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

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

II. Pro součet všech přirozených dělitelů čísla n platí

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

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

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

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

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.

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 přirozená 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 $F_5 = 641 \,.\, 6700417$. 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 $5 \,.\, 2^{38} + 1 = 2748779069441$. 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}.