5. kapitola. Soustavy kongruencí o jedné neznámé s několika moduly

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) $7154x - 64\,337 \equiv 0 \bmod 5859$.