3. kapitola. Vyšetřování dělitelnosti celých čísel

In: František Veselý (author): O dělitelnosti čísel celých. (Czech). Praha: Mladá fronta, 1966. pp. 33–45.

Persistent URL: http://dml.cz/dmlcz/403566

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.