8. kapitola. Starověký problém čínských matematiků a pseudoprvočísla

In: František Veselý (author): O dělitelnosti čísel celých. (Czech). Praha: Mladá fronta, 1966. pp. 93–97.

Persistent URL: http://dml.cz/dmlcz/403571

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 $561 \mid 3^{561} - 3$; $1105 \mid 3^{1105} - 3$; $561 \mid 33^{561} - 33$.