

DMA Domáci úkol č. 4A

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 $a \equiv b \pmod{n}$, pak $a \equiv b \pmod{m}$.
2. Nechť $p, q \in \mathbb{N}$. Dokažte, že když čísla $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{pq}$, pak $a \equiv b \pmod{p}$ a $a \equiv b \pmod{q}$.

Zkouškový speciál výpočetní (doporučeno):

- a) Najděte opačný a inverzní prvek k $a = 12$ v \mathbb{Z}_{35} .

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

- a) [rutinní] Nechť $a, b \in \mathbb{N}$. Ukažte, že číslo $\frac{a \cdot b}{\gcd(a, b)}$ je společným násobkem čísel a, b .
- b) [rutinní] Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$. Dokažte, že $a \equiv 0 \pmod{n}$ právě tehdy, když $n \mid a$.
- c) [náročnější] Nechť $a, b, c \in \mathbb{N}$. Dokažte, že když je d společný dělitel a a b , tak nutně d dělí $\gcd(a, b)$.