DMA Domácí úkol č. 4b

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 $a \equiv b \pmod{q}$.

Řešení:

1. Vezmeme a, b libovolné $\in \mathbb{Z}$. Vyjdeme z předpokladů,

$$\left.\begin{array}{l} m \mid n \iff \exists k \in \mathbb{Z}: \ n = km \\ a \equiv b \pmod{n} \iff \exists l \in \mathbb{Z}: \ b = a + ln \end{array}\right\} \text{tedy } b = a + l(km) = a + (lk)m \text{ a } lk \in \mathbb{Z}.$$

Proto $a \equiv b \pmod{m}$.

2. Vezmeme a, b libovolné $\in \mathbb{Z}$. Z předpokladu $b = a + k(pq)$ pro nějaké $k \in \mathbb{Z}$.

$$\text{Pak } \begin{cases} b = a + (kq)p, \ (kq) \in \mathbb{Z} \implies a \equiv b \pmod{p}; \\ b = a + (kp)q, \ (kp) \in \mathbb{Z} \implies a \equiv b \pmod{q}. \end{cases}$$