Jacobiho symbol

28. septembra 2023

Jacobiho symbol

Jacobiho symbol

Definícia

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

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

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

Jacobiho symbol

Jacobiho symbol

Lema

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

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

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

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

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

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

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

Jacobiho symbol

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

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

Jacobiho symbol

Príklad

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

Jacobiho symbol

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.

$$\begin{aligned} x &\equiv 1 \pmod{l_i} && \text{pre } i = 1, 2, \ldots, t \\ x &\equiv 1 \pmod{8} && \\ x &\equiv 1 \pmod{q_j} && \text{pre } j = 1, 2, \ldots, n-1 \\ x &\equiv s \pmod{q_n} && \end{aligned}$$

Kvadratické kongruencie modulo zložené čísla

Veta

Nech p je nepárne prvočíslo, $p \nmid a$ a $n \geq 1$. Potom a je kvadratický zvyšok modulo p^n práve 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* $8k + 1$.