Kongruence

ŠKOLA MLADÝCH MATEMATIKŮ

KONGRUENCE

21

Vydal ÚV Matematické olympiády a ÚV ČSM v nakladatelství Mladá fronta

ŠKOLA MLADÝCH MATEMATIKŮ

kongruence

ALOIS APFELBECK

PRAHA 1968
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
A ÚV ČSM V NAKLADATELSTVÍ
MLADÁ FRONTA

Recenzovali odb. as. ČVUT Jiří Rohlíček a dr. Jaroslav Fuka

1. kapitola

OPAKOVÁNÍ ZÁKLADNÍCH POJMŮ O DĚLITELNOSTI

V této knížce budeme většinou používat pouze celých čísel, tj. přirozených čísel, nuly a celých záporných čísel. Předpokládáme, že čtenář umí běžně používat základních aritmetických operací (sčítání, odčítání, násobení a dělení), umocňování na přirozený exponent a jednoduchých nerovností.

Látka, kterou se budeme dále zabývat, vyžaduje, aby čtenář znal některé základní pojmy z nauky o dělitelnosti celých čísel. Proto si ty pojmy, které budeme dále používat nebo ze kterých budeme při našem výkladu vycházet, stručně zopakujeme.

Věta 1. *Budiž dáno libovolné celé (kladné, nula nebo záporné) číslo a a přirozené číslo m. Potom lze najít právě jednu dvojici celých čísel x a r tak, že platí vztahy*

$$a = mx + r, \quad 0 \leqq r < m. \tag{1}$$

Celé číslo x ve větě 1 může být opět buďto přirozené, nebo nula, nebo celé záporné.

Definice 1. *Číslo x z věty 1 nazýváme částečným podílem a číslo r nejmenším nezáporným zbytkem čísla a při dělení číslem m.*

Důkaz věty 1 zde nebudeme provádět. Čtenář by jej našel v knize [6], kde je podrobně proveden.

Definice 2. *Říkáme, že celé číslo a je dělitelné přirozeným číslem m, existuje-li celé číslo x tak, že*

$$a = mx. \tag{2}$$

Symbolicky pak píšeme $m|a$.

Číslo m nazýváme dělitelem čísla a a číslo a násobkem čísla m. Celé číslo x pak nazýváme podílem čísla a při dělení číslem m.

Není-li $m|a$, píšeme $m \nmid a$.

Z rovností (1) a (2) vidíme, že vztahy $m|a$ a $r = 0$ znamenají totéž.

Věta 2. *Číslo nula je dělitelné každým přirozeným číslem.*

To plyne ze vztahu $0 = 0.m$, který platí pro libovolné přirozené číslo m, a z definice 2.

Věta 3. *Nechť pro celá čísla a a b platí současně $m|a$ a $m|b$. Potom pro libovolnou dvojici celých čísel x a y platí též $m|(ax + by)$.*

Důkaz této věty najde čtenář v knize [4] na str. 27 (věta T_9).

Nechť $m|a$. Položíme-li ve větě 3 $x = -1$ a $y = 0$, dostaneme, že také $m|(-a)$. Jestliže obráceně $m|(-a)$, dostaneme stejným způsobem, že $m|(-a).(-1)$, tj. $m|a$. Tím jsme dokázali

větu 4. *Platí-li jeden ze vztahů $m|a$ a $m|(-a)$, platí i druhý z nich.*

Příklad 1. Určete částečný podíl a nejmenší nezáporný zbytek, je-li dáno

a) $a = \quad 617, \quad m = 31;$

b) $a = -617, \quad m = 31.$

Řešení.

a) Neúplným dělením, které známe ze školy, dostaneme

$$617 : 31 = 19$$
$$307$$
$$28$$

Bude tedy $x = 19$ a $r = 28$. Snadno se přesvědčíme, že skutečně platí $617 = 31.19 + 28$.

b) Provedeme opět neúplné dělení, avšak tentokrát budeme dělit číslo $-a = 617$ číslem $m = 31$. Podle příkladu 1a) máme $617 = 31.19 + 28$. Násobíme-li tuto rovnost číslem -1, dostaneme

$$-617 = 31.(-19) - 28.$$

Zbytek, který jsme dostali, je však záporný, zatímco podle věty 1 máme najít zbytek nezáporný. Proto užijeme následující úpravy:

$$-617 = 31.(-19) - 28 = 31.(-19) - 31 + 31 -$$
$$- 28 = 31.(-19 - 1) + (31 - 28) =$$
$$= 31.(-20) + 3.$$

Bude tedy $x = -20$, $r = 3$. Skutečně pak máme ve shodě s větou 1

$$-617 = 31.(-20) + 3, \quad 0 < 3 < 31.$$

Věta 5. *Budiž dáno libovolné celé číslo a a přirozené číslo m. Potom lze najít právě jednu dvojici celých čísel ξ a ϱ tak, že platí vztahy*

$$a = m\xi + \varrho, \quad -\frac{m}{2} \leqq \varrho < \frac{m}{2}. \tag{3}$$

Definice 3. *Číslo ϱ z věty 5 nazýváme absolutně nejmenším zbytkem čísla a při dělení číslem m.*

V důkazu věty 5 nejprve ukážeme, že existuje nejvýše jedna dvojice celých čísel ξ a ϱ, která splňují vztahy (3). Nechť ξ_1, ϱ_1 a ξ_2, ϱ_2 jsou dvě takovéto dvojice. Bude tedy

$$a = m\xi_1 + \varrho_1, \quad -\frac{m}{2} \leqq \varrho_1 < \frac{m}{2},$$

$$a = m\xi_2 + \varrho_2, \quad -\frac{m}{2} \leqq \varrho_2 < \frac{m}{2}.$$

Odtud dostaneme

$$m\xi_1 + \varrho_1 = m\xi_2 + \varrho_2,$$

$$-\frac{m}{2} < -\varrho_1 \leqq \frac{m}{2},$$

$$-\frac{m}{2} \leqq \varrho_2 < \frac{m}{2}.$$

Po sečtení posledních nerovností můžeme uvedené vztahy přepsat takto:

$$m(\xi_1 - \xi_2) = \varrho_2 - \varrho_1, \quad -m < \varrho_2 - \varrho_1 < m.$$

Musí tedy současně platit

$$m|\xi_1 - \xi_2| = |\varrho_2 - \varrho_1|, \tag{4}$$

$$|\varrho_2 - \varrho_1| < m. \tag{5}$$

Předpokládejme, že $\xi_1 \neq \xi_2$. Poněvadž ξ_1 a ξ_2 jsou celá čísla, bude $|\xi_1 - \xi_2| \geqq 1$, takže z rovnosti (4) plyne

$|\varrho_2 - \varrho_1| \geqq m$, což odporuje podmínce (5). Proto tedy musí být $\xi_1 = \xi_2$. Ze vztahu (4) pak dostaneme, že i $\varrho_1 = \varrho_2$, tj. dvojice ξ_1, ϱ_1 a ξ_2, ϱ_2 jsou totožné.

Nyní dvojici celých čísel ξ a ϱ s vlastnostmi (3) sestrojíme. Podle věty 1 určíme především čísla x a r tak, aby byly splněny vztahy (1). Potom položíme

$$\varrho = \begin{cases} r, \text{ jestliže } 0 \leqq r < \dfrac{m}{2}, \\ r - m, \text{ jestliže } \dfrac{m}{2} \leqq r < m. \end{cases} \tag{6}$$

V prvním případě je $0 \leqq \varrho < \frac{m}{2}$, ve druhém pak $-\frac{m}{2} \leqq \varrho < 0$. V obou případech tedy platí

$$-\frac{m}{2} \leqq \varrho < \frac{m}{2},$$

takže je splněn druhý ze vztahů (3). Položíme-li ještě

$$\xi = \begin{cases} x, \text{ jestliže } 0 \leqq r < \dfrac{m}{2}, \\ x + 1, \text{ jestliže } \dfrac{m}{2} \leqq r < m, \end{cases}$$

dostaneme v prvním případě

$$m\xi + \varrho = mx + r = a.$$

a ve druhém případě

$$m\xi + \varrho = m(x + 1) + r - m = mx + r = a.$$

Bude tedy vždy platit i první ze vztahů (3), čímž je věta 5 úplně dokázaná.

Příklad 2. Určete číslo ξ a absolutně nejmenší zbytek, je-li dáno

a) $a = 617, \quad m = 31;$

b) $a = -617, \quad m = 31.$

Řešení.

a) V příkladu 1a) jsme vypočetli $r = 28$. Poněvadž $\frac{31}{2} < 28 < 31$, bude podle (6) $\varrho = 28 - 31 = -3$. Pro číslo ξ dostaneme v tomto případě $\xi = x + 1 = 20$. Bude tedy $617 = 31.20 - 3$.

b) Z příkladu 1b) víme, že $r = 3$. Podle (6) tedy bude $\varrho = r = 3$; pro číslo ξ dostaneme v tomto případě $\xi = x = -20$. Výsledek bude totožný s výsledkem příkladu 1b).

Z dalších pojmů nauky o dělitelnosti celých čísel budeme často užívat pojmů prvočíslo, složené číslo, největší společný dělitel a nejmenší společný násobek celých čísel $a_1, a_2, \ldots, a_k$. Tyto pojmy jsou čtenáři vesměs dobře známé ze školy. Může si je však systematicky prostudovat a zopakovat např. v knize [4]. Mimoto najde v knize [3] řadu poutavých příkladů vztahujících se k těmto pojmům.

Nyní ještě pár slov k označování. Pokud neučiníme výslovně výjimku, budeme vždy písmenem m označovat přirozené číslo, písmenem p prvočíslo, symbolem $d = (a_1, a_2, \ldots, a_k)$ největší společný dělitel celých čísel $a_1, a_2, \ldots, a_k$ a symbolem $n = [a_1, a_2, \ldots, a_k]$ nejmenší společný násobek celých čísel $a_1, a_2, \ldots, a_k$ (viz [4]). Největší společný dělitel i nejmenší společný násobek budou pro nás znamenat vždycky přirozená čísla.

Celá čísla a a b, pro která platí $(a, b) = 1$, nazýváme nesoudělná.

Závěrem si uvedeme bez důkazu ještě jednu větu, které budeme často užívat.

Věta 6. *Je-li* $(a, m) = 1$ *a* $m|ab$, *je* $m|b$.

Důkaz této věty najde čtenář opět v knize [4] (věta T_{42} na str. 89).

Úlohy

1. Určete částečný podíl, nejmenší nezáporný zbytek, absolutně nejmenší zbytek a číslo ξ, je-li dáno:

   a) $a = -329$, $m = 65$;

   b) $a = 1084$, $m = 49$;

   c) $a = 12$, $m = 35$;

   d) $a = -12$, $m = 35$.

2*. Je-li celé číslo $a \neq 0$ dělitelné přirozeným číslem m, je $m \leqq |a|$. Dokažte!

3*. Nechť $d = (a_1, a_2, \ldots, a_k)$ je největší společný dělitel čísel $a_1, a_2, \ldots, a_k$. Dokažte, že platí nerovnosti $d \leqq |a_1|$, $d \leqq |a_2|$, $\ldots$, $d \leqq |a_k|$.

2. kapitola

KONGRUENCE A JEJICH ZÁKLADNÍ VLASTNOSTI

K základním pojmům v matematice patří pojem rovnosti dvou čísel nebo jiných veličin. S tímto pojmem dovedeme dobře pracovat a známe dokonce vlastnosti, které jej charakterizují.

Máme-li čísla a, b a c, vždycky platí:

1. $a = a$ (tzv. reflexivnost).
2. Je-li $a = b$, je i $b = a$ (tzv. symetrie).
3. Je-li $a = b$ a $b = c$, je i $a = c$ (tzv. tranzitivnost).

Dále víme, že pro libovolné číslo c platí: Je-li $a = b$, je i

$$a + c = b + c,$$
$$a - c = b - c,$$
$$a.c = b.c$$

(O dělení zde zatím záměrně nemluvíme.)

Z uvedených vlastností pak plyne, že rovnosti můžeme známým způsobem sčítat, odčítat nebo násobit apod. Na tom je např. založena celá teorie algebraických rovnic nebo teorie soustav rovnic, kdy určujeme neznámé veličiny vyhovující určitým podmínkám právě pomocí rovností.

Při studiu některých otázek z nauky o dělitelnosti celých čísel můžeme řadu z nich velmi pohodlně formu-

lovat pomocí tzv. kongruencí. Důvodem k zavedení pojmu kongruence je skutečnost, že kongruence a rovnosti mají, jak dále uvidíme, řadu shodných vlastností. Můžeme proto očekávat, že práce s kongruencemi bude formálně stejná nebo velmi podobná práci s rovnostmi.

Definice 4. *Nechť m je dané přirozené číslo a a a b celá čísla. Jestliže $m \mid (a - b)$, říkáme, že a je kongruentní s b podle modulu m (nebo též a je kongruentní s b modulo m) a píšeme symbolicky*

$$a \equiv b \bmod m. \tag{7}$$

Jestliže $m \nmid (a - b)$, říkáme, že a není kongruentní s b podle modulu m nebo že a není kongruentní s b modulo m nebo že a je inkongruentní s b modulo m. Píšeme pak

$$a \not\equiv b \bmod m. \tag{8}$$

Vztah (7) *se nazývá kongruence. Číslo a budeme nazývat levou stranou a číslo b pravou stranou kongruence* (7).

Příklad 3. $916 \equiv 76 \bmod 42$, neboť $916 - 76 = 840$ a $42 \mid 840$.

Příklad 4. $-326 \equiv 22 \bmod 29$, neboť $-326 - 22 = -348$ a $29 \mid (-348)$.

Příklad 5. $615 \not\equiv -86 \bmod 14$, neboť $615 - (-86) = 615 + 86 = 701$ a $14 \nmid 701$.

Nyní si uvedeme některé základní vlastnosti kongruencí.

Věta 7. *Buďte a, b a c celá čísla. Potom pro každé přirozené číslo m platí:*

1. $a \equiv a \bmod m.$ (9)

2. *Je-li* $a \equiv b \bmod m$, *je i* $b \equiv a \bmod m$. (10)

3. *Je-li* $a \equiv b \bmod m$ *a* $b \equiv c \bmod m$, *je i* $a \equiv c \bmod m$. (11)

Důkaz.

1. Poněvadž $a - a = 0$ a poněvadž podle věty 2 je pro každé přirozené číslo $m|0$, bude podle definice 4 skutečně $a \equiv a \bmod m$.

2. Vztah $a \equiv b \bmod m$ znamená podle definice 4 totéž, co $m|(a - b)$. Podle věty 4 je však též $m|(b - a)$, což znamená, že $b \equiv a \bmod m$.

3. Vztahy $a \equiv b \bmod m$ a $b \equiv c \bmod m$ znamenají podle definice 4 totéž, co $m|(a - b)$ a $m|(b - c)$. Podle věty 3 bude pro libovolná celá čísla x a y platit $m|((a - b)x + (b - c)y)$. Zvolíme-li $x = y = 1$, dostaneme ihned, že $m|(a - c)$, tj. $a \equiv c \bmod m$.

Věta 7 říká, že kongruence podle libovolného přirozeného modulu m je, podobně jako rovnost, vztah reflexivní, symetrický a tranzitivní.

Věta 8. *Buďte* a, b *a* c *celá čísla a* m *přirozené číslo. Potom platí*: *Je-li* $a \equiv b \bmod m$, *je též*

$$a + c \equiv b + c \bmod m, \tag{12}$$

$$a - c \equiv b - c \bmod m, \tag{13}$$

$$ac \equiv bc \bmod m. \tag{14}$$

Důkaz. Podle definice 4 plyne z předpokladu $a \equiv b \bmod m$, že $m|(a - b)$. Poněvadž však $a - b = (a + c) - (b + c) = (a - c) - (b - c)$, je též $m|((a + c) - (b + c))$ a $m|((a - c) - (b - c))$, což podle definice 4 znamená, že platí (12) a (13).

Poněvadž $m|(a - b)$ a c je celé číslo, platí tím spíše $m|(a - b)c$ neboli $m|(ac - bc)$, z čehož plyne (14).

Věta 9. *Buďte a, b, c, d celá čísla a m přirozené číslo. Nechť platí*

$$a \equiv b \bmod m, \quad c \equiv d \bmod m.$$

Potom je též

$$a + c \equiv b + d \bmod m, \tag{15}$$

$$a - c \equiv b - d \bmod m, \tag{16}$$

$$ac \equiv bd \bmod m. \tag{17}$$

Důkaz. Z kongruence $a \equiv b \bmod m$ plyne podle (12) resp. (13) resp. (14), že

$$a + c \equiv b + c \bmod m, \quad a - c \equiv b - c \bmod m,$$

$$ac \equiv bc \bmod m.$$

Podobně z kongruence $c \equiv d \bmod m$ dostaneme, že

$$b + c \equiv b + d \bmod m, \quad c - b \equiv d - b \bmod m,$$

$$bc \equiv bd \bmod m.$$

Z kongruence $c - b \equiv d - b \bmod m$ však podle (14) plyne, že i $b - c \equiv b - d \bmod m$ (násobení kongruence číslem -1). Podle (11) pak plyne z kongruencí $a + c \equiv b + c \bmod m$ a $b + c \equiv b + d \bmod m$ vztah (15), z kongruencí $a - c \equiv b - c \bmod m$ a $b - c \equiv b - d \bmod m$ vztah (16) a konečně z kongruencí $ac \equiv bc \bmod m$ a $bc \equiv bd \bmod m$ vztah(17).

Věta 10. *Je-li $a \equiv b \bmod m$, platí pro každé přirozené číslo k*

$$a^k \equiv b^k \bmod m. \tag{18}$$

Důkaz této věty provedeme matematickou indukcí. Pro $k = 1$ je vztah (18) zřejmě správný, neboť $a^1 = a$ a $b^1 = b$, takže předpoklad věty můžeme psát ve tvaru $a^1 \equiv b^1 \bmod m$.

Předpokládejme, že vztah (18) platí pro jisté přirozené číslo k, tj. že $a^k \equiv b^k \bmod m$. Položíme-li ve větě 9 $c = a^k$, $d = b^k$, dostaneme podle (17)

$$a.a^k \equiv b.b^k \bmod m$$

neboli

$$a^{k+1} \equiv b^{k+1} \bmod m.$$

Tím jsme dokázali, že platí-li vztah (18) pro přirozené číslo k, platí i pro přirozené číslo $k + 1$.

Poslední tvrzení spolu s tím, že (18) platí pro $k = 1$, dokazuje platnost vztahu (18) pro všechna přirozená čísla k. (Čtenář, který by se chtěl s metodou matematické indukce podrobněji seznámit, si může prostudovat knížku R. Výborného *Matematická indukce*, která vyšla jako 6. svazek *Školy mladých matematiků*.)

Věty 9 a 10 ukazují, že při pevně zvoleném modulu m můžeme z daných kongruencí získávat další kongruence sčítáním, odčítáním, násobením a umocňováním kongruencí původních. Podobně jako je tomu u rovností, dospějeme k novým kongruencím tak, že sčítáme resp. odčítáme nebo násobíme levé strany i pravé strany daných kongruencí, resp. že obě strany dané kongruence umocníme týmž přirozeným exponentem.

Nyní si na několika příkladech ukážeme, jak lze kongruencí s výhodou využít při studiu některých otázek o dělitelnosti celých čísel.

Příklad 6. Vyšetřte, je-li číslo $12^{136} + 47^2$ dělitelné číslem 65.

Řešení. Snadno zjistíme, že $12^2 = 144$ a $144 \equiv 14 \bmod 65$. Podle (18) tedy bude $(12^2)^2 \equiv 14^2 \bmod 65$, tj. $12^4 \equiv 196 \bmod 65$. Avšak $196 \equiv 1 \bmod 65$, takže podle

(11) máme $12^4 \equiv 1 \bmod 65$. Poněvadž $12^{136} = (12^4)^{34}$, bude opět podle (18) $12^{136} \equiv 1^{34} \bmod 65$, tj. $12^{136} \equiv 1 \bmod 65$.

Dále máme $47 \equiv -18 \bmod 65$, takže podle (18) platí $47^2 \equiv (-18)^2 \bmod 65$. Avšak $(-18)^2 = 324$ a $324 \equiv -1 \bmod 65$. Užijeme-li opět vztahu (11), dostaneme $47^2 \equiv -1 \bmod 65$.

Shrneme-li dílčí výsledky, dostaneme konečně užitím vztahu (15)

$$12^{136} + 47^2 \equiv 1 - 1 \bmod 65,$$

tj.

$$12^{136} + 47^2 \equiv 0 \bmod 65.$$

Odpověď: Číslo $12^{136} + 47^2$ je dělitelné číslem 65.

Všimněme si nyní dekadického zápisu přirozeného čísla n. Např. číslo 2873 můžeme psát ve tvaru $2873 = 2.1000 + 8.100 + 7.10 + 3 = 2.10^3 + 8.10^2 + 7.10 + 3$.

Obecně, jsou-li $a_0, a_1, a_2, \ldots$ číslice (tj. znaky 0, 1, 2, 3, ..., 9), víme, že dekadický zápis $a_\nu a_{\nu-1} \ldots a_2 a_1 a_0$ přirozeného čísla n znamená součet

$$n = a_\nu . 10^\nu + a_{\nu-1} . 10^{\nu-1} + \ldots + a_2 . 10^2 + a_1 . 10 + a_0. \tag{19}$$

Pro stručnost si zavedeme ještě tři další pojmy.

Definice 5. *Je-li přirozené číslo n dáno dekadickým zápisem (19), nazýváme číslo*

$$s(n) = a_0 + a_1 + a_2 + \ldots + a_{\nu-1} + a_\nu \tag{20}$$

ciferným součtem přirozeného čísla n, číslo

$$s_0(n) = a_0 + a_2 + a_4 + \ldots \tag{21}$$

součtem číslic sudých řádů a konečně číslo

$$s_1(n) = a_1 + a_3 + a_5 + \dots \qquad (22)$$

součtem číslic lichých řádů přirozeného čísla n.

Příklad 7. Dokažte, že přirozené číslo n je dělitelné třemi (devíti) právě tehdy, je-li jeho ciferný součet dělitelný třemi (devíti).

Řešení. Poněvadž $10 \equiv 1 \bmod 3$, bude podle (18) pro každé přirozené číslo k platit $10^k \equiv 1 \bmod 3$. Podle (14) tedy bude $a_k . 10^k \equiv a_k \bmod 3$, takže můžeme psát

$$\begin{aligned} a_0 &\equiv a_0 \bmod 3, \\ a_1 . 10 &\equiv a_1 \bmod 3, \\ a_2 . 10^2 &\equiv a_2 \bmod 3, \\ &\vdots \\ a_r . 10^r &\equiv a_r \bmod 3. \end{aligned}$$

Sečtením všech těchto kongruencí dostaneme

$a_r . 10^r + a_{r-1} . 10^{r-1} + \dots + a_2 . 10^2 + a_1 . 10 + a_0 \equiv$
$\equiv a_r + a_{r-1} + \dots + a_2 + a_1 + a_0 \bmod 3$, takže podle (19) a (20) bude

$$n \equiv s(n) \bmod 3.$$

Z tohoto vztahu plyne, že $n \equiv 0 \bmod 3$ právě tehdy, když $s(n) \equiv 0 \bmod 3$, tj. podle definice 4 $3 | n$ právě tehdy, když $3 | s(n)$.

Pro dělitelnost devíti bude celý postup stejný, avšak místo mod 3 budeme všude psát mod 9 a všechno ostatní ponecháme beze změny.

Příklad 8. Dokažte, že přirozené číslo n je dělitelné jedenácti právě tehdy, je-li součet jeho číslic lichých řádů buďto roven součtu jeho číslic sudých řádů, nebo se od něho liší o celý násobek jedenácti.

Řešení. Poněvadž je $10 \equiv -1 \bmod 11$, bude opět podle (18) pro každé přirozené k platit $10^k \equiv (-1)^k \bmod 11$, takže pro sudá k bude $10^k \equiv 1 \bmod 11$ a pro lichá k podobně $10^k \equiv -1 \bmod 11$. Užitím (14) dostaneme postupně

$$\begin{aligned} a_0 &\equiv a_0 \bmod 11, \\ a_1 . 10 &\equiv -a_1 \bmod 11, \\ a_2 . 10^2 &\equiv a_2 \bmod 11, \\ a_3 . 10^3 &\equiv -a_3 \bmod 11, \\ &\vdots \end{aligned}$$

Sečteme-li tyto kongruence, dostaneme

$a_0 + a_1 . 10 + a_2 . 10^2 + a_3 . 10^3 + \ldots \equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \bmod 11$, z čehož po dosazení podle (20), (21) a (22) plyne

$$n \equiv s_0(n) - s_1(n) \bmod 11.$$

Odtud vidíme, že $n \equiv 0 \bmod 11$ právě tehdy, když $s_0(n) - s_1(n) \equiv 0 \bmod 11$, tj. $11 | n$ právě tehdy, když $11 | (s_0(n) - s_1(n))$.

Kongruencí lze s výhodou užít též pro kontrolu správnosti některých numerických výpočtů. Tato kontrola je založena na tzv. trojkové resp. devítkové resp. jedenáctkové zkoušce, jejichž princip tkví ve využití dělitelnosti třemi resp. devíti resp. jedenácti a vlastností kongruencí, které jsme dokázali v této kapitole. S těmito zkouškami se čtenář může podrobněji seznámit v příručce [4], str. 57—60 (zejména příklad 22 a cvičení 4, 5).

Věty 7 až 10 ukazují, že řada vlastností kongruencí je shodná s analogickými vlastnostmi rovností. Dokonce i postup, kterým jednotlivé vlastnosti dokazujeme, je u kongruencí stejný jako byl u rovností.

Čtenáře však mohlo při studiu věty 8 překvapit, že jsme tam vůbec neuvažovali o analogii pravidla, že rovnost zůstane správná, dělíme-li obě její strany týmž číslem, které není rovno nule. V prvním okamžiku se nabízí vysvětlení, že u kongruencí pracujeme pouze s celými čísly, takže pokud by obě strany kongruence nebyly dělitelné týmž přirozeným číslem c, nemělo by vůbec smysl kongruenci tímto číslem dělit. Ukážeme si však na příkladech, že toto vysvětlení není uspokojující.

Příklad 9. Zjistěte, zda lze kongruenci

a) $645 \equiv 15 \bmod 42$

b) $225 \equiv 15 \bmod 42$

krátit číslem 15.

Řešení. Snadno se přesvědčíme, že kongruence a) i b) jsou správné. Obě strany každé z nich jsou dělitelny patnácti, přičemž $\frac{645}{15} = 43$, $\frac{225}{15} = 15$ a $\frac{15}{15} = 1$. Po krácení patnácti dostaneme tedy v případě a) $43 \equiv 1 \bmod 42$, avšak v případě b) $15 \not\equiv 1 \bmod 42$.

Odpověď. Chceme-li dostat platnou kongruenci, můžeme krátit patnácti kongruenci a), nikoliv však kongruenci b).

Přesto dovedeme alespoň v některých případech udat jednoduché podmínky, za kterých lze provést krácení kongruence tak, aby vzniklá kongruence byla správná.

Věta 11. *Buďte a, b, c celá čísla a nechť $(c, m) = 1$. Nechť konečně $ac \not\equiv bc \bmod m$. Potom je též $a \equiv b \bmod m$.*

Důkaz. Poněvadž $ac \equiv bc \bmod m$, platí $m \mid (ac - bc)$, tj. $m \mid (a - b)c$. Poněvadž $(c, m) = 1$, bude podle věty 6 $m \mid (a - b)$, tedy $a \equiv b \bmod m$, což jsme chtěli dokázat.

Věta 11 o krácení kongruence udává pouze postačující, nikoli však nutnou podmínku pro to, aby bylo možno kongruenci $ac \equiv bc \bmod m$ krátit číslem c. V obou příkladech 9 bylo totiž $m = 42$, $c = 15$, takže $(c, m) = (15, 42) = 3 > 1$. Nebyl zde splněn předpoklad o nesoudělnosti čísel c a m, avšak přesto bylo možno kongruenci v případě a) krátit patnácti. Případ b) pak ukázal, že pro $(c, m) > 1$ nelze obecně kongruenci krátit.

Avšak i pro případy, kdy $(c, m) > 1$, lze odvodit pravidla, kdy lze kongruenci $ac \equiv bc \bmod m$ krátit číslem c. Tato pravidla jsou však už značně složitější; studiem podobných otázek se obšírně zabývá teorie čísel.

Závěrem této kapitoly si uvedeme ještě jednu vlastnost rovností, která nemá u kongruencí s obecně daným modulem vždy obdobu. Bude se v podstatě opět týkat dělení. Jde o větu, že součin dvou čísel je roven nule právě tehdy, je-li alespoň jedno z těchto čísel rovno nule.

Věta 12. *Je-li $m > 1$ složené číslo, existuje alespoň jedna dvojice přirozených čísel m_1 a m_2 takových, že $m_1 \not\equiv 0 \bmod m$, $m_2 \not\equiv 0 \bmod m$, avšak $m_1 m_2 \equiv 0 \bmod m$.*

Důkaz. Poněvadž $m > 1$ je složené číslo, můžeme najít alespoň jednu dvojici přirozených čísel $m_1 > 1$ a $m_2 > 1$ tak, že $m = m_1 m_2$. Potom však $m_1 = \frac{m}{m_2} < m$, $m_2 = \frac{m}{m_1} < m$; z úlohy 2* plyne, že $m \nmid m_1$, $m \nmid m_2$, tj. že $m_1 \not\equiv 0 \bmod m$ a $m_2 \not\equiv 0 \bmod m$. Poněvadž $m \equiv 0 \bmod m$ a $m = m_1 m_2$, bude i $m_1 m_2 \equiv 0 \bmod m$, což jsme měli dokázat.

Věta 12 tedy tvrdí, že při složeném modulu m neplyne

z kongruence $m_1 m_2 \equiv 0 \bmod m$, že platí alespoň jedna z kongruencí $m_1 \equiv 0 \bmod m$ a $m_2 \equiv 0 \bmod m$.

Příklad 10. $999 \equiv 0 \bmod 111$ a $999 = 27.37$. Přitom zřejmě $27 \not\equiv 0 \bmod 111$ i $37 \not\equiv 0 \bmod 111$.

Zcela jiná situace však nastává v případech, kdy modul m je prvočíslem.

Věta 13. *Budiž p prvočíslo. Potom $ab \equiv 0 \bmod p$ právě tehdy, je-li buďto $a \equiv 0 \bmod p$, nebo $b \equiv 0 \bmod p$.*

Důkaz. Vztah $ab \equiv 0 \bmod p$ platí právě tehdy, když $p|ab$, což je možné právě tehdy, když $p|a$ nebo $p|b$ (viz [4], str. 89, Důsledek II), tj. když buďto $a \equiv 0 \bmod p$, nebo $b \equiv 0 \bmod p$.

Porovnáním vět 12 a 13 zjistíme, že studovaná vlastnost je charakteristickou vlastností pro kongruence s prvočíselnými moduly. Proto také v dalších kapitolách budeme často věnovat pozornost kongruencím s prvočíselným modulem.

Výsledků vět 12 a 13 využívá moderní algebra v teorii tzv. dělitelů nuly, konečných grup, konstrukcí algebraických těles apod. O těchto otázkách se čtenář může podrobněji poučit např. v učebnici [6].

Úlohy

4. Pomocí kongruencí dokažte, že číslo $5.215^{20} - 79^{21}$ je dělitelné číslem 21.

5. Užitím kongruencí určete nejmenší nezáporný zbytek
   a) čísla $1428^{29} - 312^{15}.627^{11}$ při dělení číslem 77;
   b) čísla $(3466^4 + 219^{11})^{25}$ při dělení číslem 111.

6. Užitím kongruencí zdůvodněte znaky dělitelnosti přirozeného čísla dvěma, čtyřmi, pěti, osmi, deseti a dvacetipěti.

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.

4. kapitola

KONGRUENCE O JEDNÉ NEZNÁMÉ. LINEÁRNÍ KONGRUENCE

Ve druhé kapitole jsme si ukázali, že kongruence a rovnosti mají řadu společných vlastností.

S pojmem rovnosti velmi těsně souvisí pojem rovnice. Budiž n přirozené číslo a nechť $a_0, a_1, a_2, \ldots, a_n$ jsou daná reálná čísla, přičemž $a_0 \neq 0$. Sestrojme polynom n-tého stupně $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ a položme si úlohu najít všechna čísla α (obecně komplexní), pro která platí rovnost

$$P(\alpha) = 0 .$$

Najdeme-li všechna čísla α s touto vlastností, říkáme, že jsme vyřešili algebraickou rovnici n-tého stupně o jedné neznámé $P(x) = 0$. Každé číslo α, pro které platí rovnost $P(\alpha) = 0$, nazýváme pak řešením rovnice $P(x) = 0$.

Rozdíl mezi pojmem **rovnost** a **rovnice** je tedy ten, že rovnost je jistá relace (v našem případě mezi čísly), kdežto rovnicí rozumíme úlohu, kterou jsme právě popsali.

Je-li $n = 1$, nazýváme algebraickou rovnici lineární rovnicí o jedné neznámé, pro $n = 2$ hovoříme o kvadratické rovnici o jedné neznámé, pro $n = 3$ o kubické rovnici o jedné neznámé atd. Ze školy dovedeme řešit lineární a kvadratické rovnice o jedné neznámé a některé speciální typy rovnic vyšších stupňů.

Obdobná situace je i u kongruencí. Nechť m a n jsou přirozená čísla a $a_0, a_1, a_2, \ldots, a_n$ daná celá čísla, přičemž $a_0 \not\equiv 0 \bmod m$. Nechť ještě $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ je polynom n-tého stupně (s celočíselnými koeficienty). Hledejme všechna celá čísla ξ, pro která platí

$$P(\xi) \equiv 0 \bmod m. \tag{41}$$

Najdeme-li všechna celá čísla ξ s touto vlastností, říkáme, že jsme vyřešili kongruenci n-tého stupně o jedné neznámé

$$P(x) \equiv 0 \bmod m. \tag{42}$$

Každé celé číslo ξ, pro které platí vztah (41), nazýváme pak řešením kongruence (42).

Slovo **kongruence** zde vystupuje zřejmě ve dvou významech, předně jako relace mezi dvěma celými čísly, dále pak (ve spojení se rčením „o jedné neznámé") jako právě popsaná úloha. Tento dvojí význam slova **kongruence** však nezpůsobí nedorozumění, neboť z kontextu bude vždy zřejmé, o který z těchto významů jde.

Vraťme se ještě k řešení kongruence o jedné neznámé (42). Známe-li řešení ξ této kongruence, můžeme psát vztah (41) ve tvaru

$$a_0\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n \equiv 0 \bmod m.$$

Podle věty 17 můžeme však číslo ξ nahradit kterýmkoliv číslem, které je s číslem ξ ekvivalentní podle modulu m. Řešeními kongruence (42) budou tedy všechna čísla z jisté zbytkové třídy podle modulu m. Z tohoto důvodu se při hledání řešení kterékoliv kongruence o jedné neznámé můžeme omezit na řešení z libovolně zvolené úplné soustavy zbytků podle modulu m. Pokud takto dostaneme více řešení kongruence (42),

budou zřejmě tato řešení vzájemně inkongruentní podle modulu m. My budeme zpravidla za úplnou soustavu zbytků, ve které budeme hledat řešení, volit soustavu $\{0, 1, 2, \ldots, m - 1\}$.

Podobně jako u rovnic hovoříme i u kongruencí o stupni kongruence o jedné neznámé. Pro $n = 1$ nazýváme kongruenci lineární, pro $n = 2$ kvadratickou, pro $n = 3$ kubickou atd.

V další části této kapitoly a v kapitolách 5 a 6 se budeme zabývat lineárními kongruencemi o jedné případně o více neznámých, jejich soustavami a jejich užitím při řešení tzv. neurčitých rovnic.

Věta 30. *Buďte a a b celá čísla a m přirozené číslo. Nechť dále $(a, m) = 1$. Potom lineární kongruence o jedné neznámé*

$$ax + b \equiv 0 \bmod m \tag{43}$$

má v každé úplné soustavě zbytků podle modulu m právě jedno řešení.

Důkaz. Probíhá-li číslo x libovolně zvolenou úplnou soustavou zbytků podle modulu m, probíhá podle věty 26 výraz $ax + b$ rovněž úplnou soustavou zbytků podle tohoto modulu, takže existuje právě jedno celé číslo ξ z dané úplné soustavy zbytků, pro které bude $a\xi + b$ ze zbytkové třídy $A_0^{(m)}$. Bude proto $a\xi + b \equiv 0 \bmod m$, což jsme chtěli dokázat.

Věta 30 nám za předpokladu $(a, m) = 1$ zodpovídá otázku existence řešení kongruence (43) i otázku počtu řešení této kongruence, avšak nepodává návod, jak toto řešení najdeme.

Nyní si vyřešíme příklad, jehož výsledků užijeme k řešení několika kongruencí v příkladech dalších.

Příklad 18. Nechť x probíhá čísly 0, 1, 2, ..., 13, 14. Určete zbytkové třídy podle modulu 15, ve kterých leží čísla tvaru

a) $4x - 11$;
b) $6x + 9$;
c) $6x + 5$.

Řešení. Ke každému z čísel x budeme hledat číslo k vyhovující nerovnostem $0 \leqq k \leqq 14$ tak, aby platilo

a) $4x - 11 \equiv k \bmod 15$ resp.
b) $6x + 9 \equiv k \bmod 15$ resp.
c) $6x + 5 \equiv k \bmod 15$.

Výsledky máme uspořádány do tabulky 1. Vidíme, že v případě a) nabývá číslo k každé z hodnot 0, 1, 2, ..., 13, 14 právě jednou, takže výraz $4x - 11$ skutečně probíhá úplnou soustavou zbytků podle modulu 15.

Naproti tomu v případě b) nabývá k pouze hodnot 9, 0, 6, 12 a 3, přičemž každé z těchto hodnot nabývá pro tři různé hodnoty x z dané úplné soustavy zbytků podle modulu 15. Podobně v případě c) nabývá k pouze hodnot 5, 11, 2, 8 a 14 a to opět každé z nich pro tři různé hodnoty x z dané úplné soustavy zbytků.

Příklad 19. Řešte lineární kongruenci o jedné neznámé $4x - 11 \equiv 0 \bmod 15$.

Řešení. Poněvadž je $(4, 15) = 1$, existuje podle věty 30 v úplné soustavě zbytků 0, 1, 2, ..., 14 podle modulu 15 právě jedno řešení dané kongruence. Z tabulky 1 okamžitě vidíme, že $\xi = 14$. O správnosti výsledku se přesvědčíme zkouškou: $4\xi - 11 = 45$ a skutečně $45 \equiv 0 \bmod 15$.

Komplikovanější situace při řešení lineární kongruen-

Tabulka 1.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$4x - 11$	−11	−7	−3	1	5	9	13	17	21	25	29	33	37	41	45
k	4	8	12	1	5	9	13	2	6	10	14	3	7	11	0
$6x + 9$	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93
k	9	0	6	12	3	9	0	6	12	3	9	0	6	12	3
$6x + 5$	5	11	17	23	29	35	41	47	53	59	65	71	77	83	89
k	5	11	2	8	14	5	11	2	8	14	5	11	2	8	14

ce (43) nastane v případě, kdy čísla a a m nejsou nesoudělná. V tomto případě nelze použít věty 30. Aniž bychom prováděli podrobný obecný rozbor, ukážeme na dvou příkladech, jaké možnosti mohou nastat (viz úlohu 14 a knihu [7]).

Příklad 20. Řešte lineární kongruenci $6x + 9 \equiv 0 \mod 15$.

Řešení. Užijeme-li výsledku příkladu 18b), vidíme z tabulky 1, že výraz $6x + 9$ patří do zbytkové třídy $A_0^{(15)}$ pouze pro $x = 1$ nebo 6 nebo 11. Daná kongruence má tedy v úplné soustavě zbytků 0, 1, 2, ..., 14 podle modulu 15 právě tři řešení $\xi_1 = 1$, $\xi_2 = 6$ a $\xi_3 = 11$, které jsou vzájemně inkongruentní podle modulu 15. Snadno nahlédneme, že v libovolné úplné soustavě zbytků podle modulu 15 má kongruence $6x + 9 \equiv 0 \mod 15$ tři vzájemně inkongruentní řešení. Tato řešení jsou ze zbytkových tříd $A_1^{(15)}$, $A_6^{(15)}$ a $A_{11}^{(15)}$ podle modulu 15.

Příklad 21. Vyšetřte lineární kongruenci $6x + 5 \equiv 0 \mod 15$.

Řešení. Z tabulky 1 opět vidíme, že probíhá-li x úplnou soustavou zbytků podle modulu 15, leží výrazy $6x + 5$ pouze ve zbytkových třídách $A_5^{(15)}$, $A_{11}^{(15)}$, $A_2^{(15)}$, $A_8^{(15)}$ a $A_{14}^{(15)}$. Žádný z výrazů $6x + 5$ tedy neleží ve zbytkové třídě $A_0^{(15)}$ podle modulu 15, takže kongruence $6x + 5 \equiv 0 \bmod 15$ nemá řešení.

Na příkladu 19 jsme viděli, že jsou-li splněny předpoklady věty 30 a máme-li k dispozici vhodnou tabulku, můžeme najít rychle řešení kongruence (43). Metoda, kterou zde používáme, je svojí podstatou metodou zkušební. Principiálně lze takto řešení dané kongruence vždy najít. Je však zřejmé, že tato metoda nebude vhodná v případech, kdy modul m bude velké číslo, neboť počet zkoušek, které musíme provést, může být rovný číslu m (tak je tomu zrovna v příkladu 19). Proto se pokusíme najít jiné cesty, kterých by bylo možno použít k rychlejšímu určení řešení i pro velké moduly.

Předpokládejme, že čísla a a m jsou nesoudělná. Podle věty 30 víme, že v každé úplné soustavě zbytků podle modulu m existuje právě jedno řešení kongruence (43). Označíme-li toto řešení písmenem ξ, bude tedy $a\xi \equiv -b \bmod m$. Násobme tuto kongruenci celým číslem u. Dostaneme tak kongruenci $(au)\xi \equiv -bu \bmod m$. Podaří-li se nám najít celé číslo u tak, aby platilo

$$au \equiv 1 \bmod m, \tag{44}$$

můžeme podle věty 17 napsat, že pro řešení ξ kongruence (43) platí

$$\xi \equiv -bu \bmod m. \tag{45}$$

Tím tedy bude ihned stanovena zbytková třída podle modulu m, ve které leží řešení ξ kongruence (43).

Úlohu řešit lineární kongruenci (43) jsme takto pře-

vedli na úlohu řešit lineární kongruenci (44), která už má speciální pravou stranu rovnu jedné. Avšak tato kongruence má řešení, které dovedeme ihned napsat, neboť podle věty 28 pro $(a, m) = 1$ platí $a^{\varphi(m)} \equiv 1 \bmod m$, takže stačí položit $u = a^{\varphi(m)-1}$. Podle (45) tedy pro řešení ξ kongruence (43) dostaneme

$$\xi \equiv -ba^{\varphi(m)-1} \bmod m. \qquad (46)$$

Číslo $-ba^{\varphi(m)-1}$ bude však zpravidla příliš velké, a proto — chceme-li si udělat lepší představu o zbytkové třídě podle modulu m, ve které řešení leží, — bude třeba podle pravidel popsaných v předcházejících kapitolách toto číslo nahradit vhodným číslem s ním ekvivalentním.

Příklad 22. Metodou, kterou jsme právě popsali, řešte znovu kongruenci $4x - 11 \equiv 0 \bmod 15$ z příkladu 19.

Řešení. Poněvadž $(4, 15) = 1$ a poněvadž $\varphi(15) = 8$, bude podle (46) pro řešení ξ kongruence $4x - 11 \equiv 0 \bmod 15$ platit $\xi \equiv 11.4^7 \bmod 15$. Avšak $11 \equiv -4 \bmod 15$, takže $11.4^7 \equiv -4^8 \bmod 15$. Podle (34) je však $4^8 \equiv 1 \bmod 15$, takže bude $\xi \equiv -4^8 \equiv -1 \equiv 14 \bmod 15$, tj. $\xi = 14$.

K výsledku můžeme dojít v tomto případě ještě rychleji řešením kongruence (44). Hledáme celé číslo u tak, aby platilo $4u \equiv 1 \bmod 15$. Ihned vidíme, že můžeme volit $u = 4$, takže podle (45) dostaneme $\xi \equiv 44 \equiv 14 \bmod 15$.

Ukázali jsme si, že za předpokladu $(a, m) = 1$ můžeme vždy dostat řešení kongruence (43) pomocí vztahu (46). Z příkladu 22 však vidíme, že může být výhodnější určit řešení u kongruence (44) jinou cestou, zejména podaří-li se nám najít toto řešení u poměrně malé. Jedna z mož-

ných cest k tomu je např. najít nejmenší přirozené číslo k, pro které platí

$$a^k \equiv 1 \bmod m.$$

Najdeme-li takové číslo k, bude zřejmě $u = a^{k-1}$ jedním z řešení kongruence (44), takže pro řešení ξ kongruence (43) v tomto případě dostaneme

$$\xi \equiv -ba^{k-1} \bmod m. \tag{47}$$

Mimoto podle věty 29 víme, že $k|\varphi(m)$.

Snadno zjistíme, že tento postup bude tím účinnější, čím bude nalezené číslo k menší. V příkladu 17 jsme však viděli, že toto nejmenší k může být rovno číslu $\varphi(m)$. Tato skutečnost značně snižuje výhody popsané metody, neboť nedovedeme předem určit, jak velké bude hledané nejmenší přirozené číslo k. Naproti tomu má však jistý význam, že číslo k nemusíme hledat mezi $\varphi(m)$ čísly 1, 2, 3, ..., $\varphi(m)$, nýbrž že se můžeme omezit na hledání k mezi děliteli čísla $\varphi(m)$, jejichž počet je podstatně menší než $\varphi(m)$. To nám může být v některých případech cenným vodítkem při výpočtech.

Příklad 23. Určete nejmenší přirozené číslo k, pro které platí $73^k \equiv 1 \bmod 615$ a na základě nalezeného výsledku řešte kongruenci $73x - 2199 \equiv 0 \bmod 615$.

Řešení. Poněvadž $615 = 3.5.41$, bude $(73, 615) = 1$ a $\varphi(615) = 2.4.40 = 320$. Číslo k tedy budeme hledat mezi čísly 1, 2, 4, 5, 8, 10, 16, 20, 32, 40, 64, 80, 160 a 320. Zřejmě bude $k > 1$. Poněvadž $73^2 = 5329$ a $5329 \equiv -206 \bmod 615$, bude $73^2 \equiv -206 \bmod 615$. Odtud pak podle (18) bude dále $73^4 \equiv (-206)^2 \bmod 615$ a poněvadž $(-206)^2 = 42436 = 69 . 615 + 1$, bude

$(-206)^2 \equiv 1 \bmod 615$. Shrnutím částečných výsledků tedy dostaneme, že platí $73^4 \equiv 1 \bmod 615$, takže $k = 4$ je hledané nejmenší přirozené číslo.

Podle (47) bude tedy řešení ξ kongruence $73x - 2199 \equiv 0 \bmod 615$ vyhovovat vztahu $\xi \equiv 2199.73^3 \equiv -261.73.73^2 \equiv -261.73.(-206) \bmod 615$. Avšak $-261.73.(-206) = 19\,053.206$ a $19\,053 \equiv -12 \bmod 615$, $-12 . 206 = -2472$ a $-2472 \equiv 603 \bmod 615$; dostaneme $19\,053.206 \equiv -12.206 \equiv 603 \bmod 615$ a tedy $\xi \equiv 603 \bmod 615$, tj. $\xi = 603$.

O správnosti výpočtu se přesvědčíme zkouškou: $73\xi - 2199 = 73.603 - 2199 = 44\,019 - 2199 = 41\,820 = 68.615$.

Kdybychom chtěli k řešení kongruence $73x - 2199 \equiv 0 \bmod 615$ užít přímo vztahu (46), dostali bychom $\xi \equiv 2199.73^{319} \bmod 615$. Je však $73^{319} = 73^3.(73^4)^{79}$ a $(73^4)^{79} \equiv 1 \bmod 615$, takže bychom opět dostali $\xi \equiv 2199.73^3 \bmod 615$.

V příkladech, s nimiž jsme se dosud setkali, jsme často byli nuceni pracovat se značně velikými čísly. Tato skutečnost pak vedla k tomu, že výpočty byly příliš zdlouhavé a mnohdy i dosti nepřehledné. Proto bychom rádi dosáhli toho, abychom mohli pracovat s čísly v absolutní hodnotě pokud možno malými. Ukážeme si postup, kterým toho lze alespoň v některých případech dosáhnout.

Řešme znovu kongruenci $73x - 2199 \equiv 0 \bmod 615$. Podle (46) bude $\xi \equiv 2199.73^{319} \bmod 615$. Podle (34) víme, že platí $73^{320} \equiv 1 \bmod 615$. Pro libovolné celé číslo η bude však též $\xi \equiv (2199 + 615\,\eta).73^{319} \bmod 615$. Vyšetřme nyní kongruenci $615y + 2199 \equiv 0 \bmod 73$. Podle věty 17 ji můžeme nahradit kongruencí $-42y + 9 \equiv 0 \bmod 73$. Tuto kongruenci můžeme podle věty

11krátit číslem 3, takže dostaneme $-14y + 3 \equiv 0 \bmod 73$. Odtud pak plyne $14y \equiv 3 \bmod 73$. Po vynásobení poslední kongruence pěti a opětném užití věty 17 dostaneme postupně

$$70y \equiv 15 \bmod 73,$$
$$-3y \equiv 15 \bmod 73,$$

odkud krácením třemi plyne $-y \equiv 5 \bmod 73$, tj. $y \equiv -5 \equiv 68 \bmod 73$. Číslo $\eta = 68$ bude tedy řešením kongruence $615y + 2199 \equiv 0 \bmod 73$, o čemž se můžeme přesvědčit zkouškou: $615\eta + 2199 = 615 \cdot 68 + 2199 = 41\,820 + 2199 = 44\,019 = 73 \cdot 503$. Dosadíme-li za vypočtené η do pravé strany (48), dostaneme $(2199 + 615\eta) \cdot 73^{319} = 603 \cdot 73^{320}$ a poněvadž $73^{320} \equiv 1 \bmod 615$, bude $603 \cdot 73^{320} \equiv 603 \bmod 615$, tedy i $\xi \equiv 603 \bmod 615$ neboli opět $\xi = 603$.

Postup, jehož jsme právě užili, spočívá v tom, že řešíme pomocnou kongruenci, která v našem případě byla $615y + 2199 \equiv 0 \bmod 73$. Tuto kongruenci jsme už řešili přímo. Je však zřejmé, že by celý postup bylo možno opakovat. Tím bychom dostali celý systém pomocných kongruencí, které bychom postupně řešili.

V příkladech, které jsme si ukázali, jsme si mohli povšimnout, že všechny úpravy v kongruencích, které děláme s řešením (46) kongruence (43), můžeme dělat též s neznámou x. Z formálního hlediska tedy nemusíme rozlišovat neznámou x a nalezené řešení ξ. Proto se domluvíme, že od nynějška budeme řešení kongruence (42) libovolného stupně označovat stejným písmenem, jako neznámou v (42).

Příklad 24. Řešte kongruenci $91x \equiv 653 \bmod 1815$.

Řešení. Poněvadž $1815 = 3 \cdot 5 \cdot 11^2$ a $91 = 7 \cdot 13$, je $(1815, 91) = 1$ a $\varphi(1815) = 2 \cdot 4 \cdot 11 \cdot 10 = 880$. Proto

bude $91^{880} \equiv 1 \bmod 1815$ a pro řešení dané kongruence dostaneme podle (46)

$$x \equiv 653.91^{879} \equiv (653 + 1815y).91^{879} \bmod 1815. \qquad (49)$$

Budeme proto řešit první pomocnou kongruenci

$$1815y + 653 \equiv 0 \bmod 91.$$

Její úpravou dostaneme

$$-5y + 16 \equiv 0 \bmod 91$$

neboli

$$5y \equiv 16 \bmod 91.$$

Poněvadž $(5, 91) = 1$ a $\varphi(91) = 6.12 = 72$, dostaneme pro řešení této kongruence podle (46)

$$y \equiv 16.5^{71} \equiv (16 + 91z).5^{71} \bmod 91. \qquad (50)$$

Přitom je $5^{72} \equiv 1 \bmod 91$. Vztah (50) vede na druhou pomocnou kongruenci

$$91z + 16 \equiv 0 \bmod 5$$

neboli

$$z + 1 \equiv 0 \bmod 5,$$

jejíž řešení je zřejmě $z = 4$. Bude tedy $16 + 91z = 16 + 364 = 380 = 5.76$, takže vztah (50) pro $z = 4$ nabude tvaru

$$y \equiv 76.5^{72} \equiv 76 \bmod 91.$$

Tím jsme dostali řešení první pomocné kongruence $y = 76$ a protože pro toto y bude $1815y + 653 = 1815.76 + 653 = 137\,940 + 653 = 138\,593 = 91.1523$, dostaneme po dosazení do (49)

$$x \equiv 1523.91^{880} \equiv 1523 \bmod 1815.$$

Řešení kongruence $91x \equiv 653 \bmod 1815$ je tedy $x = 1523$. O správnosti výsledku se přesvědčíme zkouškou: $91 \cdot 1523 - 653 = 138\,593 - 653 = 137\,940 = 1815 \cdot 76$.

V příští kapitole si ukážeme ještě další metody řešení lineárních kongruencí.

Úlohy

11. Řešte lineární kongruence:

    a) $239x \equiv -6340 \bmod 311$;
    b) $-64x + 935 \equiv 0 \bmod 243$;
    c) $89x - 14 \equiv 0 \bmod 420$.

12. Určete nejmenší přirozené číslo k, pro které platí $26^k \equiv 1 \bmod 85$ a pomocí nalezeného výsledku řešte lineární kongruenci $26x \equiv 51 \bmod 85$.

13. Určete nejmenší přirozené číslo k, pro které platí $9^k \equiv 1 \bmod 65$ a pomocí nalezeného výsledku řešte pak lineární kongruenci $9x + 134 \equiv 0 \bmod 65$.

14*. Buďte a a b celá čísla a m přirozené číslo. Nechť dále $(a, m) = d > 1$. Dokažte, že platí:

    a) Je-li $b \not\equiv 0 \bmod d$, nemá kongruence (43) žádné řešení.
    b) Je-li $b \equiv 0 \bmod d$, má kongruence (43) v každé úplné soustavě zbytků podle modulu m právě d řešení, která jsou inkongruentní podle modulu m.

5. kapitola

SOUSTAVY KONGRUENCÍ O JEDNÉ NEZNÁMÉ S NĚKOLIKA MODULY

V předchozí kapitole jsme si ukázali základní metody řešení lineárních kongruencí o jedné neznámé. Potíže, které se přitom objevily, byly pouze početního charakteru. Byli jsme nuceni pracovat často s čísly, která byla příliš veliká, což pak vedlo k nutnosti dalších úprav. Tyto úpravy byly většinou zdlouhavé a často dosti komplikované.

Na příkladech 23 a 24 jsme si ukázali jednu cestu, kterou se můžeme alespoň u lineárních kongruencí zmíněným potížím vyhnout.

Z úvah, které jsme provedli ve čtvrté kapitole, je zřejmé, že potíže s velkými čísly se zvětšováním modulu porostou. Proto se v této kapitole budeme snažit převést danou kongruenci na soustavu kongruencí s moduly co možná nejmenšími.

Věta 31. *Buďte* $m_1 > 1$ *a* $m_2 > 1$ *celá nesoudělná čísla. Potom existují celá čísla* u *a* v *tak, že současně platí*

$$m_2 u - m_1 v = 1; \quad 0 < u < m_1; \quad 0 < v < m_2. \tag{51}$$

Důkaz. Poněvadž $(m_1, m_2) = 1$, můžeme podle věty 30 najít v úplné soustavě zbytků $\{0, 1, 2, \ldots, m_1 - 1\}$ podle modulu m_1 právě jedno číslo u, pro které platí $m_2 u \equiv 1 \bmod m_1$. Zřejmě bude $u \neq 0$, takže dostaneme

$0 < u < m$. Poněvadž $m_1 | (m_2 u - 1)$, bude číslo $\frac{m_2 u - 1}{m_1}$ celé. Položíme-li $v = \frac{m_2 u - 1}{m_1}$, bude dále $m_2 u - m_1 v = 1$. Z nerovností $1 \leqq u < m_1$ plyne násobením číslem $m_2 > 1$, že $m_2 \leqq m_2 u < m_1 m_2$ a tedy $0 < m_2 - 1 \leqq m_2 u - 1 < m_1 m_2$. Dělíme-li tyto nerovnosti číslem m_1, dostaneme konečně $0 < \frac{m_2 u - 1}{m_1} < m_2$, tj. $0 < v < m_2$, čímž je důkaz věty 31 proveden.

Příklad 25. Najděte celá čísla u a v tak, aby platilo $65u - 28v = 1$, $0 < u < 28$, $0 < v < 65$.

Řešení. Poněvadž je $(28, 65) = 1$, budeme hledat řešení kongruence $65u \equiv 1 \bmod 28$, tj. $9u \equiv 1 \bmod 28$. Vynásobíme-li poslední kongruenci třemi, dostaneme $27u \equiv 3 \bmod 28$, z čehož plyne $-u \equiv 3 \bmod 28$ neboli $u \equiv -3 \bmod 28$, a tedy $u = 25$. Nyní položíme $v = \frac{65u - 1}{28} = \frac{65 . 25 - 1}{28} = 58$. Bude tedy $u = 25$, $v = 58$.

Věta 32. *Buďte $m_1 > 1$ a $m_2 > 1$ celá nesoudělná čísla a nechť $m = m_1 m_2$. Nechť ještě celá čísla u a v vyhovují podmínkám* (51). *Potom vztah*

$$x \equiv m_2 x_1 u - m_1 x_2 v \bmod m, \tag{52}$$

platí právě tehdy, platí-li současně

$$x \equiv x_1 \bmod m_1 \quad \text{a} \quad x \equiv x_2 \bmod m_2. \tag{53}$$

Důkaz. Nechť platí vztah (52). Potom podle věty 20 bude současně

$$x \equiv m_2 x_1 u - m_1 x_2 v \bmod m_1$$

a

$$x \equiv m_2 x_1 u - m_1 x_2 v \bmod m_2,$$

tj.

$$x \equiv m_2 x_1 u \bmod m_1 \quad \text{a} \quad x \equiv -m_1 x_2 v \bmod m_2.$$

Poněvadž čísla u a v jsou zvolena podle (51), bude $m_2 u - m_1 v = 1$. Odtud pak $m_2 u = m_1 v + 1$, tj. $m_2 u \equiv 1 \bmod m_1$, a $-m_1 v = -m_2 u + 1$, tj. $-m_1 v \equiv 1 \bmod m_2$. Dostaneme tedy $x \equiv x_1 (m_2 u) \equiv x_1 \bmod m_1$ a $x \equiv x_2 (-m_1 v) \equiv x_2 \bmod m_2$, takže bude současně $x \equiv x_1 \bmod m_1$ a $x \equiv x_2 \bmod m_2$.

Nechť obráceně platí (53). Pro libovolnou dvojici celých čísel u' a v' bude tedy současně

$$x \equiv x_1 + m_1 v' \bmod m_1 \quad \text{a} \quad x \equiv x_2 + m_2 u' \bmod m_2.$$

Zvolme nyní celá čísla u a v podle (51) a položme $u' = u(x_1 - x_2)$, $v' = v(x_1 - x_2)$. Dostaneme tak, že platí $x_1 + m_1 v' = x_1 + m_1 v(x_1 - x_2) = x_1 (m_1 v + 1) - m_1 v x_2 = m_2 u x_1 - m_1 v x_2$, $x_2 + m_2 u' = x_2 + m_2 u(x_1 - x_2) = m_2 u x_1 + (1 - m_2 u) x_2 = m_2 u x_1 - m_1 v x_2$, takže bude současně

$$x \equiv m_2 u x_1 - m_1 v x_2 \bmod m_1,$$

$$x \equiv m_2 u x_1 - m_1 v x_2 \bmod m_2.$$

Poněvadž je $(m_1, m_2) = 1$, plyne z těchto kongruencí podle věty 20 vztah (52), což jsme chtěli dokázat.

Využijeme nyní výsledku věty 32 a zformulujeme větu, která má při řešení kongruencí fundamentální význam.

Věta 33. *Buďte n a m přirozená čísla a nechť existují přirozená čísla $m_1 > 1$ a $m_2 > 1$ taková, že $m = m_1 m_2$ a $(m_1, m_2) = 1$. Nechť konečně*

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

je polynom n-tého stupně s celočíselnými koeficienty.
Potom kongruence n-tého stupně o jedné neznámé

$$P(x) \equiv 0 \bmod m \tag{54}$$

je ekvivalentní se soustavou dvou kongruencí n-tého stupně o jedné neznámé

$$P(x) \equiv 0 \bmod m_1, \tag{55}$$

$$P(x) \equiv 0 \bmod m_2 \tag{56}$$

v tomto smyslu:

a) Každé řešení kongruence (54) *je též řešením obou kongruencí* (55) *a* (56).

b) Je-li x_1 libovolné řešení kongruence (55) *a x_2 libovolné řešení kongruence* (56), *je číslo x definované vztahem*

$$x \equiv m_2ux_1 - m_1vx_2 \bmod m \tag{52}$$

řešením kongruence (54), *tj. z libovolného řešení soustavy* (55)—(56) *můžeme podle* (52) *zkonstruovat řešení kongruence* (54).

c) Necháme-li x_1 probíhat množinou všech řešení kongruence (55) *vzájemně inkongruentních podle modulu m_1 a nezávisle na tom x_2 probíhat množinou všech řešení kongruence* (56) *vzájemně inkongruentních podle modulu m_2, bude číslo x definované vztahem* (52) *probíhat množinou všech řešení kongruence* (54) *vzájemně inkongruentních podle modulu m.*

Důkaz. Je-li ξ řešením kongruence (54), bude $P(\xi) \equiv 0 \bmod m$. Poněvadž $m = m_1m_2$ a $(m_1, m_2) = 1$, bude podle věty 20 též $P(\xi) \equiv 0 \bmod m_1$ a $P(\xi) \equiv 0 \bmod m_2$, tj. ξ bude též řešením obou kongruencí (55) a (56). Tím je dokázáno tvrzení a).

Nechť x_1 resp. x_2 jsou libovolná řešení kongruencí (55) resp. (56), tj. nechť $P(x_1) \equiv 0 \bmod m_1$ a $P(x_2) \equiv 0 \bmod m_2$. Podle věty 32 platí pro každé číslo x definované vztahem (52), že $x \equiv x_1 \bmod m_1$ a $x \equiv x_2 \bmod m_2$. Odtud podle věty 17 plyne, že bude též $P(x) \equiv P(x_1) \bmod m_1$ a $P(x) \equiv P(x_2) \bmod m_2$, takže podle (11) máme dále $P(x) \equiv 0 \bmod m_1$ a $P(x) \equiv 0 \bmod m_2$. Podle věty 20 plyne však z těchto vztahů, že $P(x) \equiv 0 \bmod m$, tj. číslo x definované vztahem (52) bude řešením kongruence (54). Tím jsme dokázali tvrzení b).

Nechť konečně x_1, x_2 a x_1', x_2' jsou libovolná dvě řešení soustavy (55)—(56) a nechť

$$x \equiv m_2 u x_1 - m_1 v x_2 \bmod m,$$
$$x' \equiv m_2 u x_1' - m_1 v x_2' \bmod m$$

jsou odpovídající řešení kongruence (54). Jestliže $x \equiv x' \bmod m$, bude podle (11)

$$x \equiv m_2 u x_1 - m_1 v x_2 \bmod m,$$
$$x \equiv m_2 u x_1' - m_1 v x_2' \bmod m.$$

Odtud podle věty 32 plyne

$$x \equiv x_1 \bmod m_1, \qquad x \equiv x_2 \bmod m_2,$$
$$x \equiv x_1' \bmod m_1, \qquad x \equiv x_2' \bmod m_2.$$

Z těchto kongruencí dostáváme opět podle (11), že

$$x_1 \equiv x_1' \bmod m_1, \qquad x_2 \equiv x_2' \bmod m_2.$$

Není-li tedy současně $x_1 \equiv x_1' \bmod m_1$ a $x_2 \equiv x_2' \bmod m_2$, nemůže být ani $x \equiv x' \bmod m$, čímž jsme dokázali i tvrzení c).

Všimněme si, že jsme ve větě 33 nečinili žádných

předpokladů ani o stupni polynomu $P(x)$, ani o jeho koeficientech (přirozeně kromě toho, že jsou celé). Možnost užití této věty se tedy nebude týkat jenom kongruencí lineárních, nýbrž i kongruencí libovolného stupně. Dále vidíme, že aplikujeme-li větu 33 na lineární kongruenci (43), můžeme to učinit, aniž by byl splněn předpoklad o nesoudělnosti čísel a a m. Tato skutečnost nám umožní alespoň v některých případech snadno řešit kongruenci (43) i tehdy, je-li $(a, m) > 1$ (viz příklad 27 a úlohu 17).

Příklad 26. Řešte lineární kongruenci o jedné neznámé $71x \equiv 32 \bmod 539$.

Řešení. Poněvadž $539 = 11.49 = 11.7^2$ a $(11, 49) = 1$, můžeme podle věty 33 danou kongruenci nahradit soustavou dvou kongruencí $71x \equiv 32 \bmod 11$ a $71x \equiv 32 \bmod 49$ neboli

$$5x \equiv 10 \bmod 11,$$
$$22x \equiv 32 \bmod 49.$$

Poněvadž $(5, 11) = (22, 49) = 1$, má každá z těchto kongruencí v úplné soustavě zbytků podle odpovídajícího modulu právě jedno řešení. Krátíme-li kongruenci $5x \equiv 10 \bmod 11$ pěti, dostaneme ihned její řešení $x \equiv 2 \bmod 11$. Kongruenci $22x \equiv 32 \bmod 49$ budeme nejprve krátit dvěma a pak násobit devíti. Dostaneme tak $99x \equiv 144 \bmod 49$, odkud okamžitě plyne $x \equiv 46 \bmod 49$.

Máme tedy $m_1 = 11$, $m_2 = 49$, $x_1 = 2$ a $x_2 = 46$. Nyní najdeme celá čísla u a v podle věty 31, $49u - 11v = 1$. K tomu budeme řešit kongruenci $49u \equiv 1 \bmod 11$ neboli $5u \equiv 1 \bmod 11$. Násobíme-li tuto kongruenci dvěma, dostaneme $10u \equiv 2 \bmod 11$ neboli $-u \equiv 2$

mod 11. Odtud máme $u \equiv 9 \bmod 11$. Snadno nahlédneme, že můžeme položit $u = 9$ a $v = 40$.

Podle (52) tedy dostaneme

$$x \equiv 49.9.2 - 11.40.46 \bmod 539$$

a poněvadž $49.9.2 - 11.40.46 = 882 - 20\,240 = -19\,358 = -539.36 + 46$, bude $x \equiv 46 \bmod 539$.

Kongruence $71x \equiv 32 \bmod 539$ má tedy v každé úplné soustavě zbytků podle modulu 539 právě jedno řešení $x \equiv 46 \bmod 539$.

O správnosti výsledku se můžeme přesvědčit zkouškou: $71.46 - 32 = 3266 - 32 = 3234 = 6.539$.

Pro srovnání můžeme ještě naznačit řešení dané kongruence přímo pomocí vztahu (46). Podle (31) bude $\varphi(539) = 7.6.10 = 420$, takže podle (46) bude

$$x \equiv 32.71^{419} \bmod 539.$$

Čtenář se může sám přesvědčit, jak zdlouhavé a pracné bude vyhledání výsledku přímo z tohoto vztahu. Spočítá-li tento příklad do konce, bude si moci učinit představu o výhodě postupu popsaného větou 33.

Příklad 27. Řešte lineární kongruenci o jedné neznámé $275x + 605 \equiv 0 \bmod 1445$.

Řešení. Poněvadž $1445 = 5.289 = 5.17^2$, vidíme, že $(275, 1445) = 5$. Proto nemůžeme užít vztahu (46). Poněvadž však je $(5, 289) = 1$, můžeme podle věty 33 nahradit danou kongruenci soustavou kongruencí

$$275x + 605 \equiv 0 \bmod 5,$$
$$275x + 605 \equiv 0 \bmod 289.$$

První z těchto kongruencí je splněna pro všechna celá x, takže v úplné soustavě zbytků $\{0, 1, 2, 3, 4\}$ podle mo-

dulu 5 má za řešení každé z čísel této soustavy. U druhé kongruence $275x + 605 \equiv 0 \bmod 289$ je však už splněn předpoklad $(275, 289) = 1$, takže tato kongruence bude mít v každé úplné soustavě zbytků podle modulu 289 právě jedno řešení. Snadno nahlédneme, že lze tuto kongruenci krátit číslem 55, čímž dostaneme kongruenci $5x + 11 \equiv 0 \bmod 289$. Odtud násobením číslem 58 dostaneme $290x + 638 \equiv 0 \bmod 289$ neboli $x + 60 \equiv$ $\equiv 0 \bmod 289$. Řešení druhé kongruence tedy bude $x \equiv$ $\equiv -60 \equiv 229 \bmod 289$.

Nyní můžeme položit $m_1 = 5$, $m_2 = 289$; x_1 pak bude kterékoliv z čísel 0, 1, 2, 3, 4 a $x_2 = 229$. Podle věty 31 najdeme dále celá čísla u a v tak, aby platilo $289u - 5v = 1$. Proto musíme řešit kongruenci $289u \equiv 1 \bmod 5$ neboli $-u \equiv 1 \bmod 5$. Poněvadž její řešení je $u \equiv -1 \equiv 4 \bmod 5$, můžeme položit $u = 4$. Potom snadno vypočteme $v = 231$, takže pro řešení x kongruence $275x + 605 \equiv 0 \bmod 1445$ podle (52) dostaneme $x \equiv 1156x_1 - 1155x_2 \bmod 1445$, tj. $x \equiv -289x_1 +$ $+ 290x_2 \bmod 1445$. Dosadíme-li postupně za x_1 čísla 0, 1, 2, 3, 4 a za x_2 číslo 229, dostaneme pro řešení původní kongruence postupně

$x \equiv 1385 \bmod 1445$, $x \equiv 1096 \bmod 1445$, $x \equiv 807 \bmod$ 1445, $x \equiv 518 \bmod 1445$ a $x \equiv 229 \bmod 1445$.

Kongruence $275x + 605 \equiv 0 \bmod 1445$ má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 1444\}$ podle modulu 1445 pět řešení: 229, 518, 807, 1096 a 1385.

O správnosti výsledku se můžeme přesvědčit zkouškou. Mimoto si na tomto příkladě můžeme ověřit výsledek úlohy 14b).

Postupem popsaným větami 33 a 32 můžeme tedy řešit danou kongruenci tak, že ji nahradíme ekvivalentní

soustavou dvou kongruencí s různými vzájemně nesoudělnými moduly. Vzniklé kongruence pak řešíme. Celý postup lze přirozeně matematickou indukcí rozšířit i na případy, kdy modul m je součinem více činitelů, které jsou po dvou nesoudělné. Naznačíme si teď stručně, jak se to dělá.

Nechť $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, kde $p_1, p_2, \dots, p_r$ jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_r$ přirozená čísla. Poněvadž $(p_1^{\alpha_1}, p_2^{\alpha_2}, p_3^{\alpha_3} \dots p_r^{\alpha_r}) = 1$, můžeme podle věty 33 úlohu řešit kongruenci o jedné neznámé $P(x) \equiv 0 \bmod m$ převést na úlohu řešit ekvivalentní soustavu kongruencí

$$P(x) \equiv 0 \bmod p_1^{\alpha_1} \quad \text{a} \quad P(x) \equiv 0 \bmod p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}.$$

Zcela obdobně se druhá z těchto kongruencí rozpadne na soustavu

$$P(x) \equiv 0 \bmod p_2^{\alpha_2} \quad \text{a} \quad P(x) \equiv 0 \bmod p_3^{\alpha_3} \dots p_r^{\alpha_r}$$

atd., takže místo kongruence

$$P(x) \equiv 0 \bmod p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

budeme řešit ekvivalentní soustavu r kongruencí

$$\begin{aligned} P(x) &\equiv 0 \bmod p_1^{\alpha_1}, \\ P(x) &\equiv 0 \bmod p_2^{\alpha_2}, \\ &\vdots \\ P(x) &\equiv 0 \bmod p_r^{\alpha_r}. \end{aligned}$$

Nechť $x_1, x_2, \dots, x_r$ je libovolné řešení této soustavy. Snadno nahlédneme, že řešení x kongruence $P(x) \equiv 0 \bmod p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ musí splňovat podmínky

$$x \equiv x_1 \bmod p_1^{\alpha_1},$$
$$x \equiv x_2 \bmod p_2^{\alpha_2},$$
$$\vdots$$
$$x \equiv x_r \bmod p_r^{\alpha_r}.$$

Poněvadž prvočísla $p_1, p_2, \ldots, p_r$ jsou vzájemně různá, určíme z čísel $x_1, x_2, \ldots, x_r$ podle věty 33 postupně řešení kongruencí $P(x) \equiv 0 \bmod p_1^{\alpha_1} p_2^{\alpha_2}$, dále $P(x) \equiv 0 \bmod p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ atd., až konečně dostaneme řešení kongruence $P(x) \equiv 0 \bmod p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$.

Příklad 28. Řešte kongruenci $23\,941x - 915 \equiv 0 \bmod 3564$.

Řešení. Poněvadž $3564 = 2^2 . 3^4 . 11$, rozpadne se daná kongruence na soustavu tří kongruencí

$23\,941x - 915 \equiv 0 \bmod 4$, $23\,941x - 915 \equiv 0 \bmod 11$ a $23\,941x - 915 \equiv 0 \bmod 81$,

které můžeme přepsat ve tvaru

$x \equiv 3 \bmod 4$, $5x \equiv 2 \bmod 11$ a $46x \equiv 24 \bmod 81$.

Poněvadž $(1, 4) = (5, 11) = (46, 81) = 1$, má každá z těchto kongruencí v úplné soustavě zbytků podle odpovídajícího modulu právě jedno řešení.

Kongruence $x \equiv 3 \bmod 4$ má zřejmě řešení $x_1 = 3$.

Násobíme-li druhou kongruenci $5x \equiv 2 \bmod 11$ dvěma, dostaneme $10x \equiv 4 \bmod 11$ neboli $-x \equiv -7 \bmod 11$, takže pro její řešení dostaneme $x \equiv 7 \bmod 11$. Položíme tedy $x_2 = 7$.

Násobíme-li třetí kongruenci $46x \equiv 24 \bmod 81$ sedmi, dostaneme $322x \equiv 168 \bmod 81$, tj. $-2x \equiv 6 \bmod 81$. Po zkrácení dvěma pak bude $-x \equiv 3 \bmod 81$, odkud

$x \equiv -3 \equiv 78 \bmod 81$. Můžeme proto položit $x_3 = 78$.

Soustava kongruencí, jíž jsme původní kongruenci nahradili, má tedy řešení $x_1 = 3$, $x_2 = 7$, $x_3 = 78$. Řešení x kongruence $23\,941x - 915 \equiv 0 \bmod 3564$ musí tedy splňovat podmínky

$$x \equiv 3 \bmod 4,$$
$$x \equiv 7 \bmod 11,$$
$$x \equiv 78 \bmod 81.$$

Z prvních dvou z těchto kongruencí můžeme nyní podle vět 33 a 32 sestrojit řešení kongruence $23\,941x - 915 \equiv 0 \bmod 44$. Položíme-li $m_1 = 4$, $m_2 = 11$, musíme nejprve najít celá čísla u_1 a v_1 podle věty 31. Snadno zjistíme, že rovnice $11u_1 - 4v_1 = 1$ bude splněna pro $u_1 = 3$ a $v_1 = 8$. Podle (52) tedy dostaneme $x \equiv 11.3.3 - 4.8.7 \bmod 44$ a poněvadž $11.3.3 - 4.8.7 = 99 - 224 = -125$, bude $x \equiv -125 \equiv 7 \bmod 44$.

Řešení x původní kongruence tedy musí vyhovovat podmínkám

$$x \equiv 7 \bmod 44,$$
$$x \equiv 78 \bmod 81.$$

Položíme nyní $m_1' = 44$ a $m_3 = 81$. Budeme nejprve hledat řešení u_2 a v_2 rovnice $81u_2 - 44v_2 = 1$ podle věty 31. K tomu bude třeba řešit kongruenci $81u_2 \equiv 1 \bmod 44$ neboli $-7u_2 \equiv 1 \bmod 44$. K řešení této kongruence bychom mohli opět použít metody popsané v této kapitole. Můžeme však též použít přímo vzorce (46) nebo se snažit najít řešení přímo různými dovolenými úpravami kongruence. Tak např. znásobíme-li kongruenci $-7u_2 \equiv 1 \bmod 44$ pěti, dostaneme $-35u_2 \equiv 5 \bmod 44$, tj. $9u_2 \equiv 5 \bmod 44$. Snadno zjistíme, že je výhodné násobit tuto kongruenci opět pěti, takže dostaneme $45u_2 \equiv 25$

mod 44, z čehož ihned plyne $u_2 \equiv 25 \bmod 44$. Položíme tedy $u_2 = 25$ a ze vztahu $81u_2 - 44v_2 = 1$ vypočteme $v_2 = 46$. Položíme-li ještě $x_1' = 7$ a $x_3 = 78$, dostaneme z kongruencí $x \equiv 7 \bmod 44$ a $x \equiv 78 \bmod 81$ podle (52) $x \equiv 81.25.7 - 44.46.78 \bmod 3564$, a poněvadž $81.25.7 - 44.46.78 = 2025.7 - 2024.78 = 14\,175 - 157\,872 = -143\,697 = -3564.41 + 2427$, bude konečně $x \equiv 2427 \bmod 3564$.

Kongruence $23\,941x - 915 \equiv 0 \bmod 3564$ má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 3563\}$ podle modulu 3564 právě jedno řešení $x = 2427$. O správnosti tohoto výsledku se přesvědčíme zkouškou: $23\,941.2427 - 915 = 58\,104\,807 - 915 = 58\,103\,892 = 16\,303 . 3564$.

Na příkladech 26 až 28 jsme viděli, jak lze postupem popsaným větami 33 a 32 dosáhnout toho, že čísla, s nimiž pracujeme, můžeme nahradit čísly menšími. Rovněž jsme si mohli povšimnout, že při řešení lineární kongruence o jedné neznámé můžeme kombinovat všechny metody, které jsme si dosud ukázali. Vhodnou kombinací známých metod můžeme často podstatnou část výpočtu provést zpaměti, čímž se celý postup značně urychlí.

Úlohy

15. Metodou popsanou v této kapitole řešte znovu úlohu 11 c).

16. Řešte lineární kongruence:

a) $69x - 6412 \equiv 0 \bmod 1825$;
b) $12\,013x + 9877 \equiv 0 \bmod 228\,150$.

17. Řešte lineární kongruence o jedné neznámé:

a) $81x + 765 \equiv 0 \bmod 1089$;
b) $7154x - 64\,337 \equiv 0 \bmod 5859$.

6. kapitola

SOUSTAVY LINEÁRNÍCH KONGRUENCÍ O NĚKOLIKA NEZNÁMÝCH. NEURČITÉ ROVNICE

Zcela obdobně jako u lineárních rovnic můžeme mít dánu soustavu několika lineárních kongruencí o více neznámých. Úkolem je pak vyhledat hodnoty neznámých tak, aby po dosazení těchto hodnot do kterékoliv kongruence tvořící danou soustavu byla tato kongruence splněna. Při řešení soustavy lineárních kongruencí o více neznámých se přirozeně řídíme týmiž pravidly, jakými jsme se řídili v případě jedné lineární kongruence o jedné neznámé.

U lineárních rovnic se obyčejně nejprve zabýváme takovými soustavami, u kterých je počet neznámých roven počtu rovnic tvořících danou soustavu (např. soustavou dvou lineárních rovnic o dvou neznámých, soustavou tří lineárních rovnic o třech neznámých atd.). Podobně si budeme počínat i u soustav lineárních kongruencí o více neznámých. Budeme vyšetřovat soustavu dvou lineárních kongruencí o dvou neznámých, soustavu tří lineárních kongruencí o třech neznámých apod.

V předcházející kapitole jsme si ukázali, jak lze řešit soustavu několika lineárních kongruencí o jedné neznámé s různými, po dvou nesoudělnými moduly. Tato situace nemá u lineárních rovnic obdoby, neboť máme-li např. soustavu dvou lineárních rovnic o jedné neznámé, lze buď z jedné rovnice dostat dovolenými úpravami druhou, nebo si rovnice odporují. V prvním případě

můžeme kteroukoliv z obou rovnic vyřešit a nalezené řešení bude i řešením druhé rovnice, tj. bude řešením dané soustavy. Kteroukoliv z rovnic vyšetřované soustavy tedy můžeme vynechat, čímž převádíme úlohu na řešení jedné lineární rovnice o jedné neznámé. Naproti tomu ve druhém případě nemá daná soustava žádné řešení.

Na rozdíl od soustav několika lineárních rovnic s více neznámými můžeme tedy v analogické úloze při řešení soustavy několika lineárních kongruencí o více neznámých obecně očekávat, že moduly jednotlivých kongruencí soustavy nebudou stejné. Touto obecnou úlohou se zde nebudeme zabývat; omezíme se pouze na případ, kdy budou mít všechny kongruence dané soustavy týž modul. Při řešení takovýchto soustav můžeme pak přirozeně užívat všech metod, jichž používáme při řešení soustav lineárních rovnic (metoda sčítací, vylučovací, srovnávací, případně jejich kombinování).

V souhlasu s větou 17 se opět můžeme při řešení těchto soustav lineárních kongruencí omezit na řešení ze zvolené úplné soustavy zbytků podle daného modulu.

Příklad 29. Řešte soustavu dvou lineárních kongruencí o dvou neznámých

$$6x + 5y \equiv 8 \bmod 35,$$
$$7x - 24y \equiv 101 \bmod 35.$$

Řešení. Násobíme-li první kongruenci číslem 24 a druhou číslem 5, dostaneme

$$144x + 120y \equiv 192 \bmod 35,$$
$$35x - 120y \equiv 505 \bmod 35.$$

Sečtením těchto kongruencí dostaneme dále $179x \equiv 697 \bmod 35$ neboli $4x \equiv -3 \bmod 35$. Z této kon-

gruence násobením devíti plyne $36x \equiv -27 \bmod 35$, tj. $x \equiv 8 \bmod 35$.

Nyní dosadíme za vypočtené x do jedné z působních kongruencí a hledáme pak hodnotu neznámé y. V našem případě k tomu však není vhodná kongruence první, neboť pro neznámou y bychom dostali kongruenci $5y \equiv -40 \bmod 35$. Čísla 5 a 35 nejsou nesoudělná a my jsme se takovýmito kongruencemi obecně nezabývali.

Dosadíme tedy za vypočtené x do druhé z původních kongruencí. Tím dostaneme $56 - 24y \equiv 101 \bmod 35$, odkud pak plyne $24y \equiv -45 \bmod 35$ neboli $24y \equiv -10 \bmod 35$. Krátíme-li tuto kongruenci dvěma a násobíme-li pak vzniklou kongruenci třemi, dostáváme $36y \equiv -15 \bmod 35$, z čehož $y \equiv 20 \bmod 35$.

Daná soustava dvou lineárních kongruencí o dvou neznámých má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 34\}$ podle modulu 35 právě jedno řešení $x = 8$, $y = 20$. O správnosti nalezeného výsledku se můžeme přesvědčit zkouškou.

Jiné řešení. Násobíme-li první z původních kongruencí číslem 6, dostaneme $36x + 30y \equiv 48 \bmod 35$ neboli $x - 5y \equiv 13 \bmod 35$. Odtud pak $x \equiv 5y + 13 \bmod 35$. Dosadíme-li za takto vyjádřené x do druhé z původních kongruencí, dostaneme $35y + 91 - 24y \equiv 101 \bmod 35$, odkud plyne, že $24y \equiv -10 \bmod 35$. Tuto kongruenci vyřešíme stejně jako při prvním způsobu řešení, takže dostaneme $y \equiv 20 \bmod 35$. Poněvadž $x \equiv 5y + 13 \bmod 35$, dostaneme dosazením za vypočtené y konečně $x \equiv 5.20 + 13 \equiv 8 \bmod 35$. Docházíme tedy jiným způsobem ke stejnému výsledku.

Příklad 30. Vyšetřte soustavu dvou lineárních kongruencí o dvou neznámých

$$19x + y \equiv 1 \bmod 35,$$
$$x - 11y \equiv 6 \bmod 35.$$

Řešení. Předpokládejme, že celá čísla x_1 a y_1 tvoří řešení této soustavy. Bude tedy současně

$$19x_1 + y_1 \equiv 1 \bmod 35,$$
$$x_1 - 11y_1 \equiv 6 \bmod 35.$$

Přičteme-li ke druhé z těchto kongruencí jedenáctinásobek první kongruence, dostaneme

$$(11.19 + 1)x_1 + (11 - 11)y_1 \equiv 11.1 + 6 \bmod 35$$

neboli

$$210x_1 \equiv 17 \bmod 35,$$

tj.

$$0 \equiv 17 \bmod 35,$$

což neplatí.

Nalezený spor dokazuje, že daná soustava lineárních kongruencí nemá žádné řešení.

Příklad 31. Řešte soustavu dvou lineárních kongruencí o dvou neznámých

$$3x - 5y \equiv 1 \bmod 11,$$
$$x + 2y \equiv 4 \bmod 11.$$

Řešení. Vyjádříme-li ze druhé kongruence neznámou x, dostaneme $x \equiv -2y + 4 \bmod 11$. Dosazením za toto x do první kongruence dostaneme dále pro neznámou y kongruenci

$$3.(4 - 2y) - 5y \equiv 1 \bmod 11$$

neboli

$$12 - 11y \equiv 1 \bmod 11.$$

Tato kongruence je však splněna pro každé celé číslo y.

V tomto případě se můžeme snadno přesvědčit, že obě kongruence dané soustavy jsou v podstatě stejné. Vynásobíme-li třeba první z nich čtyřmi, dostaneme $12x - 20y \equiv 4 \bmod 11$ neboli $x + 2y \equiv 4 \bmod 11$. To ovšem znamená, že zvolíme-li si např. libovolné celé číslo y, můžeme z kterékoliv z daných kongruencí určit zbývající neznámou x a takto získaná dvojice celých čísel x a y bude vždy představovat řešení dané soustavy.

Poněvadž za y stačí zvolit libovolné celé číslo z některé úplné soustavy zbytků podle modulu 11, dostaneme, že daná soustava dvou lineárních kongruencí o dvou neznámých má v každé úplné soustavě zbytků podle modulu 11 právě jedenáct vzájemně inkongruentních řešení. Pomocí druhé z původních kongruencí snadno zjistíme, že tato řešení jsou např.: $x_0 = 4, y_0 = 0; x_1 = 2, y_1 = 1; x_2 = 0, y_2 = 2; x_3 = 9, y_3 = 3; x_4 = 7, y_4 = 4; x_5 = 5, y_5 = 5; x_6 = 3, y_6 = 6; x_7 = 1, y_7 = 7; x_8 = 10, y_8 = 8; x_9 = 8, y_9 = 9; x_{10} = 6, y_{10} = 10$.

Je-li modul m složené číslo, $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, kde $p_1, p_2, \dots, p_r$ jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_r$ přirozená čísla, můžeme závěry plynoucí z vět 33 a 32 aplikovat i na soustavy několika lineárních kongruencí o více neznámých. Aniž bychom prováděli podrobný teoretický rozbor, ukážeme si postup řešení na několika příkladech.

Příklad 32. Užitím vět 33 a 32 řešte znovu soustavu dvou lineárních kongruencí o dvou neznámých

$$6x + 5y \equiv 8 \bmod 35,$$
$$7x - 24y \equiv 101 \bmod 35$$

(viz příklad 29).

Řešení. Poněvadž $35 = 5.7$ a $(5, 7) = 1$, musí řešení dané soustavy kongruencí vyhovovat též soustavám

$$6x + 5y \equiv 8 \bmod 5, \qquad 6x + 5y \equiv 8 \bmod 7,$$
$$7x - 24y \equiv 101 \bmod 5; \qquad 7x - 24y \equiv 101 \bmod 7.$$

Zjednodušením těchto kongruencí dostaneme

$$x \equiv 3 \bmod 5, \qquad -x + 5y \equiv 1 \bmod 7,$$
$$2x + y \equiv 1 \bmod 5; \qquad 4y \equiv 3 \bmod 7.$$

Ihned snadno zjistíme, že soustava kongruencí podle modulu 5 má v úplné soustavě zbytků $\{0, 1, 2, 3, 4\}$ podle tohoto modulu jediné řešení $x_1 = 3$, $y_1 = 0$.

K určení řešení soustavy kongruencí podle modulu 7 znásobíme nejprve druhou kongruenci $4y \equiv 3 \bmod 7$ dvěma, čímž dostaneme $8y \equiv 6 \bmod 7$, tj. $y \equiv 6 \bmod 7$. Dosadíme-li za toto y do první kongruence $-x + 5y \equiv 1 \bmod 7$, dostaneme $-x + 30 \equiv 1 \bmod 7$, z čehož $x \equiv 29 \equiv 1 \bmod 7$. Soustava kongruencí podle modulu 7 bude mít tedy v úplné soustavě zbytků $\{0, 1, 2, 3, 4, 5, 6\}$ podle tohoto modulu rovněž jediné řešení $x_2 = 1$, $y_2 = 6$.

Položme $m_1 = 5$, $m_2 = 7$ a hledejme podle věty 31 celá čísla u a v tak, aby platily vztahy (51). Snadno zjistíme, že v našem případě bude $u = 3$ a $v = 4$.

Poněvadž řešení x a y původní soustavy kongruencí s modulem 35 musí vyhovovat podmínkám

$$x \equiv x_1 \bmod m_1, \qquad y \equiv y_1 \bmod m_1,$$
$$x \equiv x_2 \bmod m_2, \qquad y \equiv y_2 \bmod m_2,$$

dostaneme podle (52)

$$x \equiv m_2 u x_1 - m_1 v x_2 \bmod m,$$
$$y \equiv m_2 u y_1 - m_1 v y_2 \bmod m.$$

Dosadíme-li do těchto vztahů za nalezené hodnoty, obdržíme konečně

$$x \equiv 7.3.3 - 5.4.1 \bmod 35,$$
$$y \equiv 7.3.0 - 5.4.6 \bmod 35,$$

tj. $x \equiv 43 \equiv 8 \bmod 35$, $y \equiv -120 \equiv 20 \bmod 35$.

V úplné soustavě zbytků $\{0, 1, 2, \ldots, 34\}$ podle modulu 35 má tedy daná soustava lineárních kongruencí jediné řešení $x = 8$, $y = 20$, což je výsledek shodný s výsledkem příkladu 29, který jsme řešili jinou metodou.

Příklad 33. Rešte soustavu tří lineárních kongruencí o třech neznámých

$$\begin{aligned} 27x - 613y - 49z &\equiv -215 \bmod 55, \\ -41x + 79y + 451z &\equiv 139 \bmod 55, \\ 6x - 17y + 29z &\equiv 614 \bmod 55. \end{aligned}$$

Řešení. Poněvadž $55 = 5.11$ a $(5, 11) = 1$, budeme danou soustavu řešit postupně s moduly 5 a 11.

Řešíme-li danou soustavu nejprve podle modulu 5, dostaneme po zjednoušení soustavu

$$\begin{aligned} 2x + 2y + z &\equiv 0 \bmod 5, \\ 4x + 4y + z &\equiv 4 \bmod 5, \\ x - 2y + 4z &\equiv 4 \bmod 5. \end{aligned}$$

Sečteme-li první a třetí z těchto kongruencí, dostaneme $3x + 5z \equiv 4 \bmod 5$ neboli $3x \equiv 4 \bmod 5$. Odtud po násobení dvěma plyne $6x \equiv 8 \bmod 5$, tj. $x \equiv 3 \bmod 5$. Odečteme-li dále od druhé kongruence dvojnásobek první kongruence soustavy, máme ihned $-z \equiv 4 \bmod 5$, tj. $z \equiv 1 \bmod 5$. Dosadíme-li konečně nalezené hodnoty

x a z např. do první kongruence vyšetřované soustavy, dostaneme pro poslední neznámou y podmínku $7 + 2y \equiv 0 \bmod 5$ neboli $2y \equiv -2 \bmod 5$. Po krácení dvěma dostaneme $y \equiv -1 \bmod 5$, tj. $y \equiv 4 \bmod 5$. Soustava kongruencí podle modulu 5 má tedy v úplné soustavě zbytků (0, 1, 2, 3, 4) podle tohoto modulu řešení $x_1 = 3$, $y_1 = 4$, $z_1 = 1$.

Analogicky budeme řešit danou soustavu kongruencí podle modulu 11. Po úpravě opět dostaneme soustavu

$$\begin{aligned} 5x - 8y - 5z &\equiv -6 \bmod 11, \\ -8x + 2y &\equiv 7 \bmod 11, \\ 6x - 6y + 7z &\equiv 9 \bmod 11. \end{aligned}$$

Přičteme-li k sedmínásobku první z těchto kongruencí pětinásobek kongruence třetí, dostaneme

$$(7.5 + 5.6)x - (7.8 + 5.6)y \equiv -7.6 + 5.9 \bmod 11,$$

tj. $65x - 86y \equiv 3 \bmod 11$ neboli $-x + 2y \equiv 3 \bmod 11$. Odtud pak plyne, že $x \equiv 2y - 3 \bmod 11$. Dosadíme-li za takto vyjádřené x do druhé kongruence soustavy, dostaneme dále $-16y + 24 + 2y \equiv 7 \bmod 11$. Odtud pak po úpravě obdržíme $-3y \equiv -6 \bmod 11$, z čehož po krácení číslem -3 plyne $y \equiv 2 \bmod 11$. Dále bude $x \equiv 2y - 3 \equiv 4 - 3 \bmod 11$, tj. $x \equiv 1 \bmod 11$. Dosadíme-li nyní nalezené hodnoty x a y např. do první kongruence soustavy, dostaneme pro neznámou z kongruenci $5 - 16 - 5z \equiv -6 \bmod 11$, tj. $-5z \equiv 5 \bmod 11$. Po zkrácení pěti pak máme $-z \equiv 1 \bmod 11$, z čehož $z \equiv 10 \bmod 11$. Soustava kongruencí podle modulu 11 má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 10\}$ podle modulu 11 řešení $x_2 = 1$, $y_2 = 2$, $z_2 = 10$.

Řešení x, y, z původní soustavy podle modulu 55 musí tedy vyhovovat podmínkám

$$x \equiv 3 \bmod 5, \quad y \equiv 4 \bmod 5, \quad z \equiv 1 \bmod 5,$$
$$x \equiv 1 \bmod 11, \quad y \equiv 2 \bmod 11, \quad z \equiv 10 \bmod 11.$$

Položíme-li $m_1 = 5$, $m_2 = 11$, zjistíme ihned, že rovnice $11u - 5v = 1$ má řešení $u = 1$, $v = 2$. Podle (52) tedy bude

$$x \equiv 11.3 - 10.\ 1 \bmod 55,$$
$$y \equiv 11.4 - 10.\ 2 \bmod 55,$$
$$z \equiv 11.1 - 10.10 \bmod 55,$$

tj. $x \equiv 23 \bmod 55$, $y \equiv 24 \bmod 55$ a $z \equiv -89 \equiv 21 \bmod 55$.

Původní soustava kongruencí s modulem 55 má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 54\}$ podle modulu 55 právě jedno řešení $x = 23$, $y = 24$, $z = 21$. O správnosti nalezeného výsledku se můžeme přesvědčit zkouškou.

Příklad 34. Řešte soustavu tří lineárních kongruencí o třech neznámých

$$613x - 1821y + 64z \equiv -811 \bmod 126,$$
$$-91x + 7105y + 215z \equiv 196 \bmod 126,$$
$$1503x + 208y - 782z \equiv 1966 \bmod 126.$$

Řešení. Poněvadž $126 = 2.3^2.7$, budeme řešit danou soustavu kongruencí postupně podle modulů 2, 9 a 7. Řešme nejprve danou soustavu kongruencí podle modulu 2. Po jejím zjednodušení dostaneme

$$x + y \equiv 1 \bmod 2,$$
$$x + y + z \equiv 0 \bmod 2,$$
$$x \equiv 0 \bmod 2.$$

Okamžitě zjistíme, že řešením této soustavy kongruencí v úplné soustavě zbytků $\{0, 1\}$ podle modulu 2 je $x_1 = 0$, $y_1 = 1$, $z_1 = 1$.

Řešíme-li danou soustavu kongruencí podle modulu 9, dostaneme po její úpravě

$$\begin{aligned} x - 3y + z &\equiv -1 \bmod 9, \\ -x + 4y + 8z &\equiv 7 \bmod 9, \\ y - 8z &\equiv 4 \bmod 9. \end{aligned}$$

Sečtením prvních dvou kongruencí této soustavy dostaneme $y + 9z \equiv 6 \bmod 9$, tj. $y \equiv 6 \bmod 9$. Dosazením za toto y do třetí kongruence obdržíme pak $6 - 8z \equiv 4 \bmod 9$ neboli $z \equiv -2 \equiv 7 \bmod 9$. Dosadíme-li konečně za vypočtená y a z do první kongruence, dostaneme $x - 18 + 7 \equiv -1 \bmod 9$, odkud pak plyne $x \equiv 1 \bmod 9$. Soustava kongruencí podle modulu 9 má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 8\}$ podle tohoto modulu řešení $x_2 = 1$, $y_2 = 6$, $z_2 = 7$.

Nakonec budeme řešit původní soustavu kongruencí podle modulu 7. Jejím zjednodušením dostaneme soustavu

$$\begin{aligned} 4x - y + z &\equiv -6 \bmod 7, \\ 5z &\equiv 0 \bmod 7, \\ 5x + 5y - 5z &\equiv 6 \bmod 7. \end{aligned}$$

Odtud ihned plyne $z \equiv 0 \bmod 7$. Dosazením za toto z do první a třetí kongruence této soustavy dostaneme

$$\begin{aligned} 4x - y &\equiv -6 \bmod 7, \\ 5x + 5y &\equiv 6 \bmod 7. \end{aligned}$$

Přičteme-li ke dvojnásobku druhé z těchto kongruencí kongruenci první, dostaneme $14x + 9y \equiv 6 \bmod 7$,

tj. $2y \equiv 6 \bmod 7$, takže po zkrácení dvěma bude $y \equiv$ $\equiv 3 \bmod 7$. Dosadíme-li za toto y do první z těchto kongruencí, dostaneme konečně $4x - 3 \equiv -6 \bmod 7$, odkud $4x \equiv -3 \equiv 4 \bmod 7$. Odtud pak po krácení čtyřmi plyne $x \equiv 1 \bmod 7$. Soustava kongruencí podle modulu 7 má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 6\}$ podle tohoto modulu řešení $x_3 = 1$, $y_3 = 3$, $z_3 = 0$.

Řešení x, y, z původní soustavy kongruencí podle modulu 126 musí tedy splňovat podmínky

$$x \equiv 0 \bmod 2, \quad y \equiv 1 \bmod 2, \quad z \equiv 1 \bmod 2,$$
$$x \equiv 1 \bmod 9, \quad y \equiv 6 \bmod 9, \quad z \equiv 7 \bmod 9,$$
$$x \equiv 1 \bmod 7, \quad y \equiv 3 \bmod 7, \quad z \equiv 0 \bmod 7.$$

Abychom toto řešení našli, sestrojíme nejprve řešení původní soustavy kongruencí, avšak s modulem $2.9 =$ $= 18$. K tomu je třeba najít řešení rovnice $9u_1 - 2v_1 =$ $= 1$. Snadno nahlédneme, že bude $u_1 = 1$, $v_1 = 4$. Ze vztahů

$$x \equiv 0 \bmod 2, \quad y \equiv 1 \bmod 2, \quad z \equiv 1 \bmod 2,$$
$$x \equiv 1 \bmod 9, \quad y \equiv 6 \bmod 9, \quad z \equiv 7 \bmod 9$$

pak podle (52) dostaneme

$$x \equiv 9.0 - 8.1 \equiv 10 \bmod 18,$$
$$y \equiv 9.1 - 8.6 \equiv 15 \bmod 18,$$
$$z \equiv 9.1 - 8.7 \equiv 7 \bmod 18.$$

Řešení původní soustavy kongruencí s modulem 126 tedy musí splňovat podmínky

$$x \equiv 10 \bmod 18, \quad y \equiv 15 \bmod 18, \quad z \equiv 7 \bmod 18,$$
$$x \equiv 1 \bmod 7, \quad y \equiv 3 \bmod 7, \quad z \equiv 0 \bmod 7.$$

Abychom toto řešení mohli sestrojit, budeme řešit nejprve rovnici $18u_2 - 7v_2 = 1$. Jejím řešením je zřejmě $u_2 = 2$, $v_2 = 5$, takže podle (52) dostaneme konečně

$$x \equiv 36.1 - 35.10 \equiv 64 \bmod 126,$$
$$y \equiv 36.3 - 35.15 \equiv 87 \bmod 126,$$
$$z \equiv 36.0 - 35.\ 7 \equiv\ 7 \bmod 126.$$

Daná soustava kongruencí má tedy v úplné soustavě zbytků $\{0, 1, 2, \ldots, 125\}$ podle modulu 126 řešení $x = 64$, $y = 87$, $z = 7$. O správnosti výsledku se můžeme opět přesvědčit zkouškou.

S lineárními kongruencemi velmi úzce souvisí tzv. lineární neurčité (nebo též diofantické) rovnice. Nechť n je přirozené číslo, $n \geqq 2$, a nechť $a_1, a_2, \ldots, a_n$ a b jsou daná celá čísla, přičemž žádné z čísel $a_1, a_2, \ldots, a_n$ není rovno nule. Připustíme-li, že neznámé $x_1, x_2, \ldots, x_n$ mohou nabývat pouze celočíselných hodnot, nazýváme rovnici

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \qquad (57)$$

lineární neurčitou rovnicí o n neznámých.

Řešit neurčitou rovnici (57) znamená pak najít všechny n-tice celých čísel $x_1, x_2, \ldots, x_n$ které dosazeny do (57) dávají identitu.

Budeme se zabývat pouze nejjednodušším případem lineární neurčité rovnice o dvou neznámých

$$ax + by = c, \qquad (58)$$

kde $a \neq 0$, $b \neq 0$ a c jsou daná celá čísla. Se speciálním případem této neurčité rovnice jsme se již setkali ve větě 31.

O koeficientech a, b a c můžeme bez omezení obecnosti předpokládat, že jejich největší společný dělitel je rovný jedné. Kdyby totiž bylo $(a, b, c) = d > 1$, dostali bychom dělením neurčité rovnice (58) celým číslem d neurčitou rovnici $a'x + b'y = c'$, kde $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ a $c' = \frac{c}{d}$, přičemž největší společný dělitel $(a', b', c') = 1$.

Nyní si ukážeme, že platí-li současně $(a, b, c) = 1$ a $(a, b) = d > 1$, nemá neurčitá rovnice (58) žádné řešení. V tomto případě je totiž $d|a$, $d|b$, takže podle věty 3 bude pro libovolnou dvojici celých čísel x a y též $d|(ax + by)$; kdyby dvojice celých čísel x, y byla řešením neurčité rovnice (58), muselo by zřejmě být i $d|c$, takže by bylo $(a, b, c) \geqq d > 1$. To je však proti předpokladu o celých číslech a, b a c.

Nás bude přirozeně více zajímat otázka, kdy neurčitá rovnice (58) řešení má a jak lze její řešení najít. O tom nás poučí

věta 34. *Nechť a, b, c jsou daná celá čísla a nechť $(a, b) = 1$. Potom lineární neurčitá rovnice* (58) *o dvou neznámých má nekonečně mnoho řešení. Je-li x_0, y_0 libovolně zvolené řešení této rovnice, dostaneme všechna její řešení ve tvaru $x = x_0 + bk$, $y = y_0 - ak$, kde k probíhá množinou všech celých čísel.*

Důkaz. Nejprve ukážeme, že rovnice (58) má za učiněných předpokladů vždy alespoň jedno řešení, které zkonstruujeme.

Nechť $|b| = 1$. Položíme-li $x_0 = 0$, $y_0 = bc$, bude $ax_0 + by_0 = b^2c = c$, takže dvojice celých čísel x_0, y_0 bude skutečně řešením rovnice (58).

Nechť $|b| > 1$. Poněvadž $(a, |b|) = (a, b) = 1$, má podle věty 30 kongruence $ax - c \equiv 0 \bmod |b|$ v každé

úplné soustavě zbytků podle modulu $|b|$ právě jedno řešení. Zvolme za x_0 libovolné řešení této kongruence. Bude tedy $ax_0 - c \equiv 0 \bmod |b|$, takže $\frac{ax_0 - c}{|b|}$ bude celé číslo. Položíme-li $y_0 = -\frac{ax_0 - c}{b}$, bude zřejmě $ax_0 + by_0 = c$, takže sestrojená dvojice celých čísel x_0, y_0 bude řešením rovnice (58).

Pro libovolné celé číslo $b \neq 0$ dovedeme tedy sestrojit řešení dané neurčité rovnice.

Předpokládejme, že známe nějaké řešení x_0, y_0 rovnice (58). Zvolme si libovolně celé číslo k a položme $x = x_0 + bk$, $y = y_0 - ak$. Pro takto sestrojenou dvojici celých čísel x, y pak bude platit $ax + by = a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 = c$, tj. dvojice celých čísel x, y bude opět řešením neurčité rovnice (58). Tím jsme dokázali, že tato rovnice má nekonečně mnoho řešení.

Zbývá ještě dokázat, že libovolné řešení x_1, y_1 neurčité rovnice (58) lze psát ve tvaru $x_1 = x_0 + bk$, $y_1 = y_0 - ak$, kde k je vhodné celé číslo. Poněvadž $ax_0 + by_0 = c$ i $ax_1 + by_1 = c$, dostaneme odečtením těchto rovností

$$a(x_1 - x_0) + b(y_1 - y_0) = 0. \tag{59}$$

Je-li $|b| = 1$, položíme $k = \frac{x_1 - x_0}{b}$, takže bude $x_1 = x_0 + bk$. Dosadíme-li za x_1 od vztahu (59), dostaneme $abk + b(y_1 - y_0) = 0$, z čehož plyne, že $y_1 = y_0 - ak$.

Je-li $|b| > 1$, plyne ze vztahu (59), že platí $a(x_1 - x_0) \equiv 0 \bmod |b|$. Poněvadž však $(a, |b|) = 1$, plyne

z této kongruence dále $x_1 - x_0 \equiv 0 \bmod |b|$, takže číslo $\frac{x_1 - x_0}{|b|}$ bude jistě celé. Můžeme proto položit $k = \frac{x_1 - x_0}{b}$. Bude pak $x_1 = x_0 + bk$ a po dosazení za toto x_1 do rovnosti (59) vypočteme odtud $y_1 = y_0 - ak$.

Tím je důkaz věty 34 proveden.

Příklad 35. Stanovte všechna řešení lineární neurčité rovnice o dvou neznámých

$$63x - 425y = 316. \tag{60}$$

Řešení. Poněvadž největší společný dělitel $(63, -425) = 1$, má podle věty 34 neurčitá rovnice (60) nekonečně mnoho řešení. Abychom našli jedno z těchto řešení, budeme řešit kongruenci $63x \equiv 316 \bmod 425$. Avšak $425 = 17.25$, takže tato kongruence se rozpadne na soustavu dvou kongruencí o jedné neznámé

$$63x \equiv 316 \bmod 17,$$
$$63x \equiv 316 \bmod 25.$$

Po zjednodušení bude

$$-5x \equiv 10 \bmod 17,$$
$$-12x \equiv 16 \bmod 25.$$

Krátíme-li v první kongruenci číslem -5, dostaneme $x \equiv -2 \equiv 15 \bmod 17$. Násobením druhé kongruence dvěma dostaneme $-24x \equiv 32 \bmod 25$, tj. $x \equiv 7 \bmod 25$.

Řešení x kongruence $63x \equiv 316 \bmod 425$ musí tedy splňovat podmínky

$$x \equiv 15 \bmod 17, \quad x \equiv 7 \bmod 25.$$

Abychom mohli použít vztahu (52) z věty 33, musíme řešit neurčitou rovnici $25u - 17v = 1$. To však vede opět na řešení kongruence $25u \equiv 1 \bmod 17$, tj. $8u \equiv 1 \bmod 17$. Násobíme-li tuto kongruenci dvěma, dostaneme $16u \equiv 2 \bmod 17$ neboli $-u \equiv -15 \bmod 17$, takže můžeme položit $u = 15$ a $v = \frac{25.15 - 1}{17} = \frac{374}{17} = 22$.

Podle (52) máme tedy pro řešení x kongruence $63x \equiv 316 \bmod 425$ vztah

$$x \equiv 25.15.15 - 17.22.7 \bmod 425,$$

tj. $x \equiv 3007 \equiv 32 \bmod 425$.

Můžeme proto položit $x_0 = 32$ a vypočítat y_0 ze vztahu $63x_0 - 425y_0 = 316$. Snadno zjistíme, že $y_0 = 4$.

Podle věty 34 dostaneme všechna řešení neurčité rovnice (60) ve tvaru

$$x = 32 - 425k, \quad y = 4 - 63k,$$

kde k probíhá množinou všech celých čísel. Můžeme ještě položit $h = -k$, takže i číslo h bude probíhat množinou všech celých čísel a řešení neurčité rovnice (60) budou pak dána ve tvaru

$$x = 32 + 425h, \quad y = 4 + 63h.$$

Všimněme si ještě postupu při řešení předcházejícího příkladu. Řešení dané neurčité rovnice (60) vedlo k řešení jisté kongruence. Modul této kongruence nebyl však mocninou prvočísla, takže její řešení vedlo opět k jisté neurčité rovnici, která však už byla mnohem jednodušší než neurčitá rovnice původní. Řešení této nové neurčité rovnice vedlo opět k řešení kongruence,

která měla už tentokrát prvočíselný modul. Tím byl celý tento cyklus úloh „neurčitá rovnice — kongruence — neurčitá rovnice — kongruence“ uzavřen.

Dá se patrně očekávat, že i v případech, kdy modul kongruence uzavírající naznačený cyklus úloh nebude přirozenou mocninou prvočísla, bude třeba v tomto cyklu pokračovat obdobným postupem tak dlouho, dokud nedospějeme ke kongruenci, jejímž modulem je přirozená mocnina nějakého prvočísla.

Příklad 36. Kolika způsoby můžeme vyplatit 74 Kčs, máme-li k dispozici pouze tříkorunové a pětikorunové mince?

Řešení. Označíme-li počet tříkorunových mincí x a počet pětikorunových mincí y, dojdeme k neurčité rovnici $3x + 5y = 74$. Z formulace úlohy je zřejmé, že se budeme zajímat jen o taková řešení x, y, pro která bude $x \geqq 0$ i $y \geqq 0$.

Abychom našli řešení dané neurčité rovnice, budeme nejprve řešit kongruenci $3x \equiv 74 \bmod 5$, tj. $3x \equiv 4 \bmod 5$. Vynásobíme-li tuto kongruenci dvěma, dostaneme $6x \equiv 8 \bmod 5$ neboli $x \equiv 3 \bmod 5$, takže můžeme položit $x_0 = 3$ a vypočítat $y_0 \equiv -\frac{3x_0 - 74}{5} = 13$.

Podle věty 34 dostaneme všechna řešení neurčité rovnice $3x + 5y = 74$ ve tvaru

$$x = 3 + 5k, \quad y = 13 - 3k,$$

kde k probíhá množinou všech celých čísel. Abychom ještě splnili doplňující podmínky $x \geqq 0$ a $y \geqq 0$, musíme celé číslo k volit tak, aby současně platilo $3 + 5k \geqq$

$\geqq 0$ a $13 - 3k \geqq 0$. Z těchto nerovností dostaneme, že celé číslo k musí vyhovovat nerovnostem $-\frac{3}{5} \leqq$ $\leqq k \leqq \frac{13}{3}$, tj. může nabývat pouze hodnot 0, 1, 2, 3 a 4.

Odpověď. Částku 74 Kčs můžeme pomocí tříkorunových a pětikorunových mincí vyplatit pouze pěti způsoby:

Počet tříkorun: 3, 8, 13, 18, 23,
Počet pětikorun: 13, 10, 7, 4, 1.

Úlohy

18. Řešte soustavy kongruencí:

a) $16x - 23y + 4z \equiv 12 \bmod 42$,
$9x + 86y - 95z \equiv -61 \bmod 42$,
$-8x + 10y + 3z \equiv 2 \bmod 42$.

b) $93x + 105y - 69z \equiv 156 \bmod 910$,
$-72x + 37y + 24z \equiv 603 \bmod 910$,
$69x + 231y - 52z \equiv -35 \bmod 910$.

19. Určete všechna řešení lineárních neurčitých rovnic:

a) $731x - 625y = -7$;

b) $106x + 337y = 29$.

20. Ukažte, že každý obnos od 18 Kčs výše lze vyplatit pomocí tříkorun a desetikorun. Určete, které z nižších obnosů nelze těmito platidly vyplatit.

7. kapitola

KONGRUENCE VYŠŠÍCH STUPŇŮ O JEDNÉ NEZNÁMÉ. KVADRATICKÉ KONGRUENCE O JEDNÉ NEZNÁMÉ S PRVOČÍSELNÝM MODULEM

Ve čtvrté kapitole jsme se seznámili s pojmy algebraická rovnice n-tého stupně o jedné neznámé a kongruence n-tého stupně o jedné neznámé. V této kapitole budeme nejprve zkoumat počet reálných řešení algebraické rovnice n-tého stupně s reálnými koeficienty a počet řešení kongruence n-tého stupně o jedné neznámé ve zvolené úplné soustavě zbytků podle daného modulu.

Víme, že každá lineární rovnice s reálnými koeficienty má právě jedno reálné řešení. Avšak už u kvadratických rovnic nastává situace složitější. Každá kvadratická rovnice s reálnými koeficienty má, jak známo, dva kořeny, které jsou však obecně komplexní. Mohou nastat z našeho hlediska celkem tři kvalitativně různé případy.

1. Rovnice má dva reálné kořeny vzájemně různé. Tak je tomu např. u rovnice $x^2 - 5x + 6 = 0$, kde $x_1 = 2$, $x_2 = 3$.
2. Rovnice má jeden dvojnásobný reálný kořen, jako je tomu např. u rovnice $x^2 - 4x + 4 = 0$, kde $x_1 = x_2 = 2$.
3. Rovnice má dva komplexní kořeny, které jsou vzájemně různé. Tak je tomu např. u rovnice $x^2 + 1 = 0$, kde $x_1 = \mathrm{i}$, $x_2 = -\mathrm{i}$.

Shrneme-li tyto tři případy, můžeme říci, že každá kvadratická rovnice s reálnými koeficienty má nejvýše dvě vzájemně různá reálná řešení.

V algebře se dokazuje obecně věta, že každá rovnice n-tého stupně s reálnými koeficienty má nejvýše n navzájem různých reálných řešení.

Podrobnějším studiem těchto otázek se zabývá např. učebnice [6].

Věta, kterou jsme právě vyslovili, nemá u kongruencí o jedné neznámé obecně platné obdoby. To jsme konečně už poznali u lineárních kongruencí (viz příklad 20) a ještě se s tím setkáme u kongruencí vyšších stupňů (příklad 37). Přesto však pro některé speciální případy modulů budeme moci pro kongruence vyslovit větu analogickou (viz větu 36).

V dalším textu budeme stále předpokládat, že

$$P_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

je polynom n-tého stupně s celočíselnými koeficienty.

Nechť $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, kde $p_1, p_2, \ldots, p_r$ jsou vzájemně různá prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_r$ přirozená čísla. V páté kapitole jsme zobecněním věty 33 poznali, že kongruence n-tého stupně o jedné neznámé.

$$P_n(x) \equiv 0 \bmod m \tag{61}$$

je ekvivalentní se soustavou kongruencí n-tého stupně o jedné neznámé

$$P_n(x) \equiv 0 \bmod p_i^{\alpha_i} \ (i = 1, 2, \ldots, r). \tag{62}$$

Z tvrzení a) věty 33 plyne, že nemá-li některá z kongruencí (62) řešení, nemá řešení ani kongruence (61). Z tvrzení c) této věty pak plyne, že označíme-li písmenem ν počet řešení kongruence (61) vzájemně inkongruentních podle modulu m a písmenem ν_i počet řešení kongruence $P_n(x) \equiv 0 \bmod p_i^{\alpha_i}$ vzájemně inkongruent-

ních podle modulu $p_i^{\alpha_i}$ ($i = 1, 2, \ldots, r$), bude platit

$$\nu = \nu_1 \nu_2 \ldots \nu_r. \tag{63}$$

Vět 33 a 32 lze tedy principiálně vždy užít jak ke stanovení počtu řešení kongruence (61), tak i k nalezení těchto řešení. Znamená to ovšem, že dovedeme určit počet řešení každé z r kongruencí soustavy (62), resp. že dovedeme tato řešení najít. Jak to lze někdy provést prakticky, ukážeme na jednoduchém příkladě.

Příklad 37. Řešte kongruenci 6. stupně o jedné neznámé

$$x^6 - 1 \equiv 0 \bmod 35.$$

Řešení. Poněvadž $35 = 5.7$ a $(5, 7) = 1$, rozpadne se daná kongruence na soustavu dvou kongruencí o jedné neznámé

$$x^6 - 1 \equiv 0 \bmod 5,$$

$$x^6 - 1 \equiv 0 \bmod 7.$$

Abychom našli řešení kongruence $x^6 - 1 \equiv 0 \bmod 5$, uvážíme, že podle (39) pro všechna celá x platí $x^5 \equiv x \bmod 5$. Bude tedy $x^6 \equiv x^2 \bmod 5$, takže místo kongruence $x^6 - 1 \equiv 0 \bmod 5$ budeme řešit ekvivalentní kongruenci $x^2 - 1 \equiv 0 \bmod 5$. Snadno zjistíme, že tato kongruence má v každé úplné soustavě zbytků podle modulu 5 dvě vzájemně inkongruentní řešení. V úplné soustavě zbytků $\{0, 1, 2, 3, 4\}$ podle modulu 5 budou těmito řešeními čísla 1 a 4.

Podobně podle (38) vidíme, že řešením kongruence $x^6 - 1 \equiv 0 \bmod 7$ v úplné soustavě zbytků $\{0, 1, 2, 3, 4, 5, 6\}$ podle modulu 7 bude kterékoliv z šesti čísel 1, 2, 3, 4, 5, 6.

Podle (63) bude mít tedy kongruence $x^6 - 1 \equiv 0$ mod 35 v každé úplné soustavě zbytků podle modulu 35 celkem dvanáct řešení, která budou podle tohoto modulu vzájemně inkongruentní. Abychom tato řešení našli, určíme podle věty 31 řešení neurčité rovnice $7u - 5v = 1$. Zřejmě bude $u = 3$ a $v = 4$, takže pro řešení x kongruence $x^6 - 1 \equiv 0$ mod 35 dostaneme podle (52)

$$x \equiv 21x_1 - 20x_2 \bmod 35,$$

kde x_1 je některé z čísel 1 a 4 a nezávisle na tom x_2 některé z čísel 1, 2, 3, 4, 5, 6. Postupně tedy bude

$$\begin{aligned}
x &\equiv 21.1 - 20.1 \equiv 1 \bmod 35,\\
x &\equiv 21.1 - 20.2 \equiv 16 \bmod 35,\\
x &\equiv 21.1 - 20.3 \equiv 31 \bmod 35,\\
x &\equiv 21.1 - 20.4 \equiv 11 \bmod 35,\\
x &\equiv 21.1 - 20.5 \equiv 26 \bmod 35,\\
x &\equiv 21.1 - 20.6 \equiv 6 \bmod 35,\\
x &\equiv 21.4 - 20.1 \equiv 29 \bmod 35,\\
x &\equiv 21.4 - 20.2 \equiv 9 \bmod 35,\\
x &\equiv 21.4 - 20.3 \equiv 24 \bmod 35,\\
x &\equiv 21.4 - 20.4 \equiv 4 \bmod 35,\\
x &\equiv 21.4 - 20.5 \equiv 19 \bmod 35,\\
x &\equiv 21.4 - 20.6 \equiv 34 \bmod 35.
\end{aligned}$$

Kongruence $x^6 - 1 \equiv 0$ mod 35 má tedy v každé úplné soustavě zbytků podle modulu 35 dvanáct vzájemně inkongruentních řešení. V úplné soustavě zbytků $\{0, 1, 2, \ldots, 34\}$ podle modulu 35 jsou těmito řešeními čísla 1, 4, 6, 9, 11, 16, 19, 24, 26, 29, 31 a 34.

Ekvivalence kongruence (61) se soustavou kongruencí (62) nám dovoluje zabývat se pouze kongruencemi se speciálním modulem $m = p^\alpha$, kde p je prvočíslo a α přirozené číslo. Budeme proto chvíli věnovat pozornost kongruencím tohoto tvaru.

Předpokládejme, že x_1 je libovolné řešení kongruence n-tého stupně o jedné neznámé

$$P_n(x) \equiv 0 \bmod p^\alpha, \tag{64}$$

tj. že platí $P_n(x_1) \equiv 0 \bmod p^\alpha$. Pro každé přirozené číslo $\alpha > 1$ je však $p | p^\alpha$, takže podle věty 18 bude též $P_n(x_1) \equiv 0 \bmod p$. Odtud vidíme, že každé řešení kongruence (64) bude též řešením kongruence

$$P_n(x) \equiv 0 \bmod p. \tag{65}$$

Řešení kongruence (64) můžeme proto hledat mezi řešeními kongruence (65). Nemá-li kongruence (65) řešení, nemůže mít řešení ani kongruence (64).

Dá se však dokázat, že z každého řešení kongruence (65) lze za určitých předpokladů sestrojit řešení kongruence (64). Známe-li nějaké řešení kongruence (65), je třeba pro konstrukci řešení kongruence (64) řešit ještě $\alpha - 1$ už pouze lineárních kongruencí tvaru $ax + b \equiv 0 \bmod p^\beta$, kde $1 \leqq \beta < \alpha$ a $p^\beta | a$, $p^\beta | b$. Obecnou teorií lineárních kongruencí tohoto typu jsme se však nezabývali. Kromě toho zmíněná konstrukce vyžaduje hlubších znalostí některých vlastností polynomů, které však už přesahují rámec této publikace.

Proto se až do konce této knihy omezíme pouze na studium kongruencí vyšších stupňů o jedné neznámé s prvočíselným modulem tvaru (65).

Věta 35. *Budiž p prvočíslo a nechť kongruence n-tého stupně o jedné neznámé*

$$P_n(x) \equiv 0 \bmod p$$

má více než n řešení, která jsou podle modulu p vzájemně inkongruentní.

Potom vztah $P_n(x) \equiv 0 \bmod p$ *platí pro všechna celá čísla* x.

Důkaz provedeme matematickou indukcí podle n. Nechť $n = 1$ a nechť kongruence

$$a_0 x + a_1 \equiv 0 \bmod p$$

má alespoň dvě řešení x_1 a x_2, která jsou inkongruentní podle modulu p. Bude tedy

$$a_0 x_1 + a_1 \equiv 0 \bmod p,$$
$$a_0 x_1 + a_1 \equiv 0 \bmod p.$$

Odečtením těchto kongruencí dostaneme

$$a_0(x_1 - x_2) \equiv 0 \bmod p.$$

Poněvadž však $x_1 - x_2 \not\equiv 0 \bmod p$, bude podle věty 13 $a_0 \equiv 0 \bmod p$. Odtud a ze vztahu $a_0 x_1 + a_1 \equiv 0 \bmod p$ pak plyne, že též $a_1 \equiv 0 \bmod p$. Ježto

$$a_0 \equiv 0 \bmod p,$$
$$a_1 \equiv 0 \bmod p,$$

dostaneme podle věty 17, že pro každé celé číslo x platí

$$a_0 x + a_1 \equiv 0 \bmod p.$$

Tím jsme dokázali, že tvrzení věty je správné pro $n = 1$.

Předpokládejme nyní, že věta 35 platí pro jisté přirozené číslo n. Dokážeme, že z tohoto předpokladu plyne její správnost i pro přirozené číslo $n + 1$.

Nechť

$$P_{n+1}(x) = a_0 x^{n+1} + a_1 x^n + a_2 x^{n-1} + \ldots + a_{n-1} x^2 + a_n x + a_{n+1}$$

a nechť kongruence $(n + 1)$-tého stupně o jedné neznámé

$$P_{n+1}(x) \equiv 0 \bmod p \tag{66}$$

má alespoň $n + 2$ řešení $x_1, x_2, \ldots, x_{n+1}, x_{n+2}$, která jsou vzájemně inkongruentní podle modulu p. Platí tedy

$$P_{n+1}(x_i) \equiv 0 \bmod p \ (i = 1, 2, \ldots, n + 1, n + 2), \tag{67}$$

přičemž pro $i \neq k$ $(i, k = 1, 2, \ldots, n + 1, n + 2)$ bude

$$x_i \not\equiv x_k \bmod p. \tag{68}$$

Poněvadž tedy

$$P_{n+1}(x_{n+2}) \equiv 0 \bmod p,$$

bude pro všechna celá čísla x platit

$$P_{n+1}(x) \equiv P_{n+1}(x) - P_{n+1}(x_{n+2}) \bmod p. \tag{69}$$

Avšak

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = a_0(x^{n+1} - x_{n+2}^{n+1}) + a_1(x^n - x_{n+2}^n) + \\ + a_2(x^{n-1} - x_{n+2}^{n-1}) + \ldots + a_{n-2}(x^3 - x_{n+2}^3) + \\ + a_{n-1}(x^2 - x_{n+2}^2) + a_n(x - x_{n+2}).$$

Poněvadž platí

$$x^{n+1} - x_{n+2}^{n+1} = (x - x_{n+2})(x^n + x_{n+2}x^{n-1} + x_{n+2}^2x^{n-2} + \\ + \ldots + x_{n+2}^{n-1}x + x_{n+2}^n),$$

$$x^n - x_{n+2}^n = (x - x_{n+2})(x^{n-1} + x_{n+2}x^{n-2} + x_{n+2}^2x^{n-3} + \\ + \ldots + x_{n+2}^{n-2}x + x_{n+2}^{n-1}),$$

$$x^{n-1} - x_{n+2}^{n-1} = (x - x_{n+2})(x^{n-2} + x_{n+2}x^{n-3} + x_{n+2}^2x^{n-4} +$$

$$+ \ldots + x_{n+2}^{n-3}x + x_{n+2}^{n-2}),$$
$$\vdots$$
$$x^3 - x_{n+2}^3 = (x - x_{n+2})(x^2 + x_{n+2}x + x_{n+2}^2),$$
$$x^2 - x_{n+2}^2 = (x - x_{n+2})(x + x_{n+2}),$$

můžeme dále psát

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = (x - x_{n+2})[a_0(x^n + x_{n+2}x^{n-1} + x_{n+2}^2x^{n-2} + \ldots + x_{n+2}^{n-1}x + x_{n+2}^n) + a_1(x^{n-1} + x_{n+2}x^{n-2} + x_{n+2}^2x^{n-3} + \ldots + x_{n+2}^{n-2}x + x_{n+2}^{n-1}) + a_2(x^{n-2} + x_{n+2}x^{n-3} + x_{n+2}^2x^{n-4} + \ldots + x_{n+2}^{n-3}x + x_{n+2}^{n-2}) + \ldots + a_{n-2}(x^2 + x_{n+2}x + x_{n+2}^2) + a_{n-1}(x + x_{n+2}) + a_n].$$

Avšak x_{n+2} je známé číslo. Proto výraz v hranaté závorce bude opět polynom v proměnné x. V tomto polynomu najdeme nejvýše n-tou mocninu proměnné x, přičemž koeficient u x^n je a_0. Půjde tedy o polynom n-tého stupně a označíme-li jej $P_n(x)$, dostaneme konečně

$$P_{n+1}(x) - P_{n+1}(x_{n+2}) = (x - x_{n+2})\,P_n(x).$$

Po dosazení tohoto výsledku do (69) tedy obdržíme

$$P_{n+1}(x) \equiv (x - x_{n+2})\,P_n(x) \bmod p. \qquad (70)$$

Dosadíme-li do tohoto vztahu za x postupně čísla x_1, x_2, ..., x_{n+1}, dostaneme vzhledem k (67)

$$(x_i - x_{n+2})\,P_n(x_i) \equiv 0 \bmod p \quad (i = 1, 2, \ldots, n+1),$$

odkud vzhledem k (68) podle věty 13 plyne, že

$$P_n(x_i) \equiv 0 \bmod p \quad (i = 1, 2, \ldots, n+1).$$

Z toho vidíme, že kongruence n-tého stupně o jedné neznámé $P_n(x) \equiv 0 \bmod p$ má alespoň $n + 1$ řešení $x_1, x_2, \ldots, x_{n+1}$, která jsou vzájemně inkongruentní podle modulu p. Poněvadž jsme předpokládali, že věta 35 platí pro přirozené číslo n, bude tedy pro všechna celá čísla x platit $P_n(x) \equiv 0 \bmod p$. Ze vztahu (70) pak plyne, že pro všechna celá čísla x platí též

$$P_{n+1}(x) \equiv 0 \bmod p,$$

což jsme chtěli dokázat.

Ukážeme si dva zajímavé důsledky věty 35. Prvním z nich bude

věta 36. *Budiž $P_n(x)$ polynom n-tého stupně a nechť existuje celé číslo x_0 tak, že $P_n(x_0) \not\equiv 0 \bmod p$. Potom kongruence n-tého stupně o jedné neznámé s prvočíselným modulem*

$$P_n(x) \equiv 0 \bmod p$$

má nejvýše n řešení, která jsou vzájemně inkongruentní podle modulu p.

Důkaz této věty provedeme nepřímo. Kdyby kongruence n-tého stupně o jedné neznámé $P_n(x) \equiv 0 \bmod p$ měla více než n řešení vzájemně inkongruentních podle modulu p, platilo by podle věty 35 $P_n(x) \equiv 0 \bmod p$ pro všechna celá čísla x. To však by byl spor s předpokladem $P_n(x_0) \not\equiv 0 \bmod p$. Proto může daná kongruence mít nejvýše n řešení vzájemně inkongruentních podle modulu p, což jsme měli dokázat.

Druhým důsledkem věty 35 je

věta 37. *Pro každé prvočíslo p platí*

$$(p-1)! + 1 \equiv 0 \bmod p. \tag{71}$$

Důkaz. Pro $p = 2$ je vztah (71) zřejmě správný, neboť $(2-1)! + 1 = 2$ a $2 \equiv 0 \bmod 2$.

Předpokládejme tedy, že p je liché prvočíslo, a utvořme polynom

$$Q(x) = (x-1).(x-2). \ldots .(x-p+1) - x^{p-1} + 1.$$

Snadno nahlédneme, že v tomto polynomu je koeficient u x^{p-1} roven nule a koeficient u x^{p-2} roven číslu $-\frac{p(p-1)}{2}$. Stupeň polynomu $Q(x)$ je tedy $p-2$.

Zvolíme-li za ξ kterékoliv z čísel $1, 2, \ldots, p-1$, dostaneme $Q(\xi) = -\xi^{p-1} + 1$. Pro tato ξ je však podle (38)

$$\xi^{p-1} \equiv 1 \bmod p,$$

takže

$$Q(\xi) \equiv 0 \bmod p.$$

Čísla $1, 2, \ldots, p-1$ tedy představují $p-1$ řešení kongruence $Q(x) \equiv 0 \bmod p$ vzájemně inkongruentních podle tohoto modulu. Poněvadž stupeň kongruence $Q(x) \equiv 0 \bmod p$ je $p-2$, platí podle věty 35 vztah $Q(x) \equiv 0 \bmod p$ pro každé celé číslo x. Položíme-li nyní $x = 0$, dostaneme

$$(-1).(-2). \ldots .(-(p-1)) + 1 \equiv 0 \bmod p.$$

Poněvadž p je liché prvočíslo, plyne z posledního vztahu ihned vztah (71), což jsme měli dokázat.

Vztah (71) bývá v teorii čísel nazýván Wilsonovou

větou. Poprvé byl uveřejněn ve Waringově pojednání *Meditationes Algebraicae* v roce 1770.

Porovnáme-li věty 12 a 13 z kapitoly 2, dále příklad 37 a větu 36 a konečně úlohu 9 (kapitola 3) a větu 37, zjistíme, že věty 13, 36 a 37 jsou charakteristickými pro kongruence s prvočíselnými moduly, neboť neplatí pro kongruence s moduly složenými. Z vět 14 a 36 je mimoto zřejmé, že kongruence s prvočíselnými moduly mají ve srovnání s kongruencemi se složenými moduly další vlastnosti, které jsou analogické s vlastnostmi rovností resp. algebraických rovnic.

V další části této kapitoly se budeme podrobněji zabývat kvadratickými kongruencemi o jedné neznámé s prvočíselným modulem. Celkem jednoduchá a málo zajímavá situace nastává pro $p = 2$. Proto se budeme věnovat pouze studiu kvadratických kongruencí tvaru

$$a_0x^2 + a_1x + a_2 \equiv 0 \bmod p, \tag{72}$$

kde p je liché prvočíslo, přičemž $p \nmid a_0$.

Nejprve budeme studovat speciální kvadratické kongruence tvaru

$$x^2 - a \equiv 0 \bmod p, \tag{73}$$

kde a je dané číslo.

Příklad 38. Vyšetřte kvadratické kongruence o jedné neznámé:

a) $x^2 - 5 \equiv 0 \bmod 11$;

b) $x^2 - 7 \equiv 0 \bmod 11$.

Řešení. Probíhá-li x úplnou soustavou zbytků $\{0, 1, 2, \ldots, 10\}$ podle modulu 11, bude podle tohoto modulu číslo x^2 postupně kongruentní s čísly 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1. Z toho je patrné, že $4^2 - 5 \equiv 0 \bmod 11$,

$7^2 - 5 \equiv 0 \bmod 11$. Dále vidíme, že pro každé celé x z dané úplné soustavy zbytků je $x^2 - 7 \not\equiv 0 \bmod 11$.

Odpověď.

a) Kongruence $x^2 - 5 \equiv 0 \bmod 11$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 10\}$ podle modulu 11 dvě řešení $x_1 = 4$ a $x_2 = 7$.

b) Kongruence $x^2 - 7 \equiv 0 \bmod 11$ nemá žádné řešení.

Předpokládejme, že $p \nmid a$ a že x_1 je řešením kongruence (73). Položme $x_2 = p - x_1$. Protože $x_2^2 = p^2 - 2px_1 + x_1^2$, vidíme, že $x_2^2 \equiv x_1^2 \bmod p$ a tedy též $x_2^2 - a \equiv x_1^2 - a \equiv 0 \bmod p$. Číslo x_2 je proto rovněž řešením kongruence (73). Dokážeme si ještě, že řešení x_1 a x_2 jsou podle modulu p inkongruentní. Kdyby totiž bylo $x_1 \equiv x_2 \bmod p$, měli bychom po dosazení za x_2 $x_1 \equiv p - x_1 \bmod p$, z čehož pak by plynulo $2x_1 \equiv 0 \bmod p$. Protože p je liché prvočíslo, dostali bychom z tohoto vztahu konečně $x_1 \equiv 0 \bmod p$, takže by bylo též $a \equiv x_1^2 \equiv 0 \bmod p$. To by však bylo ve sporu s předpokladem, že $p \nmid a$. Proto řešení x_1 a $x_2 = p - x_1$ jsou podle modulu p inkongruentní.

Jestliže $p \mid a$, přejde kongruence (73) v triviální kongruenci $x^2 \equiv 0 \bmod p$, jejíž jediné řešení v úplné soustavě zbytků $\{0, 1, 2, \ldots, p - 1\}$ je $x_1 = 0$.

Z této úvahy a příkladů 38a) a b) tedy plyne, že kvadratická kongruence (73) nemá buďto žádné řešení, nebo má v každé úplné soustavě zbytků podle modulu p jedno řešení, nebo konečně má v každé úplné soustavě zbytků podle modulu p dvě řešení vzájemně inkongruentní podle tohoto modulu. Z věty 36 pak plyne, že žádná jiná možnost nemůže nastat.

Zabývejme se nyní otázkou, kdy kongruence (73) má řešení. Přitom není třeba vyšetřovat případy, kdy $p|a$, neboť pro $p|a$ má zmíněná kongruence vždy řešení $x_1 \equiv 0 \bmod p$.

Definice 11. *Nechť* $(a, p) = 1$. *Má-li kongruence* (73) *řešení, nazýváme číslo* a *kvadratickým zbytkem podle modulu* p. *Nemá-li kongruence* (73) *řešení, nazýváme číslo* a *kvadratickým nezbytkem podle modulu* p.

Příklad 39. Najděte všechny kvadratické zbytky a všechny kvadratické nezbytky podle modulu 17 z redukované soustavy zbytků $\{0, 1, 2, \ldots, 16\}$ podle tohoto modulu.

Řešení. Necháme-li x probíhat redukovanou soustavou zbytků $\{1, 2, 3, \ldots, 16\}$ podle modulu 17, bude x^2 kongruentní podle modulu 17 postupně s čísly 1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1. Kvadratickými zbytky podle modulu 17 budou tedy čísla 1, 2, 4, 8, 9, 13, 15, 16, kvadratickými nezbytky pak čísla 3, 5, 6, 7, 10, 11, 12 a 14.

Věta 38. *Nechť* p *je liché prvočíslo. Potom v každé redukované soustavě zbytků podle modulu* p *je právě* $\frac{p-1}{2}$ *kvadratických zbytků a* $\frac{p-1}{2}$ *kvadratických nezbytků podle modulu* p.

Důkaz. Budeme hledat kvadratické zbytky ležící v redukované soustavě zbytků $\{1, 2, 3, \ldots, p-1\}$ podle modulu p. Probíhá-li číslo x touto redukovanou soustavou, budou kvadratické zbytky podle modulu p ležet v těch zbytkových třídách podle tohoto modulu, ve kterých leží čísla $1^2, 2^2, 3^2, \ldots, (p-1)^2$. Libovolný reprezentant kterékoliv z těchto tříd bude tedy kvadra-

tickým zbytkem podle modulu p, takže pro stanovení počtu kvadratických zbytků stačí určit, kolik z těchto tříd je navzájem různých.

Snadno nahlédneme, že probíhá-li x postupně čísly $1, 2, 3, \ldots, \frac{p-1}{2}$, bude výraz $p - x$ probíhat až na pořadí zbývajícími čísly redukované soustavy zbytků $\{1, 2, 3, \ldots, p-1\}$. Poněvadž dále $(p-x)^2 \equiv x^2 \bmod p$, leží čísla x^2 a $(p-x)^2$ vždy ve stejné zbytkové třídě podle modulu p (srovnej s příkladem 39), takže se můžeme omezit na stanovení počtu vzájemně různých zbytkových tříd podle modulu p, ve kterých leží čísla

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Dokážeme si, že tyto třídy jsou vzájemně různé.

Předpokládejme, že existují přirozená čísla x_1 a x_2 tak, že

$$x_1^2 \equiv x_2^2 \bmod p, \tag{74}$$

přičemž platí

$$\left.\begin{aligned} 1 \leqq x_1 \leqq \frac{p-1}{2}, \\ 1 \leqq x_2 \leqq \frac{p-1}{2}. \end{aligned}\right\} \tag{75}$$

Z kongruence (74) plyne, že $x_1^2 - x_2^2 \equiv 0 \bmod p$, tj. že

$$(x_1 + x_2)(x_1 - x_2) \equiv 0 \bmod p. \tag{76}$$

Sečtením obou nerovností (75) dostaneme dále

$$2 \leqq x_1 + x_2 \leqq p - 1 < p,$$

takže podle výsledku úlohy 2 bude $p \nmid (x_1 + x_2)$. Z kon-

gruence (76) pak podle věty 13 plyne, že $x_1 \equiv x_2 \bmod p$. Odtud pak vzhledem k nerovnostem (75) dostaneme podle věty 14 rovnost $x_1 = x_2$.

Jestliže tedy čísla x_1 a x_2 vyhovují nerovnostem (75) a je $x_1 \neq x_2$, nemůže být $x_1^2 \equiv x_2^2 \bmod p$, takže zbytkové třídy podle modulu p, ve kterých leží čísla 1^2, 2^2, 3^2, ..., $\left(\frac{p-1}{2}\right)^2$, jsou vzájemně různé. Počet kvadratických zbytků podle modulu p je roven počtu těchto tříd, tj. číslu $\frac{p-1}{2}$. V redukované soustavě zbytků $\{1, 2, 3, \ldots, p-1\}$ je tedy $\frac{p-1}{2}$ kvadratických zbytků podle modulu p. Zbývající čísla této soustavy, kterých je $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$, jsou tudíž kvadratickými nezbytky podle modulu p, čímž máme větu 38 dokázánu.

Při počítání s kvadratickými kongruencemi je třeba umět rychle rozhodnout, zda dané číslo je kvadratickým zbytkem nebo nezbytkem podle modulu p. Existuje řada kritérií, podle kterých lze toto rozhodnutí učinit. Dokážeme si některá z nich.

Věta 39. *Budiž p liché prvočíslo a nechť $p \nmid a$. Potom platí:*

a) Číslo a je kvadratickým zbytkem podle modulu p právě tehdy, je-li

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p. \tag{77}$$

b) Číslo a je kvadratickým nezbytkem podle modulu p právě tehdy, je-li

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p. \tag{78}$$

Důkaz. Vyšetřme nejprve kongruenci

$$u^{p-1} - 1 \equiv 0 \bmod p. \tag{79}$$

Poněvadž pro $u_0 = 0$ je $-1 \not\equiv 0 \bmod p$, má tato kongruence podle věty 36 nejvýše $p - 1$ řešení, která jsou vzájemně inkongruentní podle modulu p. Avšak podle (38) bude řešením kongruence (79) každé z čísel 1, 2, 3, ..., $p - 1$, takže kongruence (79) má právě $p - 1$ řešení, která jsou vzájemně inkongruentní podle modulu p.

Poněvadž p je liché prvočíslo, je číslo $\frac{p-1}{2}$ celé, takže kongruenci (79) můžeme přepsat ve tvaru

$$(u^{\frac{p-1}{2}} - 1)(u^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p.$$

Podle věty 13 tedy pro každé celé číslo u, které vyhovuje tomuto vztahu, platí buďto

$$u^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p, \tag{80}$$

nebo

$$u^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p. \tag{81}$$

Vztahy (80) a (81) nemohou platit současně, neboť v opačném případě bychom jejich odečtením dostali $-2 \equiv 0 \bmod p$, což není možné.

Každé řešení kongruence (79) je tedy řešením právě jedné z kongruencí (80) a (81). To znamená, že každá z těchto kongruencí má právě $\frac{p-1}{2}$ řešení, která jsou vzájemně inkongruentní podle modulu p.

Nechť nyní číslo a je kvadratickým zbytkem podle modulu p. Potom podle definice 11 má kongruence (73) řešení x_1. Poněvadž $p \nmid a$, platí též $p \nmid x_1$, takže podle (38) bude $x_1^{p-1} \equiv 1 \bmod p$. Ze vztahu $x_1^2 \equiv a \bmod p$ pak podle (18) dostaneme $(x_1^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p$. Shrnutím těchto výsledků obdržíme konečně $a^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \bmod p$. Tím jsme dokázali, že pro každý kvadratický zbytek podle modulu p platí vztah (77), tj. každý kvadratický zbytek podle modulu p je řešením kongruence (80). Avšak kongruence (80) má právě tolik řešení, kolik je v dané redukované soustavě kvadratických zbytků podle modulu p (viz větu 38). Z toho plyne, že číslo a je kvadratickým zbytkem podle modulu p právě tehdy, je-li řešením kongruence (80), tj. platí-li vztah (77). Tím jsme dokázali tvrzení a).

Dokažme ještě tvrzení b). Protože každý kvadratický nezbytek podle modulu p je řešením kongruence (79), bude řešením právě jedné z kongruencí (80) a (81). Z dokázaného tvrzení a) plyne, že číslo a je kvadratickým nezbytkem podle modulu p právě tehdy, neplatí-li vztah (77), tj. není-li řešením kongruence (80). To je však možné právě tehdy, je-li řešením kongruence (81), tj. platí-li vztah (78). Tím máme dokázáno i tvrzení b).

Příklad 40. Určete, která z čísel 5, 20, 26 a 30 jsou kvadratickými zbytky a která jsou kvadratickými nezbytky podle modulu 41.

Řešení. Užitím známých pravidel pro počítání s kongruencemi, případně i užitím vztahu (38) dostaneme postupně:

a) $5^{20} = 25^{10}$, $25 \equiv -16 \bmod 41$, takže $5^{20} \equiv (-2^4)^{10} \bmod 41$, tj. $5^{20} \equiv 2^{40} \equiv 1 \bmod 41$;

b) $20^{20} = 2^{40}.5^{20}$, $2^{40} \equiv 1 \bmod 41$, $5^{20} \equiv 1 \bmod 41$, tedy $20^{20} \equiv 1 \bmod 41$;

c) $26^{20} = 2^{20}.13^{20} = 2^{20}.169^{10}$, $169 \equiv 5 \bmod 41$, $169^{10} \equiv 5^{10} \bmod 41$, $5^{10} \equiv (-16)^5 \bmod 41$, takže $26^{20} \equiv 2^{20}.(-16)^5 \bmod 41$, tj. $26^{20} \equiv -2^{40} \equiv -1 \bmod 41$;

d) $30^{20} \equiv (-11)^{20} \bmod 41$, $(-11)^{20} = 121^{10}$ a $121 \equiv -2 \bmod 41$, takže $30^{20} \equiv (-2)^{10} \bmod 41$; avšak $(-2)^{10} = 1024$ a $1024 \equiv -1 \bmod 41$, takže $30^{20} \equiv -1 \bmod 41$.

Odpověď. Čísla 5 a 20 jsou kvadratickými zbytky a čísla 26 a 30 kvadratickými nezbytky podle modulu 41.

Abychom nemuseli obšírně vypisovat „kvadratický zbytek podle modulu p" nebo „kvadratický nezbytek podle modulu p", zavádíme v teorii kvadratických kongruencí tzv. Legendreův symbol.

Definice 12. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Potom definujeme Legendreův symbol $\left(\frac{a}{p}\right)$ takto: Je-li a kvadratickým zbytkem podle modulu p, klademe $\left(\frac{a}{p}\right) = 1$. Je-li a kvadratickým nezbytkem podle modulu p, klademe $\left(\frac{a}{p}\right) = -1$.*

Z věty 39 a definice 12 plyne okamžitě

věta 40. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Potom*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p. \qquad (82)$$

Zavedením Legendreova symbolu můžeme tedy shrnout vzorce (77) a (78) do jediného vztahu (82). Pomocí tohoto vztahu si nyní dokážeme některá pravidla pro počítání s Legendreovým symbolem.

Věta 41. *Budiž p liché prvočíslo a nechť $(a, p) = (b, p) = 1$. Potom platí:*

a) Je-li $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, *je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

b) Je-li $a \equiv b \bmod p$, *je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

c)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \tag{83}$$

$$\left(\frac{a^2}{p}\right) = 1, \tag{84}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{85}$$

Důkaz tvrzení a). Poněvadž $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, bude prvočíslo p dělitelem výrazu $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right)$. Absolutní hodnota tohoto výrazu je však nejvýše rovna dvěma a protože $p > 2$, plyne z výsledku úlohy 2 a věty 2 (kapitola 1), že $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) = 0$. Tím jsme dokázali tvrzení a).

Důkaz tvrzení b). Z kongruence $a \equiv b \bmod p$ podle (18) plyne, že též $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \bmod p$. Podle (82) je však

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p,$$

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \bmod p.$$

Podle (11) tedy dostaneme $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \bmod p$, z čehož užitím tvrzení a) plyne správnost tvrzení b).

Důkaz tvrzení c). Poněvadž $(a, p) = (b, p) = 1$, bude i $(ab, p) = 1$, takže podle (82) bude

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \bmod p.$$

Avšak $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} . b^{\frac{p-1}{2}}$ a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$, $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \bmod p$, takže podle (17) dostaneme též

$$(ab)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p.$$

Shrnutím nalezených výsledků obdržíme pak podle (11), že platí $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p$. Odtud zcela stejně, jako při důkazu tvrzení a), plyne vztah (83).

Položíme-li v (83) speciálně $b = a$, dostaneme (84), neboť $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1$.

Vztah (85) dokážeme konečně ze vztahu (82) zcela stejně, jako jsme dokazovali tvrzení a).

Ukážeme si nyní na příkladě, jak lze věty 41 užít k určení hodnoty Legendreova symbolu.

Příklad 41. Určete a) $\left(\frac{2}{139}\right)$; b) $\left(\frac{35}{139}\right)$.

Řešení.

a) $$\left(\frac{2}{139}\right) = \left(\frac{2}{139}\right)^7 = \left(\frac{128}{139}\right) = \left(\frac{-11}{139}\right) =$$

$$= \left(\frac{-1}{139}\right) \cdot \left(\frac{11}{139}\right) = -\left(\frac{11}{139}\right) = -\left(\frac{150}{139}\right) =$$

$$= -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right) \cdot \left(\frac{25}{139}\right) = -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right), \text{ tj.}$$

$$\left(\frac{2}{139}\right) = -\left(\frac{2}{139}\right) \cdot \left(\frac{3}{139}\right).$$

Z tohoto vztahu tedy vypočteme $\left(\frac{3}{139}\right) = -1$. Dále pak bude

$$\left(\frac{2}{139}\right) = \left(\frac{2}{139}\right) \cdot \left(\frac{4}{139}\right) = \left(\frac{8}{139}\right) = \left(\frac{147}{139}\right) =$$

$$= \left(\frac{3}{139}\right) \cdot \left(\frac{49}{139}\right) = \left(\frac{3}{139}\right) = -1.$$

b) $$\left(\frac{35}{139}\right) = \left(\frac{35}{139}\right) \cdot \left(\frac{4}{139}\right) = \left(\frac{140}{139}\right) = \left(\frac{1}{139}\right) = 1.$$

Odpověď. a) $\left(\frac{2}{139}\right) = -1$; b) $\left(\frac{35}{139}\right) = 1$.

Dokážeme si ještě jedno kritérium, podle něhož lze principiálně velmi jednoduše rozhodnout, zda číslo a z redukované soustavy zbytků podle modulu p je kvadratickým zbytkem či kvadratickým nezbytkem podle

tohoto modulu. Při zápisu opět s výhodou použijeme Legendreova symbolu.

Věta 42. *Budiž p liché prvočíslo a nechť $(a, p) = 1$. Buďte dále $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{\frac{p-1}{2}}$ absolutně nejmenší zbytky při dělení prvočíslem p utvořené postupně k číslům $1.a$, $2.a$, $3.a$, $\ldots$, $\frac{p-1}{2}.a$. Nechť konečně ν značí počet záporných čísel ležících v systému $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{\frac{p-1}{2}}$.*

Potom

$$\left(\frac{a}{p}\right) = (-1)^{\nu}. \tag{86}$$

Důkaz. Nechť k je některé z čísel $1, 2, 3, \ldots, \frac{p-1}{2}$. Podle věty 5 existují k danému číslu k celá čísla ξ_k a ϱ_k tak, že platí

$$k.a = \xi_k p + \varrho_k,$$

$$-\frac{p}{2} \leqq \varrho_k < \frac{p}{2}.$$

Bude tedy

$$ak \equiv \varrho_k \bmod p \quad \left(k = 1, 2, 3, \ldots, \frac{p-1}{2}\right). \tag{87}$$

Poněvadž p je liché prvočíslo, budou celá čísla ϱ_k splňovat dokonce ostré nerovnosti $-\frac{p}{2} < \varrho_k < \frac{p}{2}$, takže

$$|\varrho_k| < \frac{p}{2} \quad \left(k = 1, 2, 3, \ldots, \frac{p-1}{2}\right). \tag{88}$$

Předpokládejme, že $1 \leqq h \leqq \frac{p-1}{2}$, $1 \leqq k \leqq \frac{p-1}{2}$ a že $|\varrho_h| = |\varrho_k|$. Z této rovnosti plyne, že též $\varrho_h^2 = \varrho_k^2$, takže vzhledem ke vztahům (87) dostaneme dále $a^2h^2 \equiv a^2k^2 \bmod p$. Ježto $p \nmid a$, můžeme podle věty 11 v této kongruenci krátit číslem a^2, takže dostaneme $h^2 \equiv k^2 \bmod p$, tj. $h^2 - k^2 \equiv 0 \bmod p$. Avšak poslední kongruenci můžeme psát ve tvaru

$$(h + k)(h - k) \equiv 0 \bmod p. \tag{89}$$

Sečteme-li dále nerovnosti pro čísla h a k, dostaneme

$$2 \leqq h + k \leqq p - 1 < p,$$

takže musí platit $p \nmid (h + k)$. Podle věty 13 pak z kongruence (89) plyne, že $h - k \equiv 0 \bmod p$ neboli $h \equiv k \bmod p$. Odtud podle věty 14 dostaneme $h = k$.

Jestliže tedy $|\varrho_h| = |\varrho_k|$, je nutně $h = k$. Z toho pak plyne, že pro $h \neq k$ bude též $|\varrho_h| \neq |\varrho_k|$. Proto čísla $|\varrho_1|, |\varrho_2|, |\varrho_3|, \ldots, |\varrho_{\frac{p-1}{2}}|$ budou vzájemně různá. Žádné z nich nebude rovno nule, neboť v opačném případě bychom podle (87) dostali, že buďto $p|a$, nebo $p|k$, což by odporovalo předpokladu o číslech a a k. Vzhledem k nerovnostem (88) bude tedy $\frac{p-1}{2}$ čísel $|\varrho_1|$, $|\varrho_2|$, $|\varrho_3|$, $\ldots$, $|\varrho_{\frac{p-1}{2}}|$ nabývat až na pořadí hodnot $1, 2, 3, \ldots, \frac{p-1}{2}$, takže bude

$$\varrho_1\varrho_2\varrho_3 \ldots \varrho_{\frac{p-1}{2}} = (-1)^{\left(\frac{p-1}{2}\right)}!. \tag{90}$$

Znásobíme-li nyní mezi sebou všechny kongruence (87), dostaneme

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \varrho_1\varrho_2\varrho_3 \ldots \varrho_{\frac{p-1}{2}} \bmod p;$$

dosadíme-li do této kongruence podle (90), obdržíme

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\nu}\left(\frac{p-1}{2}\right)! \bmod p.$$

Poněvadž $p \nmid \left(\frac{p-1}{2}\right)!$, můžeme podle věty 11 v této kongruenci krátit číslem $\left(\frac{p-1}{2}\right)!$, takže dostaneme

$$a^{\frac{p-1}{2}} \equiv (-1)^{\nu} \bmod p.$$

Odtud vzhledem k (82) plyne, že

$$\left(\frac{a}{p}\right) \equiv (-1)^{\nu} \bmod p,$$

z čehož stejným postupem, jako při důkazu tvrzení a) věty 41, dostaneme dokazovaný vztah (86).

Větu, kterou jsme právě dokázali, nazýváme v teorii čísel Gaussovým lematem.

Příklad 42. Užitím Gaussova lematu určete a) $\left(\frac{5}{41}\right)$; b) $\left(\frac{26}{41}\right)$.

Řešení. a) Pro $a = 5$ budeme hledat absolutně nejmenší zbytky při dělení číslem 41 postupně k číslům 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100. Tyto zbytky budou rovny číslům 5, 10, 15, 20, —16, —11, —6, —1, 4, 9, 14, 19, —17, —12, —7, —2, 3, 8, 13 a 18. Je tedy $\nu = 8$, takže podle (86) bude $\left(\frac{5}{41}\right) = 1$.

b) Podobně pro $a = 26$ budeme hledat absolutně nejmenší zbytky při dělení číslem 41 postupně pro čísla 26, 52, 78, 104, 130, 156, 182, 208, 234, 260, 286, 312, 338, 364, 390, 416, 442, 468, 494, 520. Tyto zbytky budou rovny číslům —15, 11, —4, —19, 7, —8, 18, 3, —12, 14, —1, —16, 10, —5, —20, 6, —9, 17, 2 a —13. V tomto případě je $\nu = 11$, takže podle (86) dostaneme $\left(\frac{26}{41}\right) = -1$.

Odpověď. a) $\left(\frac{5}{41}\right) = 1$; b) $\left(\frac{26}{41}\right) = -1$.

Doposud jsme se zabývali otázkou, kdy má kongruence (73) řešení. Tuto otázku dovedeme úplně zodpovědět, neboť pro $p \nmid a$ umíme určit hodnotu Legendreova symbolu $\left(\frac{a}{p}\right)$ a tím i rozhodnout o existenci řešení kongruence (73), a pro $p|a$ umíme dokonce toto řešení přímo napsat.

Obraťme nyní pozornost k otázce, jak v případě, kdy kongruence (73) má řešení, lze toto řešení zkonstruovat. Na rozdíl od kvadratických rovnic je u kvadratických kongruencí tento problém v obecném případě mnohem komplikovanější. Avšak v některých speciálních případech už nám vyložená teorie stačí k tomu, abychom řešení kongruence (73) sestrojili.

Jeden dosti obecný případ, ve kterém dovedeme řešení kongruence (73) sestrojit, popisuje

věta 43. *Nechť* $p \equiv 3 \bmod 4$ *a nechť* $\left(\frac{a}{p}\right) = 1$. *Potom pro řešení* x_1 *kvadratické kongruence* (73) *platí*

$$x_1 \equiv a^{\frac{p+1}{4}} \bmod p. \tag{91}$$

Důkaz. Exponent $\frac{p+1}{4}$ je celé číslo, neboť z předpokladu $p \equiv 3 \bmod 4$ plyne, že $p + 1 \equiv 0 \bmod 4$. Podle (91) je dále $x_1^2 - a \equiv a^{\frac{p+1}{2}} - a \bmod p$. Avšak

$$a^{\frac{p+1}{2}} - a = -a^{\frac{p+1}{2}}\left(a^{\frac{p-1}{2}} - 1\right) =$$

$$= -a^{\frac{p+1}{2}}\left[a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right)\right].$$

Poněvadž z (82) plyne, že $a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right) \equiv 0 \bmod p$, dostaneme shrnutím těchto výsledků $x_1^2 - a \equiv 0 \bmod p$. Vidíme, že číslo x_1 definované vztahem (91) je skutečně řešením kongruence (73).

Druhé řešení x_2 kongruence (73) určíme pak snadno ze vztahu $x_2 \equiv p - x_1 \bmod p$.

Příklad 43. Vyšetřte kvadratickou kongruenci

$$x^2 - 35 \equiv 0 \bmod 59.$$

Řešení. Především zjistíme, zda daná kongruence má řešení. K tomu musíme určit hodnotu Legendreova symbolu $\left(\frac{35}{59}\right)$. Podle věty 41 postupně dostaneme

$$\left(\frac{35}{59}\right) = \left(\frac{-24}{59}\right) = \left(\frac{-6}{59}\right)\cdot\left(\frac{4}{59}\right) = \left(\frac{-6}{59}\right) =$$

$$= \left(\frac{-6}{59}\right)\cdot\left(\frac{9}{59}\right) = \left(\frac{-54}{59}\right) = \left(\frac{5}{59}\right) = \left(\frac{64}{59}\right) = \left(\frac{1}{59}\right) = 1.$$

Daná kongruence má tedy v každé redukované soustavě zbytků podle modulu 59 dvě řešení.

Poněvadž $59 \equiv 3 \bmod 4$, bude podle (91)

$$x_1 \equiv 35^{15} \bmod 59.$$

Avšak $35^{15} = 5^{15}.7^{15}$, $5^3 \equiv 7 \bmod 59$, $5^{15} \equiv 7^5 \bmod 59$, takže $x_1 \equiv 35^{15} \equiv 7^{20} \bmod 59$. Dále je $7^2 \equiv -10 \bmod 59$ a tedy $7^{20} \equiv 10^{10} \bmod 59$. Poněvadž $10^3 \equiv -3 \bmod 59$, dostaneme konečně $x_1 \equiv 7^{20} \equiv 10^{10} \equiv 10.(-3)^3 \equiv 25 \bmod 59$.

Pro druhé řešení dané kongruence pak dostaneme $x_2 \equiv 59 - 25 \bmod 59$, tj. $x_2 \equiv 34 \bmod 59$.

Odpověď. Kvadratická kongruence $x^2 - 35 \equiv 0 \bmod 59$ má v redukované soustavě zbytků $\{1, 2, 3, \ldots, 58\}$ podle modulu 59 dvě řešení, $x_1 = 25$ a $x_2 = 34$.

Věta 43 nám umožňuje konstruovat řešení kvadratické kongruence (73) pro prvočíselné moduly tvaru $p = 4m + 3$ (m celé). Postupu, jehož jsme při konstrukci řešení užili, lze však někdy užít i v případě, že prvočíslo p má tvar $p = 4m + 1$.

Nechť $p \equiv 1 \bmod 4$ a nechť $\left(\frac{a}{p}\right) = 1$. Hledejme nejmenší přirozené číslo k, pro které platí $a^k \equiv 1 \bmod p$. Víme už, že takové číslo jistě existuje. Podle věty 29 bude dokonce $k \mid (p - 1)$.

Je-li číslo k liché, bude $k + 1$ sudé a položíme-li

$$x_1 \equiv a^{\frac{k+1}{2}} \bmod p, \tag{92}$$

dostaneme $x_1^2 - a \equiv a^{k+1} - a \bmod p$. Avšak $a^{k+1} - a = a(a^k - 1)$ a $a^k - 1 \equiv 0 \bmod p$, takže konečně obdržíme $x_1^2 - a \equiv 0 \bmod p$. Vidíme-li, že číslo x_1 definované vztahem (92) je opět řešením kongruence (73).

Je-li však číslo k sudé, nelze tohoto postupu užít.

Nicméně i pro tyto případy lze řešení kongruence (73) zkonstruovat $\left(\text{přirozeně za předpokladu, že } \left(\frac{a}{p}\right) = 1\right)$. Konstrukce je však příliš komplikovaná a přesahuje rámec této knihy. Proto se jí nebudeme zabývat a omezíme se v těchto případech na stanovení řešení dané kvadratické kongruence jen zkusmo.

Obecně tedy dovedeme zkonstruovat řešení kvadratické kongruence (73) jen v těch případech, kdy buďto $p \equiv 3 \bmod 4$, nebo mezi lichými děliteli čísla $p - 1$ existuje takové číslo k, pro které je $a^k \equiv 1 \bmod p$.

Příklad 44. Vyšetřte kvadratickou kongruenci

$$x^2 - 28 \equiv 0 \bmod 53.$$

Řešení. Nejprve budeme zkoumat, zda daná kongruence má řešení. Zřejmě bude

$$\left(\frac{28}{53}\right) = \left(\frac{81}{53}\right) = 1,$$

takže kongruence má v každé redukované soustavě zbytků podle modulu 53 dvě řešení.

Poněvadž $53 \equiv 1 \bmod 4$, budeme hledat mezi lichými děliteli čísla $53 - 1 = 52$ číslo k takové, že $28^k \equiv 1 \bmod 53$. Lichými děliteli čísla 52 jsou však pouze čísla 1 a 13. Postupně určíme

$28^2 \equiv -11 \bmod 53,$

$28^4 \equiv 121 \equiv 15 \bmod 53,$

$28^6 \equiv -11.15 \equiv -6 \bmod 55,$

$28^{12} \equiv 36 \bmod 53,$

$28^{13} \equiv 36.28 \equiv 1 \bmod 53.$

Podle (92) tedy bude

$$x_1 \equiv 28^7 \equiv -6.28 \equiv 6.25 \equiv 44 \bmod 53.$$

Položíme-li ještě $x_2 = 53 - 44 = 9$, vidíme, že daná kongruence má v redukované soustavě zbytků $\{1, 2, 3, \ldots, 52\}$ podle modulu 53 dvě řešení, $x_1 = 44$ a $x_2 = 9$.

Příklad 45. Najděte všechna řešení kvadratické kongruence $x^2 \equiv 20 \bmod 41$ v úplné soustavě zbytků $\{0, 1, 2, \ldots, 40\}$ podle modulu 41.

Řešení. V příkladu 40 jsme zjistili, že $\left(\frac{20}{41}\right) = 1$. Daná kongruence bude proto mít ve zvolené úplné soustavě zbytků dvě inkongruentní řešení. (Tato řešení budou dokonce z odpovídající redukované soustavy.)

Poněvadž $41 \equiv 1 \bmod 4$, nelze ke konstrukci těchto řešení užít věty 43. Lichými děliteli čísla $41 - 1 = 40$ jsou pouze čísla 1 a 5. Přitom

$$20^2 \equiv -10 \bmod 41,$$

$$20^4 \equiv 100 \equiv 18 \bmod 41,$$

$$20^5 \equiv 18.20 \equiv -9 \bmod 41,$$

$$20^{10} \equiv 81 \equiv -1 \bmod 41,$$

$$20^{20} \equiv 1 \bmod 41.$$

Vidíme, že $20^5 \not\equiv 1 \bmod 41$. Poněvadž přirozenými děliteli čísla 40 jsou pouze čísla 1, 2, 4, 5, 8, 10 a 20 a poněvadž $20^8 \equiv 324 \equiv -4 \bmod 41$, je číslo $k = 20$ nejmenším přirozeným číslem, pro které platí $20^k \equiv 1 \bmod 41$.

Nelze tedy užít ani vztahu (92) a řešení dané kongruence bude proto třeba hledat zkusmo. Studujme

prvky zbytkové třídy podle modulu 41, ve které leží číslo 20. Zřejmě bude

$$20 \equiv 61 \equiv 102 \equiv 143 \equiv 184 \equiv 225 \bmod 41,$$

takže bude též $x^2 \equiv 225 \bmod 41$, tj. $x^2 \equiv 15^2 \bmod 41$. Jedno řešení vyšetřované kongruence bude tedy $x_1 = 15$, druhé pak dostaneme ze vztahu $x_2 = 41 - 15 = 26$.

Odpověď. Hledaná řešení kongruence $x^2 \equiv 20 \bmod 41$ jsou $x_1 = 15$, $x_2 = 26$.

Ke konstrukci řešení některých speciálních kvadratických kongruencí lze někdy užít i jiných vět, které jsme si vyložili. Jako ukázku si uvedeme příklad, kde ke konstrukci řešení využijeme Wilsonovy věty (věta 37).

Příklad 46. Nechť p je prvočíslo tvaru $p = 4m + 1$. Užitím Wilsonovy věty dokažte, že kongruence $x^2 + 1 \equiv 0 \bmod p$ má řešení

$$x_{1,2} \equiv \pm(2m)! \bmod p.$$

Řešení. Protože

$(2m)! = 1.2.3. \ldots .2m = (-1).(-2).(-3). \ldots . (-2m)$ a pro $k = 1, 2, 3, \ldots, 2m$ platí

$$-k \equiv p - k \bmod p,$$

dostaneme vynásobením všech těchto kongruencí

$$(2m)! \equiv (p-1).(p-2).(p-3). \ldots .(p-2m) \bmod p.$$

Znásobíme-li tuto kongruenci číslem $(p - 2m - 1)!$, dostaneme

$$(2m)!.(p - 2m - 1)! \equiv (p-1)! \bmod p.$$

Avšak $p - 2m - 1 = 4m + 1 - 2m - 1 = 2m$, takže bude

$$((2m)!)^2 \equiv (p-1)! \bmod p.$$

Odtud užitím vztahu (71) dostaneme

$$((2m)!)^2 \equiv -1 \bmod p$$

neboli

$$((2m)!)^2 + 1 \equiv 0 \bmod p.$$

Poněvadž $x_1^2 \equiv x_2^2 \equiv ((2m)!)^2 \bmod p$, obdržíme konečně

$$x_1^2 + 1 \equiv 0 \bmod p,$$
$$x_2^2 + 1 \equiv 0 \bmod p.$$

Čísla x_1 a x_2 budou tedy skutečně řešeními kongruence $x^2 + 1 \equiv 0 \bmod p$, což jsme měli dokázat.

Závěrem této kapitoly se ještě stručně zmíníme o obecné kvadratické kongruenci s prvočíselným modulem

$$a_0x^2 + a_1x + a_2 \equiv 0 \bmod p, \qquad (72)$$

kde p je liché prvočíslo, $p \nmid a_0$. Postup, jehož při studiu takovéto kongruence užíváme, je zcela obdobný s postupem užívaným při řešení kvadratických rovnic.

Poněvadž p je liché prvočíslo a $p \nmid a_0$, platí též, že $p \nmid 4a_0$. Vynásobíme-li tedy kongruenci (72) číslem $4a_0$, dostaneme ekvivalentní kongruenci

$$4a_0^2x^2 + 4a_0a_1x + 4a_0a_2 \equiv 0 \bmod p.$$

Doplníme-li levou stranu této kongruence na úplný čtverec a označíme-li $D = a_1^2 - 4a_0a_2$ diskriminant kvadratického trojčlenu $a_0x^2 + a_1x + a_2$, dostaneme po jednoduché úpravě kongruenci

$$(2a_0x + a_1)^2 - D \equiv 0 \bmod p,$$

která je rovněž ekvivalentní s kongruencí (72). Položme ještě

$$2a_0x + a_1 \equiv z \mod p. \tag{93}$$

Dostaneme tak kvadratickou kongruenci

$$z^2 - D \equiv 0 \mod p, \tag{94}$$

která už má tvar (73). Ze vztahu (93) plyne, že každému řešení kongruence (72) odpovídá právě jedno řešení kongruence (94). Poněvadž však $p \nmid 2a_0$, lze i obráceně z lineární kongruence (93) ke každému řešení kongruence (94) najít právě jedno řešení kongruence (72).

Nechť dvěma řešením x_1 a x_2 kongruence (72) odpovídají řešení z_1 a z_2 kongruence (94). Bude tedy

$$2a_0x_1 + a_1 \equiv z_1 \mod p,$$
$$2a_0x_2 + a_1 \equiv z_2 \mod p.$$

Je-li $x_1 \equiv x_2 \mod p$, plyne z těchto vztahů, že i $z_1 \equiv z_2 \mod p$. Je-li obráceně $z_1 \equiv z_2 \mod p$, bude $2a_0x_1 + a_1 \equiv 2a_0x_2 + a_1 \mod p$, takže $2a_0x_1 \equiv 2a_0x_2 \mod p$. Poněvadž $(2a_0, p) = 1$, plyne z této kongruence podle věty 11, že $x_1 \equiv x_2 \mod p$. Tím jsme dokázali, že řešení x_1 a x_2 kongruence (72) jsou kongruentní podle modulu p právě tehdy, jsou-li podle tohoto modulu kongruentní odpovídající řešení z_1 a z_2 kongruence (94).

Z provedených úvah vyplývá, že kvadratické kongruence (72) a (94) jsou ekvivalentní. Postup, který jsme si právě popsali, nám tedy vždy umožní rozhodnout o existenci řešení kongruence (72) a určit počet inkongruentních řešení této kongruence. V těch případech, kdy dovedeme najít řešení kongruence (94), jím dokonce dostaneme řešení kongruence (72). V ně-

kterých konkrétních případech však můžeme tento postup ještě značně zjednodušit.

Příklad 47. Vyšetřte kvadratickou kongruenci

$$57x^2 + 149x + 362 \equiv 0 \bmod 211.$$

Řešení. Pro diskriminant D kvadratického trojčlenu $57x^2 + 149x + 362$ dostaneme $D = 149^2 - 4.57.362$. Snadno zjistíme, že $149^2 - 4.57.362 \equiv (-62)^2 + 17.60 \bmod 211$, tj. $D \equiv 3844 + 1020 \equiv 11 \bmod 211$. Dostaneme tedy ekvivalentní kongruenci

$$z^2 - 11 \equiv 0 \bmod 211.$$

Abychom rozhodli o existenci řešení této kongruence, určíme hodnotu Legendreova symbolu $\left(\frac{11}{211}\right)$. Podle známých pravidel bude

$$\left(\frac{11}{211}\right) = \left(\frac{-200}{211}\right) = \left(\frac{-2}{211}\right)\cdot\left(\frac{100}{211}\right) = \left(\frac{-2}{211}\right) =$$

$$= \left(\frac{-2}{211}\right)\cdot\left(\frac{81}{211}\right) = \left(\frac{-162}{211}\right) = \left(\frac{49}{211}\right) = 1,$$

takže kongruence $z^2 - 11 \equiv 0 \bmod 211$ bude mít dvě řešení inkongruentní podle modulu 211. Poněvadž $211 \equiv 3 \bmod 4$, bude podle věty 43

$$z_1 \equiv 11^{53} \bmod 211.$$

Postupně vypočteme

$11^2 \equiv -90 \bmod 211$,

$11^4 \equiv 8100 \equiv 82 \bmod 211$,

$11^8 \equiv 6724 \equiv -28 \bmod 211$,

$11^{16} \equiv 784 \equiv -60 \bmod 211$,

$11^{48} \equiv -216\,000 \equiv 64 \bmod 211$,

$11^{52} \equiv 64.82 \equiv -27 \bmod 211$ a

$11^{53} \equiv -27.11 \equiv 125 \bmod 211$.

Řešení kongruence $z^2 - 11 \equiv 0 \bmod 211$ tedy budou $z_1 \equiv 125 \bmod 211$ a $z_2 \equiv 211 - 125 \equiv 86 \bmod 211$. Podle (93) dostaneme pro řešení původní kongruence

$$114x_1 + 149 \equiv 125 \bmod 211,$$
$$114x_2 + 149 \equiv 86 \bmod 211.$$

Po úpravě a zkrácení šesti resp. třemi dostaneme dále

$$19x_1 \equiv -4 \bmod 211, \quad 38x_2 \equiv -21 \bmod 211.$$

Znásobíme-li první kongruenci jedenácti, dostaneme $209x_1 \equiv -44 \bmod 211$ neboli $-2x_1 \equiv -44 \bmod 211$, z čehož po zkrácení číslem -2 plyne ihned $x_1 \equiv 22 \bmod 211$. Druhou kongruenci můžeme přepsat ve tvaru $38x_2 \equiv 190 \bmod 211$, z čehož po zkrácení číslem 38 plyne $x_2 \equiv 5 \bmod 211$.

Odpověď. Kongruence $57x^2 + 149x + 362 \equiv 0 \bmod 211$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 210\}$ podle modulu 211 dvě řešení, $x_1 = 22$ a $x_2 = 5$.

Ukážeme si ještě jiný způsob řešení této kongruence. Řešme nejprve lineární kongruenci $57u \equiv 1 \bmod 211$. Podle (46) dostaneme pro její řešení $u_1 \equiv 57^{209} \bmod 211$. Postupně vypočteme

$57^2 \equiv 84 \bmod 211$,

$57^4 \equiv 7056 \equiv 93 \bmod 211$,

$57^8 \equiv 8649 \equiv -2 \bmod 211$,

$57^{40} \equiv -32 \bmod 211$,

$57^{80} \equiv 1024 \equiv -31 \bmod 211,$

$57^{160} \equiv 961 \equiv -94 \bmod 211,$

$57^{200} \equiv (-32).(-94) \equiv 54 \bmod 211,$

$57^{208} \equiv -2.54 \equiv 103 \bmod 211$ a

$57^{209} \equiv 57.103 \equiv -37 \bmod 211.$

Řešení lineární kongruence $57u \equiv 1 \bmod 211$ bude tedy $u_1 \equiv -37 \bmod 211$.

Znásobme nyní původní kvadratickou kongruenci $57x^2 + 149x + 362 \equiv 0 \bmod 211$ číslem -37. Dostaneme tak kvadratickou kongruenci s ní ekvivalentní

$$-2109x^2 - 5513x - 13\,394 \equiv 0 \bmod 211.$$

Tuto kongruenci můžeme podle věty 17 psát v ekvivalentním tvaru

$$x^2 - 27x - 101 \equiv 0 \bmod 211$$

nebo ještě výhodněji ve tvaru

$$x^2 + 184x - 101 \equiv 0 \bmod 211,$$

neboť v této kongruenci můžeme bez dalších úprav doplnit její levou stranu na úplný čtverec. Dostaneme tak

$$(x + 92)^2 - 92^2 - 101 \equiv 0 \bmod 211$$

nebo po úpravě

$$(x + 92)^2 - 125 \equiv 0 \bmod 211.$$

Tato kongruence je zřejmě ekvivalentní s kongruencí původní, a položíme-li ještě $x + 92 = v$, dostaneme opět kvadratickou kongruenci tvaru (73)

$$v^2 - 125 \equiv 0 \bmod 211.$$

Pro Legendreův symbol $\left(\frac{125}{211}\right)$ dostaneme snadno

$$\left(\frac{125}{211}\right) = \left(\frac{5}{211}\right)^3 = \left(\frac{5}{211}\right) = \left(\frac{5}{211}\right)\cdot\left(\frac{9}{211}\right) =$$
$$= \left(\frac{45}{211}\right) = \left(\frac{256}{211}\right) = \left(\frac{16}{211}\right)^2 = 1,$$

takže kongruence $v^2 - 125 \equiv 0 \bmod 211$ má dvě inkongruentní řešení. Podle věty 43 dostaneme jedno z těchto řešení ve tvaru

$$v_1 \equiv 125^{53} \bmod 211.$$

Postupně vypočteme

$125^2 \equiv 11 \bmod 211,$
$125^4 \equiv 121 \equiv -90 \bmod 211,$
$125^8 \equiv 8100 \equiv 82 \bmod 211,$
$125^{12} \equiv -90.82 \equiv 5 \bmod 211,$
$125^{48} \equiv 625 \equiv -8 \bmod 211,$
$125^{52} \equiv (-8).(-90) \equiv 87 \bmod 211$ a
$125^{53} \equiv 125.87 \equiv 114 \bmod 211.$

Bude tedy $v_1 \equiv 114 \bmod 211$ a $v_2 \equiv 211 - 114 \equiv 97 \bmod 211$. Ze vztahu $x + 92 = v$ určíme nyní už snadno řešení původní kvadratické kongruence $x_1 \equiv 114 - 92 \equiv 22 \bmod 211$ a $x_2 \equiv 97 - 92 \equiv 5 \bmod 211$.

Příklad 48. Vyšetřte kvadratickou kongruenci

$$6x^2 - 5x + 21 \equiv 0 \bmod 97.$$

Řešení. Diskriminant kvadratického trojčelnu $6x^2 -$

$-5x + 21$ je $D = 25 - 4.6.21 = -479$, tedy $D \equiv 6 \bmod 97$. Snadno zjistíme, že

$$\left(\frac{6}{97}\right) = \left(\frac{6}{97}\right) \cdot \left(\frac{16}{97}\right) = \left(\frac{96}{97}\right) = \left(\frac{-1}{97}\right) = 1.$$

Kongruence $z^2 - 6 \equiv 0 \bmod 97$ i kongruence původní budou tedy mít dvě inkongruentní řešení.

Poněvadž $97 \equiv 1 \bmod 4$, nemůžeme ke konstrukci řešení kvadratické kongruence $z^2 - 6 \equiv 0 \bmod 97$ užít věty 43. Nelze však užít ani vztahu (92), neboť $6^2 \equiv 36 \bmod 97$, $6^3 \equiv 22 \bmod 97$, $6^4 \equiv 35 \bmod 97$, $6^6 \equiv -1 \bmod 97$, $6^8 \equiv -36 \bmod 97$ a $6^{12} \equiv 1 \bmod 97$, takže nejmenší přirozené číslo k, pro které platí $6^k \equiv 1 \bmod 97$, je sudé.

Znásobíme-li kongruenci $z^2 - 6 \equiv 0 \bmod 97$ šestnácti, dostaneme ekvivalentní kongruenci $16z^2 - 96 \equiv 0 \bmod 97$, kterou můžeme napsat ve tvaru $(4z)^2 \equiv -1 \bmod 97$. Protože jsme zjistili, že $6^6 \equiv -1 \bmod 97$, můžeme dále psát

$$(4z)^2 \equiv (6^3)^2 \bmod 97,$$

z čehož dostaneme $4z_1 \equiv 216 \bmod 97$, $4z_2 \equiv -216 \bmod 97$. Po zkrácení čtyřmi tedy bude $z_1 \equiv 54 \bmod 97$, $z_2 \equiv -54 \equiv 43 \bmod 97$. Tím jsme našli obě inkongruentní řešení kongruence $z^2 - 6 \equiv 0 \bmod 97$.

Abychom určili řešení x_1 a x_2 původní kvadratické kongruence, budeme řešit ještě dvě lineární kongruence. Podle (93) bude

$$12x_1 - 5 \equiv 54 \bmod 97, \quad 12x_2 - 5 \equiv 43 \bmod 97,$$

tj.

$$12x_1 \equiv 59 \bmod 97, \quad 12x_2 \equiv 48 \bmod 97.$$

Násobíme-li první kongruenci osmi, dostaneme $96x_1 \equiv$

$\equiv 472 \bmod 97$ neboli $-x_1 \equiv -13 \bmod 97$, takže bude $x_1 \equiv 13 \bmod 97$. Krátíme-li ve druhé kongruenci dvanácti, dostaneme ihned $x_2 \equiv 4 \bmod 97$.

Odpověď. Kvadratická kongruence $6x^2 - 5x + 21 \equiv 0 \bmod 97$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 96\}$ podle modulu 97 dvě řešení, $x_1 = 13$ a $x_2 = 4$.

Příklad 49. Vyšetřte kvadratickou kongruenci

$$73x^2 - 115x + 48 \equiv 0 \bmod 113.$$

Řešení. Diskriminant daného kvadratického trojčlenu bude $D = 115^2 - 4.73.48$. Snadno zjistíme, že $D \equiv 2^2 + 47.48 \equiv 0 \bmod 113$, takže kvadratická kongruence (94) má v každé úplné soustavě zbytků podle modulu 113 jediné řešení $z_1 \equiv 0 \bmod 113$. Kongruence (93) má v tomto případě tvar $146x_1 - 115 \equiv 0 \bmod 113$ neboli $33x_1 \equiv 2 \bmod 113$. Podle (46) dostaneme řešení této lineární kongruence ve tvaru $x_1 \equiv 2.33^{111} \bmod 113$. Postupně tedy vypočteme

$33^2 \equiv -41 \bmod 113$,

$33^4 \equiv 1681 \equiv -14 \bmod 113$,

$33^8 \equiv 196 \equiv -30 \bmod 113$,

$33^{16} \equiv 900 \equiv -4 \bmod 113$,

$33^{32} \equiv 16 \bmod 113$,

$33^{64} \equiv 256 \equiv 30 \bmod 113$,

$33^{96} \equiv 16.30 \equiv 28 \bmod 113$,

$33^{104} \equiv -30.28 \equiv -49 \bmod 113$,

$33^{108} \equiv (-14).(-49) \equiv 8 \bmod 113$,

$33^{110} \equiv -41.8 \equiv 11 \bmod 113$,

$33^{111} \equiv 33.11 \equiv 24 \bmod 113$,

z čehož dostaneme $x_1 \equiv 2.33^{111} \equiv 48 \bmod 113$.

Odpověď. Vyšetřovaná kongruence má v úplné soustavě zbytků $\{0, 1, 2, \ldots, 112\}$ podle modulu 113 jediné řešení $x_1 = 48$.

Příklad 50. Vyšetřte kvadratickou kongruenci

$$68x^2 - 291x - 50 \equiv 0 \bmod 53.$$

Řešení. Podle věty 17 vyšetříme ekvivalentní kvadratickou kongruenci

$$15x^2 - 26x + 3 \equiv 0 \bmod 53.$$

Diskriminant kvadratického trojčlenu $15x^2 - 26x + 3$ je $D = 26^2 - 4.15.3 = 676 - 180 = 496$, takže $D \equiv$ $\equiv 19 \bmod 53$. Podle (82) je $\left(\frac{19}{53}\right) \equiv 19^{26} \bmod 53$ a poněvadž $19^{26} = (19^2)^{13} = 361^{13}$ a $361 \equiv -10 \bmod 53$, určíme postupně

$10^3 \equiv -7 \bmod 53$,

$10^6 \equiv 49 \equiv -4 \bmod 53$,

$10^{12} \equiv 16 \bmod 53$ a

$10^{13} \equiv 160 \equiv 1 \bmod 53$.

Dostaneme tedy

$$\left(\frac{19}{53}\right) \equiv 361^{13} \equiv (-10)^{13} \equiv -10^{13} \equiv -1 \bmod 53.$$

Vidíme, že diskriminant D je kvadratickým nezbytkem podle modulu 53.

Odpověď. Kvadratická kongruence $68x^2 - 291x - 50 \equiv 0 \bmod 53$ nemá žádné řešení.

Úlohy

21. Určete hodnoty Legendreových symbolů: a) $\left(\frac{322}{307}\right)$; b) $\left(\frac{623}{179}\right)$; c) $\left(\frac{62}{83}\right)$; d) $\left(\frac{-10}{659}\right)$.

V následujících příkladech vyšetřte kvadratické kongruence:

22. $x^2 \equiv 43 \bmod 109$.

23. $x^2 - 90 \equiv 0 \bmod 83$.

24. $x^2 + 48 \equiv 0 \bmod 59$.

25. $67x^2 - 91x + 35 \equiv 0 \bmod 71$.

26. $177x^2 - 47x + 928 \equiv 0 \bmod 353$.

27. $196x^2 + 1456x + 2753 \equiv 0 \bmod 571$.

28. Užitím Gaussova lematu dokažte, že pro liché prvočíslo p platí

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

29. Nechť $p > 2$ je prvočíslo a nechť $p \mid m$. Dokažte, že kongruence $(p-1)$-tého stupně o jedné neznámé

$$x^{p-1} + 1 \equiv 0 \bmod m$$

nemá žádné řešení.

VÝSLEDKY ÚLOH

1. a) $x = -6$; $r = 61$; $\xi = -5$; $\varrho = -4$.
   b) $x = 22$; $r = 6$; $\xi = 22$; $\varrho = 6$.
   c) $x = 0$; $r = 12$; $\xi = 0$; $\varrho = 12$.
   d) $x = -1$; $r = 23$; $\xi = 0$; $\varrho = -12$.

2. Podle definice 2 existuje celé číslo $x \neq 0$ tak, že $a = mx$. Poněvadž $|x| \geqq 1$, bude $|a| = |x|.m \geqq m$.

3. Plyne z definice největšího společného dělitele a úlohy 2.

4. Poněvadž $215 \equiv 5 \bmod 21$ a $79 \equiv -5 \bmod 21$, bude podle (18) $215^{20} \equiv 5^{20} \bmod 21$ a $79^{36} \equiv (-5)^{36} \bmod 21$, takže podle (17) a (16) dostaneme $5.215^{20} - 79^{36} \equiv 5^{20} - (-5)^{36} \bmod 21$. Avšak $5^{20} - (-5)^{36} = 5^{20}(1 - 5^{6}) = 5^{20}(1 - 125^{2})$. Protože $125 \equiv -1 \bmod 21$, bude opět podle (18) $125^{2} \equiv (-1)^{2} \bmod 21$, z čehož dostaneme $1 - 125^{2} \equiv 0 \bmod 21$. Podle (17) tedy bude $5^{20}(1 - 125^{2}) \equiv 0 \bmod 21$. Shrnutím nalezených výsledků dostaneme pak podle (11) $5.215^{20} - 79^{36} \equiv 0 \bmod 21$, tj. dané číslo je dělitelno číslem 21.

5. a) $r = 38$.
   b) $r = 25$.

6. Pro každé celé $k \geqq 1$ je $10^{k} \equiv 0 \bmod 2$, $10^{k} \equiv 0 \bmod 5$ a $10^{k} \equiv 0 \bmod 10$. Podobně pro každé celé $k \geqq 2$ bude $10^{k} \equiv 0 \bmod 4$ a $10^{k} \equiv 0 \bmod 25$ a konečně pro každé celé $k \geqq 3$ bude $10^{k} \equiv 0 \bmod 8$. Užitím dekadického zápisu (19) přirozeného čísla n plyne z posledních kongruencí

podle (17) a (15) $n \equiv a_0 \bmod 2$, $n \equiv a_0 \bmod 5$, $n \equiv a_0 \bmod 10$, $n \equiv (10a_1 + a_0) \bmod 4$, $n \equiv (10a_1 + a_0) \bmod 25$ a $n \equiv (10^2 a_2 + 10a_1 + a_0) \bmod 8$. Z toho vidíme, že o dělitelnosti přirozeného čísla n dvěma, pěti nebo desíti můžeme rozhodnout podle poslední cifry, o dělitelnosti 4 nebo 25 pomocí posledního dvojčíslí a o dělitelnosti 8 pomocí posledního trojčíslí dekadického rozvoje tohoto čísla.

7. a) Pro $n = 2k + 1$ je $n^2 = 4k^2 + 4k + 1$, tedy $n^2 \equiv 1 \bmod 4$, tj. $n^2 \in A_1^{(4)}$.

   b) Poněvadž $3 \nmid n$, bude buďto $n \equiv 1 \bmod 3$, nebo $n \equiv 2 \bmod 3$. Podle (18) bude tedy v prvním případě $n^2 \equiv 1 \bmod 3$ a ve druhém pak $n^2 \equiv 4 \equiv 1 \bmod 3$. V obou případech máme $n^2 \equiv 1 \bmod 3$, tj. $n^2 \in A_1^{(3)}$.

8. a) $a = 1, 5, 7, 11, 13, 17.$
   $k = 1, 6, 3, 6, 3, 2.$

   b) $a = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$
   $k = 1, 6, 6, 2, 6, 6, 6, 3, 2, 6, 3, 2.$

9. Nechť lze složené číslo m psát ve tvaru součinu $m = m_1 m_2$, kde $m_1 > 1$, $m_2 > 1$ a $(m_1, m_2) = 1$. Poněvadž $m_1 > 1$, bude $m_2 = \frac{m}{m_1} < m$. Obdobně bude i $m_1 < m$. Mezi čísly 1, 2, 3, ..., $m - 1$ bude tedy jistě ležet číslo m_1 i číslo m_2. Poněvadž $(m - 1)! = 1.2.3. \ldots .(m - 1)$, vidíme, že bude platit $(m - 1)! \equiv 0 \bmod m_1$ i $(m - 1)! \equiv 0 \bmod m_2$. Ježto $(m_1, m_2) = 1$, bude podle věty 20 též $(m - 1)! \equiv 0 \bmod m$.

   Nechť složené číslo m nemůžeme psát ve tvaru součinu dvou nesoudělných čísel větších než jedna. V tomto případě bude číslo m alespoň druhou mocninou jistého prvočísla p, tj. $m = p^\alpha$, kde $\alpha \geqq 2$. Na ní bude třeba rozlišit dva případy.

a) Nechť předně $p = 2$. Poněvadž $m > 4$, bude v tomto případě $\alpha \geqq 3$, takže mezi čísly 1, 2, 3, ..., $2^\alpha - 1$ leží jistě čísla $2^{\alpha-2}$ a $2^{\alpha-1}$. Můžeme proto psát $(2^\alpha - 1)! = 2^{\alpha-2}.2^{\alpha-1}.a = 2^{2\alpha-3}.a = 2^\alpha.2^{\alpha-3}.a$, kde a je jisté celé číslo. Protože $\alpha \geqq 3$, je i $2^{\alpha-3}$ celé číslo, takže z poslední rovnosti plyne $(2^\alpha - 1)! \equiv 0 \bmod 2^\alpha$.

b) Nechť nakonec $p \geqq 3$. Poněvadž $\alpha \geqq 2$, budou mezi čísly 1, 2, 3, ..., $p^\alpha - 1$ jistě ležet čísla $p^{\alpha-1}$ a $2p^{\alpha-1}$, takže můžeme najít opět celé číslo a tak, že platí $(p^\alpha - 1)! = p^{\alpha-1}.2p^{\alpha-1}.a = p^\alpha.p^{\alpha-2}.2a$. Poněvadž $\alpha \geqq 2$, bude číslo $p^{\alpha-2}$ rovněž celé, takže z poslední rovnosti ihned plyne, že $(p^\alpha - 1)! \equiv 0 \bmod p^\alpha$.

10. Položme $a = \underbrace{11\ldots1}_{p \text{ cifer}}$, $b = 123\,456\,789$.

Užijeme-li dekadického zápisu, dostaneme

$$a = 10^{p-1} + 10^{p-2} + \ldots + 10^2 + 10 + 1,$$

$$b = 10^8 + 2.10^7 + 3.10^6 + 4.10^5 + 5.10^4 + 6.10^3 + 7.10^2 + 8.10 + 9.$$

Dále snadno zjistíme, že platí

$$n = a.(10^{8p} + 2.10^{7p} + 3.10^{6p} + 4.10^{5p} + 5.10^{4p} + 6.10^{3p} + 7.10^{2p} + 8.10^p + 9) - b.$$

Podle (39) však bude $10^p \equiv 10 \bmod p$, takže podle (18) dostaneme, že pro každé přirozené k platí $10^{kp} \equiv 10^k \bmod p$.

Bude tedy

$$n \equiv a.(10^8 + 2.10^7 + 3.10^6 + 4.10^5 + 5.10^4 + 6.10^3 + 7.10^2 + 8.10 + 9) - b \bmod p$$

neboli

$$n \equiv ab - b \bmod p.$$

Podle př. 7 je číslo b dělitelno devíti, neboť $s(b) = 45$.

Je tedy $b = 9c$, takže dostaneme konečně

$$n \equiv 9(a - 1)c \bmod p.$$

Pro číslo a dále obdržíme vztah

$10a + 1 = 10^p + 10^{p-1} + 10^{p-2} + \ldots + 10^2 + 10 + 1$, tj.

$$10a + 1 = 10^p + a.$$

Odtud pak plyne, že $9a = 10^p - 1$ neboli $9(a - 1) = 10^p - 10$. Bude tedy

$$n \equiv (10^p - 10).c \bmod p.$$

Podle (39) je však $10^p - 10 \equiv 0 \bmod p$, takže dostáváme konečně $n \equiv 0 \bmod p$, tj. $p \mid n$.

11. a) $x \equiv 209 \bmod 311$;

b) $x \equiv 26 \bmod 243$;

c) $x \equiv 406 \bmod 420$.

12. $k = 8$; $x \equiv 51 \bmod 85$.

13. $k = 6$; $x \equiv 14 \bmod 65$.

14. a) Nechť ξ je řešením kongruence (43), tj. nechť $a\xi + b \equiv 0 \bmod m$. Poněvadž $d \mid m_1$, bude podle věty 18 též $a\xi + b \equiv 0 \bmod d$. Ježto však též $d \mid a$, bude $a\xi \equiv 0 \bmod d$. Z těchto kongruencí pak plyne, že $b \equiv 0 \bmod d$, což je proti předpokladu o číslu b.

b) Bez újmy na obecnosti se můžeme omezit na úplnou soustavu zbytků $\{0, 1, 2, \ldots, m - 1\}$ podle modulu m. Z předpokladů o číslech m, a, b a d plyne, že $d \mid m$, $d \mid a$ a $d \mid b$. Položíme-li $m_1 = \frac{m}{d}$, $a_1 = \frac{a}{d}$ a $b_1 = \frac{b}{d}$, bude zřejmě $(a_1, m_1) = 1$, takže kongruence $a_1 x + b_1 \equiv 0 \bmod m_1$ má v úplné soustavě zbytků $\{0, 1, 2, \ldots,$

$m_1 - 1\}$ právě jedno řešení ξ. Každé řešení této kongruence můžeme pak psát ve tvaru $x = \xi + km_1$, kde k je libovolné celé číslo. Z rovnosti $\frac{ax + b}{m} = \frac{a_1x + b_1}{m_1}$ však dále plyne, že každé řešení kongruence (43) je též řešením kongruence $a_1x + b_1 \equiv 0 \bmod m_1$ a obráceně. Proto každé řešení kongruence (43) má tvar $x = \xi + km_1$. Abychom dostali řešení kongruence (43) z úplné soustavy zbytků $\{0, 1, 2, \ldots, m - 1\}$ podle modulu m, musí být $0 \leqq \xi + km_1 < m$. Přitom je $0 \leqq \xi < m_1$, takže $-m_1 < -\xi \leqq 0$. Sečtením nerovností $0 \leqq \xi + km_1 < m$ a $-m_1 < -\xi \leqq 0$ dostaneme dále $-m_1 < km_1 < m = dm_1$, tj. $-1 < k < d$. Celé číslo k může nabývat pouze d hodnot 0, 1, 2, ..., $d - 1$, což jsme chtěli dokázat.

15. $x \equiv 406 \bmod 420$.

16. a) $x \equiv 1098 \bmod 1825$;
    b) $x \equiv 61\,571 \bmod 228\,150$.

17. a) V úplné soustavě zbytků $\{0, 1, 2, \ldots, 1088\}$ podle modulu 1089 má kongruence devět vzájemně inkongruentních řešení. Těmito řešeními jsou čísla 4, 125, 246, 367, 488, 609, 730, 851 a 972.
    b) V úplné soustavě zbytků $\{0, 1, 2, \ldots, 5858\}$ podle modulu 5859 má kongruence sedm řešení vzájemně inkongruentních podle tohoto modulu. Těmito řešeními jsou čísla 760, 1597, 2434, 3271, 4108, 4945 a 5782.

18. a) $x \equiv 21 \bmod 42$, $y \equiv 14 \bmod 42$, $z \equiv 10 \bmod 42$;
    b) $x \equiv 690 \bmod 910$, $y \equiv 507 \bmod 910$, $z \equiv 631 \bmod 910$.

19. a) $x = 53 + 625k$, $y = 62 + 731k$, k celé;
    b) $x = -111 + 337k$, $y = 35 - 106k$, k celé.

20. Označíme-li a obnos, který máme vyplatit, x počet třikorun a y počet desetikorun, dostaneme neurčitou rovnici

$$3x + 10y = a,$$

přičemž hledáme celá nezáporná čísla x a y, která této rovnici vyhovují. Poněvadž je $(3, 10) = 1$, můžeme najít řešení kongruence $10y \equiv a \bmod 3$. Jedno z řešení této kongruence je zřejmě $y_0 = a$. Položíme-li ještě $x_0 = \frac{a - 10y_0}{3} = -3a$, budou mít všechna řešení vyšetřované neurčité rovnice tvar $x = -3a + 10k$, $y = a - 3k$, kde k probíhá množinou všech celých čísel. Ke splnění podmínek $x \geqq 0$ a $y \geqq 0$ je třeba volit k tak, aby platilo současně

$$-3a + 10k \geqq 0, \quad a - 3k \geqq 0.$$

Pro celé číslo k tedy budeme mít nerovnosti

$$\frac{3a}{10} \leqq k \leqq \frac{a}{3}.$$

Snadno nahlédneme, že pro $a = 18$, 19 nebo 20 vyhovuje těmto nerovnostem jediné číslo $k = 6$, pro $a = 21$, 22 nebo 23 pouze $k = 7$, pro $a = 24$, 25 nebo 26 pouze $k = 8$ a konečně pro $a = 27$, 28 nebo 29 pouze $k = 9$. Pro $a = 30$ dostaneme $k = 9$ nebo $k = 10$, takže dané neurčitá rovnice s doplňujícími podmínkami $x \geqq 0$, $y \geqq 0$ bude mít v tomto případě dvě řešení.

Je-li $a > 30$, je $\frac{a}{3} - \frac{3a}{10} = \frac{a}{30} > 1$, takže mezi čísly $\frac{3a}{10}$ a $\frac{a}{3}$ včetně bude ležet vždy alespoň jedno celé číslo k. Pro tato čísla a má tedy vyšetřovaná neurčitá rovnice vždy alespoň jedno řešení požadovaných vlastností.

Jednoduchým výpočtem se můžeme přesvědčit, že pro $a = 1$, 2, 4, 5, 7, 8, 11, 14 nebo 17 nemá úloha žádné

řešení, neboť neexistuje celé číslo k vyhovující požadovaným nerovnostem. Např. pro $a = 17$ bychom pro celé číslo dostali podmínky $\frac{51}{10} \leqq k \leqq \frac{17}{3}$, tj. $5 < k < 6$, což nelze splnit.

21. a) $\left(\frac{322}{307}\right) = 1$; b) $\left(\frac{623}{179}\right) = -1$; c) $\left(\frac{62}{83}\right) = -1$; d) $\left(\frac{-10}{659}\right) = 1$.

22. $x_1 \equiv 32 \bmod 109$, $x_2 \equiv 77 \bmod 109$.

23. $x_1 \equiv 16 \bmod 83$, $x_2 \equiv 67 \bmod 83$.

24. Kvadratická kongruence nemá řešení.

25. $D \equiv 37 \bmod 71$; $x_1 \equiv 12 \bmod 71$; $x_2 \equiv 54 \bmod 71$.

26. $D \equiv 0 \bmod 353$; existuje jediné řešení $x_1 \equiv 47 \bmod 353$.

27. $D \equiv 412 \bmod 571$; kongruence nemá žádné řešení.

28. Sestrojíme absolutně nejmenší zbytky při dělení prvočíslem p postupně k číslům $2, 4, 6, \ldots, 2.\frac{p-1}{2}$. Nechť prvočíslo p má tvar $p = 4m + s$, kde $s = 1$ nebo $s = 3$. Potom pro $k = 1, 2, \ldots, m$ bude zřejmě $\xi_k = 0$, $\varrho_k = 2k$. Avšak pro $k = m + 1, m + 2, \ldots, \frac{p-1}{2}$ bude $\xi_k = 1$ a $\varrho_k = 2k - p$, tedy $2m + 2 - p \leqq \varrho_k \leqq -1$. Snadno zjistíme, že $2m + 2 - p = 2m + 2 - 4m - s = -2m + 2 - s = -\frac{p-s}{2} + 2 - s = -\frac{p}{2} + 2 - \frac{s}{2} > -\frac{p}{2}$, takže pro tato k bude skutečně $-\frac{p}{2} < \varrho_k < 0$. Bude proto

$$v = \frac{p-1}{2} - m = 2m + \frac{s-1}{2} - m = m + \frac{s-1}{2}.$$

Avšak

$$\frac{p^2-1}{8} - v = \frac{16m^2 + 8ms + s^2 - 1}{8} - m - \frac{s-1}{2} =$$

$$= 2m^2 + m(s-1) + \frac{s^2-1}{8} - \frac{s-1}{2}$$

a poněvadž pro $s = 1$ i pro $s = 3$ je $\frac{s^2-1}{8} - \frac{s-1}{2} = 0$ a $s - 1$ je v obou případech sudé číslo, bude

$$(-1)^{\frac{p^2-1}{8} - v} = 1.$$

Odtud a ze vztahu (86) plyne

$$\left(\frac{2}{p}\right) = (-1)^v = (-1)^{\frac{p^2-1}{8}}.$$

což bylo dokázat.

29. Důkaz provedeme nepřímý. Předpokládejme, že daná kongruence má řešení x_1. Bude tedy $x_1^{p-1} + 1 \equiv 0 \bmod m$. Poněvadž však $p|m$, bude podle věty 18 též

$$x_1^{p-1} + 1 \equiv 0 \bmod p. \tag{95}$$

Je-li $x_1 \equiv 0 \bmod p$, plyne z této kongruence $1 \equiv 0 \bmod p$, což není možné. Jestliže však $x_1 \not\equiv 0 \bmod p$, bude podle (38) $x_1^{p-1} + 1 \equiv 1 + 1 \bmod p$, takže z kongruence (95) plyne $2 \equiv 0 \bmod p$. To rovněž není možné, neboť $p > 2$.

V obou případech tedy docházíme ke sporu, čímž je tvrzení úlohy 29 dokázáno.

Literatura doporučená k dalšímu studiu

a) *Pro začátečníky*

[1] A. O. Gel'fond, *Neurčité rovnice*. Populární přednášky o matematice, sv. 6, SNTL, Praha 1956.

[2] K. Hruša, *Základní věty o dělitelnosti*. Brána k vědění, sv. 9, Praha 1950.

[3] J. Sedláček, *Co víme o přirozených číslech*. Škola mladých matematiků, sv. 2, 2. vydání, Mladá fronta, Praha 1965.

[4] F. Veselý, *O dělitelnosti čísel celých*. Škola mladých matematiků, sv. 14, Mladá fronta, Praha 1966.

[5] J. Vyšín, *Neurčité rovnice*. Brána k vědění, sv. 3, Praha 1949.

b) *Pro pokročilejší*

[6] V. Kořínek, *Základy algebry*. 2. vydání, ČSAV, Praha 1956.

[7] K. Rychlík, *Úvod do elementární číselné teorie*. 2. vydání, Přírodovědecké nakladatelství, Praha 1956.

OBSAH

1. Opakování základních pojmů o dělitelnosti – – – – 3
2. Kongruence a jejich základní vlastnosti – – – – – 10
3. Zbytkové třídy podle modulu m. Úplné a redukované soustavy zbytků podle modulu m – – – – 21
4. Kongruence o jedné neznámé. Lineární kongruence 43
5. Soustavy kongruencí o jedné neznámé s několika moduly – 55
6. Soustavy lineárních kongruencí o několika neznámých. Neurčité rovnice – – – – – – – – – – – – – 67
7. Kongruence vyšších stupňů o jedné neznámé. Kvadratické kongruence o jedné neznámé s prvočíselným modulem – – – – – – – – – – – – – – – – – 85
Výsledky úloh – – – – – – – – – – – – – – – – 125
Literatura – – – – – – – – – – – – – – – – – – 133

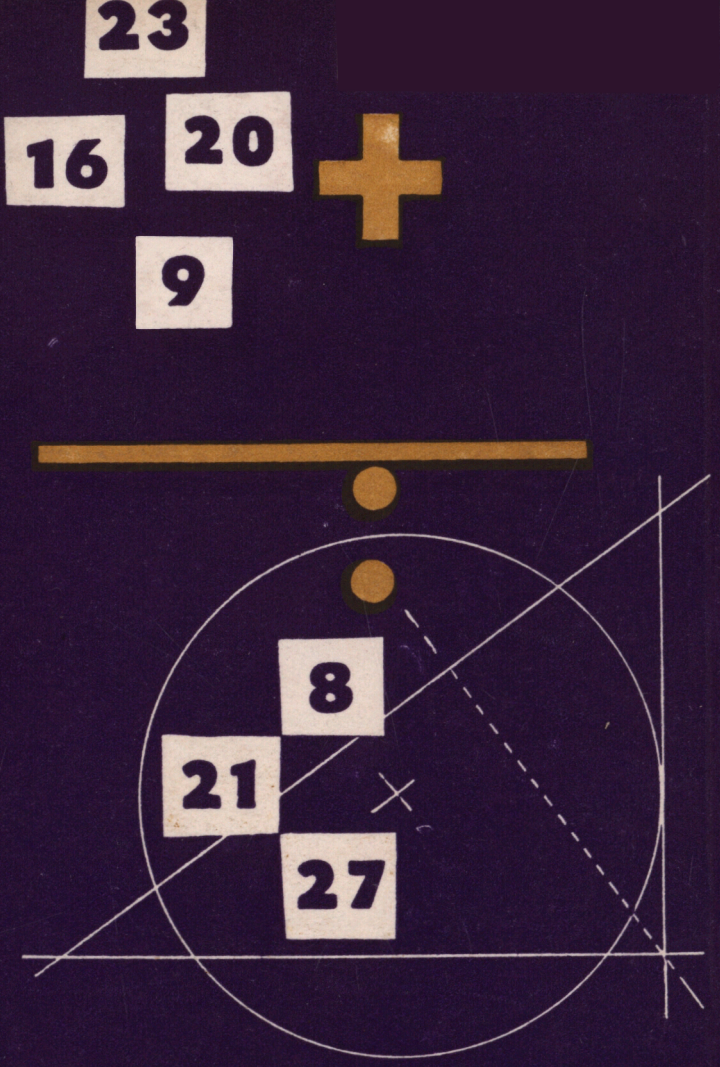
ŠKOLA MLADÝCH MATEMATIKŮ

kongruence

ALOIS APFELBECK

Pro účastníky matematické olympiády
vydává ÚV Matematické olympiády
a ÚV ČSM v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Obálku navrhl Jaroslav Příbramský
Odpovědný redaktor Milan Daneš
Publikace číslo 2694
Edice Škola mladých matematiků, svazek 21
Vytiskl Mír, novinářské závody, n. p.,
závod 1, Praha 1, Václavské nám. 15
4,84 AA, 5,01 VA. 136 stran
Náklad 5 700 výtisků. 1. vydání
Praha 1968. 507/21/8.5

23-105-68 03-2 Cena brož. výt. Kčs 6,—



23 - 105 - 68
03-2
Cena brož.
Kčs 6,—