Kongruence

4. kapitola. Kongruence o jedné neznámé. Lineární kongruence

In: Alois Apfelbeck (author): Kongruence. (Czech). Praha: Mladá fronta, 1968. pp. 43–54.

Persistent URL: http://dml.cz/dmlcz/403656

Terms of use:

© Alois Apfelbeok, 1968

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

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 $45 \equiv$ $\equiv 0 \bmod 15$.

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 $6x + 9 \equiv 0 \bmod 15$.

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 $6x + 9 \equiv 0 \bmod 15$ 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 $6x + 5 \equiv \equiv 0 \bmod 15$.

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 převedli 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

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

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 $\xi \equiv 44 \equiv$ $\equiv 14 \bmod 15$.

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 možných 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 $1, 2, 3, \ldots, \varphi(m)$, 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

11 krátit 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. $y \equiv \equiv -5 \equiv 68 \bmod 73$. Číslo $\eta = 68$ bude tedy řešením kongruence $615y + 2199 \equiv 0 \bmod 73$, o čemž se můžeme přesvědčit zkouškou: $615\eta + 2199 = 615 \,.\, 68 + + 2199 = 41\,820 + 2199 = 44\,019 = 73 . 503$. Dosadíme-li za vypočtené η do pravé strany (48), dostaneme $(2199 + 615\eta) . 73^{319} = 603 . 73^{320}$ a poněvadž $73^{320} \equiv \equiv 1 \bmod 615$, bude $603 . 73^{320} \equiv 603 \bmod 615$, 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 $1815 = 3 . 5 . 11^2$ a $91 = 7 . 13$, je $(1815, 91) = 1$ a $\varphi(1815) = 2 . 4 . 11 . 10 = 880$. 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 $91x \equiv 653 \mod 1815$ je tedy $x = 1523$. O správnosti výsledku se přesvědčíme zkouškou: $91 \,.\, 1523 - 653 = 138\,593 - 653 = 137\,940 = 1815 \,.\, 76$.

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

Úlohy

11. Řešte lineární kongruence:

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

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

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

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

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