3. kapitola. Zbytkové třídy podle modulu m. Úplné a redukované soustavy zbytků podle modulu m

In: Alois Apfelbeck (author): Kongruence. (Czech). Praha: Mladá fronta, 1968. pp. 21–42.

Persistent URL: http://dml.cz/dmlcz/403655

3. kapitola

ZBYTKOVÉ TŘÍDY PODLE MODULU m. ÚPLNÉ A REDUKOVANÉ SOUSTAVY ZBYTKŮ PODLE MODULU m

V této kapitole budeme studovat závislost nejmenšího nezáporného zbytku celého čísla a při dělení přirozeným číslem m na změnách čísla a. Poněvadž budeme často pracovat současně s několika různými moduly, budeme tento nejmenší nezáporný zbytek značit symbolem $r_m(a)$.

Podle věty 1 existuje ke každému celému číslu a a přirozenému číslu m právě jedna dvojice celých čísel x a $r_m(a)$ tak, že současně platí

$$a = mx + r_m(a), \tag{23}$$

$$0 \leqq r_m(a) < m. \tag{24}$$

Je-li přirozené číslo m dáno pevně, můžeme ke každému celému číslu a přiřadit podle (23) a (24) právě jedno celé číslo $r_m(a)$, které nabývá některé z hodnot $0, 1, 2, \ldots, m - 1$. Ze vztahu (23) a definic 2 a 4 plyne, že

$$a \equiv r_m(a) \bmod m. \tag{25}$$

Definice 6. *Nechť m je dané přirozené číslo a nechť k je některé z čísel $0, 1, 2, \ldots, m - 1$. Sestrojme m množin $A_0^{(m)}, A_1^{(m)}, A_2^{(m)}, \ldots, A_{m-1}^{(m)}$ tak, že do množiny $A_k^{(m)}$ dáme všechna celá čísla, která jsou kongruentní s číslem k podle modulu m. Tyto množiny budeme nazývat zbytkovými třídami podle modulu m.*

Příklad 11. Sestrojte zbytkové třídy podle modulu $m = 5$.

Řešení. Podle definice 6 bude

$$A_0^{(5)} = \{\ldots, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, \ldots\},$$

$$A_1^{(5)} = \{\ldots, -24, -19, -14, -9, -4, 1, 6, 11, 16, 21, 26, \ldots\},$$

$$A_2^{(5)} = \{\ldots, -23, -18, -13, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\},$$

$$A_3^{(5)} = \{\ldots, -22, -17, -12, -7, -2, 3, 8, 13, 18, 23, 28, \ldots\},$$

$$A_4^{(5)} = \{\ldots, -21, -16, -11, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}.$$

Abychom mohli vyšetřit některé vlastnosti zbytkových tříd, dokážeme nejprve.

větu 14. *Budiž m přirozené číslo a nechť každé z čísel h a k nabývá některé z hodnot* 0, 1, 2, ..., $m - 1$. *Potom* $h \equiv k \bmod m$ *právě tehdy, je-li* $h = k$.

Důkaz. Je-li $h = k$, je $h - k = 0$, takže podle věty 2 je $m \mid (h - k)$, tj. $h \equiv k \bmod m$.

Jestliže $h \neq k$, můžeme předpokládat, že je např. $h > k$, takže $0 \leqq k < h < m$ a tedy $0 < h - k < m$. Kdyby bylo $h \equiv k \bmod m$, bylo by $m \mid (h - k)$. To však není možné, neboť podle úlohy 2* by pak muselo být $h - k \geqq m$. Proto platí $h \not\equiv k \bmod m$, čímž je věta 14 dokázaná.

Podle věty 14 jsou tedy kterákoliv dvě různá čísla ze systému 0, 1, 2, ... , $m - 1$ inkongruentní podle modulu m.

Věta 15. *Nechť m je přirozené číslo. Potom celá čísla a a b leží ve stejné zbytkové třídě podle modulu m právě tehdy, je-li* $a \equiv b \bmod m$.

Důkaz. Nechť celá čísla a a b jsou obě ze zbytkové třídy $A_k^{(m)}$ podle modulu m. Podle definice 6 je $a \equiv k \bmod m$ a $b \equiv k \bmod m$, takže podle (11) je i $a \equiv b \bmod m$.

Nechť obráceně $a \equiv b \bmod m$ a nechť číslo a je ze zbytkové třídy $A_h^{(m)}$ a číslo b ze zbytkové třídy $A_k^{(m)}$ podle modulu m. Podle definice 6 je $a \equiv h \bmod m$ a $b \equiv k \bmod m$, takže podle (11) je opět $h \equiv k \bmod m$. Poněvadž však h a k jsou obě ze systému čísel $0, 1, 2, \ldots, m-1$, plyne z věty 14, že $h = k$. Čísla a a b leží tedy v téže zbytkové třídě podle modulu m, což jsme chtěli dokázat.

Poněvadž pro každé celé číslo a platí, že $a \equiv a \bmod m$, plyne z věty 15, že žádné celé číslo a nemůže ležet současně ve dvou různých zbytkových třídách podle daného modulu m. Ke každému celému číslu lze tedy najít právě jednu zbytkovou třídu podle modulu m, ve které toto číslo leží. Z věty 15 dále vidíme, že kterákoliv ze zbytkových tříd podle modulu m je zcela určena, známe-li alespoň jeden její prvek. Každý další prvek této zbytkové třídy je pak s uvedeným prvkem kongruentní podle modulu m. Všechno to, co jsme si právě ukázali, nás opravňuje k následující

definici 7. *Kterýkoliv z prvků dané zbytkové třídy podle modulu m nazýváme reprezentantem této třídy. Prvky z téže zbytkové třídy podle daného modulu nazýváme též ekvivalentními.*

Definice 8. *Budiž m přirozené číslo. Jakoukoliv soustavu m celých čísel, kterou obdržíme, vezmeme-li z každé zbytkové třídy $A_0^{(m)}, A_1^{(m)}, A_2^{(m)}, \ldots, A_{m-1}^{(m)}$ podle modulu m po jednom prvku, budeme nazývat úplnou soustavou zbytků podle modulu m.*

Příklad 12. Utvořte alespoň třemi způsoby úplnou soustavu zbytků podle modulu 7.

Řešení. Z definice 8 snadno zjistíme, že např. {0, 1, 2, 3, 4, 5, 6}, {—3, —2, —1, 0, 1, 2, 3} a {—10, 5, 13, —7, 8, 23, —32} jsou úplné soustavy zbytků podle modulu 7.

Věta 16. *Libovolný systém m po sobě jdoucích celých čísel tvoří úplnou soustavu zbytků podle modulu m.*

Důkaz. Vyšetřme systém m po sobě jdoucích celých čísel a, $a + 1$, $a + 2$, ..., $a + m - 1$. Abychom dokázali, že tato čísla tvoří úplnou soustavu zbytků podle modulu m, bude s ohledem na definici 8 třeba ukázat, že patří do vzájemně různých tříd podle tohoto modulu. Podle věty 15 to však bude splněno, budou-li kterákoliv dvě různá čísla této soustavy podle modulu m inkongruentní. Buďte tedy $a + h$ a $a + k$ libovolná dvě čísla této soustavy, která jsou vzájemně různá, takže $h \not\equiv k$, přičemž každé z čísel h a k nabývá některé z hodnot 0, 1, 2, ..., $m - 1$. Kdyby platilo $a + h \equiv a + k \bmod m$, dostali bychom podle (13) též $h \equiv k \bmod m$, takže podle věty 14 bychom měli, že $h = k$. To však je proti předpokladu o číslech h a k. Proto musí být $a + h \not\equiv a + k \bmod m$, což jsme měli dokázat.

Abychom pochopili, jaký je praktický význam pojmů zbytkových tříd a úplné soustavy zbytků podle modulu m, zobecníme si ještě větu 9.

Věta 17. *Buďte m, q, n_1, n_2, ..., n_q přirozená čísla. Nechť dále*

$$\begin{array}{llll} a_{11}, a_{12}, \ldots, a_{1n_1}; & a'_{11}, a'_{12}, \ldots, a'_{1n_1}; \\ a_{21}, a_{22}, \ldots, a_{2n_2}; & a'_{21}, a'_{22}, \ldots, a'_{2n_2}; \\ \vdots & \\ a_{q1}, a_{q2}, \ldots, a_{qn_q}; & a'_{q1}, a'_{q2}, \ldots, a'_{qn_q} \end{array}$$

jsou celá čísla a nechť pro každou dvojici indexů i a j $(1 \leqq i \leqq q;\ 1 \leqq j \leqq n_i)$ platí

$$a_{ij} \equiv a'_{ij} \bmod m. \tag{26}$$

Nechť konečně

$$a_{11}a_{12} \ldots a_{1n_1} + a_{21}a_{22} \ldots a_{2n_2} + \ldots + a_{q1}a_{q2} \ldots a_{qn_q} \equiv \equiv 0 \bmod m. \tag{27}$$

Potom je

$$a'_{11}a'_{12} \ldots a'_{1n_1} + a'_{21}a'_{22} \ldots a'_{2n_2} + \ldots + a'_{q1}a'_{q2} \ldots a'_{qn_q} \equiv \equiv 0 \bmod m. \tag{28}$$

Důkaz. Zvolme nejprve pevně index i $(1 \leqq i \leqq q)$. Z kongruencí

$$\begin{aligned} a_{i1} &\equiv a'_{i1} \bmod m, \\ a_{i2} &\equiv a'_{i2} \bmod m, \\ &\vdots \\ a_{in_i} &\equiv a'_{in_i} \bmod m \end{aligned}$$

dostaneme opakovaným použitím vztahu (17)

$$a_{i1}a_{i2} \ldots a_{in_i} \equiv a'_{i1}a'_{i2} \ldots a'_{in} \bmod m.$$

Vezmeme-li za i postupně čísla 1, 2, ..., q, máme tedy

$$\begin{aligned} a_{11}a_{12} \ldots a_{1n_1} &\equiv a'_{11}a'_{12} \ldots a'_{1n_1} \bmod m, \\ a_{21}a_{22} \ldots a_{2n_2} &\equiv a'_{21}a'_{22} \ldots a'_{2n_2} \bmod m, \\ &\vdots \\ a_{q1}a_{q2} \ldots a_{qn_q} &\equiv a'_{q1}a'_{q2} \ldots a'_{qn_q} \bmod m. \end{aligned}$$

Sečtením těchto kongruencí [tj. opakovaným použitím vztahu (15)] dostaneme

$$a_{11}a_{12} \ldots a_{1n_1} + a_{12}a_{22} \ldots a_{2n_2} + \ldots + a_{q1}a_{q2} \ldots a_{qn_q} \equiv$$

$\equiv a'_{11}a'_{12} \ldots a'_{1n_1} + a'_{21}a'_{22} \ldots a'_{2n_2} + \ldots + a'_{q1}\, a'_{q2} \ldots a'_{qn_q}$ mod m.

Z poslední kongruence a z kongruence (27) pak podle (11) plyne kongruence (28), což jsme chtěli dokázat.

V důkazu, který jsme právě provedli, jsme dvakrát mlčky užili matematické indukce. Poprvé to bylo při rozšiřování platnosti vztahu (17) pro libovolný počet činitelů, podruhé pak při rozšiřování vztahu (15) pro libovolný počet sčítanců. Podrobné provedení těchto kroků si čtenář může snadno udělat sám.

Čísla a_{ij} a a'_{ij} ($1 \leq i \leq q$; $1 \leq j \leq n_i$) nemusí být vzájemně různá. Proto vyskytne-li se v nějaké kongruenci přirozená mocnina celého čísla, můžeme ji rozepsat ve tvaru patřičného součinu. Z toho vidíme, že všechny kongruence, které jsme dosud poznali, lze psát ve tvaru (27).

Vztahy (26) znamenají, že kterýkoliv prvek a'_{ij} je ekvivalentní s odpovídajícím prvkem a_{ij}. Větu 17 můžeme tedy formulovat stručně tak, že v každé kongruenci podle modulu m lze libovolný její prvek nahradit prvkem, který je s původním ekvivalentní podle modulu m, aniž by tím byla porušena správnost kongruence.

Důsledkem toho je, že při vyšetřování jakékoliv kongruence podle modulu m nemusíme brát v úvahu všechna celá čísla, nýbrž se můžeme omezit pouze na m celých čísel, která tvoří úplnou soustavu zbytků podle modulu m. Takovouto úplnou soustavu zbytků můžeme utvořit neomezeně mnoha způsoby. My si však nyní můžeme ze všech možných soustav vybrat právě tu, se kterou se nám bude nejlépe a nejpohodlněji pracovat. Zpravidla to bývá soustava $\{0, 1, 2, \ldots, m - 1\}$ nebo $\{1, 2, 3, \ldots, m\}$.

Dosud jsme se zabývali kongruencemi, jejichž modul byl pevně zvolen. Nyní obrátíme pozornost ke kongruencím, jejichž modul se bude měnit.

Věta 18. *Buďte m a m_1 přirozená čísla a nechť $m_1 | m$. Nechť ještě $a \equiv b \bmod m$. Potom též $a \equiv b \bmod m_1$.*

Důkaz. Poněvadž $a \equiv b \bmod m$, bude $m | (a - b)$. Ze vztahů $m | (a - b)$ a $m_1 | m$ podle definice 2 plyne, že existují celá čísla x a y tak, že $a - b = mx$ a $m = m_1 y$. Z těchto rovností dostáváme dále, že existuje celé číslo $z = xy$ tak, že $a - b = m_1(xy) = m_1 z$. Podle definice 2 je tedy $m_1 | (a - b)$, tj. $a \equiv b \bmod m_1$, což bylo třeba dokázat.

Věta 19. *Buďte m_1 a m_2 přirozená čísla a nechť $(m_1, m_2) = 1$. Nechť konečně x probíhá úplnou soustavou zbytků podle modulu m_1 a y úplnou soustavou zbytků podle modulu m_2. Potom výraz $z = m_2 x + m_1 y$ probíhá úplnou soustavou zbytků podle modulu $m = m_1 m_2$.*

Důkaz. Poněvadž číslo x nabývá m_1 hodnot vzájemně inkongruentních podle modulu m_1 a nezávisle na tom číslo y pak m_2 hodnot vzájemně inkongruentních podle modulu m_2, bude výraz $z = m_2 x + m_1 y$ nabývat pro tato x a y celkem $m = m_1 m_2$ hodnot. Podle definice 8 a věty 15 stačí dokázat, že tyto hodnoty jsou vzájemně inkongruentní podle modulu m.

Předpokládejme, že tomu tak není. Potom existují čísla x, x', y, y' tak, že

$$m_2 x + m_1 y \equiv m_2 x' + m_1 y' \bmod m, \qquad (29)$$

přičemž neplatí současně $x \equiv x' \bmod m_1$ a $y \equiv y' \bmod m_2$. Poněvadž $m_1 | m$ i $m_2 | m$, plyne z kongruence (29) podle věty 18, že současně platí

$$m_2x + m_1y \equiv m_2x' + m_1y' \bmod m_1,$$
$$m_2x + m_1y \equiv m_2x' + m_1y' \bmod m_2.$$

Zjednodušením těchto kongruencí dostaneme dále

$$m_2x \equiv m_2x' \bmod m_1,$$
$$m_1y \equiv m_1y' \bmod m_2.$$

Čísla m_1 a m_2 jsou však nesoudělná, takže podle věty 11 můžeme první z kongruencí krátit číslem m_2 a druhou číslem m_1. Dostaneme tedy, že musí současně platit $x \equiv x' \bmod m_1$ a $y \equiv y' \bmod m_2$, což odporuje předpokladu o číslech x, x', y a y'. Tím je věta dokázaná.

Na základě věty, kterou jsme právě dokázali, můžeme nyní rozšířit platnost věty 18.

Věta 20. *Buďte m_1 a m_2 přirozená čísla, $(m_1, m_2) = 1$ a $m = m_1m_2$. Potom $a \equiv b \bmod m$ platí právě tehdy, platí-li současně $a \equiv b \bmod m_1$ a $a \equiv b \bmod m_2$.*

Důkaz. Nechť $a \equiv b \bmod m$. Poněvadž $m_1 | m$ i $m_2 | m$, bude podle věty 18 současně $a \equiv b \bmod m_1$ i $a \equiv b \bmod m_2$.

Obráceně, nechť je současně $a \equiv b \bmod m_1$ a $a \equiv b \bmod m_2$. Potom čísla $\frac{a-b}{m_1} = \frac{(a-b)m_2}{m}$ i $\frac{a-b}{m_2} = \frac{(a-b)m_1}{m}$ budou celá, takže bude současně platit

$$am_2 \equiv bm_2 \bmod m,$$
$$am_1 \equiv bm_1 \bmod m.$$

Odtud dostaneme pro libovolnou dvojici celých čísel ξ a η podle (14)

$$am_2\xi \equiv bm_2\xi \bmod m,$$
$$am_1\eta \equiv bm_1\eta \bmod m,$$

z čehož podle (15) obdržíme konečně

$$a(m_2\xi + m_1\eta) \equiv b(m_2\xi + m_1\eta) \bmod m. \qquad (30)$$

Podle předpokladu věty je $(m_1, m_2) = 1$. Proto necháme-li probíhat číslo x nějakou libovolně zvolenou úplnou soustavou zbytků podle modulu m_1 a číslo y obdobně úplnou soustavou zbytků podle modulu m_2, bude podle věty 19 výraz $m_2x + m_1y$ probíhat úplnou soustavou zbytků podle modulu m. Můžeme tudíž ve zvolených úplných soustavách zbytků najít čísla ξ a η taková, že výraz $m_2\xi + m_1\eta$ bude ze zbytkové třídy $A_1^{(m)}$. To však znamená, že $m_2\xi + m_1\eta \equiv 1 \bmod m$. Odtud a ze vztahu (30) dostaneme podle věty 17, že $a \equiv b \bmod m$.

Položme si nyní úkol určit všechna celá čísla, která jsou nesoudělná s daným přirozeným číslem $m > 1$.

Věta 21. *Obsahuje-li zbytková třída $A_k^{(m)}$ podle modulu m číslo, které je nesoudělné s m, jsou všechna čísla z této zbytkové třídy nesoudělná s m.*

Důkaz. Nechť číslo a je ze zbytkové třídy $A_k^{(m)}$, přičemž $(a, m) = 1$. Podle věty 15 platí pro kterýkoliv prvek b této zbytkové třídy vztah $a \equiv b \bmod m$. Předpokládejme, že $(b, m) = d > 1$. Poněvadž $d|m$, bude podle věty 18 též $a \equiv b \bmod d$. Poněvadž však též $d|b$, bude $b \equiv 0 \bmod d$. Ze vztahů $a \equiv b \bmod d$ a $b \equiv 0 \bmod d$ plyne podle (11), že $a \equiv 0 \bmod d$ neboli $d|a$. Číslo $d > 1$ je tedy dělitelem čísla a i čísla m, což odporuje předpokladu o nesoudělnosti těchto čísel. Bude proto $(b, m) = 1$, což jsme měli dokázat.

Z věty 21 vyplývá, že úlohu formulovanou výše můžeme převést na úlohu najít všechny zbytkové třídy

podle modulu m, které obsahují čísla nesoudělná s m. Avšak podle definice 6 obsahuje zbytková třída $A_k^{(m)}$ číslo k. Podle věty 21 tedy stačí určit, která z čísel 0, 1, 2, ..., $m - 1$ jsou nesoudělná s číslem m.

Přesto, že se nám podařilo původní úlohu takto zjednodušit, nedovedeme její řešení pro obecně dané přirozené číslo $m > 1$ jednoduše napsat. Při konkrétně daném m dovedeme však všechna čísla nesoudělná s číslem m rovněž konkrétně určit.

Příklad 13. Určete, která z čísel 0, 1, 2, ..., $m - 1$ jsou nesoudělná s číslem m, je-li

a) $m = 28$,

b) $m = 24$,

c) $m = 13$.

Řešení. Snadno zjistíme, že

a) pro $m = 28$ jsou to čísla 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27;

b) pro $m = 24$ jsou to čísla 1, 5, 7, 11, 13, 17, 19, 23;

c) pro $m = 13$ jsou to čísla 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

Poněkud snazší bude úloha určit počet zbytkových tříd podle modulu m, které obsahují pouze čísla nesoudělná s m. Jak už víme, bude tento počet zbytkových tříd rovný počtu čísel z úplné soustavy zbytků 0, 1, 2, ..., $m - 1$, která jsou nesoudělná s číslem m.

Definice 9. *Budiž m přirozené číslo. Počet čísel z úplné soustavy zbytků 0, 1, 2, ..., $m - 1$, která jsou nesoudělná s číslem m, budeme značit symbolem $\varphi(m)$. Funkci $\varphi(m)$ definovanou pro všechna přirozená čísla budeme nazývat Eulerovou funkcí.*

Příklad 14. $\varphi(1) = 1, \varphi(28) = 12, \varphi(24) = 8, \varphi(13) = 12$ (viz příklad 13).

Vezměme nyní zcela libovolnou úplnou soustavu zbytků podle modulu m. Z předchozích úvah už víme, že mezi těmito čísly je právě $\varphi(m)$ těch, která jsou nesoudělná s m.

Definice 10. *Budiž m přirozené číslo. Redukovanou soustavou zbytků podle modulu m nazveme soustavu $\varphi(m)$ čísel, která dostaneme, vybereme-li z libovolně dané úplné soustavy zbytků podle modulu m všechna čísla nesoudělná s číslem m.*

Z definic 10 a 8 a věty 15 ihned plyne, že žádné dva členy redukované soustavy zbytků podle modulu m nejsou spolu podle tohoto modulu kongruentní.

V příkladu 13 jsme nalezli redukované soustavy zbytků podle modulů 28, 24 a 13.

Při vytváření zbytkových tříd podle daného modulu jsme si mohli povšimnout jisté periodičnosti celého systému (viz příklad 11). Této periodičnosti lze někdy využít i v praxi.

Příklad 15. Přiřaďme jednotlivým dnům v týdnu celá čísla takto:

Neděle	... 0	Čtvrtek	... 4
Pondělí	... 1	Pátek	... 5
Úterý	... 2	Sobota	... 6
Středa	... 3		

Dostáváme tak prakticky použitelný model úplné soustavy zbytků podle modulu 7. Zbytkovými třídami jsou zde „všechny neděle“, „všechny pondělky“, „všechny úterky“ atd. Při tomto přiřazení představují pracovní

dny normálního týdne model redukované soustavy zbytků podle modulu 7.

Obdobně můžeme přiřadit jednotlivým měsícům v roce jejich pořadová čísla 1, 2, ..., 12.

Uvedených modelů se dá využít k rychlému určení dne v týdnu, na který připadá dané datum (tzv. věčný kalendář). Odvozování vzorců, pomocí kterých se tato úloha řeší, je však značně komplikované, neboť je třeba do nich zahrnout nestejnou délku měsíců, „přestupnost" roků a další nepravidelnosti kalendáře.

Vraťme se nyní ke studiu některých vlastností redukovaných soustav zbytků podle daného modulu.

Věta 22. *Buďte* m_1 *a* m_2 *přirozená čísla a nechť* $(m_1, m_2) = 1$. *Nechť dále* x *a* y *jsou celá čísla. Položme ještě* $m = m_1 m_2$ *a* $z = m_2 x + m_1 y$. *Potom* $(z, m) = 1$ *právě tehdy, je-li současně* $(x, m_1) = 1$ *a* $(y, m_2) = 1$.

Důkaz. Nechť $(z, m) = 1$. Kdyby bylo např. $(x, m_1) = d > 1$, bylo by $d | x$ a $d | m_1$, takže podle věty 3 by též bylo $d | (m_2 x + m_1 y)$ a $d | m_1 m_2$, tj. $d | z$ a $d | m$. To však odporuje předpokladu o nesoudělnosti čísel z a m. Musí být proto $(x, m_1) = 1$. Obdobně se dokáže, že i $(y, m_2) = 1$.

Nechť obráceně $(z, m) = d > 1$. Potom $d | z$ i $d | m$, takže platí $z \equiv 0 \bmod d$ a $m \equiv 0 \bmod d$. Poněvadž $d > 1$, existuje prvočíslo p takové, že $p | d$. Podle věty 18 bude tedy $z \equiv 0 \bmod p$ a $m \equiv 0 \bmod p$, takže po dosazení za z a za m máme $m_2 x + m_1 y \equiv 0 \bmod p$ a $m_1 m_2 \equiv 0 \bmod p$. Podle věty 13 plyne z kongruence $m_1 m_2 \equiv 0 \bmod p$, že buďto $m_1 \equiv 0 \bmod p$, nebo $m_2 \equiv 0 \bmod p$. Nechť např. $m_1 \equiv 0 \bmod p$, tj. $p | m_1$. Poněvadž předpokládáme, že $(m_1, m_2) = 1$, platí $p \nmid m_2$, tj. $(m_2, p) = 1$. Z kongruence $m_2 x + m_1 y \equiv 0 \bmod p$ plyne

dále $m_2 x \equiv 0 \bmod p$ a poněvadž $(m_2, p) = 1$, bude podle věty 11 $x \equiv 0 \bmod p$. Platí tedy, že $p|x$ a $p|m_1$, takže $(x, m_1) \geqq p > 1$. Proto nemůže v tomto případě platit současně $(x, m_1) = 1$ a $(y, m_2) = 1$, čímž je věta 22 dokázaná.

Věta 23. *Buďte m_1 a m_2 přirozená čísla a nechť $(m_1, m_2) = 1$. Potom, probíhá-li x redukovanou soustavou zbytků podle modulu m_1 a y redukovanou soustavou zbytků podle modulu m_2, probíhá výraz $z = m_2 x + m_1 y$ redukovanou soustavou zbytků podle modulu $m = m_1 m_2$.*

Důkaz. Zvolme si libovolnou úplnou soustavu zbytků podle modulu m_1 a libovolnou úplnou soustavu zbytků podle modulu m_2 a sestrojme k těmto soustavám příslušné redukované soustavy zbytků. Probíhá-li x zvolenou úplnou soustavou zbytků podle modulu m_1 a y úplnou soustavou zbytků podle modulu m_2, probíhá podle věty 19 výraz $z = m_2 x + m_1 y$ úplnou soustavou zbytků podle modulu $m = m_1 m_2$. Z této úplné soustavy zbytků dostaneme redukovanou soustavu zbytků podle modulu m tak, že z ní vybereme všechna čísla z nesoudělná s m. Avšak podle věty 22 dostáváme takováto z právě tehdy, když pro odpovídající čísla x a y platí $(x, m_1) = (y, m_2) = 1$, tj. když x je z dané redukované soustavy zbytků podle modulu m_1 a y z dané redukované soustavy zbytků podle modulu m_2.

Důsledkem věty, kterou jsme právě dokázali, je

věta 24. *Jsou-li m_1 a m_2 nesoudělná přirozená čísla, platí $\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2)$.*

Důkaz. Číslo x z předchozí věty nabývá $\varphi(m_1)$ hodnot vzájemně inkongruentních podle modulu m_1 a nezávisle

na tom číslo y pak $\varphi(m_2)$ hodnot vzájemně inkongruentních podle modulu m_2, takže výraz $z = m_2x + m_1y$ nabývá celkem $\varphi(m_1)\,\varphi(m_2)$ hodnot vzájemně inkongruentních podle modulu m_1m_2. Na druhé straně, poněvadž z probíhá redukovanou soustavou zbytků podle modulu m_1m_2, nabývá toto z celkem $\varphi(m_1m_2)$ hodnot vzájemně inkongruentních podle modulu m_1m_2, takže skutečně platí $\varphi(m_1m_2) = \varphi(m_1)\,\varphi(m_2)$.

Věta 25. *Nechť* $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{\nu-1}^{\alpha_{\nu-1}}p_\nu^{\alpha_\nu}$, *kde* $p_1, p_2, \dots, p_{\nu-1}, p_\nu$ *jsou vzájemně různá prvočísla a* $\alpha_1, \alpha_2, \dots, \alpha_{\nu-1}, \alpha_\nu$ *přirozená čísla. Potom*

$$\varphi(m) = p_1^{\alpha_1-1}p_2^{\alpha_2-1}\dots p_{\nu-1}^{\alpha_{\nu-1}-1}p_\nu^{\alpha_\nu-1}(p_1-1)(p_2-1)\dots \dots(p_{\nu-1}-1)(p_\nu-1). \tag{31}$$

Pro prvočíslo p *je speciálně*

$$\varphi(p) = p - 1. \tag{32}$$

Důkaz. Nejprve dokážeme, že platí

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{\nu-1}^{\alpha_{\nu-1}}p_\nu^{\alpha_\nu}) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2})\dots \dots\varphi(p_{\nu-1}^{\alpha_{\nu-1}})\,\varphi(p_\nu^{\alpha_\nu}). \tag{33}$$

Poněvadž prvočísla $p_1, p_2, \dots, p_{\nu-1}, p_\nu$ jsou vzájemně různá, bude $(p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_{\nu-1}^{\alpha_{\nu-1}}, p_\nu^{\alpha_\nu}) = 1$. Podle věty 24 je tedy

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{\nu-1}^{\alpha_{\nu-1}}p_\nu^{\alpha_\nu}) = \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{\nu-1}^{\alpha_{\nu-1}})\,\varphi(p_\nu^{\alpha_\nu}).$$

Poněvadž jsme při důkazu tohoto částečného výsledku nečinili žádné předpoklady o počtu zde vystupujících mocnin prvočísel, můžeme jej aplikovat postupně na součin dvou, tří atd. činitelů, čímž dostaneme

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}),$$
$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}) = \varphi(p_1^{\alpha_1}p_2^{\alpha_2})\,\varphi(p_3^{\alpha_3}),$$
$$\vdots$$
$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{\nu-1}^{\alpha_{\nu-1}}p_\nu^{\alpha_\nu}) = \varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{\nu-1}^{\alpha_{\nu-1}})\,\varphi(p_\nu^{\alpha_\nu}).$$

Z těchto rovností pak postupným dosazováním dostaneme vztah (33).

Nyní vypočteme pro prvočíslo p a přirozené číslo α hodnotu $\varphi(p^\alpha)$. V úplné soustavě zbytků $0, 1, 2, \ldots, p^\alpha - 1$ nejsou nesoudělná s číslem p jen ta čísla, která jsou dělitelná prvočíslem p. Jsou to tedy čísla $0.p$, $1.p$, $2.p$, $3.p$, $\ldots$, $(p^{\alpha-1} - 1).p$. Těchto čísel je $p^{\alpha-1}$. Ostatní čísla této soustavy, kterých je $p^\alpha - p^{\alpha-1}$, jsou tedy nesoudělná s číslem p^α, takže je $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. Pro $\alpha = 1$ dostaneme ihned (32).

Bude tedy $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i - 1)$ $(i = 1, 2, \ldots, \nu - 1, \nu)$, což dosazeno do (33) dá dokazovaný vztah (31).

Nyní dokážeme několik vět zásadní důležitosti, jichž budeme v dalších kapitolách často užívat.

Věta 26. *Buďte a a b celá čísla a m přirozené číslo. Nechť ještě $(a, m) = 1$. Potom, probíhá-li x úplnou soustavou zbytků podle modulu m, probíhá výraz $ax + b$ rovněž úplnou soustavou zbytků podle modulu m.*

Důkaz. Probíhá-li x úplnou soustavou zbytků podle modulu m, nabývá výraz $ax + b$ celkem m různých hodnot. Podle definice 8 a věty 15 stačí dokázat, že tyto hodnoty jsou vzájemně inkongruentní podle modulu m. Nechť x a x' jsou dvě čísla z dané úplné soustavy zbytků podle modulu m a nechť pro tato čísla platí $ax + b \equiv ax' + b \bmod m$. Odtud podle (13) dostaneme

$ax \equiv ax' \bmod m$. Poněvadž je $(a, m) = 1$, plyne z poslední kongruence podle věty 11, že $x \equiv x' \bmod m$. Čísla x a x' tedy leží ve stejné zbytkové třídě podle modulu m a protože úplná soustava zbytků podle modulu m obsahuje z každé zbytkové třídy podle tohoto modulu jediný prvek, musí být $x = x'$, což jsme měli dokázat.

Věta 27. *Buďte a celé a m přirozené číslo. Nechť dále $(a, m) = 1$. Potom, probíhá-li x redukovanou soustavou zbytků podle modulu m, probíhá i výraz ax redukovanou soustavou zbytků podle modulu m.*

Důkaz. Výraz ax nabývá celkem $\varphi(m)$ hodnot, o nichž z věty 26 víme, že jsou vzájemně inkongruentní podle modulu m. Stačí tedy dokázat, že pro každé x z redukované soustavy zbytků podle modulu m je číslo ax nesoudělné s číslem m. Nechť tedy pro některé ze zmíněných čísel x platí $(ax, m) = d > 1$. Potom $ax \equiv 0 \bmod d$ a $m \equiv 0 \bmod d$. Protože $d > 1$, existuje prvočíslo p takové, že $p|d$. Podle věty 18 tedy bude $ax \equiv 0 \bmod p$ a $m \equiv 0 \bmod p$. Poněvadž je $(a, m) = 1$ a $p|m$, musí platit $p \nmid a$, takže je $(a, p) = 1$. Z kongruence $ax \equiv 0 \bmod p$ pak podle věty 11 dostaneme, že $x \equiv 0 \bmod p$. Máme tedy $p|x$ a $p|m$, takže $(x, m) \geqq p > 1$. To však není možné, neboť číslo x jsme zvolili z redukované soustavy zbytků podle modulu m. Musí proto být $(ax, m) = 1$ a to jsme chtěli dokázat.

Příklad 16. Ověřme si větu 27 na numerickém příkladě pro $a = 5$ a $m = 42$.

Z úplné soustavy zbytků 0, 1, 2, ..., 41 podle modulu 42 vybereme $\varphi(42) = \varphi(2).\varphi(3).\varphi(7) = 1.2.6 = 12$ čísel, která jsou nesoudělná s číslem 42. Dostaneme tak

redukovanou soustavu zbytků {1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41} podle modulu 42. Určíme-li z kongruence $5x \equiv r(x) \bmod 42$ čísla $r(x)$ tak, že $0 < r(x) < 42$, dostaneme pro $r(x)$ postupně {5, 25, 13, 23, 1, 11, 31, 41, 19, 29, 17, 37}. Vidíme, že oba systémy čísel se liší pouze pořadím.

Poznatek, který jsme v příkladu 16 učinili, má však obecnou platnost. Postupu, jehož jsme v tomto příkladu užili, použijeme v důkazu následující věty.

Věta 28. *Budiž m přirozené číslo. Potom pro každé celé číslo a nesoudělné s m platí*

$$a^{\varphi(m)} \equiv 1 \bmod m. \tag{34}$$

Důkaz. Z úplné soustavy zbytků 0, 1, 2, ..., $m - 1$ podle modulu m vybereme čísla $r_1, r_2, \ldots, r_{\varphi(m)}$, která jsou nesoudělná s číslem m. Tím dostaneme redukovanou soustavu zbytků podle modulu m. Podle věty 27 tvoří čísla $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ rovněž redukovanou soustavu zbytků podle modulu m. Můžeme tedy definovat čísla $r'_1, r'_2, \ldots, r'_{\varphi(m)}$ vztahy

$$ar_i \equiv r'_i \bmod m, \tag{35}$$

$$0 < r'_i < m \tag{36}$$

$[i = 1, 2, \ldots, \varphi(m)]$. Čísla $r'_1, r'_2, \ldots, r'_{\varphi(m)}$ takto definovaná tvoří opět redukovanou soustavu zbytků podle modulu m. Z nerovností (36) vidíme, že tato redukovaná soustava zbytků je rovněž tvořena čísly vybranými z úplné soustavy zbytků 0, 1, 2, ..., $m - 1$ podle modulu m. Proto obě soustavy $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ a $\{r'_1, r'_2, \ldots, r'_{\varphi(m)}\}$ jsou vytvořeny ze stejných čísel a liší se pouze pořadím, takže platí

$$r_1 r_2 \ldots r_{\varphi(m)} = r'_1 r'_2 \ldots r'_{\varphi(m)} = c. \tag{37}$$

Z věty 27 dále plyne, že součin dvou čísel nesoudělných s číslem m je opět číslo nesoudělné s m. Snadno nahlédneme, že toto tvrzení lze rozšířit na libovolný počet činitelů. Poněvadž čísla $r_1, r_2, \ldots, r_{\varphi(m)}$ jsou vesměs nesoudělná s číslem m, bude i číslo c definované vztahem (37) nesoudělné s m. Podle (35) můžeme dále psát

$$\begin{aligned} ar_1 &\equiv r_1' \bmod m\,, \\ ar_2 &\equiv r_2' \bmod m\,, \\ &\vdots \\ ar_{\varphi(m)} &\equiv r_{\varphi(m)}' \bmod m\,. \end{aligned}$$

Vynásobíme-li navzájem všech těchto $\varphi(m)$ kongruencí, dostaneme vzhledem k (37) kongruenci

$$a^{\varphi(m)}.c \equiv c \bmod m\,.$$

Poněvadž je $(c, m) = 1$, plyne z poslední kongruence podle věty 11 vztah (34), který jsme měli dokázat.

Všimněme si ještě jednoho speciálního případu věty 28, kdy modulem bude prvočíslo p. Podle (32) je $\varphi(p) = p - 1$. Jestliže tedy $p \nmid a$, bude mít vztah (34) tvar

$$a^{p-1} \equiv 1 \bmod p\,. \tag{38}$$

Vztah (38) je v teorii čísel nazýván malou větou Fermatovou, který ji poprvé formuloval v roce 1640 v dopise svému příteli Freniclu de Bessy. V dopise též tvrdil, že zná její důkaz, avšak tento důkaz se nezachoval. První známý důkaz malé Fermatovy věty podal Leibniz, který dokázal, že pro libovolné celé číslo a platí

$$a^p \equiv a \bmod p\,. \tag{39}$$

Vztahy (38) a (39) jsou zřejmě ekvivalentní, neboť pro $p|a$ je $a \equiv 0 \bmod p$ a tedy i $a^p \equiv 0 \bmod p$, takže vzhle-

dem k (11) platí (39). Jestliže však $p \nmid a$, dostaneme násobením kongruence (38) číslem a kongruenci (39) a obráceně krácením kongruence (39) číslem a kongruenci (38).

Věta 28 bývá často nazývána větou Eulerovou, který ji dokázal v roce 1760 zobecněním malé Fermatovy věty. Není bez zajímavosti, že Leonard Euler, který žil v letech 1707—1783, už s kongruencemi pracoval, avšak do matematiky je zavedl teprve o 70 let mladší Karl Friedrich Gauss (1777—1855). Od Gausse pochází též dnešní terminologie a označení v teorii kongruencí. Ve svém latinsky napsaném díle *Disquisitiones arithmeticae* shrnul Gauss tehdy známé výsledky z teorie čísel, které buďto sám objevil, nebo které znali už jeho předchůdci.

Závěrem této kapitoly si položme úlohu najít pro celé číslo a nesoudělné s přirozeným číslem m přirozená čísla k, pro která platí

$$a^k \equiv 1 \bmod m. \tag{40}$$

Z věty 28 plyne, že takovéto k vždycky existuje, neboť stačí položit $k = \varphi(m)$. Podle věty 10 můžeme dokonce za k zvolit libovolný přirozený násobek čísla $\varphi(m)$. Nás však bude více zajímat, jaké bude nejmenší přirozené číslo k, které splňuje kongruenci (40).

Příklad 17. Určete nejmenší přirozené číslo k, pro které platí $a^k \equiv 1 \bmod 54$, jestliže

a) $a = 5$;
b) $a = 17$;
c) $a = 19$.

Řešení. Úloha má smysl, neboť každé z čísel 5, 17 a 19 je nesoudělné s číslem 54. Bude jistě $k \leqq \varphi(54) =$

$= \varphi(2.3^3) = 18$. Abychom nemuseli pracovat s příliš velkými čísly, omezíme se na redukovanou soustavu zbytků podle modulu 54, která vznikne z úplné soustavy zbytků $\{-26, -25, -24, \ldots, 24, 25, 26, 27\}$. Užívajíce stále vztahů (17) a (11) dostaneme postupným násobením:

a) $5 \equiv 5 \bmod 54$; $5^{10} \equiv -5 \bmod 54$;
$5^2 \equiv 25 \bmod 54$; $5^{11} \equiv -25 \bmod 54$;
$5^3 \equiv 17 \bmod 54$; $5^{12} \equiv -17 \bmod 54$;
$5^4 \equiv -23 \bmod 54$; $5^{13} \equiv 23 \bmod 54$;
$5^5 \equiv -7 \bmod 54$; $5^{14} \equiv 7 \bmod 54$;
$5^6 \equiv 19 \bmod 54$; $5^{15} \equiv -19 \bmod 54$;
$5^7 \equiv -13 \bmod 54$; $5^{16} \equiv 13 \bmod 54$;
$5^8 \equiv -11 \bmod 54$; $5^{17} \equiv 11 \bmod 54$;
$5^9 \equiv -1 \bmod 54$; $5^{18} \equiv 1 \bmod 54$;

b) $17 \equiv 17 \bmod 54$; $17^4 \equiv -17 \bmod 54$;
$17^2 \equiv 19 \bmod 54$; $17^5 \equiv -19 \bmod 54$;
$17^3 \equiv -1 \bmod 54$; $17^6 \equiv 1 \bmod 54$;

c) $19 \equiv 19 \bmod 54$;
$19^2 \equiv -17 \bmod 54$;
$19^3 \equiv 1 \bmod 54$.

Hledané přirozené číslo je tedy v případě a) $k = 18$, v případě b) $k = 6$ a v případě c) $k = 3$.

Z uvedeného příkladu je zřejmé, že pravděpodobně nebudeme umět jednoduchým způsobem v obecném případě číslo k stanovit. V případě a) jsme dokonce viděli, že může nastat situace, kdy $k = \varphi(m)$. Můžeme si však povšimnout, že ve všech třech případech je číslo k dělitelem čísla $\varphi(54) = 18$. Ukážeme si, že tato skutečnost platí obecně.

Věta 29. *Nechť celé číslo a je nesoudělné s přirozeným*

číslem m. Nechť dále k je nejmenší přirozené číslo, pro které platí

$$a^k \equiv 1 \bmod m. \tag{40}$$

Potom $k|\varphi(m)$.

Důkaz. Z věty 28 plyne, že $k \leqq \varphi(m)$. K daným číslům $\varphi(m)$ a k můžeme nyní podle věty 1 najít celá čísla n a r tak, že platí vztahy

$$\varphi(m) = kn + r, \quad 0 \leqq r < k.$$

Bude tedy $a^{\varphi(m)} = a^{kn+r} = (a^k)^n . a^r$. Poněvadž platí vztah (40), bude podle (18) též $(a^k)^n \equiv 1 \bmod m$, takže podle (14) dostaneme $a^{\varphi(m)} \equiv a^r \bmod m$. Ježto však je $a^{\varphi(m)} \equiv 1 \bmod m$, bude podle (11) i $a^r \equiv 1 \bmod m$. Poněvadž k je nejmenší přirozené číslo, pro které platí vztah (40), a poněvadž $0 \leqq r < k$, musí být $r = 0$. Bude tedy $\varphi(m) = kn$, což podle definice 2 znamená, že $k|\varphi(m)$.

Úlohy

7. Dokažte, že platí:

   a) Druhá mocnina lichého čísla leží ve zbytkové třídě $A_1^{(4)}$.

   b) Druhá mocnina čísla, které není dělitelno třemi, leží ve zbytkové třídě $A_1^{(3)}$.

8. Nechť a probíhá redukovanou soustavou zbytků podle modulu m. Určete pro každé a z této redukované soustavy nejmenší přirozené číslo k, pro které platí (40), jestliže

   a) $m = 18$;

   b) $m = 42$.

9*. Nechť m je složené číslo, $m > 4$. Dokažte že

$$(m - 1)! \equiv 0 \bmod m.$$

10. Budiž p prvočíslo. Užitím vztahu (39) dokažte, že číslo

$$= \underbrace{11\ldots122\ldots233\ldots3}_{p\text{ cifer }p\text{ cifer }p\text{ cifer}} \ldots \underbrace{99\ldots9}_{p\text{ cifer}} - 123456789$$

je dělitelné prvočíslem p.