

DMA Domáci úkol č. 2A

Tento úkol vypracujte a pak přineste na cvičení č. 3.

1. Dokažte, že pro každé $a, b \in \mathbb{Z}$ platí: Jestliže $a \mid b$, pak $a \mid (-b)$.
2. Dokažte, že pro každé $a, b \in \mathbb{Z}$ platí: Jestliže $a \mid b$, pak $a \mid (a + b)$.

Zkouškový speciál výpočetní (doporučeno):

a) Najděte $\gcd(192, -264)$ a příslušnou Bezoutovu identitu rozšířeným Euklidovým algoritmem.

Zkouškový speciál důkazový (pokročilejší mohou zkusit teď nebo před zkoukou):

- a) [rutinní] Nechť $a, b \in \mathbb{N}$. Dokažte, že $\gcd(a, b)$ dělí $\text{lcm}(a, b)$.
Nápověda: Stačí použít význam oněch dvou pojmů.
- b) [rutinní] Nechť $a, b \in \mathbb{N}, k \in \mathbb{N}$. Dokažte, že $k \cdot \gcd(a, b)$ je společný dělitel čísel ak, bk .
- c) [náročnější] Určete, kdy přesně platí $\gcd(a, b) = \text{lcm}(a, b)$, a odpověď dokažte.
- d) [náročnější] Nechť $a, b \in \mathbb{N}$. Dokažte, že jestliže $a \mid b$, pak $\gcd(a, b) = a$.

Řešení:

1. Uvažujme libovolné $a, b \in \mathbb{Z}$. Předpoklad: $a \mid b$. Pak existuje $k \in \mathbb{Z}$ aby $b = k \cdot a$. Odtud $-b = -ka = (-k) \cdot a$ a $-k \in \mathbb{Z}$, proto podle definice $a \mid (-b)$.
2. $a, b \in \mathbb{Z}$ libovolné. Předpoklad: $a \mid b$. Pak $b = ka, k \in \mathbb{Z}$. Přičtením a k oběma stranám dostaneme $a + b = a + ka = (1 + k)a$ a $1 + k \in \mathbb{Z}$, tedy $a \mid (a + b)$.

Zkouškový speciál výpočetní:

Typické řešení na jistotu (pro zkoušku).

a/b	(264)	(192)	Odtud $\gcd(264, 192) = 24 = 3 \cdot 264 + (-4) \cdot 192$.
264	1	0	My ale chceme
192	0	1	$\gcd(192, -264) = 24 = (-4) \cdot 192 + (-3) \cdot (-264)$.
72	1	-1	
48	-2	3	
24●	3●	-4●	
0			

Poznámka: Bezoutova identita není jediná, podle zvolených úprav lze mít i jiný výsledek, třeba $\gcd(192, -264) = 24 = 7 \cdot 192 + 5 \cdot (-264)$.

Brzy uvidíme, že možných vyjádření je nekonečně mnoho.

Verze pro prince Drsoně:

a/b	(192)	(-264)
-264	0	1
192	1	0
-72	1	1
-24	4	3
0	-11	-8
24●	-4●	-3●

Všimněte si, že v tabulce jsme nezačali v pomocných sloupcích s jednotkovou maticí, ale jinou, aby se první pomocný sloupec vztahoval k 192, přesně jak to chceme ve výsledku:

$$\gcd(192, -264) = 24 = (-4) \cdot 192 + (-3) \cdot (-264).$$

Zkouškový speciál:

- a) Vlastnosti $\gcd(a, b)$: dělí a , dělí b a je největší taková.
Vlastnosti $\text{lcm}(a, b)$: je násobkem a , je násobkem b a je nejmenší taková.
Něco si z toho vybereme a spojíme:
Podle definice $\gcd(a, b)$ dělí a a a dělí $\text{lcm}(a, b)$. Podle věty z přednášky (tranzitivita) pak $\gcd(a, b)$ dělí $\text{lcm}(a, b)$.

Elementární důkaz bez odvolávky na větu: Podle definice $\gcd(a, b)$ dělí a , tedy existuje $k \in \mathbb{Z}$ splňující $a = \gcd(a, b) \cdot k$. Podle definice a dělí $\text{lcm}(a, b)$, tedy existuje $l \in \mathbb{Z}$ splňující $\text{lcm}(a, b) = a \cdot l$. Pak $\text{lcm}(a, b) = \gcd(a, b)(kl)$ a $kl \in \mathbb{Z}$.

b) Podle definice $\gcd(a, b)$ je společný dělitel a a b , tedy $a = \gcd(a, b)l$ a $b = \gcd(a, b)m$ pro $l, m \in \mathbb{Z}$. Pak $ka = [\gcd(a, b)k]l$ a $kb = [\gcd(a, b)k]m$ pro $l, m \in \mathbb{Z}$. Proto $k \cdot \gcd(a, b)$ dělí ka a také dělí kb , tedy $k \cdot \gcd(a, b)$ je společný dělitel čísel ak, bk .

c) Po zamyšlení a pár experimentech: $\gcd(a, b) = \text{lcm}(a, b)$ právě tehdy, když $a = b$.

Důkaz \Leftarrow : Podle faktů z přednášky (nebo snadno odvodíme) víme $\gcd(a, a) = a = \text{lcm}(a, a)$.

Důkaz \Rightarrow : Protože $a, b \neq 0$, můžeme odhadovat $\gcd(a, b) \leq a \leq \text{lcm}(a, b)$ a také $\gcd(a, b) \leq b \leq \text{lcm}(a, b)$. Pokud by platilo $\gcd(a, b) = \text{lcm}(a, b)$, tak se nerovnosti změň v rovnosti a máme $a = \gcd(a, b) = b$.

Alternativa: Pro $a, b \in \mathbb{N}$ platí $a \leq b$ nebo $b \leq a$. V prvním případě máme $\gcd(a, b) \leq a \leq b \leq \text{lcm}(a, b)$. Pokud by platilo $\gcd(a, b) = \text{lcm}(a, b)$, tak se nerovnosti změň v rovnosti a vyjde $a = b$. Druhý případ se dělá obdobně.

Alternativa, kterou mi přinesli studenti: Víme:

- $\gcd(a, b)$ dělí a , proto $a = \gcd(a, b)k$, kde $k \in \mathbb{Z}$, ale díky kladnosti a je $k \in \mathbb{N}$;
- $\gcd(a, b)$ dělí $b > 0$, proto $b = \gcd(a, b)l$, kde $l \in \mathbb{N}$;
- předpoklad $\text{lcm}(a, b) = \gcd(a, b)$.

Dosadíme do $\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$:

$$\gcd(a, b) = \frac{\gcd(a, b)k \gcd(a, b)l}{\gcd(a, b)} \implies 1 = kl.$$

Pro $k, l \in \mathbb{N}$ to platí jedině v případě $k = l = 1$, tedy $a = \gcd(a, b) = b$.

d) Toto je trochu těžší, ale studenti mají často alespoň nápad, který lze dotvořit. Občas mě překvapí, zejména jsem nečekal F a G. Jdeme na to.

Důkaz: $a, b \in \mathbb{N}$. Předpoklad: $a \mid b$.

A) Jak bych to dělal já:

1. Protože $a \mid b$ a $a \mid a$ (známý fakt), víme, že a je společný dělitel čísel a a b .
2. Protože $a \neq 0$, musí všichni společní dělitelé d čísel a, b splňovat $d \leq a$. Ten společný dělitel a je tedy mezi nimi největší.

Proto $a = \gcd(a, b)$.

B) Podobný přístup od studentů:

1. Protože $a \mid b$ a $a \mid a$, je a společný dělitel, tudíž musí být menší či roven tomu největšímu: $a \leq \gcd(a, b)$.
2. Protože $\gcd(a, b)$ dělí a , je $a \geq \gcd(a, b)$.

Spojením získáme rovnost.

C) Stejný důkaz jako výše, ale s přidanou komplikací:

1. Protože $\gcd(a, b)$ dělí a , je $a = k \cdot \gcd(a, b)$ pro nějaké $k \in \mathbb{Z}$. Obě čísla jsou kladná, takže dokonce $k \in \mathbb{N}$.

2. Protože $a \mid b$ a $a \mid a$, je a společný dělitel, tudíž musí být menší či roven tomu největšímu: $a \leq \gcd(a, b)$. Takže $k \gcd(a, b) \leq \gcd(a, b)$ neboli $k \leq 1$, to lze jen pro $k = 1$. Máme $a = \gcd(a, b)$.

D) Delší způsob, jak získat jednu nerovnost, je pomocí Bezouta:

1. Protože $\gcd(a, b)$ dělí a , je $a \geq \gcd(a, b)$.
2. Víme, že $\gcd(a, b) = Aa + Bb$ pro nějaké $A, B \in \mathbb{Z}$. Protože $a \mid b$ a $a \mid a$, dělí a celou pravou stranu a proto $a \mid \gcd(a, b)$. Takže $a \leq \gcd(a, b)$.

Spojením 1. a 2. máme rovnost.

E) Zajímavá finta:

Protože $a \mid b$, je $b = k \cdot a$ pro $k \in \mathbb{Z}$. Zjevně $\gcd(1, k) = 1$. Pak ovšem podle věty ze skriptu či ze cvičení

$$\gcd(a, b) = \gcd(a, ak) = a \gcd(1, k) = a \cdot 1 = a.$$

F) Chytrá recyklace nápadu:

Protože $a \mid b$, je $a \leq b$ a $b \bmod a = 0$. Podle klíčového Lemma z první přednášky proto

$$\gcd(a, b) = \gcd(b, a) = \gcd(a, b \bmod a) = \gcd(a, 0) = a.$$

G) Důkaz algoritmem. Někdy je to možné, pokud je správnost algoritmu matematicky dokázána. Protože $a \mid b$, je $b = k \cdot a$ pro nějaké $k \in \mathbb{Z}$. Hned v prvním kroku Euklidova algoritmu tedy odečteme druhý řádek k krát od prvního a dostáváme

a, b	A	B	q
b	1	0	
$a \bullet$	$0 \bullet$	$1 \bullet$	k
0	1	$-k$	

Takže $\gcd(a, b) = a$.

H) Hardcore:

Díky $a \mid b$ máme $b = k \cdot a$ pro $k \in \mathbb{Z}$. To znamená, že

$$a = 1 \cdot a = (1 - k)a + ka = (1 - k)a + b = (1 - k)a + 1 \cdot b.$$

Číslo a se podařilo vytvořit jako lineární kombinaci čísel a, b , je o tedy jeden z kandidátů na $\gcd(a, b)$. To správné $\gcd(a, b)$ se pozná tak, že je to nejmenší možné kladné číslo vytvořitelné jako lineární kombinace a, b . Tvrdíme, že nic menšího než a už ale vytvořit nelze.

Lineární kombinace a, b vypadají takto:

$$Aa + Bb = Aa + Bka = (A + Bk)a.$$

Protože chceme kladné číslo, omezujeme se na $A + Bk > 0$. Protože je to celé číslo, pak nutně $A + Bk \geq 1$ a proto $(A + Bk)a \geq a$. Takže opravdu, a je nejmenší kladné číslo získatelné ve tvaru Bezouta a tudíž je to $\gcd(a, b)$.

Poznámka: Řada studentů to zkoušela touto cestou, našla to Bezoutí vyjádření, ale dál už to bylo moc drsné.