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

# Zahlentheorie

## Vorlesung 3

### Der euklidische Algorithmus

Euklid (4. Jahrhundert v. C.)

DEFINITION 3.1. Seien zwei Elemente $a, b$ (mit $b \neq 0$) eines euklidischen Bereichs $R$ mit euklidischer Funktion $\delta$ gegeben. Dann nennt man die durch die Anfangsbedingungen $r_0 = a$ und $r_1 = b$ und die mittels der Division mit Rest

$$r_i = q_i r_{i+1} + r_{i+2}$$

rekursiv bestimmte Folge $r_i$ die *Folge der euklidischen Reste*.

SATZ 3.2. *Seien zwei Elemente $r_0 = a, r_1 = b \neq 0$ eines euklidischen Bereichs $R$ mit euklidischer Funktion $\delta$ gegeben. Dann besitzt die Folge $r_i$, $i = 0, 1, 2, \ldots$, der euklidischen Reste folgende Eigenschaften.*

(1) *Es ist $r_{i+2} = 0$ oder $\delta(r_{i+2}) < \delta(r_{i+1})$.*
(2) *Es gibt ein (minimales) $k \geq 2$ mit $r_k = 0$.*
(3) *Es ist $\mathrm{ggT}(r_{i+1}, r_i) = \mathrm{ggT}(r_i, r_{i-1})$.*
(4) *Sei $k \geq 2$ der erste Index derart, dass $r_k = 0$ ist. Dann ist*

$$\mathrm{ggT}(a, b) = r_{k-1}\,.$$

*Beweis.* (1) Dies folgt unmittelbar aus der Definition der Division mit Rest.

(2) Solange $r_i \neq 0$ ist, wird die Folge der natürlichen Zahlen $\delta(r_i)$ immer kleiner, so dass irgendwann der Fall $r_i = 0$ eintreten muss.

(3) Wenn $t$ ein gemeinsamer Teiler von $r_{i+1}$ und von $r_{i+2}$ ist, so zeigt die Beziehung

$$r_i = q_i r_{i+1} + r_{i+2}\,,$$

dass $t$ auch ein Teiler von $r_i$ und damit ein gemeinsamer Teiler von $r_{i+1}$ und von $r_i$ ist. Die Umkehrung folgt genauso.

(4) Dies folgt aus (3) mit der Gleichungskette

$$\begin{aligned}\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r_2) = \mathrm{ggT}(r_2,r_3) = \ldots = \mathrm{ggT}(r_{k-2},r_{k-1}) \\ = \mathrm{ggT}(r_{k-1},r_k) = \mathrm{ggT}(r_{k-1},0) = r_{k-1}.\end{aligned}$$

□

Als Beispiel zum euklidischen Algorithmus lösen wir die folgende Aufgabe.

Aufgabe: Bestimme in $\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 1071 und 1029.

Lösung:

Der größte gemeinsame Teiler von 1071 und 1029 wird mit dem euklidischen Algorithmus wie folgt berechnet:

$$1071 = 1 \cdot 1029 + 42$$

$$1029 = 24 \cdot 42 + 21$$

$$42 = 2 \cdot 21 + 0$$

Der größte gemeinsame Teiler von 1071 und 1029 ist somit 21.

Aufgabe: Bestimme in $\mathbb{Z}[\mathrm{i}]$ mit Hilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von $7 + 4\mathrm{i}$ und $5 + 3\mathrm{i}$.

Lösung:

Wir setzen $a = 7 + 4\mathrm{i}$ und $b = 5 + 3\mathrm{i}$ und führen die Division mit Rest $a/b$ durch. Es ist (in $\mathbb{C}$)

$$\frac{a}{b} = \frac{7+4\mathrm{i}}{5+3\mathrm{i}} = \frac{(7+4\mathrm{i})(5-3\mathrm{i})}{(5+3\mathrm{i})(5-3\mathrm{i})} = \frac{47-\mathrm{i}}{34} = \frac{47}{34} - \frac{1}{34}\mathrm{i}\,.$$

Die beste Approximation für diese komplexe Zahl mit einer ganzen Gaußschen Zahl ist 1, so dass die Division mit Rest ergibt:

$$a = 1 \cdot b + r \text{ mit } r = a - b = 2 + \mathrm{i}\,.$$

Die nächste durchzuführende Division ist somit

$$\frac{b}{r} = \frac{5+3\mathrm{i}}{2+\mathrm{i}} = \frac{(5+3\mathrm{i})(2-\mathrm{i})}{(2+\mathrm{i})(2-\mathrm{i})} = \frac{13+\mathrm{i}}{5} = \frac{13}{5} + \frac{1}{5}\mathrm{i}\,.$$

Die beste Approximation für diese komplexe Zahl mit einer ganzen Gaußschen Zahl ist 3, so dass die Division mit Rest ergibt:

$$b = 3 \cdot r + s \text{ mit } s = b - 3r = 5 + 3\mathrm{i} - 3(2+\mathrm{i}) = -1\,.$$

Da dies eine Einheit ist, sind $a = 7 + 4\mathrm{i}$ und $b = 5 + 3\mathrm{i}$ teilerfremd.

SATZ 3.3. *(Lemma von Bezout) Sei $R$ ein Hauptidealring. Dann gilt:*

*Elemente $a_1, \ldots, a_n$ besitzen stets einen größten gemeinsamen Teiler $d$, und dieser lässt sich als Linearkombination der $a_1, \ldots, a_n$ darstellen, d.h. es gibt Elemente $r_1, \ldots, r_n \in R$ mit $r_1a_1 + r_2a_2 + \ldots + r_na_n = d$.*

*Insbesondere besitzen teilerfremde Elemente $a_1, \ldots, a_n$ eine Darstellung der $1$.*

*Beweis.* Sei $I = (a_1, \ldots, a_n)$ das von den Elementen erzeugte Ideal. Da wir in einem Hauptidealring sind, handelt es sich um ein Hauptideal; es gibt also ein Element $d$ mit $I = (d)$. Wir behaupten, dass $d$ ein größter gemeinsamer Teiler der $a_1, \ldots, a_n$ ist. Die Inklusionen $(a_i) \subseteq I = (d)$ zeigen, dass es sich um einen gemeinsamen Teiler handelt. Sei $e$ ein weiterer gemeinsamer Teiler der $a_1, \ldots, a_n$. Dann ist wieder $(d) = I \subseteq (e)$, was wiederum $e|d$ bedeutet. Die Darstellungsaussage folgt unmittelbar aus $d \in I = (a_1, \ldots, a_n)$.

Im teilerfremden Fall ist $I = (a_1, \ldots, a_n) = R$. □

LEMMA 3.4. *(von Euklid) Sei $R$ ein Hauptidealbereich und $a, b, c \in R$. Es seien $a$ und $b$ teilerfremd und $a$ teile das Produkt $bc$. Dann teilt $a$ den Faktor $c$.*

*Beweis.* Da $a$ und $b$ teilerfremd sind, gibt es nach Lemma von Bezout (Lemma 3.3) Elemente $r, s \in R$ mit $ra+sb = 1$. Die Voraussetzung, dass $a$ das Produkt $bc$ teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = a(cr + ds),$$

was zeigt, dass $c$ ein Vielfaches von $a$ ist. □

SATZ 3.5. *Sei $R$ ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

*Beweis.* Ein Primelement in einem Integritätsbereich ist nach Lemma 1.15 stets irreduzibel. Sei also umgekehrt $p$ irreduzibel, und nehmen wir an, dass $p$ das Produkt $ab$ teilt, sagen wir $pc = ab$. Nehmen wir an, dass $a$ kein Vielfaches von $p$ ist. Dann sind aber $a$ und $p$ teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von $p$ widerspricht. Damit teilt $p$ nach Lemma 3.4 den anderen Faktor $b$. □

LEMMA 3.6. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von irreduziblen Elementen.*

*Beweis.* Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei $a_{n+1}$ ein nicht-trivialer Teiler von $a_n$ ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots .$$

Die Vereinigung dieser Ideale ist aber ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. □

SATZ 3.7. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ darstellen als Produkt von Primelementen. Diese Darstellung ist eindeutig bis auf Reihenfolge und Assoziiertheit. Wählt man aus jeder Assoziiertheitsklasse von Primelementen einen festen Repräsentanten $p$, so gibt es eine bis auf die Reihenfolge eindeutige Darstellung $a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, wobei $u$ eine Einheit ist und die $p_i$ Repräsentanten sind.*

*Beweis.* Die erste Aussage folgt direkt aus Lemma 3.6 und Satz 3.5.

Die behauptete Eindeutigkeit bis auf Umordnung bedeutet, dass wenn

$$a = u \cdot p_1 \cdots p_k = v \cdot q_1 \cdots q_m \qquad (*)$$

zwei Primfaktorzerlegungen sind, dass dann $k = m$ ist und es eine Permutation $\tau$ auf $\{1, \ldots, k\}$ gibt derart, dass $p_i$ und $q_{\tau(i)}$ assoziiert sind für alle $i \in \{1, \ldots, k\}$. Wir beweisen diese Aussage durch Induktion über $k$. Sei zuerst $k = 0$ (das sei zugelassen). Dann steht links eine Einheit, also muss auch rechts eine Einheit stehen, was $m = 0$ bedeutet.

Sei also $k > 0$ und die Aussage sei für alle kleineren $k$ bewiesen. Die Gleichung $(*)$ bedeutet insbesondere, dass $p_k$ das Produkt rechts teilt. Da $p_k$ prim ist, muss $p_k$ einen der Faktoren rechts teilen. Nach Umordnung kann man annehmen, dass $q_m$ von $p_k$ geteilt wird. Da $q_m$ ebenfalls prim ist, sind $q_m$ und $p_k$ assoziiert. Also ist $q_m = wp_k$ mit einer Einheit $w$ und man kann die Gleichung $(*)$ nach $p_k$ kürzen und erhält

$$u \cdot p_1 \cdots p_{k-1} = (vw) \cdot q_1 \cdots q_{m-1} \,.$$

Die Induktionsvoraussetzung liefert dann $k - 1 = m - 1$. □

Diesen Satz kann man auch so ausdrücken, dass Hauptidealbereiche faktoriell sind im Sinne der folgenden Definition. Für solche Bereiche gilt ganz allgemein, dass die Primfaktorzerlegung eindeutig ist.

DEFINITION 3.8. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn folgende beiden Eigenschaften erfüllt sind.

(1) Jedes irreduzible Element in $R$ ist prim.
(2) Jedes Element $a \in R$, $a \neq 0$, ist ein Produkt aus irreduziblen Elementen.

KOROLLAR 3.9. *Jede positive natürliche Zahl lässt sich eindeutig als Produkt von Primzahlen darstellen.*

*Beweis.* Dies folgt sofort aus Satz 3.7. □

KOROLLAR 3.10. *Sei $R$ ein Hauptidealbereich und seien $a$ und $b$ zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

*(wobei die Exponenten auch null sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ ist für alle Exponenten $i = 1, \ldots, k$.*

*Beweis.* Wenn die Exponentbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann schreiben

$$b = vu^{-1}p_1^{s_1-r_1} \cdots p_k^{s_k-r_k} ,$$

was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in Hauptidealbereichen (siehe Satz 3.7). □

Satz 3.11. *Sei $R$ ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *$p$ ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

*Beweis.* Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von null verschieden. Wir bezeichnen einen Repräsentanten davon in $R$ ebenfalls mit $a$. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a, p)$. Ferner können wir schreiben $(a, p) = (b)$, da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da $c$ keine Einheit ist und $p$ prim (also irreduzibel) ist, muss $b$ eine Einheit sein. Es ist also $(a, p) = (1)$, und das bedeutet modulo $p$, also in $R/(p)$, dass $a$ eine Einheit ist. Also ist $R/(p)$ ein Körper. □

# Abbildungsverzeichnis