2. kapitola. Kongruence a jejich základní vlastnosti

In: Alois Apfelbeck (author): Kongruence. (Czech). Praha: Mladá fronta, 1968. pp. 10–20.

Persistent URL: http://dml.cz/dmlcz/403654

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.