IV Quadratische Reste

10 Quadratische Reste

(10.1) Die Theorie der quadratischen Reste, die in diesem Paragraphen beginnt, ist ein Spezialfall der in § 6 dargestellten Theorie der Potenzreste.

(10.2) Definition: Es sei m eine natürliche Zahl.
(1) $a \in \mathbb{Z}$ heißt ein quadratischer Rest modulo m, wenn a ein zweiter Potenzrest modulo m ist, also wenn a und m teilerfremd sind und es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{m}$ gibt.
(2) $a \in \mathbb{Z}$ heißt ein quadratischer Nichtrest modulo m, wenn a und m teilerfremd sind und für jedes $x \in \mathbb{Z}$ gilt: Es ist $x^2 \not\equiv a \pmod{m}$.

(10.3) Bemerkung: Es sei $m \in \mathbb{N}$, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m; es sei $a \in \mathbb{Z}$. Nach (6.14) ist a genau dann ein quadratischer Rest modulo m, wenn a für jedes $i \in \{1, 2, \ldots, r\}$ ein quadratischer Rest modulo $p_i^{\alpha_i}$ ist; für die Anzahl $N_2(a, m)$ der Lösungen $x \in \{0, 1, \ldots, m-1\}$ von $X^2 \equiv a \pmod{m}$ gilt $N_2(a, m) = N_2(a, p_1^{\alpha_1}) N_2(a, p_2^{\alpha_2}) \cdots N_2(a, p_r^{\alpha_r})$. Der Beweis in (6.3) zeigt, daß man eine Lösung $x \in \{0, 1, \ldots, m-1\}$ der Kongruenz $X^2 \equiv a \pmod{m}$ folgendermaßen erhält, wenn man für jedes $i \in \{1, 2, \ldots, r\}$ eine Lösung $x_i \in \mathbb{Z}$ von $X^2 \equiv a \pmod{p_i^{\alpha_i}}$ kennt: Man berechnet nach dem Chinesische Restsatz (vgl. (4.14)) das $x \in \{0, 1, \ldots, m-1\}$ mit $x \equiv x_i \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1, 2, \ldots, r\}$. Wie der Beweis in (6.3) zeigt, erhält man auf diese Weise alle Lösungen von $X^2 \equiv a \pmod{m}$, wenn man für jedes $i \in \{1, 2, \ldots, r\}$ alle Lösungen von $X^2 \equiv a \pmod{p_i^{\alpha_i}}$ kennt.

(10.4) Bemerkung: Es sei p eine ungerade Primzahl, und es sei $\alpha \in \mathbb{N}$.
(1) Eine ganze Zahl a ist genau dann ein quadratischer Rest modulo p^α, wenn gilt: Es ist

$$a^{p^{\alpha-1}(p-1)/2} \equiv 1 \pmod{p^\alpha}.$$

(2) Wenn $a \in \mathbb{Z}$ ein quadratischer Rest modulo p^α ist, so hat die Kongruenz $X^2 \equiv a \pmod{p^\alpha}$ genau zwei Lösungen $x_1, x_2 \in \{0, 1, \ldots, p^\alpha - 1\}$, und damit gilt

$$\{x \in \mathbb{Z} \mid x^2 \equiv a \pmod{p^\alpha}\} = \\ = \{x \in \mathbb{Z} \mid x \equiv x_1 \pmod{p^\alpha} \text{ oder } x \equiv x_2 \pmod{p^\alpha}\}.$$

(3) In der Menge $\{0, 1, \ldots, p^\alpha - 1\}$ gibt es $\varphi(p^\alpha)/2 = p^{\alpha-1}(p-1)/2$ quadratische Reste und ebensoviele quadratische Nichtreste modulo p^α.
Beweis: Es ist $\mathrm{ggT}(2, \varphi(p^\alpha)) = 2$, und daher folgen alle drei Aussagen aus dem Satz in (6.16).

(10.5) Bemerkung: Es sei p eine ungerade Primzahl.
(1) Aus (6.16)(1) ergibt sich das Kriterium von Euler: $a \in \mathbb{Z} \setminus p\mathbb{Z}$ ist genau dann ein quadratischer Rest modulo p, wenn $a^{(p-1)/2} \equiv 1 \pmod{p}$ gilt, und genau dann ein quadratischer Nichtrest modulo p, wenn $a^{(p-1)/2} \equiv -1 \pmod{p}$ gilt.
(2) Die $\varphi(p)/2 = (p-1)/2$ quadratischen Reste modulo p in $\{0, 1, \ldots, p-1\}$ sind die Zahlen $k^2 \bmod p$ mit $k \in \{1, 2, \ldots, (p-1)/2\}$.
Beweis: Daß (2) gilt, ist klar, und (1) folgt so: Für jedes $a \in \mathbb{Z} \setminus p\mathbb{Z}$ gilt im Körper $\mathbb{F}_p$

$$[0]_p = [a]_p^{p-1} - [1]_p = \left([a]_p^{(p-1)/2} - [1]_p\right) \cdot \left([a]_p^{(p-1)/2} + [1]_p\right)$$

(vgl. (4.21)), also $[a]_p^{(p-1)/2} = [1]_p$ oder $[a]_p^{(p-1)/2} = -[1]_p$, und somit gilt $a^{(p-1)/2} \equiv 1 \pmod{p}$ oder $a^{(p-1)/2} \equiv -1 \pmod{p}$. Die Behauptung folgt daher aus (10.4)(1).

(10.6) Satz: *Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Folgende Aussagen sind äquivalent:*
(1) *a ist ein quadratischer Rest modulo p.*
(2) *Es gibt ein $\alpha \in \mathbb{N}$ mit: a ist ein quadratischer Rest modulo p^α.*
(3) *Für jedes $\alpha \in \mathbb{N}$ ist a ein quadratischer Rest modulo p^α.*

Beweis: Man vergleiche (6.19).

(10.7) Bemerkung: Es sei p eine ungerade Primzahl, es sei α eine natürliche Zahl mit $\alpha \geq 2$, und es sei $a \in \mathbb{Z}$ ein quadratischer Rest modulo p^α. Nach (10.4)(2) hat die Kongruenz $X^2 \equiv a \pmod{p^\alpha}$ zwei verschiedene Lösungen $x_1, x_2 \in \{0, 1, \ldots, p^\alpha - 1\}$. Wegen $(-x_1)^2 = x_1^2 \equiv a \pmod{p^\alpha}$ und $-x_1 \not\equiv x_1 \pmod{p^\alpha}$ ist $x_2 \equiv -x_1 \pmod{p^\alpha}$. Man kann also alle Lösungen von $X^2 \equiv a \pmod{p^\alpha}$ angeben, wenn man eine kennt. Da a auch ein quadratischer Rest modulo $p^{\alpha-1}$ ist, gibt es ein $y \in \mathbb{Z}$ mit $y^2 \equiv a \pmod{p^{\alpha-1}}$, und das Rechenverfahren aus dem Beweis von (6.5)(1) liefert, angewandt auf das Polynom $f := X^2 - a \in \mathbb{Z}[X]$, zu y ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{p^\alpha}$: Man ermittelt ein $v \in \mathbb{Z}$ mit

$$2y \cdot v = f'(y) \cdot v \equiv -\frac{f(y)}{p^{\alpha-1}} = -\frac{y^2 - a}{p^{\alpha-1}} \pmod{p}$$

und setzt $x := y + vp^{\alpha-1}$.

Man kann also alle Lösungen von $X^2 \equiv a \pmod{p^\alpha}$ finden, wenn man eine Lösung der Kongruenz $X^2 \equiv a \pmod{p}$ kennt oder, was auf dasselbe herauskommt, eine Nullstelle des Polynoms $X^2 - [a]_p \in \mathbb{F}_p[X]$. Eine solche Nullstelle kann man dadurch finden, daß man die Primzerlegung von $X^2 - [a]_p$ im Polynomring $\mathbb{F}_p[X]$ mit Hilfe eines Faktorisierungsalgorithmus berechnet. In MuPAD verwendet man dazu die Funktion `factor` (vgl. (6.7)). Es gibt spezielle Algorithmen zur Berechnung einer Lösung von $X^2 \equiv a \pmod{p}$. Ein solcher Algorithmus wird in (12.5) behandelt werden.

(10.8) Bemerkung: (1) $a \in \mathbb{Z}$ ist dann und nur dann ein quadratischer Rest modulo 2, wenn a ungerade ist; ist dies der Fall, so hat die Kongruenz $X^2 \equiv a \pmod{2}$ in $\{0,1\}$ die eine Lösung $x = 1$.
(2) $a \in \mathbb{Z}$ ist dann und nur dann ein quadratischer Rest modulo 4, wenn $a \equiv 1 \pmod{4}$ gilt; ist dies der Fall, so hat die Kongruenz $X^2 \equiv a \pmod{4}$ in $\{0,1,2,3\}$ die zwei Lösungen $x = 1$ und $x = 3$.

(10.9) Satz: *Es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 3$.*
(1) *$a \in \mathbb{Z}$ ist dann und nur dann ein quadratischer Rest modulo 2^α, wenn $a \equiv 1 \pmod{8}$ gilt; ist dies der Fall, so hat die Kongruenz $X^2 \equiv a \pmod{2^\alpha}$ in der Menge $\{0,1,\ldots,2^\alpha - 1\}$ genau 4 verschiedene Lösungen.*
(2) *In der Menge $\{0,1,\ldots,2^\alpha - 1\}$ gibt es genau $2^{\alpha-3}$ quadratische Reste und $3 \cdot 2^{\alpha-3}$ quadratische Nichtreste modulo 2^α.*

Beweis: (1) Es sei $a \in \mathbb{Z}$ ungerade.
(a) Aus (6.18)(3) folgt: a ist genau dann ein quadratischer Rest modulo 2^α, wenn $a \equiv 1 \pmod{8}$ ist.
(b) Es gelte: a ist ein quadratischer Rest modulo 2^α. Dann ist a ungerade, und nach (5.19)(2) existieren eindeutig bestimmte Zahlen $i \in \{0,1\}$ und $j \in \{0,1,\ldots,2^{\alpha-2}-1\}$ mit $a \equiv (-1)^i 5^j \pmod{2^\alpha}$. Es gilt

$$a \equiv (-1)^i 5^j \equiv \begin{cases} 1 \pmod 8, & \text{falls } i = 0 \text{ und } j \text{ gerade ist,} \\ 7 \pmod 8, & \text{falls } i = 1 \text{ und } j \text{ gerade ist,} \\ 5 \pmod 8, & \text{falls } i = 0 \text{ und } j \text{ ungerade ist,} \\ 3 \pmod 8, & \text{falls } i = 1 \text{ und } j \text{ ungerade ist.} \end{cases}$$

Wegen $a \equiv 1 \pmod{8}$ gilt daher: Es ist $i = 0$, und j ist gerade. Es sei $x \in \mathbb{Z}$ ungerade, und es seien $k \in \{0,1\}$ und $l \in \{0,1,\ldots,2^{\alpha-2}-1\}$ die Zahlen mit $x \equiv (-1)^k 5^l \pmod{2^\alpha}$. Es gilt $x^2 \equiv a \pmod{2^\alpha}$, genau wenn $5^{2l} \equiv 5^j \pmod{2^\alpha}$ gilt, also genau wenn $2l \equiv j \pmod{2^{\alpha-2}}$ gilt (denn nach (5.19)(1) ist $\operatorname{ord}([5]_{2^\alpha}) = 2^{\alpha-2}$), also genau wenn $l = j/2$ oder $l = j/2 + 2^{\alpha-3}$ gilt. Die Kongruenz $X^2 \equiv a \pmod{2^\alpha}$ hat also in $\{0,1,\ldots,2^{\alpha-1}\}$ die vier verschiedenen Lösungen

$$5^{j/2} \bmod 2^\alpha,\ (-5^{j/2}) \bmod 2^\alpha,\ 5^{j/2} \cdot 5^{2^{\alpha-3}} \bmod 2^\alpha \text{ und } (-5^{j/2} \cdot 5^{2^{\alpha-3}}) \bmod 2^\alpha.$$

(2) Die Überlegung in (1)(b) zeigt: In der Menge $\{0,1,\ldots,2^\alpha-1\}$ gibt es $2^{\alpha-3}$ quadratische Reste modulo 2^α und $3\cdot 2^{\alpha-3}$ quadratische Nichtreste modulo 2^α; die quadratischen Reste sind die $2^{\alpha-3}$ Zahlen $5^k \bmod 2^\alpha$ mit $k \in \{0,1,\ldots,2^{\alpha-3}-1\}$, die quadratischen Nichtreste sind die übrigen ungeraden Zahlen in dieser Menge.

(10.10) Bemerkung: (1) Es sei $a \in \mathbb{Z}$ mit $a \equiv 1 \pmod 8$, und es sei $v \in \mathbb{Z}$ eine Lösung der Kongruenz $X^2 \equiv a \pmod 8$. Zu jedem $\alpha \in \mathbb{Z}$ mit $\alpha \geq 3$ gibt es eine Lösung $y_\alpha \in \{0,1,\ldots,2^\alpha-1\}$ von $X^2 \equiv a \pmod{2^\alpha}$ mit $y_\alpha \equiv v \pmod 4$. Beweis: Für $\alpha = 3$ ist nicht zu beweisen. Ist $\alpha \geq 4$ und ist bereits eine Zahl $y_{\alpha-1} \in \{0,1,\ldots,2^{\alpha-1}-1\}$ mit $y_{\alpha-1}^2 \equiv a \pmod{2^{\alpha-1}}$ gefunden, so setzt man

$$t_\alpha := \left(\frac{y_{\alpha-1}^2 - a}{2^{\alpha-1}}\right) \bmod 2 \quad \text{und} \quad y_\alpha := y_{\alpha-1} + 2^{\alpha-2}t_\alpha$$

und erhält $0 \leq y_\alpha \leq 2^\alpha - 1$ und $y_\alpha \equiv y_{\alpha-1} \equiv v \pmod 4$ und

$$y_\alpha^2 = y_{\alpha-1}^2 + 2^{\alpha-1}t_\alpha y_{\alpha-1} + 2^{2\alpha-4}t_\alpha^2 \equiv a + 2^{\alpha-1}t_\alpha(1+y_{\alpha-1}) \equiv a \pmod{2^\alpha},$$

da $y_{\alpha-1}$ ungerade ist.
(2) Es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 3$, und es sei $a \in \mathbb{Z}$ ein quadratischer Rest modulo 2^α, d.h. es gelte $a \equiv 1 \pmod 8$. Der Beweis in (1) liefert ein Verfahren, Lösungen $x_1, x_2 \in \{0,1,\ldots,2^\alpha-1\}$ der Kongruenz $X^2 \equiv a \pmod{2^\alpha}$ mit $x_1 \equiv 1 \pmod 4$ und $x_2 \equiv 3 \pmod 4$ zu berechnen. Wie man sieht, sind x_1, x_2, $(-x_1) \bmod 2^\alpha$ und $(-x_2) \bmod 2^\alpha$ die vier Lösungen der Kongruenz $X^2 \equiv a \pmod{2^\alpha}$ in $\{0,1,\ldots,p^\alpha-1\}$.

(10.11) Bemerkung: Aus (10.3), (10.7), (10.8) und (10.10) ergibt sich: Man kann für jedes $m \in \mathbb{N}$ und jeden quadratischen Rest a modulo m alle Lösungen der Kongruenz $X^2 \equiv a \pmod m$ berechnen, wenn man für jede ungerade Primzahl p und jeden quadratischen Rest a modulo p eine Lösung der Kongruenz $X^2 \equiv a \pmod p$, also im Körper $\mathbb{F}_p$ eine Quadratwurzel aus $[a]_p$ berechnen kann. Ein Algorithmus, der dieses leistet und nicht die Primzerlegung des Polynoms $X^2 - [a]_p$ im Polynomring $\mathbb{F}_p[X]$ verwendet, wird in (12.5) behandelt werden. – Aus (10.3), (10.7) und (10.9) ergibt sich noch der folgenden Satz, der zu einem $m \in \mathbb{N}$ und einem quadratischen Rest a modulo m die Anzahl der Lösungen $x \in \{0,1,\ldots,m-1\}$ der Kongruenz $X^2 \equiv a \pmod m$ liefert.

(10.12) Satz: *Es sei $m \in \mathbb{N}$, und es sei s die Anzahl der ungeraden Primteiler von m; es sei $a \in \mathbb{Z}$.*
(1) *a ist genau dann ein quadratischer Rest modulo m, wenn a für jeden ungeraden Primteiler p von m ein quadratischer Rest modulo p ist und wenn gilt:*

Ist $v_2(m) = 1$, *so ist* $a \equiv 1 \pmod 2$, *ist* $v_2(m) = 2$, *so ist* $a \equiv 1 \pmod 4$, *und ist* $v_2(m) \geq 3$, *so ist* $a \equiv 1 \pmod 8$.
(2) *Ist* a *ein quadratischer Rest modulo* m, *so gilt für die Anzahl* $N_2(a,m)$ *der Lösungen* $x \in \{0, 1, \ldots, m-1\}$ *der Kongruenz* $X^2 \equiv a \pmod m$: *Es ist*

$$N_2(a,m) = \begin{cases} 2^s, & \text{falls } v_2(m) \leq 1 \text{ ist,} \\ 2^{s+1}, & \text{falls } v_2(m) = 2 \text{ ist,} \\ 2^{s+2}, & \text{falls } v_2(m) \geq 3 \text{ ist.} \end{cases}$$

11 Legendre-Symbol und Jacobi-Symbol

(11.1) Die in dieses Paragraphen behandelte Theorie des Legendre-Symbols und des Jacobi-Symbols gehört seit Gauß zu den Höhepunkten der Elementaren Zahlentheorie. Das Kriterium von Euler (vgl. (10.5)(1)) erlaubt es zu entscheiden, ob eine ganze Zahl a ein quadratischer Rest modulo einer ungeraden Primzahl p ist. In den folgenden Abschnitten wird gezeigt, wie man diese Entscheidung auf ganz andere Weise treffen kann.

(11.2) Definition: Es sei p eine ungerade Primzahl. Für $a \in \mathbb{Z}$ setzt man

$$(a \mid p) = \left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1, & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0, & \text{falls } a \text{ durch } p \text{ teilbar ist,} \end{cases}$$

und liest dies als "a über p". Die Abbildung

$$a \mapsto \left(\frac{a}{p}\right) : \mathbb{Z} \to \mathbb{C}$$

heißt das Legendre-Symbol modulo p (nach A. M. Legendre, 1752 – 1833).

(11.3) Satz: *Es sei* p *eine ungerade Primzahl. Für jedes* $a \in \mathbb{Z}$ *gilt*

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

Beweis: Für jedes $a \in p\mathbb{Z}$ gilt $(a \mid p) = 0 \equiv a^{(p-1)/2} \pmod p$, und aus (10.5)(1) folgt für jedes $a \in \mathbb{Z} \setminus p\mathbb{Z}$: Es ist $(a \mid p) \equiv a^{(p-1)/2} \pmod p$.

(11.4) Satz: *Es sei* p *eine ungerade Primzahl.*
(1) *Für* $a, b \in \mathbb{Z}$ *mit* $a \equiv b \pmod p$ *gilt*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$