B4B01DMA

Jakub Adamec

Domácí úkol č. 4A

14. 10. 2024

Tento úkol vypracujte a pak přineste na cvičení č. 5.

1. Dokažte, že když moduly $m, n \in \mathbb{N}$ splňují $m \mid n$ a čísla $a, b \in \mathbb{Z}$ splňují $a \equiv b (\operatorname{mod} n)$, pak $a \equiv b (\operatorname{mod} m)$.

2. Nechť $p, q \in \mathbb{N}$. Dokažte, že když čísla $a, b \in \mathbb{Z}$ splňují $a \equiv b (\operatorname{mod} pq)$, pak $a \equiv b (\operatorname{mod} p)$ a $a \equiv b (\operatorname{mod} q)$.

1. Důkaz:

$m, n \in \mathbb{N}$ libovolné. $a, b \in \mathbb{Z}$ libovolné.
předpoklad: $m \mid n \quad \wedge \quad a \equiv b (\operatorname{mod} n)$.
$n = km$, $k \in \mathbb{Z}$.
$a - b = ln$, $l \in \mathbb{Z}$.
$a - b = l(km) = (lk)m$, $(lk) \in \mathbb{Z}$.
A tedy platí $a \equiv b (\operatorname{mod} m)$.

$\square$

2. Důkaz:

$p, q \in \mathbb{N}$ libovolné. $a, b \in \mathbb{Z}$ libovolné.
předpoklad: $a \equiv b (\operatorname{mod} pq)$.
$a - b = kpq$, $k \in \mathbb{Z}$.
No ale to nutně znamená, že $a - b$ je dělitelné p i q.
A tedy platí $a \equiv b (\operatorname{mod} p)$ a $a \equiv b (\operatorname{mod} q)$.

$\square$