8. Quadratische Reste. Reziprozitätsgesetz

8.1. Definition. Sei m eine natürliche Zahl $\geqslant 2$. Eine ganze Zahl a heißt *quadratischer Rest* modulo m (Abkürzung QR), falls die Kongruenz

$$x^2 \equiv a \bmod m$$

eine Lösung $x \in \mathbb{Z}$ besitzt. Andernfalls heißt a *quadratischer Nichtrest* modulo m (Abkürzung NR).

Dies lässt sich auch so ausdrücken: a ist genau dann quadratischer Rest modulo m, wenn die Klasse von a im Ring $\mathbb{Z}/m$ ein Quadrat ist. Wegen des Chinesischen Restsatzes kann man den allgemeinen Fall darauf zurückführen, dass der Modul m eine Primzahlpotenz ist, $m = p^k$. Wir beschäftigen uns in dieser Vorlesung hauptsächlich mit dem Fall $k = 1$, d.h. quadratischen Resten modulo einer Primzahl p. Der Fall $p = 2$ ist trivial (jede ganze Zahl ist Quadrat modulo 2). Sei daher jetzt p eine ungerade Primzahl. Die Frage nach den quadratischen Resten modulo p ist dann gleichbedeutend mit der Frage nach den Quadraten im Körper $\mathbb{Z}/p$. Da 0 stets ein Quadrat ist, kann man sich auf $(\mathbb{Z}/p)^*$ beschränken.

Betrachten wir zunächst ein Beispiel $p = 11$.

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

mod 11

Es sind also die Restklassen von 1,3,4,5,9 Quadrate in $(\mathbb{Z}/11)^*$, die Restklassen von 2,6,7,8,11 sind Nicht-Quadrate. Es sind also genau die Hälfte der Elemente von $(\mathbb{Z}/11)^*$ Quadrate. Wir werden sehen, dass dies auch für beliebige ungerade Primzahlen p gilt.

Dies gilt nicht mehr für zusammengesetzte Moduln. Z.B. haben wir für für $m = 15$ folgende Quadrate-Tafel für $(\mathbb{Z}/15)^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

x	1	2	4	7	8	11	13	14
x^2	1	4	1	4	4	1	4	1

mod 15

Hier gibt es also nur zwei Quadrate. Dies lässt sich so erklären: Nach dem Chinesischen Restsatz gilt $(\mathbb{Z}/15)^* \cong (\mathbb{Z}/3)^* \times (\mathbb{Z}/5)^*$. In $(\mathbb{Z}/3)^*$ gibt es nur ein Quadrat und in $(\mathbb{Z}/5)^*$ zwei Quadrate, also im Produkt auch nur zwei Quadrate.

8.2. Definition (Legendre-Symbol). Sei $a \in \mathbb{Z}$ und p eine ungerade Primzahl. Dann wird das *Legendre-Symbol* $(\frac{a}{p})$ wie folgt definiert:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{falls } p \mid a, \\ +1, & \text{falls } p \nmid a \text{ und } a \text{ ist QR mod } p, \\ -1, & \text{falls } p \nmid a \text{ und } a \text{ ist NR mod } p. \end{cases}$$

Kap. 8 zuletzt geändert am: 2008-07-08

Die Gleichung $x^2 \equiv a \bmod p$ ist also genau dann lösbar, wenn $(\frac{a}{p}) \geqslant 0$. Offenbar gilt

$$a \equiv b \bmod p \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

8.3. Satz (Euler-Kriterium). *Sei p eine ungerade Primzahl. Dann gilt für jede ganze Zahl a*

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

Beweis. Falls $p \mid a$, sind beide Seiten $\equiv 0 \bmod p$. Wir können also im folgenden voraussetzen, dass $p \nmid a$.

1. Fall: a ist quadratischer Rest modulo p. Dann gibt es eine ganze Zahl b mit $a \equiv b^2 \bmod p$. Natürlich gilt auch $p \nmid b$. Daher folgt aus dem kleinen Satz von Fermat

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

2. Fall: a ist quadratischer Nichtrest. Sei g eine Primitivwurzel modulo p. Dann ist $a \equiv g^m$ mit einer ungeraden Zahl $m = 2k+1$. Damit folgt

$$a^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \equiv g^{k(p-1)}g^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{b}\right) \bmod p.$$

Bemerkung. Wegen des schnellen Potenzierungs-Algorithmus liefert Satz 8.3 eine effiziente Methode, das Legendre-Symbol zu berechnen. Wir werden aber später sehen, dass man mittels des quadratischen Reziprozitätsgesetzes das Legendre-Symbol noch schneller berechnen kann.

8.4. Corollar. *Für jede ungerade Primzahl p und alle ganzen Zahlen a, b gilt*

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

Aus der Multiplikativität des Legendre-Symbols folgt z.B. dass das Produkt zweier quadratischer Nichtreste ein quadratischer Rest ist.

Das Corollar bedeutet, dass die Abbildung

$$\left(\frac{-}{p}\right) : (\mathbb{Z}/p)^* \longrightarrow \{\pm 1\}, \quad x \mapsto \left(\frac{x}{p}\right)$$

ein Gruppen-Homomorphismus ist. Dieser Homomorphismus ist surjektiv, da eine Primitivwurzel g modulo p sicher ein quadratischer Nichtrest ist. Der Kern dieser Abbildung ist die Menge der Quadrate in $(\mathbb{Z}/p)^*$. Dies ist eine Untergruppe vom Index 2. Es gibt also ebenso viele Quadrate wie Nichtquadrate in $(\mathbb{Z}/p)^*$.

8.5. Quadratisches Reziprozitätsgesetz

Das quadratische Reziprozitätsgesetz macht eine Aussage darüber, wie sich die Legendresymbole $(\frac{p}{q})$ und $(\frac{q}{p})$ zueinander verhalten, wobei $p \neq q$ zwei ungerade Primzahlen sind. Es stellt sich heraus, dass beide Symbole denselben Wert haben, falls wenigstens eine der beiden Primzahlen $\equiv 1 \bmod 4$ ist; dagegen sind die Symbole entgegengesetzt gleich, falls $p \equiv q \equiv 3 \bmod 4$. Das Reziprozitätsgesetz wurde zuerst von Gauß bewiesen, nachdem sich vorher schon u.a. Legendre und Euler vergeblich darum bemüht hatten. Gauß selbst hat 8 Beweise gegeben und bis heute wurden rund 200 Beweise veröffentlicht, wenn auch die meisten nur Varianten von vorherigen sind. Wir bringen hier einen elementaren, auf Gauß zurückgehenden Beweis. Dazu brauchen wir einige Vorbereitungen.

Sei p eine ungerade Primzahl. Wir bezeichnen mit $H(p)$ das 'Halbsystem' modulo p,

$$H(p) := \Big\{1, 2, \ldots, \frac{p-1}{2}\Big\}.$$

Für jede ganze Zahl n, die nicht durch p teilbar ist, lässt sich ihre Restklasse modulo p eindeutig schreiben als

$$n \equiv \varepsilon \cdot u \bmod p \quad \text{mit } \varepsilon \in \{\pm 1\} \text{ und } u \in H(p).$$

Man nennt εu den *absolut kleinsten Rest* von n modulo p.

Sei nun eine Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ vorgegeben. Für $x \in H(p)$ definieren definieren wir $\varepsilon_a(x) \in \{\pm 1\}$ und $\sigma_a(x) \in H(p)$ durch die Bedingung

$$ax \equiv \varepsilon_a(x)\sigma_a(x) \bmod p.$$

Es ist leicht zu sehen, dass die Abbildung $\sigma_a : H(p) \to H(p)$ bijektiv, d.h. eine Permutation von $H(p)$ ist.

8.6. Satz (Gaußsches Lemma). *Sei p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Dann gilt*

$$\Big(\frac{a}{p}\Big) = \prod_{x \in H(p)} \varepsilon_a(x).$$

Dies ist äquivalent mit folgender Aussage: Sei m die Anzahl der Elemente von

$$\Big\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\Big\},$$

deren absolut kleinster Rest modulo p negativ ist. Dann ist $(\frac{a}{p}) = 1$, wenn m gerade, und $(\frac{a}{p}) = -1$, wenn m ungerade ist.

Beweis. Es gilt

$$\prod_{x \in H(p)} (ax) \equiv \prod_{x \in H(p)} \varepsilon_a(x) \prod_{x \in H(p)} \sigma_a(x) \equiv \prod_{x \in H(p)} \varepsilon_a(x) \prod_{x \in H(p)} x,$$

denn durchläuft x alle Elemente von $H(p)$, so durchläuft auch $\sigma_a(x)$ alle Elemente von $H(p)$. Andrerseits ist

$$\prod_{x \in H(p)} (ax) = a^{(p-1)/2} \prod_{x \in H(p)} x,$$

also folgt mit dem Euler-Kriterium

$$\prod_{x \in H(p)} \varepsilon_a(x) \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right), \quad \text{q.e.d.}$$

Beispiel. Sei $p = 7$. Dann ist $H(p) = \{1, 2, 3\}$. Für $a = 2$ haben wir

$$2 \cdot 1 = 2, \quad 2 \cdot 2 = 4 \equiv -3, \quad 2 \cdot 3 = 6 \equiv -1,$$

also $\varepsilon_2(1) = 1$, $\varepsilon_2(2) = -1$, $\varepsilon_2(3) = -1$, woraus folgt $(\frac{2}{7}) = 1$, d.h. 2 ist quadratischer Rest modulo 7. In der Tat ist $3^2 \equiv 2 \bmod 7$.

Für die Anwendung des Gaußschen Lemmas ist eine Umformulierung nützlich. Sei weiter p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Für $\nu = 1, \ldots, a$ betrachten wir die Intervalle

$$I_\nu := \left\{ x \in \mathbb{R} : (\nu - 1) \frac{p}{2} < x < \nu \frac{p}{2} \right\}.$$

Offenbar ist für $k \in H(p) = \{1, \ldots, (p-1)/2\}$ der absolut kleinste Rest von ka modulo p genau dann negativ, d.h. $\varepsilon_a(k) = -1$, wenn ka in einem Intervall I_ν mit geradem Index ν liegt. Wir bezeichnen mit r_ν die Anzahl der ka, $k \in H$, die in I_ν liegen. Da kein ka auf einem Randpunkt eines der I_ν liegt, folgt

$$r_\nu = \left\lfloor \nu \frac{p}{2a} \right\rfloor - \left\lfloor (\nu - 1) \frac{p}{2a} \right\rfloor,$$

wobei $\lfloor x \rfloor$ für eine reelle Zahl x die größte ganze Zahl $\leqslant x$ bezeichnet. Nach dem Gaußschen Lemma ist $(\frac{a}{p}) = (-1)^m$ mit

$$m = \sum_{0 < 2\nu \leqslant a} r_{2\nu}.$$

Somit folgt

8.7. Corollar. *Sei p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Dann gilt*

$$\left(\frac{a}{p}\right) = (-1)^m \quad \text{mit} \quad m = \sum_{k=1}^{\lfloor a/2 \rfloor} \left(\left\lfloor k \frac{p}{a} \right\rfloor - \left\lfloor (k - \tfrac{1}{2}) \frac{p}{a} \right\rfloor \right).$$

Als erste Anwendung beweisen wir die sog. Ergänzungssätze zum Reziprozitätsgesetz.

8.8. Satz. *Sei p eine ungerade Primzahl. Dann gilt:*

i) (1. Ergänzungssatz)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \textit{für } p \equiv 1 \bmod 4, \\ -1 & \textit{für } p \equiv 3 \bmod 4. \end{cases}$$

ii) (2. Ergänzungssatz)

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

Beweis. i) Dies folgt aus dem Gaußschen Lemma, da $\varepsilon_{-1}(x) = -1$ für alle $x \in H(p)$. Die Behauptung ist aber auch eine direkte Anwendung des Euler-Kriteriums 8.3.

ii) Für $a = 2$ ergibt die Formel des Corollars 8.7

$$\left(\frac{2}{p}\right) = (-1)^m \quad \text{mit} \quad m = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor.$$

Wir werten dies durch Fallunterscheidung aus

p	$\lfloor p/2 \rfloor$	$\lfloor p/4 \rfloor$	m	$(-1)^m$
$8k+1$	$4k$	$2k$	$2k$	$+1$
$8k-1$	$4k-1$	$2k-1$	$2k$	$+1$
$8k+3$	$4k+1$	$2k$	$2k+1$	-1
$8k-3$	$4k-2$	$2k-1$	$2k-1$	-1

Daraus folgt die Behauptung.

8.9. Satz. *Sei p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Sei q eine weitere Primzahl mit $q \equiv \pm p \bmod 4a$. Dann folgt*

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

Beweis. Nach dem Corollar 8.7 gilt $(\frac{a}{p}) = (-1)^m$ mit

$$m = \sum_{\nu=1}^{\lfloor a/2 \rfloor} (s_{2\nu} - s_{2\nu-1}), \quad \text{wobei} \quad s_k = \left\lfloor k\frac{p}{2a} \right\rfloor$$

und entsprechend $(\frac{a}{q}) = (-1)^{m'}$ mit

$$m' = \sum_{\nu=1}^{\lfloor a/2 \rfloor} (s'_{2\nu} - s'_{2\nu-1}), \quad \text{wobei} \quad s'_k = \left\lfloor k\frac{q}{2a} \right\rfloor.$$

i) Wir behandeln zunächst den Fall $q \equiv p \bmod 4a$. Dann ist $q = p + 4at$ mit einer ganzen Zahl t. Es folgt

$$s'_k = \left\lfloor k\,\frac{p+4at}{2a} \right\rfloor = \left\lfloor k\frac{p}{2a} + 2kt \right\rfloor = \left\lfloor k\frac{p}{2a} \right\rfloor + 2kt = s_k + 2kt.$$

Also gilt $m' \equiv m \bmod 2$, woraus die Behauptung folgt.

ii) Sei jetzt $q \equiv -p \bmod 4a$, d.h. $q = 4at - p$ mit einer ganzen Zahl t. Dann ist

$$s'_k + s_k = \left\lfloor k\,\frac{4at-p}{2a} \right\rfloor + \left\lfloor k\frac{p}{2a} \right\rfloor = 2kt + \left\lfloor -k\frac{p}{2a} \right\rfloor + \left\lfloor k\frac{p}{2a} \right\rfloor = 2kt - 1$$

für $1 \leqslant k \leqslant a$, da dann $\frac{kp}{2a}$ keine ganze Zahl ist. Es folgt

$$(s'_{2\nu} - s'_{2\nu-1}) + (s_{2\nu} - s_{2\nu-1}) \equiv 0 \bmod 2 \quad \text{für } 1 \leqslant \nu \leqslant \lfloor a/2 \rfloor,$$

also $m' \equiv m \bmod 2$, q.e.d.

8.10. Satz (Quadratisches Reziprozitätsgesetz). *Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt*

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

Dies lässt sich auch so aussprechen: Ist wenigstens eine der Primzahlen $\equiv 1 \bmod 4$, so gilt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$; falls aber $p \equiv q \equiv 3 \bmod 4$, so folgt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Beweis. i) Wir behandeln zuerst den Fall $p \equiv q \bmod 4$. Dann ist $p = q + 4r$ mit einer ganzen Zahl r, die wir als positiv annehmen können (sonst vertausche man die Rollen von p und q). Außerdem gilt $q \nmid r$. Nach Satz 8.9 ist

$$\left(\frac{r}{q}\right) = \left(\frac{r}{p}\right).$$

Andrerseits ist

$$\left(\frac{r}{q}\right) = \left(\frac{4r}{q}\right) = \left(\frac{4r+q}{q}\right) = \left(\frac{p}{q}\right)$$

und unter Benutzung des 1. Ergänzungssatzes

$$\left(\frac{r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right),$$

also $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, falls $p \equiv q \equiv 1 \bmod 4$ und $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, falls $p \equiv q \equiv 3 \bmod 4$.

ii) Falls $p \not\equiv q \bmod 4$, gilt $p \equiv -q \bmod 4$, also $p + q = 4r$ mit einer ganzen Zahl r. Wieder gilt nach Satz 8.9

$$\left(\frac{r}{q}\right) = \left(\frac{r}{p}\right)$$

und

$$\left(\frac{r}{q}\right) = \left(\frac{4r}{q}\right) = \left(\frac{4r-q}{q}\right) = \left(\frac{p}{q}\right)$$

sowie

$$\left(\frac{r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{4r-p}{p}\right) = \left(\frac{q}{p}\right),$$

also $(\frac{p}{q}) = (\frac{q}{p})$. Damit ist das quadratische Reziprozitätsgesetz vollständig bewiesen.

Bemerkung. Wir haben hier das Reziprozitätsgesetz aus Satz 8.9 abgeleitet. Umgekehrt lässt sich Satz 8.9 auch leicht mithilfe des Reziprozitätsgesetzes beweisen (Übung).

Als Anwendung der Ergänzungssätze zum quadratischen Reziprozitätsgesetz beweisen wir jetzt die Existenz von unendlich vielen Primzahlen in arithmetischen Progressionen zum Modul 8.

8.11. Satz. *In jeder der arithmetischen Progressionen*

$$8k+1, \quad 8k+3, \quad 8k+5, \quad 8k+7, \quad (k \in \mathbb{N}),$$

gibt es unendlich viele Primzahlen.

Beweis. Sei $B > 0$ eine vorgegebene Schranke und U das Produkt aller ungeraden natürlichen Zahlen $\leqslant B$. Wir definieren

$$\begin{aligned} N_1 &:= (2U)^4 + 1, \\ N_3 &:= U^2 + 2, \\ N_5 &:= U^2 + 4, \\ N_7 &:= 8U^2 - 1. \end{aligned}$$

Da ein Quadrat einer ungeraden Zahl stets $\equiv 1 \bmod 8$ ist, folgt $U^2 \equiv 1 \bmod 8$ und

$$N_k \equiv k \bmod 8 \quad \text{für } k = 1, 3, 5, 7.$$

Außerdem besitzt N_k keinen Primteiler $q <= B$. Denn ein solcher Primteiler ist ungerade und teilt U. Also kann q nicht N_k ohne Rest teilen.

Unser Satz wird deshalb bewiesen sein, wenn wir zeigen, dass N_k einen Primteiler $q \mid N_k$ mit $q \equiv k \bmod 8$ besitzt.

i) Sei q ein Primteiler von $N_1 = (2U)^4 + 1$. Dann gilt $(2U)^4 + 1 \equiv 0 \bmod q$, d.h.

$$x^4 \equiv -1 \bmod q \quad \text{mit } x := 2U.$$

Daraus folgt, dass das Element x in $(\mathbb{Z}/q)^*$ die Ordnung 8 besitzt. Daher ist 8 ein Teiler von $\#(\mathbb{Z}/q)^* = q - 1$, d.h. $q \equiv 1 \bmod 8$, q.e.d.

ii) Sei q ein Primteiler von $N_3 = U^2 + 2$. Dann folgt

$$U^2 \equiv -2 \bmod q \quad \Longrightarrow \quad \left(\frac{-2}{q}\right) = 1.$$

Aus den Ergänzungssätzen zum quadratischen Reziprozitäts-Gesetz folgt dann $q \equiv 1 \bmod 8$ oder $q \equiv 3 \bmod 8$. Es können aber nicht alle Primteiler von N_3 kongruent $1 \bmod 8$ sein, denn dann wäre $N_3 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_3$ mit $q \equiv 3 \bmod 8$.

iii) Sei q ein Primteiler von $N_5 = U^2 + 4$. Dann folgt

$$U^2 \equiv -4 \bmod q \quad \Longrightarrow \quad \left(\frac{-1}{q}\right) = 1.$$

Daraus folgt $q \equiv 1 \bmod 4$, d.h. $q \equiv 1 \bmod 8$ oder $q \equiv 5 \bmod 8$. Es können aber nicht alle Primteiler von N_5 kongruent $1 \bmod 8$ sein, denn dann wäre $N_5 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_5$ mit $q \equiv 5 \bmod 8$.

iv) Sei q ein Primteiler von $N_7 = 8U^2 - 1$. Dann folgt $8U^2 - 1 \equiv 0 \bmod q$, also nach Multiplikation mit 2

$$(4U)^2 \equiv 2 \bmod q \quad \Longrightarrow \quad \left(\frac{2}{q}\right) = 1.$$

Nach dem 2. Ergänzungssatz zum quadratischen Reziprozitäts-Gesetz ist daher $q \equiv \pm 1 \bmod 8$. Es können aber nicht alle Primteiler von N_7 kongruent $1 \bmod 8$ sein, denn dann wäre $N_7 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_7$ mit $q \equiv -1 \equiv 7 \bmod 8$, q.e.d.

8.12. Das Jacobi-Symbol. Es ist für manche Zwecke nützlich, das Legendre-Symbol $(\frac{a}{p})$ auf den Fall zu verallgemeinern, dass der 'Nenner' keine Primzahl mehr ist.

Sei $m \geqslant 3$ eine ungerade Zahl und

$$m = p_1 p_2 \cdot \ldots \cdot p_r$$

die Primfaktor-Zerlegung von m (die p_j sind nicht notwendig paarweise verschieden). Dann definiert man für eine ganze Zahl a das *Jacobi-Symbol* $(\frac{a}{m})$ durch

$$\left(\frac{a}{m}\right) := \prod_{j=1}^{r} \left(\frac{a}{p_j}\right).$$

Das Jacobi-Symbol genügt folgenden Rechenregeln:

1) $\quad \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right), \quad$ falls $a \equiv b \bmod m$,

2) $\quad \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m}\right),$

3) $\left(\frac{a}{mk}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{k}\right)$ für ungerade $m, k \geqslant 3$,

4) $\left(\frac{a}{m}\right) = 0 \iff \gcd(a, m) \neq 1$.

Diese Regeln folgen unmittelbar aus der Definition und den entsprechenden Regeln für das Legendre-Symbol.

Man beachte jedoch folgenden Unterschied zum Legendre-Symbol: Ist a quadratischer Rest modulo m und $\gcd(a, m) = 1$, so folgt zwar $(\frac{a}{m}) = 1$, aber umgekehrt kann man aus $(\frac{a}{m}) = 1$ nicht schließen, dass a quadratischer Rest modulo m ist. Z.B. ist 2 weder quadratischer Rest mod 3 noch mod 5, also auch nicht quadratischer Rest mod 15, aber

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1.$$

8.13. Satz (Quadratisches Reziprozitätsgesetz für das Jacobi-Symbol).
Sei $m \geqslant 3$ eine ungerade Zahl.

(1) 1. Ergänzungssatz:

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} +1 & \textit{für } m \equiv 1 \bmod 4, \\ -1 & \textit{für } m \equiv 3 \bmod 4. \end{cases}$$

(2) 2. Ergänzungssatz:

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} +1 & \textit{für } m \equiv \pm 1 \bmod 8, \\ -1 & \textit{für } m \equiv \pm 3 \bmod 8. \end{cases}$$

(3) *Ist $k \geqslant 3$ eine weitere, zu m teilerfremde ungerade Zahl, so gilt*

$$\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{k-1}{2}},$$

d.h. $\left(\frac{k}{m}\right) = \left(\frac{m}{k}\right)$, *falls* $m \equiv 1 \bmod 4$ *oder* $k \equiv 1 \bmod 4$

und $\left(\frac{k}{m}\right) = -\left(\frac{m}{k}\right)$, *falls* $m \equiv k \equiv 3 \bmod 4$.

Beweis. (Zurückführung auf die entsprechenden Aussagen für das Legendre-Symbol)

8.14. Effiziente Berechnung des Jacobi-Symbols. Mit dem Reziprozitätsgesetz kann man einen effizienten Algorithmus zur Berechnung des Jacobi-Symbols herleiten: Es sei $(\frac{a}{m})$, $a, m \in \mathbb{Z}$, $m \geqslant 3$ ungerade, zu berechnen.

(1) Zunächst reduziere man a mod m, d.h. man bestimme ein a' mit $a \equiv a' \bmod m$ und $0 \leqslant a' < m$. Natürlich ist

$$\left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right).$$

Falls $a' = 0$ oder $a' = 1$ ist man fertig.

(2) Falls a' gerade, schreibe man $a' = 2^\nu b$ mit b ungerade. (Falls a' ungerade, ist $b = a'$ und $\nu = 0$.) Dann ist

$$\left(\frac{a'}{m}\right) = \left(\frac{2}{m}\right)^\nu \left(\frac{b}{m}\right),$$

und $(\frac{2}{m}) = \pm 1$ kann nach dem zweiten Ergänzungssatz berechnet werden. Falls $b = 1$, ist man fertig.

(3) Auf $(\frac{b}{m})$ kann jetzt das Reziprozitätsgesetz angewendet werden:

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

Dies gilt auch, wenn b und m nicht teilerfremd sind, denn dann sind beide Seiten $= 0$.

Auf $(\frac{m}{b})$ kann man jetzt wieder (1) anwenden. Da die 'Nenner' des Jacobi-Symbols immer kleiner werden, ist man nach endlich vielen Schritten fertig. Die Anzahl der Schritte ist vergleichbar mit den beim Euklidischen Algorithmus für die Berechnung von $\gcd(a, m)$ nötigen Schritte, wächst also nur linear mit der Stellenzahl von m.

Man beachte: Selbst wenn man nur ein Legendre-Symbol $(\frac{a}{p})$ mit einer Primzahl p mit dieser Methode ausrechnet, kann man zwischenzeitlich auf die allgemeineren Jacobi-Symbole stoßen.

Beispiel.

$$\begin{aligned}\left(\frac{170}{211}\right) &= \left(\frac{2}{211}\right)\left(\frac{85}{211}\right) = -\left(\frac{85}{211}\right) = -\left(\frac{211}{85}\right) = -\left(\frac{41}{85}\right) = \\ &= -\left(\frac{85}{41}\right) = -\left(\frac{3}{41}\right) = -\left(\frac{41}{3}\right) = -\left(\frac{2}{3}\right) = 1.\end{aligned}$$