

## DMA Přednáška – Kongruence, počítání modulo

**Definice.**

Nechť  $n \in \mathbb{N}$ . Řekneme, že čísla  $a, b \in \mathbb{Z}$  jsou **kongruentní modulo  $n$** , značeno  $a \equiv b \pmod{n}$ , jestliže  $n \mid (b - a)$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ . Pro čísla  $a, b \in \mathbb{Z}$  jsou následující podmínky ekvivalentní:

- (i)  $a \equiv b \pmod{n}$ ,
- (ii) existuje  $k \in \mathbb{Z}$  takové, že  $b = a + kn$ ,
- (iii)  $a \bmod n = b \bmod n$ , tj. jsou si rovny zbytky po dělení číslem  $n$ .

**Fakt.**

Nechť  $n \in \mathbb{N}$ . Pak platí:

- (i) Pro každé  $a \in \mathbb{Z}$  je  $a \equiv a \pmod{n}$ .
- (ii) Pro každé  $a, b \in \mathbb{Z}$  platí, že  $a \equiv b \pmod{n}$  je ekvivalentní s  $b \equiv a \pmod{n}$ .
- (iii) Pro každé  $a, b, c \in \mathbb{Z}$  platí, že jestliže  $a \equiv b \pmod{n}$  a  $b \equiv c \pmod{n}$ , pak také  $a \equiv c \pmod{n}$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ , uvažujme  $a, b, u, v \in \mathbb{Z}$  takové, že  $a \equiv u \pmod{n}$  a  $b \equiv v \pmod{n}$ . Pak platí následující:

- (i)  $a + b \equiv u + v \pmod{n}$ ;
- (ii)  $a - b \equiv u - v \pmod{n}$ ;
- (iii)  $ab \equiv uv \pmod{n}$ .

**Fakt.**

Nechť  $n \in \mathbb{N}$ , uvažujme  $a \in \mathbb{Z}$ . Jestliže  $r = a \bmod n$ , tedy  $r$  je zbytek po dělení  $a$  číslem  $n$ , pak  $a \equiv r \pmod{n}$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ , uvažujme  $a, u \in \mathbb{Z}$  takové, že  $a \equiv u \pmod{n}$ . Pak pro všechna  $k \in \mathbb{N}$  platí  $a^k \equiv u^k \pmod{n}$ .

**Definice.**

Nechť  $n \in \mathbb{N}$ .

Uvažujme  $a \in \mathbb{Z}$ . Řekneme, že  $b \in \mathbb{Z}$  je **inverzní číslo (inverse number) k  $a$  modulo  $n$** , jestliže  $a \cdot b \equiv 1 \pmod{n}$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ . Pro  $a \in \mathbb{Z}$  existuje inverzní číslo modulo  $n$  právě tehdy, když  $\gcd(a, n) = 1$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ . Předpokládejme, že  $a, x \in \mathbb{Z}$  a  $x$  je inverzní prvek k  $a$  modulo  $n$ . Pak  $y \in \mathbb{Z}$  je inverzní prvek k  $a$  modulo  $n$  právě tehdy, když  $y \equiv x \pmod{n}$ .

**Věta.** (malá Fermatova věta)

Nechť  $n \in \mathbb{N}$  je prvočíslo. Je-li  $a \in \mathbb{Z}$  nesoudělné s  $n$ , pak platí  $a^{n-1} \equiv 1 \pmod{n}$ .

Pro každé  $a \in \mathbb{Z}$  platí  $a^n \equiv a \pmod{n}$ .

**Definice.**

Nechť  $n \in \mathbb{N}$ , označme  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ . Pro  $a, b \in \mathbb{Z}_n$  definujme operace

$$a \oplus b = (a + b) \bmod n,$$

$$a \odot b = (a \cdot b) \bmod n.$$

**Věta.**

Nechť  $n \in \mathbb{N}$ . Pro libovolné  $a, b, c \in \mathbb{Z}_n$  platí následující:

- (i)  $a \oplus b = b \oplus a$  (komutativita);
- (ii)  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$  (asociativita);
- (iii)  $a \oplus 0 = 0 \oplus a = a$ ;
- (iv)  $a \odot b = b \odot a$  (komutativita);
- (v)  $a \odot (b \odot c) = (a \odot b) \odot c$  (asociativita);
- (vi)  $a \odot 1 = 1 \odot a = a$ ;
- (vii)  $a \odot 0 = 0 \odot a = 0$ ;
- (viii)  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  (distributivní zákon).

**Definice.**

Uvažujme  $n \in \mathbb{N}$ .

Nechť  $a \in \mathbb{Z}_n$ . Řekneme, že  $b \in \mathbb{Z}_n$  je **inverzní prvek** k  $a$  v  $\mathbb{Z}_n$ , jestliže  $a \odot b = 1$  v  $\mathbb{Z}_n$ .

Pokud takovýto prvek  $b$  existuje, pak jej značíme  $b = a^{-1}$  a řekneme, že  $a$  je **invertibilní (invertible)** v  $\mathbb{Z}_n$ .

**Věta.**

Nechť  $n \in \mathbb{N}$ .

Uvažujme  $a \in \mathbb{Z}_n$ . Inverzní prvek  $a^{-1}$  v  $\mathbb{Z}_n$  existuje právě tehdy, když  $\gcd(a, n) = 1$ . Pokud existuje, tak je tento prvek jediný.

**Algoritmus** pro hledání inverzního prvku k  $a$  v  $\mathbb{Z}_n$ .

**0.** Například pomocí rozšířeného Euklidova algoritmu najděte  $\gcd(a, n) = Aa + Bn$ .

**1.** Jestliže  $\gcd(a, n) > 1$ , pak inverzní prvek k  $a$  v  $\mathbb{Z}_n$  neexistuje.

Pokud umíte  $\gcd(a, n)$  získat snadněji než Euklidovým algoritmem (třeba pohledem) a vyjde číslo větší než 1, je možné krok **0** přeskočit.

**2.** Jestliže  $\gcd(a, n) = 1$ , pak Bezoutova identita dává  $1 = a \cdot A + B \cdot n$ . To znamená, že  $a \cdot A \equiv 1 \pmod{n}$  a  $x = A$  je inverzní číslo k  $a$  modulo  $n$ . Pak  $a^{-1} = A \pmod{n}$ .

(Ideálního kongruentního zástupce čísla  $A$  z rozmezí  $1, 2, \dots, n-1$  získáme buď přičtením/odečtením vhodného násobku  $n$ , nebo dělením se zbytkem.)

**Definice.**

Nechť  $n \in \mathbb{N}$ , nechť  $a \in \mathbb{Z}_n$ . Řekneme, že  $b \in \mathbb{Z}_n$  je **opačný prvek** k  $a$  v  $\mathbb{Z}_n$ , jestliže  $a \oplus b = 0$  v  $\mathbb{Z}_n$ .

**Fakt.**

Nechť  $n \in \mathbb{N}$ .

(i)  $(-0) = 0$ .

(ii) Jestliže  $a \in \mathbb{Z}_n$  a  $a \neq 0$ , pak  $(-a) = n - a$ .

Odečítání: **opačné prvky**  $(-a)$  splňují  $a \oplus (-a) = 0$ .

pro  $a \in \mathbb{Z}_n$ ,  $a \neq 0$  platí  $(-a) = n - a$ .

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
2	0	2	4	6	8	10	12	0	2	4	6	8	10	12
3	0	3	6	9	12	1	4	7	10	13	2	5	8	11
4	0	4	8	12	2	6	10	0	4	8	12	2	6	10
5	0	5	10	1	6	11	2	7	12	3	8	13	4	9
6	0	6	12	4	10	2	8	0	6	12	4	10	2	8
7	0	7	0	7	0	7	0	7	0	7	0	7	0	7
8	0	8	2	10	4	12	6	0	8	2	10	4	12	6
9	0	9	4	13	8	3	12	7	2	11	6	1	10	5
10	0	10	6	2	12	8	4	0	10	6	2	12	8	4
11	0	11	8	5	2	13	10	7	4	1	12	9	6	3
12	0	12	10	8	6	4	2	0	12	10	8	6	4	2
13	0	13	12	11	10	9	8	7	6	5	4	3	2	1

**Lemma.** (Euklidovo lemma)

Nechť  $a, b, d \in \mathbb{Z}$ .

Jestliže  $d \mid (ab)$  a  $\gcd(d, a) = 1$ , pak  $d \mid b$ .

**Lemma.**

Nechť  $p, q \in \mathbb{N}$  jsou nesoudělná. Pro čísla  $a, b \in \mathbb{Z}$  platí  $a \equiv b \pmod{pq}$  právě tehdy, když  $a \equiv b \pmod{p}$  a  $a \equiv b \pmod{q}$ .

$T(a) = a^e \pmod{n}$ ,  $de \equiv 1 \pmod{n-1}$  pak  $T^{-1}(b) = b^d \pmod{n}$ .