

# Prvočísla

6. októbra 2023

# Prvočísla

## Definícia

Nech  $n > 1$  je prirodzené číslo. Ak  $n = m \cdot k$  pre nejaké celé čísla  $1 < m, k < n$ , tak hovoríme, že  $n$  je *zložené číslo*. V opačnom prípade hovoríme, že  $n$  je *prvočíсло*.

Množinu všetkých prvočísel budeme označovať  $\mathbb{P}$ .

# Prvočísel je nekonečne veľa

## Lema

*Pre každé prirodzené číslo  $n > 1$  existuje prvočíslo  $p$  také, že  $p \mid n$ .*

Pri testovaní, či  $n$  je zložené, stačí skúšať deliteľnosť prvočíslami

$$p \leq \sqrt{n}.$$

## Veta (Euklides)

*Množina  $\mathbb{P}$  je nekonečná.*

# Vlastnosti prvočísel

## Lema

*Nech  $p$  je prvočíslo.*

- (i) Nech  $a \in \mathbb{Z}$ . Potom  $(a, p) = 1$  alebo  $(a, p) = p$ .*
- (ii) Nech  $a, b \in \mathbb{Z}$ . Ak  $p \mid ab$ , tak  $p \mid a$  alebo  $p \mid b$ .*
- (iii) Nech  $a_1, \dots, a_n \in \mathbb{Z}$ . Ak  $p \mid a_1 \dots a_n$ , tak  $p \mid a_k$  pre niektoré  $k = 1, \dots, n$ .*

# Základná veta aritmetiky, kanonický rozklad

## Veta (Základná veta aritmetiky)

*Každé prirodzené číslo  $n > 1$  je možné zapísať ako súčin prvočísel*

$$n = p_1 \cdot \dots \cdot p_k.$$

*Tento zápis je jednoznačný až na poradie.*

# Základná veta aritmetiky, kanonický rozklad

## Definícia

Jednoznačný zápis čísla  $n$  v tvare  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ , kde  $p_1, \dots, p_k$  sú navzájom rôzne prvočísla a  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ , nazývame *kanonický rozklad* čísla  $n$ .

$$1125 = 5^2 \cdot 7^2$$

$$5! = 120 = 2^3 \cdot 3 \cdot 5$$

$$1400 = 2^3 \cdot 5^2 \cdot 7$$