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

Zahlentheorie

Vorlesung 9

Summe von zwei Quadraten - Primzahlen

In diesem Abschnitt werden wir die Frage beantworten, welche ganze Zahlen sich als 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 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 0 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 nach Lemma 2.12 euklidisch ist, sind nach Satz 3.5 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 innerhalb der natürlichen Zahlen $p^2 = N(p) = N(w)N(z)$. 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 Restklassenring ist endlich und somit Aufgabe 9.5 genau dann ein Körper, wenn es ein Integritätsbereich ist. Dies ist wiederum äquivalent dazu, dass p prim in $\mathbb{Z}[\mathrm{i}]$ ist (man kann auch mit nach Satz 3.12 schließen). 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 6.8 gezeigt. □

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 6.7).
(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 $N(z) = p$. Eine Zerlegung $p = zw$ führt ja generell auf $N(z)N(w) = N(p) = p^2$.

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 $(13, 5-\mathrm{i})$.

Division in $\mathbb{Q}[i]$ 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 in $\mathbb{Z}[\mathrm{i}]$. Damit ist die Division mit Rest

$$13 = 2\cdot(5-\mathrm{i}) + r$$

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.

BEMERKUNG 9.4. Wenn für eine Primzahl p eine Darstellung

$$p = x^2 + y^2 = (x + iy)(x - iy)$$

als Summe von zwei Quadraten bekannt ist, so kann man daraus einfach eine Quadratwurzel der -1 in $\mathbb{Z}/(p)$ finden. In diesem Fall gibt es einen surjektiven Ringhomomorphismus

$$\varphi\colon \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/(x + iy) \cong \mathbb{Z}/(p).$$

Die Isomorphie rechts rührt dabei von

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(p) \longrightarrow \mathbb{Z}[i]/(x + iy)$$

her, wobei die Surjektivität darauf beruht, dass $\mathbb{Z}[i]/(x + iy)$ ein Körper ist und es in $\mathbb{Z}/(p)$ schon zwei Quadratwurzeln der -1 gibt. Die Eigenschaft

$$i^2 = -1$$

überträgt sich auf das Bild, und dort gilt

$$\varphi(i) = -x \cdot y^{-1}.$$

BEISPIEL 9.5. Wir wollen in $\mathbb{Z}/(29)$ eine Quadratwurzel für -1 mit Hilfe von Bemerkung 9.4 finden. Es ist

$$29 = 5^2 + 2^2 = (5 + 2i)(5 - 2i).$$

Im Restklassenkörper

$$\mathbb{Z}[i]/(5 + 2i) \cong \mathbb{Z}/(29)$$

ist

$$i = -5 \cdot 2^{-1} = -5 \cdot 15 = -75 = 12.$$

In der Tat ist

$$12^2 = 144 = -1 \mod 29$$

Primfaktorzerlegung für Gaußsche Zahlen

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

KOROLLAR 9.6. *Die Primzahlen aus $\mathbb{Z}$ haben in $\mathbb{Z}$*[i] *folgendes Zerlegungsverhalten:*

- *Es ist*

$$2 = -\mathrm{i}(1 + i)^2,$$

und $1 + \mathrm{i}$ *ist prim in* $\mathbb{Z}$[i].

- *Für* $p = 1 \mod 4$ *ist*

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

mit gewissen eindeutig bestimmten $x, y \in \mathbb{N}_+$*, wobei beide Faktoren prim sind.*

- *Für* $p = 3 \mod 4$ *ist* p *prim in* $\mathbb{Z}$[i].

Beweis. Aufgrund von Satz 9.1 gibt es im zweiten Fall eine Darstellung

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

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 2.13 prim. Die Eindeutigkeit ergibt sich aus der eindeutigen Primfaktorzerlegung im Ring der Gaußschen Zahlen und der Kenntnis der Einheiten. □

Bemerkung 9.7. 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 2.13 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 $\bar{z}$ bis auf Einheiten aus Primfaktoren der rechten Seite zusammen).
(5) Durch 2^r und die q_j kann man sofort durchdividieren, da diese Faktoren jeweils sowohl von z als auch von $\bar{z}$ ein Faktor sind.
(6) Für die möglichen Primfaktoren u_i und $\overline{u_i}$ muss man (durch Division mit Rest) überprüfen, ob sie Primfaktoren von z sind oder nicht (wenn nicht, so teilen sie $\bar{z}$). Statt Division kann man auch die möglichen Kombinationen ausmultiplizieren.

Beispiel 9.8. Es ist

$$N(17 + 13i) = 17^2 + 13^2 = 289 + 169 = 458 = 2 \cdot 229,$$

wobei 229 eine Primzahl ist. Wegen

$$229 = 225 + 4 = 15^2 + 2^2$$

besitzt 229 in $\mathbb{Z}[i]$ die Primfaktorzerlegung

$$229 = (15 + 2i)(15 - 2i)$$

und somit ergibt sich die Primfaktorzerlegung

$$17 + 13i = (1 + i)(15 - 2i).$$

Summe von zwei Quadraten

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

LEMMA 9.9. $2 = 1 + 1$ *ist eine Summe von zwei Quadraten.*

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

Ist $n = r^2 m$, und ist m eine Summe von zwei 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 9.10. *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. □

BEISPIEL 9.11. Nach Satz 9.10 ist

$$1000 = 100 \cdot 2 \cdot 5$$

eine Summe von zwei Quadraten und

$$108 = 36 \cdot 3$$

keine Summe von zwei Quadraten.

Summe von drei und von vier Quadraten

Die beiden folgenden Sätze heißen *Dreiquadratesatz* bzw. *Vierquadratesatz* (oder Satz von Lagrange).

SATZ 9.12. *Eine natürliche Zahl n lässt sich genau dann als Summe von drei Quadratzahlen darstellen, wenn n* nicht *die Form*

$$4^i(8j + 7)$$

mit $i, j \in \mathbb{N}$ besitzt.

Satz 9.13. *Jede natürliche Zahl lässt sich als Summe von vier Quadratzahlen darstellen.*

Das Waringsche Problem ist die Frage, ob man für jeden Exponenten k eine Zahl g mit der Eigenschaft derart finden kann, dass jede natürliche Zahl eine Darstellung als Summe von maximal g k-ten Potenzen besitzt. Bei $k = 2$ ist $g = 4$. Dieses Problem wurde von Hilbert positiv gelöst. Beispielsweise kann man jede natürliche Zahl als Summe von 9 Kuben darstellen. Für 23 braucht man wirklich 9 Kuben.