.
- [12] Bartsch H.J. *Matematické vzorce*. Mladá fronta, 2000.
- [13] M. Hriňák. Zadania 2. séria úloh korešpondenčnej súťaže. *Časopis MATMIX*, 2005/2006.
- [14] M. Hriňák. Zadania 3. séria úloh korešpondenčnej súťaže. *Časopis MATMIX*, 2006/2007.
- [15] M. Hriňák. Zadania 3. séria úloh korešpondenčnej súťaže. *Časopis MATMIX*, 2007/2008.

- [16] M. Hriňák. Zadania 1. série úloh korešpondenčnej súťaže. *Časopis MATMIX*, 2008/2009.
- [17] M. Hriňák. Zadania 1. série úloh korešpondenčnej súťaže. *Časopis MATMIX*, 2009/2010.
- [18] Petáková J. *Matematika – příprava k maturitě a k přijímacím zkouškám na vysoké školy*. Prometheus, 1998.
- [19] Polák J. *Přehled středoškolské matematiky*. Prometheus, 2008.
- [20] Zhouf J. Kritéria dělitelosti. [http://class.pedf.cuni.cz/NewSUMA/Download/Volne/SUMA\\_44.pdf](http://class.pedf.cuni.cz/NewSUMA/Download/Volne/SUMA_44.pdf). Navštívené dňa: 20.4.2014.
- [21] Křížek M., Somer L. a Šolcová A. *Kouzlo čísel: Od velkých objevů k aplikacím*. Academia, 2009.
- [22] Hriňák M. *Metódy riešenia matematických úloh 1.* vydalo Metodicko-pedagogické centrum, Bratislava v rámci projektu Korešpondenčný seminár MATMIX, 2008.
- [23] Jahoda P. *Základy teorie čísel a jejích aplikací pro nematematiky*. Vysoká škola báňská – Technická univerzita Ostrava a Západočeská univerzita v Plzni, projekt *Matematika pro inženýry 21. století* (reg. č. CZ.1.07/2.2.00/07.0332), 2010.
- [24] Vondruška P. *Kryptologie, šifrování a tajná písma*. Albatros Praha, 2006.
- [25] Kořínek V. *Základy algebry*. Nakladatelství ČAV, 1956.
- [26] Vejsada F. a Talafous F. *Zbierka úloh z matematiky pre SVŠ*. Slovenské pedagogické nakladateľstvo, 1972.
- [27] Šedivý J. *Základné poznatky z algebry a teórie čísel pre 1. ročník gymnázia so zameraním na matematiku*. Slovenské pedagogické nakladateľstvo, 1986.
- [28] Wells D. *Prime Numbers: The Most Mysterious Figures in Math*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2005.