Neurčité rovnice

1. O dělitelnosti - Euklidův algoritmus

In: Jan Vyšín (author): Neurčité rovnice. (Czech). Praha: Jednota československých matematiků a fyziků, 1949. pp. 4–9.

Persistent URL: http://dml.cz/dmlcz/402866

I. O DĚLITELNOSTI — EUKLIDŮV ALGORITMUS

Čísly budeme v dalším rozuměti — nebude-li nic jiného řečeno — racionální celá čísla, t. j. čísla $0, \pm 1, \pm 2, \pm 3, \ldots$ Celá kladná čísla $1, 2, 3, \ldots$ nazýváme *přirozená čísla.* Napíšeme-li číslo x jako součin dvou čísel $x = yz$, je y (a ovšem též z) *dělitel* čísla x, x je *násobek* čísla y. Každé číslo x má jistě dělitele ± 1, $\pm x$. Přirozená čísla větší než jedna, která nemají mimo ± 1, $\pm x$ jiného dělitele, se nazývají *prvočísla.* Prvočísel je nekonečně mnoho, jejich řada začíná takto: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. Čísla, která nejsou prvočísly, se jmenují *čísla složená.* Nejjednodušší čísla složená jsou mocniny prvočísel, na př. $8 = 2^3$. Každé přirozené složené číslo, které není mocninou prvočísla, lze napsati jako součin mocnin prvočísel, na př. $360 = 2^3 . 3^2 . 5^1$: tato prvočísla se nazývají *prvočinitelé* daného čísla. Tento rozklad je *jednoznačný*, t. j. prvočinitelé i příslušní mocnitelé jsou daným číslem jednoznačně určeni.

Prováděli jste jistě všichni rozklad daného přirozeného čísla v součin mocnin prvočinitelů: užívá se při tom zkoumání dělitelnosti daného čísla prvočísly. Z rozkladu čísla v součin mocnin prvočinitelů vyplývá snadno tato vlastnost dělitelnosti, které budeme v dalším užívati: *je-li x dělitelem čísel a, b, je též dělitelem čísel $a + b$, $a - b$, $a . b$.*

Rozkladu čísla v součin mocnin prvočinitelů se používá při vyhledání *největšího společného dělitele* a *nejmenšího společného násobku* daných čísel. Máme-li na př. vyhledati největšího společného dělitele čísel 84, 264, 360, rozložíme tato čísla: $84 = 2^2 . 3 . 7$, $264 = 2^3 . 3 . 11$, $360 = 2^3 . 3^2 . 5$; vybereme prvočinitele společné všem číslům, a to v nejvyšší mocnině, v které jsou ve *všech* číslech obsaženy. V našem případě dostaneme $2^2, 3^1$; číslo $\delta = 12$ je největší společný dělitel daných tří čísel. Výpočet zapisujeme obyčejně schematicky do tabulky, jak jistě víte:

$$\begin{array}{rrr|ll}
84 & 264 & 360 & 2^2 & \\
21 & 66 & 90 & 3 & \delta = 2^2 . 3 \\
7 & 22 & 30 & &
\end{array}$$

Každý jiný dělitel daných čísel je dělitelem jejich největšího společného dělitele δ a je tedy menší než δ. To platí i pro dělitele záporné. Na př. v našem případě jsou takoví společní dělitelé čísla 4, 6.

Největšího společného dělitele dvou přirozených čísel můžeme najíti také cestou postupného dělení; té se sice při zvláštních číslech užívá zřídka, ale má význam pro algebraické výrazy. Probereme si číselný příklad.

Jsou dána dvě čísla přirozená, na př. 252, 858. Dělíme větší číslo menším:

$$\begin{array}{l} 858 : 252 = 3 \\ 102 \end{array}$$

Dělitele 252 dělíme pak zbytkem tohoto dělení, t. j. číslem 102:

$$\begin{array}{l} 252 : 102 = 2 \\ 48 \end{array}$$

Dále dělíme dělitele 102 zbytkem druhého dělení, t. j. číslem 48:

$$\begin{array}{l} 102 : 48 = 2 \\ 6 \end{array}$$

Konečně při dalším dělení

$$\begin{array}{l} 48 : 6 = 8 \\ 0 \end{array}$$

vyjde zbytek 0; tím postupné dělení končí. Poslední nenulový zbytek 6 je největší společný dělitel čísel 252, 858, jak si snadno přímo ověříte.

Uvedené postupné dělení si poznamenáme do tabulky:

$$\begin{array}{rr|c} 858 & 252 & 3 \\ 252 & 102 & 2 \\ 102 & 48 & 2 \\ 48 & 6 & 8 \\ & 0 & \end{array}$$

Každá řádka znamená jedno dělení; vedle sebe jsou napsány dělenec a dělitel, vpravo od svislé čáry podíl, pod dělitele zbytek. V následujícím dělení je dělitel předchozího dělencem, zbytek dělitelem. Této schematické úpravě postupného dělení říkáme *Euklidův algoritmus.*

Nyní je třeba, abychom si obecně ukázali, že postupným dělením, jak bylo naznačeno, dojdeme vždy k největšímu společnému děliteli daných dvou čísel. Přesně vysloveno:

Provedeme-li podle Euklidova algoritmu postupné dělení, vycházejíce ze dvou daných čísel a, b, pak poslední nenulový zbytek je největším společným dělitelem δ čísel a, b a lze ho napsati ve tvaru

$$\delta = a\alpha + b\beta,$$

kde α, β jsou čísla celá (kladná, záporná nebo rovná nule).

Toto tvrzení si dokážeme, uvážíme-li:

1. Zbytky při postupném dělení se stále zmenšují, dojdeme tedy nakonec vždy k zbytku 0.

2. Jednotlivá dělení můžeme zapsat rovnicemi; v číselném příkladě jsou to tyto rovnice:

$$\begin{aligned} 858 &= 252 \,.\, 3 + 102, \\ 252 &= 102 \,.\, 2 + 48, \\ 102 &= 48 \,.\, 2 + 6, \\ 48 &= 6 \,.\, 8 + 0. \end{aligned} \tag{1,1}$$

3. Z čtvrté rovnice (1,1) plyne, že poslední nenulový zbytek 6 je dělitelem předposledního zbytku 48; z třetí rovnice (1,1) plyne, že poslední nenulový zbytek 6 je také dělitelem zbytku 102. Projdeme-li takto rovnicemi (1,1) od poslední k první, dojdeme k závěru, že poslední nenulový zbytek 6 je dělitelem obou daných čísel.

4. Z každé z rovnic (1,1) lze vyjádřit zbytek a postupným dosazováním dostaneme každý zbytek ve tvaru $a\alpha + b\beta$. Tak z první rovnice vyjde:

$$102 = 858 \,.\, 1 - 252 \,.\, 3 \quad (\alpha = +1,\ \beta = -3).$$

Z první a druhé rovnice dostaneme:

$$48 = 252 - 102 \,.\, 2 = -858 \,.\, 2 + 252 \,.\, 5 \quad (\alpha = -2,\ \beta = 5).$$

Z první, druhé a třetí rovnice (1,1) plyne:

$$6 = 102 - 48 \,.\, 2 = 858 \,.\, 5 - 252 \,.\, 17 \quad (\alpha = 5,\ \beta = -17).$$

5. Poslední nenulový zbytek je tedy nejen dělitelem čísel a, b, ale je dělitelný i jejich největším společným dělitelem δ, neboť je ve tvaru $a\alpha + b\beta$. Je tudíž poslední nenulový zbytek právě největším společným dělitelem obou čísel.

6. Důkaz jsme naznačili na číselném příkladě, aby byl konkretní; postup důkazu je však zcela obecný a proto jsme vyslovené tvrzení dokázali obecně.

Pojmu největšího společného dělitele užíváme u libovolných celých čísel tak, že nepřihlížíme k jejich znamením. Tak na př. čísla 28, 60; -28, 60; 28, -60; -28, -60 mají téhož největšího společného dělitele, totiž 4.

Pravíme, že čísla a, b jsou *nesoudělná*, je-li jejich největší společný dělitel 1. Jsou tedy na př. každá dvě prvočísla nesoudělná, ale jsou nesoudělná také složená čísla $24 = 2^3 . 3$, $175 = 5^2 . 7$. Podle předcházejícího výkladu *lze určit k nesoudělným číslům a, b celá čísla α, β tak, že platí*:

$$a\alpha + b\beta = 1. \tag{1,2}$$

Obráceně, lze-li k dvěma číslům a, b najíti celá čísla α, β tak, že platí rovnice (1,2), *jsou čísla a, b nesoudělná* (proč?).

V dalších výkladech užijeme vět:

a) *Jsou-li a, b dvě nesoudělná čísla a je-li b dělitelem součinu ac, je b dělitelem čísla c.*

b) *Jsou-li a, b dvě nesoudělná čísla a je-li každé z nich dělitelem čísla c, je také jejich součin dělitelem čísla c.*

c) *Je-li δ největší společný dělitel čísel a, b, jsou celá čísla $\frac{a}{\delta}$, $\frac{b}{\delta}$ nesoudělná.*

Tvrzení a) dokážeme třeba tak, že znásobíme rovnici (1,2) číslem c; protože je pak b dělitelem obou členů na levé straně, je také dělitelem pravé strany.

Podobně postupujeme při důkazu věty b). V rovnici $ac\alpha + bc\beta = c$ nahradíme v prvním členu $c = kb$, v druhém $c = ma$ a dostaneme $ab . (k\alpha + m\beta) = c$: odtud je správnost b) patrná.

Při důkaze tvrzení c) vyjdeme z dokázané rovnice

$$a\alpha + b\beta = \delta$$

a dělíme ji číslem δ. Dostaneme rovnici

$$\frac{a}{\delta} \,.\, \alpha + \frac{b}{\delta} \,.\, \beta = 1,$$

která říká, že čísla $\frac{a}{\delta}$, $\frac{b}{\delta}$ jsou nesoudělná.

Z rozkladu čísla v součin mocnin prvočinitelů nahlédne čtenář snadno sám větu:

Je-li δ největší společný dělitel čísel a, b, a je-li ε největší společný dělitel čísel c, δ, je ε největší společný dělitel čísel a, b, c.

Uvedené věty si objasníme na příkladě:

Čísla -84, 102 mají největšího společného dělitele 6. Z Euklidova algoritmu vyjde rovnice

$$6 = 5 \,.\, 102 - 6 \,.\, 84.$$

Dělíme-li ji šesti, dostaneme

$$1 = 5 \,.\, 17 - 6 \,.\, 14.$$

Čísla 14, 17 jsou opravdu nesoudělná. Přibereme-li k daným dvěma číslům další číslo 105, pak z rozkladu $-84 = -2^2 \,.\, 3 \,.\, 7$, $102 = 2 \,.\, 3 \,.\, 17$, $105 = 3 \,.\, 5 \,.\, 7$ vyplývá, že největší společný dělitel všech tří čísel je $\varepsilon = 3$. K témuž výsledku dojdeme, vyhledáme-li největšího společného dělitele čísel 6, 105.

Cvičení 1. K dvěma číslům 48, 84 najděte třetí číslo x tak, aby každé číslo z trojice bylo dělitelem součinu ostatních dvou. Kolik má úloha řešení? [*Návod*: rozložte $48 = 12 \,.\, 4$, $84 = 12 \,.\, 7$ a ukažte, že x je násobek čísla $4 \,.\, 7$ nikoli větší než $48 \,.\, 84$.]

2. Pro která x je $y = \dfrac{2x}{x-3}$ celé číslo? [*Návod*: položte $x = 3 + t$.]

3. Pomocí Euklidova algoritmu najděte největšího společného dělitele čísel 420, 1155.

4. Pomocí Euklidova algoritmu najděte největšího společného dělitele mnohočlenů $2x^4 + x^3 + 2x^2 + 1$, $x^3 + 2x^2 + 2x + 1$. [*Návod*: provede se postupné dělení mnohočlenu mnohočlenem, jako se provádělo při zvláštních číslech.]

5. Dokažte: je-li n číslo celé, je N dělitelné šesti. a) $N = n(n + 1)(2n + 1)$, b) $N = n^3 + 5n$. [*Návod*: v obou případech dokažte nejprve, že N je sudé, a pak, že je dělitelné třemi. K tomu užijte vztahů a) $2n + 1 = 2(n + 2) - 3$, b) $n^2 + 5 = (n + 1)(n + 2) - 3(n - 1)$ a uvažte, že jedno z čísel n, $n + 1$, $n + 2$ je vždy dělitelné třemi.]