L.A. Kaloujnine

Primzahlzerlegung

Übersetzung von G. Pfister und L. Boll
1971 Deutscher Verlag der Wissenschaften
MSB: Nr. 59
Abschrift und LaTex-Satz: 2020 https://mathematikalpha.de

Inhaltsverzeichnis

Einführung

Schon in den ersten Schuljahren lernt man die ganzen Zahlen und ihre einfachsten Eigenschaften kennen; meiner Meinung nach wäre es sehr nützlich, wenn diejenigen Schüler der oberen Klassen, die sich für Mathematik interessieren, ihre in den unteren Klassen erworbenen Kenntnisse vertiefen würden.
Diese Vertiefung ist übrigens notwendig, wenn sie später Zugang zur Zahlentheorie, zur "höheren Arithmetik", gewinnen wollen. Die vorliegende Broschüre soll ihnen dabei helfen.

Als Ausgangspunkt betrachten wir den sogenannten Hauptsatz der elementaren Zahlentheorie. Der Leser möge sich durch diese ganz wissenschaftlich klingende Bezeichnung nicht abschrecken lassen.
Dieser Satz ist allgemein bekannt und wird bei arithmetischen Berechnungen häufig verwendet (beispielsweise beim Aufsuchen des Hauptnenners von Brüchen); man ist sich aber vielfach gar nicht bewusst, dass es sich um einen tiefliegenden Satz handelt, der eines sorgfältigen und ins Einzelne gehenden Beweises bedarf. Wir werden jetzt erläutern, worum es sich dabei handelt:

Jede ganze Zahl kann als Produkt von Primzahlen zerlegt werden.

$$420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \tag{1}$$

Ist die betreffende ganze Zahl hinreichend groß, so kann es unter Umständen recht lange dauern, bis man eine solche Zerlegung gefunden hat. Trotzdem hat man bisher in allen Fällen, in denen man eine solche Zerlegung suchte, sie auch gefunden. Ist das nun immer so oder hatten wir einfach Glück ?

Sind wir denn tatsächlich sicher, dass jede ganze Zahl als Produkt von Primzahlen dargestellt werden kann? Nun, das ist wirklich so, aber diese Tatsache erfordert einen Beweis. Den ersten Tel des Hauptsatzes bildet gerade die folgende Behauptung:
Jede ganze Zahl kann als Produkt von Primzahlen zerlegt werden.

Diese Behauptung werden wir in dieser Broschüre beweisen.
Der Beweis ist übrigens ziemlich einfach, und es wäre für den Leser sehr nützlich, wenn er ihn selbst zu finden versuchte.

Schwieriger ist es allerdings, die zweite Behauptung des Satzes zu beweisen; in der Schule tut man so, als ob sie selbstverständlich wäre. Bevor wir sie formulieren, gehen wir noch einmal auf das Beispiel der Zerlegung der Zahl 420 in Primfaktoren ein. Das Verfahren ist aus der Schule wohlbekannt und lässt sich schematisch folgendermaßen darstellen:

$$\begin{array}{r|l} 420 & 2 \\ 210 & 2 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

Es liefert tatsächlich die Zerlegung (1).
Könnte es nicht noch andere Methoden der Zerlegung geben ? Und woher weiß man, dass sie dasselbe Resultat liefern?

Natürlich kann man z.B. versuchen, eine gegebene Zahl in ein Produkt zweier kleinerer (nicht notwendig teilerfremder) Zahlen zu zerlegen, danach jede von diesen wieder in ein Produkt kleinerer Zahlen usw., bis man zu Zahlen gelangt, die nicht weiter zerlegbar sind (d.h. zu Primzahlen).

Schon beim ersten Schritt wird klar, dass dieses Verfahren nicht eindeutig ist. So gilt beispielsweise für die Zahl 420:

$$420 = 20 \cdot 21 \qquad ; \qquad 420 = 15 \cdot 48$$

Daher taucht ganz naturgemäß die Frage auf, ob es ganze Zahlen gibt, die auf verschiedene Weise in ein Produkt von Primzahlen zerlegbar sind.
Es zeigt sich, dass es keine solchen ganzen Zahlen gibt, und die entsprechende Aussage - nämlich die Behauptung, dass die Zerlegung einer ganzen Zahl in ein Produkt von Primfaktoren eindeutig ist - bildet gerade den zweiten Teil des Hauptsatzes:

Wenn eine ganze Zahl n n auf zwei verschiedene Arten in ein Produkt von Primfaktoren

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l$$

zerlegt ist, so stimmen diese Zerlegungen bis auf die Anordnungen der Faktoren überein: In beiden Zerlegungen treten gleich viele Faktoren auf, es ist also $k = l$, und jeder Faktor, der in der einen Zerlegung vorkommt, kommt ebenso oft in der anderen Zerlegung vor.[1]

Diese Aussage ist offenbar nur dann richtig, wenn keine Einsen als Faktoren auftreten, und eben deshalb sieht man die Zahl 1 nicht als Primzahl an.

Den Beweis dieser Behauptung führen wir ziemlich ausführlich. Er ist, wie schon erwähnt, wesentlich schwieriger als der Beweis der ersten Behauptung. Diese Schwierigkeit ist nicht zufällig, sondern hängt mit tiefliegenden Eigenschaften der Arithmetik der ganzen Zahlen zusammen.
Es zeigt sich nämlich, dass neben der gewöhnlichen Arithmetik zahlreiche andere "Arithmetiken" existieren und dabei sogar sehr nützlich sind. In einigen dieser Arithmetiken sind die Behauptungen des Hauptsatzes richtig, in anderen nicht; dabei ist es dann immer die Behauptung über die Eindeutigkeit der Zerlegung, die nicht erfüllt ist.

Wir werden Beispiele von Arithmetiken der ersten Art und solche der zweiten Art anführen.

Sehr viel ausführlicher betrachten wir eine Arithmetik der ersten Art, nämlich die Arithmetik der ganzen komplexen Zahlen, oder, wie man sie gewöhnlich nennt, die Arithmetik der ganzen Gaußschen Zahlen.
Wir bemerken nebenbei, dass wir die gewöhnlichen ganzen Zahlen (um sie nicht mit den ganzen Gaußschen Zahlen zu verwechseln) manchmal als ganze rationale Zahlen bezeichnen. Wo jedoch kein Missverständnis auftreten kann, werden wir einfach von ganzen Zahlen sprechen, wenn wir die ganzen rationalen Zahlen meinen.

In der Arithmetik der ganzen Gaußschen Zahlen ist der Hauptsatz ebenfalls erfüllt, und diese Tatsache zieht eine ganze Reihe interessanter und bei weitem nicht offensichtlicher Eigenschaften der ganzen rationalen Zahlen nach sich.

[1] Wenn man beliebige ganze Zahlen betrachtet (die also positiv oder auch negativ sein können), dann ist die Eindeutigkeit der Zerlegung in Primfaktoren so zu verstehen, dass zwei Zerlegungen $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ und $n = q_1 \cdot q_2 \cdot ... \cdot q_l$ sich nicht nur durch die Anordnung, sondern auch durch die Vorzeichen der entsprechenden Primfaktoren unterscheiden dürfen; vgl. § 1, Formulierung des Hauptsatzes.

Am Schluss dieser Broschüre geben wir ein Beispiel für eine Arithmetik, in welcher der Hauptsatz nicht gilt. Zwar lassen sich die dort betrachteten Zahlen in ein Produkt von Primfaktoren zerlegen; es zeigt sich aber, dass die Primzahlen, die in zwei Zerlegungen vorkommen, verschieden sein können.
Wir werden jedoch diese Arithmetik nicht eingehender untersuchen; das würde es erforderlich machen, eine Reihe neuer Begriffe einzuführen und ihre Eigenschaften zu untersuchen, und das ist nur im Rahmen einer Universitätsvorlesung möglich.

Zum Verständnis unserer Ausführungen werden vom Leser keine Kenntnisse verlangt, die er nicht schon im Schulunterricht erworben hat.
Allerdings werden wir vielfach beim Beweis von Sätzen die Methode der vollständigen Induktion benutzen. Wer diese für die Mathematik äußerst wichtige Methode noch nicht auf der Schule gelernt hat, sei auf das in dieser Reihe erschienene Bändchen von I.S. Sominski, "Die Methode der vollständigen Induktion", verwiesen. Dort findet er sie an vielen Beispielen erläutert, so dass er sich mit ihr vertraut machen kann.

Schließlich möge der Leser das Literaturverzeichnis beachten, in dem er Werke ähnlicher Thematik und ähnlichen Niveaus sowie einige weiterführende Werke aufgeführt findet.

1 Der Hauptsatz der elementaren Zahlentheorie. Beweis des ersten Teils

Wir wollen jetzt die in der Einführung ausgesprochenen Behauptungen zu einem einzigen Satz, dem sogenannten Hauptsatz der elementaren Zahlentheorie, zusammenfassen.

Jede von Null verschiedene ganze Zahl kann als Produkt von Primzahlen dargestellt werden, wobei die Darstellung bis auf die Reihenfolge und die Vorzeichen der Faktoren eindeutig ist.

Wie schon gesagt, enthält dieser Satz zwei Behauptungen:
Als erstes die Behauptung, dass eine Darstellung jeder ganzen Zahl als Produkt von Primzahlen existiert, und als zweites die Behauptung, dass diese Darstellung eindeutig ist. Diese beiden Behauptungen werden wir beweisen; in diesem Paragraphen allerdings nur die erste.

Zwei einfache Bemerkungen seien vorausgeschickt.

1. Die Zahl 1 wird aus verschiedenen Gründen nicht zu den Primzahlen gerechnet, obwohl sie nicht in ein Produkt kleinerer Zahlen zerlegbar ist. Dann entsteht die Frage:
In welchem Sinne ist der oben genannte Satz für die Zahl 1 richtig oder anders ausgedrückt, in welchem Sinne lässt sich 1 als Produkt von Primzahlen darstellen? Im Gegensatz etwa zu den Philologen haben die Mathematiker nämlich nicht gern Ausnahmen. Nun, wir wollen

$$1 = 1$$

als eine Zerlegung der Zahl 1 in ein Produkt von Primzahlen ansehen, wobei die Anzahl der Primfaktoren auf der rechten Seite gleich Null ist.
Diese Vereinbarung erinnert an die Definition der nullten Potenz $a^0 = 1$ (die Anzahl der Faktoren a ist gleich 0) und erweist sich in vieler Hinsicht als zweckmäßig. Eine analoge Übereinkunft treffen wir auch für die Zahl -1.

2. Als zweite Bemerkung führen wir einfach ein Beispiel an, das den Begriff der Eindeutigkeit der Zerlegung einer ganzen Zahl in Primfaktoren erläutert. Die beiden Zerlegungen der Zahl 18

$$18 = 2 \cdot 3 - 3 \qquad \text{und} \qquad 18 = (-3) \cdot (-2) - 3$$

werden wir nicht als verschieden ansehen.

Beweis der Existenz einer Zerlegung einer ganzen rationalen Zahl in ein Produkt von Primzahlen.

Wir beschränken uns zunächst auf den Fall der positiven ganzen Zahlen. Dass man sie in Primfaktoren zerlegen kann, lässt sich mit Hilfe vollständiger Induktion beweisen:

a) Für $n = 1$ ist $1 = 1$ die gesucht Darstellung: 1 ist Produkt einer leeren Menge von Primzahlen.

b) Wir nehmen an, für alle positiven ganzen Zahlen m, die kleiner als n sind, sei die Zerlegbarkeit in ein Produkt von Primzahlen schon bewiesen. Dann beweisen wir, dass auch für die Zahl n eine solche Zerlegung existiert. Ist n Primzahl, so ist

$$n = n$$

eine gesuchte Zerlegung (ein einziger Primfaktor).

Nun sei n eine zusammengesetzte Zahl. Dann ist sie Produkt $n = n_1 \cdot n_2$ zweier ganzer Zahlen n_1 und n_2, von denen jede von n und 1 verschieden ist; folglich gilt $n_1 < n$ und $n_2 < n$. Dann gibt es aber nach der Induktionsannahme Zerlegungen der Zahlen n_1 und n_2 in ein Produkt von Primzahlen:

$$n_1 = p_1 \cdot p_2 \cdot ... \cdot p_r \qquad , \quad n_2 = q_1 \cdot q_2 \cdot ... \cdot q_s$$

wobei p_j und q_i Primzahlen sind. Es ist also

$$n = p_1 \cdot p_2 \cdot ... \cdot p_r \cdot q_1 \cdot q_2 \cdot ... \cdot q_s$$

d.h., wir haben eine Zerlegung der Zahl n erhalten.

Ist n eine negative ganze Zahl, so ist $-n$ eine positive Zahl. Wie wir schon bewiesen haben, ist $-n$ in ein Produkt von Primzahlen zerlegbar. Es sei also

$$-n = p_1 \cdot p_2 \cdot ... \cdot p_k \qquad \text{dann ist} n = (-1)p_1 \cdot p_2 \cdot ... \cdot p_k$$

oder beispielsweise

$$n = (-p_1) \cdot p_2 \cdot ... \cdot p_k$$

eine gesuchte Zerlegung der Zahl n. Damit ist der erste Teil des Satzes bewiesen.

Es existieren ziemlich viele Beweise für die Eindeutigkeit der Zerlegung. Derjenige, den wir hier führen, ist nicht der kürzeste und nicht der einfachste.
Unser Beweis hat aber den Vorteil, dass er sich unmittelbar auf eine Reihe anderer Bereiche verallgemeinern lässt, z.B. auf den Bereich der Polynome in einer Veränderlichen und auf den Bereich der ganzen komplexen Zahlen. Außerdem ergeben sich im Laufe des Beweises, sozusagen als Nebenprodukt, zahlreiche andere wichtige Sätze der Arithmetik.

2 Teilung mit Rest und größter gemeinsamer Teiler (ggT) zweier Zahlen. Beweis des zweiten Teils des Hauptsatzes

Ausgangspunkt für unsere Betrachtungen ist die Behauptung, dass im Bereich der ganzen Zahlen eine "Teilung mit Rest" möglich ist. Exakt lässt sich diese Behauptung wie folgt formulieren:

Satz 1. Es seien a und b ganze Zahlen und $b \neq 0$. Dann existieren ganze Zahlen q und r, wobei $0 \leq |r| < b$ ist[2]), derart, dass

$$a = qb + r \tag{1}$$

ist.

Die Gleichung $r = 0$ in der Darstellung (1) ist gleichbedeutend damit, dass die Zahl a durch b teilbar ist:[3] Diesen Sachverhalt wollen wir im folgenden durch das Symbol $b \mid a$ zum Ausdruck bringen - diese Bezeichnungsweise ist der Zahlentheorie entnommen.

Zunächst beweisen wir die Möglichkeit einer solchen Darstellung. Dazu bemerken wir, dass für jede rationale Zahl τ eine ganze Zahl t gefunden werden kann, für welche $|\tau - t| < 1$ gilt.[4] Es sei $\tau = \frac{a}{b}$ mit ganzen Zahlen a und b. Wir wählen eine ganze Zahl q für welche $\left|\frac{a}{b} - q\right| < 1$ ist, und setzen

$$r = b\left(\frac{a}{b} - q\right) = a - bq$$

Also ist r eine ganze Zahl, ferner

$$|r| = |b|\left|\frac{a}{b} - q\right| < |b| \cdot 1 = |b| \qquad \text{und} \qquad a = q - b + r$$

was zu beweisen war.[5]

Satz 1 erlaubt, den Begriff des größten gemeinsamen Teilers zweier Zahlen einzuführen und eine Reihe seiner Eigenschaften zu beweisen.

Definition 1. Sind a und b zwei von Null verschiedene ganze Zahlen und ist die Zahl c so beschaffen, dass $c \mid a$ und $c \mid b$ gilt, so nennt man c einen gemeinsamen Teiler der Zahlen a und b.
Wir bemerken, dass je zwei ganze Zahlen stets gemeinsame Teiler besitzen, nämlich die Zahlen 1 und -1. Wenn es keine anderen gemeinsamen Teiler gibt, dann nennt man die Zahlen a und

[2]Der Rest r kann eine beliebige ganze Zahl sein, also positiv, negativ oder Null.

[3]Für zwei ganze Zahlen a und b sind die Redeweisen "die Zahl a ist durch die Zahl b teilbar", "die Zahl b ist Teiler der Zahl a" oder schließlich "die Zahl b teilt die Zahl a" gleichbedeutend; man sagt auch "die Zahl b geht in der Zahl a auf"; wir werden sie sämtlich benutzen.

[4]In Wirklichkeit unterscheidet sich die der Zahl τ nächstliegende ganze Zahl von 1 nicht mehr als um $1/2$, aber diese schärfere Aussage wird von uns nicht benötigt.

[5]Zu bemerken ist noch, dass in der Darstellung (1) die ganzen Zahlen q und r nicht eindeutig bestimmt sind. Beispielsweise gilt für $a = 13$ und $b = 3$ die Beziehung $13 = 4 \cdot 3 + 1$ ($q = 4$, $r = 1$) oder $13 = 5 \cdot 3 + (-2)$ ($q = 5$, $r = -2$). Das ist sogar aus unserem Beweis zu ersehen. Ist nämlich a nicht durch b teilbar, so ist $\frac{a}{b}$ eine gebrochene Zahl, und dann ist $n < \frac{a}{b} < n + 1$, wobei n eine ganze Zahl ist. Als q kann $q = n$ oder $q = n + 1$ gewählt werden, was zwei Darstellungen der Form (1) ergibt. Nur im Fall $b \mid a$ ist die Zahl q eindeutig bestimmt: $a = q \cdot b$, und dann ist $r = 0$.

b zueinander teilerfremd.[6] Auf teilerfremde Zahlen werden wir später noch zurückkommen.

Definition 2. Eine Zahl d heißt größter gemeinsamer Teiler (ggT) der Zahlen a und b, wenn folgendes gilt:
1. d ist gemeinsamer Teiler von a und b,
2. d ist durch jeden beliebigen anderen gemeinsamen Teiler der Zahlen a und b teilbar.

So ist beispielsweise 6 ggt der Zahlen 18 und 30, da 6 | 18 und 6 | 30 gilt und 6 durch alle gemeinsamen Teiler dieser Zahlen, nämlich durch 1, -1, 2, -2, 3, -3, 6, -6, teilbar ist.

Dem Leser ist sicher noch aus der Schule bekannt, dass zu jedem Paar ganzer Zahlen ein ggT existiert; auch die Methode, wie man ihn findet, dürfte bekannt sein. Wenn wir uns aber dieser Methode erinnern und sie aufmerksam analysieren, können wir ohne Schwierigkeit erkennen, dass sie die Zerlegung der Zahlen a und b in Primfaktoren und die Eindeutigkeit dieser Zerlegung benutzt.
Dieser Weg ist aber für uns nicht gangbar, da wir bisher nur den Existenzsatz bewiesen haben.

Aus unserer Definition (Definition 2) ergibt sich nicht ohne weiteres, dass für je zwei ganze Zahlen a und b ein ggT existiert. Wir werden jetzt beweisen, dass das der Fall ist, und zwar ohne die Zerlegung der Zahlen a und b in Primfaktoren zu benutzen.

Satz 2. Zu jedem Paar ganzer Zahlen $a \neq 0$ und $b \neq 0$ existiert ein ggT.

Beweis. Neben den Zahlen a und b betrachten wir alle Zahlen der Form $xa + yb$, wobei x und y irgendwelche ganze Zahlen sind. Zahlen dieser Form,

$$v = xa + yb \tag{2}$$

wollen wir als Linearkombinationen der Zahlen a und b bezeichnen.
Beispielsweise sind für $a = 6$ und $b = 22$ die Zahlen

$$28(28 = 1 \cdot 6 + 1 \cdot 22), \qquad 10(10 = (-2) \cdot 6 + 1 \cdot 22), \qquad -92(-92 = 3 \cdot 6 + (-5) \cdot 22)$$

usw. Linearkombinationen.
Im allgemeinen existieren zu beliebig gegebenen Zahlen a und b unendlich viele Zahlen, welche Linearkombinationen von a und b sind.

Die Menge dieser Zahlen bezeichnen wir mit M. Wir bemerken, dass die Menge M insbesondere die Zahlen a (für $y = 0, x = 1$) und b (für $x = 0, y = 1$) sowie auch die Zahl 0 (für $y = 0, x = 0$) enthält.
Alle Zahlen v aus der Menge M sind offenbar ganze Zahlen. Wenn v zu M gehört, dann gehört auch $-v$ zu M (ist $v = xa + yb$, so ist $-v = (-x)a + (-y)b$).
Wir erwähnen noch eine Eigenschaft der Zahlen v aus M, die wir sofort benötigen: Alle diese Zahlen sind durch alle gemeinsamen Teiler der Zahlen a und b teilbar. Gilt nämlich $c \mid a$ und $c \mid b$, also etwa $a = a'c$ und $b = b'c$, dann ist

$$v = xa + yb = xa'c + yb'c = (xa' + yb')c$$

und somit $c \mid v$.

[6] Man sagt auch, a und b seien relativ prim.

Nun sei $d \neq 0$ die Zahl mit dem kleinsten absoluten Betrag [7] unter allen von Null verschiedenen Zahlen aus M.

Wir zeigen nun, dass d ein ggT der Zahlen a und b ist. Die Zahl d besitzt die Eigenschaft 2 der Definition des ggT, da diese Eigenschaft allen Zahlen aus M zukommt. Man muss nur noch nachprüfen, dass sie die Eigenschaft 1 hat, d.h., dass d gemeinsamer Teiler der Zahlen a und b ist.

Wir zeigen dazu, dass $d \mid a$ gilt.
Da d zu M gehört, lässt es sich in der Form $d = sa + tb$ darstellen, wobei s und t geeignete ganze Zahlen sind. Wenn wir jetzt a durch d mit Rest teilen, d.h. solche Zahlen q und r, $|r| < |d|$, bestimmen, für welche

$$a = qd + r$$

ist, so muss auch der Rest r zur Menge M gehören. Es ist nämlich

$$r = a - qd = a - q(as + tb) = (1 - qs)a + tb$$

Nun erinnern wir uns, dass d die Zahl mit dem kleinsten absoluten Betrag unter den von Null verschiedenen Zahlen aus M ist; die Zahl r ist aber kleiner als d. Folglich ist $r = 0$, und d geht in a auf.
Analog beweist man auch, dass $d \mid b$ gilt. Der Satz ist somit bewiesen.

Wir stellten fest, dass ein ggT zweier von Null verschiedener ganzer Zahlen existiert. Darüber hinaus haben wir aus dem Beweis die folgende wichtige Tatsache ersehen, die wir bald benötigen werden:

Satz 3. Ein ggT der Zahlen a und b lässt sich als Linearkombination dieser Zahlen darstellen.

Es entsteht die Frage: Ist der ggT der Zahlen a und b eindeutig bestimmt ?
Die Antwort lautet natürlich nein: Wenn die Zahl d die Eigenschaften 1 und 2 der Definition des ggT besitzt, dann hat auch $-d$ diese Eigenschaften. Bis auf das Vorzeichen jedoch ist der ggT eindeutig bestimmt. Es seien nämlich d und d' zwei ggT der Zahlen a und b. Da d die Eigenschaft 2 hat und d' die Eigenschaft 1 besitzt, gilt $d' \mid d$. Analog gilt auch $d \mid d'$. Also sind

$$\alpha = \frac{d}{d'} \qquad \text{und} \qquad \frac{d'}{d} = \frac{1}{d/d'} = \frac{1}{\alpha}$$

ganze Zahlen. Die einzigen ganzen Zahlen, deren Kehrwert ebenfalls eine ganze Zahl ist, sind aber die Zahlen 1 und -1. Folglich ist $\alpha = 1$ oder $\alpha = -1$, woraus $d' = d$ oder $d' = -d$ folgt. Hätten wir in der Definition des ggT gefordert, dass diese Zahl positiv ist - manchmal (aber bei weitem nicht immer) ist das zweckmäßig - dann könnten wir sagen, dass der ggT zweier von Null verschiedener ganzer Zahlen existiert und eindeutig bestimmt ist.

Im folgenden werden wir den ggT der Zahlen a und b mit (a, b) bezeichnen, wie das in der zahlentheoretischen Literatur üblich ist.

Wir wollen jetzt Paare teilerfremder Zahlen betrachten. Wir sind diesem Begriff schon begegnet

[7] Eine solche Zahl existiert tatsächlich in der Menge M. In M sind von Null verschiedene Zahlen enthalten (beispielsweise a und b), deren absolute Beträge positive ganze, also natürliche Zahlen sind. Eine der grundlegenden Eigenschaften der natürlichen Zahlen, die man gewöhnlich als Axiom annimmt (vgl. Sominski, Die Methode der vollständigen Induktion, S. 13, Bemerkung) besteht aber darin, dass jede nicht leere Menge natürlicher Zahlen eine kleinste Zahl enthält.

und wollen jetzt seine Definition noch einmal wiederholen.

Definition 3. Ganze Zahlen $a \neq 0$ und $b \neq 0$ heißen teilerfremd, wenn ihr ggT gleich 1 ist.
Mit anderen Worten, man kann sagen, dass teilerfremde Zahlen solche Zahlen sind, deren einzige gemeinsamen Teiler die Zahlen 1 und -1 sind.

Wenn $(a, b) = 1$ ist, folgt aus Satz 3, dass 1 in der Form

$$1 = sa + tb \tag{3}$$

mit geeigneten ganzen Zahlen s und t dargestellt werden kann.
Umgekehrt, wenn die Gleichung (3) für geeignete Zahlen s und t erfüllt ist, dann sind a und b teilerfremd. Denn $d = (a, b)$ ist die von Null verschiedene Zahl der Gestalt $xa + yb$ mit dem kleinsten absoluten Betrag (siehe Beweis von Satz 1). Wenn (3) erfüllt ist, ist somit $|d| \leq 1$ und $d \neq 0$, also $d = \pm 1$.
Hieraus folgt sofort die wichtigste Eigenschaft teilerfremder Zahlen.

Satz 4. Wenn $a \mid bc$ und $(a, b) = 1$ gilt, dann gilt $a \mid c$.
(In Worten: Wenn die Zahl a in dem Produkt zweier Zahlen aufgeht und zu einem der Faktoren teilerfremd ist, dann geht sie in dem anderen Faktor auf.)

Beweis. Da $(a, b) = 1$ ist, können wir solche ganze Zahlen s und t finden, dass

$$1 = sa + tb \tag{4}$$

ist. Multiplizieren wir diese Gleichung mit c, so erhalten wir

$$c = (sc)a + t(bc)$$

Beide Summanden der rechten Seite sind durch a teilbar, also auch c. Nützlich ist auch die folgende Aussage:

Satz 5. Wenn eine Zahl a zu den Zahlen b und c teilerfremd ist, dann ist sie auch zum Produkt bc teilerfremd.

Beweis. Da $(a, b) = 1$ ist, können wir ganze Zahlen s und t finden, welche die Gleichung

$$1 = sa + tb$$

erfüllen. Wegen $(a, c) = 1$ gilt auch

$$1 = ua + vc$$

für geeignete u und v. Wenn wir diese Gleichungen miteinander multiplizieren, erhalten wir

$$1 = (sa + tb)(ua + vc) = sua^2 + savc + tbua + tbvc = (sua + svc + tbu)a + (tv) \cdot (bc)$$

Wir setzen nun $m = sua + svc + tbu$ und $n = tv$; dann sind m und n ganze Zahlen, und es ist

$$1 = ma + n(bc)$$

Daraus folgt, dass a und bc teilerfremd sind.
Die Behauptung des letzten Satzes lässt sich leicht auf beliebig viele Faktoren verallgemeinern.

Satz 6. Wenn a zu den Zahlen $b_1, b_2, ..., b_k$ teilerfremd ist, dann ist a zu $b_1 \cdot b_2 \cdot ... \cdot b_k$ teilerfremd.

Diesen Satz beweist man mit Hilfe vollständiger Induktion über die Anzahl k der Faktoren.

Beweis der Eindeutigkeit der Zerlegung ganzer Zahlen in das Produkt von Primfaktoren.

Jetzt können wir den zweiten Teil des Hauptsatzes der elementaren Zahlentheorie beweisen. Dazu bemerken wir, dass schon aus der Definition des Primzahlbegriffs folgt, dass verschiedene Primzahlen zueinander teilerfremd sind.
Den Beweis der Eindeutigkeit der Zerlegung werden wir induktiv über den absoluten Betrag der Zahl n führen.

a) Wenn $|n| = 1$ ist, dann ist $n = \pm 1$ und $1 = 1$, $-1 = -1$, d.h., es gibt eine einzige Zerlegung für die Zahlen 1 und -1.

b) Wir nehmen an, die zu beweisende Eigenschaft sei schon für alle Zahlen m, für die $|m| < |n|$ ist, bewiesen. Es seien

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l$$

zwei Zerlegungen der Zahl n in das Produkt der Primzahlen $p_1, p_2, ..., p_k$ bzw. $q_1, q_2, ..., q_l$. Wir behaupten, dass die Primzahl p_k, oder $-p_k$ unter den Primzahlen $q_1, ..., q_l$ vorkommt.
Anderenfalls wäre ja $p_k \neq q_i$, $i = 1, 2, ..., l$, und p_k wäre zu allen Zahlen q_i teilerfremd, nach Satz 6 also auch zu ihrem Produkt, d. h. zur Zahl n.
Das ist aber unmöglich, da $p_k \mid n$, also $(p_k, n) = p - k$ gilt.
Demnach ist p_k gleich irgendeiner Primzahl aus der Menge der Primzahlen $\pm q_i$.

Man kann annehmen, dass $p_k = q_l$ ist, da man sonst durch Vertauschen der Faktoren q_i erreichen könnte, dass $p_k = \pm q_l$ ist; im Fall $p_k = -q_l$ ändern wir noch das Vorzeichen bei q_l und einem beliebigen anderen q_i.
Also erhalten wir

$$n = p_1 \cdot p_2 \cdot ... \cdot p_{k-1} \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_{l-1} \cdot p_k$$

daher ist

$$m = \frac{n}{p_k} = p_1 \cdot p_2 \cdot ... \cdot p_{k-1} = q_1 \cdot q_2 \cdot ... \cdot q_{l-1}$$

Jetzt ist aber $|m| < |n|$, und nach Induktionsvoraussetzung ist für m die Behauptung des Satzes schon bewiesen; also ist $k - 1 = l - 1$, die Folgen $p_1, p_2, ..., p_{k-1}$ und $q_1, q_2, ..., q_{l-1}$ enthalten bis auf das Vorzeichen ein und dieselben Primzahlen, und entsprechende Primzahlen kommen in beiden Darstellungen gleich oft vor.
Da aber $p_k = q_l$ ist, gilt das auch für die Folgen $p_1, p_2, ..., p_{k-1}, p_k$ und $q_1, q_2, ..., q_{l-1}, q_l$.

Damit ist aber der Satz bewiesen.

3 Der Euklidische Algorithmus und die Lösung linearer diophantischer Gleichungen mit zwei Unbekannten

In Satz 2 haben wir gezeigt, dass zwei ganze Zahlen a und b einen ggT haben. Wir werden jetzt ein Verfahren angeben, wie man den ggT findet; es kommt schon in den "Elementen" Euklids vor.
Deshalb wird es als Euklidischer Algorithmus bezeichnet.

Im folgenden wollen wir annehmen, es sei $|a| \geq |b|$.

Erster Schritt. Wir teilen a durch b mit Rest:

$$a = q_1 \cdot b + r_1, \qquad |r_1| < |b| \tag{1}$$

Ist $r_1 = 0$, so gilt $b \mid a$ und $(a, b) = b$. Ist $r_1 \neq 0$, so setzen wir das Verfahren fort:

Zweiter Schritt. Wir teilen b durch r_1:

$$b = q_2 \cdot r_1 + r_2, \qquad |r_2| < |r_1| \tag{2}$$

Ist $r_2 \neq 0$, so folgt

Dritter Schritt.

$$r_1 = q_3 \cdot r_2 + r_3, \qquad |r_3| < |r_2| \tag{3}$$

usw. Nach jedem Schritt ist der neue Rest kleiner als der Rest beim vorhergehenden Schritt,

$$|b| > |r_1| > |r_2| > ...$$

und nach einem gewissen k-ten Schritt ($k < |b|$) ergibt sich der Rest Null.

k-ter Schritt.

$$r_{k-2} = q_k \cdot r_{k-1} \tag{k}$$

Wir werden zeigen, dass der letzte von Null verschiedene Rest r_{k-1} die gesuchte Zahl (a, b) ist. Wir haben nämlich eine Kette von Gleichungen:

$$\begin{aligned} a &= q_1 \cdot b + r_1 && (1)\\ b &= q_2 \cdot r_1 + r_2 && (2)\\ r_1 &= q_3 \cdot r_2 + r_3 && (3)\\ &... \\ r_{k-3} &= q_{k-1} \cdot r_{k-2} + r_{k-1} && (k\text{-}1)\\ r_{k-2} &= q_k \cdot r_{k-1} && (k) \end{aligned}$$

Wir ersehen aus der letzten Gleichung die Beziehung $r_{k-1} \mid r_{k-2}$, aus der vorletzten $r_{k-1} \mid r_{k-3}$, da ja $r_{k-1} \mid r_{k-1}$ und $r_{k-1} \mid r_{k-2}$ gilt.
Demnach können wir in analoger Weise schließen, dass $r_{k-1} \mid r_{k-4}$ gilt. Geht man entsprechend von Gleichung zu Gleichung zurück, so erhält man nacheinander

$$... \quad r_{k-1} \mid r_2, \quad r_{k-1} \mid r_1, \quad r_{k-1} \mid b, \quad r_{k-1} \mid a$$

Wir sehen also, dass r_{k-1} gemeinsamer Teiler der Zahlen a und b ist.

Jetzt sei c eine ganze Zahl mit $c \mid a$ und $c \mid b$. Dann erhalten wir aus (1), (2), ..., (k-1) nacheinander, dass $c \mid r_1, c \mid r_2, ..., c \mid r_{k-1}$ gilt.
Somit ist r_{k-1} wirklich der ggT der Zahlen a und b.

Wir sehen uns ein Zahlenbeispiel an: $a = 858$, $b = 253$. Offenbar ist

$$858 = 3 \cdot 253 + 99, \tag{1}$$
$$253 = 2 \cdot 99 + 55, \tag{2}$$
$$99 = 1 \cdot 55 + 44, \tag{3}$$
$$55 = 1 \cdot 44 + 11, \tag{4}$$
$$44 = 4 \cdot 11; \tag{5}$$

daher ist $(858, 253) = 11$.

Mit Hilfe des Euklidischen Algorithmus findet man also den ggT zweier Zahlen, ohne die Zerlegung dieser Zahlen in Primfaktoren zu benutzen.
In Satz 3 stellten wir fest, dass $(a, b) = d$ in der Form

$$d = s \cdot a + t \cdot b$$

dargestellt werden kann; der Beweis gab jedoch keinen Hinweis, wie man die entsprechenden Zahlen s und t finden kann.

Mit Hilfe des Euklidischen Algorithmus lässt sich diese Aufgabe sehr leicht lösen. Wir werden dieses Verfahren jedoch nicht für den allgemeinen Fall angeben, sondern es an dem soeben untersuchten Zahlenbeispiel erklären.
Wir sollen also solche ganze Zahlen s und t finden, für welche

$$11 = s \cdot 858 + t \cdot 253$$

ist. Aus (4), (3), (2), (1) erhalten wir nacheinander

$$11 = 55 + (-1) \cdot 44,$$
$$44 = 99 + (-1) \cdot 55,$$
$$55 = 253 + (-2) \cdot 99,$$
$$99 = 858 + (-3) \cdot 253.$$

Wenn wir jetzt für 44 in der ersten Gleichung den entsprechenden Ausdruck der zweiten Gleichung einsetzen, dann für 55 den entsprechenden Ausdruck aus der dritten Gleichung usw., erhalten wir:

$$\begin{aligned} 11 &= 55 + (-1) \cdot (99 + (-1) \cdot 55) \\ &= 2 \cdot 55 + (-1) \cdot 99 = 2 \cdot (253 + (-2) \cdot 99) + (-1) \cdot 99 = 2 \cdot 253 + (-5) \cdot 99 \\ &= 2 \cdot 253 + (-5) \cdot (858 + (-3) \cdot 253) = (-5) \cdot 858 + 17 \cdot 253 \end{aligned}$$

Somit ist $s = -5$, $t = 17$.

Der Leser kann sich leicht selbst überlegen, wie das Verfahren im allgemeinen Fall verläuft. Die Gleichungen, die bei der Anwendung des Euklidischen Algorithmus zur Berechnung des ggT der Zahlen a und b entstehen, ermöglichen es, Gleichungen der Form $d = xa + yb$ (wobei

$d = (a, b)$ ist) in ganzen Zahlen zu lösen.

Eine Gleichung der Gestalt

$$xa + yb = c$$

wobei a, b, c gegebene ganze Zahlen sind, für welche ganzzahlige Lösungen x, y gesucht werden, wird üblicherweise als lineare diophantische Gleichung mit zwei Unbekannten bezeichnet. Linear heißt sie deshalb, weil die Unbekannten x und y nur in der ersten Potenz vorkommen. Das Wort "diophantisch[8]" weist darauf hin, dass die Koeffizienten der Gleichung ganze Zahlen und die gesuchten Lösungen ganzzahlig sind.

An dieser Stelle sei bemerkt, dass wir im Grunde schon lineare diophantische Gleichungen der Gestalt

$$xa + yb = c \tag{I}$$

zu lösen gelernt haben. Wir müssen aber die Frage nach allen Lösungen der Gleichung (I) etwas eingehender behandeln.

Zunächst mal sei jedoch bemerkt, dass nicht alle Gleichungen dieser Gestalt eine Lösung haben. Hat nämlich die Gleichung (I) eine Lösung in ganzen Zahlen, etwa $x = x_0$, $y = y_0$, $c = x_0a + y_0b$ und ist $d = (a, b)$, dann ist d Teiler beider Summanden auf der rechten Seite (denn es gilt $d \mid a$ und $d \mid b$), folglich auch von c. Daraus ersieht man:

Für die Existenz einer ganzzahligen Lösung der Gleichung (I) ist notwendig, dass der ggT der Zahlen a und b in der rechten Seite der Gleichung aufgeht.

So hat z.B. die Gleichung

$$9x + 15y = 7$$

keine Lösung, da 7 nicht durch 3 = (9, 15) teilbar ist. Gilt aber $d \mid c$, so hat die Gleichung (I) eine ganzzahlige Lösung, und wir wissen schon, wie man eine solche Lösung findet.

Es sei etwa $c = c'd$; ferner seien s und t solche ganzen Zahlen (man kann sie mit Hilfe des Euklidischen Algorithmus ermitteln), für welche

$$d = as + bt$$

ist. Dann ist

$$c = c'd = a(sc') + b(tc')$$

also ist $x_0 = sc'$, $y_0 = tc'$ eine Lösung der Gleichung (I).

Wir wollen einmal als Beispiel die Gleichung

$$33 = 858x + 253y \tag{II}$$

lösen. Wir haben schon gezeigt, dass

$$11 = 858 \cdot (-5) + 253 \cdot 17$$

ist. Wenn wir beide Seiten der Gleichung mit 3 multiplizieren, erhalten wir

$$33 = 858 \cdot (-15) + 253 \cdot 51$$

[8] Nach dem Mathematiker Diophant von Alexandria (ungefähr 250 u.Z.), der in seinem Buch "Arithmetik" ganzzahlige Gleichungen untersuchte. Am Schluss unserer Darlegung werden wir auch auf quadratische diophantische Gleichungen eingehen.

Also ist $x = -15$, $y = 51$ eine Lösung der Gleichung (II). Man darf aber nicht denken, die gefundene Lösung sei die einzige.
Es zeigt sich nämlich:

Hat eine diophantische Gleichung der Gestalt (I) überhaupt eine Lösung, so hat sie unendlich viele Lösungen.

Wir wollen diese Frage gleich ausführlicher untersuchen, und zwar wollen wir diese Behauptung beweisen und die allgemeine Form aller möglichen Lösungen der Gleichung (I) finden.
Wir werden mit letzterem beginnen.

Dabei nehmen wir an, neben der ganzzahligen Lösung x_0, y_0 sei uns eine weitere Lösung x_1, y_1 der Gleichung (I) bekannt. Dann ist also

$$c = ax_0 + by_0 \qquad , \qquad c = ax_1 + by_1$$

Wenn wir die zweite Gleichung von der ersten subtrahieren, erhalten wir

$$a(x_0 - x_1) + b(y_0 - y_1) = 0 \qquad \text{oder} \qquad a(x_0 - x_1) = b(y_1 - x_0) \tag{III}$$

Ist $d = (a, b)$, so setzen wir $a' = a/d$, $b' = b/d$, also

$$a = a'd \qquad , \qquad b = b'd$$

wobei a' und b' teilerfremde Zahlen sind. Wenn wir nun in der Gleichung (III) durch d kürzen, geht sie in die Gleichung

$$a'(x_0 - x_1) = b'(y_1 - x_0)$$

über. Da jetzt a' und b' teilerfremd sind, folgt $a' \mid (y_1 - y_0)$ und analog $b' \mid (x_0 - x_1)$. Setzen wir nun

$$y_1 - y_0 = a'k_1 \qquad , \qquad x_0 - x_1 = b'k_2$$

so ist $a'b'k_1 = a'b'k_2$, woraus $k_1 = k_2 = k$ folgt. Somit ergibt sich schließlich

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k \tag{IV}$$

$$x_1 = x_0 - b'k = x_0 - \frac{b}{d}k \tag{V}$$

wobei k eine beliebige ganze Zahl ist.

Umgekehrt sieht man leicht ein:
Ist x_0, y_0 eine Lösung der Gleichung (I), so sind alle Paare von Zahlen (IV), (V) bei beliebigem k Lösungen der Gleichung (I). Es ist nämlich

$$ax_1 + by_1 = a\left(x_0 - \frac{b}{d}k\right) + b\left(y_0 + \frac{a}{d}k\right) = ax_0 + by_0 + \left(-\frac{ab}{d}k + \frac{ab}{d}k\right) = c + 0 = c$$

Ist also x_0, y_0 eine Lösung der Gleichung (I), so sind auch alle Zahlen der Gestalt $x_0 - \frac{b}{d}k$, $y_0 = \frac{a}{d}k$ solche Lösungen (da k beliebig ist, ergeben sich also aus einer Lösung unendlich viele Lösungen), und andere Lösungen gibt es nicht.

4 Gaußsche Zahlen und ganze Gaußsche Zahlen

Eine natürliche Verallgemeinerung der ganzen rationalen Zahlen sind die ganzen komplexen Zahlen; gewöhnlich werden sie auch nach dem großen deutschen Mathematiker C.F. Gauß, der sie erstmalig eingehender untersuchte, als "ganze Gaußsche Zahlen" bezeichnet.

Definition 4. Eine komplexe Zahl, deren Real- und Imaginärteil ganze rationale Zahlen sind, bezeichnet man als ganze Gaußsche Zahl. Mit anderen Worten, das ist eine komplexe Zahl α der Gestalt

$$\alpha = a + bi \tag{1}$$

wobei a und b ganze (rationale) Zahlen sind.

Neben den ganzen Gaußschen Zahlen werden wir auch die Gaußschen Zahlen (schlechthin) benötigen, d. h. diejenigen komplexen Zahlen, deren Real- und Imaginärteil rationale Zahlen sind.

Der Zusammenhang zwischen dem Bereich der Gaußschen Zahlen und dem der ganzen Gaußschen Zahlen ist dem zwischen dem Bereich der rationalen Zahlen und dem der ganzen rationalen Zahlen analog. Genauer drückt sich das in den drei folgenden, vom Leser leicht nachprüfbaren Aussagen aus, die wir oft ohne weitere Erläuterungen benutzen werden:

I. Summe, Differenz und Produkt zweier ganzer Gaußscher Zahlen sind wieder ganze Gaußsche Zahlen. (Diese Eigenschaft beschreibt man in kurzen Worten dadurch, dass man sagt, die ganzen Gaußschen Zahlen bilden einen Ring.)

II. Summe, Differenz, Produkt und Quotient (wenn der Divisor von Null verschieden ist) zweier Gaußscher Zahlen sind wieder Gaußsche Zahlen. (Dafür sagt man kurz, die Gaußschen Zahlen bilden einen Körper.)

III. Der Quotient zweier ganzer Gaußscher Zahlen ist eine Gaußsche Zahl. Umgekehrt lässt sich jede Gaußsche Zahl als Quotient zweier ganzer Gaußscher Zahlen darstellen.

Die letzte Behauptung müssen wir etwas erläutern. Es seien also $\alpha = a + bi$ und $\beta = c + di$ ganze Gaußsche Zahlen (a, b, c, d ganze rationale Zahlen), und es sei $\beta \neq 0$.
Wir werden zeigen, dass $\gamma = \frac{\alpha}{\beta}$ eine Gaußsche Zahl ist. Es ist nämlich

$$\gamma = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd-adi-bci}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Die Zahlen $\frac{ac+bd}{c^2+d^2}$ und $\frac{bc-ad}{c^2+d^2}$ - Real- und Imaginärteil der Zahl γ - sind rationale Zahlen. Daher ist γ eine Gaußsche Zahl.

Schließlich wollen wir noch bemerken, dass offenbar jede rationale Zahl auch eine Gaußsche Zahl ist. Der Imaginärteil ist hier gleich 0. Ebenso ist jede ganze rationale Zahl eine ganze Gaußsche Zahl.

Für die weiteren Betrachtungen ist es zweckmäßig, sich die ganzen Gaußschen Zahlen in der komplexen Ebene angeordnet vorzustellen.
Nach ihrer Definition sind die ganzen Gaußschen Zahlen Punkte mit ganzzahligen Koordinaten (Abb. 1). Sie liegen auf den Eckpunkten eines Netzes von Quadraten der Kantenlänge, das die ganze komplexe Ebene bedeckt.

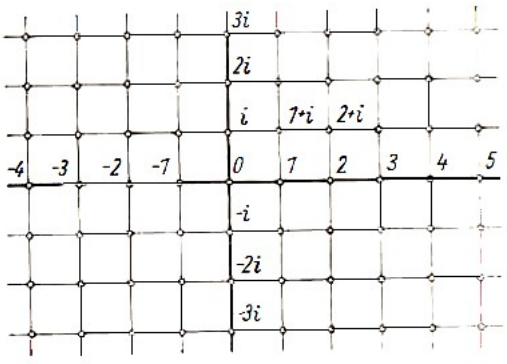

Abb. 1

Aus der Theorie der komplexen Zahlen benötigen wir die Begriffe "Norm" und "Betrag" einer komplexen Zahl. Als Norm der komplexen Zahl $a = x + iy$ wird die nichtnegative reelle Zahl $N(\alpha) = x^2 + y^2$ bezeichnet, als Betrag die nichtnegative reelle Zahl $|\alpha| = \sqrt{x^2 + y^2}$.

Geometrisch ist der Betrag einer komplexen Zahl der Abstand des entsprechenden Punktes in der komplexen Ebene vom Koordinatenursprung.
Die Norm $N(\alpha)$ der Zahl α kann als Produkt der Zahl α mit ihrer konjugiert komplexen Zahl $\overline{\alpha}$ ($\overline{\alpha} = x - iy$) dargestellt werden,

$$N(\alpha) = \alpha \cdot \overline{\alpha}$$

Die Eigenschaft

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \tag{2}$$

also die Tatsache, dass die Norm multiplikativ ist, wird als bekannt vorausgesetzt.
Wir erwähnen ferner: Ist α eine Gaußsche Zahl, so ist $N(\alpha)$ eine nichtnegative rationale Zahl; ist α sogar eine ganze Gaußsche Zahl, dann ist $N(\alpha)$ eine nichtnegative ganze Zahl.[9]
Nicht jede positive ganze Zahl ist Norm einer ganzen Gaußschen Zahl. Es gilt nämlich folgender Satz:

Satz 7. Eine positive ganze rationale Zahl c ist genau dann Norm einer ganzen Gaußschen Zahl, wenn die Zahl c als Summe zweier Quadrate ganzer Zahlen darstellbar ist.

Beweis. Ist $\alpha = a + bi$ eine ganze Gaußsche Zahl, so ist $N(\alpha) = a^2 + b^2$ die Summe der Quadrate der ganzen rationalen Zahlen a und b.
Wenn umgekehrt $c = x^2 + y^2$ ist, wobei x und y ganze rationale Zahlen sind, dann ist $c = N(x + yi)$, wobei $x + yi$ eine ganze Gaußsche Zahl ist. Damit ist der Satz bewiesen.

Nun kann man leicht zeigen, dass nicht jede positive ganze Zahl Summe zweier Quadrate ist. Wir werden z.B. zeigen, dass eine ungerade positive ganze Zahl t, die sich als Summe zweier Quadrate ganzer Zahlen darstellen lässt, bei Division durch 4 den Rest 1 ergibt, d.h. gleich einer Zahl der Gestalt $t = 4k + 1$ ist.

Ist nämlich $t = x^2 + y^2$, so muss eine der Zahlen, etwa x gerade sein, die andere, in unserem Fall y, ungerade.
Es sei $x = 2m$ und $y = 2n + 1$. Dann ist

$$x^2 = 4m^2 \qquad \text{und} \qquad y = 4(n^2 + n) + 1$$

[9] Der Betrag $|\alpha|$ einer Gaußschen Zahl braucht keine rationale Zahl zu sein. Im folgenden wird deshalb in der Hauptsache nicht der Betrag, sondern die Norm benutzt.

also

$$t = 4(m^2 + n^2 + n) + 1$$

Das beweist aber unsere Behauptung.
Demzufolge sind die Zahlen 7, 11, 15 u.a. nicht als Summe zweier Quadrate darstellbar und folglich auch nicht Norm von ganzen Gaußschen Zahlen.

Die Frage, welche ganzen Zahlen als Summe zweier Quadrate darstellbar sind, also Norm ganzer Gaußscher Zahlen sind, werden wir nach der Untersuchung der Arithmetik der ganzen Gaußschen Zahlen, zu der wir gleich übergehen wollen, beantworten.

Ebenso wie im Bereich (im Ring) der ganzen rationalen Zahlen ist auch im Bereich der ganzen Gaußschen Zahlen die Frage nach der Teilbarkeit von grundlegendem Interesse.
Wenn zu zwei ganzen Gaußschen Zahlen α und β eine ganze Gaußsche Zahl γ existiert derart, dass die Gleichung

$$\beta = \alpha \cdot \gamma \tag{3}$$

erfüllt ist, wollen wir sagen, dass α die Zahl β teilt, und diesen Sachverhalt durch $\alpha \mid \beta$ bezeichnen. Da aus (3) die Beziehung $N(\beta) = N(\alpha) \cdot N(\gamma)$ folgt, ist also $N(\alpha) \mid N(\beta)$, wobei ja $N(\alpha)$ und $N(\beta)$ ganze rationale Zahlen sind, eine notwendige Bedingung dafür, dass β durch α teilbar ist.

Im Fall ganzer rationaler Zahlen gibt es nur zwei Zahlen, welche Teiler aller ganzen Zahlen sind, nämlich +1 und -1. Bei den ganzen Gaußschen Zahlen hat man vier solcher Zahlen, nämlich +1, -1, +i, -i. Man sieht leicht, dass die vier genannten Zahlen wirklich diese Eigenschaft haben. Es ist nämlich

$$\begin{aligned} \alpha = \alpha \cdot 1 \quad &, \quad \alpha = (-\alpha) \cdot (-1) \\ \alpha = (-\alpha i) \cdot i \quad &, \quad \alpha = (\alpha i) \cdot (-i) \end{aligned}$$

Andere ganze Gaußsche Zahlen mit den oben genannten Eigenschaften gibt es nicht. Ist nämlich ξ eine beliebige ganze Gaußsche Zahl, welche alle ganzen Gaußschen Zahlen teilt, dann muss sie insbesondere die Zahl 1 teilen.
Deshalb bezeichnet man solche Zahlen als Teiler der Einheit oder einfach als Einheiten. Aus $N(\xi) \mid 1$ folgt aber $N(\xi) = 1$.

Ist ξ nun gleich $x + yi$, so muss also $x^2 + y^2 = 1$ sein. Es ist klar, dass diese Ungleichung genau vier Lösungen in ganzen rationalen Zahlen hat: $x = 1$, $y = 0$; $x = -1$, $y = 0$; $x = 0$, $y = 1$; $x = 0$, $y = -1$.
Diese vier Lösungen entsprechen gerade den ganzen Gaußschen Zahlen +1, -1, i, -i.

Genau wie für die ganzen rationalen Zahlen lassen sich im Bereich der ganzen Gaußschen Zahlen die Begriffe gemeinsamer Teiler, größter gemeinsamer Teiler, teilerfremde Zahlen und Primzahlen definieren. Die Definition der ersten drei Begriffe lässt sich wörtlich aus dem Bereich der ganzen rationalen Zahlen übertragen. Bei der Definition der Gaußschen Primzahlen müssen wir jedoch etwas länger verweilen.

Definition 5. Eine ganze Gaußsche Zahl π heißt Primzahl, wenn bei jeder Zerlegung der Zahl π in ein Produkt $\tau \cdot \sigma$ zweier ganzer Gaußscher Zahlen einer der Faktoren (τ oder σ) eine Einheit ist (man rechnet dabei die Einheiten nicht zu den Primzahlen).

Man kann diese Eigenschaft auch so ausdrücken: Eine Gaußsche Primzahl ist eine von Null verschiedene ganze Gaußsche Zahl, deren Norm größer als Eins ist und die sich nicht in ein

Produkt zweier ganzer Gaußscher Zahlen zerlegen lässt, deren Norm kleiner als die Norm der Zahl π ist.

Nach dieser Definition sind z.B. die Zahlen

$$\pi_1 = 2 + i \quad (N(\pi_1) = 5) \qquad , \qquad \pi_2 = 3 + 2i \quad (N(\pi_2) = 13)$$

Gaußsche Primzahlen.
Allgemein sind alle Zahlen Primzahlen, deren Norm eine rationale Primzahl ist. In den folgenden Betrachtungen werden wir sehen, dass diese Beispiele die Menge der Gaußschen Primzahlen nicht erschöpfen. Wir werden im Laufe unserer Untersuchungen alle Gaußschen Primzahlen angeben.
Zuerst wollen wir jedoch den Hauptsatz der elementaren Zahlentheorie für Gaußsche ganze Zahlen formulieren und beweisen.

Hauptsatz. Jede ganze Gaußsche Zahl $\alpha \neq 0$ lässt sich in ein Produkt Gaußscher Primzahlen

$$\alpha = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_k \tag{4}$$

zerlegen; dabei sind die π_i nicht notwendig voneinander verschiedene Primzahlen. Eine solche Zerlegung ist in folgendem Sinne eindeutig: Ist

$$\alpha = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_l \tag{5}$$

eine andere Zerlegung der Zahl α in ein Produkt von Gaußschen Primzahlen σ_i, so haben beide Zerlegungen die gleiche Anzahl von Faktoren, $k = l$, und die Zerlegungen (4) und (5) unterscheiden sich höchstens durch die Anordnung der Faktoren im Produkt, die eventuell noch mit Einheiten multipliziert sein können.

Zu dem Teil des Satzes, der die Eindeutigkeit betrifft, wollen wir noch folgendes bemerken: Wenn etwa

$$\alpha = \pi_1 \cdot \pi_2 \cdot \pi_3$$

das Produkt der Primzahlen π_1, π_2, π_3 ist, so ist z.B.

$$\alpha = (-\pi_3) \cdot (i\pi_2) \cdot (i\pi_1) \quad (= \pi_1 \cdot \pi_2 \cdot \pi_3)$$

eine "andere " Darstellung der Zahl α als Produkt der Primzahlen $-\pi_3$, $i\pi_2$, $i\pi_1$, die von den Primzahlen π_1, π_2, π_3 verschieden sind.

Man bemerkt jedoch sofort, dass jede der Zahlen $-\pi_3$, $i\pi_2$, $i\pi_1$ als Produkt einer der Zahlen π_3, π_2, π_1 mit einer Einheit erhalten werden kann; auch die ursprüngliche Anordnung der betreffenden Zahl war eine andere.
Derartige Unterschiede in den Zerlegungen ein und derselben Zahl seien aber zugelassen. Der zweite Teil des Satzes sagt nun gerade, dass andere Arten von Unterschieden in den Zerlegungen einer Zahl nicht auftreten können.

Diese Tatsache unterscheidet sich durch nichts von der Situation in der Arithmetik der ganzen rationalen Zahlen. Sie wird nur dadurch erschwert, dass wir im Fall der Arithmetik der ganzen Gaußschen Zahlen über mehr Einheiten verfügen.[10]

[10]Wir bemerken dazu, dass die Eindeutigkeit der Zerlegung bis auf Vorzeichen der Faktoren, von der im Fall der ganzen rationalen Zahlen die Rede war, gerade die Eindeutigkeit bis auf Faktoren, welche Einheiten sind, bedeutet. In diesem Fall sind nämlich +1 und -1 die einzigen Einheiten.

Die Behauptung über die Eindeutigkeit kann man auch kürzer formulieren, wenn man den Begriff der assoziierten ganzen Gaußschen Zahlen einführt.

Definition 6. Zwei ganze Gaußsche Zahlen heißen assoziiert, wenn sie sich voneinander durch einen Faktor, der eine Einheit ist, unterscheiden; mit anderen Worten, β, $-\beta$, $i\beta$, $-i\beta$ sind assoziierte ganze Gaußsche Zahlen, wenn β eine beliebige ganze Gaußsche Zahl ist.

Wenn wir diese Definition benutzen, lässt sich die Behauptung der Eindeutigkeit im Hauptsatz folgendermaßen formulieren:

Ist $\alpha = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_k$ und $\alpha = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_l$, wobei die π $(i = 1, 2, ..., k)$ und σ_j $(j = 1, 2, ..., l)$ Primzahlen sind, dann ist $l = k$, und die Faktoren σ_j lassen sich so anordnen, dass jedes σ_j mit der entsprechenden Primzahl π_j assoziiert ist.

Wir wollen den Beweis des Hauptsatzes skizzieren. Er wird fast genau so geführt wie der Beweis der entsprechenden Behauptung für ganze rationale Zahlen. Das ist gerade der Grund, dass wir ihn nicht im einzelnen ausführen; wir empfehlen dem Leser aber nachdrücklich, das selbst zu tun.

Die erste Behauptung des Satzes über die Existenz einer Zerlegung kann man mittels vollständiger Induktion nach der Norm der Zahl beweisen:

a) Ist $N(\alpha) = 1$, so ist $\alpha = 1, -1, i, -i$; die Zahl α ist in ein Produkt einer leeren Menge von Primzahlen zerlegbar.[11]

b) Es sei $N(\alpha) = n$, und für alle ganzen Gaußschen Zahlen mit kleinerer Norm sei die Behauptung schon bewiesen. Dann ist entweder α eine Primzahl, und es ist alles bewiesen, oder es ist $\alpha = \rho \cdot \tau$, wobei $N(\rho) < n$ und $N(\tau) < n$ ist.
Nach der Induktionsannahme existieren für ρ und τ Zerlegungen

$$\rho = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_k \qquad \text{und} \qquad \tau = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_l$$

Dann ist aber

$$\alpha = \rho = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_k \cdot \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_l$$

Zerlegung für α.

Den Beweis der Behauptung über die Eindeutigkeit kann man mit Hilfe von Eigenschaften führen, die im Bereich der ganzen Gaußschen Zahlen für den größten gemeinsamen Teiler und für teilerfremde Zahlen bestehen.
Der Schlüssel des ganzen Beweises ist die Behauptung, dass im Bereich der ganzen Gaußschen Zahlen eine Teilung mit Rest möglich ist. Sie wird folgendermaßen formuliert:

Es seien α, β $(\beta \neq 0)$ zwei ganze Gaußsche Zahlen; dann existieren solche ganzen Gaußschen Zahlen γ und ρ, wobei $N(\rho) < N(\beta)$ ist, dass

$$\alpha = \gamma \cdot \beta + \rho$$

ist.
Der Beweis beruht auf einer sehr einfachen geometrischen Tatsache:
Ist P ein Punkt, der im Inneren eines Quadrates mit der Seitenlänge a oder auf einer der Seiten liegt, so ist der Abstand des Punktes P von der nächstliegenden Ecke kleiner als a.

[11] Bezüglich der "Zerlegbarkeit" der Einheit in ein Produkt von Primfaktoren treffen wir dieselbe Übereinkunft wie auch für ± 1 im Fall ganzer rationaler Zahlen

Der Punkt nämlich, der den größten Abstand von allen Ecken hat, ist der Mittelpunkt des Quadrates. Der Abstand des Mittelpunktes von einer beliebigen Ecke ist jedoch gleich $\frac{1}{\sqrt{2}}a < a$. Für jeden anderen Punkt des Quadrates ist der Abstand von der nächstliegenden Ecke kleiner.

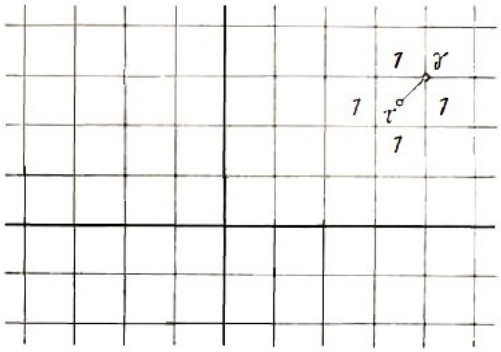

Abb. 2

Aus dieser einfachen Aussage ersieht man jetzt sofort, dass man zu jedem Punkt τ der komplexen Ebene einen Punkt γ mit ganzen Koordinaten - einen Punkt also, der eine ganze Gaußsche Zahl darstellt - finden kann, der von τ weniger als 1 entfernt ist (Abb. 2).
Das besagt also, dass zu jeder komplexen Zahl τ eine ganze Gaußsche Zahl γ existiert derart, dass $N(\tau - \gamma) < 1$ ist.
Wir können somit auch für die Zahl $\tau = \frac{\alpha}{\beta}$ eine solche Zahl γ finden; wir setzen dann ρ gleich $\alpha - \gamma\beta$. Dann ist ρ eine ganze Gaußsche Zahl, für die

$$N(\rho) = N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta) \qquad \text{und} \qquad \alpha = \gamma\beta + \rho$$

ist. Damit ist die Behauptung bewiesen.

Nachdem jetzt der Satz über die Teilbarkeit mit Rest bekannt ist, kann man alle übrigen Eigenschaften wie zuvor im Fall der rationalen Zahlen beweisen:

1. Man zeigt zunächst die Existenz des ggT zweier ganzer Gaußscher Zahlen α, β indem man für die Zahl $\delta \neq 0$ mit kleinster Norm aus der Menge der Zahlen der Gestalt $\alpha\xi + \beta\eta$ (xi und η ganze Gaußsche Zahlen) die Eigenschaften des ggT nachweist;

2. man führt den Begriff teilerfremder ganzer Gaußscher Zahlen ein und beweist das Hauptlemma:
Wenn α und β_1 teilerfremd und α und β_2 teilerfremd sind, dann sind auch α und $\beta_1 \cdot \beta_2$ teilerfremd.
Danach beweist man ganz einfach durch vollständige Induktion über die Norm die Eindeutigkeit der Zerlegung in Primfaktoren.

5 Gaußsche Primzahlen und die Darstellung ganzer rationaler Zahlen als Summe zweier Quadrate

Wir wollen jetzt zur Beschreibung aller Gaußschen Primzahlen übergehen. Zuerst beweisen wir einige Hilfssätze.

Hilfssatz 1. Jede Gaußsche Primzahl ist Teiler einer rationalen Primzahl.[12]

In der Tat, da $N(\alpha) = \alpha \cdot \overline{\alpha}$ ist, teilt jede ganze Gaußsche Zahl ihre Norm, $\alpha \mid N(\alpha)$.
Es sei jetzt π eine Gaußsche Primzahl, dann gilt $\pi \mid N(\pi)$. Wir nehmen einmal an, $N(n) = p_1 \cdot p_2 \cdot ... \cdot p_r$ sei eine Zerlegung der Zahl $N(\pi)$ in ein Produkt rationaler Primzahlen; dann gilt also $\pi \mid p_1 \cdot p_2 \cdot ... \cdot p_r$; folglich teilt π eine der Primzahlen p_i.
Würde nämlich die ganze Gaußsche Primzahl π keine der Zahlen p_i teilen, dann wäre sie zu jeder von ihnen teilerfremd, folglich auch zu ihrem Produkt $N(\pi)$. Das ist aber wegen $\pi \mid N(\pi)$ unmöglich. Somit ist die Zahl π ein Teiler einer der rationalen Primzahlen p_i. Damit ist der Hilfssatz bewiesen.

Hilfssatz 2. Die Norm $N(\pi)$ einer Gaußschen Primzahl π ist entweder eine rationale Primzahl oder das Quadrat einer rationalen Primzahl.

Wie wir schon wissen, teilt π irgendeine rationale Primzahl p. Es sei $p = \pi \cdot \gamma$.
Dann ist, wenn wir zur Norm übergeben, $N(\pi) \cdot N(\gamma) = p^2$. Es sind also zwei nur Fälle möglich:
1. $N(\pi) = N(\gamma) = p$ und
2. $N(\pi) = p^2 = N(p), N(\gamma) = 1$.
Damit ist der Hilfssatz bewiesen.

Der zweite Fall bedeutet, dass γ Einheit ist und dass eine der Gleichungen

$$\pi = p, \quad \pi = -p, \quad \pi = ip, \quad \pi = -ip$$

gilt. Demnach ist p eine rationale Primzahl, die gleichzeitig auch Gaußsche Primzahl ist.
Im ersten Fall ist γ eine Gaußsche Primzahl, da $N(\gamma) = p$ ist. Es ist $\gamma = \overline{\pi}$; es ist nämlich $N(\pi) = p = \pi \cdot \overline{\pi}$ und $\overline{\pi}$ Primzahl. Andererseits ist aber $p = \pi \cdot \gamma$; also ist $\overline{\pi} = \gamma$.

Ist andererseits p eine beliebige rationale Primzahl, so ist sie, wenn sie keine Gaußsche Primzahl ist, durch irgendeine von p verschiedene Gaußsche Primzahl teilbar, und dabei ist, wie wir gesehen haben, $p = \pi \cdot \overline{\pi}$; somit ist p das Produkt zweier konjugiert komplexer Gaußscher Primzahlen.
In diesem Fall ist p die Norm einer ganzen Gaußschen Zahl, also als Summe zweier Quadrate darstellbar. Eine solche Primzahl ist, wenn sie ungerade ist (d.h. $p \neq 2$), eine Zahl der Gestalt $4n + 1$.

Man kann zeigen, dass alle Primzahlen der Gestalt $4n+1$ als Summe zweier Quadrate darstellbar sind, d.h. Normen ganzer Gaußscher Zahlen sind; es sind also keine Gaußschen Primzahlen, fallen folglich in die Klasse derjenigen rationalen Primzahlen, die in ein Produkt zweier konjugiert komplexer Gaußscher Primzahlen zerlegbar sind. Diese Behauptung werden wir hier nicht

[12] Eine rationale Primzahl ist zwar immer auch eine ganze Gaußsche Zahl, aber als ganze Gaußsche Zahl braucht sie keine Gaußsche Primzahl zu sein; sie kann durch eine ganze Gaußsche Zahl mit kleinerer Norm teilbar sein. So ist z.B. die Zahl 2, als ganze rationale Zahl betrachtet, eine Primzahl, aber als ganze Gaußsche Zahl keine Gaußsche Primzahl. Im Bereich der ganzen Gaußschen Zahlen lässt sich 2 nämlich in $(1 + i) \cdot (1 - i)$ zerlegen, und keiner der Faktoren $1 + i$ und $1 - i$ ist Einheit. Auch 5 ist im Bereich der Gaußschen Zahlen keine Primzahl, denn es ist $5 = (2 + i) \cdot (2 - i)$.

bewiesen.[13]

Alle ungeraden rationalen Primzahlen, die nicht die Gestalt $4n+1$, also die Gestalt $4n+3$ haben, bilden gerade die Menge derjenigen rationalen Primzahlen, die auch im Bereich der Gaußschen Zahlen Primzahlen sind.

Eine gewisse Sonderstellung nimmt die Primzahl 2 ein. Offenbar ist

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

$N(1-i) = 2$. Somit ist 2 durch das Quadrat der Gaußschen Primzahl $1-i$ teilbar.

Wenn wir als bekannt voraussetzen, dass alle Primzahlen der Gestalt $4n+1$ als Summe zweier Quadrate darstellbar sind. können wir jetzt auch sagen, welche ganzen rationalen Zahlen sich als Summe zweier Quadrate darstellen lassen. Wie wir schon wissen, hat eine Zahl t diese Eigenschaft genau dann, wenn sie Norm einer ganzen Gaußschen Zahl α ist: $t = N(\alpha)$.
Die Zahl α ist in ein Produkt von Gaußschen Primzahlen zerlegbar:

$$\alpha = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_r \tag{6}$$

Wir teilen alle Primzahlen π_i $(i = 1, 2, ..., r)$ in zwei Klassen ein:
In die erste Klasse nehmen wir diejenigen Zahlen π_i auf, deren Norm eine Primzahl ist, in die zweite Klasse alle Zahlen, deren Normen Quadrate von Primzahlen sind.[14]
Wir bezeichnen die verschiedenen Zahlen der ersten Klasse mit σ_j $(j = 1, 2, ..., l)$, die der zweiten Klasse mit ρ_k $(k = 1, 2, ..., s)$. Dann gilt

$$N(\sigma_j) = p_j \qquad , \qquad N(\rho_k) = q_k^2$$

wobei die p_j, Primzahlen der Gestalt $4n+1$ oder 2, die q_k Primzahlen der Gestalt $4n+3$ sind.

Wenn wir gleiche Primzahlen auf der rechten Seite von (6) zusammenfassen, können wir α als Potenzprodukt der Primzahlen σ_j und ρ_k schreiben:

$$\alpha = \sigma_1^{a_1} \cdot ... \cdot \sigma_l^{a_l} \cdot \rho_1^{b_1} \cdot ... \cdot \rho_k^{b_k} \tag{7}$$

Für die Normen ergibt sich

$$\begin{aligned} N(\alpha) = t &= N(\sigma_1^{a_1}) \cdot ... \cdot N(\sigma_l^{a_l}) \cdot N(\rho_1^{b_1}) \cdot ... \cdot N(\rho_k^{b_k}) \\ t &= p_1^{a_1} \cdot ... \cdot p_l^{a_l} \cdot q_1^{2b_1} \cdot ... \cdot q_k^{2b_k} \end{aligned} \tag{8}$$

Wir sehen, dass die Primzahlen q_k in der Zerlegung der Zahl t in geraden Potenzen vorkommen. Es sei umgekehrt t von der Gestalt (8), wobei die p_j Primzahlen der Gestalt $4n+1$ oder 2, die q_k Primzahlen der Gestalt $4n+3$ sind und $a_1, ..., a_l, b_1, ..., b_k$ ganze nicht negative Zahlen. Dann kann man, da jedes p_j Summe zweier Quadrate ist, passende σ_j so finden, dass $N(\sigma_j) = p_j$ ist.
Setzt man ferner $\rho_k = q_k$ und schließlich

$$\alpha = \sigma_1^{a_1} \cdot ... \cdot \sigma_l^{a_l} \cdot \rho_1^{b_1} \cdot ... \cdot \rho_k^{b_k}$$

[13] Den Beweis dieser Tatsache, der auf der Theorie der Kongruenzen beruht und auf L. Euler zurückgeht, kann man in fast allen Lehrbüchern der Zahlentheorie finden.

[14] Es kann natürlich vorkommen, dass eine dieser Klassen leer ist. Dies beeinflusst jedoch den Gang unserer Überlegungen nicht wesentlich. Man muss dabei nur beachten, dass alle Zahlen a_j oder alle Zahlen b_k (in den Zerlegungen (7) und (8)) Null sein können.

so erhält man $t = N(\alpha)$, d. h., die Zahl t lässt sich als Summe zweier Quadrate darstellen. Wir haben also den folgenden Satz erhalten:

Satz 8. Eine ganze rationale Zahl ist genau dann als Summe zweier Quadrate darstellbar, wenn in der Zerlegung dieser Zahl in Primfaktoren die Primzahlen der Gestalt $4n + 3$ in gerader Potenz vorkommen.[15]

Wie wir sehen, gibt uns dieser Satz ein Kriterium dafür, wann eine diophantische Gleichung zweiten Grades

$$x^2 + y^2 = t$$

eine (ganzzahlige) Lösung hat. Wie man jedoch eine solche Lösung findet, können wir hier nicht behandeln.

Allgemein kann man sagen: Die Untersuchung diophantischer Gleichungen der Gestalt

$$ax^2 + 2bxy + cy^2 = t$$

hängt eng mit der Arithmetik in Zahlbereichen zusammen, die dem Bereich der ganzen Gaußschen Zahlen analog sind.

Bei solchen Untersuchungen ist die folgende überraschende Tatsache wesentlich, auf welche die Mathematiker um die Mitte des vorigen Jahrhunderts stießen:
Nicht in allen den Gaußschen Zahlen ähnlichen Arithmetiken gilt der Satz von der Eindeutigkeit der Zerlegung einer Zahl in ein Produkt von Primzahlen. Ohne auf die sich hier andeutende Problematik näher einzugehen, wollen wir ein Beispiel einer "Arithmetik" anführen, bei dem der Hauptsatz nicht gilt.

[15] Diese Formulierung umfasst auch den Fall, dass überhaupt keine Primzahlen der Gestalt $4n + 3$ in der Zerlegung der betrachteten Zahl vorkommen; die Zahl 0 ist ja eine gerade Zahl.

6 Die Arithmetik der Zahlen $x + y\sqrt{-5}$

Wir wollen jetzt einmal komplexe Zahlen der Gestalt

$$\alpha = x + y\sqrt{-5} \tag{1}$$

betrachten, wobei x und y ganze rationale Zahlen sind. Es ist leicht zu sehen, dass Summe, Differenz und Produkt von Zahlen der Gestalt (1) wieder von dieser Gestalt sind. Wir wollen die Menge aller Zahlen der Gestalt (1) mit Γ bezeichnen.

Offenbar enthält Γ alle ganzen rationalen Zahlen (für $y = 0$). So wie im Fall der ganzen rationalen und der ganzen Gaußschen Zahlen kann man von der Teilbarkeit in Γ sprechen:
α teilt β ($\alpha \mid \beta$), wenn β/α wieder eine Zahl aus Γ, d.h. in der Gestalt (1) darstellbar ist.
Wie im Fall der ganzen Gaußschen Zahlen spielen die Normen der Zahlen aus Γ eine wichtige Rolle bei der Frage der Teilbarkeit:

$$N(\alpha) = N(x + y\sqrt{-5}) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2$$

Die Norm jeder Zahl aus Γ ist also eine ganze rationale Zahl. Da

$$N(\xi \cdot \eta) = N(\xi) \cdot N(\eta)$$

gilt, ist $N(\alpha)N(\beta)$ eine notwendige (doch im allgemeinen nicht hinreichende) Bedingung dafür, dass β durch α teilbar ist.

Genau wie im Fall der ganzen Gaußschen Zahlen lassen sich die Begriffe Einheit und Primzahl auf natürliche Weise einführen. In bezug auf die Einheiten ist die Situation hier sogar einfacher als bei den ganzen Gaußschen Zahlen.
Es sind nämlich nur die Zahlen ± 1 Einheiten in Γ. Wenn $\xi = u + v\sqrt{-5}$ eine Einheit ist, muss die Bedingung $N(\xi) = u^2 + 5v^2 = 1$ erfüllt sein. Diese diophantische Gleichung kann jedoch offensichtlich keine von $u = \pm 1$, $v = 0$ verschiedenen Lösungen haben.

Die Tatsache, dass jede Zahl aus Γ als Produkt von Primzahlen darstellbar ist, beweist man mittels vollständiger Induktion über die Norm wörtlich so wie im Fall der ganzen Gaußschen Zahlen. Diese Zerlegung ist jedoch nicht eindeutig, wie wir an einem einfachen Beispiel zeigen werden.

Wir zeigen zunächst, dass die Zahlen

$$2 = 2 + 0\sqrt{-5}, \quad 3 = 3 + 0\sqrt{-5}, \quad 1 + \sqrt{-5}, \quad 1 - \sqrt{-5}$$

in Γ Primzahlen sind. Es ist nämlich

$$N(2) = 4, \quad N(3) = 9, \quad N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$$

Wäre eine dieser Zahlen in Γ keine Primzahl, so wäre sie nur durch eine Zahl $\alpha = x + y\sqrt{-5}$ teilbar, für die $N(\alpha) = x^2 + 5y^2 = 2$ oder $N(\alpha) = x^2 + 5y^2 = 3$ ist. Solche Zahlen gibt es aber in Γ nicht; davon überzeugt man sich leicht, da die Gleichungen

$$x^2 + 5y^2 = 2 \qquad , \qquad x^2 + 5y^2 = 3 \tag{2,3}$$

keine ganzzahligen Lösungen haben.

Die betrachteten vier Zahlen sind also Primzahlen in Γ. Nun gilt aber

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{4}$$

wie man leicht sieht.
Das zeigt, dass es für die Zahl 6 aus Γ zwei verschiedene Darstellungen als Produkt von Primzahlen gibt.

Auf diese bemerkenswerte Erscheinung stieß der deutsche Mathematiker E. Kummer (1810-1893) bei seinem Versuch, die bekannte Fermatsche Vermutung zu beweisen.
In der Folgezeit wurden die Schwierigkeiten, die im Zusammenhang damit auftauchten, dass der Hauptsatz der elementaren Zahlentheorie in einigen wichtigen Zahlbereichen nicht gilt, von Kummer selbst sowie von anderen bekannten Mathematikern, wie R. Dedekind, E. Solotarew, L. Kronecker und anderen erfolgreich überwunden.

Es entstand eine umfangreiche neue Disziplin in der Mathematik - die Theorie der algebraischen Zahlen, die sich bis in unsere Tage erfolgreich weiter entwickelt.

Literatur

Chintschin, A. J., Die Elemente der Zahlentheorie, in: Enzyklopädie der Elementarmathematik, Bd. I, 5. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1970 (Übersetzung aus dem Russischen).

Dynkin, E. B., und W. A. Uspenski, Mathematische Unterhaltungen II: Aufgaben aus der Zahlentheorie, 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1968 (Übersetzung aus dem Russischen).

Gelfond, A. O., Die Auflösung von Gleichungen in ganzen Zahlen, 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1968 (Übersetzung aus dem Russischen).

Hasse, H., Zahlentheorie, 2. Aufl., Akademie-Verlag, Berlin 1963.

Hasse, H., Vorlesungen über Zahlentheorie, 2. Aufl., Springer-Verlag, Berlin-Heidelberg-New York 1969.

Holzer, L., Zahlentheorie I-III, B. G. Teubner, Leipzig 1958, 1959 bzw. 1965.

Jung, H. W. E., Zahlentheorie, 2. Aufl., Fachbuchverlag, Leipzig 1952.

Landau, E., Vorlesungen über Zahlentheorie, 3 Bde., Hirzel, Leipzig 1927.

Landau, E., Diophantische Gleichungen mit endlich vielen Lösungen, neu herausgegeben von A. Walfisz, VEB Deutscher Verlag der Wissenschaften, Berlin 1959.

Lietzmann, W., Altes und Neues vom Kreis, 4. Aufl., B. G. Teubner, Leipzig 1966.

Lietzmann, W., Der Pythagoreische Lehrsatz, mit einem Ausblick auf das Fermatsche Problem, 9. Aufl., B. G. Teubner, Leipzig 1968.

Sominsnki, I. S., Die Methode der vollständigen Induktion, 10. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1971 (Übersetzung aus dem Russischen).

Winogradow, I. M., Elemente der Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin / Verlag R. Oldenbourg, München 1955.