Organizační úvod

Přednášky budou nahrávány, referáty ne.

Kontaktovat přes e-mail slavikova@karlin.mff.cuni.cz

Teoretické příklady odevzdávat přes Moodle.

1 Prvočísla

Definice 1.1 (Dělitel)

Číslo $d \in \mathbb{Z}$ nazýváme dělitelem čísla $n \in \mathbb{Z}$, značeno $d \div n$, pokud existuje $k \in \mathbb{Z}$ splňující $n = kd$.

Definice 1.2 (Prvočíslo)

Řekněme, že $n \in \mathbb{N}$ je prvočíslo, pokud $n > 1$ a jeho jediní kladní dělitelné jsou $1 \geq n$.

Například (Několik prvních prvočísel)
2, 3, 5, 7, 11, 13, 17, …

Věta 1.1 (Základní věta aritmetiky)

Každé přirozené číslo $n \geq 2$ lze zapsat právě jedním způsobem jako součin prvočísel ve tvaru:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$k \in N, p_1 < p_2 < \cdots < p_k jsou\ prvočísla, \alpha_1, \ldots, \alpha_k \in \mathbb{N}$$

Například

$$2020 = 2^2 \cdot 5 \cdot 101 (k = 3, p_1 = 2, p_2 = 5, p_3 = 101, \alpha_1 = 2, \alpha_2 = 1, \alpha_3 = 1)$$

Důkaz
1. krok = existence rozkladu (indukcí):

Pro $n = 2$ zjevně platí $2 = 2^1$ $(k = 1, p_1 = 2, \alpha_1 = 1)$.

Předpokládejme, že tvrzení platí pro všechna $2 \leq x \leq n$. Pokud je $n + 1$ prvočíslo, pak $n + 1 = (n + 1)^1$ $(k = 1, p_1 = n + 1, \alpha_1 = 1)$. Pokud není, pak $n + 1 = a \cdot b$, kde $1 < a \leq b < n + 1$. Podle indukčního předpokladu lze a i b rozložit na prvočísla. Zápis rozkladu $n + 1$ pak bude sjednocením všech prvočísel a součtem příslušných α, pokud se prvočísla vyskytují v a i b. (V přednášce byl zaveden zápis bez mocnin, kde prvočísla nemusí být různá, a pak proveden součin.)

2. krok = jednoznačnost rozkladu:

Lemma 1.2 (Euklidovo lemma (bez důkazu))

Nechť $a, b \in \mathbb{Z}$ a nechť p je prvočíslo takové, že $p \mid ab$. Pak $p \mid a$ nebo $p \mid b$.

Použijeme důkaz sporem. Předpokládejme, že tvrzení neplatí. Vybereme nejmenší z přirozených čísel, pro které rozklad není jednoznačný. Označme ho n.

$$n = q_1 \cdots q_l = r_1 \cdot r_m \ (q_1, \ldots, q_l, r_1, \ldots, r_m \text{prvočísla})$$

A není pravda, že $(r_1, \ldots, r_m)$ je permutací $(q_1, \ldots, q_l)$.

Protože $q_1 \mid n$, pak $q_1 \mid r_1 \cdots r_m$ a podle Euklidova lemmatu q_1 dělí alespoň jedno z čísel $r_1, \ldots r_m$. BÚNO $q_1 | r_1$, tedy $q_1 = r_1$. Vydělením n číslem q_1 dostaneme menší přirozené číslo, které nemá jednoznačný rozklad. $(\frac{n}{q_1} = q_2 \cdots q_l = r_2 \cdots r_m)$. □

Věta 1.3

Prvočísel je nekonečně mnoho.

Důkaz
Důkaz sporem. Předpokládejme, že prvočísel je konečně mnoho, a označme p největší prvočíslo. Definujeme:

$$n_p = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p + 1$$

Pak $n_p > p$ a n_p dává zbytek 1 po dělení všemi prvočísly, tedy není ani jedním dělitelné. Tedy n_p nemá prvočíselný rozklad.   se základní větou aritmetiky. □

Poznámka
Důkaz nedává konstrukci vyššího prvočísla, pouze dokazuje jeho existenci.

Například
Mezi 1 a 100 je 25 prvočísel.

Mezi 10^7 a $10^7 + 100$ jsou pouze 2 prvočísla.

Označme $\Pi(N)$ *počet prvočísel* $\leq N$.

Existují konstanty $c_1, c_2 > 0$ *takové, že*

$$\frac{c_1}{\log N} \leq \frac{\Pi(N)}{N} \leq \frac{c_2}{\log N}$$

Poznámka
Prvočísel je nekonečně mnoho, ale „řídnou“. Musí tedy existovat dlouhé úseky bez prvočísel.

Například
Interval $[n! + 2, \dots, n! + n]$ neobsahuje žádné prvočíslo. (Jelikož k-té číslo je dělitelné $k + 1$.)

2 Čísla racionální a iracionální

Definice 2.1 (Racionální a iracionální číslo)

Číslo $x \in \mathbb{R}$ je racionální, pokud ho lze zapsat ve tvaru $x = \frac{p}{q},\ q \in \mathbb{N},\ p \in \mathbb{Z}$.

Číslo $y \in \mathbb{R}$ je iracionální, pokud není racionální.

Například (Z přednášky)
$\sqrt{2}$ je iracionální.

Věta 2.1

Nechť $n \in \mathbb{N}$ *je taková, že* $\sqrt{n} \notin \mathbb{N}$ *(tedy* n *není druhou mocninou přirozeného čísla). Pak* $\sqrt{n}$ *je iracionální.*

Lemma 2.2

Jsou-li p, q *nesoudělná, pak* $p^2,\ q^2$ *jsou také nesoudělná.*

Důkaz
Dle základní věty aritmetiky každé přirozené číslo lze rozložit na součin prvočísel. Rozložíme a dokážeme. $\square$

Důkaz (Sporem)
Předpokládejme, že $\sqrt{n}$ je racionální, ale není to celé číslo. Pak $\sqrt{n} = \frac{p}{q}$, kde p, q jsou nesoudělná přirozená čísla ($q \geq 2$). Umocníme: $n = \frac{p^2}{q^2}$. $q|p$ *lightning*. $\square$

Věta 2.3 (Referát 1)

Existují iracionální čísla a,b taková, že a^b je racionální. (Text: skripta z MA, str. 14--15.)

Důkaz
Buď $\sqrt{2}^{\sqrt{2}}$ nebo $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ $\square$

Příklad (Teoretický příklad 1)
Nechť $n \in \mathbb{N}$ a nechť $a_1, \ldots, a_n$ jsou kladná reálná čísla, taková, že $a_1 \cdot \cdots \cdot a_n = 1$.

Dokažte, že
$$(1 + a_1) \cdot \cdots \cdot (1 + a_n) \geq 2^n.$$

Příklad (Teoretický příklad 2)
Nalezněte supremum a infimum množiny
$$\left\{\sqrt{n} - \lfloor\sqrt{n}\rfloor : n \in \mathbb{N}\right\}$$

3 Mohutnost množin

Definice 3.1

Množiny $\mathbb{X}$, $\mathbb{Y}$ mají stejnou mohutnost, pokud existuje bijekce $\mathbb{X}$ na $\mathbb{Y}$. Značíme $\mathbb{X} \approx \mathbb{Y}$.

Množina $\mathbb{X}$ má mohutnost menši nebo rovnu mohutnosti $\mathbb{Y}$, pokud existuje prosté zobrazení $\mathbb{X}$ do $\mathbb{Y}$. Značíme $\mathbb{X} \preceq \mathbb{Y}$.

Množina $\mathbb{X}$ má menší mohutnost než $\mathbb{Y}$, pokud $\mathbb{X} \preceq \mathbb{Y}$, ale neplatí $\mathbb{Y} \preceq \mathbb{X}$. Značíme $\mathbb{X} \prec \mathbb{Y}$.

Věta 3.1

(Cantor-Bernstein) Nechť $\mathbb{X}$ a $\mathbb{Y}$ jsou množiny splňující $\mathbb{X} \preceq \mathbb{Y}$ a $\mathbb{Y} \preceq \mathbb{X}$, pak $\mathbb{X} \approx \mathbb{Y}$.

Lemma 3.2

Nechť $\mathbb{X}$ je množina a $H : \mathcal{P}(\mathbb{X}) \to \mathcal{P}(\mathbb{X})$ je zobrazení splňující podmínku $\forall \mathbb{A}, \mathbb{B} \in \mathcal{P}(\mathbb{X}) : \mathbb{A} \subset \mathbb{B} \implies H(\mathbb{A}) \subset H(\mathbb{B})$. Pak existuje $\mathbb{C} \subset \mathbb{X}$ takové, že $H(C) = C$.

Důkaz
Položme $\mathcal{C} = \{\mathbb{A} \in \mathcal{P}(\mathbb{X}) : \mathbb{A} \subset H(\mathbb{A})\}$. Ukážeme, že $\mathbb{C} = \bigcap \mathcal{C}$ je hledanou množinou. $C \subset \mathbb{X}$ je zřejmé, $C \subset H(C)$: Pokud $\mathbb{A} \in \mathcal{C}$, pak $\mathbb{A} \subset C$, pak z vlastnosti zobrazení plyne $H(\mathbb{A}) \subset H(\mathbb{C})$. Tedy $\mathbb{A} \subset H(\mathbb{A}) \subset H(\mathbb{C})$. Z definice $\mathbb{C}$ dostáváme $C \subset H(\mathbb{C})$. Nakonec musíme ještě dokázat $H(\mathbb{C}) \subset \mathbb{C}$. Z $\mathbb{C} \subset H(\mathbb{C})$ a z vlastnosti zobrazení $H(\mathbb{C}) \subset H(H(\mathbb{C}))$ TODO! $H(\mathbb{C}) \subset \mathbb{C}$. □

Důkaz
Předpokládáme $\mathbb{X} \preceq \mathbb{Y} \implies$ existuje prosté zobrazení $f : \mathbb{X} \to \mathbb{Y}$ a $\mathbb{Y} \preceq X \implies$ existuje prosté zobrazení $f : \mathbb{Y} \to \mathbb{X}$.

Definujeme $H : \mathcal{P}(\mathbb{X}) \to \mathcal{P}(\mathbb{X})$ předpisem $H(\mathbb{A}) = \mathbb{X} \setminus g(\mathbb{Y} \setminus f(\mathbb{A}))$. (Pozorování, jestliže $f = g^{-1}$ je prosté a na, tak H je identita.) Nyní ověříme předpoklady Lemmatu.

Nechť $\mathbb{U} \subset \mathbb{V} \subset \mathbb{X}$. Pak $f(\mathbb{U}) \subset f(\mathbb{V}) \implies \mathbb{Y} \setminus f(\mathbb{V}) \subset \mathbb{Y} \setminus f(\mathbb{U}) \implies g(\mathbb{Y} \setminus f(\mathbb{V})) \subset g(\mathbb{Y} \setminus f(\mathbb{U})) \implies \mathbb{X} \setminus g(\mathbb{Y} \setminus f(\mathbb{U})) \subset \mathbb{X} \setminus g(\mathbb{Y} \setminus f(\mathbb{V})) \implies H(\mathbb{U}) \subset H(\mathbb{V})$.

Dle lemmatu existuje $\mathbb{C} \subset \mathbb{X}$ takové, že $H(\mathbb{C}) = \mathbb{C}$. Pak $\mathbb{C} = H(\mathbb{C}) = \mathbb{X} \setminus g(\mathbb{Y} \setminus f(\mathbb{C})), g(\mathbb{Y} \setminus f(\mathbb{C})) = \mathbb{X} \setminus \mathbb{C}$. Tedy $g|_{\mathbb{Y} \setminus f(\mathbb{C})}$ je prosté zobrazení $\mathbb{Y} \setminus f(\mathbb{C})$ ne $\mathbb{X}|\mathbb{C}$, a tedy $g^{-1}|_{\mathbb{X} \setminus \mathbb{C}}$ je prosté zobrazení $\mathbb{X} \setminus \mathbb{C}$ na $\mathbb{Y} \setminus f(\mathbb{C})$. Navíc jistě $f|_{\mathbb{C}}$ je prosté zobrazení $\mathbb{C}$ na $f(\mathbb{C})$

Definujeme $h(a) = f(a), a \in \mathbb{C} | h(a) = g^{-1}(a), a \in \mathbb{X} \setminus \mathbb{C}$. Potom h je prosté zobrazení $\mathbb{X}$ na $\mathbb{Y}$. □

4 Aritmetický, geometrický a harmonický průměr

Definice 4.1

Nechť $x_1, \ldots, x_n > 0$. Definujeme jejich

- aritmetický průměr jako $A_n = \frac{x_1 + \ldots + x_n}{n}$.
- geometrický průměr jako $G_n = \sqrt[n]{x_1 \cdot \cdots \cdot x_n}$
- harmonický průměr jako $H_n = \frac{n}{\frac{1}{x_1} + \ldots + \frac{1}{x_n}}$

Věta 4.1 (AGH nerovnost)

$$A_n \geq G_n \geq H_n$$

Poznámka (Pozorování)
Nerovnost $G_n \geq H_n$ snadno plyne z $A_n \geq G_N$, stačí dosadit $x_i = \frac{1}{y_i}$. Stačí ukázat nerovnost $A_n \geq G_n$.

Důkaz (1. Zpětnou indukcí)
Dokážeme pro mocniny 2. Následně dosadíme za jedno x geometrický průměr těch ostatních a budeme „indukovat" zpět. □

Důkaz (2. Indukcí)
Dokážeme pro 1.

Chceme odhadnout aritmetický průměr $n + 1$ čísel. Použijeme indukční předpoklad pro n čísel, jejichž aritmetický průměr je stejný. Za tato čísla zvolíme $x_1, \ldots, x_{n-1}, x'_n$, kde x'_n je doplnění, aby byly shodné aritmetické průměry. x'_n vyjádříme. Upravíme, řekneme, že x_n a x_{n+1} jsme zvolili, že budou nejmenší a největší číslo. □

Poznámka (2. referát)
Existuje i aritmeticko-geometrický průměr a aritmeticko-harmonický průměr (je roven geometrickému).

Příklad (3. teoretický)
Najděte všechna celá čísla m splňující

$$(1 + m)^n \geq 1 + mn, \forall n \in \mathbb{N}$$