DMA Domácí úkol č. 5b

Tento úkol vypracujte a pak přineste na cvičení č. 6.

Tento týden trochu přitvrdíme. První tvrzení se dokazuje tak, jak už umíme a jak to budeme potřebovat k první semestrální písemce (přímočará úprava vzorců), ale budete se muset vyrovnat s tím, že nejde o implikaci, ale ekvivalenci. Na přednáškách jsme už to několikrát viděli, neměl by to být problém.
Druhé tvrzení vyžaduje jiný, pokročilejší typ důkazu: Není třeba nic počítat, ale správně sestavit předpoklady a poznatky o pojmech, které se tam objeví. Opět napoví, když se na to zkusíte podívat odzadu: Co máme (podle definice) čtenáři přinést, aby nám už uvěřil, že platí závěr? Pokud si to dobře rozmyslíte, tak zjistíte, že ten důkaz je vlastně také snadný (když už je vymyšlený), takže nečekejte půlstránkové orgie.
Možná vás bude zajímat, že si takový důkaz umím představit u ústní zkoušky, někde na rozhraní B a C.

1. Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$. Dokažte, že $a \equiv 0 \pmod{n}$ právě tehdy, když $n \mid a$.

2. Nechť $a, b \in \mathbb{N}$. Dokažte, že jestliže $a \mid b$, pak $\gcd(a, b) = a$.

Řešení:

1. Vezmeme $n \in \mathbb{N}$, $a \in \mathbb{Z}$ libovolné.
Pečlivý důkaz:
$\Longrightarrow$: Předpoklad $a \equiv 0 \pmod{n}$. Pak $0 = a + kn$ pro $k \in \mathbb{Z}$ neboli $a = (-k) \cdot n$. Protože $(-k) \in \mathbb{Z}$, je $n \mid a$.
$\Longleftarrow$: Předpoklad $n \mid a$. Pak $a = kn$ pro $k \in \mathbb{Z}$ neboli $0 = a + (-k) \cdot n$. Protože $(-k) \in \mathbb{Z}$, je $a \equiv 0 \pmod{n}$.
Alternativa:
$\Longrightarrow$: Předpoklad $a \equiv 0 \pmod{n}$. Pak $n \mid (0 - a)$, tedy $n \mid (-a)$. Pak $n \mid (-(-a))$ neboli $n \mid a$.
$\Longleftarrow$: Předpoklad $n \mid a$. Pak $n \mid (-a)$ neboli $n \mid (0 - a)$, proto $a \equiv 0 \pmod{n}$.

Efektivní důkaz:
$a \equiv 0 \pmod{n} \longleftrightarrow 0 = a + kn,\ k \in \mathbb{Z} \longleftrightarrow a = (-k)n,\ (-k) \in \mathbb{Z} \longleftrightarrow n \mid a.$
Preferoval bych první verzi. Druhá je sice formálně správná, ale když se čte zprava doleva, tak se dělitelnost $n \mid a$ přepíše jako $a = (-k) \cdot n$. To je správně, ale vyžaduje to přece jen jisté myšlenkové kroky, které tam chybí: Víme, že je nějaký takový celočíselný násobek, takže když si jeho opačné číslo vezmu jako k, tak tomu násobku můžu říkat $-k$.

2. Toto je trochu těžší, ale řada lidí měla přinejmenším dobrý nápad, a to občas až překvapivý (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 skripta 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

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

G) Důkaz algoritmem. Někdy je to možné, pokud je správnost algoritmu matematicky dokázaná.
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.