§ 16. Das Quadratische Reziprozitätsgesetz

16.1. 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.

16.2. 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 $\leq x$ bezeichnet. Nach dem Gaußschen Lemma ist $(\frac{a}{p}) = (-1)^m$ mit

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

Somit folgt

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

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

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

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

i) (1. Ergänzungssatz)

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

ii) (2. Ergänzungssatz)

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

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 15.3.

ii) Für $a = 2$ ergibt die Formel des Corollars 16.3

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

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.

16.5. 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*

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

Beweis. Nach dem Corollar 16.3 gilt $(\frac{a}{p}) = (-1)^m$ mit

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

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

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

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

16.6. 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 $(\frac{p}{q}) = (\frac{q}{p})$; falls aber $p \equiv q \equiv 3 \bmod 4$, so folgt $(\frac{p}{q}) = -(\frac{q}{p})$.

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

ii) Falls $p \not\equiv q \bmod 4$, gilt $p + q = 4r$ mit einer ganzen Zahl r. Wieder gilt nach Satz 16.5

$$\Big(\frac{r}{q}\Big) = \Big(\frac{r}{p}\Big)$$

und

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

sowie

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

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

Bemerkung. Wir haben hier das Reziprozitätsgesetz aus Satz 16.5 abgeleitet. Umgekehrt lässt sich Satz 16.5 auch leicht mithilfe des Reziprozitätsgesetzes beweisen (Übung).

Wir können nun einen Primzahltest von Pépin (1877) für Fermatzahlen beweisen.

16.7. Satz. *Die n-te Fermatzahl $F_n = 2^{2^n} + 1$ ist für $n \geqslant 1$ genau dann prim, wenn*

$$3^{(F_n-1)/2} \equiv -1 \bmod F_n.$$

In diesem Fall ist 3 eine Primitivwurzel modulo F_n.

Beweis. a) Die im Satz angegebenene Bedingung

$$3^{2^{2^n-1}} \equiv -1 \bmod F_n$$

sagt, dass die Restklasse von 3 in $(\mathbb{Z}/F_n)^*$ die Ordnung 2^{2^n} hat, d.h. $(\mathbb{Z}/F_n)^*$ hat mindestens $2^{2^n} = F_n - 1$ Elemente. Dies ist nur möglich, wenn F_n prim und 3 Primitivwurzel modulo F_n ist.

b) Wir zeigen jetzt, dass die Bedingung auch notwendig ist. Sei also F_n prim. Da $F_n \equiv 1 \bmod 4$, gilt

$$\Big(\frac{3}{F_n}\Big) = \Big(\frac{F_n}{3}\Big) = \Big(\frac{2}{3}\Big) = -1.$$

Dabei wurde $F_n \equiv 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \equiv 2 \bmod 3$ benutzt. Aus dem Euler-Kriterium folgt nun

$$3^{(F_n-1)/2} \equiv -1 \bmod F_n, \quad \text{q.ed.}$$

16.8. Satz. *Jeder mögliche Primteiler p von F_n, $n \geqslant 5$, hat die Gestalt*

$$p = k \cdot 2^{n+2} + 1$$

mit einer ganzen Zahl k.

Beweis. Aus $p \mid F_n = 2^{2^n} + 1$ folgt

$$2^{2^n} \equiv -1 \bmod p.$$

Daraus folgt, dass das Element 2 in $(\mathbb{Z}/p)^*$ die Ordnung 2^{n+1} hat. Daraus folgt bereits $2^{n+1} \mid p-1$, d.h. $p = h \cdot 2^{n+1} + 1$ mit einer ganzen Zahl h. Nach dem zweiten Ergänzungssatz ist nun

$$\Big(\frac{2}{p}\Big) = 1,$$

d.h. es gibt eine ganze Zahl x mit $x^2 \equiv 2 \bmod p$. Die Ordnung von x in $(\mathbb{Z}/p)^*$ ist 2-mal die Ordnung von 2 in $(\mathbb{Z}/p)^*$, d.h. $2^{n+2} \mid p-1$, d.h.

$$p = k \cdot 2^{n+2} + 1 \quad \text{mit einer ganzen Zahl } k, \quad \text{q.e.d.}$$

Beispiel. Jeder Primteiler von $F_5 = 2^{32} + 1$ hat die Gestalt $p = k \cdot 2^7 + 1 = 128k + 1$. Für $k = 1, 2, 3, 4, 5, \ldots$ ist dies gleich

$$129, \quad 257, \quad 385, \quad 513, \quad 641, \quad \ldots$$

Davon sind 129, 385, 513 nicht prim. Ebenso scheidet $257 = F_3$ als Teiler von F_5 aus, da die Fermatzahlen paarweise teilerfremd sind. Die erste Möglichkeit, die man testen muss, ist also $p = 641$. Tatsächlich geht die Division $F_5/641 = 6700417$ auf, d.h. F_5 ist nicht prim, was schon Euler festgestellt hat.

16.9. 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

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

Das Jacobi-Symbol genügt folgenden Rechenregeln:

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

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

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

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

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

(1) 1. Ergänzungssatz:

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

(2) 2. Ergänzungssatz:

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

(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)

16.11. 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

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

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

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

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:

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

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.

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