O dělitelnosti čísel celých

František Veselý (author): O dělitelnosti čísel celých. (Czech). Praha: Mladá fronta, 1966.

Persistent URL: http://dml.cz/dmlcz/403560

Terms of use:

© František Veselý, 1966

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

1 | 561.184
G 11

MATEMATIKŮ

O DĚLITELNOSTI ČÍSEL CELÝCH

14

Vydal Matematický ústav ČSAV a ÚV ČSM v nakladatelství Mladá fronta

ŠKOLA MLADÝCH MATEMATIKŮ

FRANTIŠEK VESELÝ

o dělitelnosti čísel celých

PRAHA 1966
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
A ÚV ČSM V NAKLADATELSTVÍ
MLADÁ FRONTA

Recenzovali doc. dr. Karel Hruša a CSc. Miroslav Šisler

© František Veselý, 1966

PŘEDMLUVA

Některé vlastnosti celých čísel poznávali lidé již v době, kdy znali jen čtyři základní početní výkony. Studium takových vlastností, a to zejména zkoumání dělitelnosti čísel celých i řešení rovnic v oboru čísel celých, vedlo ke vzniku samostatného oboru teoretické aritmetiky, pro nějž se od počátku 19. století ustálil název *číselná teorie* nebo *teorie čísel*. Tyto názvy se vžily, přestože nevystihují dost dobře obsah toho oboru matematiky, který označují.

Číselná teorie patří k nejstarším oborům matematiky. Zabývali se jí skoro všichni významní matematikové všech dob, jako např. Euklides (365?—300? před n. l.), Diofantos (okolo roku 250 n. l.), P. Fermat (1601—1665), G. W. Leibniz (1646—1716), L. Euler (1707—1783), J. L. Lagrange (1736—1813), A. M. Legendre (1752—1833), K. F. Gauss (1777—1855), P. L. Čebyšev (1821—1894) aj.

Od poloviny 20. století bylo řešení některých problémů číselné teorie usnadněno tím, že se při něm začalo užívat výkonných samočinných elektronických počítacích strojů. Jejich užití přispělo nejen k odkrytí několika překvapujících poznatků novodobé číselné teorie, ale ovlivnilo i rozvoj nových pracovních metod. V té době začaly poznatky číselné teorie ovlivňovat rozvoj numerických metod matematiky, které mají velký význam pro její užití v praxi.

Některé poznatky číselné teorie ukazují vzájemné vztahy mezi určitými problémy aritmetiky, algebry a geometrie. Nadto úvahy o problémech číselné teorie jsou užitečné

k tomu, aby se na nich ukazovaly formy matematického usuzování a logická stavba matematických vět. V edici *Škola mladých matematiků* byl k tomu cíli zaměřen již druhý její svazek, který pod názvem *Co víme o přirozených číslech* napsal Jiří Sedláček. Obsahuje 28 řešených úloh spojených textem, pojednávajícím o základních pojmech číselné teorie a doplněných důkazy některých matematických vět. Jestliže jste uvedenou knížku prostudovali, získali jste tím velmi dobrou průpravu ke studiu knížky *O dělitelnosti čísel celých*, do níž byl z číselné teorie vybrán větší počet vět obecněji formulovaných i dokazovaných. Tuto knížku můžete však studovat i samostatně, neboť jsou v ní připomenuty všechny potřebné definice a základní věty z nauky o dělitelnosti celých čísel.

Není nutné, abyste studovali všechny kapitoly této knížky v tom pořadí, v němž jsou seřazeny. Tak např. po prostudování prvních tří kapitol můžete vynechat studium kapitoly 4 nebo přečíst si z ní jen matematické věty bez jejich důkazů. Studiem kapitol 5 a 6 prohloubíte své znalosti o největším společném děliteli a nejmenším společném násobku čísel. Tyto pojmy jsou vysvětleny nezávisle na větách o rozkladu přirozených čísel v prvočinitele a pojem největšího společného dělitele je osvětlen i z jiného hlediska, které jste dosud neznali. Kapitola 7 obsahuje nejdůležitější věty teorie prvočísel a tvoří s kapitolami 5 a 6 nejdůležitější část knihy.

Objevy nových matematických poznatků mají často původ v tom, že z platnosti určitých vět v mnoha zvláštních případech odvozujeme domněnku o obecné jejich platnosti; pravdivost takových domněnek musíme však dokázat. Kapitola 8 ukazuje názorný příklad, jak opatrný musí být matematik při užívání neúplné indukce. Přitom kapitoly 8 a 9 ukazují vztah mezi matematickými větami navzájem obrácenými. V kapitole 10 jsou podány některé zajímavé

informace o tom, čeho bylo v číselné teorii dosaženo pomocí moderních počítacích strojů, přičemž se objasňuje i souvislost mezi starými i novými problémy číselné teorie.

Při řešení některých úloh i při důkazech vět jsem někdy připomenul, že se dají provést matematickou indukcí, které jsem sám užil jen v kapitole 9. Podrobnější poučení o tomto principu najdete v šestém svazku této edice, který s názvem *Matematická indukce* napsal Rudolf Výborný.

Za každou kapitolou jsou uvedeny úlohy ke cvičení. Většina z nich se řeší obdobně jako úlohy řešené v příkladech textu. Některé úlohy jsou pro čtenáře náročnější, avšak znalost jejich řešení není nutná pro studium dalších článků.

Děkuji vědeckému pracovníku Ústavu dálkového studia učitelů docentu dr. Karlu Hrušovi a vědeckému pracovníku Matematického ústavu ČSAV CSc. Miroslavu Šislerovi, za to, že velmi pozorně pročetli rukopis této knížky. Svými připomínkami mi pomohli doplnit vhodně text rukopisu a zpřesnit jeho znění.

Autor

1. kapitola

NĚKTERÉ VLASTNOSTI MNOŽIN CELÝCH ČÍSEL

Při výkladu rozsáhlejší části některého oboru matematiky nebo jiné vědy je často třeba přesně stanovit význam některých odborných názvů (termínů), jichž se při výkladu používá. Věty, jimiž vyjadřujeme úmluvu o tom, jaký význam přisuzujeme určitým odborným názvům, nazývají se definice. I v této knížce se setkáte s některými definicemi, které budou vymezovat matematické pojmy označené určitým odborným názvem. V textu knížky budou vyznačeny písmenem **D** s indexem $i = 1, 2, 3, 4, \ldots$, značícím pořadové číslo definice.

Definice neslouží však jen k tomu, abychom jimi vyjadřovali úmluvu o významu nově zaváděných odborných názvů. Někdy se stává, že máme význam odborného názvu vysvětlit někomu, kdo takový název již zná, ale jeho význam přesně nechápe. V tom případě můžeme nesprávně chápaný pojem označený odborným názvem objasnit vhodně volenou definicí s uvedením charakteristického souhrnu znaků, které má každý předmět tímto názvem označený, a žádný jiný předmět. Nemůžeme zde vykládat, jaké podmínky má splňovat správná definice. Připomeneme však, že v každé definici má být užito jen takových odborných termínů, jejichž význam je již znám tomu, komu je definice určena.

Není možné, abychom zde uváděli definice všech důležitých matematických pojmů, jejichž znalost budete potřebovat ke studiu této knížky. Předpokládáme, že definice

některých pojmů znáte z hodin vyučování matematiky a že i bez definic dobře chápete základní matematické pojmy, jako jsou např. počet, číslo apod. S takovými pojmy jste se seznamovali jejich užíváním ve vhodně volených příkladech a takového postupu užijeme nyní i při objasňování matematického pojmu množina.

Význam matematického termínu množina je blízký významu slov souhrn nebo soubor, jejichž význam v obecném jazyce je různě chápán. Jestliže z libovolných, navzájem rozlišitelných předmětů našeho názoru nebo myšlení (tj. z předmětů konkrétních nebo abstraktních) utvoříme soubor myšlený jako celek, pak říkáme, že jsme tím vytvořili množinu; jednotlivé předměty tohoto souboru nazýváme prvky této množiny. K označování množin budeme užívat velkých písmen a k označování prvků množiny malých písmen nebo jiných značek, např. číslic apod. K zápisu vztahů „je prvkem" a „není prvkem" užijeme značek $\in$, $\notin$. Zápis „$x \in M$" znamená „x je prvkem množiny M" a „$y \notin M$" znamená „y není prvkem množiny M". Vztah označený symbolem $\in$ můžeme vyjádřit též slovy „patří do", „náleží do", ale musíme pamatovat na to, že tato rčení znamenají v teorii množin totéž jako „je prvkem".

Každá množina je přesně určena vždy, je-li dán předpis, podle kterého lze aspoň teoreticky rozhodnout, zda libovolný předmět je nebo není prvkem této množiny. Jde-li o množiny s konečným a nepříliš velkým počtem prvků, může být takový předpis dán prostým výčtem všech prvků množiny. V tom případě můžeme zápis takové množiny provést tak, že do složených závorek zapíšeme všechny prvky množiny. Tak např. $M = \{17; 3; 10\}$ znamená, že prvky množiny M jsou tři celá čísla 17, 3, 10 a žádná jiná čísla ani žádné jiné předměty. Můžeme tedy napsat $17 \in M$, $5 \notin M$ atd. Jde-li o množinu s velkým počtem

prvků, definujeme ji zpravidla tak, že udáme charakteristický souhrn znaků, který mají všechny prvky definované množiny a žádné jiné předměty. V tomto případě slovní definici množiny, obsahující často matematický vzorec, doplňujeme pro názornost i výčtem některých prvků množiny, což nám o ní poskytne názornější představu.

Odborný název množina nesmí vás svést k tomu, abyste se domnívali, že množina musí obsahovat mnoho prvků. Při definici určité množiny často ani nevíme, jak velký je počet jejích prvků. Tak např. množina všech žáků vaší školy, kteří jsou v tomto okamžiku, kdy čteme tuto definici, přítomni ve vaší tělocvičně, může obsahovat různý počet prvků, ale je přesně určena i v tom případě, že v tomto okamžiku není přítomný v tělocvičně ani jeden žák vaší školy. Pak říkáme, že taková množina je prázdná. Prázdnou množinu označujeme symbolem $\emptyset$, který musíme rozlišovat od symbolu 0, značícího číslo nula. Prvky množiny nemusí být předměty téhož druhu. Tak např. můžeme utvořit množinu, která obsahuje tyto předměty: budovu Národního divadla v Praze, planetu Mars a číslo π. V matematice však nejčastěji uvažujeme o množinách, které obsahují prvky téhož druhu, jako např. čísla, funkce, body, přímky, roviny apod. V tom případě musíme rozlišovat pojem množina celých čísel od pojmu množiny všech celých čísel apod. Je nekonečně mnoho množin celých čísel, ale existuje jen jedna množina všech celých čísel.

Dříve než vysvětlíme některé další základní pojmy teorie množin, uvedeme 10 příkladů číselných množin, jichž použijeme dále v tomto článku.

1) $M_1 = \emptyset$; 2) $M_2 = \{0\}$; 3) $M_3 = \{1, 5, 10\}$; 4) M_4 je množina všech čísel, která jsou koeficienty binomického rozvoje $(a + b)^6$; 5) M_5 je množina všech celých čísel x, pro která platí $-1 < x < +1$; 6) M_6 je množina všech reálných čísel x, pro něž platí $-1 < x < +1$; 7) M_7 je

množina všech celých kladných čísel; 8) M_8 je množina všech celých záporných čísel; 9) M_9 je množina všech celých čísel; 10) M_{10} je množina všech reálných čísel.

D_1 *Čísla přirozená nazýváme taková celá čísla, která jsou kladná.*

Význam termínu číslo přirozené je tak chápán snad ve všech českých matematických spisech, ale v cizojazyčné literatuře často zjistíte, že někteří matematikové užívají názvu číslo přirozené pro každé celé nezáporné číslo. Při tomto odlišném stanovisku je číslo 0 číslo přirozené, zatímco pro nás číslo 0 není prvkem množiny všech přirozených čísel. Na tomto jednoduchém příkladu vidíte, že význam určitého odborného názvu může být chápán různě podle toho, jak se o něm dohodneme.

D_2 *Jsou-li dvě množiny A, B v takovém vztahu, že každý prvek množiny A je zároveň prvkem množiny B, pak říkáme, že množina A je části množiny B nebo že množina A je podmnožinou množiny B; takový vztah zapisujeme symbolicky $A \subset B$.*

Platí tedy např. $M_2 \subset M_5$, $M_2 \subset M_6$, $M_2 \subset M_9$, $M_2 \subset M_{10}$, $M_3 \subset M_4$, $M_3 \subset M_7$, $M_3 \subset M_9$, $M_3 \subset M_{10}$ atd. Platí též $\emptyset \subset M$, ať je M jakákoli množina. Je též možné, že pro množiny A, B platí zároveň vztahy $A \subset B$, $B \subset A$, jak se snadno přesvědčíte na těchto příkladech: $M_2 \subset M_5$, $M_5 \subset M_2$ nebo $M_3 \subset M_4$, $M_4 \subset M_3$.

D_3 *Skládají-li se množiny A, B z týchž prvků, říkáme, že jsou si rovny, a zapisujeme to $A = B$; neplatí-li vztah $A = B$, pak píšeme $A \neq B$ a říkáme, že množiny A, B si nejsou rovny (jsou různé).*

Platí tedy např. $M_2 = M_5$, $M_3 = M_4$, $M_1 \neq M_2$, $M_5 \neq M_6$ apod. Poznamenáváme ještě, že rovnost množin $A = B$ platí, když platí zároveň vztahy $A \subset B$, $B \subset A$.

D$_4$ *Sjednocení množin A, B nazýváme množinu S, skládající se právě z těch prvků, které patří (buď) do množiny A, nebo do množiny B.* (Obdobně definujeme sjednocení tří a více množin.)

Příklady: Sjednocením množin M_1, M_2 je množina M_2. Sjednocením množin M_2, M_3 je množina $\{0, 1, 5, 10\}$. Sjednocením množin M_5, M_6 je množina M_8. Sjednocením tří množin M_2, M_7, M_8 je zřejmě množina M_9. Sjednocením množiny $A = \{0, 1, 2, 3\}$ a $B = \{2, 3, 4\}$ je množina $S = \{0, 1, 2, 3, 4\}$. Na tomto posledním jednoduchém příkladě množiny S, která je sjednocením množin A, B, dobře vidíme, že obsahuje: a) všechny prvky množiny A, které nepatří do množiny B, tj. čísla 0, 1, b) všechny prvky množiny B, které nepatří do množiny A, tj. číslo 4, c) všechny prvky, které patří zároveň do množiny A i B, tj. čísla 2, 3.

Definicí sjednocení množin, kterou jsme si osvětlili na jednoduchých příkladech, jsme zároveň naznačili, jaký význam přisuzujeme spojkám nebo a buď — nebo v matematických textech. V obecném jazyce se jimi naznačuje buď rozluka neúplná (alternativa), nebo rozluka úplná (disjunkce). Jejich různý význam bývá zpravidla chápán podle souvislosti s ostatním textem, podle situace, o níž se něco vypovídá apod. V matematice je zvykem chápat jejich význam tak, že tyto spojky vyjadřují neúplnou rozluku, jak jsme to již výše ukázali. Jde-li o to vyjádřit v matematickém textu úplnou rozluku, učiníme to zvláštní doplňující poznámkou. Chceme-li např. definovat množinu R, která má obsahovat jen prvky uvedené pod písmenem a), b) v předcházejícím odstavci a žádné jiné prvky, můžeme to učinit takto: R je množina skládající se ze všech prvků, které patří právě do jedné z množin (buď) A nebo B.

$\mathbf{D}_5$ *Průnik množin A, B nazýváme množinu P skládající se ze všech prvků, které patří zároveň do množin A i B.*

Příklady: Průnik množin M_2, M_3 je $\emptyset$. Průnik množin M_3, M_4 je množina $M_3 = M_4$. Průnik množin $A = \{0, 1, 2, 3\}$, $B = \{2, 3, 4\}$ je množina $P = \{2, 3\}$.

Při studiu teorie množin si musíte již od počátku zvykat na to, abyste vždy dobře rozlišovali pojmy množina a prvek množiny. Je např. možné, že v některé úvaze budete určitou přímku považovat za množinu bodů, zatímco v jiné úvaze budete tutéž přímku považovat za prvek některé množiny přímek. Nemůžeme zde však podrobněji rozbírat důsledky některých omylů, k nimž dochází po nesprávném rozlišování pojmů množina a prvek množiny. Chceme vás však upozornit zvláště na to, že je rozdíl mezi množinou $\{a\}$ a prvkem a, z něhož se tato množina skládá. Tento rozdíl je zřejmý i z toho, že má smysl zápis $a \in \{a\}$, zatímco zápis $\{a\} \in a$ nemá smysl.

Zavedení pojmu prázdná množina do matematických úvah ovlivnilo i vyjadřování matematiků způsobem, na který vás stručně upozorníme. Zamyslete se nejprve nad těmito větami:

1a) Každý český král se dožil 60 let.

2a) Žádný český král se nedožil 60 let.

Jistě si brzy uvědomíte, že není možné, aby obě tyto věty byly zároveň pravdivé. Může být pravdivá nejvýše jedna z nich. Mohou být obě nepravdivé, jestliže se některý český král dožil a některý nedožil 60 let. V klasické logice i v obecném jazyce jsou věty typu 1a, 2a považovány za pravdivé nebo nepravdivé jen za předpokladu, že podmět označuje prvky nějaké neprázdné množiny.

Uvažme nyní tyto dvě věty:

1b) Každý švýcarský král se dožil 60 let.

2b) Žádný švýcarský král se nedožil 60 let.

Poněvadž množina všech švýcarských králů je prázdnou množinou, působí věty 1b, 2b a věty toho typu nezvykle na každého, kdo se nezabývá matematikou. Vývoj matematiky již v minulém století přispěl k tomu, že novodobá logika začala uznávat věty typu 1b, 2b a jim obdobné za pravdivé; ba dokonce v tomto případě, kdy podmět označuje prvky prázdné množiny, pokládáme obě věty 1b i 2b za pravdivé. Této zásady pro posuzování pravdivosti logických výroků jsme již jednou použili, když jsme při výkladu definice $\mathbf{D}_2$ uvedli příklad: $\emptyset \subset M$, ať je M jakákoli množina, neboť podle definice $\mathbf{D}_2$ je každý prvek množiny $\emptyset$ prvkem množiny M.

$\mathbf{D}_6$ *Množina se nazývá konečná, je-li možné udat počet jejích prvků přirozeným číslem nebo číslem* 0; *není-li množina konečná, říkáme, že je nekonečná nebo že má nekonečně mnoho prvků.*

K tomu, abychom dokázali, že nějaká množina M prvků dané vlastnosti je nekonečná, užíváme často nepřímého důkazu. Vyjdeme z předpokladu, že množina M je konečná a že tedy všechny její prvky lze očíslovat přirozenými čísly 1, 2, 3, ..., n. Podaří-li se nám pak dokázat existenci dalšího prvku, který není uveden mezi očíslovanými n prvky, je to ve sporu s předpokladem, že množina M všech prvků dané vlastnosti obsahuje n prvků, kde n je číslo přirozené. Tím je však dokázáno, že množina M není konečná, čili že je nekonečná.

K vyjadřování myšlenek užíváme nejčastěji slov a z nich utvořených vět obecného jazyka mluveného nebo psaného. V odborném jazyce psaném užíváme k zapisování odborných termínů nebo rčení též zvláštních značek (symbolů), které umožňují stručnější a přehlednější zápisy vět. Studiem stavby vět a jejich významu se zabývá logika, která věnuje největší pozornost vypovídacím větám,

o nichž má smysl říci, že jsou pravdivé nebo nepravdivé. Takové věty se přesně označují názvem logický výrok; nevznikne-li nebezpečí nedorozumění, užíváme stručnějšího názvu výrok. Logickými výroky nejsou takové věty, jako: Přines mi sklenici vody! Kolik je hodin? apod.

Příklady pravdivých výroků z oboru matematiky jsou tyto věty: 1) $2 + 3 = 5$; 2) $3 < 5$; 3) pro libovolná reálná čísla a, b platí $(a + b)\,(a - b) = a^2 - b^2$; 4) pro každé reálné číslo x platí: když $x < 0$, pak $x^2 > 0$. Příklady nepravdivých výroků jsou tyto věty: 5) $3 < 3$; 6) $2 + 3 \neq 5$; 7) každý mnohoúhelník rovnostranný je rovnoúhlý; 8) pro každé reálné číslo x platí: když $x^2 > 0$, pak $x < 0$.

V matematice zkoumáme často domněnky, zda nějaký výrok je nebo není pravdivý. Ještě častějším úkolem matematiky je odvozovat pravdivé matematické výroky (věty) podle pravidel logického usuzování. Východiskem logických úvah jsou takové výroky (matematické věty), jejichž pravdivost jsme buď již dokázali, nebo uznali jejich pravdivost bez důkazu. Věty, jejichž pravdivost uznáváme bez důkazu, se nazývají *axiómy*. Pravdivé matematické věty, jichž se často v matematice užívá, se někdy nazývají *poučky* čili *teorémy*. V této knížce je označíme písmenem **T** s indexem, udávajícím jejich pořadové číslo. Termínu matematická věta přisoudíme význam o něco širší než termínu poučka, neboť v některých případech budeme vyšetřovat i nepravdivé věty a říkat např., že obrácená věta neplatí. Uvedeme nyní několik pravdivých matematických vět, na něž se v dalších kapitolách budeme odvolávat.

T_1 *Jsou-li a, b dvě přirozená čísla taková, že $a > b$, pak existuje takové přirozené číslo n, že platí $nb > a$.*

Rčení „existuje přirozené číslo n“ znamená totéž jako „existuje alespoň jedno přirozené číslo n“. Smysl věty T_1 je hlavně v tom, že se jí uznává existence čísla n s danou

vlastností. Je-li $a = 10^7$, $b = 3$, pak požadovanou vlastnost má např. číslo $n = 4.10^6$ nebo některé jiné přirozené číslo, např. 3 333 334.

T_2 *V každé neprázdné množině přirozených čísel existuje číslo nejmenší (minimální).*

Množina všech přirozených čísel, pro něž platí $3n > 10^7$, je jistě neprázdná, jak plyne z věty T_1. V této množině musí podle věty T_2 existovat nejmenší přirozené číslo s požadovanou vlastností, jímž je $n_1 = 3\,333\,334$. V množině všech přirozených čísel je nejmenší číslo 1.

T_3 *V každé neprázdné množině takových přirozených čísel x, že pro každé x platí $x \leqq h$, kde $h \geqq 1$ je libovolné reálné číslo, existuje největší číslo.*

Všechna přirozená čísla m, pro něž platí $3m < 10^7$, tvoří neprázdnou množinu, do níž zřejmě patří číslo 1, neboť $3.1 < 10^7$. Každé číslo této množiny $m < \frac{1}{3}.10^7$. Proto v této množině musí existovat největší přirozené číslo, jímž je $m_1 = 3\,333\,333$.

T_4 *Součet a součin přirozených čísel jsou vždy čísla přirozená; také každá mocnina, jejíž mocněnec i mocnitel jsou čísla přirozená, je číslo přirozené.*

V množině všech přirozených čísel není odčítání a dělení neomezeně proveditelným početním výkonem. Rozdíl přirozených čísel $a - b$ je číslo přirozené jen tehdy, když $a > b$.

T_5 *Součet, součin i rozdíl celých čísel je vždy číslo celé; také každá mocnina, jejíž mocněnec je číslo celé a mocnitel číslo přirozené, je číslo celé.*

Zatímco v množině všech čísel celých je i odčítání pro-

veditelné bez omezení, zůstává dělení celých čísel početním výkonem, který v množině všech čísel celých není vždy proveditelný. Některé důsledky věty $\mathbf{T}_5$ nyní připomeneme.

Pro libovolná reálná čísla a, b platí známé rovnosti

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2), \qquad (1,1)$$

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2), \qquad (1,2)$$

které jsou zvláštními případy vzorců

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots\ldots + ab^{n-2} + b^{n-1}, \qquad (1,3)$$

který platí pro každé přirozené číslo $n > 1$ a

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}), \qquad (1,4)$$

který platí jen pro lichá přirozená čísla $n > 1$.

Jsou-li a, b čísla celá, pak podle věty $\mathbf{T}_5$ jsou celými čísly nejen rozdíl a součet n-tých mocnin čísel a, b na levé straně rovností (1,3), (1,4), ale i činitelé součinů na pravých stranách těchto rovností. Tyto vzorce nám pomohou převádět rozdíly i součty mocnin celých čísel na součiny a tím usnadní řešení mnohých úloh z nauky o dělitelnosti celých čísel, jak to poznáme v následujících kapitolách. Je ovšem třeba pamatovat na to, že rozklad rozdílu nebo součtu mocnin čísel a, b s přirozeným mocnitelem je někdy možno provést užitím vzorců (1,3), (1,4), i když mocniny čísel a, b nemají stejného mocnitele. Tak např.:

$$a^{10} + b^{15} = (a^2)^5 + (b^3)^5 = (a^2 + b^3)(a^8 - a^6 b^3 + a^4 b^6 - a^2 b^9 + b^{12}).$$

Nyní si ještě připomeneme některé základní pojmy z algebry a matematické analýzy, a to zejména z té její části, kterou tvoří teorie reálných funkcí. To, co již z tohoto oboru matematiky znáte, vyslovíme obecnými větami, k nimž připojíme několik poznámek.

Jestliže ke každému prvku x dané množiny M je podle nějakého předpisu přiřazeno právě jedno reálné číslo, pak říkáme, že na množině M je definována reálná funkce proměnné x. Množinu M nazýváme definičním oborem této funkce proměnné x, čísla přiřazená prvkům x nazýváme funkční hodnoty dané funkce. V obecných úvahách označujeme funkční hodnoty symbolickými zápisy $f(x)$, $g(x)$, $h(x)$ apod. nebo $F(x)$, $G(x)$, $H(x)$ apod. Přitom např. zápis $f(-2) = 5$ znamená, že číslu -2, které je prvkem definičního oboru funkce dané předpisem f, je přirozené číslo 5 jako funkční hodnota.

V této knížce se budeme nejvíce zajímat o funkce, jejichž funkční hodnoty $f(x)$ jsou určeny početním (analytickým) výrazem

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n, \quad (1,5)$$

kde x je proměnná, n celé nezáporné číslo a $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ libovolná daná reálná čísla, z nichž $a_0 \neq 0$; říkáme, že *polynom* (*mnohočlen*) je stupně n. Jestliže $a_0 = 1$, mluvíme o normovaném polynomu n-tého stupně.

Jistě je vám již známo, že polynom stupně $n = 1$ se nazývá lineární, polynom stupně $n = 2$ kvadratický. Později se setkáte i s názvem polynom kubický pro polynom stupně $n = 3$ a s názvem polynom bikvadratický pro polynom stupně $n = 4$. Polynom stupně 0 je každá konstanta různá od nuly. Číslo 0 nazýváme též často nulový polynom, avšak nepřipisujeme mu žádný stupeň.

Při našich úvahách o dělitelnosti čísel celých budeme se zajímat jen o takové polynomy tvaru (1,5), v nichž koe-

ficienty $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ jsou čísla celá. Pro takové polynomy platí zřejmě jako důsledek věty $\mathbf{T}_5$, že pro každé číslo x z množiny všech celých čísel nabývají celočíselné funkční hodnoty. Jistě též již víte, že součet, rozdíl i součin polynomů s celočíselnými koeficienty je opět polynom s koeficienty z oboru čísel celých.

Pro řešení mnohých matematických úloh je často velmi užitečné rozložit (redukovat) daný polynom na součin dvou nebo více polynomů nižšího stupně, než je stupeň daného polynomu. Nemůžeme se tu zabývat otázkou rozložitelnosti (reducibility) polynomů v různých číselných oborech a připomeneme si tu dvěma příklady rozklad kvadratického polynomu na součin dvou lineárních polynomů, a to metodou převodu polynomu na druhou mocninu lineárního polynomu s doplňkem. Obdobně můžeme pak provádět i rozklad některých polynomů 4. stupně na součin dvou kvadratických polynomů, jak si to rovněž ukážeme na příkladech.

1. $x^2 - 2x - 48 = (x - 1)^2 - 1 - 48 =$
$= (x - 1)^2 - 7^2 = (x - 1 - 7)(x - 1 + 7) =$
$= (x - 8)(x + 6).$

2. $x^2 - 2x - 1 = (x - 1)^2 - (\sqrt{2})^2 =$
$= (x - 1 - \sqrt{2})(x - 1 + \sqrt{2}).$

3. $x^4 + 64 = (x^2 + 8)^2 - 16x^2 = (x^2 + 8)^2 - (4x)^2 =$
$= (x^2 - 4x + 8)(x^2 + 4x + 8).$

4. $4x^4 + 1 = (2x^2 + 1)^2 - 4x^2 = (2x^2 + 1)^2 - (2x)^2 =$
$= (2x^2 - 2x + 1)(2x^2 + 2x + 1).$

5. $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 =$
$= (x^2 - x + 1)(x^2 + x + 1).$

6. $x^4 + 1 = (x^2 + 1)^2 - (x\sqrt{2})^2 =$
$= (x^2 - x\sqrt{2} + 1)(x^2 + x\sqrt{2} + 1).$

Příklady 1, 3, 4, 5 ukazují, že je někdy možný rozklad polynomu s celočíselnými koeficienty na součin dvou polynomů s celočíselnými koeficienty. Také v příkladech 2, 6 jsme dané polynomy s celočíselnými koeficienty rozložili na součiny dvou polynomů, avšak ty nemají již všechny koeficienty z oboru čísel celých; takové rozklady při studiu této knížky potřebovat nebudeme, avšak o jejich užitečnosti se přesvědčíte při dalším studiu jiných oborů matematiky.

Cvičení

1,1. Kolikerým způsobem lze rozložit a) $x^6 - 1$, b) $x^6 + 1$ na součin dvou normovaných mnohočlenů s celými koeficienty?
1,2. Najděte rozklad polynomu a) $x^4 + 4$, b) $81x^4 + 4$ na součin dvou kvadratických trojčlenů s celými koeficienty.
1,3. Najděte podmínku, které musí vyhovovat přirozená čísla a, b, má-li být možný rozklad dvojčlenu $ax^4 + b$ na součin dvou kvadratických trojčlenů s celými koeficienty.
1,4. Užitím vět $\mathbf{T}_4$, $\mathbf{T}_5$ dokažte tyto poučky: a) součet přirozených čísel nerovná se nikdy nule; b) součet celých nezáporných čísel se rovná nule právě tehdy, když každý sčítanec součtu je rovný nule.

2. kapitola

ZÁKLADNÍ POJMY A VĚTY Z NAUKY O DĚLITELNOSTI ČÍSEL

Již v 7. třídě ZDŠ jste se seznámili s významem některých odborných názvů z nauky o dělitelnosti přirozených čísel. Definicí $\mathbf{D}_7$ stanovíme jejich význam v nauce o dělitelnosti celých čísel.

$\mathbf{D}_7$ *Existuje-li k daným celým číslům a, b takové celé číslo q, že platí* $a = bq$, *zapisujeme to symbolicky* $b \mid a$; *zápis* $b \nmid a$ *znamená, že neplatí vztah* $b \mid a$.

Zápis $b \mid a$ *čteme zpravidla jedním z těchto tří způsobů*:

1. *číslo b je dělitelem čísla a,*
2. *číslo a je dělitelné číslem b,*
3. *číslo a je násobkem čísla b.*

Mezi čísly 21 a 7 platí tedy vztah $7 \mid 21$, poněvadž lze najít celé číslo 3 tak, že platí $21 = 7.3$. Zápis $7 \mid 21$ čteme jedním z těchto tří způsobů: číslo 7 je dělitelem čísla 21, číslo 21 je dělitelné číslem 7, číslo 21 je násobkem čísla 7. Na tomto jednoduchém příkladu vidíte, že význam názvů, které jste poznali v nauce o dělitelnosti přirozených čísel, se definicí $\mathbf{D}_7$ nezměnil. Na jiných příkladech si však ukážeme jejich širší význam v oboru celých čísel. Tak např. platí $-3 \mid 12$, neboť $12 = (-3).(-4)$, $5 \mid -20$, poněvadž $-20 = 5.(-4)$, $-13 \mid -91$, poněvadž $-91 = (-13).7$. Neplatí však $3 \mid 10$, $-7 \mid 15$, čili platí $3 \nmid 10$, $-7 \nmid 15$.

Povšimněte si zvláště toho, že vždy platí $1 \mid a$, $-1 \mid a$, $a \mid a$, $-a \mid a$, $a \mid -a$, $-a \mid -a$, ať je a kterékoli celé číslo.

Dále platí vždy $b \mid 0$, ať je b kterékoli celé číslo, neboť $0 = b.0$; platí tedy i $0 \mid 0$, neboť $0 = 0.q$ pro každé celé číslo q. Neplatí $0 \mid a$, když $a \neq 0$, neboť v tom případě neexistuje takové celé číslo q, aby platilo $a = 0.q$. Platí-li $0 \mid a$, pak musí být $a = 0$.

Zápisy $\frac{5}{2} \mid 10$, $\frac{5}{2} \nmid 10$ nemají ovšem žádný smysl, i když $10 = \frac{5}{2}.4$. Vztahy $b \mid a$, $b \nmid a$ jsme totiž definovali jen pro celá čísla a, b. Věty, které nemají smysl, nelze považovat za výroky pravdivé ani nepravdivé. Musíte si dobře pamatovat, že je rozdíl mezi významem názvu dělitel z hlediska číselné teorie a jeho významem z hlediska praktické aritmetiky. V té se např. při dělení $10 : \frac{5}{2} = 4$ číslo 10 nazývá dělenec, číslo $\frac{5}{2}$ dělitel a číslo 4 podíl. Pro dva rozdílné pojmy, pro které se v češtině užívá téhož názvu dělitel, existují v některých cizích jazycích rozdílné termíny.

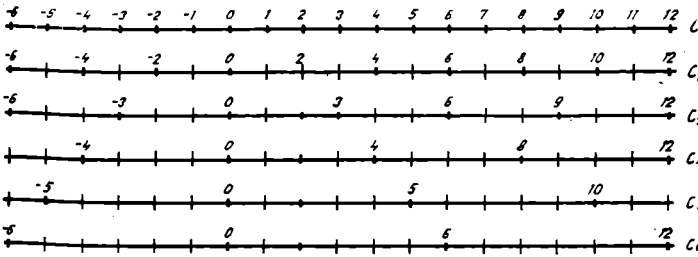
V některých případech budeme k danému celému číslu a hledat takové přirozené číslo b, které je dělitelem čísla a. Abychom se mohli stručně vyjadřovat, zavedeme ještě jeden termín následující definicí.

D$_8$ *Přirozený dělitel čísla a znamená totéž jako přirozené číslo, které je dělitelem čísla a.*

Podle této definice je např. číslo 4 přirozeným dělitelem čísla -12. Množina $M = \{-10, -5, -2, -1, 1, 2, 5, 10\}$ je množinou všech dělitelů čísla 10 i čísla -10. Množina $N = \{1, 2, 5, 10\}$ je množina všech přirozených dělitelů čísla 10 i čísla -10.

Nyní si vysvětlíme význam názvu násobek i dělitel dané-

ho čísla názorně zobrazením celých čísel na číselných osách narýsovaných v obr. 1.



Obr. 1.

Jistě víte, že *číselná osa* je dána, zvolíme-li na přímce *počátek* znázorňující číslo 0 a *jednotkový bod* znázorňující číslo 1. Vzdáleností jednotkového bodu od počátku je určena *délková jednotka*, které užíváme známým způsobem k vyhledání bodů zobrazujících daná reálná čísla. V této knížce budeme se však zajímat jen o obrazy čísel celých.

Na obr. 1 je narýsováno šest navzájem rovnoběžných číselných os, jejichž počátky leží na téže kolmici ke všem osám. Také jednotkové body všech číselných os leží na téže kolmici ke všem osám. Na těchto číselných osách jsou po řadě zobrazeny části množin celých čísel C_m, $m = (1, 2, 3, 4, 5, 6)$. Množiny C_m se skládají z těch celých čísel, jejichž obrazy dostaneme postupným nanášením úsečky o délce m jednotek od počátku v obou navzájem opačných směrech. Body, které zobrazují prvky množin C_m, jsou vyznačeny připsanými číslicemi. Všechna celá čísla, která jsou prvky množiny C_m, jsou násobky přirozeného čísla m i čísla k němu opačného $-m$; každé z čísel množiny C_m je dě-

telné číslem m i číslem $-m$, čili čísla m i $-m$ jsou děliteli každého čísla z množiny C_m.

Sestrojíme-li bodem zobrazujícím číslo 6 na kterékoli číselné ose kolmici ke všem číselným osám, zjistíme, že na ní leží obrazy prvků z množin C_1, C_2, C_3, C_6. Odtud plyne, že čísla 1, 2, 3, 6 jsou přirozenými děliteli čísla 6. Obdobně zjistíme, že na kolmici procházející bodem -4 leží body zobrazující čísla z množin C_1, C_2, C_4, a že tedy čísla 1, 2, 4 jsou přirozenými děliteli čísla -4. Podrobnější úvahou o této grafické metodě k vyhledání přirozených dělitelů daného čísla plyne, že každé celé číslo s výjimkou čísla 0 má jen konečný počet přirozených dělitelů. Číslo 0 má však zřejmě nekonečně mnoho přirozených dělitelů.

Nyní dokážeme několik důležitých vět z teorie dělitelnosti celých čísel.

T_6 *Platí-li pro celá čísla a, b kterýkoli ze čtyř vztahů*

$$b \mid a, \quad -b \mid a, \quad b \mid -a, \quad -b \mid -a,$$

pak platí zároveň všechny ostatní.

Za předpokladu, že platí $b \mid a$ čili $a = bq$, kde q je číslo celé, plyne ihned $a = (-b).(-q)$ čili $-b \mid a$, dále $-a = b.(-q)$ čili $-b \mid a$, dále konečně $-a = (-b).q$ čili $-b \mid -a$.

Z věty T_6 plyne, že vyšetřování kteréhokoli ze čtyř vztahů v ní uvedených můžeme převést na vyšetřování některého ze zbývajících vztahů. To opravdu často činíme tak, že vyšetřujeme platnost vztahu $|b| \mid |a|$, takže zkoumáme vztah dělitelnosti mezi nezápornými celými čísly $|b|$, $|a|$. Přesto většinu vět z nauky o dělitelnosti budeme formulovat pro čísla celá, neboť jejich obecnější význam nám často ušetří hodně práce.

T_7 *Nechť a, b_1, b_2 jsou libovolná celá čísla. Platí-li vztah $b_1 b_2 \mid a$, pak platí i vztahy $b_1 \mid a$, $b_2 \mid a$.*

Předpoklad $b_1 b_2 \mid a$ znamená $a = b_1 b_2\, q$, kde q je číslo celé. Z této rovnosti plyne však ihned $a = b_1.(b_2 q) = b_2.(b_1 q)$ čili $b_1 \mid a$, $b_2 \mid a$.

Kdybychom chtěli větu $\mathbf{T}_7$ vyjádřit použitím slovních rčení, jejichž význam byl definován v $\mathbf{D}_7$, zjistili bychom, že by její zápis byl obšírnější a snad méně přehledný než při použití symbolických zápisů s významem vymezeným v $\mathbf{D}_8$. Výhodou symbolických zápisů je jejich stručnost a přehlednost, jíž bychom dosáhli ještě větší měrou, kdybychom po vytknutí významu písmen a, b_1, b_2 podmínkové souvětí z věty $\mathbf{T}_7$ zapsali symbolicky

$$(b_1 b_2 \mid a) \Rightarrow [(b_1 \mid a) \text{ a } (b_2 \mid a)]. \qquad (2,1)$$

Umluvíme si, že při symbolickém zápisu tohoto druhu je nalevo od značky $\Rightarrow$ zapsán předpoklad matematické věty uvedený v podmínkové větě podmínkového souvětí, napravo od značky $\Rightarrow$ tvrzení obsažené v hlavní větě tohoto podmínkového souvětí, které je logickým důsledkem předpokladu. Po tomto vysvětlení nám bude zřejmé, že zápis

$$[(b_1 \mid a) \text{ a } (b_2 \mid a)] \Rightarrow (b_1 b_2 \mid a) \qquad (2,2)$$

vyjadřuje větu obrácenou k větě (2,1). O důkaz této věty se však nebudeme pokoušet, neboť neplatí, jak je zřejmé z jednoduchého příkladu. Z platných vztahů $6 \mid 120$, $15 \mid 120$ neplyne vztah $6.15 \mid 120$. Matematické věty $\mathbf{T}_7$ budeme často užívat při řešení různých úloh; někdy budeme užívat i obecnější věty, které sami snadno dokážete: Jestliže celé číslo a je násobkem součinu celých čísel $b_1.b_2.b_3 \ldots b_n$, pak je číslo a násobkem každého z čísel $b_1, b_2, b_3, \ldots, b_n$, kde n je libovolné číslo přirozené.

Příklad 1. Je dáno přirozené číslo $a = 2^{45} + 3^{30}$. Dokažte, že platí vztah $17 \mid a$.

Především vás upozorňujeme, že známé Valouchovy *Pětimístné tabulky logaritmické* obsahují tabulky přirozených mocnin 2^n pro přirozená čísla $n \leqq 45$, 3^n pro přirozená čísla $n \leqq 36$ a mocniny jiných přirozených čísel. Takové tabulky jsou užitečné při řešení mnohých úloh z nauky o dělitelnosti čísel. Na konci této knížky je zařazena též tabulka II, která obsahuje mocniny 2^n, 3^n, pro přirozená čísla $n \leqq 25$. Užitím Valouchových tabulek byste mohli řešiti danou úlohu tak, jak to naznačíme:

$$a = 2^{45} + 3^{30} = 35\,184\,372\,088\,832 + \\ + 205\,891\,132\,094\,649 = 241\,075\,504\,183\,481 = \\ = 17 \cdot 14\,180\,912\,010\,793.$$

Z tohoto výsledku podle věty $\mathbf{T}_7$ plyne ihned $17 \mid a$. Užitím vzorce (1,4) rozřešíme úlohu rychleji a bez pracných numerických výpočtů. Platí totiž
$a = 2^{45} + 3^{30} = (2^3)^{15} + (3^2)^{15} = (2^3 + 3^2)(2^{42} - 2^{39} \cdot 3^2 + \\ + \ldots + 3^{28}) = 17\,(2^{42} - 2^{39} \cdot 3^2 + \ldots + 3^{28})$. Odtud ihned dostaneme $17 \mid a$.

Příklad 2. Je dáno přirozené číslo $a = 2^{58} + 1$. Rozložíme číslo a na součin tří přirozených čísel, z nichž každé je větší než 1. Pokusíme se opět použít k řešení úlohy vzorce (1,4). Snadno najdeme

$$a = 2^{58} + 1 = (2^2)^{29} + 1^{29} = (2^2 + 1)(2^{56} - 2^{54} + \\ + \ldots - 2^2 + 1) = 5\,(2^{56} - 2^{54} + \ldots - 2^2 + 1).$$

Dané číslo a má při zápisu v desítkové soustavě 18 cifer, jak si snadno ověříme přibližným výpočtem čísla 2^{58} (použitím logaritmických tabulek). Přitom snadno zjistíme, že druhý činitel součinu dvou čísel, který jsme našli jako rozklad čísla a, má 17 cifer. Proto bychom jen po dlouhém a úmorném výpočtu mohli najít druhého sedmnácticiferného činitele a rozložit ho v součin dvou činitelů, jak to

v roce 1869 provedl francouzský matematik Landry. Ukážeme si nyní, že danou úlohu můžeme rozřešit jinou metodou za několik minut. Snadno vypočteme

$$a = 2^{58} + 1 = 2^2 . 2^{56} + 1 = 4.(2^{14})^4 + 1.$$

Nyní provedeme rozklad tohoto početního výrazu na součin podle vzorce $4x^4 + 1 = (2x^2 - 2x + 1)(2x^2 + 2x + 1)$, a to tak, že v něm za x dosadíme 2^{14}. Dostaneme

$$a = [2.(2^{14})^2 - 2.2^{14} + 1][2.(2^{14})^2 + 2.2^{14} + 1] = \\ = (2^{29} - 2^{15} + 1) . (2^{29} + 2^{15} + 1).$$

Užitím tabulek zjistíme snadno $2^{29} = 536\,870\,912$, $2^{15} = 32\,768$ a konečně tedy
$a = 536\,838\,145 . 539\,903\,681 =$
$= 5 . 107\,367\,629 . 539\,903\,681$. Každé ze tří čísel nalezeného součinu je podle zobecněné věty $\mathbf{T}_7$ dělitelem čísla a.

$\mathbf{T}_8$ *Nechť a, b jsou libovolná celá čísla. Vztahy $a \mid b$, $b \mid a$ platí zároveň, když a jen když $|a| = |b|$.*

Dříve než uvedeme snadný důkaz této věty, která má opět formu podmínkového souvětí, ukážeme její symbolický zápis:

$$(|a| = |b|) \Leftrightarrow [(a \mid b) \text{ a } (b \mid a)]. \qquad (2,3)$$

Umluvíme se, že tento zápis se symbolem $\Leftrightarrow$ znamená to, že zároveň platí tyto věty:

a) $|a| = |b| \Rightarrow [(a \mid b) \text{ a } (b \mid a)]$,

b) $[(a \mid b) \text{ a } (b \mid a)] \Rightarrow |a| = |b|$.

Proto také důkaz poučky $\mathbf{T}_8$ se skládá ze dvou částí.
a) Předpoklad $|a| = |b|$ znamená buď $a = b$ nebo $a = -b$;

ze vztahu $a = b$ plyne $a = b.1$, čili $b \mid a$, a také
$b = a = a.1$, což znamená $a \mid b$.
Vztah $a = -b = b.(-1)$ znamená $b \mid a$, zatímco
$b = -a = a.(-1)$ znamená $a \mid b$.
b) Nechť $a \mid b$, $b \mid a$ platí zároveň. Je-li $a = b = 0$, pak platí $a \mid b$ a též $|a| = |b|$. Kdyby jedno z čísel a, b bylo rovné nule a druhé různé od nuly, pak by jeden ze vztahů $a \mid b$, $b \mid a$ neplatil, a neplatilo by též $|a| = |b|$. Zbývá tedy případ $a \neq 0$, $b \neq 0$. Potom $a \mid b$ znamená $b = aq$, zatímco $b \mid a$ znamená $a = bq'$. Odtud snadno plyne $ab = bq'.aq$ a po zkrácení $qq' = 1$. To však znamená buď $q = q' = 1$ čili $a = b$, nebo $q = q' = -1$, čili $a = -b$. Platí-li $a = b$ nebo $a = -b$, znamená to $|a| = |b|$. Zamyslíme-li se nad stavbou věty zapsané v (2,3) užitím symbolu $\Leftrightarrow$, zjistíme, že vztahy uvedené po obou stranách tohoto symbolu buď zároveň platí, nebo zároveň neplatí. V podmínkovém souvětí věty $\mathbf{T}_8$ je to vyjádřeno slovy „když a jen když“, která bychom mohli nahradit též slovy „právě když“.

$\mathbf{T}_9$ *Jestliže pro celá čísla* a_1, a_2, b *platí zároveň* $b \mid a_1$, $b \mid a_2$, *pak platí též* $b \mid c_1a_1 + c_2a_2$, *ať jsou* c_1, c_2 *jakákoli celá čísla.*

Předpoklad $b \mid a_1$ znamená $a_1 = bq_1$, předpoklad $b \mid a_2$ znamená $a_2 = bq_2$, kde q_1, q_2 jsou celá čísla. Z platnosti těchto rovností plyne však $c_1a_1 + c_2a_2 = c_1bq_1 + c_2bq_2 = b(c_1q_1 + c_2q_2)$, což však znamená $b \mid c_1a_1 + c_2a_2$. Poučky $\mathbf{T}_9$ užíváme často se speciální volbou $c_1 = 1$, $c_2 = 1$, nebo $c_1 = 1$, $c_2 = -1$. V tom případě plyne z poučky $\mathbf{T}_9$ tento důsledek:

Je-li číslo b *dělitelem celých čísel* a_1, a_2, *pak je* b *dělitelem součtu i rozdílu čísel* a_1, a_2.

Je snadné dokázat i větu obecnější, než je $\mathbf{T}_9$:

Je-li celé číslo b *dělitelem celých čísel* $a_1, a_2, a_3, \ldots, a_n$,

pak je b dělitelem též součtu libovolných násobků čísel a_1, a_2, a_3, ..., a_n, *ať je n jakékoli přirozené číslo.*

Dříve než si na několika příkladech ukážeme užití věty $\mathbf{T_9}$ při řešení některých úloh z teorie dělitelnosti celých čísel, připomeneme ještě, že při zkoumání dělitelnosti součtu daných čísel počet sčítanců zvětšujeme přidáním dvou dalších vhodně volených sčítanců, které jsou navzájem čísly opačnými, a pak teprve sčítance vhodně sdružujeme a částečné součty rozkládáme na součiny. Často se osvědčuje přičtení $+ 1 - 1$, neboť číslo 1 má užitečnou vlastnost, že $1^n = 1$ pro každé celé číslo n.

Příklad 3. Je dáno číslo $a = 99^{61} - 50^{56}$. Dokažte, že $49 \mid a$.

Platí $a = 99^{61} - 50^{56} + 1 - 1 = (99^{61} - 1) - (50^{56} - 1) = (99 - 1) \cdot (99^{60} + 99^{59} + \ldots + 1) - (50 - 1) \cdot (50^{55} + 50^{54} + \ldots + 1) = 2 \cdot 49\,(99^{60} + 99^{59} + \ldots + 1) - 49\,(50^{55} + 50^{54} + \ldots + 1)$. Menšenec i menšitel tohoto rozdílu je dělitelný 49 (podle věty $\mathbf{T_7}$), a proto i jejich rozdíl je dělitelný číslem 49 (podle věty $\mathbf{T_9}$).

Příklad 4. Je dáno přirozené číslo $a = 103^{53} + 53^{103}$. Dokažte, že pro číslo a platí tyto vztahy: a) $3 \mid a$, b) $4 \mid a$, c) $13 \mid a$.

Platí $a = 103^{53} + 53^{103} = (103^{53} + 1) + (53^{103} - 1) = (103 + 1)\,(103^{52} - 103^{51} + \ldots - 103 + 1) + (53 - 1)\,(53^{102} + 53^{101} + \ldots + 1) = 2.4.13.\,(103^{52} - 103^{51} + \ldots - 103 + 1) + 4.13\,(53^{102} + 53^{101} + \ldots + 1)$.

Poněvadž každý sčítanec upraveného součtu je dělitelný čísly 4 a 13, je i jejich součet dělitelný čísly 4 i 13.

Dále platí též:

$a = (103^{53} - 1) + (53^{103} + 1) = (103 - 1) \cdot (103^{52} +$

$+ 103^{51} + \ldots + 1) + (53 + 1) \cdot (53^{102} - 53^{101} + \ldots - 53 + 1) = 3.34\,(103^{52} + 103^{51} + \ldots + 1) + 3.18\,(53^{102} - 53^{101} + \ldots + 1)$.
Poněvadž každý sčítanec tohoto součtu je dělitelný číslem 3, je i jejich součet dělitelný číslem 3. (Důsledky: viz větu $\mathbf{T}_{32}$.)

Příklad 5. Dokažte, že pro každé celé číslo $n \geq 0$ je přirozené číslo $a_n = 5^{2n} + 11.2^{n+1}$ násobkem čísla 23.

Početní výraz pro číslo a_n upravíme takto:

$$a_n = 5^{2n} + 11.2^{n+1} = 5^{2n} + 11.2.2^n = 5^{2n} + 22.2^n = 5^{2n} - 2^n + 2^n + 22.2^n = (25^n - 2^n) + 23.2^n.$$

Za předpokladu, že $n > 1$, můžeme užíti vzorce (1,3) pro rozklad $25^n - 2^n = (25 - 2)\,(25^{n-1} + 25^{n-2}.\,2 + \ldots + 2^{n-1}) = 23q_n$, kde q_n je celé číslo. Platí tedy stále za předpokladu $n > 1$, že $a_n = 23 \cdot q_n + 23 \cdot 2^n = 23\,(q_n + 2^n)$; to však znamená, že $23 \mid a_n$ pro $n > 1$. Dále pro $n = 0$ dostaneme $a_0 = 23$ a pro $n = 1$ dostaneme $a_1 = 69 = 3 \cdot 23$; proto $23 \mid a_0$ i $23 \mid a_1$. Shrnutím všech výsledků úvah dostáváme $23 \mid a_n$ pro každé celé číslo $n \geq 0$.

Příklad 6. Dokažte, že pro každé přirozené číslo n je $a_n = 5^{2n+1}.\,2^{n+2} + 3^{n+2}.\,2^{2n+1}$ násobkem čísla 76.

Pro číslo a_n najdeme postupnými úpravami:

$$\begin{aligned} a_n &= 5^{2n+1}.\,2^{n+2} + 3^{n+2}.\,2^{2n+1} = \\ &= 2^{n+1}\,(5^{2n}.5.2 + .3^n.3^2.2^n) = \\ &= 2^{n+1}\,(10 \cdot 5^{2n} + 9 \cdot 6^n) = \\ &= 2^{n+1}\,(10 \cdot 25^n - 10 \cdot 6^n + 10 \cdot 6^n + 9 \cdot 6^n) = \\ &= 2^{n+1}\,[10\,(25^n - 6^n) + 19 \cdot 6^n]. \end{aligned}$$

Za předpokladu $n > 1$ můžeme použít vzorce (1,3) pro rozklad. $25^n - 6^n = (25 - 6)\,(25^{n-1} + 25^{n-2} \cdot 6 + \ldots$

$+ \ldots + 6^{n-1}) = 19\, q_n$, kde q_n je celé číslo. Po dosazení do posledního početního výrazu dostaneme pro $n > 1$:
$a_n = 2^{n+1}(19\, q_n + 19 \cdot 2^n) = 2^{n-1} \cdot 2^2 \cdot 19\,(q_n + 2^n) = 76 \cdot 2^{n-1} \cdot (q_n + 2^n)$. Za předpokladu $n > 1$ platí tedy $76 \mid a_n$. Pro $n = 1$ dostaneme dosazením do výrazu $a_n = 5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$ výsledek $a_1 = 5^3 \cdot 2^3 + 3^3 \cdot 2^3 = 1216 = 76 \cdot 16$, odkud plyne $76 \mid a_1$. Platí tedy $76 \mid a_n$ pro všechna přirozená čísla $n \geqq 1$.

T_{10} *Nechť a_1, a_2, b jsou celá čísla. Jestliže $b \mid a_1$, pak $b \mid a_1 + a_2$ právě tehdy, když $b \mid a_2$.*

Pro lepší pochopení věty T_{10} (zahrnující vlastně dvě poučky) i jejího důkazu naznačíme stavbu této věty symbolickým zápisem

$$(b \mid a_1) \Rightarrow [(b \mid a_2) \Leftrightarrow (b \mid a_1 \pm a_2)].$$

Tento výrok však platí právě tehdy, když platí zároveň tvrzení $(b \mid a_1) \Rightarrow [(b \mid a_2) \Rightarrow (b \mid a_1 \pm a_2)]$, $(b \mid a_1) \Rightarrow [(b \mid a_1 \pm a_2) \Rightarrow (b \mid a_2)]$, která snadno dokážeme.

a) Platí-li $b \mid a_1$, pak z platnosti $b \mid a_2$ plyne podle věty T_9 platnost vztahu $b \mid a_1 \pm a_2$.

b) Platí-li $b \mid a_1$, pak z platnosti $b \mid a_1 \pm a_2$ plyne podle věty T_9 platnost vztahu $b \mid (a_1 \pm a_2) - a_1$ čili $b \mid \pm a_2$, tj. zejména $b \mid a_2$.

Příklad 7. Najděte všechna celá čísla x, pro která číslo $y = x^3 + 14$ je dělitelné číslem $x + 2$.

Platí $y = x^3 + 14 = x^3 + 2^3 + 6 =$
$= (x + 2)(x^2 - 2x + 4) + 6$.

Poznámka: Téhož výsledku bychom dosáhli, kdybychom mnohočlen 3. stupně $x^3 + 14$ dělili lineárním mnohočlenem $x + 2$ a přitom stanovili neúplný podíl $x^2 - 2x + 4$

se zbytkem 6. Pak bychom podle známého vztahu mezi dělencem, dělitelem, neúplným podílem a zbytkem mohli napsat

$$y = (x^2 - 2x + 4)(x + 2) + 6.$$

Číslo y je součtem dvou čísel, z nichž první je dělitelné číslem $x + 2$, a proto y bude dělitelné číslem $x + 2$, právě když tímto číslem bude dělitelný druhý sčítanec 6. Číslo 6 má však jen 8 dělitelů $d = \pm 1, \pm 2, \pm 3, \pm 6$. Řešením rovnic $x + 2 = d$ dostaneme prvky množiny všech řešení $x \in \{-8, -5, -4, -3, -1, 0, 1, 4\}$.

Příklad 8. Najděte všechna celá čísla x, pro která celé číslo $y = x^3 + x^2 + 1$ je násobkem celého čísla $x^2 + 2x + 3$.

Provedeme-li dělení $(x^3 + x^2 + x + 1) : (x^2 + 2x + 3)$, najdeme neúplný podíl $x - 1$ a zbytek -4. Proto platí $y = (x^2 + 2x + 3)(x - 1) - 4$. Číslo y je rozdílem dvou čísel, z nichž menšenec je násobkem čísla $x^2 + 2x + 3$. Podle věty $\mathbf{T}_{10}$ bude číslo y násobkem čísla $x^2 + 2x + 3$, právě když také menšenec 4 bude násobkem čísla $x^2 + 2x + 3$. Číslo 4 může však být násobkem jen čísel $d = \pm 1, \pm 2, \pm 4$. Avšak rovnice $x^2 + 2x + 3 = d$ má celočíselný kořen $x = -1 \pm \sqrt{d - 2}$ jen pro $d = 2$. Proto $x = -1$ je jediné číslo celé, které vyhovuje podmínce stanovené úlohou.

Cvičení

2,1. Dokažte platnost těchto vztahů: a) $3 \mid 41^{97} - 26^{79}$; b) $5 \mid 41^{97} - 26^{79}$; c) $30 \mid 61^{29} + 89^{23}$; d) $4 \mid 101^{103} + 103^{101}$; e) $51 \mid 101^{103} + 103^{101}$; f) $19 \mid 56^{41} - 37^{31}$.

2,2. Dokažte, že pro celá čísla $n \geq 0$ platí

a) $17 \mid 5^{2n} + 2^{3n+4}$; b) $23 \mid 3^{3n} - 3 \cdot 2^{2n+3}$.

2,3. Rozložte číslo $2^{42} + 1$ v součin tří přirozených čísel, z nichž každé je větší než 1.

2,4. Pro která celá čísla x je číslo $y = x^4 - x^3 + 4x^2 + 3x + 21$ násobkem čísla $x^2 + x + 1$?

2,5. Za předpokladu, že a_1, a_2, b_1, b_2 jsou čísla celá, dokažte:

a) $[(b_1 \mid a_1)$ a $(b_2 \mid a_2)] \Rightarrow (b_1 b_2 \mid a_1 a_2)$;

b) $[(b_2 \mid b_1)$ a $(b_1 \mid a_1)] \Rightarrow (b_2 \mid a_1)$;

c) $(b_1 \mid a_1) \Rightarrow b_1 \mid a_1 a_2$.

Symbolicky zapsané věty vyjádřete slovy s použitím termínů vymezených v definici $\mathbf{D}_7$. Na vhodně volených číselných příkladech ukažte, že obrácené věty k výše uvedeným větám neplatí.

2,6. Jsou dána čísla $a = 3^{16} + 3^8 + 1$, $b = 4.3^{16} + 1$. Užitím tabulek mocnin 3^n (tab. II.) najděte zápisy čísel a, b v desítkové soustavě a ukažte též, že obě čísla a, b lze rozložit na součin aspoň dvou přirozených čísel větších než 1.

3. kapitola

VYŠETŘOVÁNÍ DĚLITELNOSTI CELÝCH ČÍSEL

Na obr. 1 v kap. 2 jsme ukázali princip znázornění množin celých čísel $C_1, C_2, C_3, C_4 \ldots$ tak, že prvky množiny C_m byly vyznačeny na číselné ose číslicovým označením těch bodů, které jsou obrazy násobku přirozeného čísla m. Tak např. z množiny C_4 jsou na číselné ose zobrazující část množiny C_4 výrazně vyznačeny body odpovídající celým číslům $\ldots -4, 0, 4, 8, 12, 16, \ldots$, obecně číslům $4q$, kde q je libovolné číslo celé. Označme nyní ${}^1C_4$ množinu všech čísel celých, jejichž obrazy jsou na číselné ose zobrazující množinu C_4 ve vzdálenosti jedné délkové jednotky vpravo od každého čísla $4q$. Bude to množina čísel, jejímiž prvky jsou čísla, vyjádřená početním výrazem $4q + 1$, kde proměnná q zastupuje libovolné číslo celé. Dále označme ${}^2C_4$ množinu všech celých čísel, jejichž obrazy leží ve vzdálenosti dvou jednotek od obrazů čísel $4q$; bude to množina čísel vyjádřených početním výrazem $4q + 2$. Konečně do množiny ${}^3C_4$ zařaďme všechna čísla celá, která lze vyjádřit ve tvaru $4q + 3$. V zájmu jednotného způsobu označení všech množin, o nichž budeme dále jednat, použijeme symbolu ${}^0C_4$ místo C_4.

Tímto způsobem jsme množinu všech celých čísel rozdělili na části, jimiž jsou
množina ${}^0C_4$, obsahující čísla $\ldots -8, -4, 0, 4, 8, 12, 16, \ldots$, obecně $4q$,
množina ${}^1C_4$, obsahující čísla $\ldots -7, -3, 1, 5, 9, 13, 17,$

..., obecně $4q + 1$,
množina ${}^2C_4$, obsahující čísla ... $-6, -2, 2, 6, 10, 14, 18,$
..., obecně $4q + 2$,
množina ${}^3C_4$, obsahující čísla ... $-5, -1, 3, 7, 11, 15, 19,$
..., obecně $4q + 3$.

Z obr. 1 i z tohoto schématu je zřejmé, že každé celé číslo je zařazeno právě do jedné z množin ${}^0C_4$, ${}^1C_4$, ${}^2C_4$, ${}^3C_4$. Rozhodnutí o tom, do které množiny ${}^rC_4$ ($r = 0, 1, 2, 3$) patří nějaké dané číslo a, ať je kladné nebo záporné, usnadní nám dělení čísla a číslem 4. Číslo $88 = 4.22$ i číslo $-88 = 4.(-22)$ patří zřejmě do množiny ${}^0C_4$. Tato množina obsahuje s každým číslem a, které do ní patří, i opačné číslo $-a$. Máme-li rozhodnout o nějakém čísle, které není násobkem 4, do které z množin ${}^1C_4$, ${}^2C_4$, ${}^3C_4$ patří, pomůže nám opět dělení se zbytkem, jímž musí být jedno z čísel 1, 2, 3. To znamená, že vyhledáme ke zkoumanému číslu nejblíže nižší násobek čísla 4 a pak zjistíme, které z kladných čísel 1, 2, 3 je nutno přičíst k vyhledanému násobku, abychom dostali vyšetřované číslo. Tak např. $47 = 4.11 + 3$ a proto $47 \in {}^3C_4$, zatímco $-47 = 4.(-12) + 1$ a proto $-47 \in {}^1C_4$. Všimněte si dobře, že v množinách ${}^1C_4$, ${}^2C_4$, ${}^3C_4$ se nevyskytují dvojice čísel navzájem opačných; jinak řečeno: dvě čísla opačná, která nejsou násobkem čísla 4, nepatří nikdy zároveň do jedné z množin ${}^1C_4$, ${}^2C_4$, ${}^3C_4$.

Obdobně při volbě např. $m = 5$ můžeme množinu všech celých čísel rozdělit na 5 částí, které postupně označíme ${}^0C_5$, ${}^1C_5$, ${}^2C_5$, ${}^3C_5$, ${}^4C_5$. Přitom do množiny ${}^rC_5$ zahrnujeme všechna celá čísla, která jsou funkčními hodnotami lineární funkce $5t + r$, kde proměnná t může nabývat libovolné celočíselné hodnoty a r je některé z čísel 0, 1, 2, 3, 4. Procvičením si sami ověřte, že platí vztahy $17 \in {}^2C_5$, $-13 \in {}^2C_5$, $75 \in {}^0C_5$, $0 \in {}^0C_5$, $-29 \in {}^1C_5$, $29 \in {}^4C_5$, $48 \in {}^3C_5$ apod. Označení proměnné písmenem t má jen

ten smysl, abyste si zvykali na označení proměnné různými písmeny. Zvlášť často se setkáme s rozdělením množiny všech čísel celých na dvě části ${}^0C_2$, do níž patří všechny funkční hodnoty lineární funkce $2k$ a ${}^1C_2$, do níž patří všechny funkční hodnoty funkce $2k + 1$, kde k je proměnná označující libovolný prvek množiny všech celých čísel. Jistě vidíte, že naznačeným způsobem by bylo možno definovat význam názvu číslo sudé a číslo liché.

$\mathbf{T}_{11}$ *Ke každému celému číslu a a ke každému přirozenému číslu m existuje jediná dvojice takových celých čísel q, r, že platí vztahy $a = mq + r$, $0 \leqq r < m$.*

Úvodní výklad tohoto článku měl vás připravit pro pochopení významu věty $\mathbf{T}_{11}$, kterou nebudeme dokazovat. Bylo by též možné zobecnit větu $\mathbf{T}_{11}$ tak, abychom za číslo m mohli volit nejen libovolné číslo přirozené, ale i číslo opačné ke kterémukoli číslu přirozenému. Neučiníme to, neboť význam takto zobecněné věty by byl jen teoretický a nijak by nepřispěl k tomu, abychom tím získali lepší prostředky pro řešení úloh z teorie dělitelnosti celých čísel. Místo toho vyslovíme větu $\mathbf{T}_{12}$, bez níž bychom se mohli také obejít. Její užití místo věty $\mathbf{T}_{11}$ nám však často pomůže zkrátit řešení úlohy.

$\mathbf{T}_{12}$ *Ke každému celému číslu a a ke každému přirozenému číslu m existuje jediná dvojice takových celých čísel q, r, že platí vztahy $a = mq + r$, $-\frac{1}{2}m < r < \frac{1}{2}m$ při lichém m a při sudém m ještě právě jeden ze vztahů $r = \pm\frac{1}{2}m$, podle toho, který z nich je podle naší volby přípustný.*

Užitím věty $\mathbf{T}_{12}$ můžeme každé celé číslo a vyjádřit jako

součet násobku čísla m, který je nejbližší číslu a, a čísla r, o němž platí $|r| < \frac{1}{2}m$, je-li m liché. Je-li m sudé, pak k číslu a existují dva nejbližší a přitom stejně blízké násobky čísla m, a proto čísla q, r budou jednoznačně určena jen tím, že v tomto případě budeme užívat pouze jednoho předem určeného nejbližšího násobku čísla m, který leží nejblíže číslu a. Prakticky to znamená rozhodnout předem, kdy připustíme jednu z rovností $r = \frac{1}{2}m$ nebo $r = -\frac{1}{2}m$.

Je-li $r = 0$, pak q je podíl, který dostaneme při dělení čísla a číslem m. Je-li $r \neq 0$, pak q se nazývá neúplný podíl při tzv. dělení se zbytkem, jímž je právě číslo r. Pro stručnost budeme v této knížce názvem dělení označovat vždy takovou početní operaci, při níž podíl q (ať úplný nebo neúplný) je číslo celé a zbytek r vyhovuje některé z podmínek uvedených ve větách $\mathbf{T}_{11}$ a $\mathbf{T}_{12}$. Místo toho, abychom říkali, že určujeme „zbytek čísla a při dělení číslem m“, budeme říkat, že určujeme „zbytek čísla a podle modulu m“; k zápisu slov „podle modulu m“ užíváme zápisu „(mod m)“.

Podstatou rozdílu v rozkladech čísla a na součet $mq + r$ podle vět $\mathbf{T}_{11}$ a $\mathbf{T}_{12}$ je to, že v prvém případě připouštíme pro číslo r jen nezáporné hodnoty 0, 1, 2, 3, 4, ..., $m-1$, zatímco ve druhém případě nám jde o vyjádření součtem $mq + r$, při němž $|r|$ nepřevyšuje $\frac{1}{2}m$. Ve větě $\mathbf{T}_{11}$ užíváme soustavy nezáporných zbytků, zatímco ve větě $\mathbf{T}_{12}$ je užito soustavy absolutně nejmenších zbytků.

Užití věty $\mathbf{T}_{12}$ ukážeme ještě na číselných příkladech. Při volbě $m = 5$ můžeme každé celé číslo vyjádřit jako funkční hodnotu jedné z těchto lineárních funkcí: $5k - 2$, $5k - 1$, $5k$, $5k + 1$, $5k + 2$. Jejich funkční hod-

noty tvoří množiny celých čísel ${}^{-2}C_5, {}^{-1}C_5, {}^{0}C_5, {}^{1}C_5, {}^{2}C_5$ vymezené tak, že do množiny ${}^{r}C_m$ patří všechna celá čísla tvaru $mq + r$, kde q je libovolné celé číslo. Při volbě $m = 4$ bude možno každé celé číslo vyjádřit jako funkční hodnotu jedné z lineárních funkcí buď ze skupiny $4k - 1$, $4k$, $4k + 1$, $4k + 2$, nebo ze skupiny $4k - 2$, $4k - 1$, $4k$, $4k + 1$. Při volbě $m = 2$ můžeme všechna celá čísla rozdělit do dvou množin jedním z těchto způsobů: a) ${}^{0}C_2$ pro čísla tvaru $2k$, ${}^{1}C_2$ pro čísla tvaru $2k + 1$; b) ${}^{0}C_2$ pro čísla tvaru $2k$, ${}^{-1}C_2$ pro čísla tvaru $2k - 1$. Rozdíl obojího dělení tkví jen v označení množin a ve vyjádření jejich prvků lineárními funkcemi. Umluvíme si též, že rčení „číslo tvaru $mx + r$“ budeme užívat místo obšírného vyjádření „číslo, které je funkční hodnotou lineární funkce $mx + r$“, kde x je proměnná v oboru celých čísel a m, r jsou daná čísla, a že množinu ${}^{r}C_m$ budeme nazývat zbytkovou třídou celých čísel se zbytkem r podle modulu m.

Jestliže některá soustava zbytkových tříd ${}^{r}C_m$ má tu vlastnost, že každé celé číslo náleží právě do jedné ze zbytkových tříd soustavy, pak říkáme, že tvoří úplnou soustavu zbytkových tříd. Příkladem takové úplné soustavy zbytkových tříd podle modulu m je soustava množin

$$ {}^{0}C_m, {}^{1}C_m, {}^{2}C_m, {}^{3}C_m, \ldots, {}^{m-1}C_m, \qquad (3,1) $$

do nichž patří celá čísla, která při dělení číslem m dávají zbytky

$$ 0, 1, 2, 3, \ldots, m-1, \qquad (3,2) $$

o nichž též říkáme, že tvoří úplnou soustavu zbytků.

Při řešení některých úloh budeme užívat i jiných úplných soustav zbytkových tříd, jejichž příklady jsme už ukázali v předcházejícím textu. Při důkazech následujících matematických vět budeme však užívat vždy úplné soustavy zbytkových tříd (3,1), pokud nebude nic jiného poznamenáno.

$\mathbf{T}_{13}$ *Dvě celá čísla patří do téže zbytkové třídy* ${}^{r}C_m$ *právě tehdy, když jejich rozdíl je násobkem čísla* m.

Dvě celá čísla a_1, a_1' jsou prvky téže množiny ${}^{r}C_m$, jestliže o nich platí $a_1 = mk_1 + r_1$, $a_1' = mk_1' + r_1$. Jejich rozdíl $a_1 - a_1' = (mk_1 + r_1) - (mk_1' + r_1) = m(k_1 - k_1')$. Odtud však ihned plyne $m \mid a_1 - a_1'$. Nejsou-li dvě čísla a_1, a_2 prvky téže zbytkové třídy (mod m), pak musí platit $a_1 = mk_1 + r_1$, $a_2 = mk_2 + r_2$, kde $r_1 \neq r_2$. Platí pak $a_1 - a_2 = (mk_1 + r_1) - (mk_2 + r_2) = m(k_1 - k_2) + (r_1 - r_2)$. Podle předpokladu $r_1 - r_2 \neq 0$ a přitom $|r_1 - r_2| < m$, neboť $r_1 < m$, $r_2 < m$.

$\mathbf{T}_{14}$ *Je-li dáno* m *po sobě jdoucích celých čísel, pak právě jedno z nich je násobkem čísla* m *a přitom jejich součin je též násobkem čísla* m.

Označíme-li a první člen posloupnosti m po sobě jdoucích celých čísel, pak tato posloupnost má členy:

$$a, a + 1, a + 2, a + 3, \ldots, (a + m - 1). \qquad (3,3)$$

Mezi prvním a posledním členem je rozdíl $m - 1$ a rozdíl mezi kterýmikoli dvěma členy posloupnosti (3,3) nemůže být větší než $m - 1$. Proto žádná dvě čísla z posloupnosti (3,3) nemohou náležet do téže zbytkové třídy ${}^{r}C_m$, neboť jejich rozdíl by musil být m. Jestliže tedy všechny členy posloupnosti (3,3) jsou různá čísla, pak každé z nich patří do jedné ze zbytkových tříd úplné soustavy ${}^{r}C_m$ (3,1), a tedy jedno z nich také do třídy ${}^{0}C_m$, což znamená, že je násobkem čísla m. Je-li však nějaké číslo násobkem m, pak i každý jeho násobek je násobkem čísla m. Součin všech členů posloupnosti (3,3) je však násobkem některého čísla, které je dělitelné číslem m.

Příklad 9. Dokažte, že $y = x^3 + 5x - 6$ je číslo dělitelné čísly 2 i 3, ať je x kterékoli celé číslo.

Užitím vět, které již známe, můžeme provést důkaz dvojím způsobem:

1) Abychom dokázali $2 \mid y$, budeme postupně předpokládat, že x patří do zbytkových tříd ${}^0C_2$, ${}^1C_2$, které tvoří úplnou soustavu zbytkových tříd, tj. že platí $x = 2k$ nebo $x = 2k + 1$, kde k je libovolné číslo celé. V prvém případě dostaneme $y = (2k)^3 + 5.2k - 6 = 2(4k^3 + 5k - 3)$.

Ve druhém případě $y = (2k + 1)^3 + 5(2k + 1) + 6 = 2(4k^3 + 6k^2 + 8k + 6)$. Z obou těchto výsledků tedy plyne $2 \mid y$. Abychom dokázali $3 \mid y$, budeme předpokládat, že x může být prvkem kterékoli z množin ${}^{-1}C_3$, ${}^0C_3$, ${}^1C_3$, které tvoří též úplnou soustavu zbytkových tříd. Předpokládáme-li $x = 3k - 1$, dostaneme po snadné úpravě $y = 3(9k^3 - 9k^2 + 8k - 4)$; předpokládáme-li $x = 3k$, dostaneme $y = 3(9k^3 + 5k - 2)$; předpokládáme-li $x = 3k + 1$, dostaneme $y = 3(9k^3 + 9k^2 + 8k)$. Z těchto výsledků však plyne $3 \mid y$.

2) Jiný způsob řešení dané úlohy nám umožní vhodný rozklad čísla y na dva sčítance, o nichž lze snadno rozhodnout, že jsou násobky čísel 2 i 3.

$y = x^3 + 5x - 6 = x^3 - x + x + 5x + 6 =$
$= x(x^2 - 1) + 6x - 6 = (x - 1)x(x + 1) + 2.3(x - 1)$.
První sčítanec je dělitelný čísly 2 i 3 podle věty $\mathbf{T}_{14}$, druhý sčítanec podle věty $\mathbf{T}_7$. Jejich součet je proto též dělitelný čísly 2 i 3 podle věty $\mathbf{T}_9$.

Příklad 10. Najděte všechna celá čísla x, pro něž platí $5 \mid y$, když $y = 4x^2 + 1$.

Vyšetřujeme všechny možné případy, kdy $x \in {}^rC_5$ pro $r = 0, \pm 1, \pm 2$. Je-li $x = 5k$, pak $y = 4.(5k)^2 + 1 =$
$= 4.5^2.k^2 + 1$. V tomto případě podle věty $\mathbf{T}_{10}$ neplatí $5 \mid y$.

Je-li $x = 5k \pm 1$, pak $y = 4(5k \pm 1)^2 + 1 =$
$= 4.25k^2 \pm 4.2.5.k + 4 + 1 = 5(4.5k^2 \pm 4.2k + 1)$;

v tomto případě platí $5 \mid y$. Je-li $x = 5k \pm 2$, pak $y = 4.(5k \pm 2)^2 + 1 = 5(4.5k^2 \pm 16k) + 17$; poněvadž první sčítanec je a druhý není dělitelný 5, neplatí $5 \mid y$ podle věty $\mathbf{T}_{10}$. Podmínce stanovené v úloze vyhovují jen celá čísla $x \in {}^{-1}C_5$ nebo $x \in {}^{1}C_5$; stručněji: x musí být prvkem sjednocení množin ${}^{-1}C_5$, ${}^{+1}C_5$, tj. číslem z množiny $\ldots -6, -4, -1, 1, 4, 6, 9, 10 \ldots$

$\mathbf{T}_{15}$ *Označíme-li* a_i, a_i' *dvě libovolná celá čísla patřící do téže zbytkové třídy* ${}^{i}C_m$ *pro* $i = 1, 2, 3, \ldots, n$, *pak součty* $s = a_1 + a_2 + a_3 + \ldots + a_n$, $s' = a_1' + a_2' + a_3' + \ldots + a_n'$, $\bar{s} = r_1 + r_2 + r_3 + \ldots + r_n$ *jsou prvky téže zbytkové třídy* ${}^{r}C_m$.

Napíšeme-li všechny sčítance součtu s ve tvaru $a_1 = mk_1 + r_1$, $a_2 = mk_2 + r_2$, $\ldots$ $a_n = mk_n + r_n$, potom podle předpokladu pro všechny sčítance součtu s' platí $a_1' = mk_1' + r_1$, $a_2' = mk_2' + r_2$, $\ldots$, $a_n' = mk_n' + r_n$. Tvrzení $\bar{s} \in {}^{r}C_m$ znamená $\bar{s} = mk + r$. Poněvadž platí $s = (mk_1 + r_1) + (mk_2 + r_2) + \ldots + (mk_n + r_n) = m(k_1 + k_2 + \ldots + k_n) + (r_1 + r_2 + \ldots + r_n) = m(k_1 + k_2 + \ldots + k_n) + mk + r = m(k_1 + k_2 + \ldots + k_n + k) + r$, resp. při obdobné úpravě $s' = m(k_1' + k_2' + k_3' + \ldots + k_n' + k') + r$, $\bar{s} = mk + r$, plyne odtud, že s, s', $\bar{s}$ patří do téže zbytkové třídy ${}^{r}C_m$.

Máme-li tedy najít zbytek součtu celých čísel (na nějž lze převést i každý rozdíl) při dělení číslem m, pak toto zkoumání můžeme převést na vyšetřování zbytků jiných součtů, jako např. součtů s' nebo $\bar{s}$ s významem popsaným v $\mathbf{T}_{15}$. Ukážeme to na číselných příkladech.

Příklad 11. Určete zbytky součtů a) $s = 9923 + 4537 + 1965 + 2879$ při dělení číslem 9; b) $s = 859 - 731 + 708 - 636$ při dělení číslem 7.

a) Místo součtu $s = 9923 + 4537 + 1965 + 2879$ můžeme vyšetřit součet $s' = 23 + 37 + 165 + 179$, jehož sčítance vznikly ze sčítanců součtu s zmenšených o zřejmé násobky čísla 9, nebo součet $\bar{s} = 5 + 1 + 3 + 8$. Můžete se přesvědčit, že všechna tři čísla $s, s', \bar{s}$ dávají při dělení 9 týž nezáporný zbytek 8, tj. všechny tři součty $s, s', \bar{s}$, jsou čísla náležející do zbytkové třídy ${}^{8}C_{9}$.

b) Místo $s = 859 - 731 + 708 - 636$ můžeme vyšetřovat součet $s' = 159 - 31 + 8 - 6$ nebo součet $\bar{s} = 5 - 3 + 1 - 6$. Ve všech případech zjistíme, že při dělení součtů $s, s', \bar{s}$ číslem 7 dostaneme vždy zbytek 4, tj. všechna čísla $s, s', \bar{s}$ jsou prvky zbytkové třídy ${}^{4}C_{7}$.

T$_{16}$ *Označíme a_i, a_i' dvě libovolná celá čísla patřící do téže zbytkové třídy ${}^{r_i}C_m$, pro $i = 1, 2, 3, \ldots, n$, pak součiny $s = a_1 a_2 a_3 \ldots a_n, s' = a_1', a_2', a_3' \ldots a_n', \bar{s} = r_1 r_2 r_3 \ldots r_n$ jsou prvky téže zbytkové třídy ${}^{r}C_m$.*

Součiny $s = (mk_1 + r_1).(mk_2 + r_2) \ldots (mk_n + r_n)$
a $s' = (mk_1' + r_1).(mk_2' + r_2, \ldots (mk_n' + r_n)$
se po provedeném násobení změní na součty 2^n sčítanců, z nichž $2^n - 1$ sčítanců jsou součiny s činitelem m, které při dělení číslem m dávají zbytek 0, zatímco jediný součin $r_1 r_2 \ldots r_n$ neobsahuje činitele m. Podle věty **T**$_{15}$ najdeme však zbytek při dělení zmíněných součtů číslem m tím, že vyšetříme zbytek při dělení sčítance $r_1 r_2 \ldots r_n = \bar{s}$.

Příklad 12. Je dáno číslo $s = 859.731.708.636$. Je třeba rozhodnout, zda číslo s je dělitelné 7, a zároveň určit a) nejmenší nezáporný zbytek, b) absolutně nejmenší zbytek při dělení čísla s číslem 7.

Místo čísla s vyšetříme číslo $\bar{s} = 5.3.1.6 = 90$. Při dělení tohoto čísla číslem 7 dostaneme nejmenší nezáporný

zbytek 6, z čehož plyne, že neplatí $7 \mid s$. Z celých čísel, která zároveň s číslem 6 patří do zbytkové třídy ${}^{6}C_{7}$, má nejmenší absolutní hodnotu číslo -1, které je absolutně nejmenším zbytkem při dělení daného čísla se zbytkem. Přestože jsme neprovedli numerický výpočet součinu s, můžeme tvrdit, že číslo s je tvaru $7k - 1$ nebo $7k' + 6$, kde k a $k' = k - 1$ jsou celá čísla.

$\mathbf{T}_{17}$ *Je-li n číslo přirozené a a_1 celé číslo tvaru $mk_1 + r_1$, pak mocniny a_1^n i r_1^n patří do téže zbytkové třídy ${}^{r}C_{m}$.*

Platnost této věty plyne ihned z předcházející věty $\mathbf{T}_{16}$, když v ní položíme $a_1 = a_2 = a_3 = \ldots = a_n$, $r_1 = r_2 = r_3 = \ldots = r_n$. Známe-li binomickou větu, můžeme poučku $\mathbf{T}_{17}$ dokázat i jinak. Mocninu $a_1^n = (mk_1 + r_1)^n$ můžeme podle binomické věty napsat ve tvaru součtu

$$(mk_1)^n + \binom{n}{1}(mk_1)^{n-1}.r_1 + \binom{n}{2}(mk_1)^{n-2}.r_1^2 + \ldots +$$

$$+ \binom{n}{n-1} mk_1.r_1^{n-1} + r_1^n.$$

Každý ze sčítanců (kromě posledního) je zřejmě dělitelný číslem m, a proto dělitelnost čísla a_1^n i jeho zbytek závisí podle věty $\mathbf{T}_{15}$ jen na mocnině r_1^n.

Příklad 13. Určete zbytek čísla $x = 1087^3$, který dostaneme, když provedeme jeho dělení (se zbytkem) číslem 9.

Platí $x = 1087^3 = (9.120 + 7)^3$. Místo čísla $x = 1087^3$ můžeme dále podle věty $\mathbf{T}_{17}$ vyšetřit číslo $x = 7^3 = 343 = 9.38 + 1$. Hledaný zbytek při dělení čísla 1087^3 je tedy 1. Najdete-li ve Valouchových nebo jiných tabulkách $1087^3 = 1284365503$, přesvědčíte se dělením číslem 9 o správnosti nalezeného zbytku 1 (mod. 9).

Mohli jsme ovšem číslo x psát ve tvaru $(9.121 - 2)^3$ a vyšetřovat pak $(-2)^3 = -8$, což je číslo náležející do ${}^1C_9$, jak se snadno přesvědčíte, když k číslu -8 přičtete číslo 9 (podle věty $\mathbf{T}_{13}$).

Příklad 14. Určete zbytek čísla $y = 2^{100}$ při jeho dělení číslem 37.

Tuto úlohu rozřešíme opakovaným užitím věty $\mathbf{T}_{17}$ tak, jak to stručně naznačíme. Platí $y = 2^{100} = (2^5)^{20} = 32^{20} = (37.1 - 5)^{20}$. Místo čísla y budeme nyní vyšetřovat číslo $y_1 = (-5)^{20} = 5^{20}$, které patří do téže zbytkové třídy ${}^rC_{37}$ jako číslo y. Avšak $y_1 = 5^{20} = (5^4)^5 = 625^5 = (37.17 - 4)^5$. Místo čísla y_1 vyšetříme nyní dělitelnost čísla $y_2 = (-4)^5 = -4^5 = -2^{10}$, které náleží do téže zbytkové třídy jako číslo y_1. [Nyní bychom mohli již nahlédnout do tabulky II na konci této knížky a zjistit $-2^{10} = -1024$. Dělíme-li toto číslo číslem 37, dostaneme nejmenší kladný zbytek 12. Můžeme však postupovat i jinak, jak dále ukážeme.]

Platí $y_2 = -2^{10} = -(2^5)^2 = -32^2 = -(37.1 - 5)^2$. Místo y_2 můžeme vyšetřovat dále číslo $y_3 = -(-5)^2 = -25$, které náleží do třídy ${}^{12}C_{37}$ stejně jako číslo y.

Příklad 15. Je dáno přirozené číslo $a = 103^{53} + 53^{103}$. Rozhodněte, zda platí tyto vztahy: a) $3 \mid a$, b) $4 \mid a$, c) $5 \mid a$ (viz příklad 4).

a) $a = (3.34 + 1)^{53} + (3.18 - 1)^{103}$. Podle věty $\mathbf{T}_{15}$ a $\mathbf{T}_{17}$ můžeme místo čísla a vyšetřovat dělitelnost čísla $\bar{a} = (+1)^{53} + (-1)^{103} = 1 - 1 = 0$. Platí tedy $3 \mid a$.

b) $a = (4.26 - 1)^{53} + (4.13 + 1)^{103}$. Místo čísla a vyšetříme $\bar{a} = (-1)^{53} + (+1)^{103} = -1 + 1 = 0$, což znamená, že číslo $\bar{a}$ a také číslo a je násobkem čísla 4.

c) $a = (5.20 + 3)^{53} + (5.10 + 3)^{103}$. Místo čísla a

vyšetříme nyní číslo $a_1 = 3^{53} + 3^{103} = 3.3^{52} + 3.3^{102} = 3(3^2)^{26} + 3(3^2)^{51} = 3.(5.2 - 1)^{26} + 3(5.2 - 1)^{51}$. Místo čísla a_1 vyšetříme nyní (podle vět $\mathbf{T}_{15}$, $\mathbf{T}_{16}$, $\mathbf{T}_{17}$) číslo $a_2 = 3(-1)^{26} + 3(-1)^{51} = 3 - 3 = 0$. Platí tedy též $5 \mid a$. (Důsledky: viz věta $\mathbf{T}_{32}$.)

$\mathbf{T}_{18}$ *Jestliže z libovolných mocnin celých čísel* $a_1, a_2, a_3, \ldots, a_n$, *jejichž mocnitelé jsou přirozená čísla, utvoříme početní výraz konečným počtem operací sčítání, odčítání a násobení, pak číslo a takto vzniklé patří do téže zbytkové třídy* ${}^rC_m$ *jako číslo* $\bar{a}$, *které dostaneme z početního výrazu pro číslo a, když v něm nahradíme daná čísla jejich zbytky* $r_1, r_2, r_3, \ldots, r_n$ *(mod m).*

Tato věta shrnuje předcházející věty $\mathbf{T}_{15}$, $\mathbf{T}_{16}$, $\mathbf{T}_{17}$, které jsou jen speciálními případy věty $\mathbf{T}_{18}$. Užitečnost této věty pro kontrolu numerických výpočtů ukážeme jen na jednom příkladě.

Příklad 16. Je dáno číslo $a = 182^3 + (324^2 - 7354 + 2963).64 - 751.135$. Vypočtěte zbytky při dělení čísla a číslem m pro a) $m = 9$, b) $m = 11$.

a) Místo a budeme vyšetřovat podle modulu 9 číslo $\bar{a} = 2^3 + (0^2 - 1 + 2)1 - 4.0 = 8 + 1 - 0 = 9$. Odtud plyne $a \in {}^0C_9$ čili číslo a je dělitelné číslem 9.

b) Místo čísla a budeme vyšetřovat podle modulu 11 číslo $\bar{a} = 6^3 + (5^2 - 6 + 4).9 - 3.3 = 216 + 207 - 9 = 414$.

Číslo $414 \in {}^7C_{11}$ čili také $a \in {}^7C_{11}$. To znamená, že číslo a při dělení 11 dává zbytek 7.

Jestliže si provedete naznačený výpočet čísla a, dostanete $a = 12\,364\,623$, které je skutečně dělitelné číslem 9 a při dělení číslem 11 dává zbytek 7.

Cvičení

3,1. Najděte množinu všech celých čísel x, pro která platí a) $13 \mid 4x^2 + 1$, b) $11 \mid 6x^2 + 1$.

3,2. Dokažte, že pro každé celé číslo x platí: a) $3 \mid x^3 + 2x$, b) $3 \mid x^3 - 6x^2 + 2x - 3$, c) $3 \mid 3x^4 - x^3 + 9x^2 + x + 3$.

3,3. Je dáno celé číslo $y = x^6 - x^2$. Dokažte, že pro každé celé číslo x platí tyto vztahy: a) $3 \mid y$, b) $4 \mid y$, c) $5 \mid y$. Dokažte, že součet třetích mocnin tří po sobě jdoucích celých čísel je dělitelný devíti.

3,4. Dokažte, že funkční hodnoty polynomů $x^3 - 4x + 8$ mají pro celá čísla x tyto vlastnosti: a) žádná z nich není dělitelná třemi; b) je nekonečně mnoho takových, které jsou liché.

3,5. Nechť $m > 1$, n jsou čísla přirozená, x libovolné číslo celé. Dokažte, že platí tyto věty: a) je-li $x \in {}^1C_m$, pak je též $x^n \in {}^1C_m$; b) je-li $x \in {}^{-1}C_m$, pak při lichém n je $x^n \in {}^{-1}C_m$ a při sudém n je $x^n \in {}^1C_m$.

3,6. Dokažte, že pro přirozená čísla n platí:
a) $3 \mid 2^n - 7$, je-li n sudé; b) $5 \mid 2^n - 7$, je-li $n \in {}^1C_4$;
c) $61 \mid 2^{49} - 7$; d) $5 \mid 3.2^{1947} + 1$.

3,7. Je-li $f(x)$ polynom s celými koeficienty $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ a jsou-li x_1, x_1' dvě celá čísla náležející do téže zbytkové třídy, ${}^rC_m$, pak také funkční hodnoty $f(x_1), f(x_1'), f(r_1)$ patří do téže třídy ${}^rC_m$. Dokažte toto tvrzení a ověřte si je pak na vhodně volených příkladech.

3,8. Užitím binomické věty dokažte, že pro přirozená čísla n platí, že $(n+1)^{n-1}$ je násobkem čísla n^2.

3,9. Pro mocniny 10^n, kde n je nezáporné celé číslo, určete zbytky při jejich dělení čísly 3, 9, 11.

4. kapitola

ČÍSELNÉ SOUSTAVY A KRITÉRIA DĚLITELNOSTI

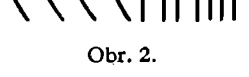
Při vyjadřování myšlenek záleží nejen na tom, abychom znali přesně obsah a rozsah různých pojmů, označených různými názvy, ale i těch různých pojmů, které jsou označeny týmž názvem. Proto jsme vás již v kap. 1 upozornili na dvojí význam termínu „dělitel". Často je též třeba si uvědomit, zda se nějaký výrok týká určitého pojmu nebo jeho názvu či značky (symbolu). Tak např. pravdivý výrok „8 je číslo sudé" se týká čísla 8, kdežto jiný pravdivý výrok „8 je arabská číslice" se týká matematické značky čísla 8, tj. číslice (cifry), sloužící k označení čísla. V dalším textu tohoto článku vás upozorníme ještě na to, že výrok „8 je jednociferné číslo" je rovněž pravdivý, když jeho význam budeme chápat ve smyslu určité úmluvy. Nesprávné chápání rozdílu mezi pojmy číslo a zápis čísla číslicemi vede někdy k používání nesprávných rčení, jako např. „číslo zakončené dvěma nulami". Takovým rčením se musíme vyhýbat, chceme-li se učit přesně myslit i vyjadřovat.

Když se v počátcích lidské kultury učili lidé počítat, užívali k označování malých přirozených čísel samostatných názvů i grafických nebo jiných značek. Přirozených čísel je však nekonečně mnoho a proto brzy vznikla potřeba sdružovat určitý počet jednotek do jednotek vyšších řádů, vytvářených podle určitých pravidel, a pomocí jejich názvů i značek vytvářet názvy i značkové výrazy pro označování větších čísel. Tak vznikaly číselné soustavy o různém základu. Nejčastěji se užívalo číselné soustavy desít-

kové (dekadické), což zřejmě souvisí s tím, že prsty na rukou byly nejčastěji používanou počtářskou pomůckou lidí na primitivním stupni kultury.

Kdyby se byl člověk vyvinul jako tvor s šesti prsty na každé ruce, pak bychom asi dnes používali nejvíce číselné soustavy dvanáctkové, která by měla některé výhody proti soustavě desítkové; číslo 12 má totiž tu vlastnost, že má v množině všech přirozených čísel šest dělitelů, tj. čísla 1, 2, 3, 4, 6, 12, zatímco číslo 10 má v téže množině jen čtyři dělitele, tj. čísla 1, 2, 5, 10. V dávnověku se užívalo i jiných číselných soustav. Tak např. Babylóňané, kteří dosáhli v matematice obdivuhodných výsledků, užívali soustavy šedesátkové; dokladem toho jsou v praxi dosud užívané soustavy časových a úhlových jednotek. V posledním čtvrtstoletí nabyla značného významu pro technickou praxi též číselná soustava dvojková (dyadická) pro některé výhody, jichž je možno využít při konstrukci číslicových elektronických počítacích strojů.

Již v dávnověku se k zapisování některých přirozených čísel používalo jednoduchých značek a k zapisování ostatních přirozených čísel složených značkových výrazů, které se vytvářely z jednoduchých značek podle určitých skladebních principů. Nejjednodušší byl princip adiční (sčítací), při jehož používání řada za sebou napsaných značek označovala číslo rovné součtu čísel, označených jednotlivými značkami. Jako příklad uvádíme v obr. 2 vyznačený egyptský hieroglyfický zápis čísla 423. V něm každá z prvních čtyř značek označuje číslo 100, každá z dalších dvou číslo 10 a každá z posledních tří číslo 1.



Obr. 2.

Při zapisování čísel se dříve užívalo i jiných skladebních principů, z nichž jistě znáte princip, který se uplatňoval při zapisování čísel římskými číslicemi. Pro vývoj matematiky nabyl však největšího významu princip poziční, jehož se částečně užívalo již před 2000 lety. V VIII. a IX. století propracovali užívání tohoto principu ve spojení s číselnou soustavou desítkovou matematikové indičtí. Znalost indického způsobu zapisování čísel, jehož dnes užívá celý kulturní svět ve formě jen málo změněné, přenesli do Evropy především Arabové, a proto snad nepřekvapuje, že původní indické číslice se nyní označují často jako arabské. V dalších odstavcích se zmíníme stručně o užívání pozičního principu při zapisování čísel v libovolné číselné soustavě, jejímž základem může být kterékoli přirozené číslo $z > 1$. Zapisování přirozených čísel tímto způsobem se opírá o následující větu.

T_{19} *Je-li dáno přirozené číslo $z > 1$, pak každé přirozené číslo y je možno vyjádřit právě jedním způsobem ve tvaru* $y = c_n z^n + c_{n-1} z^{n-1} + \ldots + c_k z^k + c_{k-1} z^{k-1} + \ldots + c_1 z + c_0$, (4,1), *v němž c_i ($i = 0, 1, 2, 3, \ldots, n$) jsou celá nezáporná čísla, pro která platí $c_i < z$, $c_n \neq 0$.*

Důkaz věty T_{19} snadno provedeme užitím věty T_{11}, přičemž se ukáže, jakým způsobem lze najít rozklad čísla y ve tvaru (4,1), který pro stručnost budeme někdy označovat $R(z)$ a nazývat *rozvoj přirozeného čísla y v soustavě z–adické*, tj. např. dyadické (dvojkové), triadické (trojkové) atd. Číslo z nazýváme *základ soustavy*.

Podle věty T_{11} existuje jediná dvojice takových čísel k_1, c_0, že platí

$$y = k_1 z + c_0, 0 \leq c_0 < z. \qquad (4,2)$$

Určíme-li dělením čísla k_1, c_0, pak lze najít taková čísla k_2, c_1, že platí

$$k_1 = k_2 z + c_1, 0 \leq c_1 < z. \qquad (4,3)$$

Po dosazení $k_1 = k_2 z + c_1$ do rovnosti (4,2) dostaneme $y = k_2 z^2 + c_1 z + c_0$. Není-li k_2 menší než z, pokračujeme obdobně v hledání rozkladu $k_2 = k_3 z + c_2$, až dospějeme nakonec k rovnosti $k_n = k_{n+1} z + c_n$, kde $k_{n+1} = 0$, a tedy $k_n = c_n$, čímž dospějeme též k hledanému rozvoji $R(z)$ uvedenému v (4,1). Ukážeme hledání rozvoje $R(z)$.

Příklad 17. Najděte rozvoj čísla 2642 v soustavě pětkové. Užitím postupu naznačeného výše dostaneme tyto rovnosti:
1) $2642 = 528.5 + 2$; 2) $528 = 105.5 + 3$; 3) $105 = 21.5 + 0$; 4) $21 = 4.5 + 1$; 5) $4 = 0.5 + 4$.
Tak jsme našli čísla $c_0 = 2$, $c_1 = 3$, $c_2 = 0$, $c_3 = 1$, $c_4 = 4$ pro hledaný rozvoj $2642 = 4.5^4 + 1.5^3 + 0.5^2 + 3.5 + 2$.

Danou úlohu můžeme řešit též jinak, zejména máme-li po ruce tabulku mocnin 5^n. Zjistíme-li, že dané číslo leží v intervalu uzavřeném dvěma po sobě jdoucími mocninami čísla 5, tj. $5^4 \leq 2642 \leq 5^5$, snadno najdeme dělením (se zbytkem) $2642 = 4.5^4 + 142$; tím je nalezen první sčítanec rozvoje 4.5^4. Ze vztahu $5^3 \leq 142 \leq 5^4$ najdeme snadno $142 = 1.5^3 + 17$, čímž je nalezen druhý hledaný sčítanec 1.5^3. Poněvadž $5^1 \leq 17 \leq 5^2$, platí $17 = 3.5 + 2$, čímž jsou nalezeny zároveň poslední dva sčítance hledaného rozvoje. Zapsání sčítance 0.5^2 do hledaného rozvoje nepotřebuje jistě vysvětlení, má-li být v rozvoji vyznačen i ten sčítanec, který je násobkem mocniny 5^2.

Příklad 18. Vyhledejte rozvoj $R(z)$ čísla 22223 v číselné soustavě o základu $z = 12$.
Postupným dělením číslem 12 najdeme tyto rovnosti:

1) $22223 = 1851.12 + 11$; 2) $1851 = 154.12 + 3$; 3) $154 = 12.12 + 10$; 4) $12 = 1.12 + 0$; 5) $1 = 0.12 + 1$. Tak jsme našli čísla $c_0 = 11$, $c_1 = 3$, $c_2 = 10$, $c_3 = 0$, $c_4 = 1$ pro hledaný rozvoj $22223 = 1.12^4 + 0.12^3 + 10.12^2 + 3.12 + 11$.

Je-li dáno přirozené číslo $z > 1$, pak posloupností celých nezáporných čísel $c_0, c_1, c_2, \ldots, c_{n-1}, c_n$ vyhovujících podmínkám věty $\mathbf{T}_{19}$, je jednoznačně určen rozvoj $R(z)$ čísla y. Stručný zápis těchto číselných údajů charakterizujících určité číslo můžeme provést ve formě

$$(\overline{|c_n}\ \overline{|c_{n-1}}\ \overline{|c_{n-2}} \ldots \overline{|c_2}\ \overline{|c_1}\ \overline{|c_0})\, z, \qquad (4,4)$$

kde $\overline{|c_0}$, $\overline{|c_1}$, $\overline{|c_2}$, $\ldots$, $\overline{|c_n}$ jsou číslice (cifry), tj. značky pro čísla $c_0, c_1, \ldots, c_n$, zapsané v závorce v pořadí odprava doleva, přičemž k závorce je připojen index z, udávající základ číselné soustavy. Při zápisech čísel ve formě (4,4) v kterékoli číselné soustavě zvolíme si za značky čísel menších než 10 arabské číslice 0, 1, 2, 3, ..., 9. Pro čísla $c_i \geq 10$ měli bychom si vymyslit další jednoduché značky (číslice) a stanovit pevně jejich význam. Tak se to dělá v některých knížkách při výkladu o zapisování čísel užitím pozičního principu v různých číselných soustavách. Abychom si nemusili pamatovat význam nově zaváděných značek, užijeme symbolů $\overline{|10}$, $\overline{|11}$, $\overline{|12}$, ... jako značek pro čísla 10, 11, 12, ... Konečně se ještě dohodneme, že při zápisu čísla v soustavě desítkové vynecháme závorku s indexem 10, tj. zápis 375 znamená totéž jako zápis $(375)_{10}$.

Užitím výsledků nalezených v příkladech 17 a 18 můžeme tedy zapsat tyto rovnosti:

$2642 = (41032)_5$, $22223 = (10\ \overline{|10}\ 3\ \overline{|11})_{12}$.

V jazyce mluveném čteme ovšem zápis $(41032)_5$ asi takto: číslo zapsané číslicemi 4, 1, 0, 3, 2 v soustavě

pětkové. Obdobně čteme zápisy čísel i v jiných číselných soustavách. Přitom platí úmluva, že vynechání slov „v soustavě pětkové“ nebo obecně „v soustavě z–adické“ znamená, že jde o zápis čísla v soustavě desítkové.

Platí-li pro rozvoj přirozeného čísla $y = R(z)$ podmínky věty $\mathbf{T}_{11}$, zejména podmínka $c_n \neq 0$, a zapisujeme-li přirozené číslo číslicemi podle vzoru (4,4), pak lze každé přirozené číslo zapsat v každé soustavě právě jedním způsobem. Zápis se přitom skládá z $n + 1$ číslic, mezi nimiž nemůže být na prvním místě číslice 0. O přirozeném čísle y, které je takto zapsáno v soustavě z–adické k ciframi (k je číslo přirozené), říkáme, že je to *číslo k–ciferné v soustavě z–adické*. Užijeme-li zkráceného názvu *číslo k–ciferné*, rozumí se tím, že jde o číslo k–ciferné při jeho zápisu v desítkové soustavě.

Čtyřciferné číslo 2642 je číslem pěticiferným v soustavě pětkové. Pěticiferné číslo 22223 je pěticiferné i v soustavě dvanáctkové, neboť každý ze symbolů $\overline{10}$, $\overline{11}$ musíme pokládat za číslici. Zapamatujme si, že podle naší úmluvy číslo 0 není jednociferné. I když to v této knížce nepotřebujeme, připomínáme to proto, že je to důležité pro správné chápání některých vět teoretické aritmetiky.

Snadným výpočtem si ověříme, že platí

$$(1000)_2 = (22)_3 = (20)_4 = (13)_5 = (12)_6 = (11)_7 = (10)_8 = (8)_9 = 8.$$

Z tohoto jednoduchého příkladu vidíme, že zápis téhož čísla osm může mít při zápisu v různých číselných soustavách (při užití poziční principu) různý počet cifer a že může být zakončen různým počtem číslic 0. Rčení „zápis čísla má na konci číslici 0“ neměl by být nahrazován méně vhodným rčením „číslo má na konci nulu“.

Upustíme-li od podmínky $c_n \neq 0$ ve větě $\mathbf{T}_{19}$, tj. připustíme-li též $c_n = 0$ s příslušným důsledkem pro zápis čísla podle vzoru (4,4), lze každé přirozené číslo v téže

soustavě zapsat více než jedním způsobem. V tom případě zřejmě platí např. $24 = 024 = 0024 = 00024 = \ldots$. S tímto způsobem zapisování přirozených čísel se ve škole zpravidla nesetkáváme kromě jedné výjimky, kterou stručně připomeneme.

Číslo 38752 můžeme rozložit v součet dvou sčítanců $38700 + 52$, z nichž druhý sčítanec můžeme charakterizovat názvem číslo zapsané posledním dvojčíslím 38752. Obdobně číslo 752 můžeme charakterizovat jako číslo zapsané posledním trojčíslím čísla 38752. Číslo zapsané posledním dvojčíslím čísla 1900024 je 24, číslo zapsané posledním trojčíslím čísla 1900024 je číslo $024 = 24$, číslo zapsané posledním čtyřčíslím čísla 1900024 je číslo $0024 = 24$. V tomto případě číslo zapsané posledním dvojčíslím, trojčíslím i čtyřčíslím je totéž číslo 24. *Posledním k-číslím daného čísla rozumíme zápis čísla skládajícího se z posledních k číslic daného čísla při jejich nezměněném pořadí.*

V praktickém životě se užívá číslicových zápisů majících tvar zápisů přirozených čísel často též k označování různých prvků některých množin, jako např. bankovek, losů, občanských průkazů, telefonních stanic aj. V číslicovém označení některých předmětů bývají někdy obsažena důležitá technická data o těch předmětech, které označují, jako např. u lokomotiv aj.

Příklad 19. Která přirozená čísla jsou v číselné soustavě o základu z zapsána n jedničkami? Numerický výpočet proveďte pro $n = 12$, $z = 2$, $z = 3$.

Označme ${}^{z}j_n$ přirozené číslo, které je v soustavě o základu z zapsáno n jedničkami, tj. tedy

$${}^{z}j_n = 1.z^{n-1} + 1.z^{n-2} + \ldots + 1.z^2 + 1.z + 1.$$

Znásobíme-li tuto rovnost číslem $z - 1$, dostaneme

$$ {}^{z}j_n(z-1) = (z^{n-1} + z^{n-2} + z^{n-3} + \ldots + z_2 + $$
$$ + z + 1)(z-1) = z^n + z^{n-1} + z^{n-2} + \ldots + z^3 + $$
$$ + z^2 + z - z^{n-1} - z^{n-2} - z^2 - z - 1 = z^n - 1. $$

Poněvadž $z > 1$, je $z - 1 \neq 0$, takže předcházející rovnost můžeme dělit číslem $z - 1$. Dostaneme tak

$$ {}^{z}j_n = (z^n - 1) : (z - 1). $$

Je-li $n = 12$, pak užitím tab. II. dostaneme snadno:
a) když $z = 2$, pak ${}^{2}j_{12} = 2^{12} - 1 = 4095$; b) když $z = 3$, pak ${}^{3}j_{12} = (3^{12} - 1) : (3 - 1) = 531440 : 2 = 265720$.

Příklad 20. Je dána posloupnost přirozených čísel a_n, v níž zápis n-tého členu v desítkové soustavě má $2n$ takových cifer, že na prvních n místech jsou čtyřky a na zbývajících n místech dvojky. Dokažte, že libovolný člen a_n této posloupnosti je součinem dvou po sobě jdoucích přirozených čísel.

Označíme-li j_n číslo, které v desítkové soustavě je zapsáno n jedničkami, pak $9\,j_n$ je číslo zapsané n devítkami a proto $9\,j_n + 1 = 10^n$ (k tomuto vztahu je možno dojít i jinou cestou; viz př. 19). V posloupnosti $a_1 = 42$, $a_2 = 4422$, $a_3 = 444222$, ..., je možno a_n vyjádřit takto: $a_n = j_n.4.10^n + j_n.2 = j_n.4\,(9j_n + 1) + j_n.2 = 36j_n^2 + 6j_n = 6j_n\,(6j_n + 1)$. Tento součin je zřejmě součin dvou po sobě jdoucích přirozených čísel, z nichž první, tj. číslo $6j_n$ je v desítkové soustavě zapsáno n šestkami. Platí tedy: $a_1 = 6.7$, $a_2 = 66.67$, $a_3 = 666.667$, ...

Příklad 21. Vypočtěte přirozené číslo z, pro které platí $(435)_z = (1352)_6$.
Daná úloha se snadno převede na řešení rovnice

$$ 4z^2 + 3z + 5 = 1.6^3 + 3.6^2 + 5.6 + 2. $$

Po snadné úpravě dostaneme rovnici $4z^2 + 3z - 351 = 0$, která má kořeny $9, -\frac{39}{4}$. Slovní úloze vyhovuje ovšem jen kořen $z = 9$.

V počtářské praxi máme často rozhodnout o tom, zda nějaké přirozené číslo je nebo není dělitelné jiným přirozeným číslem. Proto jsou užitečné poučky udávající charakteristický znak nebo souhrn znaků zkoumaného čísla, podle něhož můžeme tuto otázku rozhodnout rychleji než dělením. Takové poučky, jimž říkáme kritéria dělitelnosti, se zpravidla opírají o vlastnosti zápisu vyšetřovaných čísel v číselné soustavě z-adické, nejčastěji ovšem dekadické. V dalším textu vám ukážeme odvození některých kritérií dělitelnosti, která budou obecněji formulována než kritéria dělitelnosti, která již znáte ze školy.

Máme-li vyšetřit dělitelnost čísla $y = R(z)$, kde $R(z)$ je rozvoj vyznačený v (4,1) číslem z^k, můžeme využít toho, že číslo y lze napsat ve tvaru součtu dvou sčítanců

$$y = s_p + s_k, \tag{4,5}$$

kde s_p je součet počátečních $n - k + 1$ členů rozvoje $R(z)$ a s_k součet posledních k sčítanců rozvoje $R(z)$. Platí tedy $s_p = c_n z^n + c_{n-1} z^{n-1} + \ldots + c_k z^k =$
$= z^k(c_n z^{n-k} + \ldots + c_k)$, (4,6)

$s_k = c_{k-1} z^{k-1} + c_{k-2} z^{k-2} + \ldots + c_0 \leqq (z - 1) z^{k-1} +$
$+ (z - 1) z^{k-2} + \ldots + (z - 1) z + (z - 1) =$
$z^k - 1 < z^k$.

Poněvadž v součtu $y = s_p + s_k$ je první sčítanec zřejmě dělitelný číslem z^k, záleží zbytek čísla y při dělení číslem z^k jen na dělitelnosti čísla $s_k < z^k$. Nezáporné číslo s_k může být proto dělitelné číslem z^k jen tehdy, když $s_k = 0$, což může nastat právě jen tehdy, když $c_{k-1} = c_{k-2} = \ldots =$

$= c_1 = c_0 = 0$ (viz cvič. **1,4**). Odtud však snadnou úvahou plyne platnost následující věty.

T_{20} *Přirozené číslo y je dělitelné přirozeným číslem z^k právě tehdy, když v zápisu čísla y v číselné soustavě z–adické jsou na posledních k místech jen číslice* 0.

Podle této věty můžeme snadno rozhodnout, že např. číslo $(1101010000)_2$ je dělitelné číslem $2^4 = 16$, číslo $(341000)_5$ je dělitelné číslem $5^3 = 125$, číslo $(140200)_7$ je dělitelné číslem $7^2 = 49$ apod. Platí tedy i speciální kritéria dělitelnosti, jichž často užíváte ve škole pro čísla zapsaná v dekadické soustavě:

a) Je-li dáno přirozené číslo aspoň k–ciferným zápisem v desítkové soustavě, pak při jeho dělení číslem 10^k (k je číslo přirozené) dostaneme zbytek, který je v desítkové soustavě zapsán posledním k–číslím daného čísla. b) Přirozené číslo dané zápisem v desítkové soustavě je dělitelné číslem 10^k právě tehdy, když na všech posledních k místech jeho zápisu jsou číslice 0.

Je-li $z = 10$, pak číslo s_p (viz (4,6)) obsahuje činitele $10^k = (2.5)^k = 2^k.5^k$ a proto $2^k \mid s_p, 5^k \mid s_p$. Zbytek, který dostaneme při dělení čísla y číslem 2^k nebo 5^k, je tedy stejný jako zbytky, které dostaneme při dělení druhého sčítance s_k čísly 2^k nebo 5^k (podle věty T_{15}). Platí tedy následující dvě věty T_{21} a T_{22} a jejich důsledky.

T_{21} *Dělíme-li číslem 2^k jednak aspoň k–ciferné přirozené číslo y, jednak číslo vyznačené jeho posledním k–číslím, pak při obojím dělení dostaneme týž zbytek.*

Důsledek. *Dané přirozené číslo je dělitelné číslem 2^k právě tehdy, když je číslem 2^k dělitelné číslo zapsané posledním k–číslím v zápisu daného čísla.*

$\mathbf{T}_{22}$ *Dělíme-li číslem* 5^k *jednak aspoň k–ciferné přirozené číslo* y*, jednak číslo vyznačené jeho posledním k–číslím, pak při obojím dělení dostaneme týž zbytek.*

Důsledek. *Dané přirozené číslo je dělitelné číslem* 5^k *právě tehdy, když je číslem* 5^k *dělitelné číslo zapsané posledním k–číslím v zápisu daného čísla.*

Tak např. číslo $y = 790235$ při dělení číslem $2^1 = 2$ dává (podle věty $\mathbf{T}_{21}$) týž zbytek jako číslo 5 při dělení dvěma, tj. 1; při dělení čísla y číslem $2^2 = 4$ dostaneme týž zbytek jako při dělení čísla 35 číslem 4, tj. 3; při dělení čísla y číslem $2^3 = 8$ dostaneme týž zbytek jako při dělení čísla 235 číslem 8, tj. 3; při dělení čísla y číslem $2^4 = 16$ dostaneme týž zbytek jako při dělení čísla $0235 = 235$ číslem 16, tj. 11. Dělíme-li číslo y postupně čísly $5^1 = 5$, $5^2 = 25$, $5^3 = 125$, $5^4 = 625$ dostaneme podle věty $\mathbf{T}_{22}$ zbytky 0, 10, 110, 235.

Nechť je dáno určité přirozené číslo zápisem v dekadické soustavě, který odpovídá dekadickému rozvoji

$$c_n.10^n + c_{n-1}.10^{n-1} + \ldots + c_2 10^2 + c_1\,10 + c_0, \quad (4{,}7)$$

kde čísla $c_n, c_{n-1}, \ldots, c_2, c_1, c_0$ jsou určena jednotlivými ciframi zápisu čísla v desítkové soustavě. Utvořme nyní funkci proměnné z, která vznikne z výrazu (4,7), když v něm místo čísla 10 v mocninách 10^n píšeme všude z. Dostaneme tedy funkci

$$\mathrm{R}(z) = c_n z^n + c_{n-1}\, z^{n-1} + \ldots + c_2 z^2 + c_1 z + c_0. \quad (4{,}8)$$

Dosadíme-li $z = 1$ do výrazu $\mathrm{R}(z)$, dostaneme číslo $\mathrm{R}(1)$, pro něž platí $\mathrm{R}(1) = c_n.1^n + c_{n-1}.1^{n-1} \ldots + c_2.1^2 + + c_1.1 + c_0 = c_0 + c_1 + c_2 + \ldots + c_{n-1} + c_n$. Toto číslo $\mathrm{R}(1)$ je tedy součtem všech čísel, která jsou označena jednotlivými ciframi daného čísla při jeho zápisu v desítkové soustavě. Někdy se pro označení tohoto čísla užívá názvu

ciferný součet, který není dost vhodný, poněvadž může snadno vést k nesprávnému názoru, že je možno sčítat cifry (číslice). Název je však přípustný, když přijmeme následující definici.

D_9 *Ciferný součet daného čísla nazýváme součet všech čísel, která jsou označena jednotlivými ciframi zápisu daného čísla (v desítkové soustavě).*

Funkční hodnoty R(10) i R(1), které představují dané číslo a jeho ciferný součet, jsou v určitém vzájemném vztahu, jehož využijeme pro kritéria dělitelnosti přirozených čísel čísly 3 a 9. Číslo 1 a číslo $10 = 3.3 + 1$ patří do téže zbytkové třídy ${}^1C_3$ a proto čísla R(1) a R(10) musí patřit podle věty T_{18} rovněž do stejné zbytkové třídy ${}^rC_3$. Poněvadž číslo 1 a číslo $10 = 9.1 + 1$ patří do téže zbytkové třídy ${}^1C_9$, musí do téže zbytkové třídy ${}^rC_9$ patřit též čísla R(1) a R(10). Tak jsme ukázali odvození následujících vět T_{23} a T_{24}, které mají vám už známé důsledky.

T_{23} *Dělíme-li číslem 3 dané číslo i jeho ciferný součet, pak v obojím případě dostaneme stejný zbytek.*

Důsledek: *Přirozené číslo je dělitelné třemi právě tehdy, když je třemi dělitelný jeho ciferný součet.*

T_{24} *Dělíme-li číslem 9 dané číslo i jeho ciferný součet, pak v obojím případě dostaneme stejný zbytek.*

Důsledek: *Přirozené číslo je dělitelné devíti právě tehdy, když je devíti dělitelný jeho ciferný součet.*

Jestliže do vzorce (4,8) dosadíme $z = -1$, dostaneme funkční hodnotu $R(-1) = c_n.(-1)^n + c_{n-1}(-1)^{n-1} + \dots + c_2(-1)^2 + c_1.(-1)^1 + c_0 = c_0 - c_1 + c_2 + \dots + (-1)^{n-1}.c_{n-1} + (-1)^n.c_n = (c_0 + c_2 + c_4 + \dots) - (c_1 + c_3 + c_5 + \dots)$.

Číslo -1 a číslo $10 = 11 - 1$ patří do téže zbytkové třídy ${}^{-1}C_{11}$ a proto podle věty $\mathbf{T}_{18}$ patří čísla $R(-1)$ a $R(10)$ do stejné zbytkové třídy ${}^{r}C_{11}$. Odtud plyne snadnou úvahou následující věta $\mathbf{T}_{25}$ i její důsledek.

$\mathbf{T}_{25}$ *Dělíme-li číslem* 11 *dané číslo i součet čísel vyznačených jednotlivými ciframi na místech sudého řádu zmenšený o součet čísel vyznačených ciframi na místech lichého řádu daného čísla, pak oba zbytky jsou stejné.*

Důsledek: *Přirozené číslo je dělitelné jedenácti právě tehdy, když je jedenácti dělitelný součet čísel označených ciframi na místech sudého řádu zmenšený o součet čísel označených ciframi na místech lichého řádu.*

Tak např. číslo $s = 2597778$ je dělitelné 3 i 9, neboť číslo $8 + 7 + 7 + 7 + 9 + 5 + 2 = 45$ je dělitelné 3 a 9; ponevadž číslo $8 - 7 + 7 - 7 + 9 - 5 + 2 = 7$, musíme při dělení čísla s číslem 11 dostat zbytek 7.

Vět $\mathbf{T}_{24}$ a $\mathbf{T}_{25}$ můžeme využít k rychlému určení zbytků při dělení daných čísel čísly 9 a 11 při tzv. devítkové nebo jedenáctkové zkoušce správnosti nějakého numerického výpočtu, jak jsme je ukázali v příkladě 16 předcházející kapitoly. Ukážeme takovou zkoušku ještě na jednom jednoduchém příkladě.

Příklad 22. Proveďte devítkovou i jedenáctkovou zkoušku správnosti výpočtu součinu $3954.657 = 2957778$.

a) Při devítkové zkoušce zjistíme, že první činitel patří do zbytkové třídy ${}^{3}C_{9}$ a druhý do třídy ${}^{0}C_{9}$. Proto jejich součin patří do téže zbytkové třídy jako číslo $3.0 = 0$. Skutečně výsledek má ciferný součet $8 + 7 + 7 + 7 + 5 + 9 + 2 = 45$, který je dělitelný devíti. Tato zkouška podporuje domněnku o správnosti výpočtu daného součinu.

b) Při jedenáctkové zkoušce zjistíme, že první činitel

součinu patří do zbytkové třídy ${}^{5}C_{11}$, neboť číslo $4 - 5 + 9 - 3 = 5$ patří do třídy ${}^{5}C_{11}$. Druhý činitel patří do zbytkové třídy ${}^{8}C_{11}$, neboť $7 - 5 + 6 = 8$ náleží do třídy ${}^{8}C_{11}$. Proto součin daných čísel musí patřit do téže třídy (mod 11) jako číslo $5.8 = 40$, které patří do třídy ${}^{7}C_{11}$. V úloze udaný výsledek 2957778 náleží (mod 11) do téže třídy jako číslo $8 - 7 + 7 - 7 + 5 - 9 + 2 = -1$, tj. do třídy ${}^{-1}C_{11}$, což je v rozporu se zjištěním, že součin patří do třídy ${}^{7}C_{11}$. Tento nesouhlas ukazuje, že výpočet nebyl správně proveden. Propočtením zjistíme, že daný součin $s = 3954.657 = 2597778$, který patří do třídy ${}^{7}C_{11}$, jak jsme již dříve zjistili.

Povšimněme si, že v úloze udaný nesprávný výsledek se od správného výsledku liší změněným pořadím dvou po sobě jdoucích číslic. V tom případě je ciferný součet obou čísel stejný a proto se chyba výpočtu při devítkové zkoušce neprojevila. Provedení devítkové a jedenáctkové zkoušky zvyšuje pravděpodobnost, že případná chyba v numerickém výpočtu bude objevena.

Cvičení

4,1 Určete neznámé z, pro něž platí následující rovnosti: a) $(624)_z = (2222)_5$; b) $(1004)_z = (20110)_3$; c) $(10203)_z = (1100110)_2$.

4,2. Jestliže zápisy dvou přirozených čísel v dekadické soustavě se liší jen pořadím, ve kterém jsou uspořádány cifry v obou zápisech, pak druhá mocnina rozdílu obou čísel je násobkem čísla 81. Dokažte toto tvrzení.

4,3. Úvahou o vlastnostech soustavy dyadické (dvojkové) dokažte, že užitím sady závaží 1g, 2g, 4g, 8g, 16g, 32g, 64g, 128g je možno zvážit každé těleso, jehož váha je vyjádřena v gramech celými čísly od 1 do 255.

4,4. V každé číselné soustavě o základu $z \geq 5$ značí zápisy $(144)_z$, $(441)_z$ čísla, která jsou druhými mocninami celých čísel. Dokažte.

4,5. Ukažte, že je možné, aby selhala devítková i jedenáctková zkouška správnosti při kontrole nějakého výpočtu.

4,6. V číselné posloupnosti $\{a_n\}$ je člen a_n součinem dvou po sobě jdoucích přirozených čísel, z nichž menší je v desítkové soustavě zapsáno n trojkami. Dokažte, že zápis čísla a_n v desítkové soustavě má $2n$ cifer, z nichž prvních n cifer jsou samé jedničky, zatímco zbývající cifry jsou samé dvojky.

5. kapitola

NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

D$_{10}$ *Společný dělitel celých čísel* $a_1, a_2, a_3, \ldots, a_k$, *kde* $k \geq 2$, *se nazývá každé takové celé číslo* b, *že platí* $b \mid a_1, b \mid a_2, b \mid a_3, \ldots, b \mid a_k$.

D$_{11}$ *Největší společný dělitel celých čísel* $a_1, a_2, a_3, \ldots, a_k$ *nazýváme takové přirozené číslo, které je největší ze všech společných dělitelů čísel* $a_1, a_2, a_3, \ldots, a_k$, *a označujeme ho zpravidla* $(a_1, a_2, a_3, \ldots, a_k)$.

Pojmy vymezované v definicích **D**$_{10}$ a **D**$_{11}$ objasníme ihned na číselném příkladě. Učiníme tak přesto, že různé metody k snadnému vyhledání všech dělitelů, společných dělitelů i největšího společného dělitele daných čísel budou vyloženy teprve v dalším textu této a následující kapitoly.

Příklad 23. Jsou dána čísla $a_1 = 84$, $a_2 = 24$, $a_3 = -132$, $a_4 = 0$. Vyhledejte: a) množiny všech přirozených dělitelů daných čísel, b) množinu všech společných dělitelů daných čísel, c) (a_1, a_2), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4).

a) Pro každé přirozené číslo m, které je dělitelem čísla $a_1 = 84$, musí zřejmě platit $1 \leq m \leq 84$. Můžeme tedy konečným počtem zkoušek zjistit, která přirozená čísla vyhovují podmínkám $m \mid 84$, $1 \leq m \leq 84$. Označíme-li A_1 množinu všech přirozených dělitelů čísla a_1 a obdobně A_2, A_3, A_4 množiny všech přirozených dělitelů čísel a_2, a_3, a_4, dostaneme:

$A_1 = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$, $A_2 = \{1, 2,$

3, 4, 6, 8, 12, 24}, $A_3 = \{1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132\}$, $A_4 = \{1, 2, 3, 4, 5, 6, \ldots\}$.
Zatímco množiny A_1, A_2, A_3 mají konečný počet prvků, je množina A_4 nekonečná, neboť každé přirozené číslo je dělitelem čísla $a_4 = 0$. Kdybychom měli vyhledat všechny dělitele daných čísel, bylo by nutné ve všech případech uvést i čísla opačná k nalezeným přirozeným dělitelům (podle věty $\mathbf{T}_6$) a v případě posledním (pro číslo $a_4 = 0$) též číslo 0; děliteli čísla 0 jsou všechna čísla celá.

b) Máme-li vyhledat množinu S všech společných přirozených dělitelů daných čísel, musíme určit průnik množin A_1, A_2, A_3, A_4, tj. najít všechna přirozená čísla, která jsou zároveň prvky všech těchto množin, a shrnout je do množiny S. Nejsnáze tuto úlohu vyřešíme, vyjdeme-li od množiny A_2, která má nejmenší počet prvků, a zjistíme, které z jejích prvků jsou obsaženy ve všech ostatních množinách A_1, A_3, A_4; přitom nám práci usnadní znalost toho, že množina A_4 obsahuje každé přirozené číslo. Tak najdeme $S = \{1, 2, 3, 4, 6, 12\}$. Označíme-li S' množinu všech dělitelů čísel a_1, a_2, a_3, a_4, je zřejmě $S' = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$.

c) V množině S existuje největší přirozené číslo 12 (ve shodě s větou $\mathbf{T}_3$) a proto $(a_1, a_2, a_3, a_4) = 12$. K nalezení (a_1, a_2) je třeba najít průnik množin A_1, A_2 a v něm největší přirozené číslo; tak najdeme $(a_1, a_2) = 12$. Zjistíme-li, že (a_1, a_2) je dělitelem čísla a_3, plyne odtud $(a_1, a_2, a_3) = 12$. Je samozřejmé, že $(a_1, a_2, a_3) = (a_1, a_2, a_3, a_4) = 12$, když 12 patří do množiny A_4, která je množinou všech přirozených čísel.

Při hledání $(a_1, a_2, a_3, \ldots, a_k)$ vyloučíme z našich úvah případ $a_1 = a_2 = a_3 = \ldots = a_k = 0$, neboť v tomto případě množina všech společných přirozených dělitelů čísel $a_1, a_2, a_3, \ldots, a_k$ je množina všech přirozených čísel, v níž

neexistuje největší číslo. Podle definice $\mathbf{D}_{11}$ nemá symbol $(a_1, a_2, a_3, \ldots, a_k)$ smysl, pokud aspoň jedno z čísel $a_1, a_2, a_3, \ldots, a_k$ není různé od nuly. Je-li aspoň jedno z nich různé od nuly, pak ze snadné úvahy i ze zkušenosti, získané při řešení předcházejícího příkladu 23, plyne, že hledání $(a_1, a_2, a_3, \ldots, a_k)$ lze převést na hledání největšího společného dělitele přirozených čísel, kterého dostaneme, když ze souboru čísel $a_1, a_2, a_3, \ldots, a_k$ vynecháme nulové prvky a záporná čísla nahradíme čísly opačnými. Tak např. určení $(84, 24, -132, 0)$ můžeme nahradit určením $(84, 24, 132)$.

Při hledání $(a_1, a_2, \ldots, a_{k-1}, a_k)$, když aspoň jedno z čísel $a_1, a_2, \ldots, a_{k-1}, a_k$ je různé od nuly, můžeme použít následujících zřejmých a snadno dokazatelných vztahů, které označíme jako poučku $\mathbf{T}_{26}$.

$\mathbf{T}_{26}$ 1. $(a_1, a_2) = (a_1 - a_2, a_2)$;
2. $(a_1, a_2) = (a_2, a_1)$;
3. $(a_1, a_2) = a_1$, když $a_2 = 0$ nebo $a_2 = a_1$;
4. $(a_1, a_2, \ldots, a_{k-1}, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$.

Opakovaným užíváním těchto vztahů, z nichž první je důsledkem věty $\mathbf{T}_{10}$, můžeme výpočet (a_1, a_2) uspořádat tak, jak to bude zřejmé z následujících symbolických zápisů, jimiž bude vyznačen i důkaz správnosti našeho postupu. Jsou-li $a_1 > a_2 > 0$ dvě přirozená čísla, pak

$$(a_1, a_2) = (a_1 - a_2, a_2) = (a_1 - 2a_2, a_2) = \ldots =$$
$$= (a_1 - q_1 a_2, a_2) = (r_1, a_2) = (a_2, r_1).$$

Přechod od prvního členu (a_1, a_2) tohoto řetězce rovností až k jeho předposlednímu členu (r_1, a_2), kde $r_1 = a_1 - q_1 a_2 < a_2$, nemusíme uskutečnit postupným odčítáním čísla a_2; dělením čísla a_1 číslem a_2 můžeme najít (neúplný) podíl q_1 a zbytek r_1. Je-li $r_1 \neq 0$, pak můžeme opět najít další řetězec rovností

$$(a_2, r_1) = (a_2 - r_1, r_1) = (a_2 - 2r_1, r_1) = \ldots =$$
$$= (a_2 - q_2 r_1, r_1) = (r_2, r_1) = (r_1, r_2).$$

Číslo r_2 nemusíme hledat postupným odčítáním čísla r_1, nýbrž dělením čísla a_2 číslem r_1, při němž dostaneme celý nezáporný zbytek $r_2 < r_1$. Není-li $r_2 = 0$, pokračujeme v postupném odčítání nebo dělení naznačeným způsobem tak dlouho, až dospějeme k výrazu (r_n, r_{n+1}), kde $r_n \neq 0$, je poslední nenulový dělitel dělení, při němž zbytek $r_{n+1} = 0$. Zřejmě platí

$$(a_1, a_2) = (a_2, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots =$$
$$= (r_{n-1}, r_n) = (r_n, r_{n+1}) = r_n.$$

Tento postup výpočtu $(a_1, a_2) = r_n$ metodou postupného dělení, jež někdy nahrazujeme opakovaným odčítáním, se nazývá též algoritmus Euklidův. Jeho užití vám ukážeme na několika příkladech, ale předtím uvedeme ještě dvě definice významu názvů, jichž budeme často užívat.

D$_{12}$ *Celá čísla* $a_1, a_2, a_3, \ldots, a_k$ *nazýváme nesoudělná, jestliže platí* $(a_1, a_2, a_3, \ldots, a_k) = 1$.

D$_{13}$ *Celá čísla* $a_1, a_2, a_3, \ldots, a_k$ *se nazývají po dvou nesoudělná, platí-li* $(a_i, a_j) = 1$ *pro každou dvojici čísel vybranou z daných čísel.*

K tomu, aby celá čísla $a_1, a_2, a_3, \ldots, a_k$ (pro $k \geqq 2$) byla nesoudělná, stačí splnění slabší podmínky, než je ta, která musí být splněna, mají-li být tato čísla po dvou nesoudělná. Je zřejmé, že čísla po dvou nesoudělná (podle **D$_{13}$**) jsou vždy nesoudělná (podle **D$_{12}$**), avšak čísla nesoudělná nemusí být po dvou nesoudělná. Význam obou termínů splývá pro $k = 2$, tj. tedy pro dvojici celých čísel a_1, a_2.

Příklad 24. Vypočtěte a) (84,24); b) (84, 24, 54); c) (84, 24, 54, 37).

a) $84 = 3.24 + 12$ a proto $(84, 24) = (24, 12)$. Poněvadž $24 = 2.12 + 0$, platí $(84, 24) = (24, 12) = (12, 0) = 12$.

b) Při hledání (84, 24, 54) najdeme nejprve $(84, 24) = 12$, a pak hledáme (12, 54). Poněvadž $54 = 4.12 + 6$, $12 = 2.6 + 0$, platí $(84, 24, 54) = (12, 54) = (12, 6) = (6, 0) = 6$.

c) Při hledání (84, 24, 54, 37) vyhledáme nejprve $(84, 24, 54) = 6$ a pak hledáme (6, 37). Poněvadž $37 = 6.6 + 1$, $6 = 6.1 + 0$, platí $(6, 37) = 1$ a proto také $(84, 24, 54, 37) = 1$. Čísla 84, 24, 54, 37 jsou nesoudělná, ale nejsou po dvou nesoudělná, když např. $(84, 24) = 12 > 1$.

Příklad 25. Posloupnost čísel 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ... je určena počátečními členy $u_0 = 0$, $u_1 = 1$ a předpisem, že každý z dalších členů posloupnosti se rovná součtu dvou předcházejících členů. Čísla, která jsou členy této posloupnosti, se nazývají čísla Fibonacciova. Dokažte, že každá dvě po sobě jdoucí čísla Fibonacciova jsou nesoudělná.

Pro danou posloupnost platí rekurentní vzorec $u_{n+1} = u_n + u_{n-1}$ a z něho plyne $u_{n+1} - u_n = u_{n-1}$. Dále platí $(u_{n+1}, u_n) = (u_{n+1} - u_n, u_n) = (u_{n-1}, u_n) = (u_n, u_{n-1})$. Z toho plyne platnost vztahu $(u_{n+1}, u_n) = (u_n, u_{n-1})$ a jeho opakovaným použitím $(u_n, u_{n-1}) = (u_{n-1}, u_{n-2}) = \ldots = (u_3, u_2) = (u_2, u_1) = (u_1, u_0) = (1, 0) = 1$. Tento výsledek znamená však podle $\mathbf{D}_{12}$, že kterákoli dvě po sobě jdoucí Fibonacciova čísla jsou nesoudělná.

Příklad 26. Určete největší společný dělitel dvou po sobě jdoucích čísel a) sudých, b) lichých.

Označíme-li menší číslo x, pak je druhé $x + 2$. Avšak

$(x, x + 2) = (x, 2)$. a) Je-li x sudé číslo, pak $2 \mid x$ a proto největší společný dělitel dvou po sobě jdoucích čísel sudých je 2. b) Je-li x liché číslo, pak $2 \nmid x$ a proto $(x, 2) < 2$, tj. $(x, 2) = 1$, neboť jiné možnosti není. Proto 2 po sobě jdoucí lichá čísla jsou nesoudělná.

Příklad 27. Dokažte, že pro žádné číslo x nedostaneme v čitateli a jmenovateli zlomku $\frac{21x + 4}{14x + 3}$ taková čísla, abychom mohli zlomek krátit.

Daný zlomek má smysl pro každé celé číslo x, neboť $14x + 3 = 0$ jen pro $x = -\frac{3}{14}$. Hledejme nyní opakovaným užitím dovolených úprav největší společný dělitel čitatele i jmenovatele daného zlomku. Dostaneme postupně:

$$(21x + 4, 14x + 3) = (7x + 1, 14x + 3) = (14x + 3, 7x + 1) = (7x + 2, 7x + 1) = (1, 7x + 1) = 1.$$

Tím jsme dokázali nesoudělnost čitatele i jmenovatele pro každé celé číslo x a tím i nemožnost daný zlomek zkrátit.

Příklad 28. Je-li $d = (a_1, a_2)$ největší společný dělitel přirozených čísel a_1, a_2, pak $a_1 = dq_1$, $a_2 = dq_2$, kde $(q_1, q_2) = 1$, tj. čísla q_1, q_2 jsou nesoudělná. Dokažte.

Předpokládejme, že čísla q_1, q_2 jsou soudělná, tj. $(q_1, q_2) = d' > 1$. V tom případě platí $q_1 = d'\,q_1'$, $q_2 = d'\,q_2'$, odtud po dosazení do rovností uvedených v úloze dostaneme

$$a_1 = dq_1 = dd'\,q_1', a_2 = dq_2 = dd'\,q_2'.$$

Odtud však plyne, že součin dd' je společným dělitelem čísel a_1, a_2. Avšak z předpokladu $d' > 1$ plyne $d'd > d$, což

je v rozporu s předpokladem, že d je největší společný dělitel čísel a_1, a_2. Neplatí tedy $d' > 1$, nýbrž $d' = 1$.

V definici $\mathbf{D}_{11}$ jsme uvedli takový charakteristický souhrn znaků definovaného pojmu, aby co nejpřístupněji objasnil význam názvu největší společný dělitel. Ten však můžeme vymezit i jiným způsobem, který je pro některé důkazy užitečnější, i když při něm nejsou výslovně uvedeny vlastnosti naznačené v názvu největší společný dělitel. Ukážeme si, že z jiné definice $\mathbf{D}_{14}$ odvodíme nejen vlastnosti největšího společného dělitele, uvedené v $\mathbf{D}_{11}$, ale i jiné jeho vlastnosti, které bychom s obtížemi odvozovali z definice $\mathbf{D}_{11}$.

$\mathbf{D}_{14}$ *Největší společný dělitel d celých čísel $a_1, a_2, a_3, \ldots, a_k$, z nichž aspoň jedno je různé od nuly, je nejmenší přirozené číslo z množiny M všech celých čísel m, která lze napsat ve tvaru*

$$m = c_1 a_1 + c_2 a_2 + c_3 a_3 + \ldots + c_k a_k$$

kde $c_1, c_2, c_3, \ldots, c_k$ jsou libovolná celá čísla.

Výklad i odvození vlastností největšího společného dělitele, které vyplývají z $\mathbf{D}_{14}$, provedeme za předpokladu, že jsou dána jen 4 čísla a_1, a_2, a_3, a_4, z nichž aspoň jedno je různé od nuly. Zobecnění následujících úvah, kdy je dán libovolný počet čísel, je snadné a neuvádíme je jen proto, aby výklad i důkazy byly stručnější a přehlednější.

Množina M se skládá ze všech celých čísel m, která je možno napsat ve tvaru

$$m = c_1 a_1 + c_2 a_2 + c_3 a_3 + c_4 a_4, \qquad (5,1)$$

kde c_1, c_2, c_3, c_4 jsou libovolná celá čísla. Do této množiny M patří jistě čísla a_1, a_2, a_3, a_4 i čísla k nim opačná. Zvolíme-li např. $c_2 = c_3 = c_4 = 0$ a k tomu jednou $c_1 = 1$, podruhé $c_1 = -1$, plyne odtud, že $a_1 \in M$, $-a_1 \in M$. Obdobně to

platí i o číslech a_2, a_3, a_4. Poněvadž aspoň jedno z daných čísel je různé od nuly, existuje v množině M aspoň jedno celé číslo kladné a aspoň jedno záporné; je jich tam ovšem nekonečně mnoho, neboť do množiny M náleží zřejmě i všechny násobky čísel a_1, a_2, a_3, a_4.

Označme P množinu všech přirozených čísel z množiny M; je tedy P částí množiny M, tj. $P \subset M$. Poněvadž jsme již dokázali, že v množině M existuje aspoň jedno přirozené číslo, je P neprázdná množina a podle věty $\mathbf{T}_2$ v ní existuje číslo nejmenší. Označme d toto nejmenší přirozené číslo množiny M, které je podle $\mathbf{D}_{14}$ největším společným dělitelem daných čísel, takže platí $d = (a_1, a_2, a_3, a_4)$. Z toho ovšem plyne, že existují též taková celá čísla x_1, x_2, x_3, x_4, že

$$d = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4. \tag{5,2}$$

Nyní ukážeme, že číslo d je společným dělitelem všech čísel množiny M a tedy i společným dělitelem čísel a_1, a_2, a_3, a_4, které jsou prvky množiny M. Důkaz provedeme nepřímo.

Předpokládejme, že neplatí vztah $d \mid m$, tj. že platí

$$m = dq + r,\ 0 < r < d, \tag{5,3}$$

čili že $r = m - dq$, kde q je číslo celé, r kladný zbytek při dělení čísla m číslem d. Dosadíme-li do této rovnosti za m, d čísla ze vztahů (5,1) a (5,2), dostaneme:

$$\begin{aligned} r = m - dq = (c_1a_1 + c_2a_2 + c_3a_3 + c_4a_4) - (a_1x_1 + \\ + a_2x_2 + a_3x_3 + a_4x_4)q = a_1(x_1 - c_1q) + a_2(x_2 - \\ - c_2q) + a_3(x_3 - c_3q) + a_4(x_4 - c_4q) = a_1x_1' + \\ + a_2x_2' + a_3x_3' + a_4x_4', \end{aligned}$$

když jsme užili označení $x_1' = x_1 - c_1q$, $x_2' = x_2 - c_2q$, $x_3' = x_3 - c_3q$, $x_4' = x_4 - c_4q$. Z předpokladu (5,3) jsme odvodili, že přirozené číslo $r < d$ lze vyjádřit ve tvaru,

který svědčí o tom, že r je prvkem množiny P, avšak $r < d$ je ve sporu s předpokladem, že d je nejmenší přirozené číslo množiny M. Není tedy možné, aby platily vztahy (5,3), a musí tedy platit $r = 0$, $d \mid m$.

Každé číslo b, které je společným dělitelem čísel a_1, a_2, a_3, a_4, je též dělitelem čísla d. Z předpokladu $b \mid a_1$, $b \mid a_2$, $b \mid a_3$, $b \mid a_4$ plyne $a_1 = bq_1$, $a_2 = bq_2$, $a_3 = bq_3$, $a_4 = bq_4$ a po dosazení do vztahu (5,2) dostaneme:
$d = bq_1x_1 + bq_2x_2 + bq_3x_3 + bq_4x_4 =$
$= b(q_1x_1 + q_2x_2 + q_3x_3 + q_4x_4)$, což však znamená $b \mid d$. Přitom není možné, aby $b > d$, neboť pak by nemohlo platit $b \mid d$. Platí tedy vždy $b \leqq d$, takže největší společný dělitel ve smyslu definice $\mathbf{D}_{14}$ má vlastnost uvedenou v $\mathbf{D}_{11}$. Tím jsme dospěli k výsledku, který po snadném zobecnění vyjadřuje následující věta:

$\mathbf{T}_{27}$ *Největší společný dělitel celých čísel a_1, a_2, a_3, ..., a_k je dělitelný každým společným dělitelem čísel a_1, a_2, a_3, ..., a_k.*

Z důkazu vztahu $d \mid m$ pro každé $m \in M$ plyne, že množina M je množinou všech násobků čísla d. V důsledku toho, že množina $M = \{\ldots -3d, -2d, -d, 0, d, 2d, 3d, \ldots\}$, platí následující věta:

$\mathbf{T}_{28}$ *Všechny prvky množiny M, která je množinou všech možných součtů kterýchkoli násobků daných celých čísel a_1, a_2, a_3, ..., a_k, jsou násobky čísla $d = (a_1, a_2, a_3, \ldots, a_k)$.*

Jestliže ve vztahu (5,2) je číslo $d = 1$, pak odtud snadnou úvahou dostaneme následující zobecněnou větu.

$\mathbf{T}_{29}$ *K celým číslům a_1, a_2, a_3, ..., a_k je možno vyhledat celá čísla x_1, x_2, x_3, ..., x_k, aby platil vztah*

$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_kx_k = 1$, *když a jen když čísla* $a_1, a_2, a_3, \ldots, a_k$ *jsou nesoudělná.*

Zvláštním případem věty $\mathbf{T}_{29}$ je následující věta, jejíž znalost se předpokládá při řešení některých úloh matematických olympiád:

Ke dvěma celým číslům a, b je možno právě tehdy najít celá čísla x, y, aby platilo $ax + by = 1$, když čísla a, b jsou nesoudělná. Jinak řečeno: Jsou-li celá čísla a, b nesoudělná, pak existují taková celá čísla x, y, že platí $ax + by = 1$, a obráceně, existují-li k daným celým číslům a, b celá čísla x, y, že platí $ax + by = 1$, pak čísla a, b jsou nesoudělná.

Předcházejících poznatků můžeme využít též při hledání největšího společného dělitele daných čísel, což ukážeme nejprve na číselném příkladě.

Příklad 29. Vyhledejte $d = (198, 288, 300, 384)$

a) $(198, 288, 300, 384) = (198, 288-198, 300-198, 384-198) = (198, 90, 102, 186) = (198-2.90, 90, 102-90, 186-2.90) = (18, 90, 12, 6) = (18-3.6, 90-15.6, 12-2.6, 6) = (0, 0, 0, 6) = 6.$

V daném souboru čísel zvolili jsme číslo 198, které jsme odečetli od všech tří čísel zbývajících; pak jsme si vybrali opět nejmenší číslo souboru, tj. 90, a jeho násobky jsme odčítali od ostatních tří čísel tak, že jsme místo těchto tří čísel dostali zbytky při jejich dělení číslem 90. Další postup je již zřejmý. Číslo 6 se objevilo v poslední čtveřici čísel jako hledané číslo d, které je vlastně číslem tvaru (5,2). Výsledek nezáleží ovšem na tom, užijeme-li pro odčítání násobků nejmenšího čísla čtveřice, jak je to zřejmé z druhého řešení této úlohy.

b) $(198, 288, 300, 384) = (198 - 0.288, 288, 300 - 1.288, 384 - 1.288) = (198, 288, 12, 96) = (198 - 16.12, 288 - 24.12, 12, 96 - 8.12) = (6, 0, 12, 0) = (6, 0, 12 - 2.6, 0) = (6, 0, 0, 0) = 6.$

Příklad 30. Rozhodněte, zda rovnice $4453x + 5767y + 6497z = 1$ má řešení v oboru čísel celých.

Určíme $d = (4453, 5767, 6497) =$
$= (4453, 5767-4453, 6497-4453) = (4453, 1314, 2044) = (4453-3.1314, 1314, 2044-1314) = (511, 1314, 730) = (511, 1314 - 2.511, 730 - 511) = (511, 292, 219) = (511 - 2.219, 292 - 219, 219) = (73, 73, 219) =$
$= (73, 73 - 1.73, 219 - 3.73) = (73, 0, 0) = 73.$

Poněvadž $d = 73$, nejsou daná čísla nesoudělná a daná rovnice nemá řešení v oboru celých čísel (podle věty $\mathbf{T}_{29}$). Kdybychom však danou rovnici pozměnili tak, že by na pravé straně místo čísla 1 byl kterýkoli násobek čísla 73, měla by takto pozměněná rovnice řešení (podle věty $\mathbf{T}_{28}$) v oboru celých čísel.

Hledání největšího společného dělitele daných celých čísel můžeme usnadnit a zkrátit při znalosti některých poznatků, jež jsme tu neuvedli. Snad některé z nich sami najdete a dokážete. Mimoto v kapitole 7 poznáme ještě jiný způsob výpočtu největšího společného dělitele.

Cvičení

5,1. Dané zlomky převeďte na základní tvar:
$\frac{534}{1335}$; $\frac{9\,167}{11\,639}$; $\frac{9\,797}{10\,379}$; $\frac{610}{1597}$; $\frac{987}{1595}$.

5,2. Je dán zlomek $\frac{5x + 6}{8x + 7}$. Najděte množinu všech celých čísel x, která po dosazení do daného zlomku dávají takové zlomky, jež lze krácením převést na základní tvar.

5,3. Pro které celočíselné hodnoty x lze zlomek $\frac{6x^2 + 1}{12x^2 + 7}$ krácením převést na základní tvar?

5,4. Rozhodněte, ve kterých případech mají dané rovnice řešení v oboru čísel celých:
a) $37x + 61y = 1$; b) $4x + 5y + 6z = 1$; c) $49x + 84y = 1$; d) $49x + 84y = 7$; e) $49x + 84y = 14$.

5,5. Jestliže zlomek $\frac{p}{q}$ je pravý zlomek v základním tvaru, pak také zlomek $\frac{q-p}{q}$, který doplňuje zlomek $\frac{p}{q}$ do 1, je rovněž v základním tvaru. Dokažte.

5.6. Jaké podmínky musí splňovat čísla a, b, aby platilo $(a, b) = (a + b, a - b)$?

5,7. Dokažte, že platí $(ac, bc) = c\,(a, b)$.

6. kapitola

NEJMENŠÍ SPOLEČNÝ NÁSOBEK

D$_{15}$ *Společný násobek celých čísel* $b_1, b_2, b_3, \ldots, b_k$ $(k \geqq 2)$ *nazýváme každé celé číslo* a, *pro něž platí zároveň vztahy* $b_1 \mid a, b_2 \mid a, b_3 \mid a, \ldots, b_k \mid a$.

Existuje vždy aspoň jeden společný násobek čísel $b_1, b_2, b_3, \ldots, b_k$. Je-li jedno z těchto čísel, např. $b_k = 0$, pak b_k je dělitelem čísla a, jen když $a = 0$; v tom případě existuje jen jediný společný násobek $a = 0$. Jsou-li všechna čísla $b_1, b_2, b_3, \ldots, b_k$ různá od nuly, pak existuje nekonečně mnoho společných násobků daných čísel. Patří k nim jejich součin $b_1 b_2 b_3 \ldots b_k$ a každý jeho násobek $cb_1 b_2 b_3 \ldots b_k$, kde c je libovolné celé číslo. Již z věty **T**$_6$ plyne, že množina všech společných násobků celých čísel $|b_1|, |b_2|, |b_3|, \ldots | b_k |$ je totožná s množinou všech společných násobků čísel $b_1, b_2, b_3, \ldots, b_k$, a proto budeme řešit úlohy o společném násobku zpravidla jen v těch případech, kdy daná čísla jsou celá nezáporná nebo celá kladná, tj. přirozená. Přitom se budeme zajímat skoro výlučně jen o přirozená čísla, která jsou společným násobkem daných čísel, ale budeme si přitom vědomi toho, že v množině všech společných násobků daných čísel se vyskytuje s každým číslem a i číslo opačné $-a$.

D$_{16}$ *Nejmenší společný násobek celých čísel* $b_1, b_2, b_3, \ldots, b_k$, *jež jsou všechna různá od nuly, nazýváme nejmenší přirozené číslo* m, *pro které platí* $b_1 \mid m, b_2 \mid m, b_3 \mid m, \ldots, b_k \mid m$; *označujeme je zpravidla* $[b_1, b_2, b_3, \ldots, b_k]$.

Příklad 31. Jsou dána čísla $b_1 = 12$, $b_2 = 15$, $b_3 = 30$. Vyhledejme: a) množiny všech přirozených čísel, která jsou násobky daných čísel; b) $[b_1, b_2]$; c) $[b_1, b_2, b_3]$.

a) Hledané množiny přirozených čísel, která jsou násobky daných čísel, jsou:

$M_1 = \{12, 24, 36, 48, 60, 72, 84, \ldots\}$,
$M_2 = \{15, 30, 45, 60, 75, 90, \ldots\}$,
$M_3 = \{30, 60, 90, 120, \ldots\}$. Kdybychom ovšem měli najít množiny všech násobků daných čísel, bylo by nutné prvky každé z množin M_1, M_2, M_3 rozmnožit o čísla k nim opačná a o číslo 0.

b) Množina všech přirozených čísel, která jsou společnými násobky čísel b_1, b_2, je $P = \{60, 120, 180, \ldots\}$, která je průnikem množin M_1, M_2. Její nejmenší prvek je 60 a proto $[b_1, b_2] = 60$.

c) Množina všech přirozených čísel, která jsou společnými násobky čísel b_1, b_2, b_3 je $Q = \{60, 120, 180, \ldots\}$ a dostaneme ji jako průnik množin M_1, M_2, M_3; ten ovšem můžeme vyhledat tak, že určíme průnik množin P, M_3. Nejmenší prvek množiny Q je 60 a proto $[b_1, b_2, b_3] = 60$. Postup při jeho určení je možno naznačit $[b_1, b_2, b_3] = [[b_1, b_2], b_3]$. Snadno se přesvědčíme, že ke stejnému výsledku dojdeme cestou $[b_1, b_2, b_3] = [b_1, [b_2, b_3]]$ nebo též $[b_1, b_2, b_3] = [[b_1, b_3], b_2]$.

Sami si jistě dovedete zdůvodnit vztah $[b_1, b_2, b_3, b_4] = [[b_1, b_2, b_3], b_4]$ nebo obecně $[b_1, b_2, b_3, \ldots, b_k, b_{k+1}] = [[b_1, b_2, b_3, \ldots, b_k], b_{k+1}]$ a využít ho při hledání nejmenšího společného násobku daných čísel.

Příklad 32. Najděte nejmenší takové přirozené číslo, že po přičtení čísel 20, 25, 30 dostanete taková tři čísla, z nichž první je dělitelné čtyřmi, druhé pěti, třetí šesti.

Označíme-li hledané číslo x, pak musí zřejmě platit zároveň vztahy:

$$4 \mid x + 20; 5 \mid x + 25; 6 \mid x + 30.$$

Poněvadž $4 \mid 20$, bude platit $4 \mid x + 20$ právě tehdy, když bude platit $4 \mid x$ (podle věty $\mathbf{T}_{10}$). Obdobně zjistíme, že musí platit též $5 \mid x$, $6 \mid x$. Číslo x, které vyhovuje zároveň třem podmínkám $4 \mid x$, $5 \mid x$, $6 \mid x$, je společným násobkem čísel 4, 5, 6. Úloha vyžaduje, abychom našli nejmenší přirozené číslo x dané vlastnosti, tj. číslo $[4, 5, 6]$. Číslo $[4, 5] = 20$ snadno zpaměti najdeme na základě znalosti malé násobilky. Proto $[4, 5, 6] = [[4, 5], 6] = [20, 6] = 60$, přičemž poslední krok učiníme tak, že z přirozených násobků čísla 20, tj. 20, 40, 60, 80, ... najdeme ten nejmenší, který je dělitelný 6. Zjistili jsme tedy, že hledané číslo je 60.

$\mathbf{T}_{30}$ *Nejmenší společný násobek čísel $b_1, b_2, b_3, \ldots, b_k$ je dělitelem každého společného násobku čísel $b_1, b_2, b_3, \ldots, b_k$.*

Označme n libovolný společný násobek přirozených čísel $b_1, b_2, b_3, \ldots, b_k$ a $m = [b_1, b_2, b_3, \ldots, b_k]$, což podle definice $\mathbf{D}_{12}$ je nejmenší (minimální) prvek množiny N všech přirozených čísel, která jsou společnými násobky čísel $b_1, b_2, b_3, \ldots, b_k$. Avšak podle věty $\mathbf{T}_{11}$ můžeme k číslům n, m vyhledat taková celá čísla q, r, že platí vztahy

$$n = mq + r, \; 0 \leqq r < m.$$

Dokážeme-li, že $r = 0$ čili $n = mq$, znamená to $m \mid n$, což je tvrzení věty $\mathbf{T}_{30}$. To však dokážeme tím, že z předpokladu

$$n = mq + r, \; 0 < r < m \tag{6,1}$$

odvodíme spor. Ze vztahů (6,1) však plyne

$$r = n - mq, \; 0 < r < m. \tag{6,2}$$

Poněvadž n je společný násobek čísel $b_1, b_2, b_3, \ldots, b_k$, existují taková celá čísla $q_1, q_2, q_3, \ldots, q_k$, že

$$n = b_1 q_1 = b_2 q_2 = b_3 q_3 = \ldots = b_k q_k; \qquad (6,3)$$

poněvadž m je též společným násobkem čísel $b_1, b_2, b_3, \ldots, b_k$, existují celá čísla $s_1, s_2, s_3, \ldots, s_k$, že platí

$$m = b_1 s_1 = b_2 s_2 = b_3 s_3 = \ldots = b_k s_k. \qquad (6,4)$$

Užitím rovností (6,3) a (6,4) dostaneme po dosazení do (6,2) tyto rovnosti: $r = b_1 q_1 - b_1 s_1 q = b_1 (q_1 - s_1 q)$,
$r = b_2 q_2 - b_2 s_2 q = b_2 (q_2 - s_2 q), \ldots,$
$r = b_k q_k - b_k s_k q = b_k (q_k - s_k q)$.
Z těchto rovností však plyne, že přirozené číslo r je též společným násobkem čísel $b_1, b_2, b_3, \ldots, b_k$, o němž však platí $r < m$, což je ve sporu s předpokladem, že číslo m je nejmenší společný násobek čísel $b_1, b_2, b_3, \ldots, b_k$. Tento spor dokazuje, že musí platit $r = 0$, a tedy $m \mid n$, což jsme měli dokázat.

Příklad 33. Najděte největší trojciferné číslo x, z něhož po přičtení čísel 20, 25, 30 dostaneme 3 čísla taková, že první je dělitelné 4, druhé 5, třetí 6.

Z řešení příkladu 29 již víme, že číslo x musí být společným násobkem čísel 4, 5, 6 a že $[4, 5, 6] = 60$. Avšak z věty $\mathbf{T}_{30}$ plyne, že každý společný násobek daných čísel je násobkem jejich nejmenšího společného násobku, tj. v našem případě je tvaru $60k$, kde k je libovolné číslo celé. Z podmínek uvedených v dané úloze plyne, že je třeba najít největší celé číslo k, aby platilo $60k < 1000$, má-li být číslo $x = 60k$ trojciferné. Snadno pak najdeme, že $k < \frac{1000}{60} = 16\frac{2}{3}$. Proto hledané číslo $x = 60.16 = 960$.

Příklad 34. Je-li $d = (a_1, a_2)$ největší společný dělitel přirozených čísel a_1, a_2, pak $a_1 = dq_1$, $a_2 = dq_2$, kde q_1, q_2

jsou (nesoudělná) čísla přirozená a nejmenší společný násobek je $m = [a_1, a_2] = dq_1\, q_2$. Dokažte toto tvrzení.
Číslo $n = dq_1q_2$ je jistě společným násobkem čísel a_1, a_2, neboť $n = dq_1q_2 = (dq_1)q_2 = a_1q_2$, $n = dq_1q_2 = (dq_2)q_1 = a_2q_1$. Je však ještě třeba dokázat, že číslo n má vlastnosti čísla $m = [a_1, a_2]$, k čemuž použijeme věty $\mathbf{T}_{30}$, podle níž číslo m je dělitelem čísla n, čili $n = cm$, kde $c \geqq 1$.

Užitím daných rovností $a_1 = dq_1$, $a_2 = dq_2$ dostaneme $a_1a_2 = dq_1 . dq_2 = (dq_1q_2)d = nd = cmd$. Avšak z rovnosti

$$a_1\, a_2 = cmd \tag{6,5}$$

plynou vztahy

$$a_1 = \frac{m}{a_2} . cd = k_2cd,\ a_2 = \frac{m}{a_1} . cd = k_1cd, \tag{6,6}$$

kde $k_1 = \frac{m}{a_1}$, $k_2 = \frac{m}{a_2}$ jsou zřejmě přirozená čísla. Avšak z rovností (6,6) plyne, že čísla a_1, a_2 mají společného dělitele cd; přitom však víme, že každý společný dělitel je nejvýš rovný největšímu společnému děliteli, tj. $cd \leqq d$, odkud plyne $c \leqq 1$. Má-li však platit zároveň $c \geqq 1$, $c \leqq 1$, pak je nutně $c = 1$.

Dosadíme-li do rovnosti (6,5) $c = 1$, dostaneme vztah $md = a_1\, a_2$, který vyjádříme následující větou $\mathbf{T}_{31}$.

$\mathbf{T}_{31}$ *Jsou-li a_1, a_2 přirozená čísla, pak platí* $[a_1, a_2].(a_1, a_2) = a_1a_2$.

Důsledek I. *Nejmenší společný násobek dvou nesoudělných přirozených čísel a_1, a_2 se rovná jejich součinu a_1a_2.*

Tento důsledek plyne z věty $\mathbf{T}_{31}$, když uvážíme, že pro nesoudělná čísla a_1, a_2 platí $(a_1, a_2) = 1$.

Důsledek II. *Nejmenší společný násobek přirozených čísel $a_1, a_2, a_3, \ldots, a_k$, která jsou po dvou nesoudělná, se rovná jejich součinu $a_1a_2a_3 \ldots a_k$.*

Tato věta je zobecněním předcházející věty a dokáže se užitím matematické indukce. Při užívání této věty v praxi musíme si dobře všimnout, zda pro daná přirozená čísla $a_1, a_2, a_3, \ldots, a_k$ je splněna podmínka, aby byla po dvou nesoudělná, když $k > 2$. Slabší podmínka $(a_1, a_2, a_3, \ldots, a_k) = 1$ není při $k > 2$ postačující k tomu, aby součin daných přirozených čísel byl zároveň jejich nejmenším společným násobkem.

Příklad 35. Vypočtěte: a) (63, 147), [63, 147]; b) (5, 36, 54), [5, 36, 54]; c) (4, 11, 15), [4, 11, 15].

a) $(63, 147) = (63, 147-63.2) = (63, 21) = (63 - 21.3,21) = (0,21) = 21$; $[63, 147] = \frac{63.147}{(63;147)} = \frac{63.147}{21} = 3.147 = 441.$

b) $(5, 36) = (5, 1) = 1$, $(5, 36, 54) = ((5, 36), 54) = (1,54) = 1$.
Jsou tedy daná čísla 5, 36, 54 nesoudělná; nejsou však po dvou nesoudělná, neboť $(36, 54) = (36, 18) = (0, 18) = 18$. Dále je $[5, 36] = 5.36 = 180$ (viz důsledek I) a $[5, 36, 54] = [[5, 36], 54] = [180, 54]$. Snadno se určí $(180,54) = (18, 54) = (18, 0) = 18$.
Proto $[180, 54] = \frac{180.54}{18} = 540.$

c) $(4, 11, 15) = ((4, 11), 15) = (1, 15) = 1$. Poněvadž zřejmě platí $(4, 11) = 1, (4, 15) = 1, (11, 15) = 1$, jsou daná čísla 4, 11, 15 po dvou nesoudělná a proto (viz důsledek II) platí: $[4, 11, 15] = 4.11.15 = 660$.

T$_{32}$ *Jsou-li celá čísla $b_1, b_2, b_3, \ldots, b_k$ děliteli celého čísla a, pak také jejich nejmenší společný násobek je dělitelem čísla a, tj.* $[b_1, b_2, b_3, \ldots, b_k] \mid a$.

Z předpokladu věty plyne, že číslo a je společným násobkem čísel $b_1, b_2, b_3, \ldots, b_k$, který podle věty $\mathbf{T}_{30}$ je dělitelný číslem $[b_1, b_2, b_3, \ldots, b_k]$.

Této věty často používáme při vyšetřování dělitelnosti daných čísel. Tak např. při řešení příkladu 4 jsme našli $3 \mid a$, $4 \mid a$, $13 \mid a$, odkud podle věty $\mathbf{T}_{32}$ ihned plyne $156 \mid a$. Při vyšetřování dělitelnosti téhož čísla a v příkladě 15 jsme našli $3 \mid a$, $4 \mid a$, $5 \mid a$, odkud podle věty $\mathbf{T}_{32}$ plyne $60 \mid a$. Z těchto dvou výsledků $156 \mid a$, $60 \mid a$ plyne ovšem $[156, 60] \mid a$, tj. $780 \mid a$, neboť $[156, 60] = \frac{156.60}{(156,60)} = \frac{156.60}{12} = 780$.

V kap. 7 poznáme ještě jiný způsob výpočtu nejmenšího společného násobku daných čísel.

Cvičení

6,1. Najděte nejmenší trojciferné číslo, které při dělení čísly 12 a 18 dává zbytek 5.

6,2. Běžec, který oběhne uzavřenou závodní dráhu za 7 minut, startoval k běhu v témže okamžiku jako motocyklista, který tutéž závodní dráhu objede za 80 vteřin. Vypočtěte dobu, po které se běžec poprvé setká s motocyklistou opět na místě startu, kolik kol v té době uběhl běžec a kolik kol ujel motocyklista.

6,3. Vyhledejte takové nejmenší přirozené číslo, že při jeho dělení čísly 2, 3, 4, 5, 6, 7, 8, 9 (v tomto pořadí) dostanete vždy neúplný podíl se zbytkem, který je v každém případě o 1 menší než dělitel, tj. tedy při dělení dvěma zbytek 1, při dělení třemi zbytek 2, při dělení čtyřmi zbytek 3 atd.

6,4. Dokažte, že pro každé celé číslo x polynom $x^5 - 5x^3 + 4x$ nabývá celočíselných funkčních hodnot, které jsou násobky čísla 120.

7. kapitola

PRVOČÍSLA A ČÍSLA SLOŽENÁ

Z rozboru věty $\mathbf{T}_6$ víme, že zkoumání vlastností vztahu $b \mid a$ pro celá čísla a, b lze převést na vyšetřování dělitelnosti v oboru čísel celých nezáporných nebo dokonce často jen v oboru čísel přirozených. Zejména v této kapitole se budeme zabývat hlavně dělitelností přirozených čísel přirozenými děliteli, tj. takovými děliteli, které patří do oboru čísel přirozených.

Číslo 0 je jediné celé číslo, jehož dělitelem je každé celé číslo. Je to jediné celé číslo, které má nekonečně mnoho celých a také nekonečně mnoho přirozených dělitelů.

Každé přirozené číslo n má jen konečný počet přirozených dělitelů, který označíme $\Theta(n)$; (značka Θ je velké řecké písmeno, odpovídající skupině souhlásek th a čteme ji theta). $\Theta(n)$ je funkce, která každému přirozenému číslu n přiřazuje počet jeho přirozených dělitelů. Definičním oborem této funkce je množina všech přirozených čísel a jejím grafem množina izolovaných bodů. Část grafu této funkce můžeme sestrojit, když si připravíme tabulku, jejíž část je dále uvedena.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\Theta(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6

Snadnou úvahou si potvrdíme, co je zřejmé již z tabulky, že množinu všech přirozených čísel můžeme rozdělit na 3 části takto: 1) množinu s jediným prvkem 1, který má jen jednoho přirozeného dělitele, 2) množinu všech přiroze-

ných čísel, která mají dva různé přirozené dělitele, tj. čísel 2, 3, 5, 7, 11, 13, 17, 19, ..., 3) množinu všech přirozených čísel, která mají více než dva různé přirozené dělitele, tj. množinu čísel 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, ...; toto roztřídění přirozených čísel vede k zavedení následujících definic:

$\mathbf{D}_{17}$ *Prvočíslo nazýváme každé přirozené číslo, které má právě dva různé přirozené dělitele.*

$\mathbf{D}_{18}$ *Číslo složené nazýváme každé přirozené číslo, které má více než dva různé přirozené dělitele.*

Podle předchozích definic nepatří přirozené číslo 1 ani mezi prvočísla, ani mezi čísla složená. Kdybychom ovšem přijali jinou definici prvočísla, mohlo by se stát, že by mezi ně bylo zahrnuto i číslo 1. Tak by to bylo např. v tom případě, kdybychom za prvočíslo pokládali to přirozené číslo, které je dělitelné číslem 1 a sebou samým. Z tohoto příkladu opět vidíme, že význam určitého názvu je závislý na definici, která vyjadřuje umluvený význam názvu.

$\mathbf{T}_{33}$ *Je-li možno rozložit přirozené číslo* $n > 1$ *na součin takových přirozených čísel* a, b, *že* $a > 1$, $b > 1$, *pak je* n *číslo složené; není-li takový rozklad možný, pak* n *je prvočíslo.*

Je-li totiž $n = ab > 1$, $a > 1$, $b > 1$, pak číslo n má zřejmě aspoň 4 přirozené dělitele $(1 \mid n, a \mid n, b \mid n, n \mid n)$, když $a \neq b$, a aspoň 3 různé přirozené dělitele $(1 \mid n, a \mid n, a^2 \mid n)$, když $a = b$, a proto ve shodě s $\mathbf{D}_{18}$ je n číslo složené. Není-li takový rozklad čísla $n > 1$ možný, pak má číslo n zřejmě právě 2 dělitele $(1 \mid n, n \mid n)$ a ve shodě s definicí $\mathbf{D}_{17}$ je n prvočíslo.

$\mathbf{T}_{34}$ *Každé přirozené číslo* $n > 1$ *má alespoň jednoho prvočíselného dělitele.*

Číslo $n > 1$ má jistě aspoň jednoho dělitele, který je větší než 1. Z těchto jeho dělitelů je jeden nejmenší; označme jej p. Tento nejmenší přirozený dělitel $p > 1$ musí být prvočíslem. Kdyby totiž p bylo číslo složené, tj. $p = ab$, kde $1 < a < p$, $1 < b < p$, pak by ze vztahů $a \mid p$, $p \mid n$ plynulo $a \mid n$, což by znamenalo, že existuje dělitel $a < p$ čísla n v rozporu s naším předpokladem o čísle p.

$\mathbf{T}_{35}$ *Každé složené číslo n má alespoň jednoho prvočíselného dělitele $p \leqq \sqrt{n}$.* Jinak řečeno: *Není-li přirozené číslo $n > 1$ dělitelné žádným prvočíslem $p \leqq \sqrt{n}$, pak je n prvočíslo.*

Je-li n číslo složené, pak existuje rozklad $n = ab$, kde a, b jsou taková přirozená čísla, že $1 < a < n$, $1 < b < n$. Při vhodném označení činitelů rozkladu čísla n na součin můžeme předpokládat $a \leqq b < n$. V tom případě $a^2 \leqq ab = n$ a odtud plyne $a \leqq \sqrt{n}$. Avšak číslo a má aspoň jednoho prvočíselného dělitele $p \leqq a \leqq \sqrt{n}$. Ze vztahů $p \mid a$, $a \mid n$ plyne $p \mid n$.

Chceme-li v množině všech přirozených čísel, která nejsou větší než dané přirozené číslo n vyhledat všechna prvočísla, můžeme tak učinit způsobem, který se označuje názvem *Eratosthenovo síto*. Jeho popis i podrobnější vysvětlení najdete ve svazku 2 této knižnice. Tam najdete také informace o některých tabulkách prvočísel, jež byly a jsou vydávány pro potřebu matematiků, pracujících v číselné teorii.

Všechna prvočísla můžeme seřadit v rostoucí posloupnost prvočísel, jejíž n-tý člen označujeme zpravidla p_n. Z této posloupnosti prvočísel známe od r. 1959, kdy byly vydány dosud nejrozsáhlejší tabulky prvočísel, všechna prvočísla p_n, pro něž platí $n < 6\,000\,000$. Z posloupnosti

prvočísel uvádíme tyto příklady: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29, \ldots, p_{30} = 113$, $p_{31} = 127, \ldots, p_{96} = 503, \ldots$, $p_{100} = 541, \ldots, p_{200} = 1223, \ldots, p_{300} = 1987, \ldots$, $p_{400} = 2741, \ldots, p_{500} = 3571, \ldots, p_{1000} = 7919, \ldots$, $p_{5999\,999} = 104\,395\,301$. O některých dalších prvočíslech mnohem větších než číslo 104 395 301 se ještě dovíte v kap. 10, za níž je zařazena tabulka všech po sobě jdoucích prvočísel od 2 do 1987. Používejte ji při řešení některých úloh, z nichž jednu ihned rozřešíme, abychom si osvětlili praktický význam vět $\mathbf{T}_{33}$ a $\mathbf{T}_{35}$.

Příklad 36. O číslech $m = 255\,989$ a $n = m + 1 = 255\,990$ rozhodněte, zda jsou složená nebo prvočísla.

Dělíme-li číslo m postupně prvočísly $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots p_{95} = 499, p_{96} = 503$, zjistíme, že číslo m není dělitelné žádným z těchto prvočísel. Další dělení nemusíme již provádět, neboť jsme zjistili, že číslo m není dělitelné žádným prvočíslem $p \leq \sqrt{255\,989} < 506$, a že je tedy prvočíslo (podle věty $\mathbf{T}_{35}$). Pro vyšetření čísla n stačí uvést snadný rozklad $n = 10.255\,99$, z něhož plyne, že číslo n je složené (podle věty $\mathbf{T}_{33}$).

K rozkladu čísla $n = 255\,990$ poznamenáváme, že je možný i jiný jeho rozklad v součin dvou přirozených čísel, poněvadž snadno najdeme dělitele 2, 3, 5, 7 daného čísla. Když najdeme rozklad $n = 2.3.5.7.1219$, můžeme po nahlédnutí do tabulek zjistit, že 1219 není prvočíslo. Najdeme-li jeho rozklad $1219 = 23.53$, můžeme zapsat $n = 2.3.5.7.23.53$. V tomto součinu je každý činitel prvočíslo. Rozklad čísla n na součin prvočísel nazýváme *rozkladem čísla n v prvočinitele.*

Při nahlédnutí do tabulky prvočísel jste si jistě všimli toho, že v rostoucí posloupnosti všech přirozených čísel jsou prvočísla nepravidelně rozložena. Tak např. mezi

prvočísly 71 a 73 je rozdíl 2, takže mezi nimi leží jediné číslo složené, zatímco mezi prvočísly 89 a 97 je rozdíl 8, takže mezi nimi leží 7 čísel složených (90, 91, 92, 93, 94, 95, 96). Snad si přitom položíte otázku, jak velký je počet prvočísel. Dříve, než na ni odpovíme, připravíme vás na jedno řešení této úlohy definicí čísla $n!$ a příkladem.

$\mathbf{D}_{19}$ *Součin všech přirozených čísel, která nejsou větší než dané přirozené číslo n, tj. součin* $1.2.3.4\ldots(n-1)n$ *označujeme symbolem* $n!$ *a čteme n faktoriál; mimoto definujeme* $0! = 1$.

Snadno vypočteme, že $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$, $7! = 5040$, $8! = 40\,320$, $9! \doteq$ $\doteq 362\,880$, $10! = 3\,628\,800$ atd. Ve Valouchových tabulkách najdeme tabulku faktoriálů pro všechna $n \leqq 30$, z níž zjistíme, že např. $30!$ má zápis v desítkové soustavě o 33 cifrách. Jsou tam též dekadické logaritmy všech faktoriálů $n! \leqq 200!$, z nichž např. vyčteme, že $\log 112! \doteq$ $\doteq 182\,295\,458\ldots$, což znamená, že číslo $112!$ má při zápise v desítkové soustavě 183 cifer.

Příklad 37. Dokažte, že existuje prvočíslo větší než libovolné dané přirozené číslo n.

Číslo $n! = 1.2.3.\ldots.(n-1)n$ je jistě dělitelné každým přirozeným číslem $x \leqq n$, avšak číslo $n! + 1 > n$ není dělitelné žádným z čísel $2, 3, \ldots, n-1, n$, neboť při dělení kterýmkoli z nich dostaneme neúplný podíl a zbytek 1. Podle věty $\mathbf{T}_{34}$ má každé přirozené číslo větší než 1 aspoň jednoho prvočíselného dělitele p. Platí tedy i v tomto případě $p \mid n! + 1$, o němž však víme, že $p > n$.

$\mathbf{T}_{36}$ *Prvočísel je nekonečně mnoho.*

Nepřímý důkaz věty $\mathbf{T}_{36}$ je snadný. Předpokládejme, že množina všech prvočísel je konečná. V tom případě může-

me najít takové přirozené číslo n, že pro každé prvočíslo p platí $p \leqq n$; stačí k tomu zvolit za n největší prvočíslo z předpokládané konečné množiny všech prvočísel. To však je ve sporu s výsledkem naší úvahy v příkladu 37, v němž jsme dokázali, že lze najít vždy prvočíslo p, které je větší než libovolně dané přirozené číslo n. Není tedy možné, aby platil předpoklad o konečnosti množiny všech prvočísel. Platí jeho popření (negace), což je věta $\mathbf{T}_{36}$.

Překvapuje, že otázku o počtu prvočísel si položili již řečtí matematikové a s úspěchem ji rozřešili. Důkaz o tom, že prvočísel je nekonečně mnoho, najdeme již v IX. knize slavného Euklidova díla Stoichéia (Základy)*). Euklides (365?—300? před n. l.) uvedl důkaz jiný, ale základní idea důkazu jím uvedeného i důkazu námi provedeného je společná. Volili jsme pozměněný důkaz jen proto, abyste rychleji pochopili důkaz následující věty.

$\mathbf{T}_{37}$ *Je-li dáno libovolné přirozené číslo m, můžeme vždy najít m po sobě jdoucích přirozených čísel takových, že každé z nich je číslo složené.*

Utvoříme posloupnost m po sobě jdoucích přirozených čísel $a_1 = (m+1)! + 2$, $a_2 = (m+1)! + 3$, $a_3 = (m+1)! + 4$, ..., $a_m = (m+1)! + (m+1)$. Platí zřejmě: $2 \mid a_1$, neboť každý ze sčítanců je dělitelný dvěma, $3 \mid a_2$, neboť každý ze sčítanců je dělitelný třemi, ... $m+1 \mid a_m$, neboť každý ze sčítanců $(m+1)!$, $m+1$ je dělitelný číslem $m+1$. Tím je dokázána existence posloupnosti m po sobě jdoucích čísel složených.

Zvolíme-li např. $m = 7$, pak jistě posloupnost sedmi po sobě jdoucích přirozených čísel $8! + 2$, $8! + 3$, $8! + 4$, $8! + 5$, $8! + 6$, $8! + 7$, $8! + 8$, tj. čísel 40 322, 40 323,

*) Místo původního řeckého jména Eukleides se užívá latinizovaného jména Euklides, poněvadž jeho dílo Stoichéia (Základy) stalo se nejvíce známým z latinského překladu Elementa (Základy).

40 324, 40 325, 40 326, 40 327, 40 328 má za členy jen čísla složená. Užitím rozsáhlejších tabulek prvočísel byste mohli snadno zjistit, že právě nalezená posloupnost sedmi po sobě jdoucích čísel složených je vybrána z posloupnosti 53 po sobě jdoucích čísel složených, která začíná číslem 40 290 a končí číslem 40 342. Víme tedy nyní, že existenci sedmi po sobě jdoucích čísel složených lze dokázat různými příklady, k nimž patří i dříve nalezená čísla 90, 91, 92, 93, 94, 95, 96.

Kdybychom chtěli najít 111 po sobě jdoucích čísel složených metodou, kterou jsme ukázali při důkazu věty $\mathbf{T}_{37}$, pak bychom ihned mohli udat jako první člen takové posloupnosti číslo $112! + 2$, jehož zápis v desítkové soustavě má 183 cifer. Ale užitím některých rozsáhlejších tabulek prvočísel bychom mohli zjistit, že již mezi prvočísly 370 261 a 370 373 leží 111 čísel složených. Konstrukce číselné posloupnosti, kterou jsme popsali při důkazu věty $\mathbf{T}_{37}$, neslouží ovšem k tomu, abychom pomocí ní hledali m nejmenších po sobě jdoucích čísel složených, ani k tomu, abychom hledali interval ohraničený dvěma prvočísly, mezi nimiž leží právě m čísel složených. Má význam hlavně tím, že nám zajišťuje existenci posloupnosti m po sobě jdoucích čísel složených. Víme nyní, že na otázku, zda existuje např. milión po sobě jdoucích čísel složených, je odpověď kladná.

$\mathbf{T}_{38}$ *Každé přirozené číslo $n > 1$ je možno rozložit v součin $n = p_1 p_2 p_3 \dots p_{k-1} p_k$, v němž $p_1, p_2, \dots, p_k$ jsou prvočísla, k je číslo přirozené, takže nevylučujeme případ, kdy součin má jediného činitele. Takový rozklad čísla se nazývá rozklad v prvočinitele a je možný jen jediným způsobem, má-li platit $p_1 \leqq p_2 \leqq p_3 \dots \leqq p_k$, nebo nepokládáme-li za různé rozklady lišící se jen pořadím prvočinitelů.*

Podle věty T_{34} má každé přirozené číslo $n > 1$ aspoň jednoho prvočíselného dělitele, z nichž nejmenší označme p_1. Platí pak $n = p_1 n_1$, kde $n_1 \geqq 1$. Je-li $n_1 = 1$, pak $n = p_1$ v souhlase s uvedenou větou. Je-li $n_1 > 1$, najdeme opět nejmenší prvočíselný dělitel p_2 čísla n_1, takže platí $n_1 = p_2 . n_2$, kde $n_2 \geqq 1$; odtud $n = p_1 p_2 n_2$. Je-li $n_2 = 1$, pak $n = p_1 p_2$. Není-li $n_2 = 1$, pokračujeme dále v rozkladu obdobným způsobem a dostaneme $n_2 = p_3 n_3$, odkud $n = p_1 p_2 p_3 n_3$ atd., až konečně dospějeme k rozkladu $n_{k-1} = p_k n_k$, kde $n_k = 1$, a proto $n = p_1 p_2 \ldots p_k$. Je zřejmé, že při tomto způsobu postupného vybírání nejmenších prvočíselných dělitelů p_1, p_2, p_3 atd. musíme dospět vždy k témuž rozkladu daného čísla n v prvočinitele. Lze ovšem namítnout, že bychom snad mohli dospět k jinému rozkladu čísla n v prvočinitele, kdybychom prvočíselné dělitele rozkládaných čísel vybírali podle jiného pravidla než v postupu právě popsaném, kdy jsme pro každé rozkládané číslo vybrali za prvního činitele jeho nejmenší prvočíselný dělitel. Ještě v tomto článku ukážeme jinou metodou jednoznačnost rozkladu přirozeného čísla v prvočinitele, a to tak, že uvedená námitka odpadne.

T_{39} *Každé přirozené číslo $n > 1$ je možno rozložit v součin přirozených mocnin různých prvočísel $q_1, q_2, \ldots, q_m$ tak, že*

$$n = q_1^{r_1} q_2^{r_2} q_3^{r_3} \ldots q_m^{r_m},$$

a to jediným způsobem, má-li platit $q_1 < q_2 < q_3 \ldots < q_m$ nebo nepokládáme-li za různé takové rozklady, jež se liší jen pořadím činitelů. Tento rozklad se často nazývá kanonický rozklad přirozeného čísla $n > 1$ v prvočinitele.

Tento rozklad se liší od předcházejícího jen tím, že součin

stejných prvočinitelů je nahrazen mocninou, jejímž základem je příslušné prvočíslo a mocnitelem přirozené číslo.

Příklad 38. Rozložte v prvočinitele tato čísla: a) 360, b) 420, c) 2047, d) 4519.

a) $360 = 2.180 = 2.2.90 = 2.2.2.45 = 2.2.2.3.15 = 2.2.2.3.3.5 = 2^3.3^2.5.$

V tomto příkladě jsme chtěli osvětlit postup výše popsaný i tím, že jsme postupně hledali prvočinitele tvořící neklesající posloupnost. Jinak však je možno rozklad urychlit způsobem dále naznačeným:

b) $420 = 42.10 = 6.7.2.5 = 2.2.3.5.7 = 2^2.3.5.7.$

c) $2047 = 23.89.$

První činitel 23 najdeme tak, že nejprve zkoumáme, zda dané číslo má prvočíselné dělitele 2, 3, 5, 7, 11, 13, 17, 19 a konečně 23. Zjistíme-li tak, že $2047 = 23.89$, ustaneme již v dalším rozkládání, když totiž zpaměti (tj. ze znalosti malé násobilky) nebo z tabulky I zjistíme, že 89 je prvočíslo.

d) Při hledání rozkladu čísla 4519 zkoumáme opět jeho dělitelnost čísly 2, 3, 5, 7, 11, 13, ..., 61, 67, neboť $p = 67$ je poslední prvočíslo, pro něž platí $p \leqq \sqrt{4519} \doteq 67{,}2$ (viz $\mathbf{T}_{35}$).

$\mathbf{T}_{40}$ *Známe-li kanonický rozklad konečného počtu přirozených čísel v prvočinitele, pak jejich největšího společného dělitele najdeme jako součin mocnin všech prvočísel, která se vyskytují v rozkladech všech daných čísel, přičemž za mocnitele zvolíme nejmenší ze všech exponentů příslušného prvočísla ve všech rozkladech.*

$\mathbf{T}_{41}$ *Známe-li kanonický rozklad konečného počtu přirozených čísel v prvočinitele, pak jejich nejmenší společný násobek najdeme jako součin mocnin všech prvočísel, která se vyskytují v kanonickém rozkladu aspoň jednoho*

z daných čísel, přičemž za mocnitele každého prvočísla zvolíme největší ze všech exponentů mocnin o témže základu v jednotlivých rozkladech.

Tak např. po určení kanonických rozkladů čísel

$840 = 2^3.3.5.7$, $900 = 2^2.3^2.5^2$, $1100 = 2^2.5^2.11$

snadno najdete $(840, 900, 1100) = 2^2.5 = 20$; $[840, 900, 1100] = 2^2.3^2.5^2.7.11 = 138\,600$.

T$_{42}$ *Je-li celé číslo b dělitelem součinu celých čísel a_1, a_2 a je-li b nesoudělné s a_1, pak je b dělitelem a_2.*

Zřejmě platí $a_1 \mid a_1a_2$ a podle předpokladu též $b \mid a_1a_2$. Podle věty **T**$_{32}$ musí být i nejmenší společný násobek čísel a_1, b dělitelem součinu a_1a_2, tj. platí $[a_1, b] \mid a_1a_2$. Avšak podle věty **T**$_{31}$ $[a_1, b] = a_1b$, neboť a_1, b jsou podle předpokladu čísla nesoudělná. Ze vztahu $a_1b \mid a_1a_2$ plyne $a_1a_2 = a_1b_q$ a po zkrácení $a_2 = b_q$, což znamená $b \mid a_2$.

Věta **T**$_{42}$ bývá někdy pro svou důležitost označována jako fundamentální věta aritmetiky. Lze ji zobecnit a vyvodit z ní i jiné důsledky, zejména věty o dělitelnosti součinu přirozených čísel $a_1, a_2, a_3, \ldots a_k$ prvočíslem p.

Důsledek I. *Jestliže prvočíslo p je dělitelem součinu celých čísel $a_1a_2a_3 \ldots a_k$ a přitom není dělitelem žádného z čísel $a_1, a_2, a_3, \ldots, a_{k-1}$, pak je dělitelem čísla a_k.*

Důsledek II. *Je-li prvočíslo p dělitelem součinu celých čísel $a_1a_2a_3 \ldots a_k$, pak je dělitelem aspoň jednoho činitele tohoto součinu.*

Nyní ještě stručně naznačíme, jak je možno dokázat, že rozklad přirozeného čísla n na prvočinitele lze provést jen jediným způsobem, jak jsme to již vyslovili ve větách **T**$_{38}$ a **T**$_{39}$. Předpokládejme, že existují dva rozklady čísla n na prvočinitele, tj.

$$n = p_1p_2p_3 \ldots p_i \ldots p_k = q_1q_2q_3 \ldots q_j \ldots q_m \quad (7,1).$$

Zřejmě platí $p_1 \mid n$, avšak také $p_1 \mid q_1 q_2 \ldots q_m$. Podle důsledku II věty $\mathbf{T}_{42}$ musí být aspoň jeden činitel součinu $q_1 q_2 \ldots q_m$ dělitelný prvočíslem p_1. Nechť je to q_j, takže platí $p_1 \mid q_j$. To však je možné, jen když $p_1 = q_j$. Kdyby tomu tak nebylo, pak by p_1 bylo menší než q_j a číslo q_j by mělo dělitele $p_1 < q_j$ a nemohlo by být tedy prvočíslem, jak jsme předpokládali při rozkladu čísla n v prvočinitele. Krátíme-li rovnost součinů (7,1) číslem $p_1 = q_j$ a pokračujeme-li v důkazu naznačeným způsobem, dokážeme, že další prvočísla $p_2, p_3, \ldots, p_k$ se rovnají vždy jednomu z prvočísel $q_1, q_2, \ldots, q_m$ a že $k = m$.

Příklad 39. Určete všechna celá čísla x, pro která je $y = x^4 + 4$ prvočíslo.

Nejprve provedeme rozklad polynomu $x^4 + 4$ na součin dvou polynomů způsobem, který byl vysvětlen na konci kap. 1. Tak dostaneme

$$y = (x^2 - 2x + 2)(x^2 + 2x + 2) =$$
$$= [(x - 1)^2 + 1][(x + 1)^2 + 1].$$

K tomu, aby y bylo prvočíslo, je nutné, aby jeden z činitelů součinu se rovnal 1, což může nastat jen v případech $x = \pm 1$. V tom případě se však druhý činitel rovná 5, což je prvočíslo. Polynom $x^4 + 4$ nabývá tedy prvočíselné hodnoty jen pro $x = \pm 1$.

Příklad 40. Je-li prvočíslo $p \geq 7$, pak přirozené číslo $n = p^4 - 1$ je násobkem čísla 240. Dokažte.

Dvojčlen $p^4 - 1$ lze rozložit v součin tří činitelů $(p - 1)(p + 1)(p^2 + 1)$. Poněvadž $p \geq 7$ je liché prvočíslo, je každý činitel součinu číslo sudé. Poněvadž $p - 1$, $p + 1$ jsou dvě po sobě jdoucí sudá čísla, je jedno z nich dělitelné 4. Z toho plyne $16 \mid n$. Poněvadž $p \geq 7$ je prvočíslo, ne-

může být násobkem čísla 3, nýbrž musí být číslem tvaru $3k + 1$ nebo $3k - 1$, kde k je číslo celé. V prvém případě platí $p - 1 = 3k$, v druhém $p + 1 = 3k$ a proto v obojím případě $3 \mid n$. Poněvadž $p \geqq 7$ je prvočíslem, nemůže být rovno číslu 5 ani jeho násobku, a musí být číslem tvaru $5k \pm 1$ nebo $5k \pm 2$. Je-li $p = 5k + 1$, pak $p - 1 = 5k$; je-li $p = 5k - 1$, pak $p + 1 = 5k$; je-li $p = 5k \pm 2$, pak $p^2 + 1 = (5k \pm 2)^2 + 1 = 5(5k^2 \pm 2k + 1)$. Odtud plyne $5 \mid n$. Poněvadž číslo n je dělitelné čísly 16, 3, 5, je dělitelné též jejich nejmenším společným násobkem, tj. číslem $2^4.3.5 = 240$.

Příklad 41. Dvě posloupnosti $\{a_n\}, \{b_n\}$ jsou určeny tak, že pro $n \geqq 1$ platí: $a_n = 2^{2n+1} + 2^{n+1} + 1$, $b_n = 2^{2n+1} - 2^{n+1} + 1$. Dokažte, že pro každé přirozené číslo n platí právě jeden ze vztahů $5 \mid a_n$ nebo $5 \mid b_n$.

Součin $a_n b_n = 4^{2n+1} + 1$, jak snadno zjistíme,

$$4^{2n+1} + 1 = (4 + 1)(4^{2n} - 4^{2n-1} + \ldots + 1) \text{ [podle (1,4)]}.$$

Je tedy $5 \mid a_n b_n$ a podle důsledku II věty $\mathbf{T}_{42}$ musí být aspoň jedno z čísel a_n, b_n dělitelné 5. Není však možné, aby zároveň platilo $5 \mid a_n$, $5 \mid b_n$, neboť v tom případě by muselo též platit $5 \mid a_n \mp b_n$, čili $5 \mid 2^{n+2}$, což je zřejmě nemožné. Proto je vždy právě jedno z čísel a_n, b_n dělitelné 5. Sami si snad najdete jiné způsoby řešení této úlohy.

Cvičení

7,1. V tabulce I vyhledejte všechna prvočíselná dvojčata a určete jejich počet. Názvem prvočíselná dvojčata označujeme takové dvojice prvočísel $\{p_n, p_{n+1}\}$, pro něž platí $p_{n+1} - p_n = 2$. (Dosud nevíme, zda prvočíselných dvojčat je nekonečně mnoho.)

7,2. Najděte nejmenší přirozené číslo x, pro které funkční hodnota daného polynomu je číslo složené:
a) $x^2 + x + 5$, b) $x^2 + x + 11$, c) $x^2 + x + 17$,
d) $x^2 + x + 41$, e) $x^2 - 33x + 289$, f) $x^2 - 81x + 1681$.

7,3. Najděte 13 po sobě jdoucích čísel složených. Úlohu řešte dvojím způsobem: a) výpočtem vysvětleným v textu tohoto článku, b) užitím tabulky prvočísel.

7,4. Rozložte v prvočinitele čísla: 8190, 8191, 8192, 23 727, 32 767, 83 736.

7,5. Je dána posloupnost přirozených čísel vzorcem pro n-tý člen $a_n = n!$. Pro která n jsou členy posloupnosti $\{s_n\}$, v níž $s_1 = a_1$, $s_2 = a_1 + a_2$, $s_3 = a_1 + a_2 + a_3$, ..., $s_n = a_1 + a_2 + \ldots + a_n$ druhými mocninami přirozených čísel.

7,6. Určete posledních 249 cifer čísla $1000! + 2$ při jeho zápisu v desítkové soustavě. Udejte nejmenší počet po sobě jdoucích složených čísel, mezi která patří číslo $1000! + 2$.

7,7. Dokažte o polynomech a) $x^4 + 64$, b) $4x^4 + 81$, že nemohou nabýt prvočíselné hodnoty pro žádné celé číslo x.

7,8. Dokažte, že každé přirozené číslo $n > 11$ je součtem dvou čísel složených.

7,9. Najděte všechny aritmetické posloupnosti tří prvočísel s rozdílem a) 2, b) 4.

7,10. Dokažte, že existuje jediná pětičlenná aritmetická posloupnost prvočísel s rozdílem 6.

8. kapitola

STAROVĚKÝ PROBLÉM ČÍNSKÝCH MATEMATIKŮ A PSEUDOPRVOČÍSLA

V této kapitole budeme zkoumat dělitelnost čísel tvaru $2^n - 2$, kde n je číslo přirozené. Přitom se ukáže, že je velmi užitečné, dovedeme-li rychle určit některé dělitele čísel $2^n - 1$ a $2^n + 1$, což nám pomůže často rozložit tato čísla v prvočinitele. K tomu můžeme využít vzorců (1,3), (1,4) pro rozklad dvojčlenů $a^n \pm b^n$. Připomeneme je znovu pro ty případy, kdy $b = 1$ a n je číslo složené.

T_{43} *Pro každé složené číslo $n = rs$, kde $r > 1$ a $s > 1$ jsou čísla přirozená, je $a^n - 1$ dělitelné jednak $a^r - 1$, jednak $a^s - 1$, ať je a jakékoli číslo přirozené; je-li $a > 1$, je také $a^r - 1 > 1$, $a^s - 1 > 1$.*

Zřejmě platí $a^n - 1 = a^{rs} - 1 = (a^r)^s - 1 = (a^s)^r - 1$. Odtud však podle vzorce (1,3) plyne $a^r - 1 \mid a^{rs} - 1$ a rovněž $a^s - 1 \mid a^{rs} - 1$.

T_{44} *Pro každé složené číslo $n = rs$, kde $r > 1$ je číslo liché, a $s > 1$ libovolné číslo přirozené, je $a^n + 1$ dělitelné číslem $a^s + 1$, ať je a jakékoli číslo přirozené.*

Poněvadž $a^n + 1 = a^{rs} + 1 = (a^s)^r + 1$, dostaneme použitím vzorce (1,4) vztah $a^s + 1 \mid a^{rs} + 1$.

Příklad 42. Užitím vět T_{43} a T_{44} najděte některé dělitele čísla $2^{12} - 1$ a rozložte je pak v prvočinitele.

Číslo $2^{12} - 1 = 2^{3 \cdot 4} - 1$ a má tedy podle T_{43} dělitele $2^3 - 1 = 7$ a $2^4 - 1 = 15 = 3 \cdot 5$. Kdybychom však pro-

vedli nejprve rozklad $2^{12} - 1 = (2^6 - 1)(2^6 + 1)$, dostali bychom pro prvního činitele podle věty $\mathbf{T}_{43}$ dělitele $2^2 - 1 = 3$, $2^3 - 1 = 7$, zatímco pro druhého činitele $2^6 + 1$ bychom podle věty $\mathbf{T}_{44}$ dostali dělitele $2^2 + 1 = 5$. Tento rozbor vlastností součinu $(2^6 - 1)(2^6 + 1)$ nám nepřinesl nic nového. Víme-li však, že $2^6 + 1 = 65 = 5.13$, známe tím dalšího dělitele 13 čísla $2^{12} - 1$. Tyto výsledky nám však velmi usnadní, abychom našli rozklad v prvočinitele $2^{12} - 1 = 3^2.5.7.13$.

Použití vzorců (1,3) a (1,4) i vět $\mathbf{T}_{43}$ a $\mathbf{T}_{44}$ si ještě procvičíte na příkladech, které si sami zvolíte. Při hledání rozkladu v prvočinitele čísel $2^n - 1$ a $2^n + 1$ pro $n \leqq 25$ můžete výsledky svých výpočtů zkontrolovat podle tabulky III na konci této knížky. Tato tabulka je užitečná i při řešení jiných úloh. Víme-li např., že $73 \mid 2^9 - 1$, pak jistě platí též $73 \mid 2^{9k} - 1$ (podle $\mathbf{T}_{43}$), ať je k jakékoli přirozené číslo. Víme-li, že $43 \mid 2^7 + 1$, pak $43 \mid 2^{7r} + 1$ (podle věty $\mathbf{T}_{44}$), kde r je libovolné liché přirozené číslo, např. $43 \mid 2^{21} + 1$ apod.

Příklad 43. Dokažte, že platí $41 \mid 2^{41} - 2$.

a) Má-li být $41 \mid 2^{41} - 2$, tj. $41 \mid 2(2^{40} - 1)$, pak vzhledem k nesoudělnosti čísel 41, 2 musí platit $41 \mid 2^{40} - 1$ (podle věty $\mathbf{T}_{42}$). Z tabulky III snadno zjistíme, že $41 \mid 2^{10} + 1$ a tedy také $41 \mid (2^{10} + 1)(2^{10} - 1)$ čili $41 \mid 2^{20} - 1$. Avšak odtud již plyne $41 \mid 2^{2.20} - 1$ čili $41 \mid 2^{40} - 1$.

b) Jiné řešení je možné užitím věty $\mathbf{T}_{17}$ v kap. 3 (obdobně jako v příkladě 14). Počítejme nejprve zbytek při dělení 2^{41} číslem 41. $2^{41} = (2^5)^8.2 = 32^8.2 = (41.1 - 9)^8.2$, což je číslo, které při dělení 41 dá stejný zbytek jako číslo $(-9)^8.2 = 9^8.2 = 81^4.2 = (41.2 - 1)^4.2$. Toto číslo při dělení číslem 41 dává stejný zbytek jako číslo $(-1)^4.2 = 2$. Poněvadž 2^{41} při dělení 41 dává zbytek 2, dostaneme při dělení $2^{41} - 2$ číslem 41 zbytek 0.

Abychom v další části této kapitoly dosáhli stručnosti v zápisech některých vztahů, zvolíme označení $c_n = 2^n - 2$. Budeme-li vyšetřovat dělitelnost čísla c_n číslem n pro $n = 1, 2, 3, 4, 5, \ldots$, dostaneme tyto výsledky:
$1 \mid c_1$, $2 \mid c_2$, $3 \mid c_3$, $4 \nmid c_4$, $5 \mid c_5$, $6 \nmid c_6$, $7 \mid c_7$, $8 \nmid c_8$, $9 \nmid c_9$, $10 \nmid c_{10}$, $11 \mid c_{11}$, $12 \nmid c_{12}$, $13 \mid c_{13}$, $14 \nmid c_{14}$, $15 \nmid c_{15}$, $16 \nmid c_{16}$, $17 \mid c_{17}$, $18 \nmid c_{18}$, $19 \mid c_{19}$, $20 \nmid c_{20}$, ..., přičemž platnost všech vypsaných vztahů snadno potvrdíme užitím tabulky III. Nalezené vztahy nás opravňují k tomu, abychom vyslovili tuto domněnku:

Když $n \mid c_n$, pak n je prvočíslo.

Tato věta zřejmě platí pro všechna přirozená čísla $n \leq 20$, jak jsme se o tom přesvědčili výpočtem. Přitom ovšem číslo 1 počítáme v tomto případě též mezi prvočísla, jak to bylo zvykem ve starších dobách vývoje matematiky. Uvedenou domněnku lze symbolicky zapsat ve formě výroku, že pro každé přirozené číslo n platí

$$n \mid c_n \Rightarrow n \text{ je prvočíslo.} \qquad (8,1)$$

K tomu, abychom mohli rozhodnout, zda uvedená domněnka je nebo není pravdivá, lze zvolit jen dvě různé cesty:

1. užitím známých pravdivých matematických vět a pravidel logického usuzování dokázat, že výrok (8,1) platí pro každé přirozené číslo n;

2. dokázat, že výrok (8,1) neplatí pro každé přirozené číslo n, tj. že existuje aspoň jedno takové přirozené číslo n, že platí vztah $n \mid c_n$ a že zároveň n není prvočíslo.

Bylo by chybou domnívat se, že o pravdivosti výše uvedené domněnky svědčí velký počet přirozených čísel n, pro která výrok (8,1) platí. Této chyby se dopustili již před 2500 lety činští matematikové, když z platnosti výroku (8,1) pro mnohá přirozená čísla n usuzovali na jeho pravdivost pro všechna přirozená čísla n. Jistě asi prověřovali

pravdivost věty (8,1) pro mnohá čísla $n < 341$, neboť pro taková čísla n vztah (8,1) platí.

Teprve v 19. století bylo zjištěno, že $341 \mid 2^{341} - 2$, ale přitom $341 = 11.31$ není prvočíslo. K tomu, abychom dokázali, že číslo 341 je dělitelem čísla $2^{341} - 2 = 2(2^{340} - 1)$, je třeba dokázat, že $341 \mid 2^{340} - 1$, neboť čísla 2 a 341 jsou nesoudělná. Avšak platnost vztahu $341 \mid 2^{340} - 1$ dokážeme podle věty $\mathbf{T}_{32}$ a podle důsledku I věty $\mathbf{T}_{31}$ ze vztahů, které snadno odvodíme: $11 \mid 2^{340} - 1$ a $31 \mid 2^{340} - 1$. Poněvadž však $31 \mid 2^5 - 1$, plyne odtud ihned $31 \mid 2^{5.68} - 1$, čili $31 \mid 2^{340} - 1$. Poněvadž $11 \mid 2^{10} - 1$, platí též $11 \mid 2^{10.34} - 1$ čili $11 \mid 2^{340} - 1$. Kdybychom ovšem byli nahlédli do tabulky III, mohli jsme zjistit, že $11.31 \mid 2^{10} - 1$, odkud ihned plyne $11.31 \mid 2^{340} - 1$.

$\mathbf{D}_{20}$ *Složená čísla n, pro která platí vztah $n \mid 2^n - 2$, se nazývají pseudoprvočísla.*

Ve smyslu právě uvedené definice patří číslo 341 mezi pseudoprvočísla. Dodejme hned, že známe již dlouho i jiná lichá pseudoprvočísla, a víme dokonce, že jich je nekonečně mnoho. Ale teprve r. 1950 našel americký matematik D. H. Lehmer první sudé pseudoprvočíslo 161 038. Jeho nalezení bylo velmi obtížné, avšak důkaz, že $161\,038 \mid 2^{161038} - 2$, je možno poměrně snadno provést způsobem, který jsme již poznali. Platí $161\,038 = 2.73.1103$, číslo $161\,037 = 3^2.29.617$. Naším úkolem je nyní dokázat vztah $2.73.1103 \mid 2(2^{3^1.29.617} - 1)$. Zřejmě platí $2 \mid 2(2^{161037} - 1)$. Z tabulky III zjistíme, že $73 \mid 2^9 - 1$, odkud plyne $73 \mid 2^{9.29.617} - 1$) čili $73 \mid 2(2^{3^1.29.617} - 1)$. Z rozsáhlejší tabulky rozkladů čísel $2^n - 1$ v prvočinitele se snadno zjistí $2^{29} - 1 = 233.1103.2089$. Odtud plyne $1103 \mid 2^{29} - 1$, a protože $1103 \mid 2^{29.3^1.617} - 1$, tedy také $1103 \mid 2(2^{29.3^1.617} - 1)$. Užitím věty $\mathbf{T}_{31}$ a $\mathbf{T}_{32}$ dostaneme hledaný vztah $2.73.1103 \mid 2(2^{161037} - 1)$. Jakmile bylo

nalezeno první sudé pseudoprvočíslo, nebylo již obtížné najít další a dokázat, že takových čísel je nekonečně mnoho.

Domněnka starověkých čínských matematiků, v jejíž pravdivost věřil i slavný německý filosof a matematik Gottfried Wilhelm Leibniz (1646—1716), který se v matematice proslavil nejvíce jako spoluzakladatel diferenciálního a integrálního počtu, se tedy ukázala jako nepravdivá. Pro nás musí být tento případ varovným příkladem, abychom v matematice nevyvozovali obecné závěry o vlastnostech všech prvků nějaké nekonečné množiny z toho, že takovou vlastnost najdeme ve velkém počtu speciálních případů. Tak zv. neúplná indukce je pro matematika velmi cennou pomůckou pro vytváření domněnek; jejich správnost je ovšem nutno dokázat podle platných pravidel logického usuzování.

D_{21} *Složená čísla n, pro která platí* $n \mid a^n - a$ *pro libovolné přirozené číslo a, nazýváme absolutní pseudoprvočísla.* Nejmenší absolutní pseudoprvočíslo je $561 = 3 \cdot 11 \cdot 17$, což znamená, že platí nejen $561 \mid 2^{561} - 2$, ale i $561 \mid 3^{561} - 3$ atd.

Cvičení

8,1. Rozložte na prvočinitele čísla tvaru $2^n - 1$ a $2^n + 1$ pro $n = 22, 24, 26, 28, 30$.

8,2. Rozložte na prvočinitele čísla tvaru $2^n - 2$ pro $n = 31, 33, 35, 37, 39$.

8,3. Dokažte, že čísla 561, 645, 1105 jsou pseudoprvočísla (využívejte tab. III).

8,4. Dokažte, že platí $561 \mid 3^{561} - 3$; $1105 \mid 3^{1105} - 3$; $561 \mid 33^{561} - 33$.

9. kapitola

MALÁ VĚTA FERMATOVA

$\mathbf{T}_{45}$ *Je-li n prvočíslo, pak číslo* $2^n - 2$ *je dělitelné číslem n.*

S použitím známých symbolů mohli bychom tuto větu přehledně vyjádřit výrokem, že pro každé přirozené číslo n platí

$$n \text{ je prvočíslo} \Rightarrow n \mid 2^n - 2. \tag{9,1}$$

Důkaz věty $\mathbf{T}_{45}$ provedeme snadno užitím binomické věty pro rozvoj $(a + b)^n$, podle níž

$$(1 + 1)^n = 1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \ldots +$$

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

Odtud po převedení prvního a posledního sčítance z pravé strany rovnosti na levou dostaneme

$$2^n - 2 = \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \ldots +$$

$$+ \binom{n}{k} + \ldots + \binom{n}{n-1}. \tag{9,2}$$

Každý člen součtu na pravé straně této rovnosti je tzv. binomický koeficient

$$b_k = \binom{n}{k} = \frac{n\,(n-1)\,(n-2)\,\ldots\,(n-k+1)}{1.2.3.\,\ldots\,k} \qquad (9,3)$$

a to pro $k = 1, 2, 3, \ldots, n-1$. Z rovnosti (9,2) však snadno dostaneme rovnost

$$1.2.3\,\ldots\,(k-1)\,k.b_k = n\,(n-1)\,(n-2)\,\ldots\,(n-k+1). \qquad (9,4)$$

Součin na pravé straně rovnosti (9,4) je zřejmě dělitelný číslem n, o němž předpokládáme, že je prvočíslem. Z toho však plyne, že také součin na levé straně rovnosti (9,4) je dělitelný prvočíslem n. Poněvadž však žádný z prvních k činitelů není dělitelný prvočíslem n (vzhledem k tomu, že $k \leqq n-1$), musí jím být dělitelný poslední činitel b_k (podle důsledku II věty $\mathbf{T}_{42}$). Poněvadž na pravé straně v rovnosti (9,2) je každý sčítanec dělitelný prvočíslem n, je jím dělitelný i jejich součet (podle věty $\mathbf{T}_{8}$, resp. jejího zobecnění) a tedy také i číslo na levé straně, tj. $2^n - 2$, čímž je věta $\mathbf{T}_{45}$ dokázána.

S odvoláním na tuto větu můžeme tedy tvrdit, že např. 23 je dělitelem čísla $2^{23} - 2 = 2\,(2^{22} - 1)$ a poněvadž čísla 23 a 2 jsou nesoudělná, můžeme (podle věty $\mathbf{T}_{42}$) též tvrdit, že platí vztah $23 \mid 2^{22} - 1$. Obdobně $29 \mid 2^{29} - 2$, $31 \mid 2^{31} - 2$, $89 \mid 2^{89} - 2$ apod. nebo $29 \mid 2^{28} - 1$, $31 \mid 3^{30} - 1$, $89 \mid 2^{88} - 1$ apod.

Z věty $\mathbf{T}_{45}$ plyne, že vlastnost „n je prvočíslo“ je postačující podmínkou pro platnost vztahu „n dělitelem $2^n - 2$“. Jestliže jste studovali předcházející kapitolu, víte, že tato vlastnost není nutnou podmínkou pro platnost vztahu $n \mid 2^n - 2$, neboť jsme zjistili, že i pro některá složená čísla n (tzv. pseudoprvočísla) platí též $n \mid 2n - 2$. Jinak řečeno: Věta (9,1) platí, avšak věta k ní obrácená (8,1) neplatí.

Nyní větu $\mathbf{T}_{45}$ zobecníme. Její zobecnění vyjádříme dvojím způsobem, přičemž místo označení „prvočíslo n“

budeme užívat označení „prvočíslo p“, což trochu přispěje k zapamatování postačující podmínky v následujících větách.

T_{46} *Pro libovolné celé číslo a a pro každé prvočíslo p je p dělitelem čísla $a^p - a$.*

T_{47} *Pro každé celé číslo a nesoudělné s prvočíslem p je p dělitelem čísla $a^{p-1} - 1$.*

Dokážeme nejprve dva výroky I, II, jejichž pravdivost bude předpokladem pro logický závěr o platnosti věty T_{46}.

I. *Každé prvočíslo p je dělitelem čísla $1^p - 1$.*

Tento výrok je zvláštním případem věty T_{46} pro $a = 1$. Jeho důkaz je snadný, neboť $1^p - 1 = 0$ a pro každé prvočíslo p platí $p \mid 0$.

II. *Je-li prvočíslo p dělitelem čísla $a^p - a$, pak p je dělitelem čísla $(a + 1)^p - (a + 1)$, kde a je libovolné číslo přirozené.*

Důkaz pravdivosti tohoto výroku provedeme takto: Platí

$$(a+1)^p - (a+1) = \left[a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \right.$$

$$\left. + \ldots + \binom{p}{p-1} a + 1\right] - (a+1) = \left[\binom{p}{1} a^{p-1} + \right.$$

$$\left. + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a\right] + [a^p - a].$$

Již v první části této kapitoly jsme ukázali, že binomické koeficienty $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ jsou celá čísla dělitelná prvočíslem p. Proto je dělitelný prvočíslem p součet čísel

v první lomené závorce, neboť je jím dělitelný každý jeho sčítanec jako násobek čísla p. Je-li tedy prvočíslem p dělitelný výraz v druhé lomené závorce, musí být prvočíslem p dělitelný i součet výrazů v první a druhé lomené závorce, tj. tedy číslo $(a + 1)^p - (a + 1)$.

Jestliže v obecném výroku právě dokázaném položíme $a = 1$, dostaneme tento pravdivý výrok: Je-li prvočíslem p dělitelné číslo $1^p - 1$, pak je prvočíslem p dělitelné číslo $2^p - 2$. Spojením tohoto výroku s výrokem I dostaneme předpoklady, z nichž podle běžných pravidel logického usuzování vyplývá závěr: Každé prvočíslo p je dělitelem čísla $2^p - 2$. Tohoto výroku, který je ve shodě s větou $\mathbf{T}_{45}$, mohli bychom užít dále k důkazu věty $\mathbf{T}_{46}$ pro $a = 3$ a pak pro konečný počet dalších přirozených čísel. Budeme však postupovat jinak, abychom větu $\mathbf{T}_{46}$ dokázali pro všechna přirozená čísla a.

V matematice užíváme často následujícího pravidla pro závěr ze dvou předpokladů (premis), jejichž příklady jsme ukázali výroky I a II. Toto pravidlo, nazývané matematická indukce, můžeme formulovat takto: Jestliže nějaký výrok závislý na přirozeném čísle a platí pro přirozené číslo $a = 1$, a jestliže z platnosti tohoto výroku pro přirozené číslo a plyne platnost výroku pro číslo $a + 1$, pak odtud plyne závěr, že výrok je platný pro každé přirozené číslo a. Užitím této matematické indukce plyne tedy z premis I, II logicky správný závěr o platnosti věty $\mathbf{T}_{46}$ pro každé přirozené číslo a. (Přitom se nám nyní věta $\mathbf{T}_{45}$ jeví jako speciální (zvláštní) případ věty $\mathbf{T}_{46}$ pro $a = 2$.)

Nyní zbývá ještě dokázat, že věta $\mathbf{T}_{46}$ platí též pro číslo 0 a pro čísla opačná k číslům přirozeným. Pro $a = 0$ věta zřejmě platí, neboť $0^p - 0 = 0$ a přitom $p \mid 0$. Je-li $a < 0$ libovolné celé záporné číslo, pak $-a > 0$ je zřejmě číslo přirozené, pro něž věta $\mathbf{T}_{46}$ platí, tj. platí, že prvočíslo p je dělitelem čísla

$$(-a)^p - (-a). \qquad (9,5)$$

Je-li $p > 2$ liché prvočíslo, pak platí
$(-a)^p - (-a) = -a^p + a = -(a^p - a)$ a platí
$p \mid -a(a^p - a)$ čili též $p \mid a^p - a$, čímž je věta $\mathbf{T}_{46}$ dokázána i pro celá čísla $a < 0$ pro lichá p. Zbývá ještě případ $p = 2$. V tom případě však platí, že $p = 2$ je dělitelem čísla $(-a)^2 - (-a) = a^2 + a = a(a + 1)$, neboť ze dvou po sobě jdoucích čísel celých $a, a + 1$ je právě jedno dělitelné číslem 2. Tím je ukončen celý důkaz platnosti věty $\mathbf{T}_{46}$ pro každé celé číslo a.

Poněvadž p je dělitelem $a^p - a = a(a^{p-1} - 1)$, nemůže platit $p \mid a$ při nesoudělnosti čísel a, p a proto musí platit podle věty $\mathbf{T}_{42}$, že $p \mid a^{p-1} - 1$. Tím je dokázána věta $\mathbf{T}_{47}$.

Znalost vět $\mathbf{T}_{46}$ a $\mathbf{T}_{47}$ je velmi užitečná při vyšetřování dělitelnosti některých čísel i pro řešení jiných problémů, s nimiž se setkáme při dalším studiu matematiky. Tak např. můžeme hned psát, že $50^{97} - 50$ je dělitelné 97 (podle věty $\mathbf{T}_{47}$) apod. Užití těchto vět ukážeme ještě na několika příkladech.

Příklad 44. Dokažte, že pro každé celé číslo x je hodnota funkce $x^5 + 4x - 10$ číslo dělitelné pěti.

Tuto úlohu bychom mohli řešit metodou vyloženou v kap. 3 (viz př. 10), tj. předpokládat, že číslo x je tvaru $5k$ nebo tvaru $5k \pm 1$, nebo tvaru $5k \pm 2$, přičemž bychom zjistili, že ve všech pěti případech dostaneme číslo dělitelné pěti. Rychleji však rozřešíme úlohu, když nejprve daný mnohočlen upravíme na tvar

$$x^5 + 4x - 10 = (x^5 - x) + 5(x - 2).$$

První sčítanec $x^5 - x$ je podle věty $\mathbf{T}_{46}$ dělitelný číslem 5 pro každé celé číslo x a druhý sčítanec je rovněž dělitelný číslem 5, když součin $5(x - 2)$ obsahuje činitele 5. Proto

je jejich součet a tedy také funkční hodnota daného polynomu pro každé celé číslo x násobkem čísla 5.

Příklad 45. Dokažte, že pro každé celé číslo a je 561 dělitelem čísla $a^{561} - a$.

Rozkladem čísla 561 na prvočinitele dostaneme $561 = 3.11.17$. Dokažme nejprve, že čísla 3, 11, 17 jsou děliteli čísla $a^{561} - a = a(a^{560} - 1)$.

a) Je-li a násobkem čísla 3, pak zřejmě platí $3 \mid a(a^{560}-1)$. Když číslo a je nesoudělné s číslem 3, pak podle věty $\mathbf{T}_{47}$ platí: $3 \mid a^2 - 1$ a také $3 \mid a^{2.280} - 1$, a tedy i $3 \mid a(a^{560}-1)$.

b) Je-li a dělitelné číslem 11, pak zřejmě platí $11 \mid a(a^{560}-1)$. Není-li a dělitelné číslem 11, pak podle věty $\mathbf{T}_{47}$ platí $11 \mid a^{10} - 1$, a proto i $11 \mid a^{10.56} - 1$ čili též $11 \mid a(a^{560}-1)$.

c) Je-li a dělitelné číslem 17, pak platí $17 \mid a(a^{560} - 1)$. Není-li a dělitelné číslem 17, pak $17 \mid a^{16-1}$, a proto i $17 \mid a^{16.35} - 1$, a tedy i $17 \mid a(a^{560} - 1)$. Odtud plyne podle věty $\mathbf{T}_{32}$ pravdivost tvrzení $3.11.17 \mid a(a^{560} - 1)$. Tím je též dokázáno, že číslo $561 = 3.11.17$ je absolutní pseudoprvočíslo (viz $\mathbf{D}_{20}$ v kap. 8).

Příklad 46. Dokažte, že číslo $z = 97^{100} - 47^{100}$ je násobkem čísla 5050.

Vztah $50 \mid 97^{100} - 47^{100}$ plyne ihned ze vzorce (1,3) pro rozklad $a^n - b^n$. Upravujeme nyní: $z = 97^{100} - 47^{100} = (97^{100} - 1) - (47^{100} - 1)$. Poněvadž číslo 101 je prvočíslo, je dělitelem čísel $97^{100} - 1$, $47^{100} - 1$, a tedy i jejich rozdílu. Ze vztahů $50 \mid z$ a $101 \mid z$ plyne ihned podle $\mathbf{T}_{32}$ $50.101 \mid z$ čili $5050 \mid z$.

Příklad 47. Jsou-li a, b celá čísla nesoudělná s číslem 5, pak číslo $a^4 - b^4$ je dělitelné pěti.

Jsou-li a, b celá čísla nesoudělná s číslem 5, pak podle věty $\mathbf{T}_{47}$ jsou prvočíslem 5 dělitelná čísla $a^4 - 1$, $b^4 - 1$.

Odtud však snadno plyne, že číslem 5 je dělitelné i číslo $(a^4 - 1) - (b^4 - 1) = a^4 - b^4$.

Z věty $\mathbf{T}_{46}$ jsme odvodili snadno větu $\mathbf{T}_{47}$. Bylo by ovšem možno dokázat nejprve jiným způsobem na důkazu věty $\mathbf{T}_{46}$ nezávislým platnost věty $\mathbf{T}_{47}$ a z její platnosti odvodit větu $\mathbf{T}_{46}$. Tím by se ukázalo, že obě věty, pro něž se často užívá označení *malá věta Fermatova*, jsou rovnocenné (ekvivalentní).

Pierre Fermat (1601—1665), francouzský právník a poradce parlamentu v Toulouse, zabýval se ve volných chvílích matematikou, v níž dosáhl výsledků cenných pro rozvoj číselné teorie, analytické geometrie a matematické analýzy. Přívlastku „malá" k označení malé věty Fermatovy se užívá proto, aby se odlišila od tzv. *velké věty Fermatovy*, podle níž pro přirozená čísla $n > 2$ nelze najít taková přirozená čísla x, y, z, aby platilo $x^n + y^n = z^n$. Toto tvrzení uvedl Fermat bez důkazu v poznámce na okraji spisu, který četl. Od doby Fermatovy se mnoho matematiků marně pokoušelo o důkaz Fermatova tvrzení pro všechna přirozená čísla n. Zatím je pravdivost Fermatova tvrzení dokázána pro mnohá přirozená čísla n, jako např. pro všechna přirozená čísla n, pro která platí $2 < n \leqq 4002$.

Vlastnost celých čísel, která je vyjádřena v malé větě Fermatově, uvedl Fermat bez důkazu již roku 1640 v dopise svému příteli. První důkaz malé věty Fermatovy podal roku 1736 slavný člen petrohradské akademie věd Leonhard Euler (1707—1783) a později Fermatovu větu ještě zobecnil. Euler patří k největším a nejplodnějším matematikům všech dob. Svými pracemi zasáhl podnětně do všech oborů matematiky a dosažené výsledky aplikoval s velkým úspěchem na řešení různých problémů v jiných vědách matematicko-fyzikálních i v technické praxi.

Cvičení

9,1. S částečným využitím malé věty Fermatovy i vět dříve poznaných dokažte, že pro každé celé číslo x je číslo $y = x^7 - x$ násobkem čísla 210.
9,2. Využitím výsledku předcházející úlohy dokažte, že pro každé celé číslo x je číslo $x^7 + 105x^2 + 104x$ násobkem čísla 210.
9,3. S použitím malé věty Fermatovy dokažte pro každé celé číslo a platnost těchto vztahů:
a) $1105 \mid a^{1105} - a$; b) $1387 \mid a^{1387} - a$; c) $1729 \mid a^{1729} - a$; d) $1905 \mid a^{1905} - a$.

10. kapitola

NĚKTERÉ STARÉ A NOVÉ PROBLÉMY ČÍSELNÉ TEORIE

Již v úvodu kapitoly 7 jsme užili symbolu $\Theta(n)$ k označení funkce, která každému přirozenému číslu n přiřazuje přirozené číslo udávající počet všech přirozených dělitelů čísla n, tj. počet všech dělitelů čísla n v oboru čísel přirozených. Symbolu $\Theta(n)$ v uvedeném významu budeme užívat i v této kapitole. Mimo něj budeme dále užívat i symbolu $\sigma(n)$ k označení funkce, která každému přirozenému číslu n přiřazuje číslo udávající součet všech přirozených dělitelů čísla n. Přitom značka σ je malé řecké písmeno odpovídající našemu písmenu s; čteme ji sigma.

Poněvadž pro každého přirozeného dělitele d přirozeného čísla n platí $d \leqq n$, můžeme konečným počtem dělení zjistit všechna čísla d, pro něž platí $d \mid n$, a určit jejich počet i součet. Tak např. pro číslo $n = 144$ platí $\sigma(144) = 1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 16 + 18 + 24 + 36 + 48 + 72 + 144 = 403, \Theta(144) = 15$. Tento způsob určování funkčních hodnot $\sigma(n)$ a $\Theta(n)$ je ovšem někdy velmi pracný, a proto si ukážeme jinou metodu k určování $\sigma(n)$ a $\Theta(n)$, a to nejprve na dvou jednoduchých číselných příkladech.

Pro číslo $16 = 2^4$ je každý přirozený dělitel číslo tvaru 2^x, kde x je takové celé nezáporné číslo, že platí $0 \leqq x \leqq 4$. Přirozenými děliteli čísla 16 jsou tedy $2^0 = 1$, $2^1 = 2$, $2^2 = 4, 2^3 = 8, 2^4 = 16$. Je tedy $\Theta(16) = \Theta(2^4) = 1 + 4 = 5$, $\sigma(16) = \sigma(2^4) = 1 + 2^1 + 2^2 + 2^3 + 2^4 = (2^5 - 1) : (2 - 1) = 31$; (součet všech přirozených

dělitelů jsme přitom určili podle známého vzorce pro součet prvních n členů geometrické řady).

Máme-li určit všechny přirozené dělitele čísla $n = 144 = 2^4.3^2$, je třeba vyhledat všechna přirozená čísla tvaru $2^x.3^y$, kde $0 \leqq x \leqq 4$, $0 \leqq y \leqq 2$. Zvolíme-li $y = 0$, dostaneme 5 dělitelů $2^0.3^0$, $2^1.3^0$, $2^2.3^0$, $2^3.3^0$, $2^4.3^0$, pro $y = 1$ dostaneme dalších 5 dělitelů $2^0.3^1$, $2^1.3^1$, $2^2.3^1$, $2^3.3^1$, $2^4.3^1$ a konečně pro $y = 2$ dostaneme opět 5 dělitelů: $2^0.3^2$, $2^1.3^2$, $2^2.3^2$, $2^3.3^2$, $2^4.3^2$. Snadno usoudíme, že všech 15 uvedených dělitelů je možno najít jako sčítance všech součinů, které dostaneme, když podle známých pravidel o násobení mnohočlenu mnohočlenem znásobíme součet $2^0 + 2^1 + 2^2 + 2^3 + 2^4$ součtem $3^0 + 3^1 + 3^2$. Platí

$$\sigma(2^4.3^2) = (2^0 + 2^1 + 2^2 + 2^3 + 2^4)(3^0 + 3^1 + 3^2). \quad (10,1)$$

Užitím vzorce pro součet prvních n členů geometrické řady dostaneme

$$\sigma(2^4.3^2) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1}. \quad (10,2)$$

Nyní již snadno vypočteme $\sigma(2^4.3^2) = 31.13 = 403$. Poněvadž v součinu (10,1) má první činitel $1 + 4 = 5$ sčítanců a druhý $1 + 2 = 3$ sčítance, plyne odtud pro celkový počet přirozených dělitelů

$$\Theta(2^4.3^2) = (1 + 4)(1 + 2) = 15.$$

Nyní si již sami procvičíte naznačený způsob vyhledání všech přirozených dělitelů daného čísla n i určení součtu a počtu všech jeho přirozených dělitelů i v takových případech, kdy kanonický rozklad daného čísla n v prvočinitele je součinem tří nebo i více mocnin různých prvočísel, jejichž mocnitelé jsou čísla přirozená. Zobecněním úvah lze dojít k výsledkům, které stručně naznačíme.

Známe-li kanonický rozklad přirozeného čísla n ve tvaru

$$n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}, \tag{10,3}$$

kde $p_1, p_2, p_3, \dots, p_s$ jsou různá prvočísla a $r_1, r_2, r_3, \dots, r_s$ čísla přirozená, pak je možno zjistit tyto vlastnosti čísla n:

I. Každý přirozený dělitel čísla n má tvar $p_1^{x_1} p_2^{x_2} p_3^{x_3} \dots p_s^{x_s}$, kde mocnitelé jsou taková celá nezáporná čísla, že $x_1 \leqq r_1, x_2 \leqq r_2, x_3 \leqq r_3, \dots, x_s \leqq r_s$. Všechny tyto přirozené dělitele můžeme najít jako sčítance součtu, který dostaneme po provedeném vynásobení mnohočlenů ve výrazu

$$\begin{aligned}\sigma(n) = &\left(p_1^0 + p_1^1 + p_1^2 + \dots + p_1^{r_1}\right) \cdot \\ &\cdot \left(p_2^0 + p_1^1 + p_2^2 + \dots + p_2^{r_2}\right) \dots \\ &\dots \left(p_s^0 + p_s^1 + p_s^2 + \dots + p_s^{r_s}\right).\end{aligned} \tag{10,4}$$

II. Pro součet všech přirozených dělitelů čísla n platí

$$\begin{aligned}\sigma(n) = &\frac{p_1^{r_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{r_2+1} - 1}{p_2 - 1} \dots \\ &\dots \frac{p_s^{r_s+1} - 1}{p_s - 1}\end{aligned} \tag{10,5}$$

Součin ve tvaru (10,5) se ovšem rovná součinu (10,4) z něhož plyne po úpravě s použitím vzorce pro součet prvních n členů geometrické řady. Výpočet $\sigma(n)$ podle vzorce (10,5)

je ovšem výhodný při větších exponentech $r_1, r_2, r_3, \ldots, r_s$; při menších hodnotách $r_1, r_2, \ldots, r_s$ stačí vzorec (10,4).

III. Pro počet přirozených dělitelů čísla n platí vzorec

$$\Theta(n) = (r_1 + 1)(r_2 + 1) \ldots (r_s + 1). \qquad (10,6)$$

Příklad 48. Určete součet i počet přirozených dělitelů čísel $a = 361$, $b = 338\,800$, $c = 28$.

Poněvadž $a = 361 = 19^2$, platí $\sigma(a) = 1 + 19 + 19^2 = 381$, $\Theta(a) = 3$. Poněvadž $b = 338\,800 = 2^4.5^2.7.11^2$, platí

$$\sigma(b) = \frac{2^5 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} \cdot \frac{11^3 - 1}{11 - 1} =$$

$$= 31.31.8.133 = 1022\,504, \; \Theta(b) =$$

$$= (4 + 1)(2 + 1)(1 + 1)(2 + 1) = 90.$$

Poněvadž

$c = 28 = 2^2.7$, platí $\sigma(c) = (1 + 2 + 2^2)(1 + 7) = 56$,

$$\Theta(c) = (2 + 1)(1 + 1) = 6.$$

Čísla a, b, c v příkladu 48 byla zvolena tak, aby se ukázalo, že existují přirozená čísla n, pro která platí:
a) $\sigma(n) < 2n$, b) $\sigma(n) > 2n$, c) $\sigma(n) = 2n$. Je snadné dokázat věty $\mathbf{T}_{48}$ a $\mathbf{T}_{49}$.

$\mathbf{T}_{48}$ *Existuje nekonečně mnoho přirozených čísel n, pro něž platí $\sigma(n) < 2n$.*

$\mathbf{T}_{49}$ *Existuje nekonečně mnoho přirozených čísel n, pro něž platí $\sigma(n) > 2n$.*

Taková přirozená čísla n, pro něž platí $\sigma(n) = 2n$, jsou

vzácná a byla již ve starověku nazývána *čísla dokonalá*. K číslům tohoto druhu patří např. číslo 6, pro které platí $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2.6$, a číslo 28, pro které platí $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2.28$. Dosud nevíme, zda počet takových čísel je konečný nebo zda jich je nekonečně mnoho.

Již v Euklidově díle Základy najdeme pozoruhodnou úvahu o číslech dokonalých, v níž je též uvedena postačující podmínka k tomu, aby sudé číslo bylo číslem dokonalým. O dva tisíce let později ukázal L. Euler, že Euklidem vyslovená postačující podmínka je zároveň podmínkou nutnou. Lze tedy dokázat, že platí následující věta.

$\mathbf{T}_{50}$ *K tomu, aby sudé číslo bylo číslem dokonalým, je nutné a stačí, aby bylo číslem tvaru* $2^{n-1}(2^n - 1)$ *a aby zároveň číslo* $2^n - 1$ *bylo prvočíslem.* Jinak řečeno: *Sudé číslo je číslem dokonalým právě tehdy, když je číslem tvaru* $2^{n-1}(2^n - 1)$, *v němž činitel* $2^n - 1$ *je prvočíslo.*

Z této věty plyne, že známe právě tolik sudých dokonalých čísel, kolik známe prvočísel tvaru $2^n - 1$. Do konce roku 1963 bylo nalezeno 23 prvočísel tvaru $2^n - 1$, a to pro $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 617, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11\,213$.

K tomu, aby číslo $2^n - 1$ bylo prvočíslo, je nutné, aby číslo n bylo prvočíslem. Není to však podmínka postačující, jak je zřejmé z příkladu $2^{11} - 1 = 2047 = 23.89$.

Studiem vlastností čísel tvaru $2^n - 1$ se v 17. století hodně zabýval francouzský matematik a fyzik Marin Mersenne (1588 – 1648). Proto se dnes názvem čísla Mersennova označují všechna přirozená čísla $M_n = 2^n - 1$, kde n je libovolné číslo přirozené; u některých autorů se tímto názvem rozumějí ta přirozená čísla $M_p = 2^p - 1$, kde p je libovolné prvočíslo. Jednotně je ovšem chápán význam názvu Mersennova prvočísla, jímž se označují všechna pří-

rozená čísla tvaru $2^n - 1$, která jsou prvočísly. O těchto Mersennových prvočíslech uvedeme ještě některé zajímavosti.

Mezi čísly $M_n = 2^n - 1$ byla ve starověku nalezena jen čtyři prvočísla. Za života Eulerova jich bylo známo již osm, z nichž největší $M_{31} = 2^{31} - 1 = 2\,147\,483\,647$ našel sám Euler r. 1772. Toto desíticiferné prvočíslo zůstalo největším známým prvočíslem až do r. 1883, kdy ruský matematik — amatér I. M. Pervušin dokázal, že číslo $M_{61} = 2^{61} - 1 = 2305843009213693951$ je prvočíslo. Brzy potom byla nalezena další Mersennova prvočísla M_{89} a M_{107}. Roku 1914 dokázal francouzský matematik Fauquembergue, že M_{127} je prvočíslo. Toto číslo zůstalo pak největším známým prvočíslem po celou první polovinu 20. století.

Od poloviny 20. století začali matematikové k hledání Mersennových prvočísel užívat rychle pracujících samočinných elektronických počítacích strojů. Dnes je největším známým prvočíslem $M_{11213} = 2^{11213} - 1$, které má při zápisu v desítkové soustavě 3376 cifer. Toto prvočíslo bylo nalezeno pracovníky výpočtářské laboratoře americké university v Illinois; k zjištění, že číslo M_{11213} je prvočíslo, musel elektronický počítací stroj Illiac II pracovat 2 hod. 15 min.

Při zjištění, zda nějaké číslo M_n je nebo není prvočíslo, se užívá zvláštní zkoušky takového druhu, že není třeba hledat rozklad čísla M_n v prvočinitele. Tak je možné, že o čísle M_{101} víme, že je číslem složeným, a dokonce víme i to, že je součinem dvou prvočísel, avšak neznáme žádného jeho prvočíselného dělitele. Určení jeho prvočinitelů je výpočet tak náročný, že nemohl být dosud proveden ani za pomoci moderních elektronických počítacích strojů.

Z uvedených informací o prvočíslech Mersennových je zřejmé, že dnes známe 23 sudých dokonalých čísel, z nichž největší je $2^{11212}(2^{11213} - 1)$, které má 6751 cifer. Snad

by vás též zajímalo, zda existují lichá dokonalá čísla. Na tuto otázku neznáme dosud odpověď, ale i přitom můžeme tvrdit, že je pravdivá tato věta. *Všechna lichá dokonalá čísla jsou větší než* 10^{20} *a každé z nich je součinem nejméně šesti prvočísel.* Tvrzení o pravdivosti této věty musíme ovšem chápat tak, jak jsme si to vysvětlili v kap. 1. Z hlediska praxe novodobé matematiky i logiky zůstane tato věta pravdivá, i kdyby se jednou dokázalo, že množina všech lichých dokonalých čísel je prázdná.

Kdybychom si položili otázku, která přirozená čísla jsou v soustavě dvojkové (dyadické) zapsána n jedničkami, zjistili bychom, že to jsou čísla $M_n = 2^n - 1$ (viz příklad 19 v kap. 4). Můžeme tedy tvrdit, že dnes známe 23 prvočísel, která jsou v soustavě dvojkové zapsána samými jedničkami. V této souvislosti můžeme si dát otázku, která prvočísla jsou zapsána samými jedničkami v soustavě desítkové, tj. která z čísel v posloupnosti 1, 11, 111, 1111, 11 111, ... jsou prvočísla; n-tým členem této posloupnosti je $a_n = \frac{1}{9}(10^n - 1)$. V této posloupnosti najdeme snadno prvočíslo 11. Důkaz o tom, že a_{23} je též prvočíslo, podal asi před 40 lety M. Kraitchik; tento důkaz nebyl snadný a v jednom Kraitchikově díle zaujímá 16 stran. R. 1963 zabýval se otázkou existence prvočísel v posloupnosti s n-tým členem $a_n = \frac{1}{9}(10^n - 1)$ americký matematik John Brillhart a zjistil, že pro $n \leqq 109$ existují mezi čísly a_n jen tři prvočísla, a to pro $n = 2, 19, 23$.

R. 1956 položil maďarský matematik P. Erdös otázku, zda v množině všech přirozených čísel tvaru $2^n - 7$ pro $n > 3$ existuje nějaké prvočíslo. Trvalo to několik let, než se podařilo najít první a zatím také jediné takové prvočíslo. Polský matematik T. Kulikowski dokázal, že číslo

$2^{39} - 7 = 549755813881$ je prvočíslo. Je zjištěno, že je to jediné prvočíslo tvaru $2^n - 7$ pro $3 < n \leqq 50$.

Studium čísel tvaru $2^n - 1$ těsně souvisí se studiem čísel tvaru $2^n + 1$, jejichž rozklady v prvočinitele pro $n \leqq 25$ najdete v tabulce III. Nahlédnutím do ní zjistíte mezi těmito čísly prvočísla jen v těch případech, kdy mocnitel n nabývá těchto hodnot: $1 = 2^0$, $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, $16 = 2^4$. Není to náhoda, neboť pro každé číslo n, které je složené a obsahuje aspoň jednoho lichého prvočinitele, je $2^n + 1$ číslo složené (viz větu $\mathbf{T}_{44}$ v kap. 8). K tomu, aby číslo $2^n + 1$ bylo prvočíslem, je tedy nutné, aby platilo $n = 2^k$, kde k je celé nezáporné číslo. Tato podmínka však není postačující, jak se domníval P. Fermat, který r. 1640 vyslovil přesvědčení, že všechna čísla $F_k = 2^{2^k} + 1$ jsou prvočísla.

Mezi čísly F_k, která se často označují názvem *čísla Fermatova*, byla až dosud nalezena jen tato Fermatova prvočísla: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. O čísle F_5 zjistil však již r. 1732 L. Euler, že je číslem složeným, neboť $F_5 = 641 \cdot 6700417$. O čísle F_6 dokázal r. 1880 francouzský matematik Landry, že je číslem složeným. Od té doby byla pak objevována další Fermatova čísla F_k, která jsou čísly složenými. Již r. 1886 bylo zjištěno, že Fermatovo číslo F_{36} má prvočíselného dělitele $5 \cdot 2^{38} + 1 = 2748779069441$. Důkaz toho nelze ovšem provést dělením čísla F_{36} tímto dělitelem, protože číslo F_{36} je tak velké, že jeho zápis v desítkové soustavě by měl přes 13 miliard cifer a při jeho otištění normálním tiskem měl by řádek těchto cifer asi takovou délku jako zemský rovník.

Vyšetřování Fermatových čísel F_k se podstatně usnadnilo, když při něm bylo možno využít rychle pracujících samočinných elektronických počítacích strojů. Proto známe dnes již 46 Fermatových čísel složených, z nichž největší je F_{1945}. Zápis tohoto čísla v desítkové soustavě by měl více

než 10^{582} cifer, takže nikdy nebude možno je vypsat. Nemohli by to udělat ani všichni obyvatelé celého světa, i kdyby práci na pořízení zápisu věnovali celý svůj život. A přesto je možno dokázat, že číslo F_{1945} má nejmenšího prvočíselného dělitele $5.2^{1947} + 1$, což je prvočíslo 587 ciferné.

Nejmenší Fermatovo číslo F_k, o němž nevíme, zda je prvočíslo nebo číslo složené, je F_{17}. Rozhodnutí v této otázce se v dohledné době asi nedočkáme, poněvadž při použití dosavadních metod k vyšetřování Fermatových čísel jde o řešení problému, které je náročné nejen časově, nýbrž i finančně. Je totiž propočteno, že by moderní elektronický počítač musil pracovat asi 128 týdnů při zjišťování, zda číslo F_{17} je nebo není prvočíslo.

Neznáme tedy zatím více než pět Fermatových prvočísel a dosud nevíme, zda bude možno najít další a zda jich je konečný počet.

Prvočísla mají důležitý význam v různých oborech matematiky. Pokud jde o Fermatova prvočísla, lze říci, že mají vztah nejen k problémům z oboru aritmetiky a algebry, ale i k problémům geometrickým, jako je např. otázka konstruovatelnosti pravidelných mnohoúhelníků pravítkem a kružítkem. Jsou také dokladem pout, která spojují někdy zdánlivě různorodé poznatky matematiky.

Cvičení

10,1. Dokažte, že pro každé přirozené číslo $n = p^r$, kde p je prvočíslo a r číslo přirozené, platí $\sigma(n) < 2n$. Výsledku užijte k důkazu věty $\mathbf{T}_{48}$.

10,2. Dokažte, že pro každé přirozené číslo $n = 6k$, kde k je libovolné číslo přirozené, platí $\sigma(n) \geqq 2n$. Výsledku užijte k důkazu věty $\mathbf{T}_{49}$.

10,3. K tomu, aby číslo $2^n - 7$ bylo prvočíslem, je nutné $n = 4k + 3$, kde k je číslo přirozené. Dokažte toto tvrzení a ukažte, že podmínka $n = 4k + 3$ není postačující.

10,4. Dokažte, že zápis každého Fermatova čísla F_k v desítkové soustavě má na posledním místě číslici 7, když $k > 1$.

10,5. V letech 1962 a 1963 bylo objeveno pět Mersennových prvočísel M_n pro $n = 4253, 4423, 9689, 9941, 11\,213$. Jsou to dnes největší známá prvočísla. Dokažte, že každé z těchto prvočísel má přes 1000 cifer při zápisu v desítkové soustavě, znáte-li $\log 2 \doteq 0{,}3010300$ při zaokrouhlení na 7 desetinných míst. Najděte též první i poslední 3 cifry v zápise M_{11213}.

Prvočísla od 2 do 1987

2	127	283	467	661	877	1087	1297	1523	1741
3	131	293	479	673	881	1091	1301	1531	1747
5	137	307	487	677	883	1093	1303	1543	1753
7	139	311	491	683	887	1097	1307	1549	1759
11	149	313	499	691	907	1103	1319	1553	1777
13	151	317	503	701	911	1109	1321	1559	1783
17	157	331	509	709	919	1117	1327	1567	1787
19	163	337	521	719	929	1123	1361	1571	1789
23	167	347	523	727	937	1129	1367	1579	1801
29	173	349	541	733	941	1151	1373	1583	1811
31	179	353	547	739	947	1153	1381	1597	1823
37	181	359	557	743	953	1163	1399	1601	1831
41	191	367	563	751	967	1171	1409	1607	1847
43	193	373	569	757	971	1181	1423	1609	1861
47	197	379	571	761	977	1187	1427	1613	1867
53	199	383	577	769	983	1193	1429	1619	1871
59	211	389	587	773	991	1201	1433	1621	1873
61	223	397	593	787	997	1213	1439	1627	1877
67	227	401	599	797	1009	1217	1447	1637	1879
71	229	409	601	809	1013	1223	1451	1657	1889
73	233	419	607	811	1019	1229	1453	1663	1901
79	239	421	613	821	1021	1231	1459	1667	1907
83	241	431	617	823	1031	1237	1471	1669	1913
89	251	433	619	827	1033	1249	1481	1693	1931
97	257	439	631	829	1039	1259	1483	1697	1933
101	263	443	641	839	1049	1277	1487	1699	1949
103	269	449	643	853	1051	1279	1489	1709	1951
107	271	457	647	857	1061	1283	1493	1721	1973
109	277	461	653	859	1063	1289	1499	1723	1979
113	281	463	659	863	1069	1291	1511	1733	1987

Mocniny 2^n, 3^n

n	2^n	3^n	
1	2	3	
2	4	9	
3	8	27	
4	16	81	
5	32	243	
6	64	729	
7	128	2 187	
8	256	6 561	
9	512	19 683	
10	1 024	59 049	
11	2 048	177 147	
12	4 096	531 441	
13	8 192	1 594 323	
14	16 384	4 782 969	
15	32 768	14 348 907	
16	65 536	43 046 721	
17	131 072	129 140 163	
18	262 144	387 420 489	
19	524 288	1 162 261 467	
20	1 048 576	3 486 784 401	
21	2 097 152	10 460 353 203	
22	4 194 304	31 381 059 609	
23	8 388 608	94 143 178 827	
24	16 777 216	282 429 536 481	
25	33 554 432	847 288 609 443	

Kanonické rozklady čísel $2^n - 1$, $2^n + 1$

n	$2^n - 1$	$2^n + 1$	
1		3	
2	3	5	
3	7	3^2	
4	3.5	17	
5	31	3.11	
6	3^2.7	5.13	
7	127	3.43	
8	3.5.15	257	
9	7.73	3^3.19	
10	3.11.31	5^2.51	
11	23.89	3.683	
12	3^2.5.7.13	17.241	
13	8191	3.2731	
14	3.43.127	5.29.113	
15	7.31.151	3^2.11.331	
16	3.5.17.257	65 537	
17	131 071	3.43 691	
18	3^3.7.19.73	2^6.3^2.5.7.13	
19	524 287	3.174 763	
20	3.5^2.11.31.41	17.61 681	
21	7^2.127.337	3^2.43.5419	
22	3.23.89.683	5.397.2113	
23	47.178 481	3.2 796 203	
24	3^2.5.7.13.17.241	97.257.673	
25	31.601.1801	3.11.251.4051	

OBSAH

Předmluva – – – – – – – – – – – – – – 3
1. Některé vlastnosti množin čísel celých – – – 7
2. Základní pojmy a věty z nauky o dělitelnosti čísel 20
3. Vyšetřování dělitelnosti celých čísel – – – – 33
4. Číselné soustavy a kritéria dělitelnosti – – – 46
5. Největší společný dělitel – – – – – – – 61
6. Nejmenší společný násobek – – – – – – 73
7. Prvočísla a čísla složená – – – – – – – 80
8. Starověký problém čínských matematiků a pseudoprvočísla – – – – – – – – – 93
9. Malá věta Fermatova – – – – – – – – 98
10. Některé staré i nové problémy číselné teorie – 106

Tabulky: I. Prvočísla od 2 do 1987 – – – – 116
II. Mocniny 2^n, 3^n – – – – – – 117
III. Kanonické rozklady čísel $2^n - 1$, $2^n + 1$ – – – – – – 118

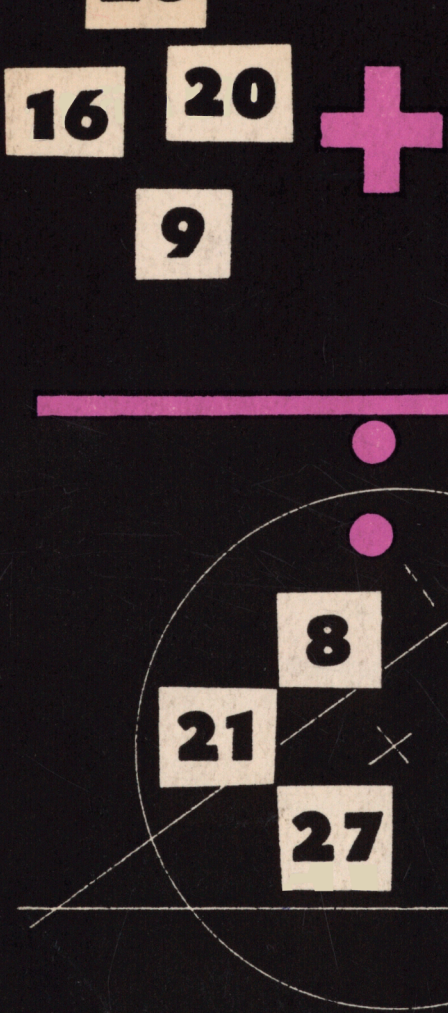
ŠKOLA MLADÝCH MATEMATIKŮ

FRANTIŠEK VESELÝ

o dělitelnosti čísel celých

Pro účastníky matematické olympiády vydává
ÚV Matematické olympiády a ÚV ČSM
v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Obálku navrhl Jaroslav Příbramský
Odpovědný redaktor Milan Daneš
Publikace číslo 2361
Edice Škola mladých matematiků, svazek 14
Vytiskl Mír, n. p., závod 2, provozovna 22
Praha 2, Legerova 22
5,47 AA, 5,65 VA. D—12*60151
Náklad 7400 výtisků. 1. vydání
120 stran. Praha 1966

23—059—66 03—2 Cena brož. výt. Kčs 4,50


16
20
9
8
21
27