II. KAPITOLA

ALGEBRA A TEORIE ČÍSEL

Algebra byla původně pouze naukou o řešení rovnic. S jejími počátky se setkáváme už ve starém Řecku. Ve III. století před naším letopočtem žil Diofantos z Alexandrie, jehož jméno se nám zachovalo v termínu diofantická rovnice; je to rovnice, jejíž řešení se hledá v oboru celých čísel. O systematickém rozvoji algebry v antice (na rozdíl od geometrie) však mluvit nelze. Započali s ním až arabští matematikové v raném středověku. Samo slovo algebra pochází z názvu knihy „Hisab al-džebr val-muqabala“ (nauka o napravování a zjednodušování), kterou napsal Muhammad ibn Músá al-Chvárizmí v IX. století. Ono „napravování a zjednodušování“ znamená postup při řešení algebraické rovnice, jak jej známe ze školy. Poznamenejme, že ve Španělsku (pod vlivem Maurů) slovo „algebrista“ značilo napravovače zlomenin, což býval zpravidla také holič.

Později se našly způsoby řešení rovnic druhého a třetího stupně. Vzorec pro řešení kvadratické rovnice jistě znáte. Vzorec pro řešení kubické rovnice $x^3 + px = q$ se nazývá Cardanův vzorec podle H. Cardana (1501—1576); je to

$$x = \sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} + \frac{q}{2}} - \sqrt[3]{\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} - \frac{q}{2}}.$$

Dlouhou dobu se matematikové snažili získat podobné vzorce pro rovnice stupně vyššího než čtvrtého. Teprve E. Galois (1811—1832) a nezávisle na něm N. H. Abel (1802—1829) dokázali, že u takovýchto rovnic nelze vypočítat kořeny z koeficientů rovnice pomocí početních operací sčítání, odčítání, násobení, dělení, umocňování a odmocňování (říkáme, že tyto rovnice nelze řešit v radikálech). Tento důkaz byl vlastně počátkem abstraktní algebry, o níž bude dále řeč. Jak vidíme z letopočtů narození a úmrtí, oba zmínění matematikové zemřeli velmi mladí; Galois měl dokonce podobný osud jako básník Puškin — zemřel v souboji.

K zapisování a řešení soustav lineárních rovnic se užívají matice; jsou to tabulky čísel uspořádané do obdélníka, popřípadě do čtverce, a jsou pro ně definovány početní operace podobně jako pro čísla. Význam matic dnes již daleko přesahuje pouhé řešení soustav rovnic; matice se uplatňují v řadě jiných matematických oborů i ve fyzice. Dokonce se definují i funkce matic. Můžeme mít například sinus matice — tedy ne sinus čísla, ale sinus celé tabulky čísel; tento sinus je opět maticí. Teorie matic se zahrnuje do takzvané lineární algebry. Ta se kromě matic zabývá vektorovými prostory, lineárními zobrazeními a podobnými pojmy.

Různé operace se dají provádět i s jinými objekty než s čísly. Známe sčítání úseček a úhlů, analogií násobení čísel může být skládání nějakých zobrazení. Zabýváme-li se různými operacemi bez ohledu na to, jakého druhu jsou objekty, s nimiž je provádíme, mluvíme o abstraktní algebře. O různých pojmech tohoto oboru si povíme později.

Samostatným oborem, který těsně souvisí s algebrou, je teorie čísel. Zdálo by se, že o číslech musí být už všechno známo; není tomu tak a stále zůstává mnoho neřešených problémů. Do teorie čísel patří například otázky dělitelnosti přirozených čísel, prvočísla a podobně. Podle metod, jichž se používá, mluvíme o algebraické teorii čísel a analytické teorii čísel.

Algebra se uplatňuje i v ostatních matematických oborech; máme například algebraickou geometrii a algebraickou topologii.

ZÁKLADNÍ VĚTA ALGEBRY

Víte, že pomocí komplexních čísel lze vyjádřit odmocniny ze záporných čísel, o nichž bychom jinak museli tvrdit, že neexistují. Víte, že pomocí nich lze řešit každou kvadratickou rovnici. To však není vše; platí takzvaná základní věta algebry (neboli fundamentální věta algebry), která říká, že každá algebraická rovnice má v oboru komplexních čísel alespoň jeden kořen. Algebraickou rovnicí nazýváme rovnici, kterou lze ekvivalentními úpravami upravit na tvar

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

kde $a_0, a_1, \ldots, a_n$ jsou nějaká komplexní čísla; samozřejmě alespoň jedno z čísel $a_0, a_1, \ldots, a_{n-1}$ musí být různé od nuly; jinak by se v rovnici vůbec nevyskytovala neznámá. Tato věta nebyla dokázána algebraickými prostředky, ale prostředky matematické analýzy. Lze z ní pak odvodit, že každá algebraická rovnice stupně n má právě n kořenů, pokud se ovšem každý kořen bere s příslušnou násobností — tedy například dvojnásobný kořen se počítá jako dva kořeny (násobnost kořenů zde definovat nebudeme). Jsou-li $x_1, x_2, \ldots, x_n$ kořeny rovnice

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

pak pro každé číslo x platí

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n =$$
$$= a_0(x - x_1)(x - x_2) \ldots (x - x_n).$$

Každý mnohočlen stupně alespoň prvního lze tedy vyjádřit jako součin lineárních mnohočlenů.

UHODNUTÍ KOŘENE ROVNICE

Umíme-li řešit kvadratickou rovnici, rozřešíme i rovnici vyššího stupně, pokud se nám podaří uhodnout některé kořeny.

Mějme rovnici

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0.$$

Nechť její kořeny jsou $x_1, x_2, \ldots, x_n$. Z předešlého odstavce víme, že platí

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n =$$
$$= a_0(x - x_1)(x - x_2) \ldots (x - x_n).$$

Představme si, že jeden kořen (nechť je to x_1) nějakým způsobem uhodneme. Potom tedy můžeme mnohočlen

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

dělit mnohočlenem $x - x_1$; dostaneme nějaký mnohočlen

$$b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}$$

stupně $n - 1$. Kořeny rovnice

$$b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1} = 0$$

jsou zbývající kořeny původní rovnice.

Uveďme si to na příkladě. Mějme kubickou rovnici

$$x^3 - 9x^2 + 23x - 15 = 0.$$

Napadne nás, že jedním kořenem této rovnice by mohlo být číslo 1. Dosadíme tedy $x = 1$, a ejhle — ono to skutečně vychází. Nyní tedy mnohočlen $x^3 - 9x^2 + 23x - 15$ dělíme mnohočlenem $x - 1$; dostáváme

$$(x^3 - 9x^2 + 23x - 15) : (x - 1) = x^2 - 8x + 15.$$

Řešíme rovnici

$$x^2 - 8x + 15 = 0.$$

Dostáváme kořeny 3 a 5. Tedy původní rovnice má kořeny 1, 3 a 5.

ABSTRAKTNÍ ALGEBRA

Jak už jsme se zmínili v úvodu, algebra se zabývá určitými operacemi (úkony), které se provádějí s matematickými objekty. Abstraktní algebra se přitom nezabývá tím, jakého druhu jsou tyto objekty; říkáme, že od toho abstrahuje.

Nejčastěji se setkáváme s operacemi, které se provádějí se dvěma objekty; říkáme jim binární operace. Je to například známé sčítání, odčítání, násobení a dělení čísel; může to být také sčítání úseček nebo úhlů nebo skládání funkcí (například složením funkcí $y = \log x$, $y = \sin x$ vznikne funkce $y = \log \sin x$, popřípadě $y = \sin \log x$). Můžeme tedy zkoumat množinu nějakých objektů takových, že s každými dvěma z nich lze provést určitou binární operaci a výsledek této operace je opět obsažen v této množině. Takovéto množině budeme říkat grupoid.

Například množina všech přirozených čísel je grupoidem vzhledem ke sčítání; každá dvě přirozená čísla lze sečíst a součet je opět přirozené číslo. Podobně je množina všech přirozených čísel grupoidem vzhledem k násobení, ale nikoliv vzhledem k odčítání a dělení; odčítáme-li nebo dělíme-li dvě přirozená čísla, nemusíme vždy dostat přirozené číslo.

Víme, že pro sčítání a násobení čísel (nikoliv pro odčítání a dělení) platí asociativní zákon

$$(a + b) + c = a + (b + c),$$
$$(ab)\, c = a(bc).$$

Tento zákon platí také pro sčítání úseček a úhlů, pro skládání funkcí a pro řadu dalších binárních operací. Máme-li tedy grupoid, jehož operace splňuje asociativní zákon (říkáme, že to je operace asociativní), tento grupoid se nazývá pologrupa. Množina všech celých čísel je tedy pologrupou vzhledem ke sčítání a násobení, vzhledem k odčítání je pouze grupoidem, nikoliv pologrupou.

U některých operací se stává, že existuje objekt té vlastnosti, že výsledek binární operace provedené s tímto prvkem a libovolným druhým prvkem je opět roven onomu druhému prvku. Tak pro číslo 0 platí

$$a + 0 = a$$

pro každé a. Pro číslo 1 opět platí

$$a\,.\,1 = a.$$

Pro funkci $y = x$ platí, že složíme-li ji s libovolnou funkcí $y = f(x)$, dostaneme opět funkci $y = f(x)$. Takovýto prvek nazýváme jednotkovým prvkem vzhledem k příslušné operaci. Pologrupa, která obsahuje jednotkový prvek vzhledem k příslušné operaci, se nazývá monoid. Tedy například množina všech nezáporných celých čísel je monoidem vzhledem ke sčítání — jednotkovým prvkem je zde 0. Množina všech přirozených čísel je monoidem vzhledem k násobení (jednotkovým prvkem je zde 1), ale nikoliv vzhledem ke sčítání.

Víme dále, že ke každému číslu a existuje jeho opačná hodnota $-a$; sečtením čísel a a $-a$ dostaneme 0. Podobně ke každému nenulovému číslu a existuje jeho převrácená hodnota $\frac{1}{a}$; vynásobením čísel a a $\frac{1}{a}$ dostaneme 1. Jestliže tedy máme monoid s tou vlastností, že ke každému prvku tohoto monoidu existuje právě jeden prvek takový, že výsledkem příslušné operace provedené s těmito prvky je jednotkový prvek monoidu, tento monoid se nazývá grupou. Tedy množina všech celých čísel je grupou vzhledem ke sčítání, ale vzhledem k násobení je pouze monoidem; opačná hodnota $-a$ celého čísla a je vždy celým číslem, převrácená hodnota $\frac{1}{a}$ nikoliv. Množina všech nenulových reálných čísel je grupou vzhledem k násobení, množina všech reálných čísel nikoliv (neexistuje převrácená hodnota čísla 0).

Příkladem grupy, která má konečný počet prvků, je grupa složená z komplexních čísel $1, -1, i, -i$ s operací násobení. Příkladem konečné grupy, jejíž prvky nejsou čísla, je grupa permutací, to jest vzájemně jednoznačných zobrazení nějaké konečné množiny M opět na množinu M; o ní si ještě něco povíme dále.

Jak už jsme uváděli, v abstraktní algebře se nestaráme o to, jakého druhu jsou objekty, s nimiž pracujeme. Říkáme jim prostě prvky; mluvíme o prvcích grupoidu, pologrupy, monoidu, grupy. Zkoumají se pouze vlastnosti souvisící přímo s příslušnou operací. Tak například u konečné grupy se mluví o řádu prvku (někdy se o něm mluví i u grupy nekonečné). Každý prvek konečné grupy má tu vlastnost, že pro nějaké přirozené číslo n jeho n-tá mocnina je rovna jednotkovému prvku. (Operaci v grupě zpravidla nazýváme násobením, i když nemusí jít vždy o násobení čísel. Umocňování se odvozuje z tohoto násobení podobně jako u násobení čísel.) Nejmenší takové n se nazývá řádem příslušného prvku. Dokazuje se věta, že řád každého prvku konečné grupy je dělitelem řádu grupy, to jest počtu všech prvků grupy. (Přesvědčte se o tom sami u grupy složené z čísel 1, —1, i, —i.) Takováto věta platí pro každou konečnou grupu, ať jsou její prvky jakékoliv matematické objekty.

Pro ilustraci si nyní uvedeme grupu všech permutací tříprvkové množiny $M = \{1, 2, 3\}$; zpravidla se označuje S_3. Každou permutaci množiny M můžeme zapsat tak, že do jednoho řádku napíšeme čísla 1, 2, 3 v obvyklém pořadí, v druhém řádku pak pod každé číslo napíšeme jeho obraz v příslušné permutaci; celek dáme do závorek. Jak víme, počet permutací tříprvkové množiny je $3! = 6$. Budou to tyto permutace:

$$p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Na množině těchto permutací budeme nyní zkoumat operaci skládání zobrazení. Jsou-li q_1, q_2 dvě z našich permutací, pak q_1q_2 bude značit permutaci, která každému prvku x množiny M přiřazuje prvek $q_1(q_2(x))$, to jest obraz prvku $q_2(x)$ v zobrazení q_1. Máme-li najít permutaci p_1p_2, pak si opět napíšeme čísla 1, 2, 3 v obvyklém pořadí a pod ně příslušné obrazy. Obrazem prvku 1 v zobrazení p_2 je prvek 2, obrazem prvku 2 v zobrazení p_1 je prvek 3; tedy obrazem prvku 1 v zobrazení p_1p_2 je prvek 3. Podobně najdeme obrazy prvků 2 a 3 a máme

$$p_1p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_4.$$

Dostali jsme opět prvek naší množiny permutací. Můžeme si takto nalézt složené zobrazení pro libovolnou dvojici permutací a sestavit si tabulku, která se nazývá Cayleyova tabulka. Každý řádek i každý sloupec tabulky odpovídá jedné permutaci (obecně jednomu prvku grupy nebo grupoidu). Permutace uvedená v řádku odpovídajícím permutaci q_1 a ve sloupci odpovídajícím permutaci q_2 je permutace q_1q_2. Tabulka vypadá takto:

	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_0	p_4	p_5	p_2	p_3
p_2	p_2	p_3	p_0	p_1	p_5	p_4
p_3	p_3	p_2	p_5	p_4	p_0	p_1
p_4	p_4	p_5	p_1	p_0	p_3	p_2
p_5	p_5	p_4	p_3	p_2	p_1	p_0

Místo o permutacích budeme nyní mluvit o prvcích grupy, místo o skládání permutací budeme mluvit o grupovém násobení. Vidíme, že násobením libovolných dvou prvků naší množiny dostaneme opět prvek této množiny. O platnosti asociativního zákona se můžete přesvědčit sami. Prvek p_0 má tu vlastnost, že pro libovolné $q \in S_3$ je

$$p_0 q = q p_0 = p_0,$$

je tedy jednotkovým prvkem. Ke každému $q \in S_3$ existuje prvek $q^{-1} \in S_3$ (inverzní prvek k prvku q) takový, že

$$q q^{-1} = q^{-1} q = p_0.$$

Máme $p_0^{-1} = p_0$, $p_1^{-1} = p_1$, $p_2^{-1} = p_2$, $p_3^{-1} = p_4$, $p_4^{-1} = p_3$, $p_5^{-1} = p_5$. Jde tedy skutečně o grupu.

Všimněme si, že pro každé $q \in S_3$ je $(q^{-1})^{-1} = q$. To platí v každé grupě.

Řád grupy S_3 je 6, jak už jsme uvedli výše. Prvky p_0, p_1, p_2, p_5 mají řád 2, neboť $p_0^2 = p_1^2 = p_2^2 = p_5^2 = p_0$ a pro přirozený exponent menší než 2 to neplatí. Prvek p_3 má řád 3, neboť $p_3^3 = p_0$, ale $p_3^2 = p_4$. Rovněž prvek p_4 má řád 3. Čísla 2 a 3 jsou ovšem děliteli čísla 6, což je řád grupy.

Vezmeme-li podmnožinu $\{p_0, p_3, p_4\}$, vidíme, že součin libovolných dvou prvků z této podmnožiny i inverzní prvek k libovolnému jejímu prvku je opět prvkem této podmnožiny a že tato podmnožina obsahuje jednotkový prvek p_0. Říkáme, že tato podmnožina je podgrupou naší grupy.

Všimněme si ještě, že v každém řádku Cayleyovy tabulky a rovněž v každém jejím sloupci se každý prvek grupy vyskytuje právě jednou. Pro libovolnou grupu totiž platí, že pro libovolné prvky a, b, c této grupy z rovnosti $ab = ac$ nebo z rovnosti $ba = ca$ plyne $b = c$.

Obecně v pologrupě toto platit nemusí. Narazíme na to v kapitole V při výkladu o latinských čtvercích.

Ještě se zmíníme o tom, že v naší grupě například $p_1p_2 \neq p_2p_1$, tedy neplatí komutativní zákon jako při násobení čísel. Grupa, v níž komutativní zákon platí, se nazývá Abelova.

Takovýmto způsobem zkoumá abstraktní algebra i jiné druhy operací. Množina s nějakou operací, popřípadě i s více operacemi, se nazývá algebrou. Tedy každý grupoid, pologrupa, monoid a grupa je algebrou. Jsou další typy algeber se speciálními názvy — okruhy, tělesa, svazy, polosvazy, kvazigrupy a podobně. Operace nemusejí být vždy binární, mohou se provádět i s jiným počtem prvků než se dvěma. Příkladem ternární operace, to jest operace prováděné s třemi prvky, je operace, která třem bodům neležícím v přímce přiřazuje těžiště příslušného trojúhelníka.

Mluvili jsme zde o operacích a mysleli jsme tím nějaké matematické úkony. Doufám, že toto slovo ve vás nevyvolává nepříjemné asociace se skalpelem a pachem chloroformu. Výraz operace má širší význam než jen chirurgický; značí prostě nějakou speciální činnost (jistě jste se setkali například s pojmem vojenské operace).

ČÍSELNÉ SOUSTAVY

Napíšeme-li číslo 1978, znamená to, že jde o číslo rovné

$$1.10^3 + 9.10^2 + 7.10^1 + 8.10^0.$$

Říkáme, že jsme toto číslo zapsali v desítkové (dekadické) soustavě. Místo čísla 10 bychom však mohli užít i jiného přirozeného čísla. Samočinné počítače počítají v soustavě dvojkové (dyadické). Zatímco desítková soustava užívá číslic 0, 1, 2, 3, 4, 5, 6, 7, 8 a 9, užívá dvojková soustava pouze číslic 0 a 1. Je to pro počítač výhodné, protože tyto číslice lze snadno vyjádřit tak, že 0 odpovídá stavu, kdy určitým obvodem neprotéká proud, a 1 odpovídá stavu, kdy proud protéká.

Jak bychom zapsali číslo 1978 ve dvojkové soustavě? Popíšeme si postup. Dělíme číslo dvěma a zbytek při tomto dělení zapíšeme jako poslední číslici dvojkového vyjádření. V našem případě 1978 : 2 = 989, zbytek je 0. Totéž provedeme s podílem — tedy 989 : 2 = 494, zbytek je 1, zapíšeme jej jako předposlední číslici. Dále 494 : 2 = 247, zbytek 0; 247 : 2 = 123, zbytek 1; 123 : 2 = 61, zbytek 1; 61 : 2 = 30, zbytek 1; 30 : 2 = = 15, zbytek 0; 15 : 2 = 7, zbytek 1; 7 : 2 = 3, zbytek 1; 3 : 2 = 1, zbytek 1; 1 : 2 = 0, zbytek 1. (Na to poslední dělení nesmíme zapomenout!) Zápis čísla 1978 ve dvojkové soustavě je tedy

$$11110111010.$$

Znamená to, že

$$1978 = 1.2^{10} + 1.2^9 + 1.2^8 + 1.2^7 + 0.2^6 + \\ + 1.2^5 + 1.2^4 + 1.2^3 + 0.2^2 + 1.2^1 + 0.2^0.$$

Můžete si to sami zkontrolovat.

Jak jsme uváděli, dvojková soustava má význam především pro samočinný počítač. Pro člověka má tu nevýhodu, že zápisy čísel v této soustavě jsou příliš dlouhé a nepřehledné. Představme si, že bychom měli použít většího množství čísel zapsaných ve dvojkové soustavě. Máme si zapsat jejich sáhodlouhá vyjádření v této soustavě nebo je mít zapsána v soustavě desítkové a až v případě potřeby je převádět do dvojkové? Obojí má jistě své nevýhody. Proto raději používáme ještě jiné soustavy, a to osmičkové (oktadické).

Číslo 8 je třetí mocnina čísla 2. Z tohoto faktu plyne snadný způsob převádění zápisu čísel z dvojkové soustavy do osmičkové a obráceně. Napišme si nejprve zápisy čísel 0, 1, 2, 3, 4, 5, 6 a 7 (to jest čísel, jimž odpovídají jednotlivé číslice osmičkové soustavy) ve dvojkové soustavě; pokud mají méně cifer než tři, píšeme před ně příslušný počet nul.

Číslo	Dvojkový zápis
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Vezměme si nyní náš zápis čísla 1978 ve dvojkové soustavě. Zapišme jej tak, že vždy po každé třetí číslici, počínaje od konce, uděláme mezeru:

11 110 111 010.

Takto máme zápis rozdělen na trojice cifer (dvojici 11 na začátku můžeme považovat za trojici 011). Ke každé z nich najdeme číslo, které tato trojice vyjadřuje ve dvojkové soustavě. Vidíme, že jde o zápisy čísel 3, 6, 7, 2 a tedy zápis čísla 1978 v osmičkové soustavě je 3672. Pro kontrolu si můžete ještě provést přímo převod čísla 1978 z desítkové soustavy do osmičkové podobným způsobem, jakým jsme převáděli do soustavy dvojkové (místo dvěma dělíme ovšem osmi); uvidíte, že dostanete tentýž výsledek. Při převodu z osmičkové soustavy do dvojkové postupujeme zase tak, že jednotlivé cifry nahradíme jejich dvojkovým vyjádřením (pokud je méně než trojmístné, napíšeme před ně příslušný počet nul). Zápis čísel v osmičkové soustavě nebývá nikdy o mnoho delší než zápis v desítkové soustavě, přitom má tu výhodu, že jej lze poměrně snadno (jak jsme viděli) převést na zápis dvojkový; z desítkové soustavy to tak jednoduché není, protože číslo 10 není mocninou dvou.

Řekněme si nyní, proč vlastně používáme desítkové soustavy. Důvod je pouze ten, že máme na obou rukou dohromady deset prstů. Stejný počet prstů měli i naši dávní předkové, jejichž jedinou výpočetní technikou byly právě tyto prsty. Na základě toho se vytvořily příslušné názvy čísel a později jejich zápisy, takže dnes bychom si už asi těžko zvykali na jinou soustavu než desítkovou. Jiný důvod než tento skutečně není; z matematického hlediska číslo 10 jakožto základ číselné soustavy je nevýhodné. Je totiž dělitelné (kromě jedničky a sama sebe) jen čísly 2 a 5. Častěji však v životě potřebujeme něco dělit na třetiny nebo čtvrtiny než na pětiny. Proto by pro nás byla výhodnější soustava dvanáctková; číslo 12 je dělitelno čísly 2, 3, 4 a 6. V této soustavě ovšem je třeba mít samostatnou číslici i pro čísla 10 a 11; užívá se k tomu účelu zpravidla písmen T a E, což jsou začáteční písmena odpovídajících anglických číslovek „ten“ a „eleven“. Číslo 1978 by se v této soustavě zapsalo jako 118T, což je

$$1.12^3 + 1.12^2 + 8.12^1 + 10.12^0.$$

V desítkové soustavě máme míry, váhy, další fyzikální jednotky i měnovou soustavu. Metr má deset decimetrů, decimetr deset centimetrů, centimetr deset milimetrů. Podobně je tomu u vah. Československá koruna se dělí na sto, to jest 10^2, haléřů.

Představme si, že by se tři kusy nějakého zboží prodávaly za korunu. Kolik vlastně potom stojí jeden kus? Třiatřicet a dvě třetiny haléře? Zde vidíme nevýhodu desítkové soustavy. Nejde ovšem jen o naše koruny a haléře; v převážné většině států je základní měnová jednotka rozdělena na sto menších jednotek.

Výjimku tvořila donedávna britská měnová soustava. Základní jednotkou byla libra šterlinků. Ta se dělila na dvacet šilinků a šilink opět na dvanáct pencí. (V češtině se mluví o pencích a čte se to tak, jak se to píše. V angličtině „pence", čteno „pens", je množné číslo slova „penny", což je označení oné nejmenší britské měnové jednotky. Je tedy jeden penny, ale dvě pence, tři pence, pět pencí.) Dříve ani jeden penny nebyl nejmenší měnovou jednotkou, ale dělil se ještě na čtrnáct farthingů.

Mnohému tato soustava připadá těžkopádná. Je to však proto, že jsme zvyklí na naše koruny a haléře. Po matematické stránce byla britská měnová soustava výhodná. Polovina libry byla deset šilinků, třetina šest šilinků a osm pencí, čtvrtina pět šilinků, pětina čtyři šilinky, šestina tři šilinky a čtyři pence, osmina dva šilinky a šest pencí. Vidíme, že libru bylo možno dělit všemi přirozenými čísly od jedné do osmi kromě sedmi. Dokud však existovaly farthingy, bylo možno vyjádřit i sedminu libry; byly to dva šilinky, deset pencí a čtyři farthingy. Dále bylo možno libru dělit deseti, dvanácti, patnácti, dvaceti, čtyřiadvaceti, třiceti, čtyřiceti a šedesáti.

Dokud nebyl příliš rozvinut mezinárodní obchod, nebylo důvodu tuto soustavu měnit. Nyní však by dělal potíže její přepočet na měny jiných států, proto byla i ve Velké Británii přijata desítková měnová soustava. Jedna libra šterlinků se dnes dělí na sto pencí. Podobnou soustavu jako Británie mívala kdysi i Francie; dodnes ji připomíná výraz „sou", který (neoficiálně) označuje částku pěti centimů. Původně to byla dvacetina franku, analogie britského šilinku.

Přestože, jak jsme uvedli, užíváme desetinné soustavy u měr, vah i měny, neužíváme jí pro měření velikostí úhlů a času. Byla navržena reforma měření úhlů, při níž by se stal jednotkou jeden grad, což by byla setina velikosti pravého úhlu; tato jednotka by se dělila na decigrady, centigrady a miligrady. Tato soustava se neujala; právě úhly potřebujeme dělit na různé počty stejných částí a víme z geometrie, že obzvláštní význam mají úhly o velikostech 30° a 60°. Těžko bychom asi říkali, že každý vnitřní úhel rovnostranného trojúhelníka má velikost 66 gradů, 6 decigradů, 6 centigradů a šest a dvě třetiny miligradu. Stejně těžko bychom si asi zvykali na to, kdybychom místo hodin, minut a sekund měli nějaké decidny, centidny a milidny. Naše obvyklé měření času a úhlů pochází už od starých Babylóňanů, kteří si už tehdy uvědomovali jeho výhodnost.

Pro zajímavost ještě uveďme, že staří Mayové užívali soustavy dvacítkové (asi proto, že dvacet je celkový počet prstů na rukou a nohou) a jistý primitivní kmen na Nové Guineji prý užívá soustavy jedenáctkové (důvod je záhadný, protože 11 je prvočíslo, tudíž je mimořádně nevýhodné jako základ číselné soustavy).

Co je to prvočíslo, jistě víte. Je to takové přirozené číslo, které má pouze dva dělitele, a to sebe samo a číslo 1. Číslo 1 mezi prvočísla nepatří. (Někdy se i opačné hodnoty prvočísel považují za prvočísla, ale tím se zde zabývat nebudeme.)

Prvočísel je nekonečně mnoho. Důkaz tohoto tvrzení je zajímavým příkladem nepřímého důkazu neboli důkazu sporem. Předpokládejme, že toto tvrzení neplatí a že tedy existuje jen konečný počet prvočísel; nechť tento počet je n a tato prvočísla jsou $p_1, p_2, \ldots, p_n$. Součin všech těchto prvočísel označme P. Číslo $P + 1$ není dělitelné žádným z prvočísel $p_1, p_2, \ldots, p_n$; kdyby bylo dělitelné některým z nich, musel by být i rozdíl čísel $P + 1$ a P, tedy číslo 1, dělitelný tímto prvočíslem, což zřejmě není možné, protože číslo 1 je dělitelné jen sebou samým. Každé přirozené číslo větší než 1 je však dělitelno alespoň jedním prvočíslem, tedy $P + 1$ musí být dělitelno nějakým prvočíslem různým od čísel p_1, $p_2, \ldots, p_n$. To však je spor, protože jsme předpokládali, že žádné takovéto prvočíslo neexistuje. Tedy náš předpoklad byl nesprávný a prvočísel je nekonečně mnoho.

K vyhledání všech prvočísel menších než dané přirozené číslo n se užívá metody zvané Eratosthenovo síto. Napišme si všechna přirozená čísla od 2 do n (o čísle 1 víme, že není prvočíslem). Nyní škrtáme všechna čísla dělitelná dvěma kromě čísla 2, pak všechna čísla dělitelná třemi kromě čísla 3 a dále vždy čísla dělitelná dalším z dosud neškrtnutých čísel kromě toho čísla samého. Tak postupujeme tak dlouho, až dojdeme k prvnímu číslu většímu než $\sqrt{n}$; pak postup končí. Ze všech napsaných čísel nám zbudou jen prvočísla. U prvního čísla většího než $\sqrt{n}$ jsme se zastavili, protože dále bychom nedostali nic nového; je-li nějaké číslo menší nebo rovné n dělitelno číslem větším než $\sqrt{n}$ a různým od n, pak je dělitelno i nějakým číslem menším než $\sqrt{n}$ a různým od jedné. Zkuste si to sami pro čísla od dvou do sta.

Nějaký vzorec, který by nám udával n-tý člen posloupnosti všech prvočísel v závislosti na n, není znám. Proto je velmi obtížné u vysokých čísel určovat, zda jsou to prvočísla či nikoliv. Největší dosud známé prvočíslo našel Tuckerman pomocí samočinného počítače. Je to číslo $2^{19937} - 1$; má 6002 cifry.

V teorii čísel se užívá funkce $\pi(x)$ definované pro kladná x, která označuje počet prvočísel nepřevyšujících číslo x. (S Ludolfovým číslem nemá nic společného.) P. L. Čebyšev (1821—1894) dokázal, že pro každé kladné x platí nerovnost

$$0{,}89 . \frac{x}{\ln x} < \pi(x) < 1{,}11 . \frac{x}{\ln x} .$$

Výraz $\ln x$ značí přirozený logaritmus čísla x (viz III. kapitola). Od té doby byly nalezeny přesnější (ovšem složitější) nerovnosti.

Je-li nějaké celé číslo n dělitelné prvočíslem p a jsou-li a, b celá čísla taková, že $ab = n$, pak buď a, nebo b je dělitelné číslem p. Pokud však zavedeme takzvaná celá komplexní čísla, což jsou komplexní čísla, jejichž reálné i imaginární části jsou celá čísla, pak v oboru těchto čísel toto tvrzení neplatí. Číslo 10 lze vyjádřit jako součin $(1 + 3i)(1 - 3i)$, přitom však žádné z čísel $1 + 3i$, $1 - 3i$ není dělitelné dvěma ani pěti (při příslušném dělení nedostaneme celé komplexní číslo).

Prvočíselnými dvojčaty nazýváme takové dvojice prvočísel, jejichž rozdíl je roven dvěma. Prvočíselnými dvojčaty jsou například dvojice $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$. Dosud se neví, zda těchto dvojic je konečně nebo nekonečně mnoho.

Kdybychom obdobně definovali prvočíselná trojčata, zjistili bychom, že neexistují jiná než $\{3, 5, 7\}$. Pro libovolné celé číslo n totiž právě jedno z čísel n, $n + 2$, $n + 4$ je dělitelno třemi. Jestliže n není dělitelno třemi, pak buď $n = 3k + 1$, nebo $n = 3k + 2$, kde k je celé číslo. V prvním případě $n + 2 = 3(k + 1)$ a je tedy dělitelno třemi. V druhém případě $n + 4 = 3(k + 2)$ a je dělitelno třemi. Jediné prvočíslo dělitelné třemi je ovšem číslo 3 a tedy nemáme jinou možnost než právě $\{3, 5, 7\}$. Z toho už je také patrné, že prvočíselná čtyřčata nemohou vůbec existovat.

M. Mersenne (1588—1648) zkoumal prvočísla, která lze vyjádřit ve tvaru $2^s - 1$, kde s je přirozené číslo; tato prvočísla se podle něho nazývají Mersennova prvočísla. Číslo $2^s - 1$ může být prvočíslem jen tehdy, je-li s prvočíslem, ale obrácené tvrzení neplatí; číslo 11 je prvočíslo, ale číslo $2^{11} - 1 = 2047 = 23 . 89$. Mersennových prvočísel je známo dosud jen 24, jsou to čísla $2^s - 1$, kde s nabývá hodnot 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937.

DOKONALÁ A SPŘÁTELENÁ ČÍSLA

Ve starověku do matematiky pronikaly různé mystické představy. Bylo tomu tak zejména u Pythagora a jeho žáků. Číslům se připisovaly různé vlastnosti, které s vlastní matematikou neměly nic společného. Tak vznikl i pojem dokonalého čísla. Je to pojem zajímavý, i když z hlediska dnešní matematiky nejde vlastně o žádnou dokonalost.

Vlastním dělitelem přirozeného čísla n se nazývá každý jeho dělitel různý od n. Dokonalým prvočíslem prvního druhu nazýváme číslo, které je součtem všech svých vlastních dělitelů. Číslo, které je součinem všech svých vlastních dělitelů, se nazývá dokonalým číslem druhého druhu.

Číslo 6 je dokonalým číslem prvního i druhého druhu; jeho vlastními děliteli jsou čísla 1, 2, 3 a platí $1 + 2 + 3 = 1.2.3 = 6$.

Veškerá dokonalá čísla prvního druhu, která jsou známa, jsou sudá. Je dokázáno, že sudé číslo n je dokonalým číslem prvního druhu právě tehdy, je-li možno je vyjádřit ve tvaru $n = 2^{s-1}(2^s - 1)$, kde s je přirozené číslo, $s > 1$ a $2^s - 1$ je prvočíslo. Tím se nám zkoumání těchto čísel převádí na zkoumání Mersennových prvočísel, o nichž jsme se zmiňovali v předešlém odstavci. Víme, že Mersennových prvočísel zatím mnoho neznáme, neznáme tedy ani mnoho dokonalých čísel prvního druhu. Největší známé je $2^{19936}(2^{19937} - 1)$.

Liché dokonalé číslo prvního druhu neznáme ani jedno. Víme jen, jaký tvar tato čísla musejí mít, pokud existují. L. Euler (1707—1783) dokázal, že každé takovéto číslo musí mít tvar $p^{4k+1}N^2$, kde k je celé nezáporné číslo, p je prvočíslo tvaru $4s + 1$ (kde s je přirozené číslo) a N není dělitelné číslem p. Dále víme, že tato čísla musejí mít tvar $12k + 1$ nebo $36k + 9$, kde k je přirozené číslo. Je rovněž zjištěno, že žádná lichá čísla menší než 10^{20} nejsou dokonalými čísly prvního druhu. Nevíme ani, zda dokonalých čísel prvního druhu je konečný, nebo nekonečný počet.

Zato dokonalá čísla druhého druhu dovedeme přesně charakterizovat. Víme, že přirozené číslo různé od jedné je dokonalým číslem druhého druhu právě tehdy, je-li buď součinem dvou různých prvočísel, nebo třetí mocninou prvočísla. Důkaz je poměrně jednoduchý. Je-li číslo součinem dvou různých prvočísel p a q, pak všichni jeho vlastní dělitelé jsou čísla 1, p, q a jejich součin dává ono číslo. Je-li číslo rovno p^3, kde p je prvočíslo, pak všichni jeho vlastní dělitelé jsou 1, p, p^2 a jejich součin je p^3. Nenastává-li pro číslo $n > 1$ žádný z těchto případů, pak buď n je prvočíslem a jediný jeho vlastní dělitel je 1, nebo je $n = p^2$, kde p je prvočíslo (pak všichni vlastní dělitelé čísla n jsou 1 a p), nebo $n = pqr$, kde p a q jsou prvočísla a r přirozené číslo různé od p a větší než 1. Pak čísla p, r, pr jsou vlastními děliteli čísla n. Pokud by n bylo dokonalé číslo druhého druhu, muselo by být dělitelno jejich součinem p^2r^2, tedy $n = p^2r^2s$, kde s je přirozené číslo. Potom by však bylo $q = prs$, což není možné, protože q je prvočíslo.

S pojmem dokonalého čísla souvisí pojem spřátelených čísel. Spřátelenými čísly nazýváme dvojici přirozených čísel $\{a, b\}$, která má tu vlastnost, že $a \neq b$, součet všech vlastních dělitelů čísla a je roven číslu b a součet všech vlastních dělitelů čísla b je roven číslu a.

Neví se dodnes, zda dvojic spřátelených čísel je konečný, nebo nekonečný počet. Nejmenší dvě čísla, která jsou spřátelená, jsou 220 a 284. Vlastními děliteli čísla 220 jsou čísla 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110; jejich součet je 284. Vlastními děliteli čísla 284 jsou čísla 1, 2, 4, 71, 142; jejich součet je 220.

Arabský matematik Thâbit ben Korrah (IX. století) dokázal, že jsou-li čísla $p = 3 . 2^{n-1} - 1$, $q = 3 . 2^n - 1$, $r = 9 . 2^{2n-1} - 1$ prvočísly (kde n je přirozené číslo větší než jedna), pak 2^npq a 2^nr jsou spřátelená čísla. Dosud není známa dvojice spřátelených čísel, z nichž by jedno bylo sudé a druhé liché, ani dvojice nesoudělných spřátelených čísel.

PYTHAGOREJSKÁ ČÍSLA

Z geometrie známe Pythagorovu větu. S ní souvisí pojem pythagorejské trojice čísel, což je trojice nesoudělných přirozených čísel $[x, y, z]$, pro něž platí $x^2 + y^2 = z^2$, to jest existuje pravoúhlý trojúhelník o odvěsnách délek x a y a o přeponě délky z. Nejznámější takovouto trojicí je [3, 4, 5].

Pythagorejské trojice lze získat tím způsobem, že zvolíme dvě nesoudělná přirozená čísla u a v, z nichž jedno je sudé a druhé liché, a položíme $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$. Skutečně vidíme, že

$$\begin{aligned} x^2 + y^2 = (u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + \\ + v^4 + 4u^2v^2 = u^4 + 2u^2v^2 + v^4 = \\ = (u^2 + v^2)^2 = z^2. \end{aligned}$$

Lze dokázat, že každou pythagorejskou trojici čísel lze získat tímto způsobem. Zkuste si sami některé takovéto trojice najít.

VELKÁ FERMATOVA VĚTA

Viděli jsme, že existuje nekonečně mnoho pythagorejských trojic čísel. Jak to však vypadá, když místo druhých mocnin bereme nějaké vyšší mocniny?

Pierre de Fermat (1601—1665) zanechal ve své pozůstalosti jistou Diofantovu knihu, do níž si na okraje stránek zapisoval své poznámky. Na jednom místě poznamenává, že pro žádná přirozená čísla x, y, z a n, kde $n \geqq 3$, neplatí rovnost

$$x^n + y^n = z^n.$$

Důkaz tohoto tvrzení se nezachoval a dodnes jej nikdo jiný nenalezl. Vyslovují se pochybnosti o tom, zda Fermat vůbec nějaký důkaz tohoto tvrzení objevil; měl přece k dispozici mnohem méně matematických poznatků a metod než dnešní matematikové.

Nicméně se toto tvrzení nazývá velkou Fermatovou větou (na rozdíl od jiné Fermatovy věty, které se říká „malá" a která dokázána je). Správně by se mělo mluvit o Fermatově hypotéze neboli domněnce. Důkaz není znám a není znám ani žádný příklad, který by tuto hypotézu vyvracel.

Jak je vidět, i taková prostá věc jako přirozená čísla skrývá ještě mnohá tajemství.

Úlohy

1. Starořecký matematik Diofantos z Alexandrie (o němž jsme se zmiňovali v úvodu této kapitoly) si dal na svůj náhrobek vytesat tento epitaf:

„Poutníče! Zde odpočívá smrtelná schránka Diofanta. Čísla, jaký div, mohou vyprávět, jak dlouho žil. Šestina jeho života bylo bezstarostné dětství. Dvanáctina uplynula, když se jeho brada pokryla chmýřím. Sedminu pak prožil v bezdětném manželství. Pak uplynulo ještě pět let, než byl obšťastněn prvním synem. Tomu však krutý osud dopřál jen polovinu života jako jeho otci. V hlubokém smutku prožil pak ctihodný stařec konec svých pozemských dnů, když svého syna o čtyři roky přežil. Řekni, poutníče, jak stár byl Diofantos, když smrt ho odvedla k předkům?"

Jistě i vy zodpovíte tuto otázku.

2. Hlemýžď leze na zeď vysokou deset metrů. Během dne povyleze o tři metry, v noci spí a sklouzne při tom o dva metry. Za jak dlouho vyleze na zeď?

3. Místa A a B jsou od sebe vzdálena 180 km. Z místa A vyjede po přímočaré silnici auto směrem k místu B rychlostí 60 km/ /hod. V okamžiku, kdy auto vyjede z místa A, vyletí z místa B moucha rychlostí 120 km/hod a letí autu naproti. Když dolétne k autu, vrátí se opět stejnou rychlostí do místa B, pak letí opět k autu a vše se opakuje tak dlouho, až auto dojede do místa B. Jakou celkovu dráhu vykoná moucha?

4. Máme deset pytlů s mincemi. Víme, že v jednom z nich jsou falešné mince; každá z nich je o desetinu gramu lehčí než pravá. V ostatních pytlích jsou mince pravé. Známe přesnou váhu pravé mince a máme k dispozici dostatečně přesné váhy a závaží. Jak zjistíme pomocí jediného vážení, v kterém pytli jsou falešné mince?

5. Lev sežere ovci za dvě hodiny, vlk za tři hodiny a pes za šest hodin. Za jakou dobu by ji sežrali společně?

6. Na pánvi se opékají topinky. Opečení každé strany krajíce trvá třicet sekund, na pánev se vejdou dvě topinky. Za jakou nejkratší dobu lze opéci tři topinky?

7. Lovci lovili zajíce, divoké králíky a bažanty. Celkem ulovili 142 kusů. Počet zajíců byl šestinásobkem počtu králíků. Celkový počet noh ulovené zvěře byl 452. Kolik bylo které zvěře?

8. Všichni známe slovo knihomol; označujeme tak člověka, který pro samé čtení zapomíná na všechno ostatní. V původním významu však toto slovo značí skutečně jistého mola, jehož housenky žerou papír a působí tak škody na knihách. V knihovně jsou vedle sebe dva díly jisté knihy. První díl (včetně předsádky) má 575 stran, druhý 498 stran. Prokousání jedné stránky trvá housence knihomola jednu minutu, prokousání desky hodinu. Housenka je v prvním dílu knihy mezi přední deskou a předsádkou. Jak dlouho jí trvá, než se prokouše na místo mezi zadní deskou a předsádkou druhého dílu?

9. Koňský potah urazil polovinu cesty bez nákladu rychlostí 12 km/hod, potom byl naložen a další polovinu cesty se pohyboval rychlostí 4 km/hod. Jaká byla jeho průměrná rychlost?

10. Konají se závody v běhu na lyžích. Pokud závodník běží celou trať rychlostí 10 km/hod, přiběhne do cíle ve 13 hodin. Pokud běží rychlostí 15 km/hod, doběhne v 11 hodin. Jakou rychlostí musí běžet, aby doběhl ve 12 hodin?

11. Toto je tak trochu detektivní hádanka. Ředitel továrny každý den jezdí autem z továrny na oběd do své vily. Jeho šofér vyjede z vily, přijede vždy přesně ve 12 hodin před továrnu, ředitel nastoupí a šofér se s ním vrátí do vily. Jednoho

dne však ředitel vyšel již před polednem pěšky k domovu. Přešel přes lesík a poté potkal svého šoféra, který pro něho jel k továrně. Šofér zastavil, ředitel nastoupil do auta a šofér ho odvezl do vily. Přijeli o půl hodiny dříve než v jiné dny. V lesíku se však toho dne udála vražda, a to, jak bylo přesně zjištěno, v 11.40. Měl ředitel alibi?

12. Pan A, který je matematik, potká na ulici svého známého, pana B. Pan B mu sděluje, že právě jde kupovat dárky pro své tři syny, kteří shodou okolností mají všichni v tentýž den narozeniny. Ptá se pana A, zda by dokázal určit jejich věk, ví-li, že součin jejich věků je 36. „To mi ovšem nestačí," odpovídá pan A. Pan B tedy dodává: „Součet jejich věků je roven počtu oken na přední stěně domu, který stojí před námi." Pan A se chvíli zamyslí a posléze řekne: „Ani to mi nestačí." Pan B tedy ještě dodá: „Můj nejstarší syn nosí brýle, které mají na levém oku 2,5 dioptrie." Nyní už pan A určil věky všech synů pana B. Vaším úkolem je určit je také, i když neznáte onen počet oken.

13. Doktor Watson dal jednou Sherlocku Holmesovi tuto hádanku: „V zahradě si hrají jednak mé děti, jednak děti mého bratra, mé sestry a mého strýce. Nejvíce dětí je mých, nejméně strýcových; bratrových dětí je více než sestřiných. Všech je příliš málo na to, aby mohly utvořit dvě devítičlenné skupiny. Součin počtů dětí jednotlivých rodin je roven číslu mého domu. Kolik je kterých dětí?" Sherlock Holmes se zamyslil a po chvíli odpověděl, že mu tyto údaje nestačí; potřeboval by ještě vědět, kolik je strýcových dětí. Když mu to doktor Watson sdělil, Holmes úlohu vyřešil. Po mnoha letech se s touto úlohou seznámil Holmesův vnuk pan Hopkins. Ten ovšem neznal číslo domu, v němž bydlíval doktor Watson, ani počet dětí jeho strýce. Přesto i on hádanku vyřešil. Dokážete to i vy?

Řešení úloh

1. Věk, kterého se Diofantos dožil, označme x. Potom doba dětství je $\frac{1}{6}x$, doba před prvním chmýřím na bradě $\frac{1}{12}x$ doba bezdětného manželství $\frac{1}{7}x$. Pak následuje pět let, po nich doba života Diofantova syna, což je $\frac{1}{2}x$, nakonec ještě čtyři roky. Dostáváme rovnici

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x.$$

Řešením této rovnice je $x = 84$.

2. Na první pohled se zdá, že stačí uvažovat, že hlemýžď za den a noc urazí délku jednoho metru a tedy na zeď vyleze za deset dní. Nezapomeňme však, že po sedmi dnech a nocích se dostane do výšky sedmi metrů a osmého dne pak vyleze zbývající tři metry a je nahoře!

3. Úloha vypadá složitě; toho, kdo zná nekonečné řady, nejspíše napadne, že by mohl použít těchto řad. Přitom však není vůbec podstatné, kudy moucha létá. Podstatné je, že se pohybuje stálou rychlostí 120 km/hod po celou dobu, kterou potřebuje auto o rychlosti 60 km/hod k tomu, aby dojelo z místa A do místa B. Tato doba jsou tři hodiny a moucha tedy nalétá 360 km.

4. Z prvního pytle vybereme jednu minci, z druhého dvě a tak dále; obecně z n-tého pytle n mincí. Tyto mince zvážíme. Rozdíl váhy 55 pravých mincí a váhy, kterou zjistíme, je roven k desetinám gramu, kde k je pořadové číslo pytle, v němž jsou falešné mince.

5. Sežerou ji za hodinu; lev sežere polovinu, vlk třetinu a pes šestinu.

6. Za devadesát sekund. Prvních třicet sekund opékáme první dvě topinky po jedné straně, potom první topinku otočíme, druhou topinku vyjmeme a položíme místo ní třetí. Dalších třicet sekund tedy opékáme druhou stranu první topinky a první stranu třetí topinky. Potom první topinku (hotovou) vyjmeme a vložíme místo ní druhou. Za posledních třicet sekund pak opečeme obě tyto topinky.

7. Kdyby všechna ulovená zvěř byli bažanti, bylo by pouze 284 noh. Protože jich je 452, tedy o 168 více, musí být polovina ze 168, tedy 84, rovna počtu ulovené čtyřnohé zvěře. Protože zajíců je šestkrát více než králíků, je počet králíků sedminou z tohoto čísla, tedy 12, a počet zajíců 72. Bažantů je 58.

8. Pouze dvě hodiny, protože potřebuje pouze prokousat přední desku prvního dílu a zadní desku druhého dílu. Jsou-li oba díly uloženy v knihovně tak, jak obvykle bývají, to jest první díl nalevo od druhého, zmíněné desky jsou přímo vedle sebe.

9. Čekali bychom, že průměrná rychlost bude aritmetickým průměrem z čísel 12 a 4, tedy 8 km/hod. Není tomu tak. Nechť celková dráha (v kilometrech) je s. Potah urazil její první polovinu za $\frac{1}{24}s$ hodin, druhou polovinu za $\frac{1}{8}s$ hodin; celkový čas byl tedy $\frac{1}{24}s + \frac{1}{8}s = \frac{1}{6}s$ hodin. Čtvrtinu z této doby, to jest $\frac{1}{24}s$ hodin, se potah pohyboval rychlostí 12 km/hod, tři čtvrtiny rychlostí 4 km/hod. Průměrná rychlost je tedy $(12 + 3.4)/4 = 6$ km/hod.

10. Nevíme zatím, v kolik hodin byl závod odstartován ani jak dlouhá je trať. Vypočteme si nejdříve tyto údaje. Nechť start byl v x hodin. Běží-li lyžař rychlostí 10 km/hod, pak proběhne trať v čase $13 - x$ hodin; běží-li rychlostí 15 km/hod, pak mu závod trvá $11 - x$ hodin. Délka tratě je tedy

$$10(13 - x) = 15(11 - x).$$

Z toho vypočteme $x = 7$. Start byl tedy v 7 hodin, trať je dlouhá 60 km. Aby závodník doběhl ve 12 hodin, musí běžet rychlostí 12 km/hod.

11. Nechť x je doba potřebná k cestě autem od továrny k vile. Obvykle tedy ředitel přijíždí do vily ve $12 + x$ hodin, onoho dne přijel ve $\frac{23}{2} + x$ hodin. Šofér vyjíždí vždy ve $12 - x$ hodin od vily. Osudného dne tedy šofér potkal ředitele ve chvíli, která je aritmetickým průměrem čísel $12 - x$ a $\frac{23}{2} + + x$; cesta tam i zpět mu totiž musela trvat stejnou dobu. Tento průměr nezávisí na x a je to $\frac{47}{4}$, to je 11 hodin 45 minut. Ředitel tedy alibi neměl.

12. Vědět, že součin věků je 36, samozřejmě nestačí. Číslo 36 lze mnoha způsoby vyjádřit jako součin tří přirozených čísel;

je to 1.1.36, 1.2.18, 1.3.12, 1.4.9, 1.6.6, 2.2.9, 2.3.6, 3.3.4. Nyní je důležité, že panu A nestačilo znát ani součet věků. Součty příslušných čísel v jednotlivých případech jsou totiž navzájem různé, s výjimkou jediné dvojice případů, a to 2, 2, 9 a 1, 6, 6; v obou těchto případech je součet 13. Kdyby byl počet oken jiný než 13, pan A by mohl už věky určit. Bylo tedy 13 oken a pan A potřeboval ještě další údaj. V tomto posledním údaji není ovšem podstatný počet dioptrií, ale to, že pan B užívá výrazu „můj nejstarší syn". V případě 1, 6, 6 by dva starší synové byli dvojčata a pan B by musel říci „jeden z mých starších synů". Věky jednotlivých synů jsou tedy 2, 2, 9.

18. Nechť a, b, c, d jsou po řadě počty dětí doktora Watsona, jeho bratra, sestry a strýce. Nechť N je číslo domu doktora Watsona. Pak platí $a > b > c > d$, $a + b + c + d < 18$, $abcd = N$. Samozřejmě a, b, c, d, N jsou přirozená čísla. Kdyby bylo $d \geqq 3$, bylo by $c \geqq 4$, $b \geqq 5$, $a \geqq 6$ a tedy $a + b + c + d \geqq 18$. Tedy $d = 1$ nebo $d = 2$. Nyní nastává piplavá práce vypsat všechny přípustné čtveřice (a, b, c, d) a určit jejich součiny. Provedeme-li to, zjistíme, že jsou tři čtveřice o stejném součinu, a to (5, 4, 3, 2), (6, 5, 4, 1) a (8, 5, 3, 1). Libovolné dvě přípustné čtveřice, z nichž alespoň jedna nepatří mezi uvedené, mají součiny různé. Některá z uvedených čtveřic je tedy řešením; jinak by Holmes mohl úlohu vyřešit i bez údaje o počtu strýcových dětí. Kdyby bylo $d = 1$, nestačil by mu ani tento údaj — měl by stále ještě dvě možnosti. Je tedy $d = 2$, $a = 5$, $b = 4$, $c = 3$, $N = 120$.