Lineární algebra 1

Přednáška č.1

Modulární aritmetika. Množina $\mathbb{Z}_n$. Malá Fermatova věta

Irena Penev

1.10.2025

- Budeme používat následující značení:
  - $\mathbb{N}$ = množina přirozených čísel (tj. kladných celých čísel)
  - $\mathbb{N}_0$ = množina nezáporných celých čísel
  - $\mathbb{Z}$ = množina celých čísel
  - $\mathbb{Q}$ = množina racionálních čísel
  - $\mathbb{R}$ = množina reálných čísel
  - $\mathbb{C}$ = množina komplexních čísel

Tato přednáška má tři části:

1. Modulární aritmetika
2. Množina $\mathbb{Z}_n$ a Malá Fermatova věta
3. Neformální úvod do těles

1. Modulární aritmetika

- Pro $n \in \mathbb{N}$ a $m \in \mathbb{Z}$: „$n \mid m$" znamená, že m je dělitelné n, tj. $\exists k \in \mathbb{Z}$ t.ž. $m = kn$.

Definice

Nechť $n \in \mathbb{N}$. Jestliže $a, b \in \mathbb{Z}$ splňují $n \mid (a - b)$, pak říkáme, že a a b jsou *kongruentní modulo* n, což zapisujeme $a \equiv b \pmod{n}$ nebo $a \equiv_n b$.

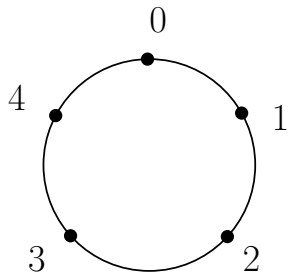
- Jinými slovy: $a \equiv b \pmod{n}$ právě když a a b dávají stejný zbytek po dělení číslem n.

Příklad

- $2 \equiv 17 \pmod{3}$;
- $-13 \equiv 8 \pmod{7}$;
- $-1 \equiv 7 \pmod{4}$;
- $2 \not\equiv 17 \pmod{2}$;
- $-13 \not\equiv 8 \pmod{5}$;
- $-1 \not\equiv 7 \pmod{6}$.

- Připomínka: $a \equiv b \pmod{n} \iff n \mid (a - b)$
- Poznámka: Pro $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ platí: $a \equiv 0 \pmod{n} \iff n \mid a$
- Poznámka: Pro pevné $n \in \mathbb{N}$, každé celé číslo je kongruentní modulo n s právě jedním z následujících čísel: $0, 1, \ldots, n - 1$.
  - Jak uvidíme, aritmetika modulo n v podstatě spočívá v počítání s n hodnotami (konkrétně $0, \ldots, n - 1$), namísto s nekonečně mnoha čísly.
  - To je užitečné pro některé aplikace (např. určité typy kódování).

- Připomínka: $a \equiv b \pmod{n} \iff n \mid (a - b)$
- Vizuálně, kongruenci modulo n si můžeme představit s pomocí „hodin s n hodinami". Např. pro $n = 5$:



- Pro nezáporné $a \in \mathbb{Z}$, začínáme na 0, pak uděláme a kroků ve směru hodinových ručiček.
  - Např. $14 \equiv 4 \pmod{5}$.
- Pro záporné $a \in \mathbb{Z}$, začínáme na 0, pak uděláme $|a| = -a$ kroků proti směru hodinových ručiček.
  - Např. $-7 \equiv 3 \pmod{5}$.

Tvrzení 1

Nechť $n \in \mathbb{N}$. Kongruence modulo n je relace ekvivalence na množině $\mathbb{Z}$, neboli:

(a) [reflexivita] $\forall a \in \mathbb{Z}$: $a \equiv_n a$;

(b) [symetrie] $\forall a, b \in \mathbb{Z}$: $a \equiv_n b \implies b \equiv_n a$

(c) [tranzitivita] $\forall a, b, c \in \mathbb{Z}$: $(a \equiv_n b \wedge b \equiv_n c) \implies a \equiv_n c$.

Důkaz. (a) a (b) jsou jednoduché. Dokažme (c). Nechť $a, b, c \in \mathbb{Z}$ jsou t.ž. $a \equiv_n b$ a $b \equiv_n c$. Dle definice, $n \mid (a - b)$ a $n \mid (b - c)$, tj. $\exists k, \ell \in \mathbb{Z}$ t.ž. $a - b = kn$ a $b - c = \ell n$. Potom platí:

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= kn + \ell n \\ &= (k + \ell)n \end{aligned}$$

$\implies n \mid (a - c)$

$\implies a \equiv_n c$

□

Tvrzení 2

Nechť $n \in \mathbb{N}$ a $a, b, c, d \in \mathbb{Z}$ t.ž. $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$. Potom platí:

(a) $a + c \equiv b + d \pmod{n}$;

(b) $a - c \equiv b - d \pmod{n}$;

(c) $ac \equiv bd \pmod{n}$.

Důkaz. (a) a (b) jsou jednoduché. Dokažme (c).

Jelikož $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, existují $k, \ell \in \mathbb{Z}$ t.ž. $a - b = kn$ a $c - d = \ell n$. Potom platí:

$$\begin{aligned} ac - bd &= ac - ad + ad - bd \\ &= a(c - d) + (a - b)d \\ &= a\ell n + knd \\ &= (a\ell + dk)n, \end{aligned}$$

a proto $n \mid (ac - bd)$, tj. $ac \equiv bd \pmod{n}$. □

Tvrzení 2

Nechť $n \in \mathbb{N}$ a $a, b, c, d \in \mathbb{Z}$ t.ž. $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$. Potom platí:

(a) $a + c \equiv b + d \pmod{n}$;

(b) $a - c \equiv b - d \pmod{n}$;

(c) $ac \equiv bd \pmod{n}$.

- Pozor: Nedělte!

$$\underbrace{6 \equiv 2 \pmod{4}}_{\text{pravdivé}} \quad \overset{\div 2}{\not\Longrightarrow} \quad \underbrace{3 \equiv 1 \pmod{4}}_{\text{nepravdivé}}$$

Tvrzení 3

Nechť $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$ t.ž. $a \equiv b \pmod{n}$. Potom platí $a^t \equiv b^t \pmod{n}$ $\forall t \in \mathbb{N}_0$.

Důkaz. Plyne z Tvrzení 2(c), které použijeme t-krát. □

- Aplikace: kritéria dělitelnosti
  - Použijeme modulární aritmetiku, abychom dokázali, že celé číslo je dělitelné 9 tehdy a jen tehdy, když je součet jeho číslic dělitelný 9 (a totéž platí pro dělitelnost 3).

- Pro $a_0, a_1, \ldots, a_k \in \{0, 1, \ldots, 9\}$:
$$\overline{a_k \ldots a_1 a_0} \quad := \quad a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0 \quad = \quad \sum_{i=0}^{k} a_i \cdot 10^i$$

Tvrzení 4

Pro každá $a_k, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$, platí:

(a) $\overline{a_k \ldots a_1 a_0} \equiv a_k + \cdots + a_1 + a_0 \pmod 9$;

(b) $9 \mid \overline{a_k \ldots a_1 a_0} \iff 9 \mid (a_k + \cdots + a_1 + a_0)$.

Tvrzení 5

Pro každá $a_k, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$, platí:

(a) $\overline{a_k \ldots a_1 a_0} \equiv a_k + \cdots + a_1 + a_0 \pmod 3$;

(b) $3 \mid \overline{a_k \ldots a_1 a_0} \iff 3 \mid (a_k + \cdots + a_1 + a_0)$.

- Dokážeme Tvrzení 4. Důkaz Tvrzení 5 je analogický.

Tvrzení 4

Pro každá $a_k, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$, platí:

(a) $\overline{a_k \ldots a_1 a_0} \equiv a_k + \cdots + a_1 + a_0 \pmod 9$;

(b) $9 \mid \overline{a_k \ldots a_1 a_0} \iff 9 \mid (a_k + \cdots + a_1 + a_0)$.

Důkaz. Nechť $a_k, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$.

Nejprve si všimněme, že $10 \equiv_9 1$, a proto $10^i \equiv_9 1^i = 1 \ \forall i \in \mathbb{N}_0$.

Pak platí:

$$\begin{aligned} \overline{a_k \ldots a_1 a_0} &= a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv_9 a_k \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \\ &= a_k + \cdots + a_1 + a_0. \end{aligned}$$

Tím je dokázáno (a).

Tvrzení 4

Pro každá $a_k, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$, platí:

(a) $\overline{a_k \ldots a_1 a_0} \equiv a_k + \cdots + a_1 + a_0 \pmod 9$;

(b) $9 \mid \overline{a_k \ldots a_1 a_0} \iff 9 \mid (a_k + \cdots + a_1 + a_0)$.

Důkaz (pokračování). Pro (b):

$$
\begin{aligned}
9 \mid \overline{a_k \ldots a_1 a_0} &\overset{\text{def.}}{\iff} \overline{a_k \ldots a_1 a_0} \equiv 0 \pmod 9 \\
&\overset{(a)}{\iff} a_k + \cdots + a_1 + a_0 \equiv 0 \pmod 9 \\
&\overset{\text{def.}}{\iff} 9 \mid (a_k + \cdots + a_1 + a_0)
\end{aligned}
$$

Tím je dokázáno (b). $\square$

2 Množina $\mathbb{Z}_n$ a Malá Fermatova věta

- Pro $n \in \mathbb{N}$ a $a \in \mathbb{Z}$, *zbytková třída čísla a modulo n* je $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.
- Např.
  - $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$;
  - $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$;
  - $[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$;
  - $[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$;
  - $[2]_3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.
- Všimněme si, že $a \in [a]_n$, protože $a \equiv a \pmod{n}$.
- Definujeme:

$$\mathbb{Z}_n \quad := \quad \{[a]_n \mid a \in \mathbb{Z}\}.$$

- Připomínka: $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.

Tvrzení 1

Nechť $n \in \mathbb{N}$. Kongruence modulo n je relace ekvivalence nad $\mathbb{Z}$, neboli:

(a) [reflexivita] $\forall a \in \mathbb{Z}$: $a \equiv_n a$;

(b) [symetrie] $\forall a, b \in \mathbb{Z}$: $a \equiv_n b \implies b \equiv_n a$

(c) [tranzitivita] $\forall a, b, c \in \mathbb{Z}$: $(a \equiv_n b \wedge b \equiv_n c) \implies a \equiv_n c$.

- Z Tvrzení 1 plyne:

Tvrzení 6

$\forall n \in \mathbb{N},\ a, b \in \mathbb{Z}$:

(a) $a \equiv b \pmod{n} \implies [a]_n = [b]_n$;

(b) $a \not\equiv b \pmod{n} \implies [a]_n \cap [b]_n = \emptyset$.

Tvrzení 6

$\forall n \in \mathbb{N},\ a, b \in \mathbb{Z}$:

(a) $a \equiv b \pmod{n} \implies [a]_n = [b]_n$;

(b) $a \not\equiv b \pmod{n} \implies [a]_n \cap [b]_n = \emptyset$.

Důkaz. Nechť $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$.

(a) Předpokládejme, že $a \equiv b \pmod{n}$. Dokážeme, že $[a]_n = [b]_n$. Stačí dokázat, že $[a]_n \subseteq [b]_n$ (důkaz opačné inkluze je analogický).

Nechť $x \in [a]_n$. Pak platí $x \equiv a \pmod{n}$. Jelikož $a \equiv b \pmod{n}$, plyne z Tvrzení 1, že $x \equiv b \pmod{n}$, a tedy $x \in [b]_n$. Tím jsme ukázali, že $[a]_n \subseteq [b]_n$, čímž je (a) dokázáno.

(b) Předpokládejme pro spor, že $a \not\equiv b \pmod{n}$, ale $[a]_n \cap [b]_n \neq \emptyset$. Nechť $x \in [a]_n \cap [b]_n$. Pak platí, že $x \equiv a \pmod{n}$ a $x \equiv b \pmod{n}$, a tedy podle Tvrzení 1 $a \equiv b \pmod{n}$, což je spor. $\square$

Tvrzení 6

$\forall n \in \mathbb{N},\ a, b \in \mathbb{Z}$:

(a) $a \equiv b \pmod{n} \implies [a]_n = [b]_n$;

(b) $a \not\equiv b \pmod{n} \implies [a]_n \cap [b]_n = \emptyset$.

- Nechť $n \in \mathbb{N}$.
  - Každé $a \in \mathbb{Z}$ je kongruentní modulo n s jedním z čísel $0, 1, \ldots, n-1$, a tedy podle Tvrzení 6(a) platí, že $[a]_n$ je rovno jednomu z $[0]_n, [1]_n, \ldots, [n-1]_n$.
  - Plyne, že $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, a zároveň $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$.
  - Na druhou stranu, žádná dva z čísel $0, 1, \ldots, n-1$ nejsou kongruentní modulo n, a tedy podle Tvrzení 6(b) platí, že $[0]_n, [1]_n, \ldots, [n-1]_n$ jsou navzájem disjunktní.
  - Plyne, že $[0]_n, [1]_n, \ldots, [n-1]_n$ tvoří „rozklad" množiny $\mathbb{Z}$, tj.
    - množiny $[0]_n, [1]_n, \ldots, [n-1]_n$ jsou neprázdné,
    - $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$,
    - $[0]_n, [1]_n, \ldots, [n-1]_n$ jsou navzájem disjunktní.

- Připomínka: Pro $n \in \mathbb{N}$:
  - $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$ pro každé $a \in \mathbb{Z}$;
  - $\mathbb{Z}_n := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

- Značení: V kontextu množiny $\mathbb{Z}_n$ ($n \in \mathbb{N}$), často píšeme prostě $0, 1, \ldots, n-1$ namísto $[0]_n, [1]_n, \ldots, [n-1]_n$ (resp.).
  - Pozor: Tohle děláme pouze v případě, že jsme už zavedli, že pracujeme s čísly v $\mathbb{Z}_n$! (Jinak jsou $0, 1, \ldots, n-1$ prostě celá čísla $0, 1, \ldots, n-1$.)
- Např. pro $n = 2$, máme
  - $[0]_2 = \{2t \mid t \in \mathbb{Z}\}$ (množina všech sudých celých čísel),
  - $[1]_2 = \{1 + 2t \mid t \in \mathbb{Z}\}$ (množina všech lichých celých čísel),

  a $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$.
  - Obvykle píšeme prostě $\mathbb{Z}_2 = \{0, 1\}$, přičemž jsou 0 a 1 technicky množiny $[0]_2$ a $[1]_2$ (resp.).

Tvrzení 2

Nechť $n \in \mathbb{N}$ a $a, b, c, d \in \mathbb{Z}$ t.ž. $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$. Potom platí:

(a) $a + c \equiv b + d \pmod{n}$;

(b) $a - c \equiv b - d \pmod{n}$;

(c) $ac \equiv bd \pmod{n}$.

- Podle Tvrzení 2 a 6, pro $n \in \mathbb{N}$ a $a, a', b, b' \in \mathbb{Z}$ t.ž. $[a]_n = [a']_n$ a $[b]_n = [b']_n$, platí:
  - $[a + b]_n = [a' + b']_n$,
  - $[a - b]_n = [a' - b']_n$, and
  - $[ab]_n = [a'b']_n$.
- Plyne, že sčítání, odčítání, násobení v $\mathbb{Z}_n$ můžeme definovat takhle: Pro $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$, definujeme
  - $[a]_n + [b]_n = [a + b]_n$;
  - $[a]_n - [b]_n = [a - b]_n$;
  - $[a]_n[b]_n = [ab]_n$.

Tvrzení 7

Pro každé $n \in \mathbb{N}$ platí:

(a) sčítání a násobení v $\mathbb{Z}_n$ jsou komutativní, tj. $\forall a, b \in \mathbb{Z}_n$: $a + b = b + a \wedge ab = ba$;

(b) sčítání a násobení v $\mathbb{Z}_n$ jsou asociativní, tj. $\forall a, b, c \in \mathbb{Z}_n$: $(a + b) + c = a + (b + c) \wedge (ab)c = a(bc)$;

(c) násobení je distributivní vzhledem ke sčítání v $\mathbb{Z}_n$, tj. $\forall a, b, c \in \mathbb{Z}_n$: $a(b + c) = ab + ac$.

- Tvrzení 7 v podstatě plyne z definicí sčítání a násobení v $\mathbb{Z}_n$, a takže ze základních vlastností sčítání a násobení v $\mathbb{Z}$.
  - Detaily necháme jako cvičení.

- Pro malé hodnoty n leze jednoduše vypsat sčítací a násobicí tabulky pro $\mathbb{Z}_n$.
- Sčítací a násobicí tabulky pro $\mathbb{Z}_2$ jsou:

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

- Obvykle vynecháváme hranaté závorky a indexy! Tedy máme následující sčítací a násobicí tabulky pro $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- Sčítací a násobicí tabulky pro $\mathbb{Z}_3$ jsou:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Připomínáme, že technicky, $0, 1, 2$ jsou množiny $[0]_3, [1]_3, [2]_3$ (resp.).

- Sčítací a násobicí tabulky pro $\mathbb{Z}_4$ jsou:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Připomínáme, že technicky, $0, 1, 2, 3$ jsou množiny $[0]_4, [1]_4, [2]_4, [3]_4$ (resp.).

- Sčítací a násobicí tabulky pro $\mathbb{Z}_5$ jsou:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Připomínáme, že technicky, $0, 1, 2, 3, 4$ jsou množiny $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$ (resp.).

$\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Nechť $n \in \mathbb{N}$.
  - Poznámka/Značení: Každé $a \in \mathbb{Z}_n$ má jediný opačný prvek, tj. číslo v $\mathbb{Z}_n$, které lze přidat číslu a, abychom dostali 0. Opačný prvek k číslu a značíme $-a$.
    - Pokud používáme hranaté závorky a indexy, pro každé $a \in \mathbb{Z}$ platí: $-[a]_n = [-a]_n = [n-a]_n$.
    - Obvykle v kontextu $\mathbb{Z}_n$ vynecháváme hranaté závorky a indexy.
  - Pro malé hodnoty n, platí:
    - v $\mathbb{Z}_2$: $-0 = 0, \quad -1 = 1;$
    - v $\mathbb{Z}_3$: $-0 = 0, \quad -1 = 2, \quad -2 = 1;$
    - v $\mathbb{Z}_4$: $-0 = 0, \quad -1 = 3, \quad -2 = 2, \quad -3 = 1;$
    - v $\mathbb{Z}_5$: $-0 = 0, \quad -1 = 4, \quad -2 = 3, \quad -3 = 2, \quad -4 = 1.$

$\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Poznámka: Pro $n = 2, 3, 5$, každé **nenulové** číslo $a \in \mathbb{Z}_n$ má (jediný) „inverzní prvek", tj. číslo v $\mathbb{Z}_n$ kterým lze vynásobit a, abychom dostali 1.
- Tohle neplatí pro $n = 4$.
- Rozdíl je v tom, že $2, 3, 5$ jsou prvočísla, zatímco 4 je složené číslo.

Věta 8

Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ jsou nesoudělná, tj. $NSD(a, n) = 1$. Pak $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{n}$, a tedy $[a]_n[b]_n = [1]_n$.

Důsledek 9

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak platí:

(a) $\forall a \in \mathbb{Z}$ t.ž. a není dělitelné p, $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{p}$, a tedy $[a]_p[b]_p = [1]_p$;

(b) $\forall a \in \mathbb{Z}_p \setminus \{0\}$, $\exists b \in \mathbb{Z}_p \setminus \{0\}$ t.ž. $ab = 1$.[a]

[a] Značení: $0 = [0]_p$ a $1 = [1]_p$.

Věta 8

Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ jsou nesoudělná, tj. $NSD(a, n) = 1$. Pak $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{n}$, a tedy $[a]_n[b]_n = [1]_n$.

Důkaz. Nejdřív dokážeme, že žádná dvě čísla z $0, a, 2a, \ldots, (n-1)a$ nejsou kongruentní modulo n (z čehož plyne, že $[0]_n, [a]_n, [2a]_n, \ldots, [(n-1)a]_n$ jsou párově odlišné).

Předpokládejme pro spor, že existují odlišné $i, j \in \{0, \ldots, n-1\}$ t.ž. $ia \equiv ja \pmod{n}$. Pak $(i-j)a \equiv 0 \pmod{n}$, tj. $n|(i-j)a$.

Jelikož $NSD(a, n) = 1$, plyne, že $n|(i-j)$, což je spor, protože $i, j \in \{0, \ldots, n-1\}$ and $i \neq j$, a tedy $0 < |i-j| < n$.

Dokázali jsme, že žádná dvě čísla z $0, a, 2a, \ldots, (n-1)a$ nejsou kongruentní modulo n.

Věta 8

Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ jsou nesoudělná, tj. $NSD(a, n) = 1$. Pak $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{n}$, a tedy $[a]_n[b]_n = [1]_n$.

Důkaz (pokračování). Připomínka: žádná dvě čísla z $0, a, 2a, \ldots, (n-1)a$ nejsou kongruentní modulo n.

Víme, že každé celé číslo je kongruentní jednomu z čísel $0, 1, \ldots, n-1$. Jelikož žádná dvě z n čísel $0, a, 2a, \ldots, (n-1)a$ nejsou kongruentní modulo n, plyne, že (právě) jedno z čísel $0, a, 2a, \ldots, (n-1)a$ je kongruentní 1 modulo n.

Jinými slovy, $\exists! b \in \{0, 1, 2, \ldots, n-1\}$ t.ž. $ba \equiv 1 \pmod{n}$, a tedy $ab \equiv 1 \pmod{n}$ a $[a]_n[b]_n = [1]_n$. $\square$

Věta 8

Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ jsou nesoudělná, tj. $NSD(a, n) = 1$. Pak $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{n}$, a tedy $[a]_n[b]_n = [1]_n$.

Důsledek 9

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak platí:

(a) $\forall a \in \mathbb{Z}$ t.ž. a není dělitelné p, $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{p}$, a tedy $[a]_p[b]_p = [1]_p$;

(b) $\forall a \in \mathbb{Z}_p \setminus \{0\}$, $\exists b \in \mathbb{Z}_p \setminus \{0\}$ t.ž. $ab = 1$.[a]

[a] Značení: $0 = [0]_p$ a $1 = [1]_p$.

Důkaz. Jelikož p je prvočíslo, pro každé $a \in \mathbb{Z}$ t.ž. $p \not| a$ platí $NSD(a, p) = 1$, a proto (a) plyne z Věty 8.

Část (b) plyne z (a). Vskutku, nechť $a \in \mathbb{Z}_p \setminus \{0\}$. Pak existuje celé číslo $a' \in \{1, \ldots, p-1\}$ t.ž. $a = [a']_p$. Podle (a), $\exists b' \in \mathbb{Z}$ t.ž. $[a']_p[b']_p = [1]_p$, tj. pro $b := [b']_p$ platí $ab = 1$. $\square$

Věta 8

Nechť $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ jsou nesoudělná, tj. $NSD(a, n) = 1$. Pak $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{n}$, a tedy $[a]_n[b]_n = [1]_n$.

Důsledek 9

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak platí:

(a) $\forall a \in \mathbb{Z}$ t.ž. a není dělitelné p, $\exists b \in \mathbb{Z}$ t.ž. $ab \equiv 1 \pmod{p}$, a tedy $[a]_p[b]_p = [1]_p$;

(b) $\forall a \in \mathbb{Z}_p \setminus \{0\}$, $\exists b \in \mathbb{Z}_p \setminus \{0\}$ t.ž. $ab = 1$.[a]

[a] Značení: $0 = [0]_p$ a $1 = [1]_p$.

- Důsledek 9 říká, že pro každé prvočíslo p, každé číslo v $\mathbb{Z}_p \setminus \{0\}$ má inverzní prvek.
- Malá Fermatova věta je silnější verze Důsledku 9, v tom smyslu, že dává vzorec pro ten inverzní prvek.

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod{p}$.

- Malou Fermatovu větu dokážeme, ale nejdříve ji přeformulujeme dvěma způsoby.
- Pro n a $a \in \mathbb{Z}_n$, mocniny čísla a definujeme rekurzivně takto:
  - $a^0 = 1$ (kde $1 := [1]_n$);
  - $a^{m+1} = a^m a$ pro každé $m \in \mathbb{N}_0$.

  Tedy pro $m \in \mathbb{N}$, jak obvykle platí

$$a^m = \underbrace{a \cdot \cdots \cdot a}_{m},$$

  přičemž násobení je v $\mathbb{Z}_n$.
- Nyní přeformulujeme dvěma způsoby.

- Stará verze:

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod{p}$.

- Dvě nové verze:

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $([a]_p)^{p-1} = [1]_p$.

- Poznámka:
  $a^{p-1} \equiv 1 \pmod{p} \iff [a^{p-1}]_p = [1]_p \iff ([a]_p)^{p-1} = [1]_p$

Malá Fermatova věta

Pro každé prvočíslo $p \in \mathbb{N}$ a každé $a \in \mathbb{Z}_p \setminus \{0\}$, platí $a^{p-1} = 1$.

Malá Fermatova věta

Pro každé prvočíslo $p \in \mathbb{N}$ a každé $a \in \mathbb{Z}_p \setminus \{0\}$, platí $a^{p-1} = 1$.

- Nechť $p \in \mathbb{N}$ je **prvočíslo** a nechť $a \in \mathbb{Z}_p \setminus \{0\}$.
  - Dle Malé Fermatovy věty, a^{p-2} je inverzní prvek k číslu a, tj. vynásobíme-li číslo a číslem a^{p-2} (zleva nebo zprava), dostaneme 1:
    - $a \cdot a^{p-2} = a^{p-2} \cdot a = 1$.
  - Navíc, a^{p-2} je **jediný** inverzní prvek k číslu a v $\mathbb{Z}_p$.
    - Vskutku, jestliže pro $b \in \mathbb{Z}_p$ platí $ab = 1$, pak po vynásobení obou stran a^{p-2} (zleva), dostaneme

$$\underbrace{a^{p-2} \cdot a}_{=a^{p-1}=1} b \quad = \quad a^{p-2} \cdot 1,$$

      a tedy $b = a^{p-2}$.
  - Inverzní prvek k číslu a značíme a^{-1}.
  - Dle Malé Fermatovy věty platí $a^{-1} = a^{p-2}$.
  - Pro malé hodnoty prvočísla p je jednodušší vyčíst a^{-1} z násobicí tabulky pro $\mathbb{Z}_p$ než vypočítat a^{p-2}.

$\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- v $\mathbb{Z}_2$: $1^{-1} = 1$;
- v $\mathbb{Z}_3$: $1^{-1} = 1, \quad 2^{-1} = 2$;
- v $\mathbb{Z}_5$: $1^{-1} = 1, \quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4$.

- Pro důkaz Malé Fermatovy věty budeme potřebovat „faktoriál", který definujeme takto:
  - $0! := 1$;
  - $(n+1)! := n! \cdot (n+1)$ pro každé $n \in \mathbb{N}_0$.
- Tedy pro $n \in \mathbb{N}$, platí $n! = 1 \cdot 2 \cdot \cdots \cdot n$.
- „$n!$" čteme „n faktoriál".

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod{p}$.

Důkaz. Nechť $p \in \mathbb{N}$ je prvočíslo. Nechť $a \in \mathbb{Z}$ je t.ž. $p \nmid a$.

Podobně jako v důkazu Věty 8, žádná dvě čísla z $0, a, 2a, \ldots, (p-1)a$ nejsou kongruentní modulo p. Pro úplnost uvedeme celý důkaz.

Předpokládejme pro spor, že existují odlišné $i, j \in \{0, \ldots, p-1\}$ t.ž. $ia \equiv ja \pmod{p}$. Pak $(i-j)a \equiv 0 \pmod{p}$, tj. $p|(i-j)a$. Jelikož p je prvočíslo, které neděli a, plyne že $p|(i-j)$, což je spor, protože $i, j \in \{0, \ldots, p-1\}$ a $i \neq j$, a tedy $0 < |i-j| < p$. Dokázali jsme, že žádná dvě čísla z $0, a, 2a, \ldots, (p-1)a$ nejsou kongruentní modulo p.

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod{p}$.

Důkaz (pokračovaní). Připomínka: Žádná dvě čísla z $0, a, 2a, \ldots, (p-1)a$ nejsou kongruentní modulo p.

Jelikož je každé celé číslo kongruentní modulo p s (právě) jedním z čísel $0, 1, \ldots, p-1$, plyne, že existuje nějaká permutace $r_1, \ldots, r_{p-1}$ posloupností $1, \ldots, p-1$ t.ž.

- $a \equiv r_1 \pmod{p}$;
- $2a \equiv r_2 \pmod{p}$;

  $\vdots$
- $(p-1)a \equiv r_{p-1} \pmod{p}$.

Plyne, že

$$\underbrace{a \cdot 2a \cdot \cdots \cdot (p-1)a}_{=(p-1)!a^{p-1}} \equiv \underbrace{r_1 r_2 \ldots r_{p-1}}_{=(p-1)!} \pmod{p},$$

a tedy $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

Malá Fermatova věta

Pro každé $p \in \mathbb{N}$ a $a \in \mathbb{Z}$ t.ž. p je prvočíslo a $p \nmid a$, platí $a^{p-1} \equiv 1 \pmod{p}$.

Důkaz (pokračovaní). Připomínka: $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

Nyní platí

$$(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p},$$

tj. $p \mid \Big((a^{p-1} - 1)(p-1)!\Big)$.

Jelikož p je prvočíslo, p and $(p-1)!$ jsou nesoudělná čísla, tj. $NSD(p, (p-1)!)$. Plyne, že $p \mid (a^{p-1} - 1)$, a tedy $a^{p-1} \equiv 1 \pmod{p}$, což jsme chtěli dokázat. $\square$

3. Neformální úvod do těles

- Formálně/axiomaticky probereme tělesa později (za několik týdnů).
- Prozatím dáme několik příkladů těles:
  - těleso $\mathbb{Q}$ racionálních čísel;
  - těleso $\mathbb{R}$ reálných čísel;
  - těleso $\mathbb{C}$ komplexních čísel;
  - těleso $\mathbb{Z}_p$, kde p je **prvočíslo**.
    - Jestliže $n \in \mathbb{N}$ není prvočíslo, pak $\mathbb{Z}_n$ **není** těleso.

- Každé těleso je vybaveno dvěma operacemi: sčítáním a násobením.
- Tyto operace jsou komutativní a asociativní, a násobení je distributivní vzhledem ke sčítání:
  - $a + b = b + a \wedge ab = ba$;
  - $(a + b) + c = a + (b + c) \wedge (ab)c = a(bc)$;
  - $a(b + c) = ab + ac$.
- Každé těleso má „aditivní neutrální prvek" 0 a „multiplikativní neutrální prvek" 1, pro které platí

$$a + 0 = 0 + a = a \qquad \text{and} \qquad a \cdot 1 = 1 \cdot a = a$$

pro každé číslo a v tělese.

- Každé číslo a v tělese má „opačný prvek", který značíme $-a$, a pro které platí $a + (-a) = 0$.
- Například:
  - opačný prvek k číslu $\sqrt{17}$ v $\mathbb{R}$ je $-\sqrt{17}$, protože $\sqrt{17} + (-\sqrt{17}) = 0$ v $\mathbb{R}$.
  - opačný prvek k číslu $2 - i$ v $\mathbb{C}$ je $-2 + i$, protože $(2 - i) + (-2 + i) = 0$ v $\mathbb{C}$;
  - opačný prvek k číslu 3 v $\mathbb{Z}_5$ je 2 (což značíme $-3 = 2$), protože $3 + 2 = 0$ v $\mathbb{Z}_5$;
  - opačný prvek k číslu 4 v $\mathbb{Z}_5$ je 1 (což značíme $-4 = 1$), protože $4 + 1 = 0$ v $\mathbb{Z}_5$;
  - opačný prvek k číslu 2 v $\mathbb{Z}_3$ je 1 (což značíme $-2 = 1$), protože $2 + 1 = 0$ v $\mathbb{Z}_3$.
- Namísto $a + (-a)$ obecně píšeme $a - a$.

- Každé **nenulové** číslo a v tělese má „inverzní prvek", které značíme a^{-1}, a pro které platí $a \cdot a^{-1} = 1$.
- Například:
  - inverzní prvek k číslu $\sqrt{17}$ v $\mathbb{R}$ je $\frac{1}{\sqrt{17}}$, protože $\sqrt{17} \cdot \frac{1}{\sqrt{17}} = 1$ v $\mathbb{R}$;
  - inverzní prvek k číslu $2 - i$ je $\frac{2}{5} + \frac{1}{5}i$, protože $(2 - i)(\frac{2}{5} + \frac{1}{5}i) = 1$ v $\mathbb{C}$;
  - inverzní prvek k číslu 3 v $\mathbb{Z}_5$ je 2 (což značíme $3^{-1} = 2$), protože $3 \cdot 2 = 1$ v $\mathbb{Z}_5$;
  - inverzní prvek k číslu 4 v $\mathbb{Z}_5$ je 4 (což značíme $4^{-1} = 4$), protože $4 \cdot 4 = 1$ v $\mathbb{Z}_5$;
  - inverzní prvek k číslu 2 v $\mathbb{Z}_3$ je 2 (což značíme $2^{-1} = 2$), protože $2 \cdot 2 = 1$ v $\mathbb{Z}_3$.

- **Poznámka:** Když pracujeme s čísly v $\mathbb{Z}_p$ (kde p je prvočíslo), je užitečné mít před sebou sčítací a násobicí tabulky pro $\mathbb{Z}_p$, protože z nich lze vyčíst opačné a inverzní prvky: pro dané číslo $a \in \mathbb{Z}_p$ prostě se podíváme, které číslo k a přičteme, abychom dostali 0 (tohle je opačný prvek k číslu a), a (pokud $a \neq 0$) jakým číslem a vynásobíme, abychom dostali 1 (tohle je inverzní prvek k číslu a).

$\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- **Varování:** Následující množiny **nejsou** tělesa: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$ (kde $n \in \mathbb{N}$ **není** prvočíslo).

Během příštích několika týdnů (dokud neprobereme tělesa formálně, tj. axiomaticky) budeme předpokládat, že uvažované těleso $\mathbb{F}$ je jedno z následujících: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ nebo $\mathbb{Z}_p$ (kde p je prvočíslo). Nicméně, všechno, co dokážeme během těchto přednášek, bude platit pro libovolná tělesa $\mathbb{F}$, nejen pro tato čtyři.

- Pro tělesa se běžně používají symboly $\mathbb{F}$ (anglicky: „field") nebo $\mathbb{T}$ („těleso").