Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 8

Im nächsten Lemma verwenden wir folgende Notation:

Zu einer ungeraden Primzahl p und einer Zahl $k \in \mathbb{Z}$ sei

$$S(k,p) = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ki}{p} \right\rfloor .$$

LEMMA 8.1. *Sei p eine ungerade Primzahl und $k \in \mathbb{Z}$ kein Vielfaches von p. Dann gelten folgende Aussagen.*

(1) *Es ist $\epsilon_i = (-1)^{\left\lfloor \frac{2ki}{p} \right\rfloor}$, wobei ϵ_i wie im Gaußschen Vorzeichenlemma (Lemma 7.8) definiert ist.*
(2) $\left(\frac{k}{p}\right) = (-1)^{S(2k,p)}$.
(3) *Ist k ungerade, so ist $\left(\frac{k}{p}\right) = (-1)^{S(k,p)}$.*

Beweis. (1). Wir schreiben

$$\left\lfloor \frac{2ki}{p} \right\rfloor = \left\lfloor 2\left\lfloor \frac{ki}{p} \right\rfloor + 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor = 2\left\lfloor \frac{ki}{p} \right\rfloor + \left\lfloor 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor .$$

Damit ist $\left\lfloor \frac{2ki}{p} \right\rfloor$ gerade genau dann, wenn $\left\lfloor 2(\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor) \right\rfloor = 0$ ist. Dies bedeutet $\frac{ki}{p} - \left\lfloor \frac{ki}{p} \right\rfloor < \frac{1}{2}$, was wiederum zu $ki - p\left\lfloor \frac{ki}{p} \right\rfloor < p/2$ äquivalent ist. Der Term $ki - p\left\lfloor \frac{ki}{p} \right\rfloor$ ist der Rest von ki bei Division durch p. Nach Definition ist ϵ_i genau dann 1, wenn dieser Rest $< p/2$ ist.

(2). Aus Teil (1) und dem Gaußschen Vorzeichenlemma (Lemma 7.8) folgt wegen (mit $t = \frac{p-1}{2}$)

$$\left(\frac{k}{p}\right) = \prod_{i=1}^{t} \epsilon_i = \prod_{i=1}^{t} (-1)^{\left\lfloor \frac{2ki}{p} \right\rfloor} = (-1)^{S(2k,p)}$$

die Behauptung.

(3). Sei nun k ungerade. Dann ist $(p+k)/2$ eine ganze Zahl. Unter Verwendung von Teil (2) erhält man

$$\left(\frac{2}{p}\right)\left(\frac{k}{p}\right) = \left(\frac{2k}{p}\right) = \left(\frac{2(p+k)}{p}\right) = \left(\frac{(p+k)/2}{p}\right) = (-1)^{S(p+k,p)} .$$

Für den Exponenten rechts gilt

$$S(p+k,p) = \sum_{i=1}^{t} \left\lfloor \frac{i(p+k)}{p} \right\rfloor = \sum_{i=1}^{t} \left\lfloor \frac{ik}{p} \right\rfloor + \sum_{i=1}^{t} i = S(k,p) + \frac{(t+1)t}{2} .$$

Wegen $\frac{p^2-1}{8} = \frac{(p+1)}{2}\frac{(p-1)}{2}\frac{1}{2} = \frac{(t+1)t}{2}$ folgt nach dem zweitem Ergänzungssatz (Satz 7.9) die Identität $\left(\frac{2}{p}\right) = (-1)^{\frac{(t+1)t}{2}}$. Man kann daher in der Gesamtgleichungskette

$$\begin{aligned}\left(\frac{2}{p}\right)\left(\frac{k}{p}\right) &= (-1)^{S(p+k,p)} = (-1)^{S(k,p)+\frac{(t+1)t}{2}} \\ &= (-1)^{S(k,p)}(-1)^{\frac{(t+1)t}{2}} = (-1)^{S(k,p)}\left(\frac{2}{p}\right)\end{aligned}$$

kürzen und erhält die Aussage. □

Satz 8.2. *(Quadratisches Reziprozitätsgesetz) Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{wenn} \quad p = q = 3 \mod 4 \\ 1 & \text{sonst.} \end{cases}$$

Beweis. Sei $t = \frac{p-1}{2}$ und $u = \frac{q-1}{2}$. Nach Teil (3) des Lemmas 8.1 gilt $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$, so dass also $tu = S(p,q) + S(q,p)$ zu zeigen ist. Betrachte

$$M = \{qi - pj : 1 \le i \le t,\, 1 \le j \le u\}.$$

Diese Menge besitzt tu Elemente, und $0 \notin M$, da ja p und q teilerfremd sind. Es seien M_- die negativen Elemente aus M und M_+ die positiven Elemente aus M. Es ist $qi - pj > 0$ genau dann, wenn $\frac{qi}{p} > j$ ist, was genau für $1 \le j \le \lfloor \frac{qi}{p} \rfloor$ der Fall ist. Zu jedem i, $1 \le i \le t$, gibt es also genau $\lfloor \frac{qi}{p} \rfloor$ Elemente in M_+. Damit hat M_+ genau $\sum_{i=1}^{t} \lfloor \frac{qi}{p} \rfloor = S(q,p)$ Elemente. Die entsprechende Überlegung liefert, dass M_- genau $S(p,q)$ Elemente besitzt, woraus

$$tu = |M| = |M_+| + |M_-| = S(q,p) + S(p,q)$$

folgt. □

Das quadratische Reziprozitätsgesetz kann man auch so formulieren: Sind p und q zwei verschiedene ungerade Primzahlen, so gilt:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{wenn } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{sonst.} \end{cases}$$

Damit kann man die Berechnung von $\left(\frac{p}{q}\right)$ auf die Berechnung von $\left(\frac{q}{p}\right)$ zurückführen. Darauf beruht der folgende Algorithmus.

Bemerkung 8.3. Seien p und q ungerade verschiedene Primzahlen, und man möchte $\left(\frac{p}{q}\right)$ berechnen, also herausfinden, ob p ein quadratischer Rest modulo q ist oder nicht. Ist $p > q$, so berechnet man zuerst den Rest $p \mod q$, und ersetzt p durch den kleineren Rest, der natürlich keine Primzahl sein muss. Ist hingegen $p < q$, so berechnet man die Reste von p und q modulo 4

und kann dann mittels dem quadratischen Reziprozitätsgesetz $\left(\frac{p}{q}\right)$ auf $\left(\frac{q}{p}\right)$ zurückführen. In beiden Fällen kommt man also auf eine Situation, wo $\left(\frac{k}{q}\right)$ zu berechnen ist, wo q eine ungerade Primzahl ist und $k < q$ beliebig.

Sei $k = 2^\alpha \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von k. Dann ist nach der Multiplikativität des Legendre-Symbols (Lemma 7.3)

$$\left(\frac{k}{q}\right) = \left(\frac{2^\alpha}{q}\right) \cdot \left(\frac{p_1^{\alpha_1}}{q}\right) \cdots \left(\frac{p_r^{\alpha_r}}{q}\right) = \left(\frac{2}{q}\right)^\alpha \cdot \left(\frac{p_1}{q}\right)^{\alpha_1} \cdots \left(\frac{p_r}{q}\right)^{\alpha_r} .$$

Jetzt kann $\left(\frac{2}{q}\right)$ nach dem 2. Ergänzungsgesetz (Satz 7.9) berechnet und die $\left(\frac{p_i}{q}\right)$ können für $i = 1, \ldots, r$ nach dem gleichen Verfahren auf die Berechnung von $\left(\frac{q}{p_i}\right)$ zurückgeführt werden (von den Exponenten α, α_i kommt es nur auf die Parität an). Bei diesem Verfahren werden natürlich die Nenner (und damit auch die Zähler) in den Legendre-Symbolen kleiner, so dass man schließlich das Resultat erhält.

Beispiel 8.4. Man möchte entscheiden, ob die Gleichung

$$x^2 = 10 \mod 13$$

eine Lösung besitzt. Dazu berechnet man

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) .$$

Der erste Faktor

$$\left(\frac{2}{13}\right)$$

lässt sich mit Hilfe des zweiten Ergänzungssatzes zu -1 bestimmen, weil $13 \mod 8 = 5$ und $p = 5 \mod 8$ ergibt das Vorzeichen -1.

Um den zweiten Faktor zu berechnen, wendet man das Reziprozitätsgesetz an:

$$\left(\frac{5}{13}\right) = + \left(\frac{13}{5}\right) ,$$

weil $5 \mod 4 = 1$ gilt. $13 \mod 4$ braucht gar nicht mehr berechnet zu werden, da es ausreicht, dass hier 5 oder 13 modulo 4 den Rest 1 lässt, damit das Vorzeichen + ist. Jetzt nutzt man, dass $13 = 3 \mod 5$ ist. Man schreibt:

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) .$$

Wiederum wendet man hier das Quadratische Reziprozitätsgesetz an: Es ist

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 ,$$

da $5 \mod 4 = 1$ ist und da $2 = -1$ kein Quadrat modulo 3 ist.

Setzt man nun beide Faktoren zusammen, so ergibt sich folgendes Resultat:

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1) \cdot (-1) = 1 .$$

Und damit weiß man, dass die obige Gleichung eine Lösung besitzt. (Die beiden Lösungen lauten 6 und 7. Auf dieses Ergebnis kommt man leider nur durch Probieren. Hat man aber eine Lösung, z.B. die 6, so berechnet man die zweite Lösung, indem man das additive Inverse im Körper $Z \mod 13$ bestimmt $(13 - 6 = 7)$.

Beispiel 8.5. Man möchte entscheiden, ob die Gleichung

$$x^2 = 57 \mod 127$$

eine Lösung besitzt. Dazu berechnet man

$$\left(\frac{57}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{19}{127}\right)$$

und kann wie oben die beiden Faktoren mit dem Reziprozitätsgesetz weiter vereinfachen:

$$\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

und

$$\left(\frac{19}{127}\right) = -\left(\frac{127}{19}\right) = -\left(\frac{13}{19}\right) = -\left(\frac{19}{13}\right) = -\left(\frac{6}{13}\right)$$

$$= (-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1)(-1)\left(\frac{13}{3}\right) = (-1)(-1)\left(\frac{1}{3}\right) = (-1)(-1)1 = 1$$

Setzt man alles zusammen, so ergibt sich

$$\left(\frac{57}{127}\right) = -1$$

und damit die Erkenntnis, dass die obige Gleichung keine Lösung besitzt.

Zur Berechnung des Legendre-Symbols muss man die Primfaktorzerlegung der beteiligten Zahlen kennen, was für große Zahlen ein erheblicher Rechenaufwand darstellen kann. Die Einführung des Jacobi-Symbols erlaubt es, zu entscheiden, ob eine Zahl quadratischer Rest ist oder nicht, ohne Primfaktorzerlegungen zu kennen.

Definition 8.6. Für eine ungerade Zahl n und eine ganze Zahl k definiert man das *Jacobi-Symbol*, geschrieben $\left(\frac{k}{n}\right)$ (k *nach* n), wie folgt. Es sei $n = p_1 \cdots p_r$ die Primfaktorzerlegung von n. Dann setzt man

$$\left(\frac{k}{n}\right) := \left(\frac{k}{p_1}\right) \cdots \left(\frac{k}{p_r}\right) .$$

Carl Gustav Jacob Jacobi (1804-1851)

Im Fall $n = p$ eine ungerade Primzahl ist das Jacobi-Symbol nichts anderes als das Legendre-Symbol. Das Jacobi-Symbol ist also eine Verallgemeinerung des Legendre-Symbols. Es ist aber zu beachten, dass die inhaltliche Definition des Legendre-Symbols sich im allgemeinen nicht auf das Jacobi-Symbol überträgt. Das Jacobi-Symbol ist *nicht* genau dann 1, wenn k ein Quadrat modulo n ist.

LEMMA 8.7. *(Eigenschaften des Jacobi-Symbols) Seien k, k_1, k_2 ganze Zahlen und seien n, n_1, n_2 ungerade positive Zahlen. Dann gelten folgende Aussagen.*

(1) *Das Jacobi-Symbol $\left(\frac{k}{n}\right)$ hängt nur vom Rest $k \mod n$ ab.*
(2) *Es ist $\left(\frac{k_1k_2}{n}\right) = \left(\frac{k_1}{n}\right)\left(\frac{k_2}{n}\right)$.*
(3) *Es ist $\left(\frac{k}{n_1n_2}\right) = \left(\frac{k}{n_1}\right)\left(\frac{k}{n_2}\right)$.*

Beweis. Diese Aussagen folgen sofort aus der Definition des Jacobi-Symbols bzw. aus der Multiplikativität des Legendre-Symbols im Zähler. □

Für das Jacobi-Symbol gilt das quadratische Reziprozitäts mitsamt den Ergänzungssätzen.

SATZ 8.8. *(Quadratisches Reziprozitätsgesetz mit Jacobi-Symbol) Seien n und m positive ungerade Zahlen. Dann gelten folgende Aussagen.*

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

Beweis. Diese Aussagen werden in den Übungen bewiesen. □

BEMERKUNG 8.9. Seien n und m ungerade verschiedene Zahlen, und man möchte das Jacobi-Symbol $\left(\frac{n}{m}\right)$ berechnen (man berechnet im Allgemeinen nicht, ob n ein quadratischer Rest modulo m ist, dies ist nur dann der Fall, wenn m eine Primzahl ist). Durch die Restberechnung $n \mod m$ können wir

sofort annehmen, dass $n < m$ ist. Wir schreiben

$$n = 2^\alpha k\,,$$

wobei k ungerade sei. Dann gilt nach Lemma 8.7

$$\left(\frac{n}{m}\right) = \left(\frac{2^\alpha}{m}\right) \cdot \left(\frac{k}{m}\right) = \left(\frac{2}{m}\right)^\alpha \cdot \left(\frac{k}{m}\right)\,.$$

Hier kann, nach dem quadratischen Reziprozitätsgesetz für das Jacobi-Symbol (Satz 8.8) (und der Ergänzungssätze), $\left(\frac{2}{m}\right)$ berechnet werden und $\left(\frac{k}{m}\right)$ kann auf $\left(\frac{m}{k}\right)$ zurückgeführt werden. Bei diesem Verfahren werden natürlich die Nenner (und damit auch die Zähler) in den Jacobi-Symbolen kleiner, so dass man schließlich das Resultat erhält.

Abbildungsverzeichnis