7. kapitola. Prvočísla a čísla složená

In: František Veselý (author): O dělitelnosti čísel celých. (Czech). Praha: Mladá fronta, 1966. pp. 80–92.

Persistent URL: http://dml.cz/dmlcz/403570

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.