Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Vorlesung 7

Quadratische Reste modulo einer Primzahl

Modulo 2 ist jede Zahl ein quadratischer Rest. Für ungerade Primzahlen kann man ebenfalls sofort eine Aussage über die Anzahl der Quadratreste machen.

SATZ 7.1. *Sei p eine ungerade Primzahl. Dann gibt es $\frac{p+1}{2}$ quadratische Reste modulo p und $\frac{p-1}{2}$ nichtquadratische Reste modulo p.*

Beweis. Zunächst ist 0 ein quadratischer Rest. Wir betrachten im folgenden nur noch die Einheiten in $\mathbb{Z}/(p)$ (also die von 0 verschiedenen Reste) und zeigen, dass es darunter gleich viele quadratische und nichtquadratische Reste gibt. Die Abbildung

$$(\mathbb{Z}/(p))^\times \longrightarrow (\mathbb{Z}/(p))^\times, \, x \longmapsto x^2,$$

ist offenbar ein Gruppenhomomorphismus der Einheitengruppe in sich selbst. Ein Element $k \in (\mathbb{Z}/(p))^\times$ ist genau dann ein Quadratrest, wenn es im Bild dieses Homomorphismus liegt. Nach dem Isomorphiesatz ist „Bild = Urbild modulo Kern“, so dass wir den Kern bestimmen müssen. Der Kern besteht aus allen Elementen x mit $x^2 = 1$. Dazu gehören 1 und -1, und diese beiden Elemente sind verschieden, da p ungerade ist. Aus der polynomialen Identität $x^2 - 1 = (x+1)(x-1)$ folgt, dass es keine weiteren Lösungen geben kann. Der Kern besteht also aus genau 2 Elementen und damit besteht das Bild aus $\frac{p-1}{2}$ Elementen. □

BEMERKUNG 7.2. Wenn zu einer Primzahl p eine primitive Einheit $g \in (\mathbb{Z}/(p))^\times$ vorliegt, so hat man einen Gruppenisomorphismus

$$(\mathbb{Z}/(p-1), 0, +) \longrightarrow \left((\mathbb{Z}/(p))^\times, 1, \cdot\right), \, i \longmapsto g^i.$$

Dabei entsprechen die Quadrate rechts denjenigen Elementen links, die ein Vielfaches der 2 sind. Bei p ungerade besitzt die Hälfte der Elemente links diese Eigenschaft. Insbesondere ist ein Element $k \in (\mathbb{Z}/(p))^\times$ genau dann ein Quadratrest, wenn es von der Form

$$k = g^{2j}$$

ist.

Definition 7.3. Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl $k \in \mathbb{Z}$ definiert man das *Legendre-Symbol*, geschrieben $\left(\frac{k}{p}\right)$ (sprich „k nach p“), durch

$$\left(\frac{k}{p}\right) := \begin{cases} 1, \text{ falls } k \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, \text{ falls } k \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Insbesondere ist $\left(\frac{k}{p}\right) = \left(\frac{k \mod p}{p}\right)$. Die Werte des Legendre-Symbols, also 1 und -1, kann man dabei in $\mathbb{Z}$, in $\mathbb{Z}^\times$ oder in $(\mathbb{Z}/(p))^\times$ auffassen. Für Vielfache von p definierte man manchmal das Legendre-Symbol ebenfalls, und zwar mit dem Wert 0.

Lemma 7.4. *Sei p eine ungerade Primzahl. Dann ist die Abbildung*

$$(\mathbb{Z}/(p))^\times \longrightarrow \{\pm 1\},\ k \longmapsto \left(\frac{k}{p}\right),$$

ein Gruppenhomomorphismus.

Beweis. Die Quadrate bilden offenbar eine Untergruppe in der Einheitengruppe $(\mathbb{Z}/(p))^\times$, die nach Satz 7.1 den Index 2 besitzt. Daher ist

$$(\mathbb{Z}/(p))^\times / \text{Quadrate} \cong \mathbb{Z}/(2) \cong \{\pm 1\}$$

und die Restklassenabbildung ist gerade die Abbildung auf das Legendre-Symbol. □

Die folgende Aussage heißt das *Euler-Kriterium* für quadratische Reste.

Satz 7.5. *Sei p eine ungerade Primzahl. Dann gilt für eine zu p teilerfremde Zahl k die Gleichheit*

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

Beweis. Es ist $\left(k^{\frac{p-1}{2}}\right)^2 = k^{p-1} = 1$ nach Lemma 4.6. Daher ist

$$k^{\frac{p-1}{2}} = \pm 1.$$

Die Abbildung

$$(\mathbb{Z}/(p))^\times \longrightarrow \{\pm 1\},\ k \longmapsto k^{\frac{p-1}{2}},$$

ist (wie jedes Potenzieren) ein Gruppenhomomorphismus. Die Quadrate werden darunter auf 1 abgebildet, da für $k = x^2$ die Gleichheit

$$k^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$$

gilt. Da nach Satz 5.11 die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch ist, muss diese Abbildung surjektiv sein (sonst hätte jedes Element eine kleinere Ordnung). Damit muss diese Abbildung mit der durch das Legendre-Symbol gegebenen übereinstimmen. □

Das Quadratische Reziprozitätsgesetz

Seien p und q zwei ungerade Primzahlen. Dann kann p ein quadratischer Rest modulo q sein (oder nicht) und q kann ein quadratischer Rest modulo p sein, oder nicht. Das Quadratische Reziprozitätsgesetz, das von Euler entdeckt und von Gauß erstmals bewiesen wurde, behauptet nun, dass es einen direkten Zusammenhang zwischen diesen beiden Eigenschaften gibt. Es erlaubt weiterhin mit den beiden unten genannten Ergänzungssätzen algorithmisch zu entscheiden, ob eine Zahl ein quadratischer Rest oder ein nichtquadratischer Rest ist.

Carl Friedrich Gauss (1777-1855)

SATZ 7.6. *Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:*

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

Beweis. Dies wird weiter unten nach einigen Vorbereitungen bewiesen. Die zweite Gleichung ist elementar. □

In Worten: Wenn p und q beide den Rest 3 modulo 4 haben, so ist p modulo q ein quadratischer Rest genau dann, wenn q modulo p ein nichtquadratischer Rest ist. In allen anderen Fällen ist p modulo q ein quadratischer Rest genau dann, wenn q modulo p ein quadratischer Rest ist.

BEISPIEL 7.7. Betrachten wir die beiden Primzahlen 11 und 19, die beide modulo 4 den Rest 3 haben. Es ist $19 = 8$ modulo 11 und dies ist nach Beispiel 6.4 kein Quadratrest. Gemäß dem Reziprozitätsgesetz muss also 11 modulo 19 ein quadratischer Rest sein. In der Tat ist

$$7^2 \;=\; 49 \;=\; 11 \mod 19.$$

Betrachtet man hingegen die Primzahlen 11 und 13, so hat 11 modulo 4 den Rest 3 und 13 hat modulo 4 den Rest 1. Es ist $13 = 2 \mod 11$ ein nichtquadratischer Rest, und daher ist auch 11 ein nichtquadratischer Rest modulo 13.

Die beiden folgenden Sätze werden die Ergänzungssätze zum quadratischen Reziprozitätsgesetz genannt, da sie klären, wann die -1 und wann die 2 quadratische Reste sind. In der algorithmischen Bestimmung von Quadratresten sind diese beiden Fälle ebenfalls unerlässlich.

SATZ 7.8. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1\,, \text{ falls } p = 1 \mod 4\,, \\ -1\,, \text{ sonst (also bei } p = 3 \mod 4)\,. \end{cases}$$

Beweis. Die Gleichung von links und rechts wurde bereits in Satz 6.8 bewiesen. Die erste Gleichung ist auch ein Spezialfall von Satz 7.5 und die zweite Gleichung ist elementar. □

SATZ 7.9. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1\,, & \text{falls} \quad p = \pm 1 \mod 8\,, \\ -1 & \text{sonst} \quad (\text{also } p = \pm 3 \mod 8) \end{cases}.$$

Beweis. Dies wird weiter unten bewiesen. □

Die Elemente im Restklassenkörper $\mathbb{Z}/(p)$ werden meist durch die Zahlen von 0 bis $p-1$ repräsentiert. Für das folgende Vorzeichenlemma von Gauß ist es sinnvoll, ein anderes Repräsentantensystem (für die von 0 verschiedenen Elemente) zu fixieren. Wir setzen $t = \frac{p-1}{2}$ und

$$S = S_- \cup S_+ \text{ mit } S_- = \{-t, -t+1, \ldots, -2, -1\} \text{ und } S_+ = \{1, 2, \ldots, t-1, t\}\,.$$

Wir unterteilen also die Einheitengruppe in eine positive und eine negative Hälfte. Dieses Repräsentantensystem ist dadurch ausgezeichnet, dass jedes Element durch das betragmäßig kleinste Element repräsentiert wird. Im folgenden Lemma betrachtet man zu einer zu p teilerfremden Zahl k die Menge der Vielfachen ik, $i = 1, \ldots, t$, in $\mathbb{Z}/(p)$ und schaut, ob sie in der negativen oder der positiven Hälfte liegen. Man definiert die sogenannten *Gaußschen Vorzeichen*

$$\epsilon_i = \epsilon_i(k) = \begin{cases} 1, \text{ falls } ik \in S_+\,, \\ -1, \text{ falls } ik \in S_-\,. \end{cases}$$

BEISPIEL 7.10. In $\mathbb{Z}/(11)$ ist $S_+ = \{1, 2, 3, 4, 5\}$ und $S_- = \{-1, -2, -3, -4, -5\}$. Für $k = 3$ muss man, um die Gaußschen Vorzeichen zu bestimmen, die ersten fünf Vielfachen berechnen und schauen, ob sie zur negativen oder zur positiven Hälfte gehören. Es ist

$$3 \in S_+,\ 6 = -5 \in S_-,\ 9 = -2 \in S_-,\ 12 = 1 \in S_+,\ 15 = 4 \in S_+\,,$$

die Vorzeichen sind also der Reihe nach

$$1, -1, -1, 1, 1\,.$$

Ihr Produkt ist 1, und mit dem folgenden Gaußschen Vorzeichenlemma folgt, dass 3 ein Quadratrest ist. In der Tat ist $3 = 5^2 \mod 11$.

Die folgende Aussage heißt *Gaußsches Vorzeichenlemma*.

LEMMA 7.11. *Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl k gilt mit den zuvor eingeführten Bezeichnungen*

$$\left(\frac{k}{p}\right) = \epsilon_1 \cdot \epsilon_2 \cdots \epsilon_t.$$

Beweis. Es sei $s_i \in S_+$ durch die Bedingung

$$ik = \epsilon_i s_i \mod p$$

festgelegt. Wir betrachten alle Vielfachen jk, $j \in S = (\mathbb{Z}/(p))^\times$. Die Menge all dieser Vielfachen ist selbst ganz S, da ja k eine Einheit und daher die Multiplikation mit k eine Bijektion ist. Es ist $(-i)k = -ik = -\epsilon_i s_i$ für $i \in S_+ = \{1, \ldots, t\}$. Daher ist $S_+ = \{1, \ldots, t\} = \{s_1, \ldots, s_t\}$. Deshalb gilt $t! = \prod_{i=1}^t s_i$ und somit

$$\begin{aligned} t!k^t &= \left(\prod_{i=1}^t i\right)\left(\prod_{i=1}^t k\right) \\ &= \prod_{i=1}^t ik \\ &= \prod_{i=1}^t \epsilon_i s_i \\ &= \left(\prod_{i=1}^t \epsilon_i\right)\left(\prod_{i=1}^t s_i\right) = \left(\prod_{i=1}^t \epsilon_i\right) t! \mod p. \end{aligned}$$

Durch kürzen mit $t!$ (das ist eine Einheit) ergibt sich

$$k^t = \prod_{i=1}^t \epsilon_i \mod p,$$

und das Euler-Kriterium, nämlich

$$k^t = k^{\frac{p-1}{2}} = \left(\frac{k}{p}\right) \mod p,$$

liefert das Ergebnis. □

Mit dem Gaußschen Vorzeichenlemma beweisen wir zunächst den zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz, der beschreibt, wann 2 ein quadratischer Rest ist.

SATZ 7.12. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1\,, & \textit{falls} \quad p = \pm 1 \mod 8\,, \\ -1 & \textit{sonst} \quad \textit{(also } p = \pm 3 \mod 8\textit{)} \end{cases}.$$

Beweis. Wir benutzen Lemma 7.11 und haben zu bestimmen, wie viele der Zahlen $2i$, $i = 1, \ldots, t = \frac{p-1}{2}$, in S_- liegen. Nun ist $2i \in S_-$ genau dann, wenn $2i > \frac{p-1}{2}$ ist (alle zu betrachtenden Vielfachen von 2 sind kleiner als p). Dies ist äquivalent zu $i > \frac{p-1}{4}$ und wir haben das kleinste i mit dieser Eigenschaft zu finden. Ist $p-1$ ein Vielfaches von 4, so ist $\frac{p-1}{4}+1$ das kleinste i und insgesamt gibt es in diesem Fall

$$\frac{p-1}{2} - \left(\frac{p-1}{4} + 1\right) + 1 = \frac{p-1}{4}$$

solche i. Diese Anzahl ist bei $p = 1 \mod 8$ gerade und bei $p = 5 \mod 8$ ungerade, was das Ergebnis in diesen Fällen ergibt.

Sei also nun $p = 3, 7 \mod 8$ bzw. $p = 3 \mod 4$. Dann ist das kleinste i derart, dass $2i > \frac{p-1}{2}$ ist, gleich $\frac{p-1}{4} + \frac{1}{2}$, und es gibt insgesamt

$$\frac{p-1}{2} - \left(\frac{p-1}{4} + \frac{1}{2}\right) + 1 = \frac{p-1}{4} + \frac{1}{2} = \frac{p+1}{4}$$

solche i. Diese Anzahl ist bei $p = 3 \mod 8$ ungerade und bei $p = 7 \mod 8$ gerade, was die Behauptung in diesen Fällen ergibt. □

Abbildungsverzeichnis