

Zahlentheorie

Vorlesung 7

Für ungerade Primzahlen kann man sofort eine Aussage über die Anzahl der Quadratreste machen.

SATZ 7.1. (*Anzahl von Quadratresten*) 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 genau aus 2 Elementen und damit besteht das Bild aus $(p - 1)/2$ Elementen. \square

DEFINITION 7.2. 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 $\left(\frac{k}{p}\right) = \left(\frac{k \bmod p}{p}\right)$. 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.

LEMMA 7.3. (*Multiplikativität des Legendre-Symbols*) 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 Einheitsgruppe $(\mathbb{Z}/(p))^\times$, 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. \square

SATZ 7.4. (Euler-Kriterium) Sei p eine ungerade Primzahl. Dann gilt für eine zu p teilerfremde Zahl k die Gleichheit

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

Beweis. Es ist $(k^{\frac{p-1}{2}})^2 = k^{p-1} = 1$ nach Fermat (Satz 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 dem 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. \square

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 quadratischer Nichtrest ist.



Carl Friedrich Gauss (1777-1855)

SATZ 7.5. (*Quadratisches Reziprozitätsgesetz*) Seien p und q zwei verschiedene ungerade Primzahlen. Dann gilt:

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

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

Die beiden folgenden Sätze werden die Ergänzungssätze zum quadratischen Reziprozitätsgesetz genannt.

SATZ 7.6. (*1. Ergänzungssatz zum quadratischen Reziprozitätsgesetz*) Für eine ungerade Primzahl p gilt:

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

Beweis. Die Gleichung von links und rechts wurde bereits im Satz 6.7 bewiesen. Die erste Gleichung ist auch ein Spezialfall des Eulerschen Kriteriums (Satz 7.4) und die zweite Gleichung ist elementar. \square

SATZ 7.7. (*2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz*) Für eine ungerade Primzahl p gilt:

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

Beweis. Dies wird weiter unten bewiesen. \square

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

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

Wir unterteilen also die Einheitengruppe in eine positive und eine negative Hälfte. Dieses Repräsentantensystem ist dadurch ausgezeichnet, dass jedes Element durch das betragsmäßig kleinste Element repräsentiert wird. Im folgenden Lemma betrachtet man zu einer zu p teilerfremden Zahl k die Menge der Vielfachen

$$ik, i = 1, \dots, t,$$

in $\mathbb{Z}/(p)$ und schaut, ob sie in der negativen oder der positiven Hälfte liegen. Man definiert die sogenannten Gaußschen Vorzeichen

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

LEMMA 7.8. (*Gaußsches Vorzeichenlemma*) Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl k gilt mit den soeben 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

$$ik = \epsilon_i s_i \pmod{p}$$

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 $i \in S_+ = \{1, \dots, t\}$. Daher ist $S_+ = \{1, \dots, t\} = \{s_1, \dots, s_t\}$. Deshalb gilt $t! = \prod_{i=1}^t s_i$ und somit

$$t!k^t = \left(\prod_{i=1}^t i\right)\left(\prod_{i=1}^t k\right) = \prod_{i=1}^t ik = \prod_{i=1}^t \epsilon_i s_i = \left(\prod_{i=1}^t \epsilon_i\right)\left(\prod_{i=1}^t s_i\right) = \left(\prod_{i=1}^t \epsilon_i\right)t! \pmod{p}.$$

Durch kürzen mit $t!$ (das ist eine Einheit) ergibt sich $k^t = \prod_{i=1}^t \epsilon_i \pmod{p}$, und das Eulersche Kriterium (Satz 7.4), nämlich $k^t = k^{\frac{p-1}{2}} = \left(\frac{k}{p}\right) \pmod{p}$, liefert das Ergebnis. \square

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

SATZ 7.9. (*2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz*) Für eine ungerade Primzahl p gilt:

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

Beweis. Wir benutzen das Gaußsche Vorzeichenlemma (Lemma 7.8) und haben zu bestimmen, wie viele der Zahlen $2i$, $i = 1, \dots, t = (p-1)/2$, in S_- liegen. Nun ist $2i \in S_-$ genau dann, wenn $2i > (p-1)/2$ ist (alle zu betrachtenden Vielfachen von 2 sind kleiner als p). Dies ist äquivalent zu $i > (p-1)/4$ und wir haben das kleinste i mit dieser Eigenschaft zu finden. Ist $p-1$ ein Vielfaches von 4, so ist $(p-1)/4 + 1$ das kleinste i und insgesamt gibt es in diesem Fall

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

solcher i . Diese Anzahl ist bei $p \equiv 1 \pmod{8}$ gerade und bei $p \equiv 5 \pmod{8}$ ungerade, was das Ergebnis in diesen Fällen ergibt.

Sei also nun $p \equiv 3, 7 \pmod{8}$ bzw. $p \equiv 3 \pmod{4}$. Dann ist das kleinste i derart, dass $2i > (p-1)/2$ ist, gleich $(p-1)/4 + 1/2$, 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 $p = 3 \pmod{8}$ ungerade und bei $p = 7 \pmod{8}$ gerade, was die Behauptung in diesen Fällen ergibt. \square

Abbildungsverzeichnis

Quelle = Carl Friedrich Gauss.jpg, Autor = Benutzer Bcrowell auf Commons, Lizenz = PD

2