9. kapitola. Malá věta Fermatova

In: František Veselý (author): O dělitelnosti čísel celých. (Czech). Praha: Mladá fronta, 1966. pp. 98–105.

Persistent URL: http://dml.cz/dmlcz/403572

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) $1905 \mid a^{1905} - a$.