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*

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

(2) *Für alle* $a, b \in \mathbb{Z}$ *gilt*

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

(3) *Für jedes* $a \in \mathbb{Z}$ *und jedes* $b \in \mathbb{Z} \setminus p\mathbb{Z}$ *gilt*

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

(4) *Es gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod 4 \text{ gilt,} \\ -1, & \text{falls } p \equiv 3 \pmod 4 \text{ gilt.} \end{cases}$$

(5) *Es gilt*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{falls } p \equiv 1 \text{ oder } 7 \pmod 8 \text{ gilt,} \\ -1, & \text{falls } p \equiv 3 \text{ oder } 5 \pmod 8 \text{ gilt.} \end{cases}$$

Beweis: (1) ist klar, (2) und (4) folgen aus (11.3), und (3) folgt aus (2).
(5) Für jedes ungerade $k \in \{1, 2, \ldots, (p-1)/2\}$ gilt $p - k \equiv (-1)^k k \pmod p$, und für jedes gerade $k \in \{1, 2, \ldots, (p-1)/2\}$ gilt $k = (-1)^k k$; außerdem ist $\{p - k \mid 1 \le k \le (p-1)/2; k \text{ ungerade}\} = \{j \mid (p+1)/2 \le j \le p-1; j \text{ gerade}\}$. Also gilt

$$2 \cdot 4 \cdot 6 \cdots (p-3) \cdot (p-1) = \left(\prod_{\substack{k=1 \\ k \equiv 0 \,(\mathrm{mod}\, 2)}}^{(p-1)/2} k \right) \cdot \left(\prod_{\substack{j=(p+1)/2 \\ j \equiv 0 \,(\mathrm{mod}\, 2)}}^{p-1} j \right) =$$

$$= \left(\prod_{\substack{k=1 \\ k \equiv 0 \,(\mathrm{mod}\, 2)}}^{(p-1)/2} k \right) \cdot \left(\prod_{\substack{k=1 \\ k \equiv 1 \,(\mathrm{mod}\, 2)}}^{(p-1)/2} (p-k) \right) \equiv \prod_{k=1}^{(p-1)/2} (-1)^k k =$$

$$= (-1)^{1+2+\cdots+(p-1)/2} \left(\frac{p-1}{2}\right)! = (-1)^{(p^2-1)/8} \left(\frac{p-1}{2}\right)! \pmod p,$$

denn es gilt

$$1 + 2 + \cdots + \frac{p-1}{2} = \frac{1}{2} \cdot \frac{p-1}{2} \left(\frac{p-1}{2} + 1\right) = \frac{1}{8}(p^2 - 1).$$

Wegen $2 \cdot 4 \cdot 6 \cdots (p-3) \cdot (p-1) = 2^{(p-1)/2}((p-1)/2)!$ gilt daher

$$2^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv (-1)^{(p^2-1)/8} \left(\frac{p-1}{2}\right)! \pmod p.$$

Da $((p-1)/2)!$ nicht durch p teilbar ist, folgt

$$\left(\frac{2}{p}\right) \overset{(11.3)}{\equiv} 2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod{p},$$

und weil p ungerade ist, gilt daher

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

(11.5) Hilfssatz: *Es sei p eine ungerade Primzahl.*
(1) (J. Wilson, 1741 - 1793): *Es gilt*

$$(p-1)! \equiv -1 \pmod{p}.$$

(2) *Es gilt*

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

Beweis: (1) Es sei g eine Primitivwurzel modulo p. Es ist $\{1, 2, \ldots, p-1\} = \{g^i \bmod p \mid 0 \le i \le p-2\}$, und daher gilt

$$\begin{aligned}(p-1)! &= \prod_{i=0}^{p-2}(g^i \bmod p) \equiv \prod_{i=0}^{p-2} g^i = g^{1+2+\cdots+(p-2)} = \\ &= g^{(p-2)(p-1)/2} = \left(g^{(p-1)/2}\right)^{p-2} \equiv (-1)^{p-2} = -1 \pmod{p},\end{aligned}$$

denn im Körper $\mathbb{F}_p$ ist

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

und wegen $\operatorname{ord}([g]_p) = p-1$ folgt $[g]_p^{(p-1)/2} = -[1]_p$.
(2) Es gilt

$$\left\{j \;\middle|\; \frac{p+1}{2} \le j \le p-1\right\} = \left\{p-k \;\middle|\; 1 \le k \le \frac{p-1}{2}\right\}$$

und daher

$$\begin{aligned}-1 \overset{(1)}{\equiv} (p-1)! &= \left(\prod_{j=1}^{(p-1)/2} j\right) \cdot \left(\prod_{j=(p+1)/2}^{p-1} j\right) = \\ &= \left(\prod_{j=1}^{(p-1)/2} j\right) \cdot \left(\prod_{k=1}^{(p-1)/2} (p-k)\right) \equiv\end{aligned}$$

$$\equiv (-1)^{(p-1)/2} \left(\prod_{j=1}^{(p-1)/2} j \right) \cdot \left(\prod_{k=1}^{(p-1)/2} k \right) =$$

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

Hieraus folgt

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

(11.6) Satz: *Es seien p und q verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q} \right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p} \right).$$

Beweis: (1) Es sei

$$G := \mathbb{F}_p^\times \times \mathbb{F}_q^\times = \left\{ (\alpha, \beta) \,\middle|\, \alpha \in \mathbb{F}_p^\times,\ \beta \in \mathbb{F}_q^\times \right\}.$$

Mit der Verknüpfung

$$\big((\alpha, \beta), (\alpha', \beta')\big) \mapsto (\alpha\alpha', \beta\beta') : G \times G \to G$$

ist G eine endliche abelsche Gruppe. Neutrales Element in G ist $(1_{\mathbb{F}_p}, 1_{\mathbb{F}_q}) = ([1]_p, [1]_q)$, und für jedes $(\alpha, \beta) \in G$ gilt: Invers zu (α, β) in der Gruppe G ist $(\alpha^{-1}, \beta^{-1})$.

$$U := \left\{ ([1]_p, [1]_q), (-[1]_p, -[1]_q) \right\} = \left\{ ([1]_p, [1]_q), ([-1]_p, [-1]_q) \right\}$$

ist eine Untergruppe der Ordnung 2 von G. Die Faktorgruppe G/U ist eine abelsche Gruppe der Ordnung $\#(G)/\#(U) = (p-1)(q-1)/2$. Für alle (α, β), $(\alpha', \beta') \in G$ gilt $[(\alpha, \beta)]_U = [(\alpha', \beta')]_U$, genau wenn entweder $(\alpha, \beta) = (\alpha', \beta')$ oder $(\alpha, \beta) = (-\alpha', -\beta')$ gilt, also genau wenn entweder $\alpha = \alpha'$ und $\beta = \beta'$ oder $\alpha = -\alpha'$ und $\beta = -\beta'$ gilt.
Setzt man für jedes $a \in \mathbb{Z} \setminus p\mathbb{Z}$ und jedes $b \in \mathbb{Z} \setminus q\mathbb{Z}$ zur Abkürzung

$$[a, b] := \left[([a]_p, [b]_q) \right]_U,$$

so ist

$$G/U = \left\{ [a, b] \mid a \in \mathbb{Z} \setminus p\mathbb{Z};\ b \in \mathbb{Z} \setminus q\mathbb{Z} \right\} =$$
$$= \left\{ [a, b] \mid 1 \le a \le p-1;\ 1 \le b \le q-1 \right\},$$

und für alle a, $a' \in \mathbb{Z} \setminus p\mathbb{Z}$ und alle b, $b' \in \mathbb{Z} \setminus q\mathbb{Z}$ gilt: Es ist $[a,b] \cdot [a',b'] = [aa', bb']$, und es gilt $[a,b] = [a',b']$, genau wenn entweder $a \equiv a' \pmod p$ und $b \equiv b' \pmod q$ oder $a \equiv -a' \pmod p$ und $b \equiv -b' \pmod q$ gilt.
Der Beweis des Satzes erfolgt nun dadurch, daß man auf zwei verschiedene Weisen das Produkt π aller Elemente der abelschen Gruppe G/U berechnet.
(2) (a) Es seien a, $a' \in \{1,2,\dots,p-1\}$ und b, $b' \in \{1,2,\dots,(q-1)/2\}$ mit $a \neq a'$ oder $b \neq b'$. In der Gruppe G/U gilt dann $[a,b] \neq [a',b']$, denn wäre $[a,b] = [a',b']$, so wäre $b \equiv -b' \pmod q$, also wäre $b + b'$ durch q teilbar, im Widerspruch zu $2 \leq b + b' \leq q - 1$.
(b) Es ist $\#(G/U) = (p-1)(q-1)/2$, und daher folgt aus (a): Die Elemente von G/U sind die $(p-1)(q-1)/2$ Äquivalenzklassen $[a,b] \in G/U$ mit $a \in \{1,2,\dots,p-1\}$ und mit $b \in \{1,2,\dots,(q-1)/2\}$. Für das Produkt π aller Elemente von G/U gilt daher: Es ist

$$\begin{aligned}\pi &= \left[((p-1)!)^{(q-1)/2}, \left(\left(\frac{q-1}{2}\right)! \right)^{p-1} \right] = \\ &= \left[((p-1)!)^{(q-1)/2}, \left(\left(\left(\frac{q-1}{2}\right)! \right)^2 \right)^{(p-1)/2} \right] = \\ &\overset{(11.5)}{=} \left[(-1)^{(q-1)/2}, (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(q-1)/4} \right].\end{aligned}$$

(3) Es sei $\mathcal{M} := \{c \in \mathbb{N} \mid 1 \leq c \leq (pq-1)/2;\ \mathrm{ggT}(c,pq) = 1\}$. Es gilt

$$\begin{aligned}\mathcal{M} := \Bigg(&\left\{ i + jp \,\middle|\, 1 \leq i \leq p-1;\ 0 \leq j \leq \frac{q-1}{2} - 1 \right\} \cup \\ &\cup \left\{ i + \frac{q-1}{2} p \,\middle|\, 1 \leq i \leq \frac{p-1}{2} \right\} \Bigg) \setminus \left\{ kq \,\middle|\, 1 \leq k \leq \frac{p-1}{2} \right\}\end{aligned}$$

und

$$\#(\mathcal{M}) = (p-1) \cdot \frac{q-1}{2} + \frac{p-1}{2} - \frac{p-1}{2} = \frac{(p-1)(q-1)}{2} = \#(G/U).$$

Die Abbildung $c \mapsto [c,c] = [([c]_p, [c]_q)]_U : \mathcal{M} \to G/U$ ist injektiv, denn sind c, $c' \in \mathcal{M}$ und ist $[c,c] = [c',c']$, so gilt entweder $c \equiv c' \pmod p$ und $c \equiv c' \pmod q$ oder $c \equiv -c' \pmod p$ und $c \equiv -c' \pmod q$, also entweder $c \equiv c' \pmod{pq}$ oder $c \equiv -c' \pmod{pq}$, und wegen $2 \leq c + c' \leq pq - 1$ folgt $c \equiv c' \pmod{pq}$, also $c = c'$. Wegen $\#(\mathcal{M}) = \#(G/U)$ ist daher die Abbildung $c \mapsto [c,c] : \mathcal{M} \to G/U$ bijektiv, also ist $G/U = \{[c,c] \mid c \in \mathcal{M}\}$. Es gilt

$$\prod_{c \in \mathcal{M}} c = \left(\prod_{j=0}^{(q-1)/2-1} \left(\prod_{i=1}^{p-1} (i + jp) \right) \right) \cdot \left(\prod_{i=1}^{(p-1)/2} \left(i + \frac{q-1}{2} p \right) \right) \Bigg/ \left(\prod_{k=1}^{(p-1)/2} kq \right),$$

und wegen

$$\prod_{k=1}^{(p-1)/2} kq \;=\; q^{(p-1)/2}\Big(\frac{p-1}{2}\Big)!$$

und

$$\prod_{j=0}^{(q-1)/2-1}\Big(\prod_{i=1}^{p-1}(i+jp)\Big) \;\equiv\; \prod_{j=0}^{(q-1)/2-1}\Big(\prod_{i=1}^{p-1} i\Big) \;=$$

$$= \prod_{j=0}^{(q-1)/2-1}(p-1)! \;=\; \big((p-1)!\big)^{(q-1)/2} \;\equiv\; (-1)^{(q-1)/2} \pmod p$$

folgt

$$q^{(p-1)/2}\Big(\frac{p-1}{2}\Big)!\cdot\prod_{c\in\mathcal{M}} c \;\equiv\; \Big(\prod_{k=1}^{(p-1)/2} kq\Big)\cdot\Big(\prod_{c\in\mathcal{M}} c\Big) \;=$$

$$= \Big(\prod_{j=0}^{(q-1)/2-1}\Big(\prod_{i=1}^{p-1}(i+jp)\Big)\Big)\cdot\Big(\prod_{i=1}^{(p-1)/2}\Big(i+\frac{q-1}{2}p\Big)\Big) \;\equiv$$

$$\equiv (-1)^{(q-1)/2}\Big(\frac{p-1}{2}\Big)! \pmod p.$$

Weil $((p-1)/2)!$ nicht durch p teilbar ist, folgt

$$q^{(p-1)/2}\prod_{c\in\mathcal{M}} c \;\equiv\; (-1)^{(q-1)/2} \pmod p,$$

also

$$\prod_{c\in\mathcal{M}} c \overset{(4.21)(1)}{\equiv} q^{p-1}\prod_{c\in\mathcal{M}} c \;=\; q^{(p-1)/2}\cdot q^{(p-1)/2}\prod_{c\in\mathcal{M}} c \;\equiv$$

$$\equiv\; q^{(p-1)/2}\cdot(-1)^{(q-1)/2} \overset{(11.3)}{\equiv} (-1)^{(q-1)/2}\Big(\frac{q}{p}\Big) \pmod p.$$

Auf dieselbe Weise ergibt sich: Es ist

$$\prod_{c\in\mathcal{M}} c \;\equiv\; (-1)^{(p-1)/2}\Big(\frac{p}{q}\Big) \pmod q.$$

Also gilt für das Produkt π aller Elemente von G/U: Es ist

$$\pi \;=\; \Big[\prod_{c\in\mathcal{M}} c, \prod_{c\in\mathcal{M}} c\Big] \;=\; \Big[(-1)^{(q-1)/2}\Big(\frac{q}{p}\Big), (-1)^{(p-1)/2}\Big(\frac{p}{q}\Big)\Big] \;=$$

$$= \Big[(-1)^{(q-1)/2}, (-1)^{(p-1)/2}\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big)\Big],$$

denn es gilt $(q \mid p) = 1$ oder $(q \mid p) = -1$, und in der Gruppe G/U gilt für alle $a \in \mathbb{Z} \setminus p\mathbb{Z}$ und $b \in \mathbb{Z} \setminus q\mathbb{Z}$: Es ist $[a, b] = [-a, -b]$.
(4) Nach (2) und (3) gilt

$$\left[(-1)^{(q-1)/2}, (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(q-1)/4}\right] = \boldsymbol{\pi} =$$
$$= \left[(-1)^{(q-1)/2}, (-1)^{(p-1)/2} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)\right],$$

und daraus folgt

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

also

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

(11.7) Bemerkung: (1) Die Aussage in (11.6) ist das berühmte quadratische Reziprozitätsgesetz, das von L. Euler und von A. M. Legendre gefunden und zuerst von C. F. Gauß bewiesen wurde (vgl. [37], Artikel 131 und 262). Die Aussagen (4) und (5) in (11.4) nennt man die Ergänzungssätze dazu; sie wurden wohl von P. de Fermat gefunden und von L. Euler und J. L. Lagrange erstmals bewiesen. Für das quadratische Reziprozitätsgesetz gibt es sicher über hundert verschiedene Beweise; Gauß hat dafür sieben Beweise angegeben. Der Beweis in (11.6) stammt von G. Rousseau [95]; fünfzehn andere Beweise findet man in Piper [80].
(2) Mit Hilfe des quadratischen Reziprozitätsgesetzes und der Ergänzungssätze dazu kann man entscheiden, ob eine ganze Zahl ein quadratischer Rest modulo einer gegebenen ungeraden Primzahl p ist oder nicht; man damit auch untersuchen, für welche Primzahlen p eine gegebene ganze Zahl quadratischer Rest ist.

(11.8) Beispiele: (1) Es gilt

$$\left(\frac{219}{383}\right) = \left(\frac{3 \cdot 73}{383}\right) \overset{(11.4)(2)}{=} \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right),$$
$$\left(\frac{3}{383}\right) \overset{(11.6)}{=} (-1)^{(3-1)(383-1)/4} \left(\frac{383}{3}\right) \overset{(11.4)(1)}{=} -\left(\frac{2}{3}\right) =$$
$$\overset{(11.4)(5)}{=} -(-1)^{(3^2-1)/8} = 1 \quad \text{und}$$
$$\left(\frac{73}{383}\right) \overset{(11.6)}{=} (-1)^{(73-1)(383-1)/4} \left(\frac{383}{73}\right) = \left(\frac{383}{73}\right) \overset{(11.4)(1)}{=} \left(\frac{18}{73}\right) =$$
$$\overset{(11.4)(2)}{=} \left(\frac{2}{73}\right) \cdot \left(\frac{3}{73}\right)^2 = \left(\frac{2}{73}\right) \overset{(11.4)(5)}{=} (-1)^{(73^2-1)/8} = 1.$$

Also gilt

$$\left(\frac{219}{383}\right) = 1,$$

und somit ist 219 ein quadratischer Rest modulo 383.

(2) Es sei $p \geq 5$ eine Primzahl. Dann gilt nach (11.6)

$$\left(\frac{3}{p}\right) = (-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

Es gilt

$$(-1)^{(p-1)/2} = \begin{cases} 1, \text{ falls } p \equiv 1 \pmod 4 \text{ gilt,} \\ -1, \text{ falls } p \equiv 3 \pmod 4 \text{ gilt,} \end{cases}$$

und

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, \text{ falls } p \equiv 1 \pmod 3 \text{ gilt,} \\ \left(\frac{2}{3}\right) = -1, \text{ falls } p \equiv 2 \pmod 3 \text{ gilt.} \end{cases}$$

Somit ist 3 quadratischer Rest modulo p, genau wenn entweder $p \equiv 1 \pmod 4$ und $p \equiv 1 \pmod 3$ gilt oder $p \equiv 3 \pmod 4$ und $p \equiv 2 \pmod 3$, also genau wenn $p \equiv 1 \pmod{12}$ oder $p \equiv 11 \pmod{12}$ gilt.

(11.9) Bemerkung: Das erste Beispiel in (11.8) zeigt, daß man mit Hilfe des quadratischen Reziprozitätsgesetzes Legendre-Symbole berechnen kann, aber auch, daß man dabei unter Umständen Primzerlegungen ermitteln muß. Die im folgenden Abschnitt definierte Verallgemeinerung des Legendre-Symbols erlaubt die Berechnung von Legendre-Symbolen, ohne daß dabei Primzerlegungen zu berechnen sind.

(11.10) Definition: Es sei $m \in \mathbb{N}$ ungerade, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Für $a \in \mathbb{Z}$ setzt man

$$(a \mid m) = \left(\frac{a}{m}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i},$$

wobei in dem Produkt rechts Legendre-Symbole stehen. Die Abbildung

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

heißt das Jacobi-Symbol modulo m (nach C. G. J. Jacobi, 1804 - 1851).

(11.11) Bemerkung: (1) Ist p eine ungerade Primzahl, so ist das Jacobi-Symbol modulo p genau das Legendre-Symbol modulo p.
(2) Für jedes $a \in \mathbb{Z}$ ist $(a \mid 1) = 1$.
(3) Es sei $m \in \mathbb{N}$ ungerade, und es sei $a \in \mathbb{Z}$. Auch wenn $(a \mid m) = 1$ ist, kann a ein quadratischer Nichtrest modulo m sein: Es ist $(5 \mid 9) = (5 \mid 3)^2 = 1$, aber 5 ist nicht quadratischer Rest modulo 9.

(11.12) Satz: *Es seien $m_1, m_2 \in \mathbb{N}$ ungerade. Für jedes $a \in \mathbb{Z}$ gilt*

$$\left(\frac{a}{m_1 m_2}\right) = \left(\frac{a}{m_1}\right)\left(\frac{a}{m_2}\right).$$

Beweis: Die Behauptung folgt unmittelbar aus der Definition in (11.10).

(11.13) Satz: *Es sei $m \in \mathbb{N}$ ungerade.*
(1) *Für alle $a, b \in \mathbb{Z}$ mit $a \equiv b \pmod{m}$ gilt*

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

(2) *Für $a \in \mathbb{Z}$ gilt $(a \mid m) = 0$, genau wenn $\mathrm{ggT}(a, m) > 1$ ist.*
(3) *Für alle $a, b \in \mathbb{Z}$ gilt*

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

(4) *Sind $a, b \in \mathbb{Z}$ und ist $\mathrm{ggT}(b, m) = 1$, so gilt*

$$\left(\frac{ab^2}{m}\right) = \left(\frac{a}{m}\right).$$

Beweis: Die Behauptungen folgen unmittelbar aus der Definition des Jacobi-Symbols und aus den entsprechenden Eigenschaften des Legendre-Symbols (vgl. dazu (11.4)).

(11.14) Satz (Die Ergänzungssätze für das Jacobi-Symbol): *Es sei $m \in \mathbb{N}$ ungerade. Dann gilt*

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} \quad \textit{und} \quad \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Beweis: Es gilt $m = p_1 p_2 \cdots p_r$ mit nicht notwendig verschiedenen ungeraden Primzahlen $p_1, p_2, \ldots, p_r$. Dann gilt für jedes $a \in \mathbb{Z}$

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

(1) Es gilt

$$m = \prod_{i=1}^{r}(1+(p_i-1)) \equiv 1+\sum_{i=1}^{r}(p_i-1) \pmod 4$$

und daher

$$\frac{1}{2}(m-1) \equiv \sum_{i=1}^{r}\frac{1}{2}(p_i-1) \pmod 2.$$

Also gilt wegen (11.4)(4)

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{r}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i-1)/2} = (-1)^{\sum_{i=1}^{r}(p_i-1)/2} = (-1)^{(m-1)/2}.$$

(2) Für jedes ungerade $x \in \mathbb{Z}$ gilt: Die Zahlen $x-1$ und $x+1$ sind beide gerade, und eine von ihnen ist durch 4 teilbar, und daher ist x^2-1 durch 8 teilbar. Es folgt

$$m^2 = \prod_{i=1}^{r}(1+(p_i^2-1)) \equiv 1+\sum_{i=1}^{r}(p_i^2-1) \pmod{64},$$

also

$$\frac{1}{8}(m^2-1) \equiv \sum_{i=1}^{r}\frac{1}{8}(p_i^2-1) \pmod 8$$

und daher wegen (11.4)(5)

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8} = (-1)^{\sum_{i=1}^{r}(p_i^2-1)/8} = (-1)^{(m^2-1)/8}.$$

(11.15) Satz (Quadratisches Reziprozitätsgesetz für das Jacobi-Symbol): *Es seien m eine ungerade natürliche Zahl und a eine ungerade ganze Zahl. Dann gilt*

$$\left(\frac{a}{m}\right) = (-1)^{(a-1)(m-1)/4}\left(\frac{m}{|a|}\right).$$

Beweis: (a) Ist $\mathrm{ggT}(a,m) > 1$, so gilt

$$\left(\frac{a}{m}\right) = 0 \quad \text{und} \quad \left(\frac{m}{|a|}\right) = 0.$$

(b) Es gelte $\mathrm{ggT}(a,m) = 1$ und $a > 0$. Dann gilt mit nicht notwendig verschiedenen ungeraden Primzahlen $p_1, p_2, \ldots, p_r$ und $q_1, q_2, \ldots, q_s$

$$m = p_1 p_2 \cdots p_r \quad \text{und} \quad a = q_1 q_2 \cdots q_s,$$

und wegen $\mathrm{ggT}(a,m) = 1$ ist $\{p_1, p_2, \ldots, p_r\} \cap \{q_1, q_2, \ldots, q_s\} = \varnothing$. Es gilt

$$\begin{aligned}
\left(\frac{a}{m}\right) &= \prod_{i=1}^{s}\left(\frac{a}{p_i}\right) = \\
&\overset{(11.13)(3)}{=} \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right) \overset{(11.6)}{=} \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(p_i-1)(q_j-1)/4}\left(\frac{p_i}{q_j}\right) = \\
&= (-1)^t \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right) = (-1)^t \prod_{i=1}^{r}\left(\frac{p_i}{a}\right) \overset{(11.13)(3)}{=} (-1)^t \left(\frac{m}{a}\right)
\end{aligned}$$

mit

$$\begin{aligned}
t &= \sum_{i=1}^{r}\sum_{j=1}^{s}\frac{1}{2}(p_i-1)\cdot\frac{1}{2}(q_j-1) = \left(\sum_{i=1}^{r}\frac{1}{2}(p_i-1)\right)\left(\sum_{j=1}^{s}\frac{1}{2}(q_j-1)\right) \equiv \\
&\overset{(*)}{\equiv} \frac{1}{2}(m-1)\cdot\frac{1}{2}(a-1) = \frac{(a-1)(m-1)}{4} \pmod 2.
\end{aligned}$$

(Zu $(*)$ vergleiche man die Überlegung im ersten Teil des Beweises in (11.14)).
(c) Es gelte $\mathrm{ggT}(a,m) = 1$ und $a < 0$. Dann gilt

$$\begin{aligned}
\left(\frac{a}{m}\right) &= \left(\frac{-|a|}{m}\right) \overset{(11.13)(3)}{=} \left(\frac{-1}{m}\right)\left(\frac{|a|}{m}\right) \overset{(11.14)}{=} (-1)^{(m-1)/2}\left(\frac{|a|}{m}\right) = \\
&\overset{(b)}{=} (-1)^{(m-1)/2}\cdot(-1)^{(|a|-1)(m-1)/4}\left(\frac{m}{|a|}\right) = \\
&= (-1)^{(|a|+1)(m-1)/4}\left(\frac{m}{|a|}\right) = (-1)^{(-a+1)(m-1)/4}\left(\frac{m}{|a|}\right) = \\
&= (-1)^{(a-1)(m-1)/4}\left(\frac{m}{|a|}\right).
\end{aligned}$$

(11.16) Bemerkung: Die folgenden Beispiele zeigen, wie man mit Hilfe von Jacobi-Symbolen Legendre-Symbole berechnen kann. Sie zeigen auch, wie die Ergebnisse aus (11.13), aus (11.14) und insbesondere aus (11.15) einen Algorithmus zur Berechnung von Legendre-Symbolen und Jacobi-Symbolen liefern. Ein solcher Algorithmus wird in (11.18) angegeben.

(11.17) Beispiele: (1) 317 ist eine Primzahl, und es ist

$$\left(\frac{105}{317}\right) \overset{(11.15)}{=} (-1)^{(105-1)(317-1)/4}\left(\frac{317}{105}\right) = \left(\frac{317}{105}\right) =$$
$$= \left(\frac{3\cdot 105+2}{105}\right) \overset{(11.13)(1)}{=} \left(\frac{2}{105}\right) =$$
$$\overset{(11.14)}{=} (-1)^{(105^2-1)/8} = 1.$$

Also ist 105 ein quadratischer Rest modulo 317.

(2) 1999 ist eine Primzahl, und es gilt

$$\left(\frac{888}{1999}\right) = \left(\frac{2^3\cdot 111}{1999}\right) = \left(\frac{2}{1999}\right)^3\left(\frac{111}{1999}\right) =$$
$$= (-1)^{(1999^2-1)/8}\cdot(-1)^{(111-1)(1999-1)/4}\left(\frac{1999}{111}\right) =$$
$$= -\left(\frac{18\cdot 111+1}{111}\right) = -\left(\frac{1}{111}\right) = -1,$$

und daher ist 888 ein quadratischer Nichtrest modulo 1999.

(11.18) Ein Algorithmus zur Berechnung von Jacobi-Symbolen:
(1) Es seien m eine ungerade natürliche Zahl, und es sei a eine ganze Zahl. Der folgende Algorithmus berechnet das Jacobi-Symbol $(a \mid m)$:

(JS1) Ist $m = 1$, so gibt man 1 aus und bricht ab.
(JS2) Ist $\mathrm{ggT}(a, m) > 1$, so gibt man 0 aus und bricht ab.
(JS3) Man setzt $\varepsilon := 1$, $x := a \bmod m$ und $y := m$.
(JS4) Ist x ungerade, so geht man zu (JS6).
(JS5) Man ermittelt $\alpha := v_2(x)$ und setzt $x := x/2^\alpha$. Ist α ungerade und gilt entweder $y \equiv 3 \pmod 8$ oder $y \equiv 5 \pmod 8$, so setzt man $\varepsilon := -\varepsilon$.
(JS6) Ist $x = 1$, so gibt man ε aus und bricht ab.
(JS7) Gilt $x \equiv 3 \pmod 4$ und $y \equiv 3 \pmod 4$, so setzt man $\varepsilon := -\varepsilon$.
(JS8) Man setzt $z := y \bmod x$, $y := x$ und $x := z$.
(JS9) Ist $x = 1$, so gibt man ε aus und bricht ab. Ist $x > 1$, so geht man zu Schritt (JS4).

(2) Der Algorithmus bricht nach endlich vielen Schritten ab, denn jedesmal, wenn (JS8) durchlaufen wird, nimmt die natürliche Zahl x mindestens um 1 ab. Er berechnet wirklich das Jacobi-Symbol $(a \mid m)$, denn wenn $m > 1$ ist und a und m teilerfremd sind, so gilt von (JS3) an zu jedem Zeitpunkt $(a \mid m) = \varepsilon \cdot (x \mid y)$.

(11.19) Bemerkung: Es sei m eine ungerade natürliche Zahl, und es sei a eine ganze Zahl.
(1) Der Algorithmus in (11.18) ist für MuPAD formuliert. Man könnte ihn auch so formulieren, daß er nicht gleich zu Beginn $\mathrm{ggT}(a,m)$ berechnet, sondern erst am Ende erkennt, ob a und m teilerfremd sind oder nicht. Da `igcd` eine Funktion des MuPAD-Kerns und daher sehr schnell ist, spielt in einem MuPAD-Programm für diesen Algorithmus ein Aufruf von `igcd` keine wesentliche Rolle.
(2) Sieht man von der Berechnung von $\mathrm{ggT}(a,m)$ in (JS2) ab, so kann man den Aufwand des Algorithmus in (11.18) zur Berechnung von $(a \mid m)$ an der Anzahl der Anwendungen des quadratischen Reziprozitätsgesetzes im Schritt (JS8) messen. Diese Anzahl ist, wenn a und m teilerfremd sind, höchstens gleich

$$\lfloor 1.32 \cdot \log\bigl((a \bmod m) + m\bigr) - 0.72 \rfloor,$$

wie J. Shallit in [102] in einer lesenswerten Diskussion verschiedener Verfahren zur Berechnung von Jacobi-Symbolen gezeigt hat.

(11.20) MuPAD: Den in (11.18) beschriebenen Algorithmus JS verwenden die Funktionen `numlib::legendre` und `numlib::jacobi` zur Berechnung von Legendre-Symbolen und Jacobi-Symbolen. Zu einer natürlichen Zahl m und einer ganzen Zahl a liefert die Anweisung `numlib::isquadres(a,m)` die Ausgabe `TRUE`, falls a ein quadratischer Rest modulo m ist, bzw. die Ausgabe `FALSE`, falls a ein quadratischer Nichtrest modulo m ist; sind m und a nicht teilerfremd, wird eine Fehlermeldung ausgegeben.

(11.21) Bemerkung: Zum Abschluß dieses Paragraphen wird der bereits in (2.9)(3) angegebene Satz von Lucas und Lehmer bewiesen. Dieser Beweis, wie auch der des Satzes von Pepin in (11.24), Aufgabe 3, zeigt, welche nützlichen Beweismethoden die Theorie der quadratischen Reste dem Zahlentheoretiker zu Verfügung stellt.

(11.22) Satz (E. Lucas 1878, D. H. Lehmer 1930/35): *Es sei $(a_n)_{n\geq 1}$ die Folge mit $a_1 := 4$ und mit $a_{n+1} := a_n^2 - 2$ für jedes $n \in \mathbb{N}$, und es sei p eine ungerade Primzahl. Die Mersenne-Zahl $M(p) = 2^p - 1$ ist dann und nur dann eine Primzahl, wenn a_{p-1} durch $M(p)$ teilbar ist.*

Beweis: (0) Für

$$\omega := 2+\sqrt{3}, \quad \overline{\omega} := 2-\sqrt{3} \quad \text{und} \quad \tau := \frac{1}{\sqrt{2}}\,(1+\sqrt{3})$$

gilt $\omega \cdot \overline{\omega} = 1$ und $\tau^2 = \omega$. Für jedes $n \in \mathbb{N}$ ist, wie man leicht durch Induktion beweist,

$$a_n = \omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}}.$$

(1) Es gelte: $M(p)$ teilt a_{p-1}. Dann gibt es ein $v \in \mathbb{N}$ mit

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = a_{p-1} = vM(p),$$

und damit gilt

$$\omega^{2^{p-1}} = \omega^{2^{p-2}}\omega^{2^{p-2}} = \left(vM(p) - \overline{\omega}^{2^{p-2}}\right)\omega^{2^{p-2}} = vM(p)\,\omega^{2^{p-2}} - 1.$$

(a) Es sei q ein Primteiler von $M(p)$. Auf $R := \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ werden folgendermaßen eine Addition $+$ und eine Multiplikation $\cdot$ definiert: Für alle a, b, c, $d \in \mathbb{Z}$ setzt man

$$\begin{aligned}([a]_q,[b]_q) + ([c]_q,[d]_q) &:= ([a+c]_q,[b+d]_q) = \\ &= ([a]_q + [c]_q, [b]_q + [d]_q) \quad \text{und}\\ ([a]_q,[b]_q) \cdot ([c]_q,[d]_q) &:= ([ac+3bd]_q,[ad+bc]_q) = \\ &= ([a]_q[c]_q + [3]_q[b]_q[d]_q, [a]_q[d]_q + [b]_q[c]_q).\end{aligned}$$

Wie man ohne Schwierigkeit nachrechnet, ist R ein kommutativer Ring mit dem Nullelement $0_R := ([0]_q,[0]_q)$ und dem Einselement $1_R := ([1]_q,[0]_q)$.
(b) $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a,b \in \mathbb{Z}\}$ ist ein Unterring des Körpers $\mathbb{R}$, und weil $\sqrt{3}$ eine irrationale Zahl ist, gibt es zu jedem $x \in \mathbb{Z}[\sqrt{3}]$ eindeutig bestimmte a, $b \in \mathbb{Z}$ mit $x = a + b\sqrt{3}$. Die Abbildung

$$\psi : \mathbb{Z}[\sqrt{3}] \to R \quad \text{mit} \quad \psi(a+b\sqrt{3}) := ([a]_q,[b]_q) \quad \text{für alle } a,b \in \mathbb{Z}$$

ist ein Homomorphismus von Ringen, d.h. es ist $f(1) = 1_R$, und für alle x, $y \in \mathbb{Z}[\sqrt{3}]$ gilt $\psi(x+y) = \psi(x) + \psi(y)$ und $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$. ω und $\overline{\omega}$ sind Elemente von $\mathbb{Z}[\sqrt{3}]$, und es gilt $\psi(\omega)\cdot\psi(\overline{\omega}) = \psi(\omega\,\overline{\omega}) = \psi(1) = 1_R$. Also ist $\psi(\omega)$ ein Element der Einheitengruppe $E(R)$ des Rings R. Wegen $q \mid M(p)$ ist $\psi(M(p)) = ([M(p)]_q,[0]_q) = ([0]_q,[0]_q) = 0_R$, und daher gilt

$$\begin{aligned}\psi(\omega)^{2^{p-1}} = \psi\left(\omega^{2^{p-1}}\right) &\overset{(1)}{=} \psi\left(vM(p)\cdot\omega^{2^{p-2}} - 1\right) = \\ &= \psi(v)\cdot\psi\left(M(p)\right)\cdot\psi(\omega)^{2^{p-2}} + \psi(-1) = \left([-1]_q,[0]_q\right) = -1_R.\end{aligned}$$

Hieraus folgt $\psi(\omega)^{2^p} = (-1_R)^2 = 1_R$, und daher ist die Ordnung von $\psi(\omega)$ in der Gruppe $E(R)$ ein Teiler von 2^p (vgl. (3.5)(3)). Da q ungerade ist, gilt $\psi(\omega)^{2^{p-1}} = -1_R \neq 1_R$, und somit ist die Ordnung von $\psi(\omega)$ gleich 2^p. In $E(R)$ gibt es also mindestens 2^p verschiedene Elemente, und wegen $E(R) \subset R \setminus \{0_R\}$ folgt $q^2 - 1 = \#(R) - 1 \geq 2^p$. Also gilt $q^2 \geq 2^p + 1 > 2^p - 1 = M(p)$.
(c) Für jeden Primteiler q von $M(p)$ gilt nach (c): Es ist $q > \sqrt{M(p)}$. Also ist $M(p)$ eine Primzahl.

(2) Es gelte: $M := M(p) = 2^p - 1$ ist eine Primzahl.
(a) Für jedes $j \in \{1, 2, \ldots, M-1\}$ ist die ganze Zahl

$$\binom{M}{j} = \frac{M(M-1)\cdots(M-j+1)}{j!}$$

durch M teilbar, weil auf der rechten Seite der Zähler durch die Primzahl M teilbar ist, aber nicht der Nenner. Also gilt

$$\begin{aligned} 2^{(M-1)/2}\sqrt{2}\cdot\tau^M &= \left(\sqrt{2}\cdot\tau\right)^M = \left(1+\sqrt{3}\right)^M = \sum_{j=0}^{M}\binom{M}{j}\sqrt{3}^j = \\ &= \sum_{i=0}^{(M-1)/2}\binom{M}{2i}3^i + \sum_{i=0}^{(M-1)/2}\binom{M}{2i+1}3^i\sqrt{3} = \\ &= 1 + aM + bM\sqrt{3} + 3^{(M-1)/2}\sqrt{3} \end{aligned}$$

mit den ganzen Zahlen

$$a := \frac{1}{M}\sum_{i=1}^{(M-1)/2}\binom{M}{2i}3^i \quad \text{und} \quad b := \frac{1}{M}\sum_{i=0}^{(M-3)/2}\binom{M}{2i+1}3^i.$$

(b) Wegen $p \geq 3$ gilt $8 \mid 2^p$ und daher $M = 2^p - 1 \equiv -1 \equiv 7 \pmod 8$. Nach (11.4)(5) ist daher 2 ein quadratischer Rest modulo M, und somit liefert das Kriterium von Euler in (10.5)(1): Es gilt $2^{(M-1)/2} \equiv 1 \pmod M$. Weil p ungerade ist, gilt $M = 2^p - 1 \equiv (-1)^p - 1 \equiv -1 - 1 \equiv 1 \pmod 3$, und daher folgt mit Hilfe des quadratischen Reziprozitätsgesetzes (vgl. (11.6))

$$\begin{aligned} \left(\frac{3}{M}\right) &= (-1)^{(3-1)(M-1)/4}\left(\frac{M}{3}\right) = (-1)^{2^{p-1}-1}\left(\frac{M}{3}\right) = \\ &= -\left(\frac{M}{3}\right) \overset{(11.4)(1)}{=} -\left(\frac{1}{3}\right) = -1. \end{aligned}$$

Also ist 3 ein quadratischer Nichtrest modulo M, und daher liefert das Kriterium von Euler: Es ist $3^{(M-1)/2} \equiv -1 \pmod M$.
(c) Nach (b) gibt es ganze Zahlen c und d mit $2^{(M-1)/2} = 1 + cM$ und mit $3^{(M-1)/2} = -1 + dM$. Damit gilt nach (a)

$$(1+cM)\sqrt{2}\cdot\tau^M = 1 + aM + bM\sqrt{3} + (-1+dM)\sqrt{3},$$

und daraus ergibt sich

$$(1+cM)\cdot\tau^{M+1} = \frac{\tau}{\sqrt{2}}\cdot\left(1 + aM + bM\sqrt{3} + (-1+dM)\sqrt{3}\right) =$$

$$= \frac{(1+\sqrt{3})(1-\sqrt{3})}{2} + \frac{1+\sqrt{3}}{2} \cdot M \cdot \left(a + (b+d)\sqrt{3}\right) =$$

$$= -1 + \frac{M}{2}\left(e + f\sqrt{3}\right)$$

mit

$$e := a + 3b + 3d \in \mathbb{Z} \quad \text{und} \quad f := a + b + d \in \mathbb{Z}.$$

Wegen $\tau^2 = \omega$ gilt somit

$$(1+cM)\cdot\omega^{2^{p-1}} = (1+cM)\cdot\tau^{2^p} = (1+cM)\cdot\tau^{M+1} = -1 + \frac{M}{2}\left(e+f\sqrt{3}\right),$$

und wegen $\omega \cdot \overline{\omega} = 1$ folgt daraus

$$2(1+cM)\cdot\omega^{2^{p-2}} = \left((1+cM)\cdot\omega^{2^{p-1}}\right)\cdot\left(2\,\overline{\omega}^{2^{p-2}}\right) =$$

$$= \left(-1 + \frac{M}{2}\left(e+f\sqrt{3}\right)\right)\cdot 2\,\overline{\omega}^{2^{p-2}} = -2\,\overline{\omega}^{2^{p-2}} + M\left(e+f\sqrt{3}\right)\cdot\overline{\omega}^{2^{p-2}}.$$

Also gilt

$$2a_{p-1} \overset{(0)}{=} 2\omega^{2^{p-2}} + 2\overline{\omega}^{2^{p-2}} = -2cM\cdot\omega^{2^{p-2}} + M\left(e+f\sqrt{3}\right)\cdot\overline{\omega}^{2^{p-2}} = xM$$

mit

$$x := -c\cdot\omega^{2^{p-2}} + \left(e+f\sqrt{3}\right)\cdot\overline{\omega}^{2^{p-2}} \in \mathbb{Z}[\sqrt{3}].$$

Es existieren ganze Zahlen g und h mit $x = g + h\sqrt{3}$, und damit gilt

$$2a_{p-1} = gM + hM\sqrt{3}.$$

Da $\sqrt{3}$ irrational ist, ist darin $h = 0$, also gilt $2a_{p-1} = gM$. Damit ist gezeigt, daß a_{p-1} durch $M = M(p)$ teilbar ist.

(11.23) Bemerkung: Der erste Teil des Beweises in (11.22) stammt aus Bruce [16]; der zweite Teil läßt sich kürzer formulieren, wenn man einige einfache Tatsachen aus der Algebraischen Zahlentheorie ausnützt (vgl. Rosen [93]). Es gibt noch andere Beweise des Satzes von Lucas und Lehmer: Der Beweis in Sierpiński [104], Kap. X, § 2, ist im wesentlichen der Beweis von Lehmer in [61]; lesenswert ist auch der Beweis in Kranakis [58], Abschnitt 2.9.

(11.24) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion zur Berechnung von Jacobi-Symbolen mit dem in (11.18) beschriebenen Algorithmus, die außerdem noch abzählt, wie oft im Schritt (JS8) das quadratische Reziprozitätsgesetz verwendet wird, und vergleiche mit der in (11.19)(2) angegebenen Abschätzung.

Aufgabe 2: (1) Es sei $a \in \mathbb{Z}$, und es sei $m \in \mathbb{N}$ ungerade. G. Eisenstein gab 1844 in [30] das folgende Verfahren zur Berechnung des Jacobi-Symbols $(a \mid m)$ an:

Man setzt $x_0 := a$ und $x_1 := m$ und ermittelt Zahlen $q_0, q_1, \ldots, q_{n-1} \in \mathbb{N}_0$, $x_2, x_3, \ldots, x_n \in \mathbb{N}$ und $\varepsilon_2, \varepsilon_3, \ldots, \varepsilon_n \in \{1, -1\}$ mit

$$\begin{aligned} x_0 &= q_0 x_1 + \varepsilon_2 x_2, \\ x_1 &= q_1 x_2 + \varepsilon_3 x_3, \\ &\vdots \qquad\qquad \vdots \\ x_{n-2} &= q_{n-2} x_{n-1} + \varepsilon_n x_n, \\ x_{n-1} &= q_{n-1} x_n, \end{aligned}$$

wobei $x_2, x_3, \ldots, x_n$ ungerade sind und $x_1 > x_2 > \cdots > x_{n-1} > x_n$ gilt. Wenn $x_n > 1$ ist, so ist $(q \mid m) = 0$. Wenn $x_n = 1$ ist, so setzt man für jedes $i \in \{0, 1, \ldots, n-2\}$

$$\delta_i := \begin{cases} -1, & \text{falls } x_{i+1} \equiv 3 \pmod 4 \text{ und } \varepsilon_{i+2} x_{i+2} \equiv 3 \pmod 4 \text{ gilt,} \\ 1, & \text{falls } x_{i+1} \equiv 1 \pmod 4 \text{ oder } \varepsilon_{i+2} x_{i+2} \equiv 1 \pmod 4 \text{ gilt,} \end{cases}$$

und erhält

$$\left(\frac{a}{m}\right) = \prod_{i=0}^{n-2} \delta_i.$$

(2) Man überlege sich, daß dieses Verfahren wirklich für jedes $a \in \mathbb{Z}$ und jedes ungerade $m \in \mathbb{N}$ das Jacobi-Symbol $(a \mid m)$ berechnet.
(3) Man schreibe eine MuPAD-Funktion, die zu ganzen Zahlen a und ungeraden natürlichen Zahlen m das Jacobi-Symbol $(a \mid m)$ berechnet und dabei das Verfahren aus (1) verwendet. Man schreibe diese Funktion so, daß darin auch gezählt wird, wie oft sie jeweils das quadratische Reziprozitätsgesetz verwendet, und vergleiche mit dem Verfahren aus (11.18) (vgl. Aufgabe 1).

Aufgabe 3 (T. Pepin 1878): Es sei n eine natürliche Zahl.
(1) Man beweise: Ist die n-te Fermat-Zahl $F(n) = 2^{2^n} + 1$ eine Primzahl, so ist 3 ein quadratischer Nichtrest modulo $F(n)$, und daher gilt

$$3^{(F(n)-1)/2} \equiv -1 \pmod{F(n)}.$$

(2) Man beweise: Gilt $3^{(F(n)-1)/2} \equiv -1 \pmod{F(n)}$, so ist $F(n)$ eine Primzahl. (Dazu ermittle man die Ordnung der Restklasse $[3]_{F(n)}$ in der Gruppe $E(\mathbb{Z}/F(n)\mathbb{Z})$).

Aufgabe 4: In (5.5) wurde erwähnt, daß es zu jeder positiven reellen Zahl M eine Primzahl p gibt, für die gilt: Die kleinste positive Primitivwurzel $g(p)$ modulo p ist größer als M. Der in dieser Aufgabe angedeutete Beweis stammt von K. Kearns (vgl. [52]); darin wird der Primzahlsatz von P. G. L. Dirichlet (1811

bis 1871) verwendet: Zu jeder natürlichen Zahl m und jeder ganzen Zahl a mit $\mathrm{ggT}(a,m) = 1$ gibt es unendlich viele Primzahlen p mit $p \equiv a \pmod{m}$. (Zum Beweis vergleiche man etwa den Abschnitt 1.6 des Buchs [17] von J. Brüdern).

Es sei M eine positive reelle Zahl, es seien $q_1, q_2, \ldots, q_n$ die ungeraden Primzahlen $\leq M$. Aus dem Primzahlsatz von Dirichlet folgt: Es gibt eine natürliche Zahl k, für die $p := 1 + 8q_1q_2\cdots q_n \cdot k$ eine Primzahl ist. Man beweise der Reihe nach:

(a) 2 und $q_1, q_2, \ldots, q_n$ sind quadratische Reste modulo p.

(b) Jede natürliche Zahl $\leq M$ ist ein quadratischer Rest modulo p.

(c) Für jede positive Primitivwurzel g modulo p gilt $g > M$.

Bemerkung: Man braucht hier übrigens nicht den Primzahlsatz von Dirichlet in seiner vollen Allgemeinheit. Hier benötigt man nur den Spezialfall: Zu jedem $m \in \mathbb{N}$ gibt es unendlich viele Primzahlen p mit $p \equiv 1 \pmod{m}$. Einfache Beweise hierfür oder besser Beweise, die einfacher als ein Beweis des vollen Primzahlsatzes von Dirichlet sind, findet man im zweiten Kapitel des Buchs [89] von P. Ribenboim und in der Arbeit [75] von I. Niven und B. Powell.

Aufgabe 5: Mit dem in Aufgabe 4 angegebenen Verfahren finde man Primzahlen p, für die die kleinste positive Primitivwurzel $g(p)$ modulo p größer als 50, größer als 100, größer als 200 ist.

Aufgabe 6: Das Kriterium von Euler in (10.5) führt direkt zu einem Primzahltest, der 1977 von R. Solovay und V. Strassen in [105] angegeben wurde. Von diesem Test handelt diese Aufgabe.

(1) Es sei $m \geq 3$ eine ungerade natürliche Zahl, und es seien

$$E(m) := \{a \in \mathbb{Z} \mid 0 \leq a \leq m-1;\ \mathrm{ggT}(a,m) = 1\} \quad \text{und}$$
$$A(m) := \left\{a \in E(m) \mid a^{(m-1)/2} \equiv \left(\frac{a}{m}\right) \pmod{m}\right\}.$$

Das Kriterium von Euler besagt: Ist m eine Primzahl, so ist $A(m) = E(m)$. Die nächsten beiden Aussagen zeigen: Ist m keine Primzahl, so ist $A(m)$ eine echte Teilmenge von $E(m)$. Man beweise:

(a) Wenn m durch das Quadrat einer Primzahl p teilbar ist, so ist

$$b := 1 + \frac{m}{p} \in E(m) \setminus A(m).$$

(b) Ist $m = p_1p_2\cdots p_r$ mit $r \geq 2$ paarweise verschiedenen Primzahlen p_1, $p_2, \ldots, p_r$ und ist $z \in \mathbb{Z}$ ein quadratischer Nichtrest modulo p_1, so gibt es ein $b \in \{0, 1, \ldots, m-1\}$ mit

$$b \equiv z \pmod{p_1} \quad \text{und} \quad b \equiv 1 \pmod{p_2p_3\cdots p_r},$$

und hierfür gilt $b \in E(m) \setminus A(m)$.

(2) Es sei $m \geq 3$ eine ungerade natürliche Zahl, die keine Primzahl ist. Dann ist nach (1) $A(m)$ eine echte Teilmenge von $E(m)$. Man zeige, daß

$$\{[a]_m \mid a \in A(m)\}$$

eine Untergruppe der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ ist, und folgere daraus: Es gilt

$$\#(A(m)) \leq \frac{1}{2}\#(E(m)).$$

(3) Man formuliere mit Hilfe von (1) und (2) einen stochastischen Primzahltest; dabei orientiere man sich an dem Algorithmus RABIN in (7.5). Man schreibe dazu eine MuPAD-Funktion.

Bemerkung: Leider ist der Primzahltest von Solovay und Strassen nicht dazu geeignet, den Primzahltest von Rabin zu ergänzen: Ist m eine starke Pseudoprimzahl zu einer Basis $b \in \mathbb{N}$, so liegt $b \bmod m$ in der Menge

$$A(m) = \left\{a \in E(m) \,\middle|\, a^{(m-1)/2} \equiv \left(\frac{a}{m}\right) \pmod m\right\}.$$

(Zum Beweis vergleiche man Koblitz [57], V, § 1). Wenn also der Primzahltest von Rabin eine Nichtprimzahl m als Primzahl deklariert, so tut dies auch der Primzahltest von Solovay und Strassen, falls in beiden Tests dieselben Zufallszahlen verwendet werden.

12 Ein Rechenverfahren

(12.1) In diesem Paragraphen wird die Aufgabe gelöst, zu einer ungeraden Primzahl p und zu einem quadratischen Rest $a \in \mathbb{Z}$ modulo p eine ganze Zahl x mit $x^2 \equiv a \pmod p$ zu berechnen. Einen Algorithmus, der dieses leistet, gab D. Shanks 1972 in [103] an; er nannte ihn RESSOL (= RESidue SOLver). Einen Vorläufer dieses Algorithmus publizierte A. Tonelli bereits im Jahr 1891 in [108]. Der Algorithmus RESSOL benötigt einen quadratischen Nichtrest z modulo der Primzahl p, auf die er angewandt wird. Daher muß man sich zuerst überlegen, wie man ein solches z findet.

(12.2) Satz: *Es sei p eine ungerade Primzahl, und es sei $z(p)$ der kleinste positive quadratische Nichtrest modulo p. Es gilt*

$$z(p) < 1 + \sqrt{p}.$$

Beweis: Für $z := z(p)$ gilt $2 \leq z \leq p-1$. Für $k := \lceil p/z \rceil$ gilt $k-1 < p/z \leq k$, wegen $p/z > 1$ ist daher $k \geq 2$, und es ist $p/z < k$, denn sonst wäre $p = zk$.