

Kvadratni recipročnostni zakon

Dejan Perić

Mentor: izr. prof. dr. Aleš Vavpetič

Ljubljana 2022

1 Uvod

Vemo že, da ima enačba $x^2 = a$ v polju kompleksnih števil $\mathbb{C}$ vedno dve rešitvi za katerikoli $a \in \mathbb{C} \setminus \{0\}$. Nadalje vemo tudi, da ima ta ista enačba v polju realnih števil dve rešitvi le za pozitiven a , eno pri $a = 0$ in nobene za negativne a -je. V delu nas bo zanimala rešljivost enačbe $x^2 = a$ v polju ostankov celih števil pri deljenju s praštevilom p ($\mathbb{Z}/p\mathbb{Z}$). Pri ugotavljanju rešljivosti take enačbe si bomo pomagali s kvadratnim recipročnostnim zakonom.

2 Kvadratni ostanki

Opazujemo enačbo $x^2 \equiv a \pmod{p}$. Zanima nas, ali obstaja rešitev za vsak $a \in \mathbb{Z}/p\mathbb{Z}$. Naj bo najprej $p = 2$. V kolobarju $\mathbb{Z}/2\mathbb{Z}$ imamo le 2 elementa, 0 in 1. Preverimo, kako je z rešljivosti teh dveh enačb:

$$\begin{aligned} x^2 \equiv 0 \pmod{2} &\Rightarrow x = 0 \text{ reši enačbo} \\ x^2 \equiv 1 \pmod{2} &\Rightarrow x = 1 \text{ reši enačbo} \end{aligned}$$

Vidimo, da imata obe enačbi rešitev v $\mathbb{Z}/2\mathbb{Z}$. Poglejmo, kako je s kvadratnimi enačbami v $\mathbb{Z}/3\mathbb{Z}$, tu imamo tri elemente v kolobarju, se pravi tri različne kvadratne enačbe:

$$\begin{aligned} x^2 \equiv 0 \pmod{3} &\Rightarrow x = 0 \text{ reši enačbo} \\ x^2 \equiv 1 \pmod{3} &\Rightarrow x = 1 \text{ reši enačbo} \\ x^2 \equiv 2 \pmod{3} &\Rightarrow \text{Rešitev ne obstaja,} \end{aligned}$$

Opazimo, da v $\mathbb{Z}/3\mathbb{Z}$ niso vse kvadratne enačbe rešljive.

Definicija 1. Naj bo p praštevilo. Število $a \in \mathbb{Z}/p\mathbb{Z}$, za katerega obstaja rešitev enačbe $x^2 \equiv a \pmod{p}$, imenujemo **kvadratni ostanek** po modulu p . Množico vseh kvadratnih ostankov po modulu p označimo kot

$$KOST_p = \{a \in \mathbb{Z}/p\mathbb{Z} : \exists x : x^2 \equiv a \pmod{p}\}.$$

Zgled 1. Za praštevila 2, 3 in 5 bodo množice kvadratnih ostankov izgledala takole:

$$\begin{aligned} KOST_2 &= \{0, 1\} \\ KOST_3 &= \{0, 1\} \\ KOST_5 &= \{0, 1, 4\} \end{aligned}$$

x	0	1	2	3	4
x^2	0	1	4	4	1

O velikosti množice kvadratnih ostankov nam pove naslednja trditev.

Trditev 1. Za vsa liha praštevila velja

$$|KOST_p| = \frac{p+1}{2}.$$

3 Legendrov simbol in Eulerjev izrek

Definicija 2. Naj bo p liho praštevilo in $a \in \mathbb{Z}$. Definiramo **Legendrov simbol**:

$$\left(\frac{a}{p}\right) = \begin{cases} 1; & a \in KOST_p \text{ in } a \not\equiv 0 \pmod{p}, \\ -1; & a \notin KOST_p \text{ in } a \not\equiv 0 \pmod{p}, \\ 0; & a \equiv 0 \pmod{p}. \end{cases}$$

Legendrov simbol nam pove o rešljivosti kvadratne enačbe $x^2 \equiv a \pmod{p}$. Če je Legendrov simbol enak 1 ali 0, je kvadratna enačba rešljiva, drugače pa ne. S pomočjo zgleda 1 lahko ugotovimo, da je

$$\left(\frac{3}{5}\right) = -1 \text{ in } \left(\frac{4}{5}\right) = 1$$

S pomočjo izreka o homomorfizmu in malega Fermatovega izreka se da pokazati naslednje dejstvo.

Izrek 1. (*Euler*) Naj bo p liho praštevilo in $a \in \mathbb{Z}$. Velja

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

Za Legendrov simbol veljajo naslednje lastnosti:

- $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
- $\left(\frac{a^2}{p}\right) = 1$, saj je kar a rešitev kvadratne enačbe,
- $\left(\frac{1}{p}\right) = 1$,
- Multiplikativnost: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Dokažimo multiplikativnost, pomagali si bomo z zgornjim Eulerjevim izrekom.

$$\begin{aligned}\left(\frac{ab}{p}\right) &= ab^{\frac{p-1}{2}} \pmod{p} \\ &= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p} \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\end{aligned}$$

4 Pomožni trditvi

Zraven kvadratnega recipročnostnega zakona se omenjata tudi dve pomožni trditvi, ki povesta o vrednosti Legendrovega simbola, ko sta na vrhu -1 in 2 .

Trditev 2. *Naj bo p liho praštevilo. Velja*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1; & p \equiv 1 \pmod{4}, \\ -1; & p \equiv 3 \pmod{4} \end{cases}$$

Dokaz. Po Eulerjevem izreku velja $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Eksponent $\frac{p-1}{2}$ bo sodo število natanko tedaj, ko bo $\frac{p-1}{2}$ enak $2k$ za neko celo število k . Nadalje pomnožimo enačbo z 2 in ugotovimo, da mora biti $p-1 = 4k$ za neko celo število k . Sledi, da to velja natanko takrat, ko je $p \equiv 1 \pmod{4}$. $\square$

Trditev 3. *Naj bo p liho praštevilo. Velja*

$$\left(\frac{2}{p}\right) = \begin{cases} 1; & p \equiv \pm 1 \pmod{8}, \\ -1; & p \equiv 3, 5 \pmod{8} \end{cases} = (-1)^{\frac{p^2-1}{8}}$$

S pomočjo zgornjih dveh trditev lahko dokaj enostavno ugotovimo vrednosti naslednjih Legendrovih simbolov.

Zgled 2.

$$\left(\frac{-1}{6301}\right) = 1, \text{ ker } 6301 \equiv 1 \pmod{4}$$

$$\left(\frac{2}{11213}\right) = -1, \text{ ker } 11213 \equiv 5 \pmod{8}$$

Enačba $x^2 \equiv -1 \pmod{6301}$ je torej rešljiva, $x^2 \equiv 2 \pmod{11213}$ pa ne.

5 Kvadratni recipročnostni zakon

Izrek 2. (Kvadratni recipročnostni zakon) *Naj bosta p in q različni lihi praštevili. Velja*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1; & p \equiv 1 \text{ ali } q \equiv 1 \pmod{4}, \\ -1; & p \equiv q \equiv 3 \pmod{4} \end{cases} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

S pomočjo izreka in lastnosti Legendrovega simbola lahko dokaj enostavno ugotovimo naslednje vrednosti Legendrovega simbola.

Zgled 3. *Koliko je $\left(\frac{3}{6700417}\right)$?*

$$\begin{aligned}\left(\frac{3}{6700417}\right)\left(\frac{6700417}{3}\right) &= 1, \text{ ker je } 6700417 \equiv 1 \pmod{4} \\ \left(\frac{6700417}{3}\right) &= \left(\frac{1}{3}\right), \text{ ker je } 6700417 \equiv 1 \pmod{3} \\ &= 1 \\ \Rightarrow \left(\frac{3}{6700417}\right) &= 1\end{aligned}$$

Enačba $x^2 \equiv 3 \pmod{6700417}$ je rešljiva.

Kvadratni recipročnostni zakon je znan kot izrek, ki ima poleg Pitagorovega izreka največje število dokazov. Obstaja namreč preko 200 dokazov izreka. Prvi ga je dokazal Carl Friedrich Gauss leta 1796 pri svojih 19 letih, kasneje pa je zakon dokazal še na 7 različnih načinov. V diplomskem delu bomo kvadratni recipročnostni zakon dokazali s pomočjo Zolotareve leme in si pogledali, kje je izrek nadalje uporaben v teoriji števil in drugje.

Literatura

- [1] E. Brown, The first proof of the quadratic reciprocity law, revisited. Amer. Math. Monthly 88 (1981), no. 4, 257—264