Kapitola 3

Základy elementární teorie čísel

Elementární teorie čísel se zabývá dělitelností v oboru celých čísel ($\mathbb{Z}$) nebo v oboru přirozených čísel ($\mathbb{N}$). Základními pojmy jsou prvočíslo, číslo složené,, společný dělitel a společný násobek. Můžeme sem také zařadit pojmy jako trojúhelníkové číslo, čtvercové číslo, číslo dokonalé, spřátelená čísla, prvočíselná dvojčata a podobně.

Co se tím myslí? Jakýmsi základním problémem je nalezení řešení rovnice $ax = b$ v oboru celých čísel, tzn. zajímají nás pouze celočíselná řešení. Celočíselným řešením rovnice $2x = 3$ *není* (pochopitelně) číslo $1,5$; v oboru reálných čísel samozřejmě ano.

V zápalu řešení rovnici někdy zapomínáme, v jakém oboru jsme ji měli řešit. Proč vůbec omezovat výsledky dělení na celočíselné, když si např. dokážeme představit, že koláč lze rozdělit na sedm dílů? Například proto, že praktické provedení (rozkrájení koláče na sedm stejných nebo dokonce i jen stejně velkých kousků) není úplně jednoduché.Podobně asi nelze dost dobře rozdělit na sedminy plod lesní jahody nebo třeba knihy. Rozlišujme tedy mezi *dělitelností*, která se týká výhradně celých čísel, a operací *dělení*, která probíhá v tom oboru, který si zvolíme. Formální definice dělitelnosti vypadá následovně:

Definice 3.1 *Nechť a, b jsou celá čísla. Říkáme, že číslo a je dělitelné číslem b právě tehdy, když existuje celé číslo q takové, že platí $a = bq$. Číslo a nazýváme q-násobkem (nebo jen násobkem) čísla b.*

Lehce nahlédneme, že platí následující tvrzení:

(a) Pokud a dělí b a současně b dělí c, pak také a dělí c.

(b) Pokud a dělí b a současně a dělí c, pak a dělí rozdíl b-c.

(c) Pro nenulová c platí: a dělí b právě tehdy když ac dělí bc.

(d) Pokud a dělí b a b je kladné, pak a je menší nebo rovno b.

Tato tvrzení lze dokázat například tak, že si zapíšeme b jako k-násobek a a analogicky c zapíšeme jako m-násobek b, kde k a m jsou vhodná celá čísla. Tvrzení (b) je základem postupu nazvaného Eukleidův algoritmus.

Dále platí věta:

Věta 3.2 (O dělení se zbytkem) *Pro libovolné celé číslo a a přirozené číslo m existují právě jedno celé číslo q a právě jedno číslo r z množiny čísel $\{0, 1, ...(m-1)\}$ taková, že platí: $a = mq + r$.*

Zápis čísla pomocí věty o dělení se zbytkem. Předchozí větu lze dobře využít k tomu, abychom mohli odpovědět na otázky:

- Jaký zbytek po dělení dávají mocniny čísla, které po dělení šesti dává zbytek 1?
- Jaký zbytek po dělení dávají mocniny čísla, které po dělení šesti dává zbytek 5?
- Ukažte, že součin tří po sobě jdoucích čísel je vždy dělitelný třemi.
- ...

3.1 Znaky dělitelnosti (známe často ze ZŠ)

Všechna pravidla uváděná ve školské matematice jsou založena na zápisu čísel v desítkové soustavě poziční soustavě a nelze je jen tak používat, pracujeme-li se zápisem čísla v jiné číselné soustavě.

Zápis čísla v poziční desítkové soustavě

Co je to desítková (dekadická) poziční soustava? Je to způsob zápisu čísel, který se děti učí v první třídě ZŠ. Používáme pri něm deset cifer (0, ..., 9) a jejich význam souvisí s místem, které v číselném zápisu zaujímají: tak 910 je jiné číslo než 109. Jednotlivé cifry stojí na místě (zprava do leva) jednotek, desítek, stovek, tisíců atd.

```
formální zápis:

 a(n)-a(n-1)-\ldots - a(1) - a(0) =
 a x (10 na n) + \ldots + a(1) x 10 + a(0)
```

Shrňme nyní některé poznatky o dělitelnosti, které znáte ze základní a střední školy:

- **dělitelnost 10, 5, 2** určíme podle poslední cifry.
- **dělitelnost 4, resp. 8** určíme podle toho, zda je poslední dvojčíslí dělitelné 4, resp. poslední trojčíslí 8.
- **dělitelnost 3 a 9** určíme pomocí ciferného součtu.

Důkaz pravidla dělitelnosti 3 a 9 (v desítkové poziční soustavě):
zápis čísla v desítkové soustavě:

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

Víme, že:

Jako cvičení dokažte pravidla o dělitelnosti výše uvedená (2, 4, 5 a 8)

```
Pro zajímavost uvedeme
dělitelnost 7 a 11
```

Dělitelnost 7 lze určit např. takto:

(a) rozdíl součtu čísel vzniklých ze „sudých“ a „lichých“ trojic cifer je dělítelný 7;

(b) je-li 7 dělitelný součet násobků číslic daného čísla *odzadu* postupně čísly 1, 2, 3, 4, 5, 6, 1, 2, ldotst (atd., periodicky se opakuje), pak je číslo dělitelné 7.

(c) rozdíl dvou čísel, z nichž první je tvořeno číslicemi daného čísla vyjma poslední a druhé je dvojnásobkem poslední číslice, je dělitelný 7 (periodicky opakujeme, podobně jako když používáme kritérium pro dělitelnost 3 a 9).

```
Používá se pro čísla letenek nebo čísla zakázek, odhalí 94 procent nesrovnalostí
k tomu slouží teorie kódování --- na konci čísla zakázky nebo letenky bývá
tzv. kontrolní číslice --- rozmyslete si, že stačí jedna číslice.
```

Proč to platí?

```
např. (c)
n=10a +b
je-li a - 2b dělitelné 7, pak
existuje m přirozené: a-2b=7m
Pak a = 7m + 2b, tedy 10a=70m+20b

jelikož n = 10a+b (předpoklad), pak 10a=n-b
ale je-li a-2b=7m, pak také 10a= 70m +20b

dohromady: n-b=70m+20b, tedy n=70m+21b = 7(10m+3b)
tedy n je dělitelné 7
```

Po přečtení výše uvedených pravidel vzniká otázka, zda není rychlejší dané číslo sedmi vydělit. U dělitelnosti 11 vypadají pravidla na první pohled schůdněji:

Dělitelnost 11 lze určit třemi způsoby:

(a) rozdíl součtu číslic na sudých a lichých místech je dělitelný 11;

(b) součet jednotlivých dvojčíslí je dělitelný 11;

(c) rozklad trojčíslí na sudých a lichých místech dělitelný 11.

```
K zamyšlení:
Rozmyslete si, odkud se počítají trojčíslí, ev. dvojčíslí.
Nebo je to jedno?
```

Kontrola dělitelnosti 11 se používá jako kontrolní znak pro rodná čísla nebo čísla účtů. U rodných čísel je prvních šest cifer určeno pohlavím a datem narození, další dvě číslice bývaly kódem pro místo narození a poslední dvě číslice byly kontrolní — byly doplněny tak, aby výsledek byl dělitelný 11.

3.2 Prvočísla a čísla složená. Základní věta aritmetiky.

Pojmy prvočíslo a číslo složené znáte patrně již ze základní školy. Pro naše účely budemme používat následující definici

již na ZŠ jste se dozvěděli o existenci prvočísel

Definice 3.3 prvočíslo - má právě dva různé kladné dělitele
číslo složené - více než dva různí kladní dělitelé
zvláštní případ - číslo 1

Samozřejmě pokud a dělí b, pak také a dělí -b; -a dělí b; -a dělí -b
triviální dělitelé: čísla 1 a -1

0 má nekonečně mnoho děliteů
ale nulou nelze dělit

říkat, že nula dělí pouze nulu může být matoucí,
ale podle definice je to tak:
pokud 0=km,
pak je k = 0 nebo je m=0

(Poznámka: spojka "nebo" je zde využita tak, jak jste
se s ní seznámili ve výrokové logice, např. v předmětu
Základy matematiky: může nastat i situace, kdy k=0=m)

Tohoto tvrzení využíváme např. hledáme-li body na ose x,
v nichž daná funkce vyjádřená polynomem nabývá hodnoty 0

Přinejmenším intuitivně znáte následující tvrzení:[1]

Věta 3.4 (Základní věta aritmetiky) *Každé přirození číslo lze jednoznačně vyjádřit ve tvaru součinu mocnin prvočísel.*

* * * * *

Definice 3.5 (Největší společný dělitel) *Nechť a, b jsou celá čísla. Celé číslo m, pro něž platí, že m dělí a i že m dělí b, se nazývá společným dělitelem těchto dvou čísel. Kladný společný dělitel čísel a, b, který je dělitelný libovolným společným dělitelem těchto dvou čísel, se nazývá jejich největším společným dělitelem.*

Analogicky lze definovat nejmenší společný násobek dvou čísel:

Definice 3.6 (Nejmenší společný násobek) *Nechť a, b jsou celá čísla. Celé číslo m, pro něž platí, že m je násobkem a i že m je násobkem b, se nazývá společným násobkem těchto dvou čísel. Kladný společný násobek čísel a, b, který je dělitelem libovolného společného násobku těchto dvou čísel, se nazývá jejich nejmenším společným násobkem.*

[1] Je-li základní vět aritmetiky formulována takto, potřebujeme, aby 1 nebylo prvočíslo. Na druhou stranu, kdyby 1 byla považována za prvočíslo, jistě bychom si s definicí poradili; například tak, že bychom do ní zahrnuli podmínku, že žádně z prvočísel použitých v rozkladu nesmí být rovno 1. Jinými slovy, to, že 1 nepovažujeme za prvočíslo, je *konvence*.

Známe-li největšího společného dělitele, můžeme nejmenšího společného dělitele určit pomocí následující vět:

Věta 3.7 (Nejmenší společný násobek) `PODMÍNKY`

$$nsn(a,b) = \frac{(axb)}{NSD(a,b)}$$

Nesoudělná čísla

```
Dvě čísla jsou nesoudělná, pokud
jejich největším společným dělitelem je 1.
NSD (a, b) = 1

Největší společný násobek dvou
nesoudělných čísel je jejich součin, tj.
nsn (a, b) = a x b
```

Uveďme (zatím bez důkazu) následující tvrzení:

Věta 3.8 (Bezoutova) *Pro libovolná celá čísla a, b existují celá čísla x, y taková, že $NSD(a,b) = ax + by$.*

Pak také platí, jakékoliv celé číslo tvaru $ax + by$ je násobkem d.

Než Bezoutovu větu dokážeme, uvedem si postup známý jako *Eukleidův algoritmus.*

3.3 Diofantovské rovnice a Eukleidův algoritmus

Obecně jsou jako diofantovské (diofantické) rovnice označovány všechny rovnice (libovolného stupně a s libovolným počtem neznámých), které mají celočíselné koeficienty a pro které mají význam jen celočíselná řešení. Takovou rovnicí je tak i Pythagorova věta

$$x^2 + y^2 = z^2,$$

pokud hledáme pouze celočíselná řešení. Takovými řešeními jsou například pythagorejské trojice$x = 3, y = 4, z = 5$ nebo $x = 5, y = 12, z = 13$.

Diofantovské rovnice lze nalézt v různých starších sbírkách úloh, např. v této úloze ze sbírky *Úlohy k bystření mladíků* Alcuina z Yorku, tj. z doby kolem roku 800 našeho letopočtu:

Úloha o kupci kupujícím sto zvířat (Alcuin, Propositiones, č. 38): Nějaký muž chtěl koupit sto zvířat za sto zlatých, přičemž kůň se kupuje za třii zlaté, kráva za jeden zlatý a 24 ovcí za jeden zlatý. Řekni, kdo jsi s to, kolik bylo koní, kolik krav a kolik ovcí.
Řešení: sestavíme dvě rovnice o třech neznámých, v nichž x bude představovat počet koní, y počet krav a z počet ovcí.

$$\begin{aligned} x + y + z &= 100 \\ 3x + y + \frac{z}{24} &= 100 \end{aligned}$$

Druhou rovnici vynásobíme 24 a první číslem -1

$$\begin{aligned} -x - y - z &= -100 \\ 72x + 24y + z &= 2400 \end{aligned}$$

Obě rovnice sečteme a dostáváme rovnici

$$71x + 23y = 2300,$$

z níž po vydělení číslem 23 získáváme rovnici

$$\frac{71}{23}x + y = 100,$$

která bude mít celočíselné řešení pouze tehdy, bude-li x násobkem 23. Pak zřejmě $y = 100 - \frac{71}{23}x$. Dosadíme-li $x = 23$, vypočtem $y = 29$; odtud $z = 48$. Dosaddíme-li za x další násobek 23, tedy 46, vyjde y záporné, což nevyhovuje zadání příkladu. Jedinou možností nákupu zvířat je tedy koupě 23 koní (69 zlatých), 29 krav (29 zlatých) a 48 ovcí (2 zlaté).

Nyní uvedeme postup řešení nejjednodušší netriviální diofantovské rovnice (jednodušší je jen lineární rovnice o jedné neznámé, tj. rovnice tvaru $ax = b$, u níž je podmínka řešitelnosti v oboru celých čísel zřejmá: číslo b musí být násobkem čísla a.

Lineární diofantovskou rovnicí o dvou neznámých nazveme rovnici tvaru $ax + by = c$, kde a, b, c jsou celá čísla a hledáme pouze celočíselná řešení ($x, z \in \mathbb{Z}$, ne nutně kladná). Zda má tato rovnice řešení lze zjistt pomocí následující věty:

Věta 3.9 *Lineární diofantovská rovnice $ax + by = c$ ($a, b, c \in \mathbb{Z}$) má alespoň jedno (celočíselné) řešení právě tehdy, když c je násobkem největšího společného dělitele čísel a, b.*

Poznámka: Předchozí věta má tvar ekvivalence $A \Leftrightarrow B$, můžeme tedy říci, že B je nutnou a také dostatečnou podmínkou pro A (tedy řešitelnost diofantovské rovnice). V předmětu Základy matematiky jste si řekli, že obecně v implikaci $A \Rightarrow B$ platí, že B je nutnou podmínkou pro A. Platnost této implikace („zleva doprava“) je zřejmá, totiž rovnice $ax + by = c$ nemůže mít řešení v oboru celých čísel, pokud pravá strana není násobkem největšího společného dělitele čísel a a b.

Pokud platí i opačná implikace, tj. $B \Rightarrow A$, tedy pokud z toho, že pravá strana rovnice je násobkem největšího společného dělitele čísel a a b, přímo plyne existence celočíselného řešení rovnice, nazýváme B podmínkou *dostatečnou*; dohromady potom jde o podmínku *nutnou a dostatečnou.*

Uveďme nyní příklad diofantovské rovnice a postupu nalezení jejích řešení.

Příklad 3.10 Řešte v oboru celých čísel rovnice

(a) $2x + 3y = 1$

(b) $x + 3y = 4$

(c) $3x + 11y = 28$

Řešení: Nějaké řešení dokážeme ve všech případech odhadnout:

(a) $x = -1,\ y = 1$ nebo $x = 2\ y = -1$

(b) $x = 1,\ y = 1$ nebo $x = 7\ y = -1$

(c) $x = 2\ y = 2$ nebo $x = 13\ y = -1$

Co mají tato řešení společného a jak najdeme všechna? To ukážeme za chvíli.

Poznámka: Důkaz následující věty podává návod, jak najít největšího společného dělitele dvou čísel.[2]

Větu **??** můžeme přefprmulovat pro libovolný počet *nesoudělných* neznámých. Je-li totiž pravá i levá strana rovnice dělitelná největším společným dělitelem koeficientů na levé straně, pak můžeme tímto číslem vydělit pravou i levou stranu.

Věta 3.11 *Lineární diofantovská rovnice*

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = c,$$

kde $a_i \in \mathbb{Z}$ *a největší společný dělitel koeficientů* a_i *je roven* 1*, má vždy celočíselné řešení. Všechna celočíselná řešení této rovnice lze popsat pomocí* $n - 1$ *celočíselných parametrů.*

```
zopakujte si, co víte z kongruencích
z předmětu Základy matematiky
```

Důkaz: K důkazu této věty využijeme vlastnostni zvané kongruence, tj. vyjádření, že dva výrazy dávají stejný zbytek po dělení daným číslem (tzv. modulem). Připomeňmě, že zápis $a \equiv b(\mod m)$ čteme „a je kongruentní s b modulo m“.

Při důkazu budeme postupovat matematickou indukcí vzhledem k počtu neznámých. Pro jednu neznámou dostáváme rovnici $a_1x = 1$. Podmínka NSD(a) = 1 znamená, že a_1 může nabývat hodnot 1 nebo -1.Pro každou z těchto hodnot má rovnice jediné řešení, které nezavisí na žádném parametru (ve shodě s tvrzením věty, neboť (n-1)=(1-1)=0).

Předpokládáme tedy, že počet neznámých v rovnici je alespoň 2 ($n \geq 2$). Potom pro libovolné řešení musí platit:

$$a_1x_1 + a_2x_2 + \cdots a_nx_n \equiv c(\mod d),$$

kde d je největší společný dělitel koeficientů $a_1, a_2, \ldots, a_{n-1}$. Musí tedy platit také kongruence

$$a_nx_n \equiv c(\mod d)$$

[2]Pro zajímavost: **z hlediska filosofie matematiky** můžeme rozlišovat mezi důkazy existence a důkazy pomocí pomocí konstrukce daného objektu (v tomto případě jde o nalezení největšího společného dělitele). Eukleidův algoritmus dává návod, jak nalézt největšího společného dělitele, a tím dává i důkaz o jeho existenci pro ibovolná dvě celá čísla; naopak to neplatí: je-li nám známo, že jistý objekt existuje, neznamená to, že jej umíme najít.

(od levé strany kongruence jsme odečetli násobek čísla d, tedy zbytek po dělení pravé a levé strany číslem d se nezměnil). Podle předpokldau jsou čísla a_n a d nesoudělná, tedy platí:

$$x_n = k + d \cdot t,$$

kde k je vhodné celé číslo a t je libovolné celé číslo. Tím je důkaz hotov, neboť rovnice s $(n-1)$ neznámými má podle předpokladu řešení závislé na $(n-2)$ parametrech, a my jsme právě vyjádřili n-tou neznámou s pomocí parametru t, tedy máme všechna řešení dané rovnice vyjádřena pomocí $(n-1)$ parametrů.

Postup nyní ukážeme na konkrétním příkladu:

Příklad 3.12 Řešte v oboru celých čísel rovnici

(d) $3x + 7y = 2$

Řešení: Podle předchozí věty musí platit:

$$3x + 7y \equiv 2(\mod 3),$$

tedy $7y \equiv 2(\mod 3)$.
Dalšími úpravami získáváme: $y \equiv 2(\mod 3)$, a tedy $y = 2 + 3t$ (slovně vyjádříme: y dává po dělení třemi zbytek 2).
Dosadíme do původní rovnice:

$$3x + 7(2 + 3t) = 2$$

a odtud

$$3x = 2 - 14 - 21t = -12 - 21t,$$

tedy

$$x = 4 - 7t.$$

Řešením rovnice jsou všchny dvojice celých čísel tvaru $[4 - 7t; 2 + 3t]$, kde t je libovolné celé číslo.

Postup zvaný Eukleidův algoritmus se používá k hledání největšího společného dělitele dvou čísel. Využíváme při něm (zřejmého?!?) k tvrzení z předchozího odstavce:

(b) Pokud a dělí b a současně a dělí c, pak a dělí rozdíl b-c.

Je výpočetně jednodušší než hledání NSD pomocí rozkladu čísla na prvočísla, o jejichž existenci jsme se v rámci tohoto textu dosud nezmínili. Pro výpočet NSD pomocí Eukleidova algoritmu tento pojem ani nepotřebujeme.

xxx

3.4 Úlohy na zbytkové třídy (důkazy)

Cvičení 3.13 *Dokažte: 2. mocnina lichého čísla dává po dělení* 4 *zbytek* 1.

Cvičení 3.14 *Dokažte: 2. mocnina násobku* 3 *dává po dělení* 3 *zbytek* 1.

Cvičení 3.15 *Nechť m je prvočíslo. Dokažte, že m nedělí $(m-1)!$.*

Cvičení 3.16 *Nechť m je číslo složené. Dokažte, že m dělí $(m-1)!$.*