Kvadratické zvyšky a Legendrov symbol

8. decembra 2020

Kvadratické zvyšky

Kvadratické zvyšky

Definícia

Nech $n \nmid q$. Potom sa číslo q sa nazýva *kvadratický zvyšok* modulo n, ak existuje také $x \in \mathbb{Z}$, že

$$x^2 \equiv q \pmod{n}.$$

Inak: q je *kvadratický nezvyšok* modulo n.
Stručnejší zápis:
qRn, ak q je kvadratický zvyšok modulo n
$q\overline{R}n$, ak q je kvadratický nezvyšok modulo n.

Zaujíma nás prípad, keď n je nepárne prvočíslo.

Kvadratické zvyšky

Kvadratické zvyšky

Príklad

Kvadratické zvyšky modulo 7 sú 1, 2 a 4.

$$1^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$4^2 \equiv (-3)^2 \equiv 3^2 \equiv 2 \pmod 7$$
$$5^2 \equiv (-2)^2 \equiv 2^2 \equiv 4 \pmod 7$$
$$6^2 \equiv (-1)^2 \equiv 1^2 \equiv 1 \pmod 7$$

Kvadratické zvyšky

Kvadratické zvyšky

Definícia

Množina čísel $n_1, \ldots, n_{\varphi(n)}$ sa nazýva *redukovaný zvyškový systém* modulo n ak sú tieto čísla reprezentantmi všetkých redukovaných zvyškových tried modulo n.

Ekvivalentne: Je to takých $\varphi(n)$ čísel, že žiadne dve z nich nie sú kongruentné modulo n a navyše každé z nich je nesúdeliteľné s n.

Kvadratické zvyšky

Kvadratické zvyšky

Veta

Nech $p > 2$ prvočíslo. Ľubovoľný redukovaný zvyškový systém $\{a_1, \ldots, a_{p-1}\}$ modulo p obsahuje $\frac{p-1}{2}$ kvadratických zvyškov a $\frac{p-1}{2}$ kvadratických nezvyškov modulo p.
Kvadratické zvyšky sú práve tie čísla, ktoré sú kongruentné s číslami $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Medzi číslami $1, 2, \ldots, p-1$ máme $\frac{p-1}{2}$ kvadratických zvyškov a $\frac{p-1}{2}$ kvadratických nezvyškov modulo p.

Legendrov symbol

Legendrov symbol

Definícia

Ak p je prvočíslo a a je celé číslo, tak *Legendrov symbol* $\left(\frac{a}{p}\right)$ definujeme nasledovne:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } aRp, \\ -1 & \text{ak } a\overline{R}p, \\ 0 & \text{ak } p \mid a. \end{cases}$$

Niekedy sa používa aj označenie $(a|p)$.

$\left(\frac{1}{p}\right) = 1$, $\left(\frac{3}{7}\right) = -1$, $\left(\frac{4}{7}\right) = 1$, $\left(\frac{a^2}{p}\right) = 1$

Legendrov symbol

Eulerovo kritérium

Veta (Eulerovo kritérium)

Nech $p > 2$ je prvočíslo. Potom pre všetky n platí

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

Príklad

$\left(\frac{4}{7}\right) \equiv 4^3 \equiv 2 \cdot 4 \equiv 1 \pmod{7}$

Legendrov symbol

Legendrov symbol

Lema

Nech p je nepárne prvočíslo 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) $\left(\frac{a^2}{p}\right) = 1$

(v) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Legendrov symbol

Kedy je -1 kvadratický zvyšok?

Tvrdenie

Pre každé nepárne prvočíslo platí

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Teda -1 je kvadratický zvyšok modulo p ak $p = 4k + 1$ a kvadratický nezvyšok modulo p ak $p = 4k + 3$.

Tvrdenie

Existuje nekonečne veľa prvočísel tvaru $4k + 1$.

Legendrov symbol

Kedy je 2 kvadratický zvyšok?

Tvrdenie

Nech $p > 2$ je prvočíslo. Potom

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Teda 2 je kvadratický zvyšok pre prvočísla tvaru $8k \pm 1$ a kvadratický nezvyšok pre prvočísla tvaru $8k \pm 3$.

Tvrdenie

Existuje nekonečne veľa prvočísel tvaru $8k + 7$.

Legendrov symbol

Mersennove prvočísla

Veta

Ak $p = 4k + 3$ *je prvočíslo,* $k > 1$, *tak* $q = 2p + 1$ *je prvočíslo práve vtedy, keď* $2p + 1 \mid M_p = 2^p - 1$.

Prvočísla Sophie-Germainovej = p aj $2p + 1$ sú prvočísla

Gaussova lema

Gaussova lema

Veta (Gaussova lema)

Nech $p > 2$ je prvočíslo a $p \nmid a$. Nech m je počet tých čísel z množiny $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, ktorých zvyšok po delení p je väčší než $\frac{p}{2}$. Potom

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Gaussova lema

Gaussova lema

Veta

Pre číslo m z Gaussovej lemy platí

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor \pmod 2.$$

Teda

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{2ak}{p} \rfloor}.$$

Pre nepárne a platí

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}.$$