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

Zahlentheorie

Vorlesung 6

Der Charakterisierungssatz für zyklische Einheitengruppen

Wir beenden zunächst unsere Überlegungen, wann die Einheitengruppe eines Restklassenringes von $\mathbb{Z}$ zyklisch ist.

LEMMA 6.1. *Die Einheitengruppe von $\mathbb{Z}/(2^r)$ ist nicht zyklisch für $r \geq 3$.*

Beweis. Bei $r = 3$ ist dies eine direkte Berechnung. Generell ist für $r \geq 3$ die Abbildung

$$(\mathbb{Z}/(2^r))^\times \longrightarrow (\mathbb{Z}/(8))^\times$$

surjektiv (da genau die ungeraden Elemente die Einheiten sind). Da eine Restklassengruppe einer zyklischen Gruppe wieder zyklisch ist, folgt, dass $(\mathbb{Z}/(2^r))^\times$ nicht zyklisch sein kann. □

Unser abschließendes Resultat ist nun der folgende Satz.

SATZ 6.2. *Die Einheitengruppe $(\mathbb{Z}/(n))^\times$ ist genau dann zyklisch, wenn*

$$n = 1, 2, 4, p^s, 2p^s$$

ist, wobei p eine ungerade Primzahl und $s \geq 1$ ist.

Beweis. In den beschriebenen Fällen ist die Einheitengruppe $(\mathbb{Z}/(n))^\times$ zyklisch aufgrund von Satz 5.11, Bemerkung 5.12 und der Isomorphie

$$(\mathbb{Z}/(2p^r))^\times \cong (\mathbb{Z}/(2))^\times \times (\mathbb{Z}/(p^r))^\times \cong (\mathbb{Z}/(p^r))^\times .$$

Sei also umgekehrt n mit der Eigenschaft gegeben, dass $(\mathbb{Z}/(n))^\times$ zyklisch sei. Es sei $n = 2^r \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ die kanonische Primfaktorzerlegung mit ungeraden Primzahlen $p_1, \ldots, p_k$ und $r_i \geq 1$, die nach dem Chinesischen Restsatz zur Isomorphie

$$(\mathbb{Z}/(n))^\times = (\mathbb{Z}/(2^r))^\times \times (\mathbb{Z}/(p_1^{r_1}))^\times \times (\mathbb{Z}/(p_2^{r_2}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times$$

führt. Da Restklassengruppen von zyklischen Gruppen wieder zyklisch sind, folgt nach Lemma 6.1, dass $r = 0, 1$ oder 2 ist. Ein Produkt von zyklischen Gruppen ist nur dann zyklisch, wenn die beteiligten Ordnungen paarweise teilerfremd sind. Die Ordnungen von $(\mathbb{Z}/(p_i^{r_i}))^\times$ sind aber gerade für p_i ungerade und $r_i \geq 1$, und die Ordnung von $(\mathbb{Z}/(2^r))^\times$ ist gerade für $r \geq 2$. Also ist $k \leq 1$. Bei $k = 1$ ist $r = 2$ nicht möglich. Bei $k = 0$ verbleiben die angeführten Fälle $n = 1, 2, 4$. □

Quadratische Reste

Wir wollen nun wissen, welche Zahlen k modulo einer fixierten Zahl n (häufig einer Primzahl) ein Quadrat sind, also eine Quadratwurzel besitzen. Man spricht von quadratischen Resten und nichtquadratischen Resten (häufig wird auch von quadratischen Nichtresten gesprochen).

Definition 6.3. Eine ganze Zahl k heißt *quadratischer Rest* modulo n, wenn es eine Zahl x gibt mit

$$x^2 = k \mod n\,.$$

Im anderen Fall heißt k ein *nichtquadratischer Rest* modulo n.

Eine Quadratzahl ist natürlich auch ein quadratischer Rest modulo jeder Zahl n. Umgekehrt ist eine Zahl, die selbst keine Quadratzahl ist, modulo gewisser Zahlen ein quadratischer Rest und modulo gewisser Zahlen ein nichtquadratischer Rest. Grundsätzlich kann man zu gegebenen k und n naiv testen, ob k ein quadratischer Rest ist oder nicht, indem man alle Reste quadriert und schaut, ob der durch k definierte Rest dabei ist. Die Frage nach den Quadratresten weist aber eine Reihe von Gesetzmäßigkeiten auf, die wir im folgenden kennen lernen werden und mit deren Hilfe man effektiver entscheiden kann, ob ein Quadratrest vorliegt oder nicht.

Beispiel 6.4. In $\mathbb{Z}/(11)$ sind die Zahlen $0, 1, 4, 9, 16 = 5, 25 = 3$ Quadratreste, die Zahlen $2, 6, 7, 8, 10$ sind nichtquadratische Reste.

Satz 6.5. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$ (die p_i seien also verschieden). Dann ist k genau dann Quadratrest modulo n, wenn k Quadratrest modulo $p_i^{r_i}$ ist für alle $i = 1, \ldots, s$.*

Beweis. Dies folgt unmittelbar aus Satz 4.13. □

Satz 6.6. *Sei p eine ungerade Primzahl und sei $k \in \mathbb{Z}/(p^r)$.*

(1) *Ist k teilerfremd zu p (also kein Vielfaches von p), dann ist k genau dann ein Quadratrest modulo p^r, wenn k ein Quadratrest modulo p ist.*
(2) *Ist $k = p^s u$ mit u teilerfremd zu p und $s < r$, so ist k genau dann ein Quadratrest modulo p^r, wenn s gerade und wenn u ein Quadratrest modulo p ist.*

Beweis. Die natürliche Abbildung

$$\mathbb{Z}/(p^r) \longrightarrow \mathbb{Z}/(p)$$

liefert sofort, dass ein Quadratrest modulo p^r auch ein Quadratrest modulo p ist. Wir zeigen zunächst die Umkehrung für Einheiten. Nach Lemma 5.9 ist die Abbildung

$$(\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

surjektiv und nach Satz 5.11 sind die beteiligten Gruppen zyklisch. D.h. ein Erzeuger wird auf einen Erzeuger abgebildet. Insbesondere kann man diese Gruppen so mit additiven zyklischen Gruppen identifizieren, dass der Homomorphismus die den additiven Erzeuger 1 auf die 1 schickt. Dies erreicht man, indem man im folgenden kommutativen Diagramm die Identifikation links mit einem primitiven Element $g \in \mathbb{Z}/(p^r)$ und rechts ebenfalls mit g (jetzt aufgefasst in $\mathbb{Z}/(p)$) stiftet.

$$\begin{array}{ccc} (\mathbb{Z}/(p^r))^\times & \longrightarrow & (\mathbb{Z}/(p))^\times \\ \cong \uparrow & & \uparrow \cong \\ \mathbb{Z}/(p^{r-1}(p-1)) & \longrightarrow & \mathbb{Z}/(p-1) \end{array} .$$

Wir schreiben die untere horizontale Abbildung, unter Verwendung des Chinesischen Restsatzes, als

$$\mathbb{Z}/(p^{r-1}) \times \mathbb{Z}/(p-1) \cong \mathbb{Z}/(p^{r-1}(p-1)) \longrightarrow \mathbb{Z}/(p-1) \text{ mit } 1 = (1,1) \longmapsto 1\,.$$

Da überdies p und $p-1$ teilerfremd sind, liegt hier insgesamt einfach die Projektion $(b_1, b_2) \mapsto b_2$ vor.

Die Voraussetzung, dass k modulo p ein Quadratrest ist, übersetzt sich dahingehend, dass das k entsprechende Element (sagen wir $b = (b_1, b_2)$) in $\mathbb{Z}/(p-1)$ ein Vielfaches von 2 ist. D.h. die zweite Komponente, also b_2, ist ein Vielfaches der 2. Da modulo der ungeraden Zahl p^{r-1} jede Zahl ein Vielfaches von 2 ist (da 2 eine Einheit in $\mathbb{Z}/(p^{r-1})$ ist), ist auch die erste Komponente, also b_1, ein Vielfaches von 2 und so muss b insgesamt ein Vielfaches der 2 sein.

Sei nun $k = p^s u$, $1 \leq s \leq r-1$, und zunächst angenommen, dass k ein Quadrat ist. D.h wir können k als $k = x^2$ mit $x = p^t v$, schreiben, wobei v eine Einheit sei. Es ist also $p^s u = p^{2t} v^2$ in $\mathbb{Z}/(p^r)$ und es ist $2t < r$ (sonst steht hier 0). Durch Betrachten modulo p^s und modulo p^{2t} sieht man, dass $s = 2t$ sein muss. Insbesondere ist s gerade. Es gilt also $p^s u = p^s v^2 \mod p^r$ und somit können wir $p^s(u - v^2) = cp^r$ schreiben. Kürzen in $\mathbb{Z}$ ergibt $u - v^2 = cp^{r-s}$, also $u = v^2 \mod p$. Also ist u ein quadratischer Rest modulo p und nach dem ersten Teil auch modulo p^r.

Die Umkehrung von (2) ist nach der unter (1) bewiesenen Aussage klar. □

Satz 6.7. *Sei $p = 2$ und sei $k \in \mathbb{Z}/(2^r)$.*

(1) *Für $r = 2$ ist k genau dann quadratischer Rest, wenn $k = 0, 1 \mod 4$ ist.*
(2) *Für $r \geq 3$ und k ungerade ist k genau dann quadratischer Rest modulo 2^r, wenn $k = 1 \mod 8$ ist.*

Beweis. (1) ist trivial.

(2). In $\mathbb{Z}/(8)$ ist von den ungeraden Zahlen lediglich die 1 ein Quadrat, so dass der Ringhomomorphismus

$$\mathbb{Z}/(2^r) \longrightarrow \mathbb{Z}/(8)$$

für $r \geq 3$ zeigt, dass die numerische Bedingung notwendig ist. Sei diese umgekehrt nun erfüllt, also $a \in (\mathbb{Z}/(2^r))^\times$ mit $a = 1 \mod 8$. Dann kann man nach Bemerkung 5.12

$$a = \pm 5^i.$$

schreiben. Dies gilt aber auch modulo 8, woraus sofort folgt, dass i gerade und dass das Vorzeichen positiv ist. Dann ist $5^{i/2}$ eine Quadratwurzel von a in $\mathbb{Z}/(2^r)$. □

Wir werden uns im folgenden weitgehend darauf beschränken, welche Zahlen modulo einer Primzahl Quadratreste sind. Da allerdings die Primfaktorzerlegung einer größeren Zahl nicht völlig unproblematisch ist, müssen wir später auch Techniken entwickeln, die ohne Kenntnis der Primfaktorzerlegung auskommen. Direkt beantworten lässt sich die Frage, wann -1 ein Quadratrest modulo einer Primzahl ist.

Satz 6.8. *Sei p eine Primzahl. Dann gelten folgende Aussagen.*

Für $p = 2$ ist $-1 = 1$ ein Quadrat in $\mathbb{Z}/(2)$.

Für $p = 1 \mod 4$ ist -1 ein Quadrat in $\mathbb{Z}/(p)$.

Für $p = 3 \mod 4$ ist -1 kein Quadrat in $\mathbb{Z}/(p)$.

Beweis. Die erste Aussage ist klar, sei also p ungerade. Nach Satz 5.3 ist die Einheitengruppe zyklisch der geraden Ordnung $p - 1$. Identifiziert man $((\mathbb{Z}/(p))^\times, 1, \cdot)$ mit $(\mathbb{Z}/(p-1), 0, +)$, so entspricht -1 dem Element $\frac{p-1}{2}$, und -1 besitzt genau dann eine Quadratwurzel, wenn $\frac{p-1}{2}$ in $\mathbb{Z}/(p-1)$ ein Vielfaches von 2 ist. Dies ist aber genau dann der Fall, wenn $\frac{p-1}{2}$ selbst gerade ist, was zu $p = 1 \mod 4$ äquivalent ist. □