MASTERARBEIT/ MASTER'S THESIS

Titel der Masterarbeit/ Title of the Master's Thesis

„Die Gaußschen ganzen Zahlen (Gaußscher Zahlenring)"

verfasst von/ submitted by

Patrick Schneider BEd

angestrebter akademischer Grad/ in partial fulfilment of the requirements for the degree of

Master of Education (MEd)

Wien, 2021/ Vienna 2021

Studienkennzahl lt. Studienblatt/ degree programme code as it appears on the student record sheet:	UA 199 520 523 02
Studienrichtung lt. Studienblatt/ degree programme as it appears on the student record sheet:	Masterstudium Lehramt Sek (AB) UF Mathematik UF Physik
Betreut von/ Supervisor:	ao. Univ.-Prof. Mag. Dr. Christoph Baxa

Zusammenfassung

Die vorliegende Masterarbeit gibt einen Überblick über die Gaußschen ganzen Zahlen. Bei diesen Zahlen handelt es sich um einen Zahlenring, der sich in den komplexen Zahlen befindet. Um die Eigenschaften dieser speziellen Zahlen zu verstehen, müssen zuerst einige Begriffe aus der Zahlentheorie erklärt werden. Hierbei werden die komplexen Zahlen im Allgemeinen eingeführt und anschließend werden Primzahlen in $\mathbb{Z}$ näher beleuchtet. Zuletzt wird geklärt, welche Primzahlen sich als Summe von zwei Quadratzahlen darstellen lassen. Also welche Primzahlen p die Eigenschaft $x^2 + y^2 = p$ für $x, y \in \mathbb{Z}$ erfüllen.
Im Hauptteil werden die Gaußschen ganzen Zahlen näher beschrieben. Anfangs können einige Eigenschaften der Gaußschen ganzen Zahlen gefunden werden. Anschließend wird die Division mit Rest in diesem Zahlenring erarbeitet, worauf auch der euklidische Algorithmus aufgebaut werden kann. Abschließend werden Primzahlen für die Gaußschen ganzen Zahlen eingeführt und damit gearbeitet. Zu guter Letzt wird eine Anwendung der Gaußschen ganzen Zahlen für die ganzen Zahlen gezeigt.

Abstract

This master thesis gives an overview of the Gaussian integers. These numbers are a ring in the complex numbers. To understand the properties of these special numbers, some concepts from Number theory have to be explained first. For this the complex numbers will be introduced in general and afterwards prime numbers in $\mathbb{Z}$ are closer examined. Finally, it will be clarified which prime numbers can be represented as the sum of two squares. So which primes p satisfy the property $x^2 + y^2 = p$ for some $x, y \in \mathbb{Z}$.
In the main section, the Gaussian integers are described in more detail. Initially, some properties of the Gaussian integers can be found. Then division with remainder is worked out in this ring, on which the Euclidean algorithm can also be based. Finally, prime numbers on the Gaussian integers are introduced and then worked with it. Ultimately, an application of the Gaussian integers is shown for the integers.

Inhaltsverzeichnis

1 Einleitung

Jeder Mensch in Österreich und in vielen anderen Ländern der Welt muss sich irgendwann in seinem Leben mit Mathematik beschäftigen. Meistens geschieht das schon in jungen Jahren. Einige lieben sie, doch die meisten hassen sie.

Aufgrund meines Wunsches, Lehrer zu werden, hatte ich schon oft das Vergnügen, mit Schülerinnen und Schüler über Mathematik reden zu dürfen. Tatsächlich habe ich von den meisten gehört, dass sie Mathematik für absolut nutzlos halten und sie alles, das sie in der Schule im Mathematikunterricht lernen, nie wieder in ihrem weiteren Leben brauchen werden. Doch hier steckt der Denkfehler. Mathematik umgibt uns ständig, auch wenn wir sie nicht immer aktiv wahrnehmen. Auch wenn es vielleicht viele nicht glauben können oder wollen, ohne die Mathematik würde unser Leben ziemlich leer aussehen.

Hätte Archimedes nicht vor ungefähr 2300 Jahren die "Kunst" der Mathematik beherrscht, wüssten wir heute vielleicht nicht, was ein Flaschenzug ist. Ohne Newton, der 1666 die theoretische Physik erfand, indem er sein Buch über die "Mathematischen Prinzipien der Naturphilosphie"verfasste, würden wir wahrscheinlich heute nicht so ein fortgeschrittenes Physikwissen besitzen. Ohne Keplers Gesetze über die Bewegungen der Himmelskörper wüssten wir vermutlich immer noch nicht, dass sich die Planeten beziehungsweise andere Himmelskörper in Ellipsenbahnen bewegen. [9]

Es geht hier klar hervor, dass die Physik, im Übrigen auch ein weniger beliebtes Fach bei Schülerinnen und Schülern, sehr eng mit der Mathematik zusammenspielt. Nicht nur die Physik braucht viel Mathematik. Auch die Informatik benötigt viele mathematische Konstrukte, um zu funktionieren. Hier geht es jetzt noch einen Schritt weiter. Ohne die Physik und die Informatik wäre die heutige Technik nicht möglich. Ebenfalls wäre eine bequeme Fahrt mit den öffentlichen Verkehrsmitteln oder mit dem Auto in die Schule oder in die Arbeit nicht vorstellbar. Das schnelle Anrufen der Freundin oder des Freundes, um sich zu verabreden, wäre ebenso nicht machbar. Kaum vorstellbar, aber es gäbe heutzutage kein Internet. In der

heutigen Gesellschaft ist das Internet auf keinen Fall mehr wegzudenken. Das sind nur einige Beispiele, die ohne Mathematik nicht funktionieren würden.

Einige Teilgebiete der Mathematik sind in der Technik stärker vertreten als andere. In dieser Arbeit möchte ich eines dieser Teilgebiete bearbeiten. Nämlich ein kleines Gebiet, die Zahlentheorie. Einige Teile der Zahlentheorie sind sehr wertvoll in der Informatik. Viele Eigenschaften von Zahlen sind sehr wichtig, um beispielsweise das sichere Kommunizieren über das Internet zu gewährleisten. Aber nun zum Thema dieser Arbeit.

Wie aus der Zusammenfassung entnommen wurde, geht es in dieser Arbeit um die Gaußschen ganzen Zahlen. Ich sehe dieses Thema als Erweiterung meiner Bachelorarbeit. Diese beschäftigte sich mit der Frage "Welche Primzahlen sind als Summe von zwei Quadratzahlen darstellbar?". Diese Frage wird auch in dieser Arbeit eine wichtige Rolle spielen, da es sehr wichtig für die Gaußschen Primzahlen sein wird, diese Frage beantworten zu können. Ich habe dieses Thema für meine Masterarbeit gewählt, da ich es sehr gut an mein Vorwissen anknüpfen konnte und ich die komplexen Zahlen sehr interessant und bewundernswert finde.

1.1 Aufgabenstellung

Damit die Gaußschen ganzen Zahlen gut verstanden werden können, muss ein wenig Vorarbeit geleistet werden.

Im ersten Kapitel wird anfangs erklärt, was ein mathematisches Konstrukt zu einem kommutativen Ring mit Eins macht. Anschließend wird erläutert, wie die Division mit Rest in $\mathbb{Z}$ funktioniert. Danach werden die komplexen Zahlen ($\mathbb{C}$) näher beleuchtet. Zuerst muss geklärt werden, warum komplexe Zahlen in der Mathematik überhaupt notwendig sind und wie sie dargestellt werden. Im Anschluss werden die Rechenregeln für komplexe Zahlen beschrieben und wichtige Eigenschaften gefunden. Des Weiteren wird gezeigt, dass es sich bei den komplexen Zahlen um einen Körper handelt. Am Ende des ersten Kapitels wird die Frage „Welche Primzahlen lassen sich als Summe von zwei Quadratzahlen darstellen?" behandelt.

Im zweiten und letzten Kapitel werden die Gaußschen ganzen Zahlen, also der Gaußsche Zahlenring, näher beschrieben. Hierbei werden zuerst wichtige Eigenschaften der Gaußschen ganzen Zahlen erhoben. Anschließend wird die Division mit Rest in den Gaußschen ganzen Zahlen eingeführt, worauf der euklidische Algorithmus aufgebaut werden kann. Folgend wird das Lemma von Bézout gezeigt. Im Anschluss werden Primzahlen in den Gaußschen ganzen Zahlen definiert und die dazugehörige Primfaktorzerlegung gezeigt. Am Ende des zweiten Kapitels wird eine Anwendung der Gaußschen ganzen Zahlen präsentiert.

2 Einführung

2.1 Kommutativer Ring mit Eins

Definition 2.1. Kommutativer Ring mit Eins

Ein Ring $(A, +, \cdot)$ ist eine Struktur, die aus einer nichtleeren Menge A und zwei verschiedenen inneren Verknüpfungen $+$ und $\cdot$ besteht. Man nennt die Verknüpfung $+$ Addition und die Verknüpfung $\cdot$ Multiplikation. Die Verknüpfungen sind Abbildungen $A \times A \to A$, das heißt, sie bilden Paare von Elementen aus A auf Elemente aus A ab. Ein kommutativer Ring mit Eins muss folgende Eigenschaften besitzen:

1) A bildet unter der Verknüpfung $+$ eine abelsche Gruppe, das heißt:

- A ist abgeschlossen bezüglich $+$, das heißt $\forall x, y \in A : x + y \in A$.
- Die Verknüpfung $+$ ist assoziativ, das heißt $(x + y) + z = x + (y + z)$ $\forall x, y, z \in A$.
- Die Verknüpfung $+$ ist kommutativ, das heißt $x + y = y + x$ $\forall x, y \in A$.
- Es existiert ein additives neutrales Element $0 \in A$, sodass für alle $x \in A$ gilt:

$$x + 0 = 0 + x = x$$

- Für alle $x \in A$ existiert ein additives inverses Element $-x \in A$, sodass:

$$x + (-x) = (-x) + x = 0$$

2) Die Multiplikation $\cdot$ erfüllt folgende Eigenschaften:

- A ist abgeschlossen bezüglich $\cdot$, das heißt $\forall x, y \in A : x \cdot y \in A$.
- Die Verknüpfung $\cdot$ ist assoziativ, das heißt $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\forall x, y, z \in A$.

3) Die beiden Verknüpfungen + und · müssen miteinander verträglich sein, das heißt, sie müssen sich distributiv verhalten. Somit muss für alle Elemente $x, y, z \in A$ gelten:

- $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$

Diese oben genannten Eigenschaften beschreiben einen Ring. Um nun einen kommutativen Ring mit Eins zu erhalten, werden noch zwei zusätzliche Eigenschaften benötigt. Diese sind:

- Ein Ring A heißt kommutativ, wenn die Verknüpfung · kommutativ ist, das heißt $x \cdot y = y \cdot x$ für alle $x, y \in A$.
- Ein Ring A wird Ring mit Eins oder unitär genannt, wenn ein multiplikatives neutrales Element $1 \in A$ existiert, sodass für alle $x \in A$ gilt: $x \cdot 1 = 1 \cdot x = x$.

2.2 Division mit Rest in $\mathbb{Z}$

Proposition 2.1. Es seien $a, b \in \mathbb{Z}$, wobei $b > 0$. Dann gibt es $q, r \in \mathbb{Z}$ so, dass

$$a = qb + r \text{ mit } 0 \leq r < b.$$

Die Zahlen q und r sind eindeutig bestimmt. Der Ausdruck q wird Quotient bei Division von a durch b genannt. Der Summand r heißt der Rest bei Division von a durch b.

Beweis.

- Existenz: Sei q die größte ganze Zahl die kleiner als $\frac{a}{b}$ ist, dann gilt $q \leq \frac{a}{b} < q+1$. Daraus folgt: $qb \leq a < qb+b \Rightarrow 0 \leq a-qb < b$. Sei $r = a-qb$, dann $a = qb + r$ und $0 \leq r < b$.
- Eindeutigkeit: Sei $a = qb+r = q_1b+r_1$ mit $0 \leq r, r_1 < b$. Dann ist $(q-q_1)b = r-r_1$. Daraus folgt: $q-q_1 = \frac{r-r_1}{b}$. Wegen $-b < r-r_1 < b$ folgt $-1 < \frac{r-r_1}{b} < 1$. Die einzige natürliche Zahl die sich zwischen -1 und 1 befindet, ist die Zahl 0. Das heißt $\frac{r-r_1}{b} = 0$ und daraus folgt: $r_1 = r \Rightarrow q_1b = qb \Rightarrow q_1 = q$.

□

2.3 Die komplexen Zahlen ($\mathbb{C}$)

2.3.1 Notwendigkeit der komplexen Zahlen

Es ist nicht möglich die Gleichung $x^2 + 1 = 0$ in den reellen Zahlen zu lösen. Dennoch können für diese Gleichung Lösungen mit Hilfe von komplexen Zahlen gefunden werden. Dafür müssen die reellen Zahlen um eine sogenannte imaginäre Einheit i erweitert werden, wobei i die folgende Eigenschaft besitzt:

$$i^2 = -1$$

Nun lässt sich sagen, dass die Zahlen i und $-i$ die Lösungen der quadratischen Gleichung $x^2 + 1 = 0$ sind.

2.3.2 Darstellung der komplexen Zahlen

Eine komplexe Zahl z lässt sich mit dieser imaginären Einheit i und zwei reellen Zahlen a und b darstellen.

$$z = a + ib,\ a, b \in \mathbb{R},\ i^2 = -1$$

Somit setzt sich eine komplexe Zahl z aus einem imaginären Teil b, auch Imaginärteil genannt, und einem reellen Teil a, auch Realteil genannt, zusammen. Wenn die reellen Zahlen a und b alle möglichen reellen Zahlen durchlaufen, dann können so auch alle komplexen Zahlen erzeugt werden. Alle diese Zahlen bilden die Menge $\mathbb{C}$ der komplexen Zahlen.

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$$

Falls bei einer komplexen Zahl der Realteil 0 ist (also $a = 0$), dann heißen diese Zahlen imaginäre Zahlen. Ist bei einer komplexen Zahl der Imaginärteil 0 (also $b = 0$), dann werden damit die reellen Zahlen abgebildet. Somit sind die komplexen Zahlen Summen von reellen und imaginären Zahlen.

2.3.3 Rechnen mit komplexen Zahlen

Addition

Zwei komplexe Zahlen $z = a + ib$ und $w = c + id$ werden addiert, indem die Realteile und Imaginärteile separat addiert werden.

$$z + w = (a + ib) + (c + id) = (a + c) + i(b + d)$$

Subtraktion

Zwei komplexe Zahlen $z = a + ib$ und $w = c + id$ werden subtrahiert, indem die Realteile und Imagniärteile separat subtrahiert werden.

$$z - w = (a + ib) - (c + id) = (a - c) + i(b - d)$$

Multiplikation

Zwei komplexe Zahlen $z = a + ib$ und $w = c + id$ werden multipliziert, indem sie wie algebraische Summen multipliziert werden.

$$z \cdot w = (a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc)$$

Division

Zwei komplexe Zahlen $z = a + ib$ und $w = c + id \neq 0$ (und daher $c^2 + d^2 > 0$) werden dividiert, indem mit der konjugiert komplexen Zahl des Nenners, also des Divisors, erweitert wird. (Das heißt, wenn $c + id$ der Nenner ist, muss mit $c - id$ erweitert werden.)

$$\frac{z}{w} = \frac{a + ib}{c + id} = \frac{a + ib}{c + id} \cdot \frac{c - id}{c - id} = \frac{(a + ib) \cdot (c - id)}{c^2 + d^2} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2}$$

2.3.4 Eigenschaften von komplexen Zahlen

Definition 2.2. Komplexe Konjugation

Sei $z = a + ib$ eine komplexe Zahl. Die Zahl $\overline{z} = a - ib$ ist die komplex konjugierte Zahl zu z.

Bemerkung:
Aus $z + \overline{z} = 2a$ und $z - \overline{z} = 2ib$ folgen sofort die folgenden beiden praktischen Darstellungen von Real- und Imaginärteil einer komplexen Zahl z mittels z und ihrer komplex Konjugierten $\overline{z}$:

$$a = \tfrac{1}{2} \cdot (z + \overline{z}) \text{ und } b = \tfrac{1}{2i} \cdot (z - \overline{z})$$

Definition 2.3. Gaußsche Zahlenebene

Die komplexen Zahlen lassen sich nicht mehr auf einer Zahlengeraden abbilden, sondern nur auf einer Zahlenebene. Diese Ebene wird Gaußsche Zahlenebene genannt, benannt nach seinem Entdecker Carl Friedrich Gauß. Hierbei wird in einem kartesischen Koordinatensystem der Realteil einer komplexen Zahl auf der x-Achse (reelle Achse) aufgetragen und der Imaginärteil auf der y-Achse (imaginäre Achse) aufgetragen. Jeder Punkt auf der Ebene entspricht so einer komplexen Zahl.

Definition 2.4. Betrag einer komplexen Zahl

Sei $z = a + ib$ eine komplexe Zahl. Der Ausdruck $|z| = \sqrt{a^2 + b^2}$ wird als Betrag der komplexen Zahl z bezeichnet. Der Betrag lässt sich als Abstand interpretieren, den die komplexe Zahl vom Nullpunkt der Gaußschen Zahlenebene hat.

Bemerkung:
Aus $z \cdot \overline{z} = (a + ib) \cdot (a - ib) = a^2 - i^2 b^2 = a^2 + b^2 = |z|^2$ lässt sich sofort die praktische Beziehung $z \cdot \overline{z} = |z|^2$ erkennen.

Lemma 2.1. Die komplexe Konjugation ist auf den oben beschriebenen vier Grundrechnungsarten verträglich, das heißt, sind $z, w \in \mathbb{C}$, so gelten die folgenden Eigenschaften:

i) $\overline{z+w} = \overline{z} + \overline{w}$

ii) $\overline{z-w} = \overline{z} - \overline{w}$

iii) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

iv) $\overline{(\frac{z}{w})} = \frac{\overline{z}}{\overline{w}}$

Beweis.

i)

$$\begin{aligned} \overline{z+w} &= \overline{(a+c)+i(b+d)} \\ &= (a+c)-i(b+d) \\ &= (a-ib)+(c-id) \\ &= \overline{z}+\overline{w} \end{aligned}$$

ii)

$$\begin{aligned} \overline{z-w} &= \overline{(a-c)+i(b-d)} \\ &= (a-c)-i(b-d) \\ &= (a-ib)-(c-id) \\ &= \overline{z}-\overline{w} \end{aligned}$$

iii) ($*$) Ist $|z| = 1$ so ist $z \cdot \overline{z} = |z|^2 = 1$ und daher $\frac{1}{z} = \overline{z}$. Setze $z = i$, so folgt daraus $\frac{1}{i} = \overline{i} = -i$.

$$\begin{aligned}
\overline{z \cdot w} &= \overline{(ac - bd) + i(ad + bc)} \\
&= (ac - bd) - i(ad + bc) \\
&= ac - (-b)(-d) + i(a(-d) + (-b)c) \\
&= ac + (-b)d - iad + i(-b)c \\
&= a \cdot (c - id) + (-b) \cdot (ic + d) \\
&= a \cdot (c - id) + (-ib) \cdot (c + \frac{d}{i})(*) \\
&= a \cdot (c - id) + (-ib) \cdot (c - id) \\
&= (a - ib) \cdot (c - id) \\
&= \overline{z} \cdot \overline{w}
\end{aligned}$$

iv) $(*)$ siehe iii)

$$\begin{aligned}
\overline{\frac{z}{w}} &= \overline{\frac{a+ib}{c+id}} \\
&= \frac{\overline{(ac+bd)+i(bc-ad)}}{c^2+d^2} \\
&= \frac{(ac+bd)-i(bc-ad)}{c^2+d^2} \\
&= \frac{(ac+(-b)(-d))+i((-b)c-a(-d))}{c^2+d^2} \\
&= \frac{ac+(-b)(-d)+i(-b)c-ia(-d)}{c^2+d^2} \\
&= \frac{ac-ia(-d)+(-b)(-d)+i(-b)c}{c^2+d^2} \\
&= \frac{a\cdot(c-i(-d))+(-b)\cdot(ic+(-d))}{c^2+d^2} (*) \\
&= \frac{a\cdot(c+id)+i(-b)\cdot(c+id)}{c^2+d^2} \\
&= \frac{(a-ib)\cdot(c+id)}{c^2+d^2} \\
&= \frac{(a-ib)\cdot(c+id)}{(c-id)\cdot(c+id)} \\
&= \frac{(a-ib)}{(c-id)} \\
&= \frac{\overline{z}}{\overline{w}}
\end{aligned}$$

□

Lemma 2.2. Der Betrag auf den komplexen Zahlen erfüllt folgende drei Eigenschaften:

i) Für alle $z \in \mathbb{C}$ ist $|z| \geq 0$ und $|z| = 0 \iff z = 0$.

ii) Für alle $z, w \in \mathbb{C}$ gilt $|z \cdot w| = |z| \cdot |w|$.

iii) Für alle $z, w \in \mathbb{C}$ gilt $|z + w| \leq |z| + |w|$ (Dreiecksungleichung).

Beweis.

i) Ist $z = a + ib$, so folgt das sofort aus $|z| = \sqrt{a^2 + b^2} \geq 0$ und $|z| = 0 \iff |z|^2 = a^2 + b^2 = 0 \iff a = b = 0 \iff z = 0$.

ii) Seien $z = a + ib$ und $w = c + id$ so gilt:

$$\begin{aligned}
|z \cdot w|^2 &= |(ac - bd) + i(ad + bc)|^2 \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
&= a^2 \cdot (c^2 + d^2) + b^2 \cdot (c^2 + d^2) \\
&= (a^2 + b^2) \cdot (c^2 + d^2) \\
&= |z|^2 \cdot |w|^2
\end{aligned}$$

woraus sofort die Behauptung $|z \cdot w| = |z| \cdot |w|$ folgt.

iii) Um die Dreiecksungleichung zu beweisen, muss zuerst festgestellt werden, dass für beliebige $a, b, c, d \in \mathbb{R}$ Folgendes gilt:

$$0 \leq (bc - ad)^2 = b^2c^2 - 2abcd + a^2d^2$$

und daher gilt:

$$2abcd \leq b^2c^2 + a^2d^2$$

Daraus folgt nun:

$$\begin{aligned}
(ac + bd)^2 &= a^2c^2 + 2abcd + b^2d^2 \\
&\leq a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\
&= (a^2 + b^2) \cdot (c^2 + d^2)
\end{aligned}$$

und somit $ac + bd \leq \sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2}$.

Mithilfe dieser Ungleichung lässt sich nun die Dreiecksungleichung beweisen.

$$\begin{aligned}
|z+w|^2 &= |(a+c)+i(b+d)|^2 \\
&= (a+c)^2+(b+d)^2 \\
&= a^2+2ac+c^2+b^2+2bd+d^2 \\
&= a^2+b^2+2(ac+bd)+c^2+d^2 \\
&\leq a^2+b^2+2\cdot\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}+c^2+d^2 \\
&= |z|^2+2|z||w|+|w|^2 \\
&= (|z|+|w|)^2
\end{aligned}$$

und daraus folgt sofort $|z+w| \leq |z|+|w|$.

□

2.3.5 Der Körper der komplexen Zahlen

Definition 2.5. Körper

Es sei $(K,+,\cdot)$ ein kommutativer Ring mit Eins. Besitzt jedes Element $x \in K$, $x \neq 0$ ein multiplikatives Inverses, das heißt $\forall x \in K \setminus \{0\}\ \exists x^{-1} \in K : x \cdot x^{-1} = = x^{-1} \cdot x = 1$, so wird $(K,+,\cdot)$ Körper genannt.

Lemma 2.3. Die komplexen Zahlen $(\mathbb{C},+,\cdot)$ bilden mit der in 2.3.3 beschriebenen Addition $+$ und Multiplikation $\cdot$ einen Körper.

Beweis.
1) $\mathbb{C}$ bildet unter der Verknüpfung $+$ eine abelsche Gruppe:

- Seien $z,w \in \mathbb{C}$ mit $z = a+ib, w = c+id$ mit $a,b,c,d \in \mathbb{R}$. Dann gilt:

$$\begin{aligned}
z+w &= a+ib+c+id \\
&= (a+c)+i(b+d)
\end{aligned}$$

Da $a+c, b+d \in \mathbb{R}$, ist auch $z+w \in \mathbb{C}$. Somit ist $\mathbb{C}$ bezüglich $+$ abgeschlossen.

- Seien $z, w, v \in \mathbb{C}$ mit $z = a + ib, w = c + id, v = e + if$ so ist:

$$\begin{aligned}(z + w) + v &= (a + c) + i(b + d) + e + if \\ &= ((a + c) + e) + i((b + d) + f) \\ &= (a + (c + e)) + i(b + (d + f)) \\ &= a + ib + (c + e) + i(d + f) \\ &= z + (w + v)\end{aligned}$$

  Das heißt, die Addition ist auf $\mathbb{C}$ assoziativ.

- Seien $z, w \in \mathbb{C}$ mit $z = a + ib, w = c + id$, so ist

$$\begin{aligned}z + w &= (a + c) + i(b + d) \\ &= (c + a) + i(d + b) \\ &= w + z\end{aligned}$$

  Das heißt, die Addition ist auf $\mathbb{C}$ kommutativ.

- Es existiert ein additives neutrales Element $0 = 0 + i0 \in \mathbb{C}$, sodass für alle $z = a + ib \in \mathbb{C}$ gilt:

$$\begin{aligned}z + 0 &= a + ib + 0 + i0 \\ &= (a + 0) + i(b + 0) \\ &= a + ib \\ &= z\end{aligned}$$

- Es existiert ein additives inverses Element $-z = -a - ib \in \mathbb{C}$, sodass für alle $z \in \mathbb{C}$ gilt:

$$\begin{aligned} z + (-z) &= a + ib + (-a - ib) \\ &= (a + (-a)) + i(b + (-b)) \\ &= 0 + i0 \\ &= 0 \end{aligned}$$

2) Die Multiplikation $\cdot$ erfüllt in $\mathbb{C}$ folgende Eigenschaften:

- Seien $z, w \in \mathbb{C}$ mit $z = a + ib, w = c + id$, so gilt:

$$\begin{aligned} z \cdot w &= (a + ib) \cdot (c + id) \\ &= ac + iad + ibc + ibid \\ &= ac - bd + iad + ibc \\ &= (ac - bd) + i(ad + bc) \end{aligned}$$

  Da $ac - bd, ad + bc \in \mathbb{R}$, ist auch $x \cdot y \in \mathbb{C}$. Somit ist $\mathbb{C}$ bezüglich $\cdot$ abgeschlossen.

- Seien $z, w, v \in \mathbb{C}$ mit $z = a + ib, w = c + id, v = e + if$, so gilt:

$$\begin{aligned} (x \cdot y) \cdot z &= ((ac - bd) + i(ad + bc)) \cdot (e + if) \\ &= ((ac - bd)e - (ad + bc)f) + i((ac - bd)f + (ad + bc)e) \\ &= (ace - bde - adf - bcf) + i(acf - bdf + ade + bce) \\ &= (a(ce - df) - b(cf + de)) + i(a(cf + de) + b(ce - df)) \\ &= (a + ib) \cdot ((ce - df) + i(cf + de)) \\ &= z \cdot (w \cdot v) \end{aligned}$$

  Das heißt, die Multiplikation ist auf $\mathbb{C}$ assoziativ.

- Seien $z, w \in \mathbb{C}$ mit $z = a + ib, w = c + id$, so ist

$$\begin{aligned} z \cdot w &= (ac - bd) + i(ad + bc) \\ &= (ca - db) + i(da + cb) \\ &= w \cdot z \end{aligned}$$

  Das heißt, die Multiplikation ist auf $\mathbb{C}$ kommutativ.

- Es existiert ein multiplikatives neutrales Element $1 = 1 + i0 \in \mathbb{C}$, sodass für alle $z = a + ib \in \mathbb{C}$ gilt:

$$\begin{aligned} z \cdot 1 &= (a + ib) \cdot (1 + i0) \\ &= (a \cdot 1 - b \cdot 0) + i(a \cdot 0 + b \cdot 1) \\ &= a + ib \\ &= z \end{aligned}$$

- Es existiert ein multiplikatives inverses Element $z^{-1} = \frac{1}{z} \in \mathbb{C}$, sodass für alle $z \in \mathbb{C}$ mit $z \neq 0$ gilt:

$$\begin{aligned} z \cdot z^{-1} &= z \cdot \frac{1}{z} \\ &= (a + ib) \cdot \frac{1}{a + ib} \\ &= (a + ib) \cdot \frac{1}{a + ib} \cdot \frac{a - ib}{a - ib} = (a + ib) \cdot \frac{a - ib}{(a + ib) \cdot (a - ib)} \\ &= (a + ib) \cdot \frac{a - ib}{a^2 + b^2} = \frac{a^2 + iab - iab - i^2 b^2}{a^2 + b^2} \\ &= \frac{a^2 + b^2}{a^2 + b^2} + i\frac{ab - ab}{a^2 + b^2} \\ &= 1 + i0 \\ &= 1 \end{aligned}$$

3) Die Addition und die Multiplikation erfüllen auf $\mathbb{C}$ das Distributivgesetz:

- Seien $z, w, v \in \mathbb{C}$ mit $z = a + ib, w = c + id, v = e + if$, so gilt:

$$\begin{aligned} z \cdot (w + v) &= (a + ib) \cdot ((c + e) + i(d + f)) \\ &= (a(c + e) - b(d + f) + i(a(d + f) + b(c + e) \\ &= (ac + ae - bd - bf) + i(ad + af + bc + be) \\ &= (ac - bd) + i(ad + bc) + (ae - bf) + i(af + be) \\ &= (a + ib) \cdot (c + id) + (a + ib) \cdot (e + if) \\ &= z \cdot w + z \cdot v \end{aligned}$$

Daraus folgt, dass es sich bei $(\mathbb{C}, +, \cdot)$ um einen Körper handelt. □

2.4 Primzahlen in $\mathbb{N}$

Definition 2.6. Primzahlen

Eine Zahl $p \in \mathbb{N}$, $p > 1$ heißt Primzahl, wenn sie genau zwei positive Teiler hat, nämlich 1 und p.

Einteilung von Primzahlen
Es ist möglich die Menge der Primzahlen in drei Gruppen zu unterteilen. Die erste Gruppe beinhaltet alle geraden Primzahlen. Hier gibt es nur eine, nämlich die Zahl $p = 2$. Alle anderen, ungeraden Primzahlen, lassen sich in die beiden anderen Gruppen einordnen. Die restlichen Zahlen sind in der Form $p = 4m+1$ oder in der Form $p = 4m+3$ darstellbar. Alle Primzahlen können in diese drei oben genannten Gruppen eingeordnet werden.

Warum ist das so?
Ist p ungerade, so gibt es ein $k \in \mathbb{N}$ mit der Eigenschaft $p = 2k+1$. Ist dieses k gerade, so gibt es ein $m \in \mathbb{N}$, sodass $k = 2m$ und daher $p = 2 \cdot 2m+1 = 4m+1$. Ist k ungerade, so gibt es ein $m \in \mathbb{N}$, sodass $k = 2m+1$ und $p = 2 \cdot (2m+1)+1 = 4m+3$.

2.5 Welche Primzahlen lassen sich als Summe von zwei Quadratzahlen darstellen?

Nun ist zu klären, für welche Primzahlen $p \in \mathbb{N}$ gilt, dass $p = a^2 + b^2$ für $a, b \in \mathbb{Z}$ ist. Wie in 2.4 beschrieben, lässt sich die Menge der Primzahlen in $\mathbb{N}$ in drei Untergruppen einteilen. Um nun die oben genannte Frage zu beantworten, müssen genau diese drei Gruppen genauer unter die Lupe genommen werden.

Für die Gruppe, die nur die Primzahl 2 enthält, ist leicht zu zeigen, dass diese Primzahl als Summe zweier Quadratzahlen darstellbar ist, nämlich $2 = 1^2 + 1^2$. Somit kann die Frage für eine Gruppe bereits beantwortet werden. Um nun eine weitere Gruppe abzuarbeiten, wird folgendes Lemma näher betrachtet.

Proposition 2.2. Eine ganze Zahl $n = 4m + 3$ ist nicht als Summe von zwei Quadratzahlen darstellbar.

Beweis.
Hierzu werden einfach die Quadrate einer geraden und einer ungeraden Zahl gebildet:

$$(2k)^2 = 4k^2$$
$$(2k+1)^2 = 4k^2 + 4k + 1$$

Nun können drei verschiedene Fälle eintreten:

i) $x^2 + y^2$ mit x gerade und y ungerade:

$$\begin{aligned}(2k)^2 + (2l+1)^2 &= 4k^2 + 4l^2 + 4l + 1 \\ &= 4(k^2 + l^2 + l) + 1 \\ &= 4m + 1\end{aligned}$$

ii) beide Zahlen sind gerade:

$$\begin{aligned}(2k)^2 + (2l)^2 &= 4k^2 + 4l^2 \\ &= 4(k^2 + l^2) \\ &= 4m + 0\end{aligned}$$

iii) beide Zahlen sind ungerade:

$$\begin{aligned}(2k+1)^2 + (2l+1)^2 &= 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \\ &= 4(k^2 + k + l^2 + l) + 2 \\ &= 4m + 2\end{aligned}$$

Damit ist gezeigt, dass die ganze Zahl $n = 4m + 3$ nicht als Summe von zwei Quadratzahlen darstellbar ist. Das heißt, es können auch keine Primzahlen p der Form $4m + 3$ als Summe von zwei Quadraten dargestellt werden. □

Im Gegensatz zur vorherigen Gruppe ist für diese Gruppe gezeigt, dass es für diese Primzahlen keine Möglichkeit gibt, als Summe von zwei Quadratzahlen gebildet zu werden. Zu guter Letzt wird die letzte Gruppe untersucht. Für diese Gruppe ist es etwas aufwändiger zu zeigen, dass diese Primzahlen als Summe von zwei Quadratzahlen dargestellt werden können. Deswegen werden im Anschluss des Beweises zwei Beispiele angeführt, um den Beweis verständlicher darstellen zu können.

Lemma 2.4. Jede Primzahl der Form $p = 4m + 1$ ist eine Summe von zwei Quadratzahlen. Sie kann als $p = x^2 + y^2$ dargestellt werden, mit den natürlichen Zahlen x und y.

Der Beweis wurde von Roger Heath-Brown im Jahr 1971 entdeckt und erst im Jahr 1984 publiziert ([1], [5]). Er verwendete sehr elementare Hilfsmittel und hat die Aussage mithilfe von drei Involutionen bewiesen. In der Mathematik ist eine Involution eine Abbildung, die zu sich selbst invers ist (oder formaler ausgedrückt: Eine Abbildung $f : A \to A$, bei der Definitionsmenge und Zielmenge (A) übereinstimmen, heißt genau dann Involution, wenn gilt, dass für alle $x \in A$ die Beziehung $f(f(x)) = x$ erfüllt ist.).

Beweis.
Es wird die Menge

$$S := \{(x, y, z) \in \mathbb{Z}^3 : \ 4xy + z^2 = p, \ x > 0, \ y > 0\}$$

untersucht. Diese Menge ist endlich: aus $x \geq 1$ und $y \geq 1$ folgt nämlich $y \leq \frac{p}{4}$ und $x \leq \frac{p}{4}$. Damit gibt es aber nur endlich viele mögliche Werte für x und y und für gegebenes x und y gibt es höchstens zwei Werte für z. Die Menge S ist nicht leer, da sie das Tripel $(\frac{p-1}{4}, 1, 1)$ enthält.

Die erste lineare Involution ist

$$f : S \to S,\ (x, y, z) \mapsto (y, x, -z),$$

also „vertausche x und y und negiere z". Dies bildet ganz offensichtlich S auf sich selbst ab und es ist eine Involution. Zweimal angewendet ergibt es die Identität. Dieses f hat offenbar keine Fixpunkte, weil aus $z = 0$ sofort $p = 4xy$ folgen würde, was nicht möglich ist. Schließlich bildet f die Lösungen in

$$T := \{(x, y, z) \in S : z > 0\}$$

auf die Lösungen in $S \setminus T$ ab, die $z < 0$ erfüllen. Also vertauscht f die Vorzeichen von $x - y$ und von z und bildet somit auch die Lösungen in

$$U := \{(x, y, z) \in S : (x - y) + z > 0\}$$

auf die Lösungen in $S \setminus U$ ab. Dafür muss überprüft werden, dass es keine Lösungen mit $(x - y) + z = 0$ gibt. Aber die gibt es nicht, weil daraus sofort $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$ folgen würde.

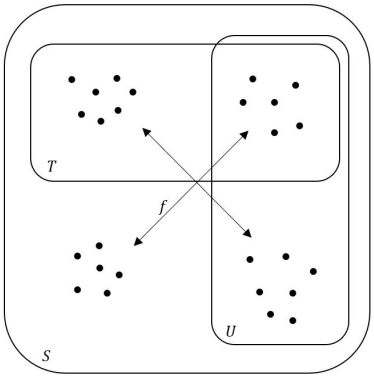

Abbildung 1: Abbildungen von f in die Mengen T und U [1]

Was liefert nun diese Analyse von f? Die hauptsächliche Beobachtung ist, dass f die Mengen T und U mit ihren Komplementen $S \setminus T$ beziehungsweise $S \setminus U$ in Bijektion setzt, deshalb haben T und U beide die halbe Kardinalität von S. Also haben T und U dieselbe Kardinalität (siehe Abbildung 1).

Die zweite Involution, die betrachtet werden soll, lebt auf der Menge U:

$$g : U \to U,\ (x, y, z) \mapsto (x - y + z,\ y,\ 2y - z).$$

Zunächst wird überprüft, dass dies eine wohldefinierte Abbildung ist: Wenn $(x, y, z) \in U$ ist, dann gilt $x - y + z > 0,\ y > 0$ und

$$4(x - y + z)y + (2y - z)^2 = 4xy + z^2 = p,$$

also $g(x, y, z) \in S$. Mit

$$(x - y + z) - y + (2y - z) = x > 0$$

liefert dies $g(x, y, z) \in U$.
Weiterhin ist g eine Involution: $g(x, y, z) = (x - y + z,\ y,\ 2y - z)$ wird durch g auf $((x - y + z) - y + (2y - z),\ y,\ 2y - (2y - z)) = (x, y, z)$ abgebildet.
Und schließlich hat g genau einen Fixpunkt:

$$(x, y, z) = g(x, y, z) = (x - y + z,\ y,\ 2y - z)$$

gilt genau dann, wenn $y = z$ ist. Dann haben wir aber $p = 4xy + y^2 = (4x + y)y$, was nur für $y = 1 = z$ und $x = \frac{p-1}{4}$ gelten kann. Und wenn g eine Involution auf U ist, die genau einen Fixpunkt hat, dann hat U eine ungerade Kardinalität (siehe Abbildung 2).

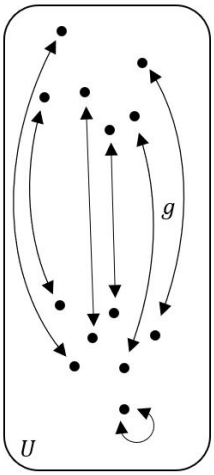

Abbildung 2: Visualisierung von g in der Menge U [1]

Die dritte, letzte und womöglich die trivialste Involution lebt auf der Menge T und sie vertauscht nur x und y miteinander:

$$h : T \to T, (x, y, z) \mapsto (y, x, z).$$

Diese Abbildung ist ganz offensichtlich wohl definiert und sie ist eine Involution. Nun wird das Wissen kombiniert, das aus den beiden anderen Involutionen abgeleitet wurde: T hat dieselbe Kardinalität wie U und diese ist ungerade. Aber da h somit eine Involution auf einer endlichen Menge von ungerader Kardinalität ist, muss h einen Fixpunkt haben, denn auf jeder endlichen Menge mit ungerader Kardinalität muss jede Involution mindestens einen Fixpunkt haben (siehe Abbildung 3).

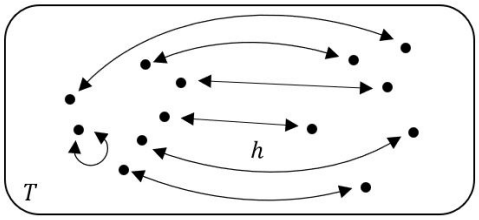

Abbildung 3: Visualisierung von h in der Menge T [1]

Somit gibt es einen Punkt $(x, y, z) \in T$ mit $x = y$, also eine Lösung der Gleichung

$$p = 4x^2 + z^2 = (2x)^2 + z^2,$$

was nichts anderes bedeutet, als dass p als Summe von zwei Quadratzahlen dargestellt werden kann.

□

Zwei Beispiele zu Lemma 2.4

Da der Beweis in Lemma 2.4 mit elementaren Mitteln arbeitet, könnte das Ende des Beweises möglicherweise etwas unbefriedigend sein. Der Beweis ist sehr verwunderlich. Es hat am Schluss den Anschein, als wäre das Ergebnis aus der Luft gegriffen. Um dem entgegenzuwirken, werden im Folgenden noch zwei Beispiele angegeben, damit der Beweis besser verstanden werden kann und um dem Anschein entgegenzuwirken, dass das Ergebnis des Beweises aus dem Nichts kommt.

Wie sieht der Sachverhalt für die Primzahl $p = 5$ aus? Die Menge S würde dann folgendermaßen aussehen:

$$S = \{(1, 1, 1), (1, 1, -1)\}$$

Somit wären die Teilmengen T und U gegeben durch:

$$T = U = \{(1, 1, 1)\}$$

In Abbildung 4 sind die Mengen S, T und U sowie auch die Involutionen f, g und h illustriert. Es lässt sich erkennen, dass dieses Beispiel mit der Primzahl $p = 5$ zu trivial ist. Anhand dieses Beispiels lässt sich leider nichts erkennen.

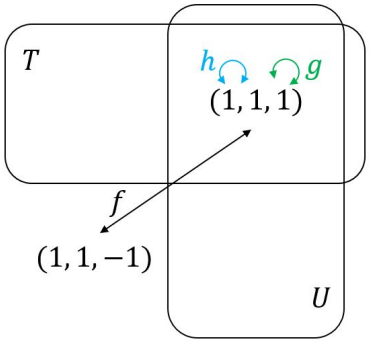

Abbildung 4: Visualisierung der Mengen T und U bzw. den Involutionen f, g und h für $p = 5$ [1]

Es muss ein besseres Beispiel gefunden werden. Die Primzahl $p = 13$ ist hierfür womöglich gut geeignet. Hierbei lässt sich eine mächtigere Menge S finden als im vorherigen Beispiel. Wir konstruieren zuerst die Menge S, anschließend die beiden anderen Mengen U und T. Danach werden die Involutionen f, g und h auf den jeweiligen Mengen gebildet. Um sich dies besser vorstellen zu können, muss die Abbildung 5 genauer betrachtet werden.

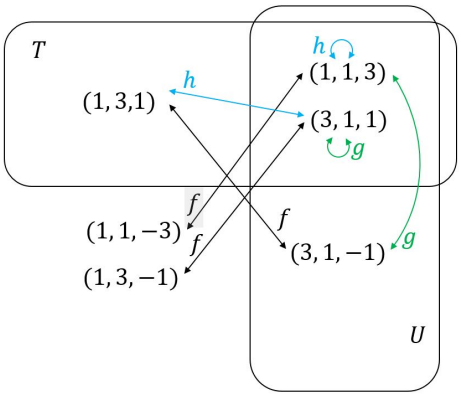

Abbildung 5: Visualisierung der Mengen T und U bzw. den Involutionen f, g und h für $p = 13$ [1]

Die Mengen U und T entstehen indem die Involution f auf die Menge S angewendet wird. In Abbildung 5 ist zu sehen, dass die beiden Mengen jeweils die halbe Kardinalität von S haben. Was lässt sich nun über die beiden Mengen sagen? Die beiden Mengen T und U müssen dieselbe Kardinalität besitzen.
Anschließend wird g auf der Menge U angewandt und hier lässt sich nun ein Fixpunkt finden. Da sich dieser finden lässt, muss die Menge U eine ungerade Kardinalität aufweisen. Wenn jeder Punkt einer Menge auf einen anderen Punkt derselben Menge abgebildet wird und es einen Fixpunkt gibt, dann kann die Menge nur eine ungerade Anzahl an Elementen besitzen.
Da U ungerade ist, muss auch T ungerade sein. Das heißt, T muss ebenfalls einen Fixpunkt besitzen. Um diesen Fixpunkt herauszufinden, wird die Involution h auf die Menge T angewandt. Mit diesem Fixpunkt haben wir dann ein Tripel gefunden, für das gilt, dass $x = y$ und die Gleichung

$$4xy + z^2 = 4x^2 + z^2 = (2x)^2 + z^2 = p$$

In diesem Beispiel wäre dies das Tripel $(1, 1, 3)$ und die Gleichung

$$4 \cdot 1 \cdot 1 + 3^2 = 4 + 3^2 = 2^2 + 3^2 = 13$$

zeigt, dass die Primzahl 13 als Summe von 2^2 und 3^2 geschrieben werden kann.

3 Die Gaußschen ganzen Zahlen $\mathbb{Z}[i]$

Definition 3.1. Die Gaußschen ganzen Zahlen (Gaußscher Zahlenring)

Die Menge $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ wird als Menge der Gaußschen ganzen Zahlen bezeichnet. Man nennt $(\mathbb{Z}[i], +, \cdot)$ den Ring der Gaußschen ganzen Zahlen.

3.1 Einige Eigenschaften der Gaußschen ganzen Zahlen

Lemma 3.1. Die Menge $\mathbb{Z}[i]$ bildet mit der Addition $+$ und Multiplikation $\cdot$ der komplexen Zahlen einen kommutativen Ring mit Eins $(\mathbb{Z}[i], +, \cdot)$.

Beweis.
1) $\mathbb{Z}[i]$ bildet unter der Verknüpfung $+$ eine abelsche Gruppe:

- $\mathbb{Z}[i]$ ist abgeschlossen bezüglich $+$.
- Die Verknüpfung $+$ ist in $\mathbb{Z}[i]$ assoziativ.
- Die Verknüpfung $+$ ist in $\mathbb{Z}[i]$ kommutativ.
- Es existiert in $\mathbb{Z}[i]$ ein additives neutrales Element.
- Es existiert in $\mathbb{Z}[i]$ zu jedem Element ein additives inverses Element.

2) Die Multiplikation $\cdot$ erfüllt in $\mathbb{Z}[i]$ folgende Eigenschaften:

- $\mathbb{Z}[i]$ ist abgeschlossen bezüglich $\cdot$.
- Die Verknüpfung $\cdot$ ist in $\mathbb{Z}[i]$ assoziativ.

3) Die Verknüpfungen $+$ und $\cdot$ verhalten sich in $\in \mathbb{Z}[i]$ distributiv.

Diese Eigenschaften muss $\mathbb{Z}[i]$ erfüllen, damit $\mathbb{Z}[i]$ ein Ring genannt werden darf. Um als kommutativer Ring mit Eins bezeichnet zu werden, muss $\mathbb{Z}[i]$ noch zwei weitere Eigenschaften erfüllen:

- Die Verknüpfung $\cdot$ ist in $\mathbb{Z}[i]$ kommutativ.
- Es existiert in $\mathbb{Z}[i]$ ein multiplikatives neutrales Element.

Alle oben genannten Eigenschaften sind notwendig, um $\mathbb{Z}[i]$ einen kommutativen Ring mit Eins nennen zu dürfen. Praktischerweise erfüllt $\mathbb{Z}[i]$ all diese Eigenschaften. $\mathbb{Z}[i]$ ist eine echte Teilmenge von $\mathbb{C}$ und diese Eigenschaften wurden schon in Lemma 2.3 gezeigt bzw. können den Beweisen leicht entnommen werden. Daraus folgt, dass es sich bei $\mathbb{Z}[i]$ um einen kommutativen Ring mit Eins handeln muss. □

Bemerkung:
$\mathbb{Z}[i]$ ist kein Körper. Dafür müsste es ein multiplikatives Inverses zu jeder Zahl $z \neq 0$ in $\mathbb{Z}[i]$ geben. Somit müsste für das multiplikative Inverse $\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}$ gelten, dass $(a^2+b^2)|a$ und $(a^2+b^2)|b$. Das ist aber nicht für alle $a, b \in \mathbb{Z}$ mit $(a,b) \neq (0,0)$ möglich und somit kann nicht für alle Elemente $\neq 0$ ein multiplikatives Inverses in $\mathbb{Z}[i]$ existieren.

Definition 3.2. Teilbarkeit von Gaußschen ganzen Zahlen

Sei $z, w \in \mathbb{Z}[i]$. Man sagt w teilt z in $\mathbb{Z}[i]$, falls ein $v \in \mathbb{Z}[i]$ existiert mit $z = w \cdot v$ und man schreibt hierfür kurz $w \mid z$. In diesem Fall heißt w Teiler von z und z heißt Vielfaches von w. v wird Komplementärteiler von z zu w genannt.

Beispiel 3.1.
Wegen $9 - 7i = (3+i)(2-3i)$, teilt $3+i$ (oder auch $2-3i$) die Gaußsche ganze Zahl $9-7i$ und $9-7i$ ist ein Vielfaches von $3+i$.

Beispiel 3.2.
Teilt $3 + i$ auch $9 + 7i$?

$$\frac{9+7i}{3+i} = \frac{(9+7i)(3-i)}{(3+i)(3-i)} = \frac{34+12i}{10} = \frac{34}{10} + \frac{12}{10}i$$

Dieses Ergebnis befindet sich nicht in $\mathbb{Z}[i]$, weil sich der Realteil $\frac{34}{10}$ und der Imaginärteil $\frac{12}{10}$ jeweils nicht in $\mathbb{Z}$ befinden. Somit teilt $3 + i$ die Zahl $9 + 7i$ nicht.

Proposition 3.1. Eine Gaußsche ganze Zahl $z = a + ib$ ist genau dann durch eine Zahl $c \in \mathbb{Z}$ teilbar, wenn gilt, dass $c \mid a$ und $c \mid b$.

Beweis.
Angenommen $c \mid a+ib$ in $\mathbb{Z}[i]$, dann heißt das nichts anderes als $a+ib = c\cdot(m+in)$ für irgendwelche $m, n \in \mathbb{Z}$. Das ist aber äquivalent zu $a = c \cdot m$ und $b = c \cdot n$, was nichts anderes bedeutet als $c \mid a$ und $c \mid b$. □

Definition 3.3. Die Norm einer Gaußschen ganzen Zahl

Sei $z \in \mathbb{Z}[i]$ mit $z = a + ib$ wobei $a, b \in \mathbb{Z}$. Die Norm $N(z) = N(a + ib)$ von z ist definiert durch: $N(z) = N(a + ib) = a^2 + b^2$ $(= (a + ib) \cdot (a - ib) = z \cdot \overline{z})$

Beispiel 3.3.
Als Beispiel ist die Norm von $3 + 4i$ gesucht:
$N(3 + 4i) = 3^2 + 4^2 = 9 + 16 = 25$.

Bemerkungen:
1) Für ein $m \in \mathbb{Z}$ ist $N(m) = m^2$. Inbesondere ist $N(1) = 1$.
2) Der Grund dafür, sich lieber mit Normen auf $\mathbb{Z}[i]$ zu beschäftigen als mit Beträgen auf $\mathbb{Z}[i]$, ist, dass es sich bei Normen um ganze Zahlen und nicht um Quadratwurzeln handelt.

Außerdem werden die Teilbarkeitseigenschaften von Normen in $\mathbb{Z}$ wichtige Informationen über Teilbarkeitseigenschaften in $\mathbb{Z}[i]$ liefern. Das jedoch basiert auf dem folgenden Lemma (3.2).

Lemma 3.2. Es gelten folgende Eigenschaften über Normen:

i) $N(zw) = N(z)N(w)\ \forall z, w \in \mathbb{Z}[i]$

ii) Wenn $w \mid z$ in $\mathbb{Z}[i]$, dann $N(w) \mid N(z)$ in $\mathbb{Z}$

iii) $\mathbb{Z}[i]$ ist nullteilerfrei. Das heißt es ist nicht möglich, dass $z \cdot w = 0$ wenn $z, w \neq 0$.

Beweis.

i)

$$\begin{aligned} N(zw) &= N((a+bi)(c+id)) \\ &= N((ac-bd)+i(ad+bc)) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2adbc + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(d^2+c^2) = \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(a+ib)N(c+id) \\ &= N(z)N(w) \end{aligned}$$

ii) Wenn $w \mid z$ in $\mathbb{Z}[i]$ dann existiert ein $v \in \mathbb{Z}[i]$ für das gilt $z = wv$. Damit gilt auch $N(z) = N(wv)$. Aufgrund des vorherigen Beweises gilt: $N(z) = N(w)N(v)$. Somit wurde eine Zahl $u = N(v) \in \mathbb{Z}$ gefunden, für die $N(z) = N(w) \cdot u$ gilt. Daraus folgt $N(w) \mid N(z)$ in $\mathbb{Z}$.

iii) Angenommen $zw = 0$ mit $z, w \neq 0$. Dann muss auch die Norm $N(zw) = 0$ sein. Da $N(zw) = N(z)N(w)$, muss laut dem Produktnullsatz entweder

$N(z) = 0$ oder $N(w) = 0$ sein. Wenn $N(z) = 0$ gilt, dann muss $z = 0$ auch gelten. Selbiges gilt auch bei $N(w)$. Dies stellt einen Widerspruch dar. Somit ist $zw = 0$ nicht möglich, wenn $z, w \neq 0$ sind.

□

Lemma 3.2 *ii*) ist sehr nützlich, um auf schnellem Wege zu sehen, ob eine Gaußsche ganze Zahl eine andere teilen kann. Zuerst wird überprüft, ob die Teilbarkeit der Normen zutrifft. Als Beispiel soll herausgefunden werden, ob $2 + i$ die Zahl $8 + 5i$ teilt. Es werden zuerst die Normen gebildet. $N(2 + i) = 5$ und $N(8 + 5i) = 89$. Hier ist leicht zu erkennen, dass 5 die Zahl 89 nicht teilt. Somit teilt $2 + i$ die Zahl $8 + 5i$ auch nicht.
Bricht man das Teilbarkeitsproblem in $\mathbb{Z}[i]$ auf ein Teilbarkeitsproblem in $\mathbb{Z}$ herunter, lässt sich das Problem angenehmer behandeln, da hier die üblichen Regeln der Teilbarkeit in $\mathbb{Z}$ genutzt werden können. Lemma 3.2 sagt aber nur, dass die Teilbarkeit der Normen in $\mathbb{Z}$ aus der Teilbarkeit in $\mathbb{Z}[i]$ folgt. Die Umkehrung gilt nicht.
Gegeben seien zwei Zahlen $3 + i$ und $9 + 7i$. Dann gilt $N(3 + i) = 10$ und $N(9 + 7i) = 130 = 10 \cdot 13$, somit gilt $N(3 + i) \mid N(9 + 7i)$ in $\mathbb{Z}$. In Beispiel 3.2 wurde jedoch gezeigt, dass $(3 + i) \mid (9 + 7i)$ nicht gilt.
Eine sichere Methode, um die Teilbarkeit in $\mathbb{Z}[i]$ zu verifizieren, ist die Überprüfung, ob der Quotient, nachdem der Nenner zu einer ganzen Zahl umgeformt wurde, in $\mathbb{Z}[i]$ liegt, genauso wie es in Beispiel 3.2 gemacht wurde. Die Normteilbarkeit in $\mathbb{Z}$ ist eine notwendige Bedingung für die Teilbarkeit in $\mathbb{Z}[i]$. Wenn die Normteilbarkeit versagt, dann versagt auch die Teilbarkeit in $\mathbb{Z}[i]$. Dennoch reicht die Normteilbarkeit nicht aus, um die Teilbarkeit in $\mathbb{Z}[i]$ zu bestätigen.

Eine erste Anwendung von Lemma 3.2 wird sein, die Gaußschen ganzen Zahlen herauszufinden, die in $\mathbb{Z}[i]$ multiplikative Inverse besitzen. Dafür werden die Normen ein sehr nützliches Werkzeug sein.

Proposition 3.2. Die einzigen Gaußschen ganzen Zahlen, die multiplikative Inverse in $\mathbb{Z}[i]$ besitzen, sind $1, -1, i$ und $-i$.

Beweis.
Es ist einfach zu sehen, dass $1, -1, i$ und $-i$ multiplikative Inverse in $\mathbb{Z}[i]$ besitzen: 1 und -1 sind ihre eigenen multiplikativen Inversen und i bzw. $-i$ sind die multiplikativen Inversen zueinander.
Nun ist zu zeigen, dass es keine anderen Gaußschen ganzen Zahlen gibt, die in $\mathbb{Z}[i]$ multiplikative Inverse besitzen:
Angenommen die Zahl $z = a + ib \in \mathbb{Z}[i]$ besitzt ein multiplikatives Inverses. Dann muss gelten: $z \cdot w = 1$ für irgendein $w \in \mathbb{Z}[i]$. Nun wird gezeigt, dass $z \in \{1, -1, i, -i\}$ sein muss. Hierzu wird die Norm auf beiden Seiten der Gleichung $zw = 1 \Rightarrow N(z)N(w) = 1$ gebildet. Das stellt eine Gleichung in $\mathbb{Z}$ dar und deswegen muss $N(z) = \pm 1$ sein. Weil die Norm keine negativen Werte annehmen kann, wird nur $N(z) = 1$ näher betrachtet. Somit ergibt sich die Gleichung $N(z) = a^2 + b^2 = 1$. Da das nur für $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ möglich ist, kann z nur die Werte $1, -1, i$ und $-i$ annehmen. □

Bemerkungen:
1) Diese Elemente werden Einheiten genannt. Die Einheiten in $\mathbb{Z}$ sind 1 und -1. Die Einheiten von $\mathbb{Z}[i]$ wurden in Proposition 3.2 näher erläutert (siehe auch Definition 3.4). Das Wissen darüber, mit welcher Einheit eine Gaußsche ganze Zahl multipliziert werden kann, ist mit dem Wissen zu vergleichen, welches Vorzeichen eine ganze Zahl besitzt.

2) Da es auf den Gaußschen ganzen Zahlen keine Ordnungsrelation gibt, ist es nicht möglich, über Ungleichungen zu sprechen. Auch hierfür können wieder Normen herangezogen werden, denn bei Normen lässt sich sehr wohl über Ungleichungen reden. Um eine Aussage mit Hilfe von Induktion für die Gaußschen ganzen Zahlen zu beweisen, ist es notwendig, dies mit der Norm zu bewerkstelligen.

3) Die Norm von jeder Gaußschen ganzen Zahl ist eine positive ganze Zahl, aber nicht jede positive ganze Zahl ist eine Norm einer Gaußschen ganzen Zahl. Das

liegt an der Definition der Norm (vgl. Definition 3.3). Die Norm ist ja eine ganze Zahl in der Form a^2+b^2. Hier liegt das Problem. Es ist nicht möglich, jede beliebige positive ganze Zahl als Summe von zwei Quadratzahlen darzustellen (vgl. Lemma 2.2). Beispiele dafür wären die Zahlen $3, 7, 11, 15, 19$ oder 21. Keine Gaußsche ganze Zahl hat eine dieser Zahlen als Norm.

Definition 3.4. Einheit von $\mathbb{Z}[i]$

Ein $z \in \mathbb{Z}[i]$ wird als Einheit von $\mathbb{Z}[i]$ bezeichnet, wenn es ein multiplikatives Inverses in $\mathbb{Z}[i]$ besitzt. Das heißt $\exists w \in \mathbb{Z}[i]$ mit der Eigenschaft $zw = 1$. Die Menge der Einheiten von $\mathbb{Z}[i]$ wird mit $\mathbb{Z}[i]^*$ bezeichnet.

Proposition 3.3. Ein $z \in \mathbb{Z}[i]$ ist genau dann eine Einheit von $\mathbb{Z}[i]$, wenn $N(z) = 1$.

Beweis.
Ist z eine Einheit, so existiert ein $w \in \mathbb{Z}[i]$ mit $zw = 1$. Nach Proposition 3.2 ist $N(z)N(w) = N(zw) = N(1) = 1$. Da die Norm einer Gaußschen ganzen Zahl in $\mathbb{N}$ liegt, folgt daraus $N(z) = N(w) = 1$. Ist $N(z) = N(a + ib) = 1$, so ist nach Definition von $N(z) = (a+ib)(a-ib)$ das Produkt $(a+ib)(a-ib) = 1$. Das heißt, $a + ib = z$ ist eine Einheit. □

Mit Hilfe dieser Kenntnis kann ebenfalls gezeigt werden, welche Einheiten in $\mathbb{Z}[i]$ existieren.

Proposition 3.4. $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{1, -1, i, -i\}$

Beweis.
Die Gültigkeit dieser Proposition wurde schon in Proposition 3.2 gezeigt. Dennoch wird hier ein Beweis geschildert, dem Proposition 3.3 zu Grunde liegt.
$N(z) = N(a+ib) = a^2+b^2 = 1$. Es gibt zwei Möglichkeiten, die Gleichung in $\mathbb{Z}$ zu lösen. Entweder ist $a^2 = 1$ oder $b^2 = 1$. In diesen beiden Fällen kann die Lösung nur 1 oder -1 sein. Somit kann x nur $1, -1, i$ oder $-i$ sein. □

Proposition 3.5. Die Norm einer Gaußschen ganzen Zahl ist gerade, genau dann, wenn die Gaußsche ganze Zahl ein Vielfaches von $1 + i$ ist.

Beweis.
$\Rightarrow$ Wegen $N(1+i) = 2$ muss jedes Vielfaches von $1+i$ eine gerade Norm aufweisen.
$\Leftarrow$ Angenommen eine Zahl $a + ib \in \mathbb{Z}[i]$ hat eine gerade Norm, dann gilt:
$a^2 + b^2 = 2k$ für irgendein $k \in \mathbb{Z}$. Nun gibt es drei Fälle:

i) a und b sind beide gerade. Das heißt, es gibt $m, n \in \mathbb{Z}$, für die gilt $a = 2m$ und $b = 2n$.

$$\begin{aligned} a^2 + b^2 &= (2m)^2 + (2n)^2 \\ &= 4m^2 + 4n^2 \\ &= 2(2m^2 + 2n^2) \end{aligned}$$

Das Ergebnis ist in der Form $2k$, somit ist $a^2 + b^2$ gerade.

ii) a und b sind beide ungerade. Das heißt, es gibt $m, n \in \mathbb{Z}$, für die gilt $a = 2m + 1$ und $b = 2n + 1$.

$$\begin{aligned} a^2 + b^2 &= (2m + 1)^2 + (2n + 1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &= 2(2m^2 + 2m + 2n^2 + 2n + 1) \end{aligned}$$

Das Ergebnis ist in der Form $2k$, somit ist $a^2 + b^2$ gerade.

iii) O.B.d.A ist a gerade und b ungerade. Das heißt, es gibt $m, n \in \mathbb{Z}$, für die gilt $a = 2m$ und $b = 2n + 1$.

$$\begin{aligned} a^2 + b^2 &= (2m)^2 + (2n + 1)^2 \\ &= 4m^2 + 4n^2 + 4n + 1 \\ &= 2(2m^2 + 2n^2 + 2n) + 1 \end{aligned}$$

Das Ergebnis ist in der Form $2k + 1$, somit ist $a^2 + b^2$ ungerade.

Das Resultat bedeutet, dass a und b entweder beide gerade oder beide ungerade sein müssen. Nun muss gezeigt werden, dass $1 + i \mid a + ib$ gilt. Das heißt es gibt ein $x + iy \in \mathbb{Z}[i]$, für das gilt: $a + ib = (1 + i)(x + iy)$, was dasselbe ist wie:

$$a + ib = (x - y) + i(x + y)$$

Nun wird diese Gleichung nach x und nach y aufgelöst und die Ergebnisse lauten wie folgt: $x = \frac{b+a}{2}$ und $y = \frac{b-a}{2}$. Das sind ganze Zahlen, da a und b immer dieselbe Parität haben. Daraus folgt $1 + i \mid a + ib$ □

Beispiel 3.4.
Die Norm von $1 + 5i$ ist 26, also gerade, weil $1 + 5i = (1 + i)(3 + 2i)$.

Beispiel 3.5.
Weil die Norm von $1 - i$ gleich 2 ist, muss auch diese Zahl ein Vielfaches von $1 + i$ sein und tatsächlich gilt $1 - i = (-i)(1 + i)$.

3.2 Division mit Rest in $\mathbb{Z}[i]$

Lemma 3.3. Für alle $z, w \in \mathbb{Z}[i]$, wobei $w \neq 0$, existieren $v, u \in \mathbb{Z}[i]$, die die Eigenschaften $z = wv + u$ und $N(u) < N(w)$ aufweisen. Der Summand u kann so gewählt werden, dass sogar $N(u) \leqslant \frac{1}{2}N(w)$ gefordert werden kann.
Der Ausdruck v heißt Quotient bei Division von z durch w. Der Summand u wird Rest bei Division von z durch w genannt.

Bevor Lemma 3.3 bewiesen wird, ist es sinnvoll zu sehen, dass es nicht so einfach ist, v und u zu berechnen. Anhand eines Beispiels lässt sich dieses Lemma womöglich am einfachsten verstehen.

Beispiel 3.6.
Sei $z = 27 - 23i$ und $w = 8 + i$. Die Norm von w ist 65. Es soll die Beziehung $z = wv + u$ erfüllt werden wobei $N(u) < 65$ gelten soll.

Die Idee ist zuerst den Quotienten $\frac{z}{w}$ zu bilden und dann den Nenner zu einer ganzen Zahl umzuformen:

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{(27-23i)(8-i)}{65} = \frac{193-211i}{65}$$

Weil $\frac{193}{65} = 2.969...$ und $\frac{-211}{65} = -3.246...$ sind, wird bei zweimaliger Anwendung der üblichen Division mit Rest (wie in Proposition 2.1) der wahre Quotient durch eine ganze Zahl ersetzt, die nicht am nächsten liegt. Dadurch kann die Zahl v gebildet werden. Sei somit $v = 2 - 4i$. Anschließend wird u berechnet:

$$z - w(2-4i) = 7 + 7i = u$$

Das wäre aber eine schlechte Idee, weil $N(u) = N(7+7i) = 98 > 65 = N(w)$ gilt. Das Nützliche an einer Division mit Rest ist ja der betragsmäßig kleinere Rest, als der Divisor. Somit ist die Wahl, die für v getroffen wurde, nicht die beste. Das ist eben die Schwierigkeit, von der zuvor gesprochen wurde. Es muss genauer darüber nachgedacht werden, durch welche ganzen Zahlen die Quotienten $\frac{193}{65} = 2.969...$ und $\frac{-211}{65} = -3.246...$ ersetzt werden können. Werden die Quotienten genauer betrachtet, kann festgestellt werden, dass sich $\frac{193}{65} = 2.969...$ näher an 3 als an 2 befindet. Ebenfalls befindet sich $\frac{-211}{65} = -3.246...$ näher an -3 als an -4. Damit lässt sich ein anderes $v = 3-3i$ bilden, mit dem sich u anschließend wieder berechnen lässt:

$$z - w(3-3i) = -2i = u$$

Letztendlich erfüllt das die gewollte Eigenschaft, denn
$N(u) = N(-2i) = 4 < 65 = N(w)$.
Das heißt, es ist in $\mathbb{Z}$ möglich, diejenigen ganzen Zahlen zu wählen, die am nächsten an dem Quotienten sind und nicht jene ganzen Zahlen, die man bei der üblichen Division mit Rest erhält.
Zum Beispiel ist $\frac{34}{9} = 3.77...$ näher bei 4 als bei 3.

Um das mit Hilfe der Division mit Rest auszudrücken, ist die Gleichung

$$34 = 9 \cdot 4 - 2$$

der Gleichung

$$34 = 9 \cdot 3 + 7$$

zu bevorzugen. Der Rest ist in der ersten Gleichung zwar negativ, dennoch ist er betragsmäßig der kleinere Wert. Was hier gefunden wurde, ist eine Modifikation der Division mit Rest in $\mathbb{Z}$, die Division mit absolut kleinstem Rest.
Eigentlich sagt Proposition 2.1: bq, ein Vielfaches von b, ist das nächste Vielfache von b an a, das kleiner oder gleich ist: $bq \leq a < b(q+1)$. Dann ist $r = a - bq$ mit $r \geq 0$, weil $bq \leq a$, und $r < |b|$, weil bq und $b(q+1)$ ja $|b|$ ganze Zahlen voneinander entfernt sind und a muss nicht näher an bq als an $b(q+1)$ liegen.
Bei der Divsision mit absolut kleinstem Rest ist bq ebenfalls ein Vielfaches von b. Jedoch ist bq das absolut nächste Vielfache von b, aber nicht unbedingt kleiner oder gleich a. Rechnerisch gesehen, kann das q in der Divsion mit absolut kleinstem Rest die nächste ganze Zahl bei $\frac{a}{b}$ sein, die größer statt kleiner als $\frac{a}{b}$ ist.
Eine ganze Zahl ist nie weiter weg als $\frac{1}{2}|b|$ von einem Vielfachen von b in beide Richtungen. Somit gilt: $|a - bq| \leq \frac{1}{2}|b|$. Damit ist $r = a - bq$ und das ergibt $a = bq + r$ mit $|r| \leq \frac{1}{2}|b|$.
Bei der ursprünglichen Division mit Rest ist der Rest r nicht negativ und nach oben begrenzt durch $|b|$. Die Obergrenze wurde somit verkleinert, jedoch auf Kosten der Nichtnegativität des Restes.
Manchmal jedoch kann a direkt zwischen zwei Vielfachen von b landen. In diesen Fällen ist die Eindeutigkeit des Quotienten q und des Restes r nicht mehr gegeben. Das wäre der Fall bei $a = 26$ und $b = 4$. a liegt genau zwischen $6b$ und $7b$:

$$26 = 4 \cdot 6 + 2$$
$$26 = 4 \cdot 7 - 2$$

Nun gibt es zwei Möglichkeiten für den Rest r, 2 oder -2. Wie schon gesagt, sind der Quotient und der Rest in der ursprünglichen Division mit Rest eindeutig. In der erweiterten Version wird diese Eindeutigkeit aufgegeben.

Das klingt zwar nach einer regelrechten Katastrophe, dennoch ist das genau das, was benötigt wird, um die Division mit Rest in $\mathbb{Z}[i]$ (Lemma 3.3) zu beweisen. Das wird auch der nächste Schritt sein. In dem Beweis wird die erfolgreiche Vorgangsweise in Beispiel 3.6 in allgemeinen algebraischen Begriffen formuliert.

Beweis. von Lemma 3.3
Gegeben sei $z, w \in \mathbb{Z}[i]$ mit $w \neq 0$. $v, u \in \mathbb{Z}[i]$ sind so zu konstruieren, dass $z = wv + u$ gilt, wobei $N(u) \leq \frac{1}{2}N(w)$:

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{z\overline{w}}{N(w)} = \frac{m + in}{N(w)}$$

Hier wird $z\overline{w} = m + in$ gesetzt, wobei $m, n \in \mathbb{Z}$. Nun wird m und n durch $N(w)$ geteilt und die eben besprochene Division mit absolut kleinstem Rest angewendet:

$$m = N(w)q_1 + r_1,\ n = N(w)q_2 + r_2, \text{ mit } q_i, r_i \in \mathbb{Z}$$

Weiters gilt: $0 \leq |r_1|, |r_2| \leq \frac{1}{2}N(w)$, dann ist:

$$\begin{aligned}\frac{z}{w} &= \frac{N(w)q_1 + r_1 + i(N(w)q_2 + r_2)}{N(w)} \\ &= q_1 + iq_2 + \frac{r_1 + ir_2}{N(w)}\end{aligned}$$

Sei nun $v = q_1 + iq_2$, so gilt:

$$\begin{aligned}\frac{z}{w} = q_1 + iq_2 + \frac{r_1 + ir_2}{N(w)} &\Leftrightarrow \frac{z}{w} = v + \frac{r_1 + ir_2}{N(w)} \\ &\Leftrightarrow \frac{z}{w} = v + \frac{r_1 + ir_2}{w\overline{w}} \\ &\Leftrightarrow z = wv + \frac{r_1 + ir_2}{\overline{w}} \\ &\Leftrightarrow z - wv = \frac{r_1 + ir_2}{\overline{w}}\end{aligned}$$

Anschließend wird die Beziehung $N(z - wv) \leq \frac{1}{2}N(w)$ gezeigt, somit wäre mit $u = z - wv$ die Division mit Rest in $\mathbb{Z}[i]$ bestätigt. Es wird die Norm auf beiden Seiten der Gleichung berechnet. Aus $(z - wv)\overline{w} = r_1 + ir_2$ folgt sofort

$$N(z - wv) = \frac{r_1^2 + r_2^2}{N(\overline{w})}$$

Weil die Norm einer Zahl $w \in \mathbb{Z}[i]$ denselben Wert hat wie die Norm von $\overline{w}$, ergibt dies:

$$N(z - wv) = \frac{r_1^2 + r_2^2}{N(w)}$$

Diese Gleichung wird nun mit der Bedingung $0 \leq |r_1|, |r_2| \leq \frac{1}{2}N(w)$ verbunden und somit gilt:

$$N(u) = N(z - wv) \leq \frac{\frac{1}{4}N(w)^2 + \frac{1}{4}N(w)^2}{N(w)} = \frac{1}{2}N(w)$$

Schlussendlich ist damit Lemma 3.3 bewiesen. □

Beispiel 3.7.
Sei $z = 23 + 10i$ und $w = 2 - i$. Damit ist:

$$\frac{z}{w} = \frac{23 + 10i}{2 - i} \cdot \frac{2 + i}{2 + i} = \frac{36 + 43i}{5} = \frac{36}{5} + \frac{43}{5}i$$

Sei nun $v = 7 + 8i$. Die Zahl $u = z - wv = 1 + i$ erfüllt die Bedingung
$N(u) = 2 < 5 = N(w)$. Somit gilt $z = wv+u$, also: $23+10i = (7+8i)\cdot(2-i)+(1+i)$

Beispiel 3.8.
Bei Beispiel 3.7 ist das Ergebnis nicht verwunderlich. Es wurden genau die Schritte befolgt, nur kürzer, die bei Beispiel 3.6 durchgeführt wurden. Wie sieht es nun aus, wenn bei einem Beispiel zwei unterschiedliche Werte gewählt werden können. Sei $z = 1 + 8i$ und $w = 2 - 4i$, dann ist:

$$\frac{z}{w} = \frac{1 + 8i}{2 - 4i} \cdot \frac{2 + 4i}{2 + 4i} = \frac{-30 + 20i}{20} = -\frac{3}{2} + i$$

Hier liegt jetzt $-\frac{3}{2}$ zwischen -2 und -1 genau in der Mitte. Das heißt, es ist möglich für v zwei verschiedene Zahlen einzusetzen. Das heißt $v_1 = -1 + i$ oder $v_2 = -2 + i$. Setzt man v_1 ein, so:

$$z = w(-1 + i) + (-1 + 2i) \text{ und } N(v_1) = 5 < 20 = N(w)$$

Für v_2 dann:

$$z = w(-2 + i) + (1 - 2i) \text{ und } N(v_2) = 5 < 20 = N(w)$$

Dieser Division in $\mathbb{Z}[i]$ fehlt zwar die Eindeutigkeit des Quotienten und des Restes, dennoch schränkt dies die Nützlichkeit keineswegs ein. Die Division mit Rest in $\mathbb{Z}[i]$ wird deswegen im nächsten Kapitel sehr nützlich sein.

3.3 Der Euklidische Algorithmus in $\mathbb{Z}[i]$

Definition 3.5. Größter gemeinsamer Teiler in $\mathbb{Z}[i]$

Für zwei Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$ wird eine Zahl $g \in \mathbb{Z}[i]$ größter gemeinsamer Teiler genannt, wenn folgende beiden Eigenschaften gelten:

i) g ist ein Teiler von z und w, das heißt $g \mid z$ und $g \mid w$.

ii) Wenn für ein $h \in \mathbb{Z}[i]$ gilt, dass $h \mid z$ und $h \mid w$, dann gilt auch $h \mid g$.

Eine Folgerung aus dieser Definition ist:
Für zwei Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$ ist ein größter gemeinsamer Teiler ein Teiler, der die maximale Norm aufweist. Aus $h \mid g$ (in $\mathbb{Z}[i]$) in ii) folgt ja $N(h) \mid N(g)$ (in $\mathbb{Z}$) und daher $N(h) \leqslant N(g)$. Sind g und g' zwei größte gemeinsame Teiler, so folgt aus ii) $g \mid g'$ und $g' \mid g$, das heißt $\exists u, v \in \mathbb{Z}[i]$ mit $g' = ug$ und $g = vg'$. Daraus folgt $g = vg' = uvg$ und daher $uv = 1$ und $u, v \in \mathbb{Z}[i]^*$. Also ist $N(g') = N(ug) = N(u)N(g) = 1 \cdot N(g) = N(g)$.

Die Folgerung aus Definition 3.5 ist analog zur Definition des größten gemeinsamen Teilers in $\mathbb{Z}$, außer dass in $\mathbb{Z}[i]$ der größte gemeinsame Teiler keine eindeutige Zahl ist.
Angenommen g ist ein größter gemeinsamer Teiler von z und w, so sind auch die Einheitenvielfachen $-g$, ig und $-ig$ größte gemeinsame Teiler von z und w. Es lässt sich somit nur von einem größten gemeinsamen Teiler sprechen, nicht aber von dem größten gemeinsamen Teiler.

Definition 3.6. Relativ prim (teilerfremd)

Zwei Zahlen $z, w \in \mathbb{Z}[i]$ werden relativ prim (oder teilerfremd) genannt, wenn einer ihrer größten gemeinsamen Teiler eine Einheit ist.

Lemma 3.4. (**Euklidischer Algorithmus**) Wird die Division mit Rest aus Lemma 3.3 für die Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$ immer wieder durchgeführt, das heißt:

$$\begin{aligned}
z &= wv_0 + u_1 \\
w &= u_1v_1 + u_2 \\
u_1 &= u_2v_2 + u_3 \\
... &= ... \\
&... \\
... &= ... \\
u_{n-2} &= u_{n-1}v_{n-1} + u_n \\
u_{n-1} &= u_nv_n + 0
\end{aligned}$$

mit $N(w) > N(u_1) > ... > N(u_{n-2}) > N(u_{n-1}) > N(u_n)$, so bricht dieses Verfahren irgendwann ab. Dieses Verfahren wird auch euklidischer Algorithmus genannt. Daraus folgt, dass u_n ein größter gemeinsamer Teiler von z und w ist.

Beweis.

- Werden die oben genannten Gleichungen von unten nach oben betrachtet, so zeigt sich bei der letzten Gleichung, dass u_n ein Teiler von u_{n-1} sein muss. Da u_n ein Teiler von u_{n-1} ist, folgt aus der vorletzten Gleichung, dass u_n auch u_{n-2} teilt. Wenn dies weitergeführt wird, lässt sich erkennen, dass u_n alle u_k mit $k \in \{n, n-1, n-2, ..., 3, 2, 1\}$ teilt. Schließlich erhält man, dass u_n auch gemeinsamer Teiler von z und w ist.

- Jeder Teiler h von z und w ist auch ein Teiler von u_n. Um das zu erkennen, werden die oben genannten Gleichungen von oben nach unten betrachtet. Aus der ersten Gleichung folgt, dass h auch ein Teiler von u_1 ist. Da h ein Teiler von w und u_1 ist, folgt aus der zweiten Gleichung, dass h auch ein Teiler von u_2 ist. Und so weiter und so fort. Zum Schluss ergibt sich, dass h auch ein Teiler von u_n sein muss.

□

Bemerkung:
Lemma 3.4 zeigt, dass für zwei Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$ stets ein größter gemeinsamer Teiler existiert.

Beispiel 3.9.
Der größte gemeinsame Teiler von $z = 32 + 9i$ und $w = 4 + 11i$ soll ermittelt werden. Somit lautet der euklidische Algorithmus:

$$\begin{aligned} 32 + 9i &= (4 + 11i)(2 - 2i) + (2 - 5i) \\ 4 + 11i &= (2 - 5i)(-2 + i) + (3 - i) \\ 2 - 5i &= (3 - i)(1 - i) - i \\ 3 - i &= (-i)(1 + 3i) + 0 \end{aligned}$$

Der letzte Rest, der nicht 0 ergibt, ist $-i$. Das ist also ein größter gemeinsamer Teiler von z und w. Somit sind sie auch teilerfremd zueinander (vgl. Definition 3.6). Man stellt hier fest, dass es hier einen großen Unterschied zu dem Algorithmus in $\mathbb{Z}$ gibt. Hier muss bei teilerfremden Zahlen nicht notwendigerweise 1 der größte gemeinsame Teiler sein. Hier reicht es, eine Einheit in $\mathbb{Z}[i]$ zu erhalten.

Beispiel 3.10.
Mit diesem Beispiel lässt sich zeigen, dass $4 + 5i$ und $4 - 5i$, die ja zueinander komplex konjugiert sind, somit auch teilerfremd zueinander sind:

$$\begin{aligned} 4 + 5i &= (4 - 5i)i - (1 - i) \\ 4 - 5i &= -(1 - i)(-4) - i \\ -(1 - i) &= -i(-1 - i) + 0 \end{aligned}$$

Der letzte Rest, der nicht 0 ist, ist eine Einheit, somit ist die Aussage gezeigt.

Proposition 3.6. Für zwei Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$ sei g ein größter gemeinsamer Teiler, der mit Hilfe des euklidischen Algorithmus gefunden wurde. Jeder andere größte gemeinsame Teiler von z oder w ist ein Einheitenvielfaches von g.

Beweis.
Sei g' ein größter gemeinsamer Teiler von z und w. Aufgrund des Beweises des euklidischen Algorithmus (Lemma 3.4) muss $g' \mid g$, weil g' ein gemeinsamer Teiler ist. Somit gilt $g = g'v$ für ein $v \in \mathbb{Z}[i]$, also:

$$N(g) = N(g')N(v) \geq N(g')$$

Weil ja g' der größte gemeinsame Teiler ist, hat dessen Norm den maximalen Wert (vgl. Definition 3.5). Somit muss die Ungleichung $N(g) \geq N(g')$ einer Gleichung entsprechen. Das impliziert $N(v) = 1$, somit muss $v \in \{1, -1, i, -i\}$. Damit sind g' und g Einheitenvielfache voneinander. □

3.4 Das Lemma von Bézout

In $\mathbb{Z}$ sagt das Lemma von Bézout, dass für irgendwelche Zahlen $a, b \in \mathbb{Z}$, Zahlen $x, y \in \mathbb{Z}$ mit Hilfe des euklidischen Algorithmus mittels Rücksubstitution gefunden werden können, sodass gilt: $ggT(a, b) = ax + by$. Das heißt, der größte gemeinsame Teiler kann mit Hilfe einer Summe $ax + by$ dargestellt werden. Diese Idee funktioniert auch in $\mathbb{Z}[i]$. Somit gibt es auch hier ein Lemma von Bézout.

Lemma 3.5. (**Lemma von Bézout**) Sei g ein größter gemeinsamer Teiler der beiden Zahlen $z, w \in \mathbb{Z}[i]\backslash\{0\}$. Dann gilt:

$$g = zx + wy$$

für bestimmte $x, y \in \mathbb{Z}[i]$

Beweis.
Da sich die größten gemeinsamen Teiler um Einheiten unterscheiden, reicht es, den Satz nur für einen größten gemeinsamen Teiler zu zeigen (angenommen der größte gemeinsame Teiler wäre zum Beispiel ig, dann muss man die Gleichung nur mit $-i$ multiplizieren und es steht wieder nur g in der Gleichung).
Unter allen Zahlen $k = zx + wy \in \mathbb{Z}[i]$ mit $x, y \in \mathbb{Z}[i]$ beliebig, gibt es sicher auch solche, die $\neq 0$ sind. Sei $g = zx + wy$ eine Zahl mit der kleinsten Norm unter diesen. Da ein größter gemeinsamer Teiler $\tilde{g}$ sowohl z als auch w teilt, teilt ein größter gemeinsamer Teiler auch g, das heißt $\tilde{g} \mid g$.

Nun muss gezeigt werden, dass g auch ein Teiler von z und w ist. Die Division mit Rest in $\mathbb{Z}[i]$ liefert eine Darstellung für $z = vg + u$, wobei $0 \leq N(u) < N(g)$. Wird nun für g die Darstellung $g = zx + wy$ eingesetzt und die Gleichung nach u aufgelöst, so erhält man

$$\begin{aligned} z &= vg + u \\ z &= v(zx + wy) + u \\ z - u &= vzx + vwy \\ -u &= vzx - z + vwy \\ u &= -vzx + z - vwy \\ u &= (1 - vx)z + (-vy)w \end{aligned}$$

Wegen der Forderung, dass g minimale Norm besitzen soll, muss $u = 0$ gelten und deswegen ist g ein Teiler von z. Entsprechend gilt auch, dass g ein Teiler von w ist. Ist h irgendein gemeinsamer Teiler von z und w, so muss $h \mid \tilde{g}$ gelten, woraus (wegen $\tilde{g} \mid g$) auch $h \mid g$ folgt. Damit ist gezeigt, dass g ein größter gemeinsamer Teiler von z und w ist. □

Proposition 3.7. Zwei Zahlen $z, w \in \mathbb{Z}[i]$ sind genau dann teilerfremd zueinander, wenn gilt:

$$1 = zx + wy$$

für bestimmte $x, y \in \mathbb{Z}[i]$

Beweis. Wenn z und w teilerfremd zueinander sind, dann ist 1 ein größter gemeinsamer Teiler, somit gilt $1 = zx + wy$ für bestimmte $x, y \in \mathbb{Z}[i]$ (vgl. Lemma 3.5). Wenn $1 = zx + wy$ für bestimmte $x, y \in \mathbb{Z}[i]$ gilt, dann ist ein gemeinsamer Teiler von z und w, ein Teiler von 1, also eine Einheit. Das sagt aus, dass z und w teilerfremd sind. □

Beispiel 3.11.
Wie in Beispiel 3.9 herausgefunden, sind die beiden Zahlen $z = 32 + 9i$ und $w = 4 + 11i$ teilerfremd zueinander. Ein Beispiel soll veranschaulichen, wie die Linearkombination $zx + wy$ in $\mathbb{Z}[i]$ gebildet werden kann.

$$\begin{aligned}
-i &= (2 - 5i) - (3 - i)(1 - i) \\
&= (2 - 5i) - (w - (2 - 5i)(-2 + i))(1 - i) \\
&= (2 - 5i)(1 + (-2 + i)(1 - i)) - w(1 - i) \\
&= (2 - 5i)(3i) - w(1 - i) \\
&= (z - w(2 - 2i))(3i) - w(1 - i) \\
&= z(3i) - w(7 + 5i)
\end{aligned}$$

Um nun 1 schreiben zu können, wird einfach mit i multipliziert und daraus folgt:

$$1 = z(-3) + w(5 - 7i)$$

Proposition 3.8. Seien $z, w, v \in \mathbb{Z}[i]$, dann gelten folgende Eigenschaften:

i) Wenn z und w teilerfremd sind und es gilt $z \mid wv$, dann gilt auch $z \mid v$.

ii) Wenn z und w teilerfremd sind und gilt $z \mid v$ und $w \mid v$, dann gilt auch $zw \mid v$.

iii) Wenn z, w und v teilerfremd zueinander sind (das heißt aus $u \mid z$, $u \mid w$ und $u \mid v$ folgt, dass $u \in \mathbb{Z}[i]^*$), dann ist das Produkt eines größten gemeinsamen Teilers von z und w und eines größten gemeinsamen Teilers von z und v ein größter gemeinsamer Teiler von z und wv.

iv) Wenn z und w jeweils teilerfremd zu v sind, dann ist auch zw teilerfremd zu v.

Beweis.

i) Wenn z und w teilerfremd sind, dann existieren laut Proposition 3.7 $x, y \in \mathbb{Z}[i]$, für die $zx + wy = 1$ gilt. Daraus folgt: $zvx + wvy = v$. Wegen $z \mid wv$ gilt auch $z \mid zvx + wvy$, also gilt auch $z \mid v$.

ii) $w \mid v$ impliziert $w \mid z\frac{v}{z}$. Weil z und w teilerfremd sind, gilt laut *i)* $w \mid \frac{v}{z}$. Somit gilt auch $zw \mid v$.

iii) Sei g_1 ein größter gemeinsamer Teiler von z und w, g_2 ein größter gemeinsamer Teiler von z und v und g ein größter gemeinsamer Teiler von z und wv. Laut Lemma 3.7 gibt es $x_1, x_2, y_1, y_2 \in \mathbb{Z}[i]$, sodass gilt:

$$g_1 = zx_1 + wy_1$$

$$g_2 = zx_2 + vy_2$$

$\Rightarrow g_1 g_2 = (zx_1 + wy_1)(zx_2 + vy_2) = z(x_2 y_1 w + x_1 y_2 v + x_1 x_2 z) + (wv)(y_1 y_2)$
Das heißt $g \mid g_1 g_2$. Sei g' ein größter gemeinsamer Teiler von g_1 und g_2. Dann muss gezeigt werden, dass g' eine Einheit ist. Es gilt $g' \mid z$, $g' \mid w$ und $g' \mid v$. Das heißt, g' ist ein gemeinsamer Teiler von z, w und v und daher eine Einheit. Das impliziert, g_1 und g_2 sind teilerfremd.
Da jeder gemeinsame Teiler von z und w auch gemeinsamer Teiler von z und wv ist, folgt $g_1 \mid g$. Analog kann $g_2 \mid g$ gezeigt werden. Weil g_1 und g_2 teilerfremd sind, folgt nach *ii)*, dass $g_1 g_2 \mid g$. Also unterscheiden sich g und $g_1 g_2$ nur um eine Einheit und $g_1 g_2$ ist ein größter gemeinsamer Teiler von z und wv.

iv) Wenn z teilerfremd zu v ist und w auch teilerfremd zu v ist, dann sind alle Zahlen teilerfremd zueinander und aus *iii)* folgt die Behauptung.

□

3.5 Primzahlen und Primfaktorzerlegung in $\mathbb{Z}[i]$

In diesem Kapitel werden Gauß-Primzahlen und zusammengesetzte Gaußsche ganze Zahlen eingeführt und die Primfaktorzerlegung in $\mathbb{Z}[i]$ wird bewiesen.
In Lemma 3.2 wurde gezeigt, wenn $w \mid z$ gilt, dann gilt auch $N(w) \mid N(z)$. Somit gilt die Beziehung $1 \leq N(w) \leq N(z)$, wenn $z \neq 0$. Aber welche Teiler von z besitzen die Norm von 1 oder $N(z)$?

Proposition 3.9. Für ein $z \in \mathbb{Z}[i]\backslash\{0\}$ ist jeder Teiler, der die Norm 1 bzw. $N(z)$ hat, eine Einheit bzw. ein Einheitenvielfaches von z.

Beweis.
Sei $w \in \mathbb{Z}[i]\backslash\{0\}$. Wenn $w \mid z$ und $N(w) = 1$, dann ist $w = \pm 1$ oder $w = \pm i$. Wenn $w \mid z$ und $N(w) = N(z)$, dann existiert ja ein Komplementärteiler $v \in \mathbb{Z}[i]$ mit $z = wv$. Auf beiden Seiten wird die Norm gebildet und der gemeinsame Wert von $N(z)$ fällt weg. Daraus folgt, dass $N(v) = 1$ sein muss. Somit ist $v = \pm 1$ oder $v = \pm i$. Das bedeutet, dass w nur $\pm z$ oder $\pm iz$ sein kann. □

Proposition 3.9 sagt nicht, dass die einzigen Gaußschen ganzen Zahlen, die die Norm $N(z)$ haben, nur die Zahlen $\pm z$ oder $\pm iz$ sein können. Das ist nämlich nicht der Fall. Zum Beispiel haben die beiden Zahlen $8 + i$ und $7 + 4i$ die gleiche Norm von 65, dennoch sind sie keine Einheitenvielfachen voneinander.
Was Proposition 3.9 sagt, ist, dass die einzigen Gaußschen ganzen Zahlen, die z teilen und deren Norm $N(z)$ ist, $\pm z$ und $\pm iz$ sind.
Wenn $N(z) > 1$, dann gibt es immer acht offensichtliche Teiler von z: ± 1, $\pm i$, $\pm z$ und $\pm iz$. Diese Teiler werden auch triviale Teiler von z genannt. (Analog gilt dasselbe in $\mathbb{Z}$, nur dass es hier vier triviale Teiler, nämlich $(\pm 1, \pm n)$, gibt, für irgendeine ganze Zahl n mit $|n| > 1$.) Jeder andere Teiler einer Gaußschen ganzen Zahl z wird nicht trivial genannt. Laut Proposition 3.9 sind alle nicht trivialen Teiler von z die Teiler, deren Norm echt zwischen 1 und $N(z)$ liegt.

Definition 3.7. Primelement (Gauß-Primzahl)

Sei $p \in \mathbb{Z}[i]$ mit $N(p) > 1$. p wird zusammengesetzt genannt, wenn p mindestens einen nicht trivialen Faktor besitzt. p wird Primelement, prim oder Gauß-Primzahl genannt, wenn p nur triviale Teiler besitzt.

Für $z = wv$ mit $1 < N(w) < N(z)$ ist zusammengesetzt zu sein äquivalent zu $N(w) > 1$ und $N(v) > 1$. Diese Zerlegung von z, die ein Produkt von Gaußschen ganzen Zahlen darstellt, wird auch nicht triviale Zerlegung genannt. Eine zusammengesetzte Gaußsche ganze Zahl ist also eine Zahl, die eine nicht-triviale Zerlegung zulässt. Als Beispiel ist eine triviale Zerlegung von $7 + i = i(1 - 7i)$. Eine nicht triviale Zerlegung wäre $7 + i = (1 - 2i)(1 + 3i)$.
Eine nicht triviale Zerlegung von 5 wäre $(1 + 2i)(1 - 2i)$. Das ist aber höchst interessant. Anscheinend ist 5 in $\mathbb{Z}[i]$ eine zusammengesetzte Zahl, obwohl 5 in $\mathbb{Z}$ eine Primzahl ist. Sogar die Zahl 2 ist in $\mathbb{Z}[i]$ eine zusammengesetzte Zahl, weil $2 = (1 + i)(1 - i)$.
Aber anscheinend ist 3 auch prim in $\mathbb{Z}[i]$. Das heißt, manche Zahlen sind sowohl in $\mathbb{Z}[i]$ als auch in $\mathbb{Z}$ prim. Um zu zeigen, dass 3 prim in $\mathbb{Z}[i]$ ist, wird eine Aussage auf einen Widerspruch geführt. Angenommen 3 ist eine zusammengesetzte Zahl, dann sei die nicht triviale Zerlegung $3 = zw$. Nun wird die Norm auf beiden Seiten genommen $9 = N(z)N(w)$. Weil diese Zerlegung nicht trivial ist, muss $N(z) > 1$ und $N(w) > 1$ gelten. Somit muss $N(z) = 3$ sein. Das heißt, für ein $z = a + ib$ erhält man $a^2 + b^2 = 3$. Laut Lemma 2.2 ist das aber nicht möglich. Das stellt einen Widerspruch dar. Somit gibt es für 3 nur eine triviale Zerlegung in $\mathbb{Z}[i]$ und somit ist 3 auch prim in $\mathbb{Z}[i]$.
Die folgende Proposition bietet einen Test, um herauszufinden, ob eine Zahl in $\mathbb{Z}[i]$ prim ist. Hierzu wird die Norm benötigt. Das ist ein einfacher Weg, sehr viele Gauß-Primzahlen zu finden. Es ist jedoch notwendig, Primzahlen in $\mathbb{Z}$ zu kennen.

Proposition 3.10. Wenn die Norm $N(p)$ einer Zahl $p \in \mathbb{Z}[i]$ eine Primzahl $r \in \mathbb{Z}$ ist, dann ist auch p prim in $\mathbb{Z}[i]$.

Beweis.
Angenommen p hat die Norm $N(p) = r$, wobei r eine Primzahl in $\mathbb{Z}$ ist. Es kann gezeigt werden, dass p nur triviale Teiler besitzt, somit haben diese Teiler nur die Norm 1 oder $N(p)$. Somit wäre p prim in $\mathbb{Z}[i]$.
Angenommen eine Zerlegung von p wäre $p = zw$ mit $z, w \in \mathbb{Z}[i]$. Auf beiden Seiten die Norm anwenden, ergibt: $r = N(z)N(w)$. Das stellt eine Gleichung dar, die nur aus positiven ganzen Zahlen besteht und r ist eine Primzahl in $\mathbb{Z}$, somit ist $N(z) = 1$ oder $N(w) = 1$. Das heißt, entweder ist z oder w eine Einheit. Somit kann in einer Zerlegung von p kein nicht trivialer Teiler auftauchen. Das heißt, p ist prim. □

Zum Beispiel ist $4 + 5i$ prim in $\mathbb{Z}[i]$, weil $N(4 + 5i) = 41$ ist und 41 ist eine Primzahl in $\mathbb{Z}$. Genau aus diesem Grund ist auch $4 - 5i$ eine Gauß-Primzahl. Genauso wie $1 \pm i$, $1 \pm 2i$, $2 \pm 3i$ und $15 \pm 22i$. All diese Gaußschen ganzen Zahlen sind Gauß-Primzahlen, weil deren Norm eine Primzahl in $\mathbb{Z}$ ist.

Die Umkehrung von Proposition 3.10 gilt nicht. Eine Gauß-Primzahl muss nicht unbedingt eine Primzahl als Norm besitzen. Wie vorhin erwähnt, hat die Zahl 3 die Norm 9, aber 3 ist eine Gauß-Primzahl.
Von nun an soll die Primfaktorzerlegung in $\mathbb{Z}[i]$ in den Vordergrund rücken. Die Existenz der Primfaktorzerlegung wird ähnlich gezeigt wie es in $\mathbb{Z}$ geschieht. Zuerst wird die Existenz der Primfaktorzerlegung in $\mathbb{Z}[i]$ gezeigt und anschließend wird die Eindeutigkeit bewiesen.

Lemma 3.6. (**Existenz der Primfaktorzerlegung in** $\mathbb{Z}[i]$) Jede Zahl $z \in \mathbb{Z}[i]$ mit $N(z) > 1$ kann als Produkt von Gauß-Primzahlen geschrieben werden.

Beweis.
Dieser Beweis wird mit Hilfe von Induktion nach $N(z)$ (nicht nach z) geführt. Sei $N(z) = 2$, dann ist z laut Proposition 3.10 prim. Angenommen $n \in \mathbb{Z}$, $n \geq 3$ und das Lemma ist für jede Gaußsche ganze Zahl, deren Norm zwischen 1 und n liegt schon gezeigt. Dann soll gezeigt werden, dass jede Gaußsche ganze Zahl mit Norm n als Produkt von Gauß-Primzahlen geschrieben werden kann.
Wenn es keine Gaußsche ganze Zahl gibt, die die Norm n besitzt, dann ist nichts zu beweisen. Somit darf angenommen werden, dass es Gaußsche ganze Zahlen gibt, die die Norm n besitzen. Sind alle $z \in \mathbb{Z}[i]$ mit Norm $N(z) = n$ Gaußsche Primzahlen, ist nichts mehr zu zeigen. Angenommen es gibt eine Zahl z mit der Norm n, die aber zusammengesetzt ist, dann existiert eine nicht triviale Zerlegung von z mit $z = wv$, wobei $w, v \in \mathbb{Z}[i]$. Dabei gilt $N(w), N(v) < N(z) = n$. Aufgrund der Anfangshypothese sind w und v Produkte von Gauß-Primzahlen. Somit ist das Produkt dieser beiden Zahlen, also z, auch ein Produkt von Gauß-Primzahlen. Das bedeutet, z kann als Produkt von Gauß-Primzahlen geschrieben werden. □

Somit ist die Existenz der Primfaktorzerlegung in $\mathbb{Z}[i]$ gezeigt. Nun ist noch die Eindeutigkeit zu klären. Dazu kann folgende Proposition benutzt werden, die ein bekanntes Ergebnis von Primzahlen in $\mathbb{Z}$ verallgemeinert.

Proposition 3.11. Sei p prim in $\mathbb{Z}[i]$. Für $z_1, z_2, ..., z_k \in \mathbb{Z}[i]$, wobei $k \in \mathbb{N}$ gilt: Wenn $p \mid z_1 z_2 ... z_k$, dann teilt p auch irgendein z_j (mit $1 \leqslant j \leqslant k$).

Beweis.
Angenommen $k = 2$. Der Beweis für größere k kann durch Induktion geführt werden. Es soll Folgendes gelten: $p \mid z_1 z_2$. Angenommen p teilt z_1 nicht. Das impliziert jedoch, dass p und z_1 teilerfremd sein müssen. Wären sie nicht teilerfremd, dann hätten p und z_1 einen gemeinsamen Teiler, der keine Einheit ist. Dieser würde dann ein Einheitenvielfaches von p sein, da p ja nur triviale Teiler hat, und p ja prim ist. Das würde aber heißen, dass $p \mid z_1$. Das ist laut Annahme aber nicht der Fall. Da p und z_1 teilerfremd sind, ergibt sich durch Proposition 3.8: $p \mid z_2$. □

Nun könnte die Eindeutigkeit der Primfaktorzerlegung gezeigt werden. Es ist jedoch nicht so einfach. Das Folgende ist nämlich falsch. Wenn

$$p_1 p_2 ... p_r = p'_1 p'_2 ... p'_s$$

gilt, wobei die p_k und die p'_j alle Gauß-Primzahlen sind, dann gilt $r = s$ und $p_k = p'_k$ nach geeigneter Umordnung. Der Teil $r = s$ ist richtig. Es ist aber nicht richtig zu erwarten, dass alle Primzahlen, Faktor für Faktor, übereinstimmen. Anschaulich wird das an folgendem Beispiel:

$$5 = (1 + 2i)(1 - 2i) = (2 - i)(2 + i)$$

Hier sind alle Faktoren Gauß-Primzahlen, weil deren Norm 5 ist. Dennoch erscheinen die zwei Gauß-Primzahlen, die in der einen Zerlegung auftauchen, nicht in der anderen Zerlegung. Heißt das nun, dass die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[i]$ nicht bewiesen werden kann? Nein, das heißt es nicht. Wenn Einheitenvielfache zugelassen werden, dann kann eine Übereinstimmung der beiden Zerlegungen gefunden werden.

$$1 + 2i = (2 - i)i$$
$$1 - 2i = (2 + i)(-i)$$

Tatsächlich kann dieses Phänomen auch in $\mathbb{Z}$ auftauchen. Zum Beispiel ist

$$15 = 3 \cdot 5 = (-3) \cdot (-5)$$

Das ist aber keinesfalls ein Beispiel für eine nicht eindeutige Primfaktorzerlegung in $\mathbb{Z}$, weil die Faktoren, bis auf das Vorzeichen, übereinstimmen. Vorzeichen stellen in $\mathbb{Z}$ kein Problem dar, wenn nur positiven ganzen Zahlen und positiven Primzahlen Aufmerksamkeit geschenkt wird. Das Problem ist, dass es in $\mathbb{Z}[i]$ oder generell bei komplexen Zahlen so etwas wie Positivität nicht gibt. Das heißt es ist zwingendermaßen notwendig die Mehrdeutigkeit für die Einheitenvielfachen zu erlauben. Das erklärt auch die Rolle der Einheiten in der eindeutigen Primfaktorzerlegung in $\mathbb{Z}[i]$.

Lemma 3.7. (**Eindeutigkeit der Primfaktorzerlegung in** $\mathbb{Z}[i]$) Jede Zahl $z \in \mathbb{Z}[i]$ mit $N(z) > 1$ besitzt eine eindeutige Primfaktorzerlegung im folgendem Sinne: Wenn

$$z = p_1 p_2 ... p_r = p'_1 p'_2 ... p'_s,$$

wobei die p_k und die p'_j alle Gauß-Primzahlen sind, dann gilt $r = s$ und nach geeigneter Umordnung ist jedes p_k ein Einheitenvielfaches von p'_k

Beweis.
Laut Lemma 3.6 besitzt jedes $z \in \mathbb{Z}[i]$ mit $N(z) > 1$ eine Primfaktorzerlegung. Nun wird die Eindeutigkeit allgemein mit Hilfe von Induktion nach $N(z)$ gezeigt. In dem Fall, dass $N(z) = 2$, ist schon gezeigt, dass solche z Gauß-Primzahlen sind. Angenommen $n \in \mathbb{Z}$, $n \geq 3$ und jede Gaußsche ganze Zahl, dessen Norm zwischen 1 und n liegt, besitzt eine eindeutige Primfaktorzerlegung. Weiters wird angenommen, dass es Gaußsche ganze Zahlen gibt, die die Norm n besitzen (andernfalls müsste nichts bewiesen werden). Dann muss man zusammengesetzte z mit Norm n betrachten. Es werden zwei verschiedene Primfaktorzerlegungen betrachtet, wie im Lemma angesprochen. Weil $p_1 \mid z$ gilt:

$$p_1 \mid p'_1 p'_2 ... p'_s$$

Proposition 3.11 sagt, dass $p_1 \mid p'_j$ für irgendein $j \in \mathbb{N}$. Durch Umordnung kann $j = 1$ erreicht werden, also $p_1 \mid p'_1$. Die einzigen Faktoren von p'_1, die keine Einheiten sind, sind Einheitenvielfache von p'_1. Das heißt $p_1 = ep'_1$ für ein $e \in \{\pm 1, \pm i\}$. Die beiden Primfaktorzerlegungen sehen somit folgendermaßen aus.

$$z = ep'_1 p_2 ... p_r = p'_1 p'_2 ... p'_s,$$

Nun kann auf beiden Seiten p'_1 wegfallen und daraus folgt:

$$ep_2 ... p_r = p'_2 ... p'_s,$$

Sei hierbei der gemeinsame Wert $w \in \mathbb{Z}[i]$, dann gilt $N(w) = \frac{N(z)}{N(p'_1)} < N(z)$. Weil e eine Einheit ist, ist das Produkt ep_2 ebenfalls eine Gauß-Primzahl und es können somit zwei Primzahlzerlegungen für w gefunden werden. Diese beiden

Primfaktorzerlegungen haben $r-1$ Gauß-Primzahlen auf der linken Seite und $s-1$ Gauß-Primzahlen auf der rechten Seite. Weil $N(w) < n$ ist, sagt die Induktionsvoraussetzung, dass w eine eindeutige Primfaktorzerlegung besitzt. Somit gilt $r-1 = s-1$ (und $r = s$) und nach geeigneter Umstrukturierung ergibt sich, dass ep_2 und p'_2 Einheitenvielfache zueinander sind. Das heißt, p_k und p'_k sind Einheitenvielfache für alle $k > 2$. Weil ep_k und p'_k Einheitenvielfache sind, sind auch p_k und p'_k Einheitenvielfache. Somit ist jedes p_k ein Einheitenvielfaches zu p'_k und der Beweis ist damit komplett. □

Das bloße Wissen über Lemma 3.7 und 3.6 ermöglicht noch lange nicht, eine Primfaktorzerlegung für eine Gaußsche ganze Zahl zu finden. Was wäre zum Beispiel die Primfaktorzerlegung von $3+4i$ oder von $2319+1694i$? Es ist ungewohnt, in $\mathbb{Z}[i]$ die Primfaktorzerlegung zu bilden. In $\mathbb{Z}$ sollte dies jedoch vergleichsweise einfach sein. Man kann sich hierbei auf die Norm stützen. Um es im Vorhinein klarzustellen, hier wird kein Lemma oder Ähnliches bewiesen, wie für eine Gaußsche ganze Zahl die Primfaktorzerlegung konstruiert werden kann. Im Anschluss wird nur eine Methode beschrieben.
Die Schlüsselidee dahinter ist, dass eine Zerlegung in $\mathbb{Z}[i]$ eine Zerlegung in $\mathbb{Z}$ impliziert, nämlich:

$$z = wv \Rightarrow N(z) = N(w)N(v)$$

Daraus lässt sich schlussfolgern: „Benutze die Primfaktorzerlegung in $\mathbb{Z}$ für die Norm, um eine mögliche Primfaktorzerlegung in $\mathbb{Z}[i]$ zu finden."
Sei $z = 3 + 4i$. Die Norm von z ist $25 = 5 \cdot 5$. Wenn $3 + 4i$ zerlegt werden soll, dann muss ein nicht trivialer Teiler die Norm 5 haben. So eine Gaußsche ganze Zahl lässt sich leicht finden. Bis auf die Einheitenvielfachen sind das $1 + 2i$ und $1 - 2i$. Nun gibt es drei Varianten, diese beiden Zahlen zu multiplizieren:

$$\begin{aligned}(1+2i)(1+2i) &= -3+4i\\ (1+2i)(1-2i) &= 5\\ (1-2i)(1-2i) &= -3-4i\end{aligned}$$

Hier lässt sich erkennen, dass die letzte Gleichung $-z$ darstellt. Somit ist:

$$3 + 4i = -(1 - 2i)(1 - 2i) = -(1 - 2i)^2$$

Und das ist die Primfaktorzerlegung von $3 + 4i$.

Was ist mit der Zahl $2319 + 1694i$? Ihre Norm ist 8247397. Die Primfaktorzerlegung in $\mathbb{Z}$ von dieser Zahl lautet:

$$8247397 = 17 \cdot 29 \cdot 16729$$

Nun ist es notwendig die Gaußschen ganzen Zahlen mit den Normen $17, 29$ und 16729 zu finden. Diese müssen anschließend so miteinander multipliziert werden, dass $2319 + 1694i$ das Ergebnis ist. Wie können solche Gaußschen ganzen Zahlen gefunden werden? Die Zahlen $17, 29$ und 16729 werden als Summe von Quadraten dargestellt (Kapitel 2.5):

$$\begin{aligned} 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \\ 16729 &= 40^2 + 123^2 \end{aligned}$$

Damit lässt sich die Primfaktorzerlegung in $\mathbb{Z}[i]$ bilden:

$$\begin{aligned} 17 &= (1 + 4i)(1 - 4i) \\ 29 &= (2 + 5i)(2 - 5i) \\ 16729 &= (40 + 123i)(40 - 123i) \end{aligned}$$

(Die Gaußschen ganzen Zahlen, die hier verwendet werden, sind Gauß-Primzahlen, weil ihre Normen alle Primzahlen in $\mathbb{Z}$ sind.) Nun wird von jeder Gleichung ein Faktor gewählt und alle werden miteinander multipliziert. Glücklicherweise ergibt die erste Wahl das gewünschte Ergebnis.

$$2319 + 1694i = -(1 + 4i)(2 + 5i)(40 + 123i)$$

Mit Ausnahme des Vorzeichens ist jeder Faktor auf der rechten Seite der Gleichung prim in $\mathbb{Z}[i]$, weil ihre Normen Primzahlen in $\mathbb{Z}$ sind.

Proposition 3.10 gibt eine hinreichende Bedingung an, wann Gaußsche ganze Zahlen prim sind, nämlich wann ihre Normen Primzahlen in $\mathbb{Z}$ sind. Dennoch ist diese Bedingung keine notwendige. Zum Beispiel ist 3 eine Gauß-Primzahl, obwohl hier die Norm 9 beträgt.
Das Ziel ist es nun, die Gauß-Primzahlen genauer zu klassifizieren. Das wird hier nicht in einem absoluten Sinne betrachtet, sondern eher als eine Anlehnung an die Primzahlen in $\mathbb{Z}$.

Proposition 3.12. Sei $p \in \mathbb{Z}[i]$ prim. Es gibt eine Primzahl $r \in \mathbb{Z}$, für die gilt: $p \mid r$.

Beweis. Es ist immer der Fall, dass p irgendeine positive ganze Zahl teilt, nämlich ihre Norm, weil $N(p) = p\overline{p}$ und somit gilt $p \mid N(p)$. Weil $N(p) > 1$, ist $N(p)$ als ein Produkt von Primzahlen $r_1, r_2, ..., r_k$ in $\mathbb{Z}$ schreibbar:

$$N(p) = r_1 r_2 ... r_k$$

Weil $p \mid N(p)$ in $\mathbb{Z}[i]$ und p eine Gauß-Primzahl ist, muss $p \mid r_j$ für irgendein $j \in \{1, 2, ..., k\}$ gelten (laut Proposition 3.11). □

Proposition 3.12 sagt, dass alle Gauß-Primzahlen in den Griff zu bekommen sind, wenn alle Primzahlen in $\mathbb{Z}$ in Produkte von Gaußschen ganzen Zahlen zerlegt werden. Jede Gauß-Primzahl ist somit ein Teiler einer Primzahl in $\mathbb{Z}$.
Das heißt, aus den Primfaktoren (die in $\mathbb{Z}[i]$ liegen) der Primzahlen aus $\mathbb{Z}$, können alle Gauß-Primzahlen gebildet werden. Hier sind die Primfaktorzerlegungen der ersten drei Primzahlen in $\mathbb{Z}$.

$$2 = (2 + i)(2 - i) \qquad 3 = 3 \qquad 5 = (1 + 2i)(1 - 2i)$$

Beispielsweise ist bei der Primfaktorzerlegung jede andere Gauß-Primzahl, die ein Teiler von 5 ist, ein Einheitenvielfaches von $1+2i$ oder $1-2i$. Das ergibt dann die folgenden acht Zahlen:

$$\begin{array}{cccc} 1+2i & -1-2i & -2+i & 2-i \\ 1-2i & -1+2i & -2-i & 2+i \end{array}$$

Bis auf die Einheitenvielfachen sind diese acht Zahlen in Wirklichkeit nur zwei, nämlich $1+2i$ und $1-2i$.

Lemma 3.8. Eine Primzahl r in $\mathbb{Z}$ ist zusammengesetzt in $\mathbb{Z}[i]$, genau dann, wenn r als Summe von zwei Quadratzahlen in $\mathbb{Z}$ darstellbar ist.
Das heißt, jede Primzahl r in $\mathbb{Z}$, die nicht als Summe von zwei Quadratzahlen in $\mathbb{Z}$ darstellbar ist, ist auch eine Primzahl in $\mathbb{Z}[i]$, also eine Gauß-Primzahl.

Beweis.
Wenn die Primzahl r zusammengesetzt in $\mathbb{Z}[i]$ ist, dann sei eine nicht triviale Zerlegung $r = zw$, wobei $z, w \in \mathbb{Z}[i]$. Wenn auf beiden Seiten die Norm gebildet wird, ergibt das: $r^2 = N(z)N(w)$.
Weil die Zerlegung von r aber nicht trivial war und $r > 0$, muss $N(z) = r$ sein. Wenn $z = a + ib$ ist, dann gilt ja $r = a^2 + b^2$ wegen der vorherigen Gleichung.
Umgekehrt sei angenommen, dass r als Summe von zwei Quadratzahlen darstellbar ist. Das heißt $r = a^2 + b^2$, dann lässt sich ja die nicht triviale Zerlegung

$$r = (a + ib)(a - ib)$$

finden und damit ist r zusammengesetzt in $\mathbb{Z}[i]$. □

Die ersten Primzahlen in $\mathbb{Z}$, die als Summe von zwei Quadratzahlen dargestellt werden können, sind $2, 5, 13, 17$ und 29.

$$2 = 1^2 + 1^2 \qquad 5 = 1^2 + 2^2 \qquad 13 = 2^2 + 3^2$$
$$17 = 1^2 + 4^2 \qquad 29 = 2^2 + 5^2$$

Somit ist jede dieser Primzahlen zusammengesetzt in $\mathbb{Z}[i]$. Beispielsweise ist $17 = (1 + 4i)(1 - 4i)$. Das ist eine Gaußsche Primfaktorzerlegung, weil die Faktoren eine prime Norm in $\mathbb{Z}$ aufweisen und somit sind diese Faktoren auch selbst Gauß-Primzahlen. Die Zerlegung für 2 ist speziell, weil die Primfaktoren ja Einheitenvielfache von einander sind. $1 - i = -i(1 + i)$, somit ist

$$2 = -i(1 + i)^2$$

Beispiele für Primzahlen, die nicht als Summe von zwei Quadraten darstellbar sind, sind $3, 7, 11$ und 19 (siehe Kapitel 2.5).

Proposition 3.13. Wenn eine Primzahl r in $\mathbb{Z}$ zusammengesetzt in $\mathbb{Z}[i]$ ist und $r \neq 2$, dann hat r bis auf Einheitenvielfache genau zwei Gaußsche Primfaktoren, die zueinander komplex konjugiert sind und die Norm r haben.

Beweis.
Laut Lemma 3.8 gibt es $a, b \in \mathbb{Z}$, wenn r zusammengesetzt in $\mathbb{Z}[i]$ ist, derart dass:

$$r = a^2 + b^2 = (a + ib)(a - ib)$$

Weil $a+ib$ und $a-ib$ die Norm r haben und r eine Primzahl in $\mathbb{Z}$ ist, sind diese beiden Zahlen auch prim in $\mathbb{Z}[i]$. Könnten diese beiden Zahlen aber Einheitenvielfache voneinander sein? Dazu muss man sich vier Fälle ansehen:

i) Wenn $a + ib = a - ib$, dann ist $b = 0$ und $r = a^2$. $\Rightarrow$ Widerspruch

ii) Wenn $a + ib = -(a - ib)$, dann ist $a = 0$ und $r = b^2$. $\Rightarrow$ Widerspruch

iii) Wenn $a + ib = i(a - ib)$, dann ist $b = a$ und $r = a^2 + a^2 = 2a^2$.
$\Rightarrow$ Widerspruch zu $r \neq 2$

iv) Wenn $a + ib = -i(a - ib)$, dann ist $b = -a$ und $r = a^2 + a^2 = 2a^2$.
$\Rightarrow$ Widerspruch zu $r \neq 2$

Alle Fälle laufen auf einen Widerspruch hinaus. Damit ist die Behauptung bewiesen. □

Proposition 3.14. Wenn es für eine Primzahl $r \in \mathbb{Z}$ ein $m \in \mathbb{Z}$ mit $r = 4m + 3$ gibt, dann ist r nicht als Summe von zwei Quadratzahlen in $\mathbb{Z}$ darstellbar und r ist somit auch eine Gauß-Primzahl.

Beweis.
Dass r in diesem Fall nicht als Summe von zwei Quadraten in $\mathbb{Z}$ darstellbar ist, wurde schon in Proposition 2.2 gezeigt. Ist r nicht so darstellbar, dann ist r laut Lemma 3.8 eine Primzahl in $\mathbb{Z}[i]$. □

Wie in Kapitel 2.5 behandelt, müssen die drei Gruppen der Primzahlen in $\mathbb{Z}$ näher betrachtet werden, um eine Aussage darüber treffen zu können, welche dieser Primzahlen als Summe von zwei Quadraten in $\mathbb{Z}$ dargestellt werden können. Genau das Gleiche wurde in diesem Kapitel mit den Gauß-Primzahlen gemacht. Es ist klar, wie die Primzahl 2 in Gaußsche Primfaktoren zu zerlegen ist. Kurz vorher wurde geklärt, wie die Primzahlen $r = 4m + 3$ in Gaußsche Primfaktoren zu zerlegen sind. Sie können nicht zerlegt werden, laut Proposition 3.14. Was ist aber nun mit der Primzahlgruppe in $\mathbb{Z}$ mit $r = 4m + 1$?

Proposition 3.15. Wenn es für eine Primzahl $r \in \mathbb{Z}$ ein $m \in \mathbb{Z}$ mit $r = 4m + 1$ gibt, dann ist r als Summe von zwei Quadratzahlen in $\mathbb{Z}$ darstellbar und r ist somit auch in Gauß-Primzahlen zerlegbar.

Beweis.
Dass r in diesem Fall als Summe von zwei Quadraten in $\mathbb{Z}$ darstellbar ist, wurde in Lemma 2.4 gezeigt. Ist r ebenso darstellbar, dann ist r laut Lemma 3.8 zusammengesetzt in $\mathbb{Z}[i]$. □

Um die Gauß-Primzahlen noch näher zu bestimmen, sind noch zwei Propositionen notwendig.

Proposition 3.16. Sei $r \in \mathbb{Z}$, wobei r eine Primzahl ist. Die Primfaktorzerlegung in $\mathbb{Z}[i]$ ist bestimmt durch:

i) $2 = (1 + i)(1 - i) = -i(1 + i)^2$

ii) Wenn $r = 4m + 1$ für ein $m \in \mathbb{Z}$, dann ist $r = p\overline{p}$ ein Produkt von zwei Gauß-Primzahlen p und $\overline{p}$, die zueinander komplex konjugiert sind und keine Einheitenvielfachen voneinander sind.

iii) Wenn $r = 4m + 3$ für ein $m \in \mathbb{Z}$, dann ist r auch eine Gauß-Primzahl.

Beweis.
Teil *i*) muss nur nachgerechnet werden. Teil *ii*) ist eine Konsequenz von Proposition 3.13 und Proposition 3.15. Teil *iii*) ist eine Schlussfolgerung von Proposition 3.14. □

Lemma 3.9. (**Die Gauß-Primzahlen:**) Es existieren genau 3 verschiedene Gruppen von Gauß-Primzahlen. Alle Gauß-Primzahlen sind in diese Gruppen einzuteilen und unterscheiden sich von den angegebenen höchsten um eine Einheit.

i) $1 + i$

ii) p oder $\overline{p}$, wobei $N(p) = r = 4k + 1$ eine Primzahl ist. Dabei sind $r, k \in \mathbb{Z}$ und $p \in \mathbb{Z}[i]$.

iii) r , wobei r eine Primzahl in $\mathbb{Z}$ ist und $r = 4k + 3$ für irgendein $k \in \mathbb{Z}$ gilt.

Beweis.
Proposition 3.12 sagt, dass jede Gauß-Primzahl ein Teiler einer Primzahl in $\mathbb{Z}$ ist. Proposition 3.16 und die Primfaktorzerlegung in $\mathbb{Z}[i]$ sagen, wie sich die Primzahlen in $\mathbb{Z}$ in $\mathbb{Z}[i]$ zerlegen lassen, bis auf ihre Einheitenvielfachen. □

Die Gauß-Primzahlen, die in Lemma 3.9 in Teil i) und ii) vorkommen, besitzen in $\mathbb{Z}$ Norm z bzw. v, während die Gauß-Primzahlen, die in iii) vorkommen, die Norm r^2 besitzen. Das heißt, die Primzahlen $r \in \mathbb{Z}$ für die gilt $r = 4m + 3$ haben in $\mathbb{Z}[i]$ folgende Einheitenvielfache: $\pm r$ und $\pm ir$.
Obwohl die Umkehrung von Proposition 3.10 streng gesehen nicht wahr ist, ist sie dennoch wahr für die interessanten Gauß-Primzahlen, nämlich jene, deren Real- und Imaginärteil nicht 0 ist. Dann ist p eine Primzahl in $\mathbb{Z}[i]$, also eine Gauß-Primzahl, genau wenn $N(p)$ prim in $\mathbb{Z}$ ist.
Diese Klassifikation der Gauß-Primzahlen sagt, dass Gauß-Primzahlen entweder die Norm r oder r^2 aufweisen können, wobei r eine Primzahl in $\mathbb{Z}$ ist. r ist somit Teiler der Norm der Gauß-Primzahl. Insbesondere hat jede Gauß-Primzahl, außer $1+i$, und deren Einheitenvielfache, eine ungerade Norm. Somit hat eine Gaußsche ganze Zahl, die nicht durch $1 + i$ teilbar ist, eine ungerade Norm. Das bedeutet jedoch auch, dass jede Gaußsche ganze Zahl, die durch $1+i$ teilbar ist, eine gerade Norm aufweisen muss.

Das wurde schon in Proposition 3.5 festgestellt, aber nun lässt sich die Richtigkeit dieser Proposition aus einer viel höheren Sicht betrachten, nämlich in Verbindung mit der Primfaktorzerlegung in $\mathbb{Z}[i]$. Proposition 3.5 ist deswegen auch richtig, weil jede Gaußsche ganze Zahl, die eine Norm von größer als 1 hat, ein Produkt von Gauß-Primzahlen ist. $1 + i$ ist die einzige Gauß-Primzahl, bis auf ihre Einheitenvielfache, die eine gerade Norm aufweist.

3.6 Eine Anwendung von $\mathbb{Z}[i]$ auf die Arithmetik in $\mathbb{Z}$

In diesem Kapitel lässt sich eine Erweiterung von Kapitel 2.5 finden.

Proposition 3.17. Sei $r \in \mathbb{Z}$ eine Primzahl, die als Summe von zwei Quadratzahlen geschrieben werden kann. Das heißt $r = x^2 + y^2$ für $x, y \in \mathbb{Z}$. Dann ist es im Wesentlichen so, dass die ganzen Zahlen x und y eindeutig, bis auf Vorzeichen und Reihenfolge, sind. Besonders sind die Quadratzahlen x^2 und y^2 eindeutig, bis auf ihre Reihenfolge.

Beweis.
An der Formulierung der Proposition lässt sich erkennen, dass sie eigentlich gar nichts mit $\mathbb{Z}[i]$ zu tun hat. Sie handelt regelrecht nur von $\mathbb{Z}$. Aber die Kenntnis über $\mathbb{Z}[i]$ wird in diesem Beweis sehr nützlich sein.
Sei $r = x^2 + y^2$, dann gilt in $\mathbb{Z}[i]$, dass r zerlegbar ist im folgenden Sinne:

$$r = (x + iy)(x - iy)$$

Weil $x + iy$ und $x - iy$ beide die Norm r (welche eine Primzahl in $\mathbb{Z}$ ist) besitzen, sind diese beiden Gaußschen ganzen Zahlen ebenfalls prim in $\mathbb{Z}[i]$ (Proposition 3.10). Falls eine zweite Darstellung $r = m^2 + n^2$ existiert, dann sei diese:

$$r = (m + in)(m - in)$$

und $m \pm in$ sind prim in $\mathbb{Z}[i]$.

Aufgrund der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[i]$, muss gelten:

$$x + iy = e(m + in) \text{ oder } x + iy = e(m - in)$$

für irgendeine Einheit $e \in \mathbb{Z}[i]$. Der einzige Unterschied zwischen $m+in$ und $m-in$ ist das Vorzeichen vor dem Imaginärteil. Es soll gezeigt werden, dass die Zahlen x und y eindeutig, bis auf die Ordnung, bestimmt sind und deswegen reicht es, sich den Fall

$$x + iy = e(m + in)$$

anzusehen.

Wenn $e = 1$, dann $m = x$ und $n = y$.
Wenn $e = -1$, dann $m = -x$ und $n = -y$.
Wenn $e = i$, dann $m = y$ und $n = -x$.
Wenn $e = -i$, dann $m = -y$ und $n = x$.

Somit sind m und n das Gleiche wie x und y bis auf die Ordnung und Vorzeichen. □

Proposition 3.17 sagt nicht, dass jede ganze Zahl, die als Summe von zwei Quadratzahlen geschrieben werden kann, nur eine Darstellung in dieser Form hat. Die Proposition bezieht sich nur auf Primzahlen in $\mathbb{Z}$. Hier sind zwei zusammengesetzte Zahlen, für die es mehr als eine Darstellung gibt:

$$50 = 5^2 + 5^2 = 1^2 + 7^2$$
$$65 = 1^2 + 8^2 = 4^2 + 7^2$$

Weiters werden hier einige Primzahlen, die als Summe von zwei Quadraten darstellbar sind, aufgezeigt (notwendigerweise eindeutig bis auf die Ordnung laut Propostition 3.17):

$$2 = 1^2 + 1^2 \qquad 5 = 1^2 + 2^2 \qquad 13 = 2^2 + 3^2$$
$$17 = 1^2 + 4^2 \qquad 29 = 2^2 + 5^2$$

4 Schlussworte

Ich habe die Bearbeitung dieses zahlentheoretischen Themas sehr genossen. Außerdem empfand ich es als sehr interessant, da ich sehr gut an mein Vorwissen zu meiner Bachelorarbeit anknüpfen konnte. Das Entdecken von noch nicht gelernten Inhalten zu dem Thema, motivierte mich enorm. Ich konnte viele neue Sachen bezüglich Mathematik lernen, die nicht notwendigerweise in Vorlesungen im Studium vorkommen. Bei manchen Beweisen musste ich ziemlich knobeln, um sie wirklich bis auf den letzten Punkt zu verstehen. Schlussendlich gelang es mir jedoch immer hinter jeden Beweis zu kommen und die Gaußschen ganzen Zahlen zur Gänze zu verstehen.

Zu guter Letzt möchte ich mich noch bei den Personen bedanken, die mich zu diesem Punkt gebracht haben. Ich bedanke mich recht herzlich bei meinem Betreuer, Herrn Professor Dr. Christoph Baxa. Sie haben mir dieses außerordentlich interessante Thema vorgeschlagen und mich bei Verständnisschwierigkeiten immer tatkräftig unterstützt. Bei unseren Gesprächen waren Sie immer sehr verständnisvoll.
Weiters möchte ich mich mich bei meiner Familie und Freunden bedanken, die mich während meines gesamten Studiums unterstützt haben. Bei zwei Personen möchte ich mich ganz besonders bedanken. Beginnend bei meinem Bruder, der mir bei vielen technischen Schwierigkeiten am Computer und mit LaTeX unter die Arme gegriffen hat. Ebenso bedanke ich mich bei meiner Freundin, die mich des öfteren motivieren musste, mein Studium durchzuziehen.
$DANKE$

Literatur

[1] Aigner, Martin ; Ziegler, Günter M.: *Das BUCH der Beweise*. Springer, Berlin Heidelberg, 2014

[2] Bartholomé, Andreas ; Rung, Josef ; Kern, Hans: *Zahlentheorie für Einsteiger*. Vieweg+Teubner Verlag, Wiesbaden, 2010

[3] Baxa, Christoph: *Zahlentheorie*. Vorlesung der Universität Wien Sommersemester, 2017

[4] Conrad, Keith: *The Gaussian Integers, 2005*. `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf`. – abgerufen am: 01.07.2020

[5] Heath-Brown, David R.: Fermat's two squares theorem. In: *Invariant* (1984), S. 2–5

[6] Reiss, Kristina ; Schmieder, Gerald: *Basiswissen Zahlentheorie*. Springer, Berlin Heidelberg, 2014

[7] Schichl, Hermann ; Steinbauer, Roland: *Einführung in das mathematische Arbeiten*. Springer, Berlin Heidelberg, 2012

[8] Seiler, Wolfgang: *Zahlentheorie*. Vorlesung der Universität Mannheim Wintersemester, 2018

[9] Taschner, Rudolf: *Vom 1x1 zum Glück*. Brandstätter Verlag, Wien, 2017

[10] Ziegenbalg, Jochen: *Elementare Zahlentheorie*. Springer, Berlin Heidelberg, 2015