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

Zahlentheorie

Vorlesung 9

In diesem Abschnitt werden wir die Frage beantworten, welche ganze Zahlen sich also Summe von zwei Quadraten darstellen lassen, oder, anders formuliert, wann die diophantische Gleichung

$$n = x^2 + y^2$$

eine Lösung mit ganzen Zahlen x, y besitzt. Wir werden dabei wesentlich den Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ verwenden und schließen dabei an Vorlesung 2 an. Zunächst betrachten wir den Fall, wo $n = p$ eine ungerade Primzahl ist. Es gilt folgende Charakterisierung.

Satz 9.1. *Sei p ein ungerade Primzahl. Dann sind folgende Aussagen äquivalent.*

(1) *p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.*
(2) *p ist die Norm eines Elementes aus $\mathbb{Z}[\mathrm{i}]$.*
(3) *p ist zerlegbar (nicht prim) in $\mathbb{Z}[\mathrm{i}]$.*
(4) *-1 ist ein Quadrat in $\mathbb{Z}/(p)$.*
(5) $p = 1 \mod 4$

Beweis. (1) $\Leftrightarrow$ (2). Dies folgt sofort aus $x^2+y^2 = (x+y\mathrm{i})(x-y\mathrm{i}) = N(x+y\mathrm{i})$ (diese Äquivalenz gilt für alle ganze Zahlen).

(2) $\Rightarrow$ (3). Die Normdarstellung

$$p = N(x + y\mathrm{i}) = (x + y\mathrm{i})(x - y\mathrm{i})$$

ist eine Faktorzerlegung in $\mathbb{Z}[\mathrm{i}]$. Da x und y beide von null verschieden sind, ist $N(x + iy) \geq 2$ und $x + y\mathrm{i}$ ist keine Einheit, also ist die Zerlegung nicht trivial. Da der Ring der Gaußschen Zahlen euklidisch ist, sind prim und unzerlegbar äquivalent.

(3) $\Rightarrow$ (2). Sei p zerlegbar, sagen wir $p = wz$ mit Nichteinheiten $w, z \in \mathbb{Z}[\mathrm{i}]$. Dann ist $p^2 = N(p) = N(w)N(z)$. Dann muss $N(w) = p$ sein.

(3) $\Leftrightarrow$ (4). Es gilt

$$\mathbb{Z}[\mathrm{i}]/(p) \cong (\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}[X]/(X^2+1, p) \cong (\mathbb{Z}/(p)[X])/(X^2+1)\,.$$

Dieser (endliche) Restklassenring ist ein Körper genau dann, wenn p prim in $\mathbb{Z}[\mathrm{i}]$ ist (wegen Satz 3.11). Andererseits zeigt die Darstellung rechts, dass ein Körper genau dann vorliegt, wenn das Polynom $X^2 + 1$ ein irreduzibles Polynom in $(\mathbb{Z}/(p))[X]$ ist, und dies ist genau dann der Fall, wenn das Polynom keine Nullstelle in $\mathbb{Z}/(p)$ besitzen, was bedeutet, dass -1 kein Quadrat in $\mathbb{Z}/(p)$ ist.

Die Äquivalenz (4) $\Leftrightarrow$ (5) wurde schon im Satz 6.7 gezeigt. $\square$

BEMERKUNG 9.2. Sei p eine Primzahl, die modulo 4 den Rest 1 besitzt, so dass es nach Satz 9.1 eine Darstellung als Summe von zwei Quadraten geben muss. Wie findet man eine solche Darstellung explizit? Einerseits durch probieren, andererseits kann man aber entlang dem Beweis des Satzes vorgehen. Dazu muss man folgende Schritte gehen:

(1) Finde in $\mathbb{Z}/(p)$ ein Element a mit $a^2 = -1$. Um dies zu finden braucht man in der Regel ein primitives Element in diesem Restklassenkörper (ist b ein primitives Element, so kann man $a = b^{(p-1)/4}$ nehmen; siehe auch Aufgabe 11.9).
(2) Die Abbildung $\mathbb{Z}[\mathrm{i}] \to \mathbb{Z}/(p)$, die ganze Zahlen modulo p nimmt und i auf a schickt, ist ein surjektiver Ringhomomorphismus auf einen Körper. Der Kern ist ein Hauptideal, das von p und von $a-\mathrm{i}$ erzeugt wird.
(3) Finde mit dem euklidischen Algorithmus einen Erzeuger z für das Hauptideal $(p, a - \mathrm{i})$. Ein solcher Erzeuger hat die Norm $N(z) = p$.

BEISPIEL 9.3. Sei $p = 13$ (man sieht natürlich sofort eine Darstellung). Mit dem oben beschriebenen Verfahren müsste man wie folgt vorgehen:

In $\mathbb{Z}/(13)$ ist $5^2 = 25 = -1$, also kann man $a = 5$ nehmen. Dies führt zum Ideal $(13, 5 - \mathrm{i})$.

Die Division mit Rest liefert

$$\frac{13}{5-\mathrm{i}} = \frac{13(5+\mathrm{i})}{(5-\mathrm{i})(5+\mathrm{i})} = \frac{65+13\mathrm{i}}{26}\,.$$

und 2 ist eine beste Approximation. Damit ist:

$$13 = 2 \cdot (5 - \mathrm{i}) + r \text{ mit } r = 3 + 2\mathrm{i}\,.$$

Die nächste durchzuführende Division liefert

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

Damit ist also $5 - \mathrm{i} = (1 - \mathrm{i})(3 + 2\mathrm{i})$ und somit ist $3 + 2\mathrm{i}$ ein Erzeuger des Ideals.

Aus dem Hauptsatz können wir problemlos ableiten, wie sich die Primzahlen in $\mathbb{Z}[\mathrm{i}]$ verhalten:

KOROLLAR 9.4. *(Primzahlen in $\mathbb{Z}[\mathrm{i}]$) Die Primzahlen haben in $\mathbb{Z}[\mathrm{i}]$ folgendes Zerlegungsverhalten:*

- *Es ist $2 = -\mathrm{i}(1+i)^2$, und $1 + \mathrm{i}$ ist prim in $\mathbb{Z}[\mathrm{i}]$.*
- *Für $p = 1 \mod 4$ ist $p = (x + y\mathrm{i})(x - y\mathrm{i})$, wobei beide Faktoren prim sind.*
- *Für $p = 3 \mod 4$ ist p prim in $\mathbb{Z}[\mathrm{i}]$.*

Beweis. Aufgrund von Satz 9.1 ist im zweiten Fall lediglich noch zu zeigen, dass die beiden Faktoren prim sind. Wegen

$$p^2 = N(p) = N(x + y\mathrm{i})N(x - y\mathrm{i})$$

haben die beiden Faktoren die Norm p und sind deshalb nach Lemma 2.14 prim. □

Bemerkung 9.5. Für eine Gaußsche Zahl $z \in \mathbb{Z}[i]$ kann man folgendermaßen entscheiden, ob sie prim ist bzw. wie ihre Primfaktorzerlegung aussieht:

(1) Berechne die Norm $N(z)$. Ist diese eine Primzahl, so ist nach Lemma 2.14 das Element z selbst prim.
(2) Bestimme die (ganzzahligen) Primfaktoren von $N(z)$. Schreibe
$$N(z) = z\bar{z} = 2^r p_1 \cdots p_s q_1 \cdots q_t \,,$$
wobei die p_i ungerade mit Rest 1 modulo 4 und die q_j ungerade mit Rest 3 modulo 4 seien.
(3) Schreibe $p_i = N(u_i) = u_i\overline{u_i}$ für die Primfaktoren p_i mit Rest 1 modulo 4, und $2^r = (-i)^r(1+i)^{2r}$. Damit ist
$$z\bar{z} = (-i)^r(1+i)^{2r} u_1\overline{u_1} \cdots u_s\overline{u_s} q_1 \cdots q_t \,.$$
(4) Liste die möglichen Primfaktoren von z (und zugleich von $\overline{z}$) auf: das sind $1+i$ (falls 2 mit positivem Exponenten vorkommt), die u_i und $\overline{u_i}$ sowie die q_j (da $\mathbb{Z}[i]$ ein Hauptidealbereich ist und somit die eindeutige Primfaktorzerlegung gilt, setzt sich die Primfaktorzerlegung von z und von $\bar{z}$ aus Primfaktoren der rechten Seite zusammen).
(5) Durch 2^r und die q_j kann man sofort durchdividieren.
(6) Für die möglichen Primfaktoren u_i und $\overline{u_i}$ muss man überprüfen (durch Division mit Rest), ob sie Primfaktoren von z sind oder nicht (wenn nicht, so teilen sie $\bar{z}$). Statt Division kann man auch die möglichen Kombinationen ausmultiplizieren.

Wie kommen nun zur Bestimmung aller ganzen Zahlen, die Summe von zwei Quadraten sind.

Lemma 9.6. $2 = 1 + 1$ *ist eine Summe von Quadraten.*

Sind die natürlichen Zahlen m und n jeweils eine Summe von Quadratzahlen, so ist auch das Produkt mn eine Summe von Quadratzahlen.

Ist $n = r^2 m$, und ist m eine Summe von Quadratzahlen, so auch n.

Beweis. Die erste Aussage ist klar, für die zweite hat man die Charakterisierung mit der Norm und die Multiplikativität der Norm auszunutzen. Ist $m = x^2 + y^2$, so kann man einfach mit r^2 multiplizieren. □

Satz 9.7. *(Charakterisierung von Quadratsummen) Sei n eine positive natürliche Zahl. Schreibe $n = r^2 m$, wobei jeder Primfaktor von m nur einfach vorkomme. Dann ist n die Summe von zwei Quadraten genau dann, wenn in der*

Primfaktorzerlegung von m nur 2 und Primzahlen vorkommen, die modulo 4 den Rest 1 haben.

Beweis. Erfüllt n die angegebene Bedingung an die Primfaktorzerlegung, so ist n nach dem vorangehenden Lemma und dem Hauptsatz die Summe zweier Quadrate. Sei umgekehrt angenommen, dass n die Summe zweier Quadrate ist, so dass also eine Zerlegung $n = (x + \mathrm{i}y)(x - \mathrm{i}y)$ vorliegt. Sei p ein Primfaktor von n, der modulo 4 den Rest 3 besitze. Dann ist nach Satz 9.1 p prim in $\mathbb{Z}[\mathrm{i}]$ und teilt einen und damit (betrachte die Konjugation) beide Faktoren in der Zerlegung, jeweils mit dem gleichen Exponenten. Damit ist der Exponent von p in der Primfaktorzerlegung von n gerade und p kommt in der Primfaktorzerlegung von m nicht vor. □