

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 (Prvočíslu)

Řekněme, že $n \in \mathbb{N}$ je prvočíslu, 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:

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

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

┌
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 .

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

A není pravda, že (r_1, \dots, r_m) je permutací (q_1, \dots, 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, \dots, r_m . BÚNO $q_1 \mid r_1$, tedy $q_1 = r_1$. Vydělením n číslem q_1 dostaneme menší přirozené číslo, které nemá jednoznačný rozklad. ($\frac{n}{q_1} = q_2 \cdots q_l = r_2 \cdots r_m$). \square

Věta 1.3

Prvočísel je nekonečně mnoho.

┌
Důkaz

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

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

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. \square

┌
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 „řídnu“. Musí tedy existovat dlouhé úseky bez prvočísel.

┌ *Například*

Interval $[n! + 2, \dots, n! + n]$ neobsahuje žádné prvočíslu. (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.

Věta 2.2 (Referát 1)

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

Příklad (Teoretický příklad 1)

Nechť $n \in \mathbb{N}$ a necht a_1, \dots, a_n jsou kladná reálná čísla, taková, že $a_1 \cdot \dots \cdot a_n = 1$.

Dokažte, že

$$(1 + a_1) \cdot \dots \cdot (1 + a_n) \geq 2^n.$$