6. kapitola. Soustavy lineárních kongruencí o několika neznámých. Neurčité rovnice

In: Alois Apfelbeck (author): Kongruence. (Czech). Praha: Mladá fronta, 1968. pp. 67–84.

Persistent URL: http://dml.cz/dmlcz/403658

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.