B4B01DMA

Jakub Adamec

Domácí úkol č. 5A

23. 10. 2024

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 $a \equiv 0 (\operatorname{mod} n)$ právě tehdy, když $n \mid a$.

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

1. Důkaz:

„$\Longrightarrow$“:
$n \in \mathbb{N}$ libovolné, $a \in \mathbb{Z}$ libovolné.
předpoklad: $a \equiv 0 (\operatorname{mod} n)$.
$a - 0 = kn$, $k \in \mathbb{Z}$.
$a = kn$.
což znamená $n \mid a$.

„$\Longleftarrow$“:
$n \in \mathbb{N}$ libovolné, $a \in \mathbb{Z}$ libovolné.
předpoklad: $n \mid a$.
$a = kn$, $k \in \mathbb{Z}$.
$a + (-0) = kn + (-0)$.
$a - 0 = kn$.
a to je stejný zápis jako $a \equiv 0 (\operatorname{mod} n)$.

□

2. Důkaz:

$a, b \in \mathbb{N}$ libovolné.
předpoklad: $a \mid b$.
$b = ka$, $k \in \mathbb{Z}$.
$b \geq a$.
protože každé číslo, které dělí a musí dělit i b,
a zároveň gcd(a, a)= a, tak gcd(a, b)= a.

$a, b \in \mathbb{N}$ libovolné.
předpoklad: $a \mid b$.
$b = ka$, $k \in \mathbb{Z}$.
obecně také platí, že $a \mid a$.
$\Longrightarrow a$ je společným dělitelem a, b.

$\forall d \in \mathbb{N}$ taková, že $d \mid a \ \wedge \ d \mid b \Longleftrightarrow d$ je společný dělitel a, b.
dosadíme předpoklad: $d \mid a \ \wedge \ d \mid (ka)$.
$d \mid a \Longrightarrow |d| \leq |a|$.
a protože a i d jsou společnými děliteli a, b, a zároveň platí $|d| \leq |a|$, tak gcd(a, b)= a.

□