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

Zahlentheorie

Vorlesung 5

In diesem Abschnitt beschäftigen wir uns mit der Einheitengruppe der Restklassenringe $\mathbb{Z}/(n)$, also mit $(\mathbb{Z}/(n))^\times$. Ihre Anzahl wird durch die Eulersche Funktion φ ausgedrückt. Wir brauchen noch kurz einige Vorbereitungen über Polynomringe.

Satz 5.1. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a - a)Q(a) = 0\,.$$

Im Allgemeinen gibt es aufgrund Fakt eine Darstellung

$$P = (X - a)Q + R\,,$$

wobei $R = 0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R\,.$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X - a)Q$ ist. Also ist $X - a$ ein Linearfaktor von P. □

Korollar 5.2. *Sei K ein Körper und $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom (ungleich null) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X - a)$ nach Satz 5.1 und Q hat den Grad $d - 1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d - 1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b - a)$. Dies kann nur dann null sein, wenn einer der Faktoren null ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

Satz 5.3. *Sei $U \subseteq K^\times$ eine endliche Untergruppe der multiplikativen Gruppe eines Körpers K. Dann ist U zyklisch.*

Beweis. Sei $n = \mathrm{ord}(U)$ und $e = \exp(U)$ der Exponent dieser Gruppe. Dies bedeutet, dass alle Elemente $x \in U$ eine Nullstelle des Polynoms $X^e - 1$ sind. Nach Korollar 5.2 ist die Anzahl der Nullstellen aber maximal gleich dem Grad, so dass $n = e$ folgt. Nach Lemma 4.14 ist dann U zyklisch. □

Wir können damit im Fall einer Primzahl die Struktur der Einheitengruppe des Restklassenringes verstehen.

Satz 5.4. *Sei p eine Primzahl. Dann ist die Einheitengruppe $(\mathbb{Z}/(p))^\times$ zyklisch der Ordnung $p-1$. Es gibt also (sogenannte primitive) Elemente g mit der Eigenschaft, dass die Potenzen g^i, $i = 0, 1, \ldots, p-2$, alle Einheiten durchlaufen.*

Beweis. Dies folgt unmittelbar aus Satz 5.3, da $\mathbb{Z}/(p)$ ein endlicher Körper ist. □

Definition 5.5. Eine Einheit $u \in (\mathbb{Z}/(n))^\times$ heißt *primitiv* (oder eine *primitive Einheit*), wenn sie die Einheitengruppe erzeugt.

Bemerkung 5.6. Der Satz 5.4 sagt insbesondere, dass es für eine Primzahl p primitive Elemente im Restklassenkörper $\mathbb{Z}/(p)$ gibt. Er ist lediglich ein Existenzsatz und gibt keinen Hinweis, wie primitive Elemente zu konstruieren oder zu finden sind. Für eine beliebige natürliche Zahl n ist die Einheitengruppe der Restklassenringe $\mathbb{Z}/(n)$ im Allgemeinen nicht zyklisch. Wir werden später diejenigen Zahlen charakterisieren, die diese Eigenschaft besitzen. Für eine Primzahl p und eine Einheit $g \in (\mathbb{Z}/(p))^\times$ bedeutet die Eigenschaft, primitiv zu sein, dass ein Gruppenisomorphismus

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

vorliegt.

Korollar 5.7. *(Anzahl von primitiven Elementen) Sei p eine Primzahl. Dann gibt es in $\mathbb{Z}/(p)$ genau $\varphi(p-1)$ primitive Elemente.*

Beweis. Aufgrund der Existenz von primitiven Elementen gibt es eine Isomorphie $\mathbb{Z}/(p-1) \cong (\mathbb{Z}/(p))^\times$. Daher geht es um die Anzahl der Erzeuger der additiven Gruppe $\mathbb{Z}/(p-1)$. Ein Element aus $\mathbb{Z}/(p-1)$ ist ein Gruppen-Erzeuger genau dann, wenn es in $\mathbb{Z}/(p-1)$ (als Ring betrachtet) eine Einheit ist. Deshalb ist die Anzahl gerade $\varphi(p-1)$. □

Wir kehren nun zum allgemeinen Fall zurück, wo n eine beliebige positive ganze Zahl ist.

Satz 5.8. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$. Dann induziert der Isomorphismus (des Chinesischen Restsatzes) $\mathbb{Z}_n/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k})$ einen Isomorphismus der Einheitengruppen*

$$(\mathbb{Z}/(n))^\times \cong (\mathbb{Z}/(p_1^{r_1}))^\times \times (\mathbb{Z}/(p_2^{r_2}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times\,.$$

Insbesondere ist die Einheitengruppe von $\mathbb{Z}/(n)$ höchstens dann zyklisch, wenn die Einheitengruppen von $\mathbb{Z}/(p_i^{r_i})$ zyklisch sind für alle $i = 1, \ldots, k$.

Beweis. Ein Ringisomorphismus induziert natürlich einen Isomorphismus der Einheitengruppen, und die Einheitengruppe eines Produktringes ist die Produktgruppe der beteiligten Einheitengruppen. Ist eine Produktgruppe zyklisch, so muss auch jede Komponentengruppe zyklisch sein, da diese auch Restklassengruppen der Produktgruppe sind (unter der Projektion auf die Komponente). □

Aus obiger Einheitenversion des Chinesischen Restsatzes folgt für die Eulersche Funktion, wenn $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ die Primfaktorzerlegung ist, die Identität

$$\varphi(n) = \varphi(p_1^{r_1}) \cdot \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}) \, .$$

Man muss also nur noch $\varphi(p^r)$ für eine Primzahl p berechnen, wobei natürlich $\varphi(p) = p - 1$ ist. Für p^r mit $r \geq 2$ ist eine Zahl $0 < a < p^r$ genau dann teilerfremd zu p^r, wenn sie teilerfremd zu p ist, und das ist genau dann der Fall, wenn sie kein Vielfaches von p ist. Die Vielfachen von p im beschriebenen Intervall sind genau die Zahlen bp mit $0 \leq b < p^{r-1}$. Dies sind p^{r-1} Stück, so dass es also $p^r - p^{r-1} = p^{r-1}(p-1)$ Einheiten gibt. Wir erhalten demnach

$$\varphi(p^r) = p^{r-1}(p-1)$$

und insgesamt

$$\varphi(n) = p_1^{r_1-1}(p_1 - 1) \cdot p_2^{r_2-1}(p_2 - 1) \cdots p_k^{r_k-1}(p_k - 1) \, .$$

Lemma 5.9. *Sei p eine Primzahl und $r \geq 1$. Dann ist der durch die kanonische Projektion $\mathbb{Z}/(p^r) \longrightarrow \mathbb{Z}/(p)$ induzierte Homomorphismus*

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

der Einheitengruppen surjektiv.

Beweis. Sei $a \in (\mathbb{Z}/(p))^\times$ eine Einheit. Dann ist a teilerfremd zu p und damit kein Vielfaches von p. Wir fassen a als Element in $\mathbb{Z}/(p^r)$ auf. Da a nach wie vor kein Vielfaches von p ist, ist es auch in $\mathbb{Z}/(p^r)$ eine Einheit, und zugleich ein Urbild von $a \in (\mathbb{Z}/(p))^\times$. □

Lemma 5.10. *Sei $p \geq 3$ eine Primzahl und $r \geq 1$. Dann ist der Kern des Einheiten -Homomorphismus*

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

zyklisch der Ordnung p^{r-1}.

Beweis. Wir zeigen, dass das Element $a = 1 + p$, das offensichtlich zum Kern von $\varphi : (\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p))^\times$ gehört, in der Einheitengruppe $(\mathbb{Z}/(p^r))^\times$ die Ordnung p^{r-1} besitzt. Da diese Kerngruppe die Ordnung p^{r-1} hat, muss die (multiplikative) Ordnung von a ein Teiler davon sein, also von der Gestalt p^s

mit $s \leq r-1$ sein. Wir zeigen, dass $a^{p^{r-2}} \neq 1$ in $(\mathbb{Z}/(p^r))^\times$ ist, so dass also nur noch die Ordnung p^{r-1} möglich bleibt.

Nehmen wir also $a^{p^{r-2}} = 1 \mod p^r$ an, das bedeutet

$$a^{p^{r-2}} - 1 = (1+p)^{p^{r-2}} - 1 = 0 \mod p^r .$$

Ausmultiplizieren ergibt den Ausdruck

$$\binom{p^{r-2}}{1} p + \binom{p^{r-2}}{2} p^2 + \binom{p^{r-2}}{3} p^3 + \ldots = 0 \mod p^r .$$

Der erste Summand ist dabei $\binom{p^{r-2}}{1} p = p^{r-1}$ und wir betrachten die weiteren Summanden

$$\binom{p^{r-2}}{k} p^k .$$

mit $k \geq 2$. Wir schreiben

$$\begin{aligned} \binom{p^{r-2}}{k} &= \frac{p^{r-2}!}{k!(p^{r-2}-k)!} \\ &= \frac{p^{r-2} \cdot (p^{r-2}-1) \cdots (p^{r-2}-k+1)}{k \cdot (k-1) \cdots 1} \\ &= \frac{p^{r-2} \cdot (p^{r-2}-1) \cdots (p^{r-2}-k+1)}{k \cdot 1 \cdots (k-1)} . \end{aligned}$$

So geordnet steht vorne $\frac{p^{r-2}}{k}$ und dann folgen Ausdrücke der Form $\frac{p^{r-2}-j}{j}$, $j = 1, \ldots, k-1$. Der Exponent der Primzahl p in diesen letztgenannten Brüchen ist oben und unten gleich. Daher hängt der p-Exponent des Binomialkoeffizienten $\binom{p^{r-2}}{k}$ nur von $\frac{p^{r-2}}{k}$ ab. Sei i der p-Exponent von k. Der p-Exponent von $\frac{p^{r-2}}{k}$ ist dann $r-2-i$ und damit ist der p-Exponent von $\binom{p^{r-2}}{k} p^k$ gleich

$$r - 2 - i + k .$$

Wir behaupten, dass dies $\geq r$ ist, was für $i = 0$ klar ist (wegen $k \geq 2$). Sei also $i \geq 1$. Dann gilt aber, wegen $p \geq 3$, die Abschätzung

$$i \leq p^i - 2 \leq k - 2 ,$$

was genau die Aussage ergibt. Damit ist insgesamt in der obigen Summation der erste Summand, also p^{r-1}, kein Vielfaches von p^r, aber alle weiteren Summanden sind Vielfache von p^r, was einen Widerspruch bedeutet. □

Satz 5.11. *Sei $p \geq 3$ eine Primzahl und $r \geq 1$. Dann ist die Einheitengruppe*

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

des Restklassenrings $\mathbb{Z}/(p^r)$ zyklisch.

Beweis. Nach Lemma 5.9 ist die Abbildung

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

surjektiv. Die Einheitengruppe $(\mathbb{Z}/(p))^\times$ ist zyklisch aufgrund der Aussage (Satz 5.4). Sei $v \in (\mathbb{Z}/(p))^\times$ ein erzeugendes (also primitives) Element dieser Gruppe (der Ordnung $p-1$) und sei $u \in (\mathbb{Z}/(p^r))^\times$ ein Element, das auf v abgebildet wird. Die Ordnung von u ist dann ein positives Vielfaches von $p-1$. Es gibt daher auch ein $w \in (\mathbb{Z}/(p))^\times$ (nämlich eine gewissse Potenz von u), das genau die Ordnung $p-1$ besitzt.

Auf der anderen Seite gibt es nach Lemma 5.10 ein Element $a \in (\mathbb{Z}/(p))^\times$, das den Kern von φ erzeugt und die Ordnung p^{r-1} besitzt. Die Ordnung von ¡aw ist somit das kleinste gemeinsame Vielfache von p^{r-1} und $p-1$, also $p^{r-1}(p-1)$. Da dies die Gruppenordnung ist, muss die Gruppe zyklisch sein und awist ein Erzeuger. □

Bemerkung 5.12. Für $p=2$ ist die Einheitengruppe von $\mathbb{Z}/(2^r)$ im Allgemeinen nicht zyklisch. Für $r=1$ ist sie zyklisch (sogar trivial) und für $r=2$ ist $(\mathbb{Z}/(2^2))^\times = (\mathbb{Z}/(4))^\times$ ebenfalls zyklisch der Ordnung zwei, und zwar ist 3 primitiv. Für $r=3$ hingegen ist $(\mathbb{Z}/(2^3))^\times = (\mathbb{Z}/(8))^\times$ nicht zyklisch. Es gilt nämlich

$$1^2 = 1 \mod 8,\ 3^2 = 9 = 1 \mod 8,\ 5^2 = 25 = 1 \mod 8 \text{ und}$$
$$7^2 = 49 = 1 \mod 8,$$

so dass alle Einheiten die Ordnung zwei haben und es keinen Erzeuger gibt. Die Einheitengruppe ist isomorph zu

$$(\mathbb{Z}/(8))^\times \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)\,.$$

Ähnliche Überlegungen wie in Lemma 5.10 zeigen, dass die Einheitengruppe von $\mathbb{Z}/(2^r)$ für $r \geq 3$ isomorph zu $\mathbb{Z}/(2^{r-2}) \times \mathbb{Z}/(2)$ ist, und zwar ist 5 ein Element der Ordnung 2^{r-2}. Jede Einheit in $\mathbb{Z}/(2^r)$ hat somit eine Darstellung der Form $\pm 5^i$.