DMA Přednáška – Dělitelnost

Definice.
Nechť $a, b \in \mathbb{Z}$. Řekneme, že a **dělí** b, značeno $a \mid b$, jestliže existuje $k \in \mathbb{Z}$ takové, že $b = k \cdot a$.
V takovém případě říkáme, že a je **faktor** b a že b je **násobek** a. Také říkáme, že b je **dělitelné** a.

Fakt.
Pro každé $a \in \mathbb{Z}$ platí $1 \mid a, \quad a \mid a \quad \text{a} \quad a \mid 0$.

Věta.
Nechť $a, b, c \in \mathbb{Z}$.
(i) Jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$.
(ii) $a \mid b$ právě tehdy, když $|a| \mid |b|$.
(iii) Jestliže $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

Věta.
Nechť $a, b \in \mathbb{N}$. Jestliže $a \mid b$ a $b \mid a$, pak $a = b$.

Definice.
Nechť $a \in \mathbb{N}$, $a \geq 2$.
Řekneme, že je to **prvočíslo** (**prime**), jestliže jediná přirozená čísla, která a dělí, jsou 1 a a.
Řekneme, že a je **složené číslo**, jestliže to není prvočíslo.

Definice.
Nechť $a, b \in \mathbb{Z}$.
Číslo $d \in \mathbb{N}$ je **společný dělitel** čísel a, b, jestliže $d \mid a$ a $d \mid b$.
Číslo $d \in \mathbb{N}$ je **společný násobek** čísel a, b, jestliže $a \mid d$ a $b \mid d$.

Definice.
Nechť $a, b \in \mathbb{Z}$.
Definujeme jejich **největší společný dělitel**, značeno $\gcd(a, b)$, jako největší prvek množiny jejich společných dělitelů, pokud je alespoň jedno z a, b nenulové. Jinak definujeme $\gcd(0, 0) = 0$.

Definujeme jejich **nejmenší společný násobek**, značeno $\operatorname{lcm}(a, b)$, jako nejmenší prvek množiny jejich společných násobků, pokud jsou a, b obě nenulové. Jinak definujeme $\operatorname{lcm}(a, 0) = \operatorname{lcm}(0, b) = 0$.

Definice.
Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná**, jestliže $\gcd(a, b) = 1$.

Fakt.
Nechť p je prvočíslo. Pak pro libovolné $a \in \mathbb{Z}$ platí, že buď je s p nesoudělné, nebo p dělí a.

Fakt.
Nechť $a \in \mathbb{N}$. Pak $\gcd(a, 0) = a$, $\operatorname{lcm}(a, 0) = 0$ a $\gcd(a, a) = \operatorname{lcm}(a, a) = a$.

Fakt.
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(|a|, |b|)$ a $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.

Věta.
Nechť $a, b \in \mathbb{Z}$. Pak $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$.

Věta. (o dělení se zbytkem)
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Pak existují $q \in \mathbb{Z}$ a $r \in \mathbb{N}_0$ takové, že $a = qd + r$ a $0 \leq r < |d|$.
Čísla q a r jsou jednoznačně určena.

Definice.
Číslu r říkáme **zbytek** při dělení a číslem d a značíme jej $r = a \bmod d$.
Číslu q říkáme **částečný podíl**.

Fakt.
Nechť $a, b \in \mathbb{Z}$, $a \neq 0$. Pak $a \mid b$ právě tehdy, když $b \bmod |a| = 0$, tedy zbytek po dělení b číslem $|a|$ je 0.

Lemma.
Nechť $a > b \in \mathbb{N}$, nechť $q, r \in \mathbb{N}_0$ splňují $a = qb + r$. Pak platí následující:
(i) $d \in \mathbb{N}$ je společný dělitel a, b právě tehdy, když je to společný dělitel b, r.
(ii) $\gcd(a, b) = \gcd(b, r)$.

Euklidův algoritmus pro nalezení $\gcd(a, b)$ pro $a > b \in \mathbb{N}$.

Verze 1.
Iniciace: $r_0 := a$, $r_1 := b$, $k := 0$.
Krok: $k := k + 1$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$
Opakovat dokud nenastane $r_{k+1} = 0$.
Pak $\gcd(a, b) = r_k$.

nebo

Verze 2.
`procedure` $gcd(a, b$: integer)
`repeat`
  $r := a \bmod b$;
  $a := b$; $b := r$;
 `until` $b = 0$;
`output:` a;

Věta. (Bezoutova věta/rovnost)
Nechť $a, b \in \mathbb{Z}$. Pak existují $A, B \in \mathbb{Z}$ takové, že $\gcd(a, b) = Aa + Bb$.

Rozšířený Euklidův algoritmus pro nalezení $\gcd(a, b) = Aa + Bb$ pro $a > b \in \mathbb{N}$.

Verze 1.

Inicializace: $r_0 := a$, $r_1 := b$, $k := 0$,
$A_0 := 1$, $A_1 := 0$, $B_0 := 0$, $B_1 := 1$.

Krok: $k := k + 1$, , $q_k := \left\lfloor \frac{r_{k-1}}{r_k} \right\rfloor$,
$r_{k+1} := r_{k-1} - q_k r_k$,
$A_{k+1} := A_{k-1} - q_k A_k$,
$B_{k+1} := B_{k-1} - q_k B_k$.

Opakovat dokud nenastane $r_{k+1} = 0$.
Pak $\gcd(a, b) = r_k = A_k a + B_k b$.

nebo

Verze 2.

`procedure` *gcd-Bezout*(a, b: integer)
$A_0 := 1$; $A_1 := 0$; $B_0 := 0$; $B_1 := 1$;
`repeat`
  $q_k := \left\lfloor \frac{r_{k-1}}{r_k} \right\rfloor$;
  $r := a - qb$;
  $a := b$; $b := r$;
  $r_a := A_0 - qA_1$;
  $r_b := B_0 - qB_1$;
  $a := b$; $b := r$;
  $A_0 := A_1$; $A_1 := r_a$;
  $B_0 := B_1$; $B_1 := r_b$;
`until` $b = 0$;
`output:` a, A_0, B_0;

Lemma. (Euklidovo lemma)
Nechť $a, b, d \in \mathbb{Z}$.
Jestliže $d \mid (ab)$ a $\gcd(d, a) = 1$, pak $d \mid b$.

Prvočísla v první stovce:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$

Lemma.
Nechť $a_1, \dots, a_m \in \mathbb{N}$ a p je prvočíslo.
Jestliže $p \mid (a_1 a_2 \cdots a_m)$, pak existuje i takové, že $p \mid a_i$.

Lemma.
Pro každé $a \in \mathbb{N}$, $a \geq 2$ existuje prvočíslo, které jej dělí.

Věta. (Fundamentální věta aritmetiky, prvočíselný rozklad)
Nechť $n \in \mathbb{N}$. Pak existují prvočísla $p_1, p_2, \dots, p_m$ a exponenty $k_1, k_2, \dots, k_m \in \mathbb{N}_0$ takové, že

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} = \prod_{i=1}^{m} p_i^{k_i}.$$

Jestliže přidáme podmínky $p_1 < p_2 < \ldots < p_m$ a $k_i > 0$, tak je tato dekompozice jednoznačně určena.

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

$$\begin{aligned} a \oplus b &= (a + b) \bmod n, \\ a \odot b &= (a \cdot b) \bmod n. \end{aligned}$$

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 $a^{-1} = A \bmod n$.
(Ideálního kongruentního zástupce čísla A z rozmezí $1, 2, \ldots, n-1$ 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 $p, p \in \mathbb{N}$ jsou nesoudělná. Pro čísla $a, b \in \mathbb{Z}$ platí $a \equiv b \pmod{pq}$ právě tehdy, když $a \equiv b \pmod{p}$ a $a \equiv b \pmod{q}$.

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

DMA Přednáška – Rovnice nad $\mathbb{Z}$

Definice.
Pojmem **lineární diofantická rovnice** označujeme libovolnou rovnici typu $ax + by = c$ s neznámými x, y, kde $a, b, c \in \mathbb{Z}$ a vyžadujeme také řešení $x, y \in \mathbb{Z}$.

Věta.
Nechť $a, b, c \in \mathbb{Z}$. Lineární diofantická rovnice $ax+by = c$ má alespoň jedno řešení právě tehdy, když c je násobkem $\gcd(a, b)$.

Definice.
Je-li dána lineární diofantická rovnice $ax + by = c$, pak definujeme její **přidruženou homogenní rovnici** jako $ax + by = 0$.

Věta.
Nechť $a, b, c \in \mathbb{Z}$. Uvažujme lineární diofantickou rovnici $ax + by = c$.
Nechť $(x_p, y_p) \in \mathbb{Z}^2$ je nějaké její **partikulární** řešení.
Dvojice $(x_0, y_0) \in \mathbb{Z}^2$ je řešení této rovnice právě tehdy, když
existuje $(x_h, y_h) \in \mathbb{Z}^2$ takové, že $(x_0, y_0) = (x_p, y_p) + (x_h, y_h)$ a (x_h, y_h) řeší přidruženou homogenní rovnici.

Věta.
Uvažujme rovnici $ax + by = 0$ pro $a, b \in \mathbb{Z}$. Množina všech jejích celočíselných řešení je

$$\left\{\left(k\frac{b}{\gcd(a,b)}, -k\frac{a}{\gcd(a,b)}\right) : k \in \mathbb{Z}\right\}.$$

Algoritmus pro nalezení všech celočíselných řešení rovnice $ax + by = c$.
0. Například pomocí rozšířeného Euklidova algoritmu najděte $\gcd(a, b) = Aa + Bb$.
1. Jestliže c není násobkem $\gcd(a, b)$, pak řešení rovnice neexistuje.
2. Případ $\gcd(a, b)$ dělí c:
a) Získanou rovnost $aA + bB = \gcd(a, b)$ vynásobte číslem $c' = \frac{c}{\gcd(a,b)} \in \mathbb{Z}$ tak, aby se zachovaly koeficienty a, b, a dostanete $a(Ac') + b(Bc') = c$, tudíž i jedno partikulární řešení $x_p = Ac'$, $y_p = Bc'$ neboli vektor (Ac', Bc').
b) Přidruženou homogenní rovnici $ax + by = 0$ zkraťte číslem $\gcd(a, b)$ na tvar $a'x + b'y = 0$, což dává řešení $x_h = b'k$, $y_h = -a'k$ neboli dvojice $(b'k, -a'k)$ pro $k \in \mathbb{Z}$, popřípadě $x_h = -b'k$, $y_h = a'k$ neboli dvojice $(-b'k, a'k)$.
c) Sečtením partikulárního a obecného homogenního řešení získáte množinu všech celočíselných řešení

$$\{(x_p + kb', y_p - ka') : k \in \mathbb{Z}\} \text{ neboli } x = x_p + kb',\ y = x_p - ka' \text{ pro } k \in \mathbb{Z},$$

popřípadě verzi s mínusem u y_h.

Definice.
Termínem **lineární kongruence** označujeme rovnice typu $ax \equiv b \pmod{n}$, kde $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ a hledáme celočíselná řešení x.

Fakt.
Nechť $n \in \mathbb{N}$. Uvažujme $a, b \in \mathbb{Z}$. Číslo $x_0 \in \mathbb{Z}$ řeší lineární kongruenci $ax \equiv b \pmod{n}$ právě tehdy, když pro nějaké $y_0 \in \mathbb{Z}$ řeší vektor (x_0, y_0) diofantickou rovnici $ax + ny = b$.

Věta.
Nechť $n \in \mathbb{N}$, uvažujme $a, b \in \mathbb{Z}$.
(i) Jestliže b není násobkem $\gcd(a, n)$, tak řešení rovnice $ax \equiv b \pmod{n}$ neexistuje.
(ii) Jestliže $\gcd(a, n)$ dělí b, tak rovnice $ax \equiv b \pmod{n}$ má nějaké řešení $x_p \in \mathbb{Z}$. Označme $n' = \frac{n}{\gcd(a,n)}$. Množina všech řešení lineární kongruence $ax \equiv b \pmod{n}$ je

$$\{x_p + kn' : k \in \mathbb{Z}\}.$$

Věta.
Nechť $n \in \mathbb{N}$, uvažujme kongruenci $ax \equiv b \pmod{n}$ pro nějaká $a, b \in \mathbb{Z}$. Nechť x_p je nějaké její partikulární řešení. Definujme čísla $x_i = x_p + \frac{n}{\gcd(a,n)} i$ pro $i = 0, 1, \ldots, \gcd(a, b) - 1$. Množina všech řešení dané kongruence je sjednocením množin $\{x_i + kn : k \in \mathbb{Z}\}$ pro $i = 0, 1, \ldots, \gcd(a, b) - 1$, tyto množiny jsou navzájem disjunktní.

Věta.
Nechť $n \in \mathbb{N}$. Uvažujme kongruenci $ax \equiv b \pmod{n}$ pro nějaká $a, b \in \mathbb{Z}$, nechť x_p je nějaké její řešení.
Číslo $x_0 \in \mathbb{Z}$ je řešením kongruence $ax \equiv b \pmod{n}$ právě tehdy, když existuje $x_h \in \mathbb{Z}$, které splňuje $x_0 = x_p + x_h$ a je řešením přidružené homogenní rovnice $ax \equiv 0 \pmod{n}$.

• Množinu všech řešení rovnice $a \odot x = b$ v $\mathbb{Z}_n$ získáme tak, že v množině všech řešení kongruence $ax \equiv b \pmod{n}$ nahradíme všechna čísla jejich zbytky po dělení n neboli jejich kongruentními zástupci z množiny $\mathbb{Z}_n$.

Věta.
Nechť $n \in \mathbb{N}$, uvažujme rovnici $ax = b$ v $\mathbb{Z}_n$ pro nějaká $a, b \in \mathbb{Z}_n$.
(i) Jestliže $\gcd(a, n)$ nedělí b, pak řešení neexistuje.
(ii) Předpokládejme, že $\gcd(a, n)$ dělí b. Nechť $x_p \in \mathbb{Z}$ řeší kongruenci $ax \equiv \pmod{n}$, označme $n' = \frac{n}{\gcd(a,n)}$.
Nechť $x_0 = \min\{x_p + kn' : k \in \mathbb{Z} \text{ a } x_p + kn' \geq 0\}$. Pak množina všech řešení rovnice $ax = b$ v $\mathbb{Z}_n$ je

$$\{x_0 + in' : i = 0, 1, \dots, \gcd(a, n) - 1\}.$$

Jde o $\gcd(a, n)$ různých čísel.

Soustavy lineárních kongruencí:
Jsou dány moduly $n_1, \dots, n_m \in \mathbb{N}$ a pravé strany $b_1, \dots, b_m \in \mathbb{Z}$. Hledáme celá čísla x taková, že

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Věta.
Uvažujme moduly $n_1, n_2, \dots, n_m \in \mathbb{N}$ a čísla $b_1, b_2, \dots, b_m \in \mathbb{Z}$.
Nechť x_p je nějaké řešení soustavy kongruencí

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Číslo x_0 je také řešením této soustavy právě tehdy, pokud existuje číslo x_h takové, že $x_0 = x_p + x_h$ a x_h je řešením přidružené homogenní soustavy kongruencí

$$\begin{aligned} x &\equiv 0 \pmod{n_1} \\ x &\equiv 0 \pmod{n_2} \\ &\vdots \\ x &\equiv 0 \pmod{n_m}. \end{aligned}$$

Věta. (Čínská věta o zbytcích)
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$, $b_1, b_2, \dots, b_m \in \mathbb{Z}$. Uvažujme soustavu rovnic

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Jestliže jsou všechna čísla n_i po dvou nesoudělná, pak má tato soustava řešení $x_0 \in \mathbb{Z}$. Množina všech řešení je $\{x_0 + kn : k \in \mathbb{Z}\}$, kde $n = n_1 n_2 \cdots n_m$.

Algoritmus pro řešení soustavy kongruencí $x \equiv b_1 \pmod{n_1}, x \equiv b_2 \pmod{n_2}, \ldots, x \equiv b_m \pmod{n_m}$ pro případ, že jsou všechna čísla n_i po dvou nesoudělná.
1. Označte $n = n_1 n_2 \cdots n_m$ a $N_i = \frac{n}{n_i}$ pro všechna i.
2. Pro každé i najděte inverzní číslo k N_i vzhledem k násobení modulo n_i.
3. Nechť $x_p = \sum_{i=1}^{m} b_i N_i x_i$. Množina všech řešení soustavy je $\{x_p + kn : k \in \mathbb{Z}\}$.

DMA Přednáška – Relace

Definice.

Nechť A, B jsou množiny. Libovolná podmnožina $R \subseteq A \times B$ se nazývá **relace** z A do B.

Jestliže $(a, b) \in R$, pak to značíme aRb a řekneme, že a **je v relaci k** b vzhledem k R.

Definice.

Nechť A je množina. Řekneme, že R je relace na A, jestliže je to relace z A do A.

Příklad: Uvažujme malou školu se studenty **F**rodo, **M**erry, **P**ippin a **S**am, škola nabízí kursy **c**estování, **d**iskrétní matiky, **e**lfštiny a **f**rodologie.

Frodo si zapsal cestování a elfštinu, Merry a Pippin si zapsali cestování a diskrétku, Sam si zapsal elfštinu a frodologii.

Definice.

Nechť $A = \{a_1, a_2, \ldots, a_m\}$ a $B = \{b_1, b_2, \ldots, b_n\}$ jsou množiny. Pro relaci R z A do B definujeme **matici relace** $M_R = (m_{ij})_{i,j=1}^{m,n}$ předpisem

$$m_{ij} = \begin{cases} 1, & (a_i, b_j) \in R; \\ 0, & (a_i, b_j) \notin R. \end{cases}$$

Příklad: Nechť je A množina všech měst (v České republice, aby jich nebylo tolik). Nechť R_1 je relace na A definovaná tak, že aR_1b právě tehdy, jestli se dá z a do b dostat autobusem, a R_2 je relace na A definovaná tak, že aR_2b právě tehdy, jestli se dá z a do b dostat vlakem.

Definice.

Nechť R je relace z nějaké množiny A do nějaké množiny B. Definujeme **relaci inverzní k** R, značeno R^{-1}, jako relaci z B do A předpisem

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

Tedy

$$bR^{-1}a \text{ právě tehdy, když } aRb.$$

Definice.
Nechť R je relace z nějaké množiny A do nějaké množiny B a S je relace z B do nějaké množiny C. Definujeme jejich **složení** $S \circ R$ jako relaci z A do C definovanou

$$S \circ R = \big\{(a,c) \in A \times C : \exists b \in B \colon\ [(a,b) \in R \wedge (b,c) \in S]\big\}.$$

Příklad: Připomeňme, že $A = \{F, M, P, S\}$ jsou studenti, $B = \{b, c, d, e\}$ kursy a relace
$R = \{(F,c), (F,e), (M,c), (M,d), (P,c), (P,d), (S,e), (S,f)\}$ říká, který student si zapsal jaký kurs.
Množina učitelů $C = \{\mathcal{E}$lrond, $\mathcal{G}$andalf, $\mathcal{T}$om Bombadil$\}$,
relace který kurs je učen kterým učitelem: $S = \{(c,\mathcal{G}), (d,\mathcal{T}), (e,\mathcal{E}), (f,\mathcal{G})\}$.

Fakt.
Nechť R je relace z nějaké množiny A do nějaké množiny B, S je relace z B do nějaké množiny C a T je relace z C do nějaké množiny D. Pak $(T \circ S) \circ R = T \circ (S \circ R)$.

Definice.
Nechť R je relace na nějaké množině A. Pak definujeme její **mocninu** rekurzivně jako
(0) $R^1 = R$;
(1) $R^{n+1} = R \circ R^n$ pro $n \in \mathbb{N}$.

Definice.
Nechť R je relace na množině A.
Řekneme, že R je **reflexivní**, jestliže pro všechna $a \in A$ platí aRa.
Řekneme, že R je **symetrická**, jestliže pro všechna $a, b \in A$ platí $aRb \implies bRa$.
Řekneme, že R je **antisymetrická**, jestliže pro všechna $a, b \in A$ platí $(aRb \wedge bRa) \implies a = b$.
Řekneme, že R je **tranzitivní**, jestliže pro všechna $a, b, c \in A$ platí $(aRb \wedge bRc) \implies aRc$.

DMA Přednáška – Speciální relace

Definice.
Nechť R je relace na nějaké množině A. Řekneme, že R je **částečné uspořádání**, jestliže je reflexivní, antisymetrická a tranzitivní.
V tom případě značíme relaci $\preceq$ a řekneme, že dvojice $(A, \preceq)$ je **částečně uspořádaná množina**.

Fakt.
Jestliže je $(A, \preceq)$ částečně uspořádaná množina, pak je i $(A, \preceq^{-1})$ částečně uspořádaná množina.

Definice.
Nechť $(A, \preceq)$ je částečné uspořádání. Definujeme relaci $\prec$ na A předpisem
$a \prec b$ právě tehdy, když $a \preceq b$ a $a \neq b$.

Algoritmus pro vytváření Hasseova diagramu částečného uspořádání $(A, \preceq)$ pro konečnou množinu A.
1. Najít prvky $a \in A$, které v ostrém srovnání nikdy nejsou napravo, tedy v pozici $x \prec a$ (nevedou do nich šipky). Dát do spodní řady. Odebrat tyto prvky z A, odebrat všechna srovnání s těmito body.
2. Ve zbylé množině hledat prvky, které v ostrém srovnání nikdy nejsou napravo (nevedou do nich šipky). Dát do druhé řady zdola, odebrat je z množiny prvků.
Spojit horní řadu s dolní tam, kde je relace, odebrat tyto dvojice ze seznamu srovnání.
3. Ve zbylé množině hledat prvky, které ve srovnání $\prec$ nikdy nejsou napravo (nevedou do nich šipky). Vytvořit z nich novou řadu nahoře, odebrat z množiny prvků.
Spojit horní řadu s nižšími tam, kde je relace, přičemž postupujeme shora dolů (nejprve spojujeme horní řadu s tou pod ní, pak horní s tou o jedno níže, atd. až po horní s dolní). Existující dvojice vyškrtáváme ze seznamu, ale do grafu je kreslíme jen tehdy, pokud ještě tuto cestu nelze absolvovat pomocí již nakreslených spojnit, a to vždy směrem zdola nahoru.
4. Opakovat krok 3., dokud jsou v množině body.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina a $\prec$ odpovídající odvozená relace. Nechť M je neprázdná podmnožina A.
Řekneme, že prvek $m \in A$ je **nejmenší prvek** množiny M, jestliže $m \in M$ a pro všechna $x \in M$ platí $m \preceq x$.
Řekneme, že prvek $m \in A$ je **největší prvek** množiny M, jestliže $m \in M$ a pro všechna $x \in M$ platí $x \preceq m$.
Řekneme, že prvek $m \in A$ je **minimální prvek** množiny M, jestliže $m \in M$ a neexistuje $x \in M$: $x \prec m$.
Značíme to $m = \min(M)$.
Řekneme, že prvek $m \in A$ je **maximální prvek** množiny M, jestliže $m \in M$ a neexistuje $x \in M$: $m \prec x$.
Značíme to $m = \max(M)$.

Věta.
Nechť je $(A, \preceq)$ částečně uspořádaná množina, uvažujme neprázdnou podmnožinu $M \subseteq A$. Pak platí následující:
(i) Jestliže existuje nejmenší prvek M, pak je jediný.
Jestliže existuje největší prvek M, pak je jediný.
(ii) Jestliže je m nejmenší prvek M, pak $m = \min(M)$ a jiné minimum už není.
Jestliže je m největší prvek M, pak $m = \max(M)$ a jiné maximum už není.

Věta.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Jestliže je M konečná neprázdná podmnožina A, pak existuje $\min(M)$ a $\max(M)$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $a, b \in A$ jsou **porovnatelné**, jestliže $a \preceq b$ nebo $b \preceq a$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $\preceq$ je **lineární uspořádání**, jestliže jsou každé dva prvky z A porovnatelné.

Věta.
Nechť $(A, \preceq)$ je lineárně uspořádaná množina. Jestliže je M její neprázdná konečná podmnožina, pak má nejmenší a největší prvek.

Věta.
Nechť $(A, \preceq)$ je konečná částečně uspořádaná množina. Je to lineární uspořádání právě tehdy, jestliže lze prvky A napsat jako $A = \{a_1, \ldots, a_n\}$ tak, aby $a_1 \prec a_2 \prec \cdots \prec a_n$.

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Relace $\preceq_L$ na A se nazývá **lineární rozšíření** relace $\preceq$, jestliže je $(A, \preceq_L)$ lineárně uspořádaná množina a $\preceq \subseteq \preceq_L$, tedy pro všechna $a, b \in A$ splňující $a \preceq b$ platí i $a \preceq_L b$.

Věta.
Pro každou konečnou částečně uspořádanou množinu $(A, \preceq)$ existuje lineární rozšíření $\preceq_L$ na A.

```
procedure topological sort((A, ⪯))
k := 0;
while A ≠ ∅ do
    k := k + 1
    a_k := min(A)
    A := A − {a_k};
output: (a_1 ≺_L a_2 ≺_L ··· ≺_L a_k);
```

Definice.
Nechť $(A, \preceq)$ je částečně uspořádaná množina. Řekneme, že $(A, \preceq)$ je **dobře uspořádaná množina**, jestliže každá neprázdná podmnožina množiny A má nejmenší prvek.

Fakt.
Každé dobré uspořádání je také lineární.

Axiom (princip dobrého uspořádání)
$(\mathbb{N}, \leq)$ je dobře uspořádaná množina.

Definice.
Uvažujme částečně uspořádané množiny $(A_1, \preceq_1), \dots, (A_n, \preceq_n)$. Definujeme **lexikografické uspořádání** na $A = A_1 \times \dots \times A_n$ následovně: Pro $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in A$ platí $a \preceq_L b$ právě tehdy, jestliže $a_i = b_i$ pro všechna $i = 1, \dots, n$ (tedy $a = b$), nebo existuje index k takový, že $a_i = b_i$ pro všechna i splňující $1 \leq i < k$ a $a_k \prec_k b_k$.

Věta.
Uvažujme dobře uspořádané množiny $(A_1, \preceq_1), \dots, (A_n, \preceq_n)$. Pak je $A = A_1 \times \dots \times A_n$ spolu s lexikografickým uspořádáním $\preceq_L$ dobře uspořádaná množina.

Definice.
Relace na množině se nazývá **ekvivalence**, jestliže je reflexivní, symetrická a tranzitivní.

Definice.
Nechť R je relace ekvivalence na nějaké množině A. Pro $a \in A$ definujeme **třídu ekvivalence** prvku a vzhledem k R jako

$$[a]_R = \{b \in A : aRb\}.$$

Věta.
Nechť R je relace ekvivalence na nějaké množině A, nechť $a \in A$.
(i) Pro každé $b, c \in [a]_R$ platí bRc.
(ii) Pro každé $b \in [a]_R$ a $c \in A$ platí, že jestliže bRc, pak $c \in [a]_R$.
(iii) Pro každé $b \in [a]_R$: $[a]_R = [b]_R$.
(iv) Pro každé $a, b \in A$ platí: aRb právě tehdy, když $[a]_R = [b]_R$.
(v) Pro všechna $a, b \in A$ platí, že buď $[a]_R = [b]_R$, nebo $[a]_R \cap [b]_R = \emptyset$.

Definice.
Uvažujme množinu A. Jejím **rozkladem** rozumíme libovolný soubor $\{A_i\}_{i \in I}$ neprázdných podmnožin A takových, že $A = \bigcup\limits_{i \in I} A_i$ a pro všechna $i \neq j \in I$ jsou A_i, A_j disjunktní.

Věta.
Nechť A je množina.
(i) Jestliže je R ekvivalence na A, pak $\{[a]_R\}_{a \in A}$ je rozklad množiny A.
(ii) Jestliže je $\{A_i\}_{i \in I}$ nějaký rozklad množiny A, pak existuje relace ekvivalence R na A taková, že $\{A_i\}_{i \in I}$ jsou přesně třídy ekvivalence R.

Věta.
Pro každé $n \in \mathbb{N}$ je relace „být kongruentní modulo n“ ekvivalence na $\mathbb{Z}$.

Definice.
Prostor $\mathbb{Z}_n$ definujeme jako množinu všech tříd ekvivalence v $\mathbb{Z}$ vzhledem k relaci být kongruentní modulo n, tedy $\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}$.
Pro $[a]_n, [b]_n \in \mathbb{Z}_n$ definujeme

$$[a]_n \oplus [b]_n = [a+b]_n,$$
$$[a]_n \odot [b]_n = [a \cdot b]_n.$$

Věta.
Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $[a]_n = [u]_n$ a $[b]_n = [v]_n$. Pak $[a+b]_n = [u+v]_n$ a $[a \cdot b]_n = [u \cdot v]_n$.

Věta.
Nechť $n \in \mathbb{N}$, uvažujme $[a]_n \in \mathbb{Z}_n$.
(i) Vždy existuje prvek opačný $-[a]_n = [n-a]_n$.
(ii) $[a]_n$ je invertibilní vůči $\odot$ právě tehdy, když jsou a a n nesoudělné.

DMA Přednáška – Zobrazení

Definice.
Nechť A,B jsou množiny. Definujeme **zobrazení** z A do B jako libovolnou podmnožinu $A\times B$ splňující

$$\forall a\in A\ \exists! b\in B\colon\ (a,b)\in T.$$

Množina A je **definiční obor** T, značeno $D(T)$, množina B je cílová množina T. Definujeme také **obor hodnot** T jako

$$R(T)=\{b\in B : \exists a\in A\colon\ T(a)=b\}=\{T(a) : a\in A\}.$$

Definice.
Nechť $T\colon\ A\mapsto B$ a $S\colon\ C\mapsto D$ jsou zobrazení. Řekneme, že jsou si rovna, značeno $T=S$, jestliže $A=C$, $B=D$ a

$$\forall a\in A\colon\ T(a)=S(a).$$

Definice.
Nechť $T\colon\ A\mapsto B$ a $S\colon\ B\mapsto C$ jsou zobrazení. Definujeme jejich **složené zobrazení** či **kompozici** $S\circ T\colon\ A\mapsto C$ předpisem

$$(S\circ T)(a)=S(T(a)) \text{ pro } \ a\in A.$$

Značíme také $S\circ T=S(T)$.

Věta.
Nechť $T\colon\ A\mapsto B$, $S\colon\ B\mapsto C$ a $R\colon\ C\mapsto D$ jsou zobrazení. Pak platí $(R\circ S)\circ T=R\circ(S\circ T)$.

Definice.
Nechť $T\colon\ A\mapsto B$ je zobrazení. Řekneme, že zobrazení $S\colon\ B\mapsto A$ je **inverzní** k T, jestliže platí
- $(S\circ T)(a)=a$ pro všechna $a\in A$
- $(T\circ S)(b)=b$ pro všechna $b\in B$.

Pokud takové zobrazení existuje, tak řekneme, že T je **invertibilní**, a inverzní zobrazení značíme T^{-1}.

Fakt.
Nechť $T\colon A \mapsto B$ je invertibilní zobrazení. Pak $T^{-1}(b) = a$ právě tehdy, když $T(a) = b$.

Důsledek.
Nechť $T\colon A \mapsto B$ je zobrazení. Jestliže je invertibilní, tak je jeho inverzní zobrazení T^{-1} dáno jednoznačně.

Věta.
Nechť $T\colon A \mapsto B$ a $S\colon B \mapsto C$ jsou zobrazení. Jestliže jsou invertibilní, tak je i $S \circ T$ invertibilní a navíc platí $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$.

Definice.
Nechť $T\colon A \mapsto B$ je zobrazení.
Řekneme, že T je **prosté** či **injektivní**, jestliže

$$\forall x, y \in A\colon T(x) = T(y) \implies x = y.$$

Řekneme, že T je **na** či **surjektivní**, jestliže $R(T) = B$.
Řekneme, že T je **vzájemně jednoznačné** či **bijekce**, jestliže je prosté a na.

Věta.
Nechť $T\colon A \mapsto B$ je zobrazení. Je invertibilní právě tehdy, když je to bijekce.

Fakt.
Nechť T: $A \mapsto B$ a S: $B \mapsto C$ jsou zobrazení. Pak platí:
(i) Jestliže jsou T a S prosté, tak je $S \circ T$ prosté.
(ii) Jestliže jsou T a S na, tak je $S \circ T$ na.
(iii) Jestliže jsou T a S bijekce, tak je $S \circ T$ bijekce.

Fakt.
Nechť $T\colon A \mapsto B$ je zobrazení a A, B mají konečně mnoho prvků.
(i) Jestliže má B více prvků než A, pak T nemůže být na.
(ii) Jestliže má A více prvků než B, pak T nemůže být prosté.
(iii) Jestliže A a B nemají stejně prvků, pak T nemůže být bijekce.

Definice.
Řekneme, že množiny A, B mají stejnou **mohutnost**, značeno $|A| = |B|$, jestliže existuje bijekce z A na B.
Řekneme, že množina A má mohutnost stejnou nebo menší než B, značeno $|A| \leq |B|$, jestliže existuje prosté zobrazení z A do B.

Fakt.
Nechť A, B jsou množiny.
(i) $|A| = |B|$ právě tehdy, když $|B| = |A|$.
(ii) Jestliže $|A| = |B|$, pak $|A| \leq |B|$ a $|B| \leq |A|$.

Věta. (Cantor-Bernstein-Schroeder)
Nechť A, B jsou množiny. Jestliže $|A| \leq |B|$ a $|B| \leq |A|$, pak $|A| = |B|$.

Fakt.
Jestliže $A \subseteq B$, pak $|A| \leq |B|$.

Definice.
Množina A se nazve **konečná**, jestliže $A = \emptyset$ (pak píšeme $|A| = 0$) nebo existuje takové $m \in \mathbb{N}$, aby $|A| = |\{1, 2, \dots, m\}|$, pak píšeme $|A| = m$.
Jinak se množina nazve **nekonečná**.
Množina A se nazve **spočetná**, jestliže má stejnou mohutnost jako množina $\mathbb{N}$.
Množina A se nazve **nespočetná**, jestliže je nekonečná, ale není spočetná.

Věta.
(i) Jestliže je A konečná množina, pak je i každá její podmnožina B konečná a platí $|B| \leq |A|$.
Je-li navíc B podmnožina vlastní, pak $|B| < |A|$.
(ii) Nechť A, B jsou konečné množiny. Pak je i $A \cup B$ konečná a platí $|A \cup B| \leq |A| + |B|$.
Jsou-li navíc A, B disjunktní, pak $|A \cup B| = |A| + |B|$.
(iii) Nechť A, B jsou konečné množiny. Pak je $A \times B$ konečná a platí $|A \times B| = |A| \cdot |B|$.

Věta.
(i) Jsou-li A_i pro $i = 1, 2, \dots, n$ konečné množiny, pak je i $\bigcup\limits_{i=1}^{n} A_i$ konečná a $\Bigl|\bigcup\limits_{i=1}^{n} A_i\Bigr| \leq \sum\limits_{i=1}^{n} |A_i|$.
Jsou-li navíc po dvou disjunktní, tak $\Bigl|\bigcup\limits_{i=1}^{n} A_i\Bigr| = \sum\limits_{i=1}^{n} |A_i|$.
(ii) Jsou-li A_i pro $i = 1, 2, \dots, n$ konečné množiny, pak je i $A_1 \times \dots \times A_n$ konečná a

$$|A_1 \times \dots \times A_n| = |A_1| \cdots |A_n| = \prod_{i=1}^{n} |A_i|.$$

Věta.
(i) Jestliže je A nekonečná množina, pak je i každá její nadmnožina B nekonečná.
(ii) Nechť A, B jsou množiny. Jestliže je A nekonečná, pak je i $A \cup B$ nekonečná.
(iii) Nechť A, B jsou množiny. Jestliže je A nekonečná a $B \neq \emptyset$, pak je $A \times B$ nekonečná.

Fakt.
Nechť A je množina. Jestliže je nekonečná, pak $|\mathbb{N}| \leq |A|$.

Věta.
(i) Množina $\mathbb{N}_0$ je spočetná.
(ii) Množina $\mathbb{Z}$ je spočetná.
(iii) Množina $\mathbb{N} \times \mathbb{N}$ je spočetná.
(iv) Množina $\mathbb{Z} \times \mathbb{Z}$ je spočetná.

Věta.
Množina racionálních čísel $\mathbb{Q}$ je spočetná.

Věta.
(i) Jestliže je množina nekonečná, tak má vlastní podmnožinu, která má stejnou mohutnost.
(ii) Nechť A, B jsou množiny, A je nekonečná a $|B| \leq |A|$. Pak $|A \cup B| = |A|$.
(iii) Nechť A, B jsou množiny, A je nekonečná a $|B| \leq |A|$. Pak $|A \times B| = |A|$.

Fakt.
(i) Jestliže jsou A_n pro $n \in \mathbb{N}$ nejvýše spočetné množiny, pak je $\bigcup\limits_{n=1}^{\infty} A_n$ nejvýše spočetná.
(ii) Jestliže jsou navíc A_n neprázdné a po dvou disjunktní, pak je $\bigcup\limits_{n=1}^{\infty} A_n$ spočetná.

Věta.
Interval reálných čísel $\langle 0, 1)$ je nespočetný.

Důsledek.
Množina reálných čísel $\mathbb{R}$ je nespočetná.

Definice.
Nechť A je množina. Definujeme **potenční množinu** A, značeno $P(A)$, jako množinu všech podmnožin A.

Fakt.
Jestliže je A konečná množina, pak $|P(A)| = 2^{|A|}$.

Věta. (Cantorova)
Pro každou množinu A platí $|A| < |P(A)|$.

DMA Přednáška – Indukce

Kroky při důkazu indukcí:
1. Zformulujeme přesně tvrzení a oznámíme, jak jej dokážeme.
2. Dokážeme základní krok.
3. Dokážeme indukční krok. Pro jisté (libovolné) $n \geq n_0$ předpokládáme, že platí „indukční předpoklad“ $V(n)$, pomocí něj pak dokážeme platnost $V(n+1)$.
4. Uděláme závěr.

Slabý princip matematické indukce.
Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$.
Předpokládejme, že následující předpoklady jsou splněny:
(0) $V(n_0)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace: Jestliže platí $V(n)$, pak platí i $V(n+1)$.
Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Věta.
Princip indukce je ekvivalentní s principem dobrého uspořádání.

Silný princip matematické indukce.
Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$.
Předpokládejme, že následující předpoklady jsou splněny:
(0) $V(n_0)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0$ je pravdivá následující implikace: Jestliže platí $V(k)$ pro všechna $k = n_0, n_0+1, \dots, n$, pak platí i $V(n+1)$.
Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Věta.
Slabý a silný princip matematické indukce jsou ekvivalentní.

Modifikovaný silný princip matematické indukce.
Nechť $n_0 \in \mathbb{Z}$, nechť $V(n)$ je vlastnost celých čísel, která má smysl pro $n \geq n_0$. Nechť $m \in \mathbb{N}$.
Předpokládejme, že následující předpoklady jsou splněny:
(0) $V(n_0)$, $V(n_0+1)$, $V(n_0+2)$, ... ,$V(n_0+m-1)$ platí.
(1) Pro každé $n \in \mathbb{Z}$, $n \geq n_0+m-1$ je pravdivá následující implikace: Jestliže platí $V(k)$ pro všechna $k = n-m+1, n-m+2, \dots, n$, pak platí i $V(n+1)$.
Potom $V(n)$ platí pro všechna $n \in \mathbb{Z}$, $n \geq n_0$.

Induktivní definice množin.
Při definici konkrétní množiny M uvažujme následující dva druhy specifikací:
(0) **Základní pravidla** definují přímo, které prvky jsou v množině M.
(1) **Induktivní pravidla** určují, jak lze pomocí prvků, které již v množině jsou (tzv. **předpoklady** pravidla), vytvářet další prvky z M (tzv. **závěr** pravidla).
Množina M se pak skládá ze všech prvků, které lze obdržet konečným počtem použití pravidel (0) a (1) (tedy prvky, které lze takto získat, leží v M, a ty, které takto získat nelze, pak v M neleží).

Princip strukturální indukce.
Uvažujme množinu M definovanou induktivně pomocí nějakých základních pravidel (0) a induktivních pravidel (1). Uvažujme vlastnost $V(m)$, která má smysl pro všechny $m \in M$.
Předpokládejme, že jsou splněny následující podmínky:
(0) V je splněna pro všechny prvky, které jsou do M dodány základními pravidly.
(1) Pro každé induktivní pravidlo platí: Jestliže je V splněna pro prvky z jeho předpokladů, pak je splněna i pro prvek z jeho závěru.
Pak je vlastnost V splněna pro všechny prvky $m \in M$.

Věta.
Platnost principu strukturální indukce je ekvivalentní platnosti principu matematické indukce.

DMA Přednáška – Posloupnosti

Definice.
Posloupnost je libovolné zobrazení z nějaké množiny $\{n_0, n_0+1, n_0+2, \dots\}$ do $\mathbb{R}$, kde pro $n_0 \in \mathbb{Z}$.

Definice.
Nechť $\{a_k\}$ je posloupnost.
Řekneme, že tato posloupnost jde do nekonečna, popřípadě že má limitu nekonečno, značeno $\lim(a_k) = \infty$ popřípadě $a_k \to \infty$, jestliže

pro každé $K > 0$ existuje k_0 tak, aby $a_k > K$ pro všechna $k \geq k_0$.

Řekneme, že tato posloupnost jde k nule, popřípadě že konverguje k nule, popřípadě že má limitu rovnou nule, značeno $\lim(a_k) = 0$ popřípadě $a_k \to 0$, jestliže

pro každé $K > 0$ existuje k_0 tak, aby $|a_k| < K$ pro všechna $k \geq k_0$.

Fakt.
(i) Nechť $a > 0$. Pak $k^a \to \infty$ a $\frac{1}{k^a} \to 0$.
(ii) Jestliže $q > 1$, pak $q^k \to \infty$.
Jestliže $|q| < 1$, pak $q^k \to 0$.
(iii) $k! \to \infty$.
(iv) $k^k \to \infty$.
(v) Nechť $b > 0$. Pak $[\ln(k)]^b \to \infty$.

10^6 operací za 1 sec. čas in ms. s=sec m=min d=den r=rok

$k =$	5	10	20	50	100	1000	10^5	10^8
$\ln(k)$:	0.0016	0.0023	0.003	0.004	0.0046	0.007	0.01	0.018
• k:	0.005	0.01	0.02	0.05	0.1	1	0.1s	1.7m
• k^2:	0.025	0.1	0.4	2.5	10	1s	28m	317r
$\frac{1}{100}k^2$:	0.0002	0.001	0.004	0.025	0.01	10	1.7m	3.2r
$k^{1.585}$:	0.013	0.038	0.12	0.49	1.5	57	1.4m	55d
2^k:	0.03	1	1s	35.7r	4×10^{16}r	3×10^{287}r		

Hardware setup: $k = 10 \implies$ 1sec. čas in s. m=min d=den r=rok

$k =$	10	20	30	40	50	100
$\ln(k)$:	1	1.3	1.5	1.6	1.7	2
• k:	1	2	3	4	5	10
$20k$:	1	2	3	4	5	10
$20k + 5$:	1	2	3	3.9	4.9	9.8
k^2:	1	4	9	16	25	1m40s
k^3:	1	8	27	1m	2m	17m
2^k:	1	17m	12d	34r	35×10^3r	4×10^{19}r
$k!$:	1	21×10^3r	2×10^{18}r	7×10^{33}r	3×10^{50}r	

Definice.
Nechť $\{a_k\}$, $\{b_k\}$ jsou posloupnosti splňující $a_k \to \infty$, $b_k \to \infty$.
Řekneme, že a_k je $o(b_k)$, jestliže $\frac{a_k}{b_k} \to 0$ neboli $\frac{b_k}{a_k} \to \infty$.
Řekneme, že a_k je $\omega(b_k)$, jestliže $\frac{a_k}{b_k} \to \infty$ neboli $\frac{b_k}{a_k} \to 0$.
Řekneme, že a_k je $O(b_k)$, jestliže $\exists N \in \mathbb{N}\ \exists K > 0$ aby $\forall k \geq N$: $a_k \leq K b_k$.
Řekneme, že a_k je $\Omega(b_k)$, jestliže $\exists N \in \mathbb{N}\ \exists L > 0$ aby $\forall k \geq N$: $a_k \geq L b_k$.
Řekneme, že a_k je $\Theta(b_k)$ nebo že $a_k \asymp b_k$, jestliže $\exists N \in \mathbb{N}\ \exists K, L > 0$ aby $\forall k \geq N$: $L b_k \leq a_k \leq K b_k$.

Fakt.
Nechť $\{a_k\}$, $\{b_k\}$ jsou posloupnosti splňující $a_k \to \infty$, $b_k \to \infty$.
Jestliže $\frac{a_k}{b_k} \to A > 0$, pak a_k je $\Theta(b_k)$.

Věta. (škála mocnin)
(i) Nechť $a, b > 0$ a $q > 1$. Pak platí
$$[\ln(k)]^a \text{ je } o(k^b),\ \ k^b \text{ je } o(q^k),\ \ q^k \text{ je } o(k!) \text{ a } k! \text{ je } o(k^k).$$
(ii) Jestliže $0 < a < b$, pak $[\ln(k)]^a$ je $o([\ln(k)]^b)$ a k^a je $o(k^b)$.
(iii) Jestliže $1 < q < r$, pak q^k je $o(r^k)$.

Fakt.
Jestliže $b_k = o(a_k)$, pak $a_k + b_k = \Theta(a_k)$.

DMA Přednáška – Rekurentní rovnice

Definice.
Rekurentní rovnice či **rekurzivní rovnice** pro posloupnost $\{a_n\}$ je vztah

$$a_{n+1} = G(a_n, a_{n-1}, \dots, a_{n-m}),\ n \geq n_0 + m,$$

kde G je nějaká funkce $m+1$ proměnných.
Jejím **řešením** nazveme libovolnou posloupnost $\{a_n\}_{n=n_0}^{\infty}$ takovou, že po dosazení odpovídajících členů do dané rovnice dostáváme pro všechna $n \geq n_0 + m$ pravdivý výrok.

Definice.
Lineární rekurentní rovnice, popřípadě **lineární rekursivní rovnice řádu** $k \in \mathbb{N}_0$ je libovolná rovnice ve tvaru

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \dots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = b_n, \quad n \geq n_0,$$

kde $n_0 \in \mathbb{Z}$, $c_i(n)$ pro $i = \{0, \dots, k-1\}$ (tzv. **koeficienty** rovnice) jsou nějaké funkce $\mathbb{Z} \mapsto \mathbb{R}$, přičemž $c_0(n)$ není identicky nulová funkce, a $\{b_n\}_{n=n_0}^{\infty}$ (tzv. **pravá strana rovnice**) je pevně zvolená posloupnost reálných čísel.

Jestliže $b_n = 0$ pro všechna $n \geq n_0$, pak se příslušná rovnice nazývá **homogenní**.

Zápis rovnice pomocí sumačního znaménka:

$$a_{n+k} + \sum_{i=0}^{k-1} c_i(n)a_{n+i} = b_n.$$

Definice.
Nechť je dána lineární rekurentní rovnice řádu k

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \ldots + c_1(n)a_{n+1} + c_0(n)a_n = b_n, \quad n \geq n_0.$$

Za **počáteční podmínky** (**initial conditions**) pro tuto rovnici považujeme libovolnou soustavu rovnic $a_{n_0} = A_0$, $a_{n_0+1} = A_1, \ldots, a_{n_0+k-1} = A_{k-1}$, kde $A_i \in \mathbb{R}$ jsou pevně zvolená čísla.

Definice.
Uvažujme lineární rekurentní rovnici

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \ldots + c_1(n)a_{n+1} + c_0(n)a_n = b_n, \quad n \geq n_0.$$

Pak se lineární rekurentní rovnice

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \ldots + c_1(n)a_{n+1} + c_0(n)a_n = 0, \quad n \geq n_0$$

nazývá k ní **přidružená homogenní rovnice**.

Věta. (o struktuře řešení lineární rekurentní rovnice)
Nechť je dána lineární rekurentní rovnice

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \ldots + c_1(n)a_{n+1} + c_0(n)a_n = b_n, \quad n \geq n_0$$

a nějaké její řešení $\{a_{p,n}\}_{n=n_0}^{\infty}$.
Posloupnost $\{a_n\}_{n=n_0}^{\infty}$ je řešením této rovnice právě tehdy, pokud se dá napsat jako $\{a_n\} = \{a_{p,n}\} + \{a_{h,n}\}$, kde $\{a_{h,n}\}_{n=n_0}^{\infty}$ je nějaké řešení přidružené homogenní rovnice.

Množina všech řešení dané lineární rekurentní rovnice je tedy

$$\big\{\{a_{p,n}\} + \{a_{h,n}\};\ \{a_{h,n}\} \text{ řeší přidruženou homogenní rovnici}\big\}.$$

Věta. (o prostoru řešení homogenní lineární rekurentní rovnice)
Množina všech řešení dané homogenní lineární rekurentní rovnice řádu k je vektorový prostor dimenze k.

Definice.
Lineární rekurentní rovnice s konstantními koeficienty je libovolná rovnice ve tvaru

$$a_{n+k} + c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n = b_n, \quad n \geq n_0,$$

kde $n_0 \in \mathbb{Z}$, $c_i \in \mathbb{R}$ pro $i = 0, \ldots, k-1$ jsou pevně zvolená čísla a $\{b_n\}_{n=n_0}^{\infty}$ je pevně zvolená posloupnost reálných čísel.

Definice.
Nechť je dána lineární rekurentní rovnice s konstantními koeficienty

$$a_{n+k} + c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n = b_n, \quad n \geq n_0.$$

Její **charakteristický polynom** je definován jako polynom

$$p(\lambda) = \lambda^k + c_{k-1}\lambda^{k-1} + \ldots + c_1\lambda + c_0.$$

Kořeny charakteristického polynomu se nazývají **charakteristická čísla**, popřípadě **vlastní čísla** dané rovnice. Řešené rovnici

$$\lambda^k + c_{k-1}\lambda^{k-1} + \ldots + c_1\lambda + c_0 = 0$$

se také říká **charakteristická rovnice**.

Fakt.
Jestliže je λ_0 charakteristickým číslem dané homogenní lineární rekurentní rovnice s konstantními koeficienty, pak je posloupnost $\{\lambda_0^n\}_{n=n_0}^{\infty}$ jejím řešením.

Věta.
Uvažujme homogenní lineární rekurentní rovnici s konstantními koeficienty. Jestliže jsou λ_i různá její charakteristická čísla, pak $\{\lambda_i^n\}_{n=n_0}^{\infty}$ tvoří lineárně nezávislou množinu řešení této rovnice.

Fakt.
Nechť je dána homogenní lineární rekurentní rovnice s konstantními koeficienty. Jestliže je λ_0 její charakteristické číslo a má násobnost m jako kořen charakteristického polynomu, pak posloupnosti $\{\lambda_0^n\}, \{n\lambda_0^n\}, \dots, \{n^{m-1}\lambda_0^n\}$ jsou řešení dané rovnice a tvoří lineárně nezávislou množinu.

Věta.
Nechť je dána homogenní lineární rekurentní rovnice s konstantními koeficienty řádu k. Nechť jsou $\lambda_1, \dots, \lambda_M$ její různá charakteristická čísla, přičemž každé λ_i má násobnost $m_i \in \mathbb{N}$. Pak je množina

$$\big\{\{\lambda_1^n\}, \{n\lambda_1^n\}, \dots, \{n^{m_1-1}\lambda_1^n\}, \{\lambda_2^n\}, \{n\lambda_2^n\}, \dots, \{n^{m_2-1}\lambda_2^n\}, \dots, \{\lambda_M^n\}, \{n\lambda_M^n\}, \dots, \{n^{m_M-1}\lambda_M^n\}\big\}$$

bází prostoru řešení dané rovnice.

Algoritmus pro řešení homogenní lineární rekurentní rovnice $a_{n+k} + \sum\limits_{i=0}^{k-1} c_i a_{n+i} = 0,\ \ n \geq n_0$, řádu k.

1. Sestavte charakteristický polynom $p(\lambda) = \lambda^k + \sum\limits_{i=0}^{k-1} c_i \lambda^i$.

Řešením rovnice $p(\lambda) = 0$ najděte všechna charakteristická čísla dané rovnice.
2. Sestavte množinu posloupností B takto:
• pro každé reálné charakteristické číslo λ přidejte do B posloupnost $\{\lambda^n\}_{n=n_0}^{\infty}$;
• pro každé reálné charakteristické číslo λ, jehož násobnost je $m > 1$, přidejte do B rovněž posloupnosti $\{n\lambda^n\}_{n=n_0}^{\infty}, \dots, \{n^{m-1}\lambda^n\}_{n=n_0}^{\infty}$;
• pro každé komplexní charakteristické číslo $\lambda = r[\cos(\varphi) + i\sin(\varphi)]$, které není reálné, přidejte do B posloupnosti $\{r^n\cos(n\varphi)\}_{n=n_0}^{\infty}$ a $\{r^n\sin(n\varphi)\}_{n=n_0}^{\infty}$; pro jeho komplexně sdružené číslo λ^* již do B nic nepřidáváme;
• pro každé komplexní charakteristické číslo $\lambda = r[\cos(\varphi) + i\sin(\varphi)]$, které není reálné a jehož násobnost je $m > 1$, přidejte do B posloupnosti $\{nr^n\cos(n\varphi)\}_{n=n_0}^{\infty}, \dots, \{n^{m-1}r^n\cos(n\varphi)\}_{n=n_0}^{\infty}$
a $\{nr^n\sin(n\varphi)\}_{n=n_0}^{\infty}, \dots, \{n^{m-1}r^n\sin(n\varphi)\}_{n=n_0}^{\infty}$; pro jeho komplexně sdružené číslo λ^* již do B nic nepřidáváme.
Množina B je bází prostoru řešení.

3. Označíme-li $B = \big\{\{a_{1,n}\}, \dots, \{a_{k,n}\}\big\}$, pak je obecné řešení dané rovnice určeno vzorcem $\Big\{\sum\limits_{i=1}^{k} u_i a_{i,n}\Big\}_{n=n_0}^{\infty}$ pro $u_1, \dots, u_k \in \mathbb{R}$.
4. Jsou-li dány počáteční podmínky, pak do nich za příslušná a_j pro $j = n_0, \dots, n_0 + k - 1$ dosadíme vzorce $a_j = \sum\limits_{i=1}^{k} u_i a_{i,j}$ a vyřešíme vzniklých k rovnic pro k neznámých u_i. Ty po dosazení do obecného řešení určí příslušné partikulární řešení.

Definice.
Řekneme, že posloupnost $\{b_n\}_{n=n_0}^{\infty}$ je **kvazipolynom**, jestliže existuje $\lambda \in \mathbb{R}$ a polynom $P(n)$ takový, že $b_n = P(n)\lambda^n$ pro všechna $n \geq n_0$.

Věta.
Uvažujme rovnici

$$a_{n+k} + c_{k-1}a_{n+k-1} + \cdots + c_1 a_{n+1} + c_0 a_n = b_n, \quad n \geq n_0.$$

Předpokládejme, že existují $\lambda \in \mathbb{R}$ a polynom P takový, že $b_n = P(n)\lambda^n$ pro všechna $n \geq n_0$. Nechť m je násobnost tohoto čísla λ jako charakteristického čísla přidružené homogenní rovnice, přičemž $m = 0$ v případě, že toto λ vůbec charakteristickým číslem není.
Pak existuje polynom $Q(n)$ stupně stejného jako P takový, že $\{n^m Q(n)\lambda^n\}$ je řešením dané rovnice.

$a_{n+2} - 9a_n =$ $[\lambda = -3, 3]$	$a_{n+2} - 3a_{n+1} + 2a_n =$ $[\lambda = 1, 2]$	$a_{n+2} - 4a_{n+1} + 4a_n =$ $[\lambda = 2\ (2\times)]$	$L =$ / $= b_n$
			$= n\,2^n$ $[\lambda = 2]$
			$= n^2(-1)^n$ $[\lambda = -1]$
			$= 2n - 5$ $[\lambda = 1]$
			$= (-3)^n$ $[\lambda = -3]$

Algoritmus pro nalezení řešení rovnice $a_{n+k} + c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n = b_n$, $n \geq n_0$, kde $b_n = P(n)\lambda^n$, $c_i \in \mathbb{R}$ a $c_0 \neq 0$ (tedy řád k).

1. Nejprve řešte přidruženou homogenní rovnici $a_{n+k} + c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n = 0$.
a) Najděte všechna charakteristická čísla λ_j s násobnostmi m_j řešením rovnice $\lambda_k + c_{k-1}\lambda^{k-1} + \cdots + c_1\lambda + c_0 = 0$.
b) Sestavte bázi prostoru řešení $B = \big\{\{a_{i,n}\}_{n=n_0}^{\infty};\ i = 1, \ldots, k\big\}$.
c) Obecné řešení přidružené homogenní rovnice je $\{a_{h,n}\} = \Big\{\sum\limits_{i=1}^{k} u_i a_{i,n}\Big\}$ pro $u_i \in \mathbb{R}$.
Pokud byla zadaná rovnice již homogenní, jděte na **3**.
2. Pokud nebyla zadaná rovnice homogenní, zkontrolujte, že je pravá strana kvazipolynom, tedy $b_n = P(n)\lambda^n$ pro nějaké $\lambda \in \mathbb{R}$ a polynom P.
a) Porovnejte λ s charakteristickými čísly λ_j z kroku **1**. Pokud se žádnému nerovná, položte $m = 0$. Pokud pro nějaké j platí $\lambda = \lambda_j$, položte $m = m_j$ (násobnost dotyčného charakteristického čísla).
b) Sestavte obecný polynom Q stupně stejného jako P, tradičně se používá $Q(n) = A + Bn + \cdots$.
c) Uhádněte řešení $a_n = n^m Q(n)\lambda^n$. Dosaďte jej do dané rovnice a po zkrácení λ zjednodušte levou stranu do tvaru polynomu. Porovnáním koeficientů polynomů na levé a pravé straně získáte tolik rovnic, kolik je neznámých koeficientů v Q.
d) Vyřešte tyto rovnice a obdržené konstanty dosaďte zpět do Q. Získáte jedno konkrétní řešení $a_{p,n}$.
e) Obecné řešení dané úlohy je $\Big\{a_{p,n} + \sum\limits_{i=1}^{k} u_i a_{i,n}\Big\}_{n=n_0}^{\infty}$ či $a_n = a_{p,n} + \sum\limits_{i=1}^{k} u_i a_{i,n}$ pro $n \geq n_0$.
3. Pokud byly s rovnicí zadány také počáteční podmínky, dosaďte za a_j v těchto podmínkách vzorce pro a_j z obecného řešení, které jste našli. Získáte k rovnic pro k neznámých $u_1, \ldots, u_k$. Vyřešte tuto soustavu, získaná u_i dosaďte do vzorce pro obecné řešení a dostanete tak partikulární řešení pro zadanou úlohu.

Věta.
Nechť $k \in \mathbb{N}$, uvažujme funkce $c_0(n), c_1(n), \ldots, c_{k-1}(n)\colon \mathbb{Z} \mapsto \mathbb{R}$.

Jestliže posloupnost $\{a_n\}_{n=n_0}^{\infty}$ řeší rovnici $\quad a_{n+k} + \sum\limits_{i=0}^{k-1} c_i(n) a_{n+i} = b_n,\ \ n \geq n_0$

a posloupnost $\{\tilde{a}_n\}_{n=n_0}^{\infty}$ řeší rovnici $\quad a_{n+k} + \sum\limits_{i=0}^{k-1} c_i(n) a_{n+i} = \tilde{b}_n,\ \ n \geq n_0,$

pak posloupnost $\{a_n + \tilde{a}_n\}_{n=n_0}^{\infty}$ řeší rovnici $\quad a_{n+k} + \sum\limits_{i=0}^{k-1} c_i(n) a_{n+i} = b_n + \tilde{b}_n \quad$ pro všechna $n \geq n_0$.

Fakt.
Nechťje funkce f na $\mathbb{N}$ dána vzorcem $f(n) = a \cdot f\left(\frac{n}{b}\right)$ pro $a > 0$ a $b \in \mathbb{N}$, $b \geq 2$.
Pak pro $n \in \{b^k;\ k \in \mathbb{N}\}$ platí $f(n) = n^{\log_b(a)} f(1)$.

Věta. (The Master theorem)
Uvažujme neklesající nezápornou funkci f na $\mathbb{N}$. Pro nějaké $b \in \mathbb{N}$, $b \geq 2$ označme $M = \{b^k;\ k \in \mathbb{N}\}$ a předpokládejme, že f splňuje na M rovnici $f(n) = a \cdot f\left(\frac{n}{b}\right) + cn^d$ pro konstanty $a, c \in \mathbb{R}$, $d \in \mathbb{N}_0$ splňující $a \geq 1$ a $c > 0$. Pak platí následující:
(i) Jestliže $a > b^d$, tak $f(n) = \Theta(n^{\log_b(a)})$.
(ii) Jestliže $a = b^d$, tak $f(n) = \Theta(n^d \log_2(n))$.
(iii) Jestliže $a < b^d$, tak $f(n) = \Theta(n^d)$.

Důsledek.
Uvažujme neklesající nezápornou funkci f na $\mathbb{N}$. Pro nějaké $b \in \mathbb{N}$, $b \geq 2$ označme $M = \{b^k;\ k \in \mathbb{N}\}$ a předpokládejme, že f splňuje na M rovnici $f(n) = a \cdot f\left(\frac{n}{b}\right) + cn^d$ pro konstanty $a, c \in \mathbb{R}$, $d \in \mathbb{N}_0$ splňující $a \geq 1$ a $c \geq 0$. Pak platí následující:
(i) Jestliže $d < \log_b(a)$ nebo $c = 0$, tak $f(n)$ je $\Theta(n^{\log_b(a)})$.
(ii) Jestliže $d = \log_b(a)$, tak $f(n)$ je $\Theta(n^{\log_b(a)} \log_2(n)) = \Theta(n^d \log_2(n))$.
(iii) Jestliže $d > \log_b(a)$, tak $f(n)$ je $\Theta(n^d)$.

DMA Přednáška – Kombinatorika

	bez opakování	s opakováním
s pořadím (variace)	$\frac{n!}{(n-k)!}$	n^k
bez pořadí (kombinace)	$\binom{n}{k}$	$\binom{n+k-1}{k}$

Věta. (Princip inkluze a exkluze)
Jsou-li A_i pro $i = 1, 2, \ldots, n$ konečné množiny, pak

$$\Big|\bigcup_{i=1}^{n} A_i\Big| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1}\Big|\bigcap_{i=1}^{n} A_i\Big|$$
$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|.$$

Dirichletův šuplíkový princip

• Jestliže je alespoň $k+1$ objektů rozděleno do k krabiček, tak musí být krabička obsahující alespoň dva objekty.

• Nechť A, B jsou konečné množiny. Jestliže $|A| > |B|$, pak pro každé zobrazení $T\colon A \mapsto B$ existuje $b \in B$ takové, že $|T^{-1}[\{b\}]| > 1$.

• Nechť $c, k \in \mathbb{N}$. Je-li alespoň $ck+1$ objektů umístěno do k krabiček, pak existuje krabička, která má více než c objektů.

• Je-li N objektů umístěno do k krabiček, pak existuje krabička, která má alespoň $\lceil \frac{N}{k} \rceil$ objektů.