

### DMA Domáci úkol č. 3A

Tento úkol vypracujte a pak přineste na cvičení č. 4.

1. Nechť  $n \in \mathbb{N}$ . Dokažte, že  
jestliže  $a, b \in \mathbb{Z}$  splňují  $a \equiv b \pmod{n}$ , pak  $13a \equiv 13b \pmod{n}$ .
2. Nechť  $n \in \mathbb{N}$ . Dokažte, že  
jestliže  $a, b, c \in \mathbb{Z}$  splňují  $a \equiv b \pmod{n}$  a  $b \equiv c \pmod{n}$ , pak  $a \equiv c \pmod{n}$ .

Zkouškový speciál výpočetní (doporučeno):

- a) Vypočítejte tento výraz modulo 13, použijte malou Fermatovu větu:  $(7 + 8)^{146} - 21$ .
- b) Najděte inverzní prvek k  $a = 13$  modulo  $n = 20$ .

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

Příklady a) až c) jsou rutinní.

- a) Nechť  $n \in \mathbb{N}$  a  $a, b \in \mathbb{Z}$ . Dokažte, že jestliže  $a \equiv b \pmod{n}$ , pak  $b - a \equiv 0 \pmod{n}$ .
- b) Nechť  $n \in \mathbb{N}$  a  $a, b \in \mathbb{Z}$ . Dokažte, že jestliže  $a \equiv b \pmod{n^2}$ , pak  $a \equiv b \pmod{n}$ .
- c) Nechť  $n \in \mathbb{N}$  a  $a, b \in \mathbb{Z}$ . Dokažte, že jestliže  $a \equiv b \pmod{n}$ , pak  $2a + 3b \equiv 5b \pmod{n}$ .
- d) Nechť  $n \in \mathbb{N}$ . Dokažte, že jestliže  $a \in \mathbb{N}$ ,  $a > 1$  dělí  $n$ , pak existuje  $k \in \mathbb{N}$ ,  $k < n$  takové, že  $ak \equiv 0 \pmod{n}$ .

#### Řešení:

1. Dk: Nechť  $a, b \in \mathbb{Z}$ . Z předpokladu  $a \equiv b \pmod{n}$  dostáváme  $\exists k \in \mathbb{Z}: a = b + kn$ . Pak  $13a = 13b + (13k)n$  a  $13k \in \mathbb{Z}$ , tedy  $13a \equiv 13b \pmod{n}$ .

2. Dk: Nechť  $a, b, c \in \mathbb{Z}$ . Z předpokladu  $a \equiv b \pmod{n}$  a  $b \equiv c \pmod{n}$  dostáváme  $\exists k, l \in \mathbb{Z}: a = b + kn$  a  $b = c + ln$ . Pak  $a = c + (k+l)n$  a  $k+l \in \mathbb{Z}$ , tedy  $a \equiv c \pmod{n}$ .

Zkouškový speciál výpočetní:

a) Mocninu rozložíme na násobek  $n - 1 = 12$  a zbytek, rozdělíme, aplikujeme malého Fermata a dokončíme.

$$= 15^{146} - 21 \equiv 2^{146} + 5 = 2^{12 \cdot 12 + 2} + 5 = (2^{12})^{12} \cdot 2^2 + 5 \stackrel{\text{mF}}{\equiv} 1^{12} \cdot 4 + 5 = 9 \pmod{13}.$$

Výpočet je platný, protože 13 je prvočíslo a  $\text{gcd}(2, 13) = 1$ .

b) Hledáme  $x \in \mathbb{Z}$  aby  $13x + 20m = 1$

pro nějaké  $m \in \mathbb{Z}$ ,

toto děláme Euklidem

(ukážu standardního a rychlého).

Dostali jsme  $1 = 2 \cdot 20 + (-3) \cdot 13$ ,

modulo 20 to dává  $-3 \cdot 13 \equiv 1$ .

Takže  $x = -3$ . Nebo  $x = 17$ . Nebo ...

$a/b$	(20)	(13)
20	1	0
13	0	1
7	1	-1
6	-1	2
1●	2●	-3●
0		

$a/b$	(20)	(13)
20	1	0
13	0	1
-6	1	-2
1●	2●	-3●
0		

Zkouškový speciál důkazový:

a) Nechť  $a, b \in \mathbb{Z}$ . Předpoklad  $a \equiv b \pmod{n}$ .

Pak  $b = a + kn$ ,  $k \in \mathbb{Z} \rightarrow b - a = kn = n + (k-1)n \rightarrow n = b - a + (1-k)n$ ,  $1-k \in \mathbb{Z}$ .

b) Nechť  $a, b \in \mathbb{Z}$ . Předpoklad  $a \equiv b \pmod{n}$ .

Pak  $b = a + kn^2$ ,  $k \in \mathbb{Z} \rightarrow b = a + (kn)n$ ,  $kn \in \mathbb{Z}$ .

c) Nechť  $a, b \in \mathbb{Z}$ . Předpoklad  $a \equiv b \pmod{n}$ .

Pak  $b = a + kn$ ,  $k \in \mathbb{Z} \rightarrow 5b = 3b + 2a + (2k)n$ ,  $2k \in \mathbb{Z}$ .

d) Nechť  $a, b \in \mathbb{Z}$ . Předpoklad  $a \mid n$ .

Pak  $n = ka \rightarrow ka \equiv 0 \pmod{n}$ ,  $a > 1 \rightarrow k < n$ .