Kongruence

1. kapitola. Opakování základních pojmů o dělitelnosti

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 $d \leqq |a_1|$, $d \leqq |a_2|$, $\ldots$, $d \leqq |a_k|$.