§ 13. Quadratische Reste

Wir behandeln jetzt bei den Potenzresten den Spezialfall $\underline{m = 2}$ und führen die folgende Begriffsbildung ein:

<u>(13.1) DEF:</u> Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd. a heißt **quadratischer Rest modulo** n (abgekürzt **QR mod** n), wenn die Kongruenz

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

lösbar ist, d.h. wenn a 2–ter Potenzrest modulo n ist. Anderenfalls heißt a **quadratischer Nichtrest modulo** n (abgekürzt **QNR mod** n).

Wir spezialisieren zunächst einige frühere Ergebnisse auf den Fall $m = 2$. Aus (12.12) folgt:

<u>(13.2) BEM:</u> Besitzt die natürliche Zahl $n \geq 2$ die kanonische Primfaktorzerlegung $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$, so ist eine zu n teilerfremde Zahl $a \in \mathbb{Z}$ genau dann QR mod n, wenn a QR mod $p_i^{k_i}$ für alle $i = 1, 2, \ldots, r$ ist.

<u>(13.3) BEM:</u> Aus (12.16) folgt: Seien $a \in \mathbb{Z}$ ungerade und $k \in \mathbb{N}$ mit $k \geq 3$. Genau dann ist a QR mod 2^k, wenn gilt:

i) $a \equiv 1 \pmod{4}$ und **ii)** $a^{2^{k-3}} \equiv 1 \pmod{2^k}$.

<u>(13.4) LEMMA:</u> Seien $k \in \mathbb{N}$, $k \geq 3$ und $a \in \mathbb{Z}$. Dann gilt:

a) a QR mod 2 $\iff$ $a \equiv 1 \pmod{2}$

b) a QR mod 4 $\iff$ $a \equiv 1 \pmod{4}$

c) a QR mod 2^k $\iff$ $a \equiv 1 \pmod{8}$.

Da es Primitivwurzeln mod p^k gibt ($p \in \mathbb{P}$, $p > 2$), folgt aus (12.14)

<u>(13.5) BEM:</u> Seien $p \in \mathbb{P}$, $p > 2$ und $k \in \mathbb{N}$. Eine Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ ist genau dann ein QR modulo p^k, wenn gilt:

$$a^{\frac{1}{2}\varphi(p^k)} \equiv 1 \pmod{p^k}.$$

<u>(13.6) SATZ:</u> Seien $p \in \mathbb{P}$, $p > 2$ und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann folgt:

a) a ist genau dann QR mod p, wenn $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ gilt.

b) a ist genau dann QNR mod p, wenn $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ gilt.

<u>(13.7) KOROLLAR:</u> p sei eine ungerade Primzahl, und es seien $a \in \mathbb{Z}$ und $k \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:

a) a ist QR mod p^k **b)** a ist QR mod p.

(13.8) KOROLLAR: Sei p eine ungerade Primzahl. Dann gilt:

a) Das Produkt zweier QR'e mod p ist ein QR mod p.

b) Das Produkt zweier QNR'e mod p ist ein QR mod p.

c) Das Produkt eines QR'es mod p und eines QNR'es mod p ist ein QNR mod p.

(13.9) DEF: Sei $p > 2$ eine (ungerade) Primzahl. Ist dann die Zahl $a \in \mathbb{Z}$ teilerfremd zu p, so ist das **Legendre–Symbol** $\left(\frac{a}{p}\right)$ (lies: "a nach p") definiert durch:

$$\left(\frac{a}{p}\right) := \begin{cases} 1\,, & \text{wenn } a \text{ QR mod } p \text{ ist} \\ -1\,, & \text{wenn } a \text{ QNR mod } p \text{ ist} \end{cases} .$$

Adrien Marie Legendre (1752–1833), französischer Mathematiker.

(13.10) Kriterium von Euler

Seien $p \in \mathbb{P}$, $p > 2$ und $a \in \mathbb{Z}$ mit $p \not| \, a$. Dann gilt

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

Leonhard Euler (1707–1783), Schweizer Mathematiker.

(13.11) KOROLLAR: **a)** Für eine Primzahl $p > 2$ gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$.

b) -1 ist genau dann QR mod p, wenn $p \equiv 1 \pmod 4$ gilt.

c) -1 ist genau dann QNR mod p, wenn $p \equiv 3 \pmod 4$ gilt.

(13.12) Rechenregeln für das Legendre–Symbol

Sei $p > 2$ eine ungerade Primzahl. Die Zahlen $a, b, c \in \mathbb{Z}$ seien alle teilerfremd zu p. Dann gilt:

a) $a \equiv b \pmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

b) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ **c)** $\left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)$.

(13.13) BEM: Sei p eine ungerade Primzahl.

a) Dann ist $\{0, 1, 2, \ldots, p-1\}$ ein vRS mod p. Wir werden im folgenden auch das folgende vRS mod p betrachten

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -2, -1, 0, 1, 2, \ldots \frac{p-3}{2}, \frac{p-1}{2}\right\} ,$$

das wir das **System der absolut kleinsten Reste modulo** p nennen.

b) Zu jeder Zahl $a \in \mathbb{Z}$ mit $p \not| \, a$ existiert genau eine Zahl $r \in \mathbb{Z}$ mit **i)** $a \equiv r \pmod p$ und **ii)** $0 < |r| = \min\{ |b| \mid b \in [a]_p \} \leq \frac{1}{2}(p-1) < \frac{1}{2}p$.

(13.14) LEMMA: Sei p eine ungerade Primzahl, und es sei $S := \{1, 2, 3, \ldots, \frac{1}{2}(p-1)\}$. Ferner sei $a \in \mathbb{Z}$ mit $p \not| \, a$. Dann gilt:

a) Zu jedem $s \in S$ existieren eindeutig bestimmte Zahlen $\varepsilon_s(a) \in \{+1, -1\}$ und $s_a \in S$ mit der Eigenschaft $s \cdot a \equiv \varepsilon_s(a) \cdot s_a \pmod p$.

b) Die Abbildung $\beta_a : S \longrightarrow S \, , \; s \longmapsto s_a$ ist bijektiv.

(13.15) Lemma von Gauß

Seien $p > 2$ eine Primzahl und $a \in \mathbb{Z}$ mit $p \not| \, a$. Dann gilt

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s(a) = (-1)^\alpha \, ,$$

wobei α die Anzahl der Zahlen unter $\{a, 2a, 3a, \ldots, \frac{1}{2}(p-1) \cdot a\}$ ist, die modulo p einen negativen absolut kleinsten Rest haben.

Carl Friedrich Gauß (1777–1855), deutscher Mathematiker

(13.16) KOROLLAR: Sei $p > 2$. Dann gilt:

a) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

b) 2 ist genau dann QR mod p, wenn $p \equiv 1 \pmod 8$ oder $p \equiv 7 \pmod 8$ gilt.

c) 2 ist genau dann QNR mod p, wenn $p \equiv 3 \pmod 8$ oder $p \equiv 5 \pmod 8$ gilt.

(13.17) Quadratisches Reziprozitätsgesetz für das Legendre–Symbol

Für verschiedene ungerade Primzahlen p und q gilt

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

Dieses Ergebnis wurde 1785 von Legendre vermutet, aber noch nicht vollständig bewiesen. Ein erster Beweis dafür wurde von Gauß erbracht (1801), der insgesamt 8 verschiedene Beweise gefunden hat. Insgesamt gibt es mehr als 100 Beweise für diesen Satz.

(13.18) BEM: Stellt man $a \in \mathbb{Z} \setminus \{0\}$ in der Form

$$a = (-1)^k 2^l p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

dar mit $k \in \{0, 1\}, l \geq 0, r \geq 0, k_i \geq 1$, wobei $p_1, \ldots, p_r$ paarweise verschiedene ungerade Primzahlen sind, so gilt für eine ungerade Primzahl p mit $p \not| \, a$

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^k \cdot \left(\frac{2}{p}\right)^l \cdot \left(\frac{p_1}{p}\right)^{k_1} \cdot \ldots \cdot \left(\frac{p_r}{p}\right)^{k_r} \, .$$

Die Legendre–Symbole $\left(\frac{p_i}{p}\right)$ lassen sich häufig mit (13.17) vereinfachen und berechnen.

Das **Jacobi–Symbol** ist eine Verallgemeinerung des Legendre–Symbols.
Carl Gustav Jacob Jacobi (1804–1851), deutscher Mathematiker

(13.19) DEF: Seien $a, b \in \mathbb{Z}$ teilerfremde Zahlen, wobei $b \geq 3$ ungerade ist. Besitzt dann b die Primfaktorzerlegung $b = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ mit paarweise verschiedenen (ungeraden) Primzahlen $p_1, p_2, \ldots, p_r$ und Exponenten $k_i \geq 0$, so ist das **Jacobi–Symbol** $\left(\frac{a}{b}\right)$ definiert durch

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{k_i} .$$

Hierbei ist $\left(\frac{a}{p_i}\right)$ das "normale" Legendre–Symbol.

Beispiel: $\left(\frac{6}{245}\right) = \left(\frac{6}{5}\right) \cdot \left(\frac{6}{7}\right)^2 = \left(\frac{6}{5}\right) = \left(\frac{1}{5}\right) = 1$

(19.20) BEM: a) Da b ungerade ist, sind auch alle Primfaktoren p_i von b ungerade und teilen a nicht wegen $\mathrm{ggT}(a, b) = 1$. Folglich ist $\left(\frac{a}{p_i}\right)$ definiert. Ist $b = p$ eine ungerade Primzahl, so erhalten wir die alte Definition des Legendre–Symbols.

b) Es gilt $\left(\frac{a}{b}\right) \in \{+1, -1\}$

c) $\left(\frac{a}{b}\right) = -1 \implies a$ ist QNR modulo b

d) Aus $\left(\frac{a}{b}\right) = 1$ läßt sich aber i.a. nicht schließen, daß a QR modulo b ist.

Gegenbeispiel: $\left(\frac{2}{15}\right) = 1$, aber 2 ist QNR modulo 15, da 2 QNR modulo 3 ist.

(13.21) Rechenregeln für das Jacobi–Symbol

Seien $a, a', b, b', c \in \mathbb{Z}$, wobei $b \geq 3$ und $b' \geq 3$ beide ungerade sind. Dann gilt:

a) Aus $a \equiv a' \pmod{b}$ und $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, b') = 1$ folgt $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$

b) Aus $\mathrm{ggT}(aa', b) = 1$ folgt $\left(\frac{a \cdot a'}{b}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a'}{b}\right)$

c) Aus $\mathrm{ggT}(a, bb') = 1$ folgt $\left(\frac{a}{b \cdot b'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$

d) Aus $\mathrm{ggT}(ac, b) = 1$ folgt $\left(\frac{a \cdot c^2}{b}\right) = \left(\frac{a}{b}\right)$

e) Aus $\mathrm{ggT}(a, bc) = 1$ folgt $\left(\frac{a}{b \cdot c^2}\right) = \left(\frac{a}{b}\right)$

(13.22) HILFSSATZ: Für ungerade Zahlen $u, v \in \mathbb{Z}$ gilt:

a) $\dfrac{u-1}{2} + \dfrac{v-1}{2} \equiv \dfrac{uv-1}{2} \pmod 2$

b) $\dfrac{u^2-1}{8} + \dfrac{v^2-1}{8} \equiv \dfrac{(uv)^2-1}{8} \pmod 8$

(13.23) LEMMA: Für jede ungerade ganze Zahl $b \geq 3$ gilt $\left(\dfrac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

(13.24) LEMMA: Für jede ungerade ganze Zahl $b \geq 3$ gilt $\left(\dfrac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.

(13.25) Quadratisches Reziprozitätsgesetz für das Jacobi–Symbol

Für ungerade teilerfremde Zahlen a und b, die beide ≥ 3 sind, gilt:

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