

DMA Domáci úkol č. 2B

Tento úkol vypracujte po přednášce a před cvičením, na druhé straně je řešení.
Pokud vám něco není jasné, zeptejte se na cvičení nebo na konzultaci.

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

Řešení:

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

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

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

2. 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	A	B	a/b	A	B
20	1	0	20	1	0
13	0	1	13	0	1
7	1	-1	-6	1	-2
6	-1	2	1●	2●	-3●
1●	2●	-3●	0		
0					