

Kvadratiske rester:

Låt p vara ett udda primtal.

Ett tal $a \not\equiv 0 \pmod{p}$ är en kvadratisk rest mod p om det finns heltal x så $x^2 \equiv a \pmod{p}$.

Ett tal $a \not\equiv 0 \pmod{p}$ är en icke-kvadratisk rest om $x^2 \equiv a \pmod{p}$ saknar lösning.

Notera att $a \equiv 0 \pmod{p}$ varken är kvadratisk eller icke-kvadratisk enligt definitionen.

Om $a \equiv b \pmod{p}$ är ekvationerna

$$x^2 \equiv a \pmod{p}$$

$$x^2 \equiv b \pmod{p}$$

ekvivalenta, så a kvadratisk rest $(\Leftrightarrow)$ b kvadratisk rest.

Det finns, upp till kongruens, exakt $\frac{p-1}{2}$ kvadratiske rester mod p och $\frac{p-1}{2}$ icke-kvadratiske rester mod p .

Exempel:

- 1 är en kvadratisk rest för alla p $\exists y \ x^2 \equiv 1 \pmod{p}$
har lösning $x = \pm 1$
- 9 är en kvadratisk rest för alla $p \neq 3$.
 $\exists y \ x^2 \equiv 9 \pmod{p}$ har lösning $x = \pm 3$ och $9 \not\equiv 0 \pmod{p}$ för $p \neq 3$

Exempel: Bestäm de kvadratiske och
icke-kvadratiske resterna mod 11.

Vilka värden kan x^2 mod 11 anta?

x	x^2 mod 11
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Vi ser att $x^2 \equiv a \pmod{11}$ är lösbar om

$a \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$ och saknar lösning

om $a \equiv 2, 6, 7, 8, 10 \pmod{11}$.

$a \equiv 0 \pmod{11}$ är per definition varken rest, eller
icke-rest.

De kvadratiske resterna ges upp till kongruens mod 11
av: 1, 3, 4, 5, 9 och de icke-kvadratiske resterna av
2, 6, 7, 8, 10.

Låt p vara ett udda primtal och a, b heltal så $a, b \not\equiv 0 \pmod{p}$.

Legendresymbolen $\left(\frac{a}{p}\right)$ (Obs ej division) definieras

av

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{om } a \text{ kvadratisk rest mod } p. \\ -1 & \text{om } a \text{ ickekvadratisk rest mod } p. \end{cases}$$

Legendresymbolen har egenskaper:

- $\left(\frac{a}{p}\right) = 1$
- $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ om $a \equiv b \pmod{p}$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

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

- $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{om } p \equiv 1 \pmod{4} \\ -1 & \text{om } p \equiv 3 \pmod{4} \end{cases}$
- $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{om } p \equiv 1, 7 \pmod{8} \\ -1 & \text{om } p \equiv 3, 5 \pmod{8} \end{cases}$

Kvadratisk reciprocitetssatsen: Låt p, q udda primtal. Då gäller

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} 1 & \text{om } \text{sgn } p, q \equiv 1 \pmod{4} \\ -1 & \text{om } \text{både } p, q \equiv 3 \pmod{4}. \end{cases}$$

Exempel: Finns det något heltal s.a.

$$x^2 \equiv 85 \pmod{101}?$$

101 är ett (udda) primtal.

Detta är samma som att $\left(\frac{85}{101}\right) = 1$.

$$85 = 5 \cdot 17$$

$$\left(\frac{85}{101}\right) = \left(\frac{5}{101}\right) \left(\frac{17}{101}\right)$$

$$\stackrel{\text{kr. rec}}{=} \left(\frac{101}{5}\right) \left(\frac{101}{17}\right)$$

$$= \left(\frac{1}{5}\right) \left(\frac{-1}{17}\right)$$

$$= 1 \cdot \left(\frac{-1}{17}\right)$$

$$= 1$$

$$\dagger 101 \equiv 5 \equiv 17 \equiv 1 \pmod{4}$$

$$\dagger 101 \equiv 1 \pmod{5}$$

$$101 = 6 \cdot 17 - 1 \equiv -1 \pmod{17}$$

$\dagger 1$ kvadratisk rest mod allt

$$\dagger 17 \equiv 1 \pmod{4}$$

Ja, $x^2 \equiv 85 \pmod{101}$ har lösningar.