Quadratische Reste II

Dr. Stephan Ehlen

Valerie Dang, Arian Joharian
(Seminar über „Elementare Zahlentheorie und Algebra“) 30. April 2019

Definition 8 (Jacobi-Symbol)

Sei n eine ungerade natürliche Zahl und $n = \prod_{i=1}^{s} q_i^{r_i}$ ihre Primfaktorzerlegung. Dann ist das **Jacobi-Symbol** als

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right)^{r_i}$$

definiert.

Warnung: Falls a ein quadratischer Rest modulo n ist, ist das Jacobi-Symbol 1. Die Umkehrung gilt jedoch nicht!

Die Eigenschaften des Legendre-Symbols vererben sich auf das Jacobi-Symbol. So hängt es nur von a modulo n ab und ist multiplikativ in a. Seine Multiplikativität in n folgt direkt aus der Definition.

Satz 9 (Reziprozitätsgesetz für Jacobi-Symbol)

Seien $m \neq n \geq 3$ ungerade natürliche Zahlen. Dann gilt

1. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
2. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.
3. $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} \cdot \left(\frac{n}{m}\right)$

Lemma 10

Sei p eine Primzahl mit $p \equiv 3 \mod 4$ und d ein quadratischer Rest modulo p. Dann ist $d^{\frac{p+1}{4}}$ eine Lösung von $x^2 \equiv d \mod p$.

Algorithmus (Tonelli-Shanks)

Sei p eine ungerade Primzahl. Dann lässt sich mit dem **Algorithmus von Tonelli und Shanks** eine Lösung für $x^2 \equiv d \mod p$ finden:

(0) Prüfe, ob d ein quadratischer Rest mod p ist mithilfe des Jacobi-Symbols.
Ja $\rightarrow$ (1).
Nein $\rightarrow$ keine Lösung.

(1) Schreibe $p - 1 = 2^e \cdot q$ mit $e, q \in \mathbb{N}$ und $2 \nmid q$.

(2) Bestimme $a := d^{\frac{q+1}{2}}$.

(3) Wähle ein $x \in \mathbb{N}$, $0 < x < p$. Bestimme $\sigma := x^q$.

(4) Prüfe $\sigma^{2^{e-1}} \mod p$.
Falls $\sigma^{2^{e-1}} \equiv 1 \mod p \rightarrow$ (3).
Sonst $\rightarrow$ (5).

(5) Wir suchen ein $l \in \mathbb{N}$, $0 \leq l < 2^e$: $\frac{d}{a^2} \equiv \sigma^l \mod p$. Schreibe l binär, dh. $l = \sum_{i=0}^{e-1} l_i \cdot 2^i$, $l_i \in \{0, 1\}$. Seien $l_0, l_1, ..., l_{s-1}$ gegeben und l_s gesucht, dann gilt:

$$(\frac{d}{a^2} \cdot \exp_\sigma(-\sum_{i=0}^{s-1} l_i \cdot 2^i))^{2^{e-s-1}} \equiv (-1)^{l_s} \mod p.$$

$\rightsquigarrow$ Bilde l.

(6) $a \cdot \sigma^{\frac{l}{2}}$ ist Lösung von $x^2 \equiv d \mod p$.