

## 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  $\gcd(a, b)$ .

**Řešení:**

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

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

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

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

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

Zkouškový speciál výpočetní:

- a)  $(-a) = n - a = 23$ .

Inverze: Hledáme  $x \in \mathbb{Z}$  aby  $12x + 35m = 1$  pro nějaké  $m \in \mathbb{Z}$ , toto děláme Euklidem.

Dostali jsme  $3 \cdot 12 + (-1) \cdot 35 = 1$ , modulo 35 to dává  $3 \cdot 12 \equiv 1$ .

Takže  $12^{-1} = 3$ .

$a/b$	$A$	$B$
35	1	0
12	0	1
11	1	-2
1●	-1●	3●
0		

Zkouškový speciál důkazový:

- a) Dáno  $a, b \in \mathbb{N}$ .

$\gcd(a, b)$  dělí  $a$ , proto  $a = \gcd(a, b)k$ , kde  $k \in \mathbb{Z}$ . Pak

$$\frac{a \cdot b}{\gcd(a, b)} = \frac{\gcd(a, b)k \cdot b}{\gcd(a, b)} = k \cdot b,$$

takže je to násobek  $b$ .

Obdobně ukážeme, že je to násobek  $a$ .

b) Vezmeme  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  libovolné.

Pečlivý důkaz:

$\implies$ : 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  $n \mid a$ .

$\impliedby$ : 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:

$\implies$ : Předpoklad  $a \equiv 0 \pmod{n}$ . Pak  $n \mid (0 - a)$ , tedy  $n \mid (-a)$ . Pak  $n \mid (-(-a))$  neboli  $n \mid a$ .

$\impliedby$ : Předpoklad  $n \mid a$ . Pak  $n \mid (-a)$  neboli  $n \mid (0 - a)$ , proto  $a \equiv 0 \pmod{n}$ .

Efektivní důkaz:

$a \equiv 0 \pmod{n} \iff 0 = a + kn, k \in \mathbb{Z} \iff a = (-k)n, (-k) \in \mathbb{Z} \iff n \mid a$ .

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  $-k$ .

c) Dány  $a, b, c \in \mathbb{N}$ . Bezoutova identita:  $\gcd(a, b) = Aa + Bb$  pro  $A, B \in \mathbb{Z}$ .

Když je  $d$  společný dělitel  $a$  a  $b$ , tak  $a = dk, b = dl$ , kde  $k, l \in \mathbb{Z}$ . Pak

$$\gcd(a, b) = Adk + Bdl = d(Ak + Bl)$$

a  $Ak + Bl \in \mathbb{Z}$ , tedy  $d \mid \gcd(a, b)$ .