Dělitelnost

Termín odeslání: 11. 12. 2017

autoři: *Matouš a Dominik*

Text je rozdělen na dvě části. V první jsou uvedeny základní definice a poznatky týkající se dělitelnosti v celých číslech. Čtenář, který tyto základy již zná, si může v první části vše jen rychle připomenout a vrhnout se rovnou na druhou, abstraktnější část. V té zkusíme rozšířit myšlenku dělitelnosti na obecnější struktury než přirozená nebo celá čísla. Zavedeme obecnější definici a pokusíme se ji aplikovat v konkrétních příkladech.

Základní pojmy

Definice 2.1. *Uvažme dvě celá čísla a, b (značíme $a, b \in \mathbb{Z}$). Řekneme, že a **dělí** b, psáno $a|b$ právě tehdy, když existuje nějaké $c \in \mathbb{Z}$ takové, že platí $a \cdot c = b$. Číslo a se pak nazývá **dělitelem** čísla b.*

Příklad 2.1. *Kolik má 0 dělitelů?*

Z definice vyplývá, že aby bylo nějaké číslo a dělitelem nuly, musí splňovat rovnici $a \cdot b = 0$ pro nějaké $b \in \mathbb{Z}$. Pokud se ale b bude rovnat nule, může být dělitelem nuly kterékoliv celé číslo. Odtud vidíme, že pro každé $a \in \mathbb{Z}$ platí $a|0$.

Příklad 2.2. *Kolik čísel dělí nula?*

Opět se budeme řídit definicí. Hledáme tedy $a \in \mathbb{Z}$ takové, že $0 \cdot b = a$ pro nějaké $b \in \mathbb{Z}$. Jenže pro libovolné takové b platí, že $0 \cdot b = 0$. Jediné číslo, které tedy nula dělí, je nula.

Definice 2.2. *Mějme celá čísla a, b. Libovolné celé číslo m takové, že $m|a$, $m|b$ se nazývá **společný dělitel** čísel a, b. Nezáporný společný dělitel čísel a, b, který je dělitelný libovolným společným dělitelem čísel a, b, se nazývá **největší společný dělitel** čísel a, b a značí se (a, b).*

Definice 2.3. *Mějme celá čísla a, b. Libovolné celé číslo n takové, že $a|n$, $b|n$ se nazývá **společný násobek** čísel a, b. Nezáporný společný násobek čísel a, b, který dělí libovolný společný násobek čísel a, b, se nazývá **nejmenší společný násobek** čísel a, b a značí se $[a, b]$.*

Definice 2.4. *Pokud pro dvě celá čísla platí $(a, b) = 1$, řekneme, že jsou tzv. **nesoudělná**. Pro nesoudělná čisla platí $[a, b] = a \cdot b$. V opačném případě řekneme, že jsou čísla **soudělná**.*

Věta 2.1. *Pro libovolná $a, b \in \mathbb{Z}$ platí $(a, b) \cdot [a, b] = a \cdot b$.*

DŮKAZ: Věta je triviální pro a a b nesoudělná (viz poznámka). Pakliže jsou čísla soudělná, označme x největšího společného dělitele čísel a, b a zapišme čísla jako $a = x \cdot a'$

a $b = x \cdot b'$. Čísla a', b' jsou nyní nesoudělná. Kdyby nebyla, existoval by nějaký jejich společný dělitel y:$y|a', y|b'$, pak xy je společný dělitel a, b a platilo by $x|xy$, takže x by nebyl největší společný dělitel a, b.

Jelikož jsou čísla a', b' nesoudělná, platí $[a', b'] = a' \cdot b'$. Což znamená, že všechny společné násobky musí být dělitelné číslem $a' \cdot b'$, a tudíž všechny společné násobky čísel $a = x \cdot a'$, $b = x \cdot b'$ musí být dělitelné číslem $a' \cdot b' \cdot x$. Číslo $a' \cdot b' \cdot x$ je tedy nejmenším společným násobkem a, b.

Konečně dostáváme $(a, b) \cdot [a, b] = x \cdot a' \cdot b' \cdot x = a \cdot b$.

Definice 2.5. *Přirozené číslo p nazveme* ***prvočíslem****, pokud existují právě dva kladní dělitelé čísla n, a sice 1 a samotné n. V opačném případě a pokud $n \neq 1$, řekneme, že je číslo n* ***složené****.*

Poznámka. Prvočíslo je se všemi celými čísly kromě svých násobků nesoudělné.

Věta 2.2. *Každé přizené číslo větší než 1 lze rozložit na součin konečně mnoha prvočísel, a to jednoznačně, až na pořadí činitelů.*

DŮKAZ: Neuveden pro svoji délku.

Levá a pravá dělitelnost

Myšlenka na úvod:

Jeden z přístupů k dělitelnosti by mohl být následující: a dělí b, jestliže „b děleno a“ dopadne dobře, například bude celé číslo. Problém je ale v tom, že s dělením jako operací se nedá moc dobře pracovat (už v celých číslech máme problém s dělení nulou a na dalších strukturách se „děleno“ těžko zavádí). To znamená že obecně se na dělitelnost musíme koukat pouze pomocí násobení. Tedy a dělí b, jestliže a umíme něčím vhodně vynásobit tak, aby součin byl b. Musíme si ale dát pozor, neboť obecné „násobení“ se nemusí vždy chovat tak hezky, jak jsme zvyklí, a proto je třeba rozlišovat mezi dvěma typy dělitelnosti (ukážeme si později na příkladech):

Definice 2.6. *Je dána množina A a operace $* : u * v = w$ pro $u, v, w \in A$. Řekneme, že prvek a* ***dělí*** *b* ***zleva****, jestliže existuje $q \in A$ tak, že $b = a * q$. Říkáme, že a je* ***levý dělitel*** *prvku b. Obdobně prvek a* ***dělí*** *b* ***zprava****, jestliže existuje $r \in A$ tak, že $b = r * a$, a je* ***pravý dělitel*** *prvku b.*

Pojďme si tuto abstraktní definici trochu „ošahat“:

Příklad 2.3. Pokud si místo množiny A představíme množinu celých čísel $\mathbb{Z}$ a místo $*$ klasické násobení $\cdot$, vidíme, že levá i pravá dělitelnost je to samé jako klasická dělitelnost v $\mathbb{Z}$. Platí totiž $q \cdot a = a \cdot q$ a každý levý dělitel je zároveň pravý dělitel, proto zde nemá smysl dělitelnosti rozlišovat.

Příklad 2.4. Další příklad ukazuje operaci na množině trojic celých čísel, u které záleží na pořadí operandů, a tedy záleží, zda uvažujeme pravou nebo levou dělitelnost:

$$* : (a, b, c) * (d, e, f) = (ad, ae + bf, cf) \neq (ad, db + ec, cf) = (d, e, f) * (a, b, c)$$

Trojice $(3, 1, 5)$ je pravý dělitel $(36, 32, 35)$, neboť lze najít trojici $(12, 4, 7)$, že $(36, 32, 35) = (12, 4, 7) * (3, 1, 5)$. Ukážeme, že $(3, 1, 5)$ není levý dělitel. Podle definice by musela existovat trojice (d, e, f) tak, že $(36, 32, 35) = (3, 1, 5) * (d, e, f) = (3d, 3e + f, 5f)$.

Porovnáním jednotlivých složek dostáváme:

$$36 = 3d \Rightarrow d = 12$$
$$35 = 5f \Rightarrow f = 7$$
$$32 = 3e + 7 \Rightarrow 25 = 3e$$

To ale nemůže nastat, protože e má být celé číslo.

Příklad 2.5. Vezměme množinu lineárních funkcí s celočíselnými koeficienty a operaci skládání:

$$f(x) = ax + b, g(x) = cx + d, a, b, c, d \in \mathbb{Z}, f \circ g = f(g(x)) = a(cx + d) + b$$

I zde záleží na pořadí, v jakém funkce skládáme:

$$f \circ g \neq g \circ f$$
$$a(cx + d) + b \neq c(ax + b) + d$$
$$acx + ad + b \neq cax + cb + d$$

Ukážeme, že každá lineární funkce má někonečně mnoho levých dělitelů.

Nechť $h(x) = ux + v$. Číslo u můžeme napsat jako $u = 1 \cdot u$. Dále zvolme libovolné celé číslo c. Funkce $g(x) = ux + c$ dělí $h(x)$, neboť existuje funkce $f(x) = 1x + (v - c)$, která po složení s $g(x)$ dává $f \circ g = f(g(x)) = 1(ux + c) + v - c = ux + v$, a tedy $g(x)$ je levý dělitel funkce $h(x)$. Číslo c však bylo libovolné, proto je takových dělitelů nekonečně mnoho.

Příklad 2.6. Vezměme nyní racionální čísla $\mathbb{Q}$ s násobením jak jsme zvyklí. Opět díky to u, že nezáleží na pořadí činitelů $(q \cdot a = a \cdot q)$ nemusíme rozlišovat mezi pravou a levou dělitelností. Zkuste se nyní znovu pořádně podívat na definici a zamyslet se, kolik dělitelů má číslo 1 a kolik dělitelů má potom libovolné racionální číslo.

Závěrem textu přejeme hodně zdaru při řešení úloh.

BRKOS Team 2017