

# Jacobiho symbol

16. decembra 2022

# Jacobiho symbol

## Definícia

Nech  $P$  je nepárne číslo a  $P = p_1 \cdot \dots \cdot p_r$ , kde  $p_1, \dots, p_r$  sú (nepárne) prvočísla. Potom *Jacobiho symbol*  $\left(\frac{m}{P}\right)$  je definovaný ako

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p_1}\right) \left(\frac{m}{p_2}\right) \dots \left(\frac{m}{p_r}\right).$$

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1)(-1) = 1 \text{ ale } 2\overline{R}15$$

# Jacobiho symbol

## Lema

Nech  $P, Q$  sú nepárne prirodzené čísla a  $a, b \in \mathbb{Z}$ . Potom

$$(i) \quad a \equiv b \pmod{P} \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$$

$$(ii) \quad \left(\frac{1}{P}\right) = 1$$

$$(iii) \quad \left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right)$$

$$(iv) \quad \left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \left(\frac{a}{Q}\right)$$

$$(v) \quad Ak \ (b, P) = 1, \text{ tak } \left(\frac{b^2}{P}\right) = 1.$$

$$(vi) \quad Ak \ (b, P) = 1, \text{ tak } \left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right).$$

# Jacobiho symbol

## Tvrdenie

*Nech  $P$  je nepárne prirodzené číslo. Potom*

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}$$

$$\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}$$

# Jacobiho symbol

## Veta (Zákon reciprocity pre Jacobiho symbol)

Pre ľubovoľné nepárne prirodzené čísla  $P \neq Q$  platí

$$\left(\frac{P}{Q}\right) = (-1)^{(P-1)(Q-1)/4} \left(\frac{Q}{P}\right).$$

## Dôsledok

Ak  $P \neq Q$  sú nepárne čísla, tak

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)$$

s výnimkou prípadu, že  $P \equiv Q \equiv 3 \pmod{4}$ . (V tomto prípade

$$\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right).$$

# Jacobiho symbol

## Príklad

$$\begin{aligned} \left(\frac{219}{383}\right) &= \left(\frac{383}{219}\right) (-1)^{109 \cdot 191} = -\left(\frac{383}{219}\right) = -\left(\frac{383 - 219}{219}\right) = \\ &= -\left(\frac{164}{219}\right) = -\left(\frac{4 \cdot 41}{219}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{41}{3}\right) \left(\frac{41}{73}\right) \end{aligned}$$

# Jacobiho symbol

## Tvrdenie

*Nech  $a$  je celé číslo, ktoré nie je druhou mocninou celého čísla. Potom existuje nekonečne veľa prvočísel  $p$ , pre ktoré je  $a$  kvadratický nezvyšok.*

$$x \equiv 1 \pmod{l_i} \quad \text{pre } i = 1, 2, \dots, t$$

$$x \equiv 1 \pmod{8}$$

$$x \equiv 1 \pmod{q_j} \quad \text{pre } j = 1, 2, \dots, n - 1$$

$$x \equiv s \pmod{q_n}$$

# Kvadratické kongruence modulo zložené čísla

## Veta

*Nech  $p$  je nepárne prvočíslo,  $p \nmid a$  a  $n \geq 1$ . Potom  $a$  je kvadratický zvyšok modulo  $p^n$  právě vtedy, keď  $\left(\frac{a}{p}\right) = 1$ .*



# Kvadratické kongruencie modulo zložené čísla

## Tvrdenie

*Modulo 2, 4 alebo 8 je jediným nepárnym kvadratickým zvyškom číslo 1.*

*Ak  $n \geq 3$ , tak existuje  $2^{n-3}$  nepárnych kvadratických zvyškov modulo  $2^n$  a sú to práve čísla tvaru  $8k + 1$ .*