# Největší společný dělitel

Štěpán Šimsa

Abstrakt. Největší společný dělitel je základní pojem elementární teorie čísel. Tento pojem, zvláště ve spojení s Euklidovým algoritmem, má přes svou jednoduchost nejedno praktické využití. V olympiádní matematice nám usnadní řešení spousty příkladů nebo aspoň jejich částí a tento příspěvek má právě za úkol procvičit techniky, jak největší společný dělitel vypočítat a jak ho využít při řešení úloh.

Není-li řečeno jinak, číslem budeme myslet celé číslo.

**Definice.** Řekneme, že číslo $a \neq 0$ dělí číslo $b$ (píšeme $a \mid b$), pokud existuje číslo $c$ takové, že $ac = b$.

**Tvrzení.** *Pokud $a \mid b$, tak buď $b = 0$, nebo $|a| \leq |b|$. Pokud navíc $|a| \neq |b|$, tak $|a| \leq 2|b|$ atd.*

**Úloha 1.** Určete všechna celá kladná čísla $m, n$ taková, že $n$ dělí $2m - 1$ a zároveň $m$ dělí $2n - 1$. (MO 59–A–II–3)

**Definice.** Mějme čísla $a, b$. Pak jejich největší společný dělitel (NSD) je největší přirozené číslo $d$ takové, že $d \mid a$, $d \mid b$. Značíme ho $(a, b)$. Podobně nejmenší společný násobek je nejmenší přirozené číslo $d$ takové, že $a \mid d$, $b \mid d$, a značíme jej $[a, b]$.

**Cvičení.** Spočítejte $(-15, 24)$.

**Tvrzení.** *Platí:*

(i) $(a, a) = (a, 0) = (-a, 0) = [a, a] = [a, 0] = |a|$.
(ii) $(a, b) = (b, a) = (a - b, b) = (b - a, b) = (a - b, a) = (a + b, a)$.
(iii) $(a, b) = |a|$, *právě když* $a \mid b$, *a také právě když* $[a, b] = |b|$.
(iv) $(ab, ac) = a(b, c)$.
(v) $(a, b)[a, b] = ab$.
(vi) *Pokud* $d \mid a, d \mid b$, *tak i* $d \mid (a, b)$.
(vii) $(b, c) \mid (ab, c) \mid (a, c)(b, c) \mid a(b, c)$.

**Tvrzení.** (Euklidův algoritmus) *Díky druhé vlastnosti můžeme spočítat $(a, b)$ tak, že odečteme menší číslo od většího, dostaneme novou dvojici čísel (se stejným NSD) a postup budeme opakovat, dokud nebude jedno z čísel nula.*

**Úloha 2.** Určete, kolik (uspořádaných) dvojic přirozených čísel $a$, $b$ splňuje rovnici $[a, 70] + [b, 70] = 210$.

**Definice.** O číslech $a$, $b$ řekneme, že jsou *nesoudělná*, pokud $(a, b) = 1$.

**Tvrzení.** *Platí:*

(i) *Pokud* $(b, c) = 1$, *pak* $(ab, c) = (a, c)$.
(ii) *Pokud* $(b, c) = 1$, *pak* $(a, bc) = (a, b)(a, c)$.

**Úloha 3.** Určete, pro která čísla $a$, $b$, $c$ platí $[a, c] + [b, c] = (a + b)c$.

**Úloha 4.** Určete možné hodnoty výrazů pro nesoudělná čísla $a$, $b$:

(i) $(a + b, ab)$,
(ii) $(a^2 + b^2, ab)$,
(iii) $(a + b, a - b)$,
(iv) $(a^3, (a + 1)^5)$.

**Úloha 5.** Ukažte, že zlomek

$$\frac{21n + 4}{14n + 3}$$

je v základním tvaru pro každé přirozené číslo $n$. (IMO 1959)

**Úloha 6.** Dokažte, že pro každá přirozená $m$, $n$ platí

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

**Úloha 7.** Pro která celá čísla $n$ je výraz

$$\frac{n^3 - 3}{n - 3}$$

celočíselný? (Náboj 2007)

**Úloha 8.** S využitím vztahu $F_n = F_k \cdot F_{n-k-1} + F_{k-1} \cdot F_{n-k}$ ukažte, že pro Fibonacciho posloupnost platí

$$(F_m, F_n) = F_{(m,n)}.$$

**Úloha 9.** Zjistěte, pro která přirozená čísla $a, b$ je hodnota podílu

$$\frac{b^2 + ab + a + b - 1}{a^2 + ab + 1}$$

rovna celému číslu. (MO 57–A–III–3)

### Rozklad na $du$, $dv$

Často se v úlohách vyplatí rozepsat čísla $a$, $b$ jako $a = du$, $b = dv$, kde $d = (a, b)$.

**Úloha 10.** Určete, pro která čísla $a$, $b$ platí $(a,b)+[a,b]=a+b$.

**Úloha 11.** Rozhodněte, zda součet některých dvou přirozených čísel je dělitelem jejich nejmenšího společného násobku.

**Úloha 12.** Najděte všechny dvojice přirozených čísel $x$, $y$ takové, že

$$\frac{xy^2}{x+y}$$

je prvočíslo. (MO 58–A–I–3)

**Úloha 13.** Nechť $n,k$ jsou přirozená čísla a $k$ je navíc bezčtvercové[1]. Předpokládejme, že

$$\frac{n^3+2n^2+k}{n^2+k}$$

je celé číslo. Dokažte, že pak už platí $n=k$. (MKS 33–9–1)

**Úloha 14.** Pro dané prvočíslo $p$ najděte všechny trojice přirozených čísel $(a,b,c)$ splňující

$$\frac{[a,c]+[b,c]}{a+b}=\frac{p^2+1}{p^2+2}\cdot c.$$

(MO 59–A–I–6)

**Úloha 15.** Dokažte, že pro libovolná přirozená čísla $a$, $b$, $c$ platí

$$\frac{[a,b,c]^2}{[a,b]\cdot[b,c]\cdot[c,a]}=\frac{(a,b,c)^2}{(a,b)\cdot(b,c)\cdot(c,a)}.$$

(USAMO 1972)

**Úloha 16.** Nechť $a_1,\ldots,a_k,b_1,\ldots,b_k$ jsou přirozená čísla, která splňují $(a_i,b_i)=1$ pro každé $i\in\{1,\ldots,k\}$. Dále buď $m=[b_1,\ldots,b_k]$. Ukažte, že platí

$$\left(\frac{a_1m}{b_1},\ldots,\frac{a_km}{b_k}\right)=(a_1,\ldots,a_k).$$

(IMO shortlist 1974)

**Úloha 17.** Ukažte, že pokud je $p$ takové liché prvočíslo, že i $2p+1$ je prvočíslo, pak existují právě čtyři přirozená čísla $k$ taková, že

$$2p+k \mid 2p+k^2.$$

(Variace na MO 58–A–III–4)

[1] Bezčtvercové číslo je takové, které pro $a>1$ není dělitelné číslem $a^2$

**Tvrzení.** $(a, b) = d$ *je nejmenší kladné číslo z čísel tvaru* $ka + lb$ *a čísla tohoto tvaru jsou právě násobky čísla* $d$.

**Tvrzení.** (Bézoutova věta) *Pro čísla* $a, b$ *existují taková čísla* $k, l$, *že* $ka+lb = (a, b)$.

### Návody

**1.** Rozeberte možnosti $n = 2m-1$ (resp. $m = 2n-1$) a pak využijte první tvrzení.

**2.** Jedno z čísel musí být dělitel 70 a druhé násobek 4 a dělitel 140.

**3.** Zřejmě $[a, c] \mid ac$ a musí nastat rovnost.

**4.** (i), (ii) použijte $(a, bc) = (a, b)(a, c)$ pro nesoudělná $b, c$, (iii) použijte $(2a, b) \mid 2(a, b)$, (iv) co znamená nesoudělnost pro prvočíselné rozklady?

**5.** Euklidův algoritmus.

**6.** Pro $m \geq n$ rozepište $2^m = (2^n - 1)2^{m-n} + 2^{m-n}$.

**7.** Výraz je celočíselný, právě když $|n-3| = (n^3-3, n-3)$. Nyní můžeme aplikovat Euklidův algoritmus.

**8.** Nejprve dokažte, že po sobě jdoucí členy jsou nesoudělné.

**9.** Jmenovatel musí dělit i součet čitatele s jmenovatelem. Tento součet rozložte na součin a ukažte, že jeden člen je s jmenovatelem nesoudělný.

**10.** Po substituci $a = du$, $b = dv$ a úpravě výrazu rozložte na součin.

**11.** Po substituci $a = du$, $b = dv$ a podělení obou stran dělitelnosti $d$ ukažte, že obě strany dělitelnosti jsou nyní nesoudělné.

**12.** Po substituci $x = du$, $y = dv$ ukažte, že $u + v \mid d^2$ a $uv^2$ dělí celý zlomek. Rozeberte dva případy, $u = 1$ a $u > 1$. V druhém případě rozložte $d^2 - 1$ na součin.

**13.** Po substituci $n = du$, $k = dv$ si uvědomte, že $(d, v) = 1$.

**14.** Využijte $[a, c] = \frac{ac}{(a,c)} = \frac{a}{(a,c)}c$.

**15.** Pro $d = (a, b, c)$ rozepište $a = d(\frac{a}{d}, \frac{b}{d})(\frac{a}{d}, \frac{c}{d})u$. Uvědomte si, že to jde díky tomu, co musí být s čím nesoudělné. Poté trpělivě upravujte.

**16.** Dokazujte pro jedno prvočíslo. Pokud $p \mid m$, tak si vyberte takové $i$, že $b_i$ má maximální mocninu $p$.

**17.** Rozeberte čtyři možnosti podle toho, čemu se rovná $(2p, k)$.

### Literatura a zdroje

[1] Michal Rolínek, *Důkazové metody v teorii čísel*, *http://mks.mff.cuni.cz/library/*.
[2] Josef Svoboda, Štěpán Šimsa: *Seriál Teorie čísel*, *mks.mff.cuni.cz/archive/*.