# Quadratische Reste I

Dr. Stephan Ehlen

Arian Joharian, Valerie Dang
(Seminar über „Elementare Zahlentheorie und Algebra“) 23. April 2019

---

## Definition 0 (Quadratischer Rest)

Für ein a mit $a \not\equiv 0 \mod p$ heißt a **quadratischer Rest** mod p, falls

$$x^2 \equiv a \mod p$$

lösbar ist, sonst **quadratischer Nichtrest**.

## Definition 1 (Legendre-Symbol)

Für eine Primzahl p ist das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } x^2 \equiv a \mod p \text{ lösbar ist und } a \not\equiv 0 \mod p. \\ -1 & \text{falls } x^2 \equiv a \mod p \text{ nicht lösbar ist.} \\ 0 & \text{falls } a \equiv 0 \mod p. \end{cases}$$

## Satz 3

Sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$, dann gilt:

1. $a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. (Gilt auch für p=2.)
2. *(Euler)* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.
3. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{für } p \equiv 1 \mod 4 \\ -1 & \text{für } p \equiv 3 \mod 4. \end{cases}$
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
5. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ für $b \not\equiv 0 \mod p$.

## Lemma 4 (Gauß)

Sei p eine ungerade Primzahl. Dann gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{für } p \equiv \pm 1 \mod 8 \\ -1 & \text{für } p \equiv \pm 3 \mod 8. \end{cases}$$

## Satz 5 (Quadratisches Reziprozitätsgesetz von Gauß)

Seien $p \neq q$ ungerade Primzahlen. Dann gilt

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

dh.

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{für } p \equiv q \equiv 3 \mod 4 \\ \left(\frac{p}{q}\right) & \text{sonst.} \end{cases}$$