Kvadratni ostatci

Ivan Novak

16.6.2019.

Uvod

Neka je p prost broj. Za prirodan broj n koji nije djeljiv s p kažemo da je kvadratni ostatak modulo p ako postoji prirodan broj a takav da $p \mid a^2 - n$. U suprotnom, kažemo da je neostatak.

Za cijeli broj a i neparan prost broj p, Legendreov simbol $\left(\frac{a}{p}\right)$ definiramo na sljedeći način:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ ako p dijeli a} \\ 1, \text{ ako je a kvadratni ostatak modulo p} \\ -1, \text{ ako je a kvadratni neostatak modulo p.} \end{cases}$$

Svojstva Legendreovog simbola

(a, b su proizvoljni cijeli brojevi, a p proizvoljan neparan prost broj):

- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- $\left(\frac{a+bp}{p}\right) = \left(\frac{a}{p}\right)$
- (Eulerov kriterij) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Gaussov zakon reciprociteta

Neka su p i q različiti neparni prosti brojevi. Tada vrijedi Gaussov zakon reciprociteta:

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

I njegov suplement

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ ako je } p \text{ oblika } 8k \pm 1 \\ -1, \text{ inače.} \end{cases}$$

Jacobijev simbol

Jacobijev simbol je generalizacija Legendreovog simbola.

Jacobijev simbol dopušta da drugi argument nije samo prosti broj, nego može biti i neparan složeni broj. Za prirodan broj a i neparan prirodan broj $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, definiramo Jacobijev simbol $\left(\frac{a}{n}\right)$ preko Legendreovog na sljedeći način:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{a_k}.$$

Važno je primijetiti da ako je Jacobijev simbol $\left(\frac{a}{n}\right)$ jednak -1, tada je a sigurno kvadratni neostatak modulo n, ali ako je Jacobijev simbol jednak 1, tada a nije nužno kvadratni ostatak.

Svojstva Jacobijevog simbola

Navedena svojstva relativno jednostavno slijede iz svojstava Legendreovog simbola. (m i n su neparni prirodni brojevi, a i b su cijeli)

- $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$
- $\left(\frac{a}{m}\right)\left(\frac{a}{n}\right) = \left(\frac{a}{mn}\right)$
- $\left(\frac{a+bm}{n}\right) = \left(\frac{a}{n}\right)$
- $\left(\frac{a}{n}\right) = \begin{cases} 0 \text{ ako je } \gcd(a,n) > 1 \\ \pm 1, \text{ inače} \end{cases}$
- $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
- $\left(\frac{2}{n}\right) = \begin{cases} 1, \text{ ako je } n \text{ oblika } 8k \pm 1 \\ -1, \text{ inače.} \end{cases}$
- (Analogon zakona reciprociteta) Za relativno proste m i n, vrijedi
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Zadaci

I Dokaži Eulerov kriterij.

II Dokaži da ako $a \in \mathbb{N}$ nije potpun kvadrat, tada postoji beskonačno prostih brojeva p takvih da a nije kvadratni ostatak modulo p.

III Dokaži da za svaki prost broj p vrijedi da postoji $x \in \mathbb{Z}$ takav da $p \mid x^2 - x + 3$ ako i samo ako postoji $y \in \mathbb{Z}$ takav da $p \mid y^2 - y + 25$.

IV Postoji li normirani polinom P s cjelobrojnim koeficijentima bez cjelobrojnih nultočaka takav da za svaki prost broj p postoji cijeli broj x_p takav da je $P(x_p)$ djeljiv s p?

V Neka je $f : \mathbb{N} \to \mathbb{N}$ funkcija takva da je $f(n) < 2019\sqrt{n}$ te vrijedi da je $2f(n)^2 - n^2$ potpun kvadrat za sve $n \in \mathbb{N}$. Dokaži da f ima beskonačno fiksnih točaka, odnosno brojeva n za koje je $f(n) = n$.

VI Dokaži da $4xyz - x - y$ nije potpun kvadrat ni za koja tri prirodna broja x, y, z.

VII Dokaži da ne postoje prirodni brojevi a, b, c takvi da je

$$\frac{a^2 + b^2 + c^2}{3(ab + bc + ca)}$$

prirodan broj.