A.A. Belski und L.A. Kalujnine

Division mit Rest

Übersetzung und Redaktion: Ludwig Boll, Horst Belkner
1982 Deutscher Verlag der Wissenschaften
MSB: Nr. 115
Abschrift und LaTex-Satz: 2021 https://mathematikalpha.de

Inhaltsverzeichnis

1 Der Hauptsatz der Zahlentheorie

[1] Dieser Satz ist den Lesern wohlbekannt; sie benutzen ihn häufig beim Rechnen (beispielsweise bei der Bestimmung des Hauptnenners von Brüchen), wobei sie sich zuweilen nicht darüber im klaren sind, dass es sich um ein wichtiges Theorem handelt, das eines strengen und ausführlichen Beweises bedarf. Dabei geht es um folgendes:

Jede von null verschiedene ganze Zahl können wir in ein Produkt von Primzahlen zerlegen. Beispielsweise ist

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

Dabei kann es, wenn die Zahl sehr groß ist, manchmal ziemlich lange dauern, bis wir eine solche Zerlegung ermittelt haben; es lässt sich aber immer eine solche Zerlegung finden.
Oder haben wir bisher einfach immer Glück gehabt? Können wir wirklich davon überzeugt sein, dass jede von null verschiedene ganze Zahl als Produkt von Primzahlen dargestellt werden kann?
Nun, es ist tatsächlich so, doch muss diese Tatsache bewiesen werden. Der erste Teil des Hauptsatzes besagt:

Jede von null verschiedene ganze Zahl lässt sich als Produkt von Primzahlen darstellen.

Diese Aussage werden wir alsbald beweisen.
Ehe wir die zweite Aussage des Satzes formulieren, wenden wir uns nochmals dem Beispiel der Zerlegung der Zahl 420 in Primfaktoren zu. In der Schule wird dieses Verfahren folgendermaßen beschrieben:

420	2
210	2
105	3
35	5
7	7
1	

In dieser Weise haben wir die Zerlegung (1) erhalten. Kann es noch andere Methoden der Zerlegung geben? Woher wissen wir, dass sie immer dasselbe Ergebnis liefern?
Natürlich kann man beispielsweise versuchen, die gegebene Zahl in ein Produkt zweier kleinerer Zahlen zu zerlegen (die nicht teilerfremd zu sein brauchen), und dann jede dieser Zahlen wieder in ein Produkt kleinerer Zahlen usw., bis man zu Zahlen kommt, die nicht weiter zerlegbar, also Primzahlen, sind.
Jedoch ist schon nach dem ersten Schritt klar, dass dieses Verfahren nicht eindeutig ist. So finden wir etwa für die Zahl 420 die beiden Zerlegungen

$$420 = 20 \cdot 21 \qquad \text{und} \qquad 420 = 12 \cdot 28$$

Daher taucht 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

[1] Das Originalbuch enthält außergewöhnlich viele Druckfehler. In der Abschrift wurde versucht, diese zu korrigieren. Es ist nicht sicher, dass alle Fehler gefunden wurden.

ganzen Zahlen gibt, und die entsprechende Aussage, nämlich die Behauptung, dass die Zerlegung einer von null verschiedenen ganzen Zahl in ein Produkt von Primzahlen eindeutig ist, bildet den zweiten Teil des Hauptsatzes:

Wenn eine von null verschiedene ganze Zahl n auf zwei verschiedene Arten in ein Produkt von Primzahlen zerlegt ist,

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

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

Bemerkung. Wenn beliebige (positive oder negative) ganze Zahlen betrachtet werden, ist die Eindeutigkeit der Zerlegung in Primfaktoren so zu verstehen, dass zwei Zerlegungen sich nicht nur durch die Anordnung, sondern auch durch die Vorzeichen entsprechender Primfaktoren unterscheiden dürfen.

Den Beweis dieser Behauptung führen wir ausführlich. Er ist schwieriger als der Beweis der ersten Aussage, da er mit einer Reihe von Eigenschaften der Arithmetik der ganzen Zahlen zusammenhängt.

1.1 Division mit Rest und größter gemeinsamer Teiler (ggT) zweier ganzer Zahlen

Ausgangspunkt unserer folgenden Überlegungen ist die Aussage, dass es im Bereich der ganzen Zahlen eine "Division mit Rest" gibt. Wir formulieren sie so:

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

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

ist.
Die Zahlen q und r sind durch a und b eindeutig bestimmt, d.h., ist

$$a = q_1 b + r_1 = a_2 b + r_2$$

mit $0 \leq r_i < |b|$ $(i = 1, 2)$, so ist $q_1 = q_2$ und $r_1 = r_2$. Ist in der Beziehung (1) die Zahl r gleich 0, so heißt das, dass die Zahl a durch die Zahl b teilbar ist; dafür schreibt man in der Zahlentheorie $b \mid a$.

Bemerkung. Für zwei ganze Zahlen a und b sind die Redeweisen "die Zahl a ist durch die Zahl b teilbar", "die Zahl a ist ein Vielfaches der Zahl b", "die Zahl b ist ein Teiler der Zahl a", "die Zahl b geht in der Zahl a auf" oder "die Zahl b teilt die Zahl a" gleichbedeutend; wir werden sie sämtlich benutzen.

Als erstes beweisen wir die Möglichkeit einer Darstellung der Form (1). Zunächst sei

$b > 0$. Wir bemerken, dass zu jeder rationalen Zahl τ (übrigens zu jeder reellen Zahl) eine ganze Zahl t mit $t \leq \tau < t + 1$ existiert. Insbesondere gibt es für $\tau = \frac{a}{b}$ ein ganzzahliges t mit

$$t \leq \frac{a}{b} < t + 1$$

Hieraus folgt

$$bt \leq a < bt + b \qquad \text{und} \qquad 0 \leq a - bt < b$$

Setzen wir $r = a - bt$ und $q = t$, so ist $a = bq + r$, wobei, wie aus der letzten Ungleichung folgt, $0 \leq r < b$ gilt. Damit haben wir die Darstellung (1) für den Fall $b > 0$ erhalten.

Nun sei $b < 0$; wieder existiert eine ganze Zahl t mit

$$t < \frac{a}{b} \leq t + 1$$

Multiplizieren wir diese Ungleichung mit b und beachten, dass $b < 0$ ist, so erhalten wir $b(t + 1) \leq a < bt$, also $0 \leq a - b(t + 1) < -b$.
Wir setzen jetzt $r = a - b(t + 1)$ und $q = t + 1$. Dann erhalten wir wieder eine Darstellung (1), $a = bq + r$, mit $0 \leq r < -b$, also $0 \leq r < |b|$.

Jetzt beweisen wir die Eindeutigkeit der Darstellung (1). Es sei

$$a = q_1 b + r_1 = q_2 b + + r_2$$

Dann ist $b(q_1 - q_2) = r_2 - r_1$. Wegen $0 \leq r_i < |b|$ $(i = 1, 2)$ ist aber die Differenz $r_2 - r_1$ dem absoluten Betrage nach kleiner als $|b|$. Daher ist eine Division durch b hier nur möglich, wenn $r_2 - r_1 = 0$ ist. Dann ist aber $r_1 = r_2$, also $q_1 b = q_2 b$ und somit $q_1 = q_2$.

Die Zahl q wird der Quotient, die Zahl r der Rest bei der Division von a durch b genannt.
Mit Hilfe des Satzes 1 können wir den Begriff des größten gemeinsamen Teilers (ggT) zweier Zahlen einführen und einige seiner Eigenschaften beweisen.

Definition 1. Sind a und b zwei von null verschiedene ganze Zahlen und existiert eine ganze Zahl c, für die $c \mid a$ und $c \mid b$ gilt, so nennen wir c einen gemeinsamen Teiler von a und b.

Wir weisen darauf hin, dass je zwei von null verschiedene ganze Zahlen stets gemeinsame Teiler haben, nämlich die Zahlen 1 und -1. Gibt es sonst keinen weiteren gemeinsamen Teiler, so nennt man die Zahlen a und b teilerfremd oder auch relativ prim. Auf teilerfremde Zahlen gehen wir später ein.

Definition 2. Eine ganze Zahl d heißt größter gemeinsamer Teiler (kurz ggT) der von null verschiedenen ganzen Zahlen a und b, wenn gilt:
1. Die Zahl d ist Teiler von a und von b;
2. Die Zahl d ist durch jeden anderen gemeinsamen Teiler von 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.

Aus dieser Definition folgt nicht ohne weiteres, dass zu je zwei von null verschiedenen Zahlen a und b ein ggT existiert. Es ist zwar tatsächlich der Fall, aber wir müssen es beweisen. Dabei werden wir die Zerlegung der Zahlen a und b in Primfaktoren nicht benutzen.

Satz 2. Zu jedem Paar ganzer von null verschiedener Zahlen a und b existiert ein ggT.

Beweis. Neben den Zahlen a und b betrachten wir alle Zahlen der Gestalt $xa + yb$ mit beliebigen ganzen Zahlen x und y; eine Zahl

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

nennt man eine Linearkombination der Zahlen a und b.
Für $a = 6$, $b = 22$ sind beispielsweise $28 = 1 \cdot 6 + 1 \cdot 22$, $10 = (-2) \cdot 6 + 1 \cdot 22$, $-92 = 3 \cdot 6 + (-5) \cdot 22$ usw. Linearkombinationen.
Zu gegebenen ganzen Zahlen a und b existieren unendlich viele ganze Zahlen, welche Linearkombinationen von a und b sind. Die Menge dieser Zahlen bezeichnen wir mit M. Insbesondere enthält M die Zahl a (für $x = 1$ und $y = 0$) und die Zahl b (für $x = 0$ und $y = 1$) sowie die Zahl 0 (für $x = 0$ und $y = 0$).

Alle Zahlen v der Menge M sind offenbar ganze Zahlen. Gehört v zu M, so auch $-v$ (ist $v = xa + yb$, so ist $-v = (-x)a + (-y)b$). Wir erwähnen noch eine Eigenschaft der Zahlen v der Menge M, die wir sofort benötigen:

Alle diese Zahlen sind durch alle gemeinsamen Teiler von a und b teilbar. Gilt nämlich $c \mid a$ und $c \mid b$ und ist $a = a' \cdot c$ und $b = b' \cdot c$, so ist $v = xa + yb = xa'c + yb'c = (xa' + yb')c$, also $c \mid v$. Nun sei $d \neq 0$ die Zahl mit dem kleinsten absoluten Betrag unter allen von null verschiedenen Zahlen der Menge M.

Eine solche Zahl existiert tatsächlich in der Menge M. Die Menge M enthält von null verschiedene ganze Zahlen, beispielsweise a oder b, deren absolute Beträge ganze positive, also natürliche Zahlen sind. Eine der grundlegenden Eigenschaften der Menge der natürlichen Zahlen, die auch als Axiom angesehen werden kann (vgl. I.S. Sominski, Die Methode der vollständigen Induktion), besteht aber darin, dass jede nichtleere Menge natürlicher Zahlen eine kleinste natürliche Zahl enthält.

Nun beweisen wir, dass d ein ggT von a und b ist. Die Zahl d besitzt die Eigenschaft 2 der Definition eines ggT, da diese Eigenschaft allen Zahlen aus M zukommt. Wir brauchen also nur noch zu zeigen, dass d auch die Eigenschaft 1 besitzt, d.h. gemeinsamer Teiler von a und b ist.
Wir beweisen $d \mid a$. Da d zu M gehört, lässt es sich in der Form $d = sa + tb$ darstellen, wobei s und t geeignete ganze Zahlen sind. Dividieren wir a durch d mit Rest, d.h., bestimmen wir zwei Zahlen q und r, $0 \leq r < |d|$, so dass

$$a = qd + r$$

gilt, so muss auch der Rest r zu M gehören. Es ist nämlich

$$r = a - qd = q - q(sa + tb) = (1 - qs)a + t'b$$

Nun erinnern wir uns, dass d die dem absoluten Betrage nach kleinste von null verschiedene Zahl der Menge M ist und $r < |d|$ gilt. Daher muss $r = 0$, also d ein Teiler von a sein.
Analog lässt sich beweisen, dass d die Zahl b teilt. Damit ist der Satz bewiesen.

Wir haben also bewiesen, dass zu je zwei von null verschiedenen ganzen Zahlen ein ggT existiert. Bei dem Beweis haben wir überdies gezeigt:

Satz 3. Jeder ggT zweier von null verschiedener ganzer Zahlen a und b kann als Linearkombination von a und b dargestellt werden.

(Diese Darstellung wird auch als Bezoutsche Identität bezeichnet.) Nun erhebt sich die Frage:
Besitzen je zwei von null verschiedene ganze Zahlen a und b genau einen ggT? Natürlich nicht! Denn mit d besitzt auch $-d$ die Eigenschaften 1 und 2 der Definition 2. Diese Mehrdeutigkeit lässt sich jedoch beseitigen.

Sind nämlich d und d' zwei ggT der Zahlen a und b, so besitzt d die Eigenschaft 2 und d' die Eigenschaft 1, so dass $d' \mid d$ gilt. Entsprechend gilt auch $d \mid d'$.
Daher sind $\alpha = \frac{d}{d'}$ und $\frac{d}{d'} = \frac{1}{d/d'} = \frac{1}{\alpha}$ ganze Zahlen. Die einzigen ganzen Zahlen, deren Kehrwert ebenfalls eine ganze Zahl ist, sind aber die Zahlen 1 und -1. Daher ist $\alpha = 1$ oder $\alpha = -1$, also $d' = d$ oder $d' = -d$.
Wenn man daher in die Definition eines ggT die Bedingung aufnimmt, dass diese Zahl positiv ist (was manchmal zweckmäßig ist), dann kann man sagen, dass der ggT zweier von null verschiedener ganzer Zahlen existiert und eindeutig bestimmt ist.

Im folgenden bezeichnen wir den ggT zweier von null verschiedener ganzer Zahlen a und b, wie in der Zahlentheorie üblich, mit (a, b).

Nun betrachten wir Paare teilerfremder von null verschiedener ganzer Zahlen; diesem Begriff waren wir schon begegnet.

Definition 3. Ganze Zahlen $a \neq 0$ und $b \neq 0$ werden teilerfremd genannt, wenn ihr ggT gleich 1 ist.

Mit anderen Worten, teilerfremde ganze Zahlen sind solche, deren einzige gemeinsame Teiler die Zahlen 1 und -1 sind.
Für $(a, b) = 1$ ergibt sich aus Satz 3, dass 1 in der Gestalt

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

mit ganzzahligen s und t dargestellt werden kann. Umgekehrt, wenn die Identität (3) für passende s und t erfüllt ist, sind a und b teilerfremd.
Denn (siehe den Beweis von Satz 1) die ganze Zahl $d = (a, b)$ ist die dem absoluten Betrage nach kleinste Zahl unter den von null verschiedenen ganzen Zahlen der Gestalt $xa + yb$. Daher gilt, wenn (3) erfüllt ist, $|d| \leq 1$ und $d \neq 0$, also $d = \pm 1$.

Hieraus folgt sofort die wichtigste Eigenschaft teilerfremder ganzer Zahlen:

Satz 4. Gilt $a \mid bc$ und $(a, b) = 1$, so gilt $a \mid c$. In Worten: Geht die ganze Zahl a in dem Produkt zweier ganzer Zahlen auf und ist a zu einem der Faktoren teilerfremd, so ist a ein Teiler des anderen Faktors.

Beweis. Wegen $(a, b) = 1$ existieren zwei ganze Zahlen s und t mit

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

Durch Multiplikation mit c ergibt sich hieraus $c = (sc)a + t(bc)$. Da beide Summanden rechts durch a teilbar sind, ist c durch a teilbar.

Satz 5. Wenn die ganze Zahl a zu den ganzen Zahlen b und c teilerfremd ist, dann ist sie auch zu dem Produkt bc teilerfremd.

Beweis. Wegen $(a, b) = 1$ können wir ganze Zahlen s und t finden, die der Gleichung $1 = sa + tb$ genügen, und wegen $(a, c) = 1$ ist auch

$$1 = ua + vc$$

für geeignet gewählte ganze Zahlen u und v. Multiplizieren wir diese Gleichungen miteinander, so erhalten wir

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

Setzen wir $m = sua + svc + tbu$ und $n = tv$, so sind m und n ganze Zahlen, und es ist $1 = ma + n(bc)$, also sind a und bc zueinander teilerfremd.

Die Aussage dieses Satzes lässt sich leicht auf beliebig viele Faktoren verallgemeinern.

Satz 6. Wenn die ganze Zahl a zu den ganzen Zahlen $b_1, b_2, ..., b_k$ teilerfremd ist, dann ist sie auch zu dem Produkt $b_1 \cdot b2 \cdot ... \cdot b_k$ teilerfremd.

Diesen Satz beweist man durch vollständige Induktion nach der Anzahl k der Faktoren.

1.2 Der Hauptsatz der elementaren Zahlentheorie

Satz. Jede von null verschiedene ganze Zahl lässt sich als Produkt von Primzahlen darstellen, wobei die Darstellung bis auf die Reihenfolge und das Vorzeichen der Faktoren eindeutig bestimmt ist.

Beweis. Existenz einer Zerlegung einer ganzen Zahl in ein Produkt von Primzahlen. Wir beschränken uns zunächst auf den Fall positiver ganzer Zahlen.

Bemerkung. Die Zahl 1 wird aus mehreren Gründen nicht zu den Primzahlen gerechnet, obwohl sie nicht in ein Produkt kleinerer Zahlen zerlegt werden kann. So erhebt sich die Frage: In welchem Sinne ist der obige Satz für die Zahl 1 wahr? Oder, anders, in welchem Sinne ist 1 als Produkt von Primzahlen darstellbar!

Wir nehmen an, $1 = 1$ sei die Zerlegung der Zahl 1 in ein Produkt von Primzahlen,

wobei die Anzahl der Primfaktoren auf der rechten Seite 0 ist. Diese Vereinbarung erinnert an die Definition der 0-ten Potenz $a^0 = 1$ (die Anzahl der Faktoren ist null). Eine analoge Vereinbarung treffen wir für die Zahl -1.

Wir wenden vollständige Induktion an:

a) Für $n = 1$ ist $1 = 1$ die gesuchte Darstellung, die Zahl 1 ist in ein Produkt einer leeren Menge von Primzahlen zerlegbar.

b) Wir nehmen an, für alle positiven ganzen Zahlen m, die kleiner als n sind, sei die Darstellbarkeit als Produkt von Primzahlen schon bewiesen, und beweisen dann, dass auch die Zahl n in dieser Weise zerlegbar ist. Wenn n eine Primzahl ist, ist

$$n = n$$

die gesuchte Zerlegung (in einen einzigen Primfaktor).
Ist n eine zusammengesetzte Zahl, so ist sie ein Produkt $n = n_1 \cdot n_2$ zweier ganzer Zahlen n_1 und n_2 von denen jede von 1 und von n verschieden ist, so dass $n_1 < n$ und $n_2 < n$ gilt. Nach der Induktionsannahme sind dann aber die Zahlen n_1 und n_2 als Primzahlprodukte darstellbar:

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

wobei die p_i und die q_i Primzahlen sind. Dann ist jedoch

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

also n in ein Produkt von Primzahlen zerlegbar.

Ist n eine negative ganze Zahl, so ist $-n$ eine positive ganze Zahl. Wie wir bewiesen haben, ist $-n$ als Primzahlprodukt darstellbar. Es sei

$$-n = p_1 \cdot p_2 \cdot ... \cdot p_t$$

Dann ist

$$n = -(1) \cdot p_1 \cdot p_2 \cdot ... \cdot p_t$$

eine Zerlegung von n in ein Primzahlprodukt. Damit ist der erste Teil des Satzes bewiesen.

Bemerkung. Für die Eindeutigkeit der Primzahlzerlegung existieren ziemlich viele Beweise. Der Beweis, den wir hier führen, ist nicht der kürzeste und nicht der einfachste. Er hat aber den Vorzug, dass er unmittelbar auf eine Reihe anderer Bereiche übertragen werden kann, beispielsweise auf den Bereich der Polynome in einer Veränderlichen und auf den Bereich der ganzen komplexen Zahlen (der sogenannten Gaußschen ganzen Zahlen).

Beweis der Eindeutigkeit der Zerlegung einer von null verschiedenen ganzen Zahl in ein Produkt von Primfaktoren. Wir weisen daraufhin, dass nach Definition einer Primzahl zwei verschiedene Primzahlen zueinander teilerfremd sind. Den Beweis der Eindeutigkeit der Primzahlzerlegung von n führen wir durch vollständige Induktion nach dem

absoluten Betrag der Zahl n.

a) Ist $|n| = 1$, so ist $n = \pm 1$ und $1 = 1$, $-1 = -1$; daher ist die Zerlegung der Zahlen 1 und -1 in Primzahlen eindeutig.

b) Wir nehmen an, die zu beweisende Eigenschaft (d.h. die Eindeutigkeit der Primzahlzerlegung) sei für alle ganzen 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 die Primfaktoren $p_1, p_2, ..., p_k$ bzw. $q_1, q_2, ..., q_l$. Wir behaupten, dass die Primzahl p_k oder $-p_k$ unter den Primzahlen $_1, ..., q_l$ vorkommt. Anderenfalls wäre $p_k \neq q_i$, $i = 1, 2, ..., l$, und p_k wäre zu allen Primzahlen q_i teilerfremd, nach Satz 6 also auch zu ihrem Produkt, d.h. zu n.

Es gilt aber $p_k \mid n$, also $(p_k, n) = p_k$. Somit ist p_k gleich einer der Primzahlen $\pm q_i$. Durch Vertauschen der Faktoren q_i können wir erreichen, 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 $(i \neq l)$.
Daher erhalten wir

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

und hieraus

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

Nun ist aber $|m| < |n|$ und nach Induktionsannahme ist die Eindeutigkeit der Primzahlzerlegung für m schon bewiesen. Daher ist $k - 1 = l - 1$.
Die Folgen $p_1, p_2, ..., p_{k-1}$ und $q_1, q_2, ..., q_{l-1}$ enthalten bis aufs Vorzeichen ein und dieselben Primzahlen, und entsprechende Primzahlen kommen in beiden Darstellungen gleich oft vor, da aber $p_k = q_l$ ist, gilt dies 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 der Satz bewiesen.

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

In Satz 2 haben wir gezeigt, dass zwei von null verschiedene 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:

$$a = q_1 \cdot b + r_1, \qquad 0 \leq r_1 < |b| \tag{1}$$

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:

$$b = q_2 \cdot r_1 + r_2, \qquad 0 \leq r_2 < r_1 \tag{2}$$

Ist $r_2 \neq 0$, so folgt

Dritter Schritt.

$$r_1 = q_3 \cdot r_2 + r_3, \qquad 0 \leq r_3 < r_2 \tag{3}$$

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

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

ergibt sich etwa nach dem k-ten Schritt ($k < |b|$) 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 ..., $r_{k-1} \mid r_2$, $r_{k-1} \mid r_1$, $r_{k-1} \mid b$, $r_{k-1} \mid a$. 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} der ggT der Zahlen a und b.

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

$$\begin{aligned} 858 &= 3 \cdot 253 + 99, && (1)\\ 253 &= 2 \cdot 99 + 55, && (2)\\ 99 &= 1 \cdot 55 + 44, && (3)\\ 55 &= 1 \cdot 44 + 11, && (4)\\ 44 &= 4 \cdot 11 && (5) \end{aligned}$$

daher ist $(858, 253) = 11$.
Mit Hilfe des Euklidischen Algorithmus findet man also den ggT zweier von null verschiedener ganzer 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 erläutern.

Wir sollen also solche ganzen Zahlen s und t finden, für welche

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

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

$$\begin{aligned} 11 &= 55 + (-1) \cdot 44, \\ 44 &= 99 + (-1) \cdot 55, \\ 55 &= 253 + (-2) \cdot 99, \\ 99 &= 858 + (-3) \cdot 253. \end{aligned}$$

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 $s = -5$, $t = 17$.
Die Gleichungen, die bei der Anwendung des Euklidischen Algorithmus zur Berechnung des ggT der Zahlen a und b entstehen, ermöglichen es, Gleichungen der Gestalt $d = xa + yb$ (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" weist darauf hin, dass die Koeffizienten der Gleichung ganze Zahlen und die gesuchten Lösungen ganzzahlig sind.

Bemerkung. 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. Der interessierte Leser sei auf das Bändchen I.G. Basmakova, Diophant und diophantische Gleichungen, verwiesen.

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 sei jedoch bemerkt, dass nicht alle Gleichungen dieser Gestalt eine Lösung haben.
Hat nämlich die Gleichung (I) eine Lösung in ganzen Zahlen, etwa $x = x_0$, $y = y_0$, also $c = x_0a + y_0b$ 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) mit $a \neq 0$, $b \neq 0$ 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 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

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

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

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

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 ganze Zahlen sind. Wenn wir nun in der Gleichung (III) durch d kürzen, geht sie in die Gleichung

$$a'(x_0 - x_1) = b'(y_1 - y_0)$$

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

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k \qquad , \qquad x_1 = x_0 - b'k = x_0 - \frac{b}{d}k \qquad \text{(IV,V)}$$

wobei k eine beliebige ganze Zahl ist. Umgekehrt sieht man leicht ein:
Ist x_0, y_0 eine ganzzahlige Lösung der Gleichung (I), so sind alle Paare von ganzen Zahlen (IV), (V), wobei k alle ganzen Zahlen durchläuft, 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 ganzzahlige Lösung der Gleichung (I), so sind auch alle ganzen Zahlen der Gestalt $x_0 - \frac{b}{d}k$, $y_0 + \frac{a}{d}k$ Lösungen von (I) (da k beliebig ist, ergeben sich also aus einer Lösung unendlich viele Lösungen), und andere Lösungen gibt es nicht.

1.4 Pythagoreische Tripel

Die Methode, nach der wir die Lösungen einer linearen diophantischen Gleichung in zwei Unbekannten gefunden haben, und die allgemeine Form, in der wir diese Lösungen angegeben haben, wenden wir nun zur Lösung des folgenden klassischen Problems an:

Man bestimme alle Tripel ganzer Zahlen a, b, c für welche

$$a^2 + b^2 = c^2 \qquad (1)$$

gilt.

Ein solches Zahlentripel wird pythagoreisch genannt, weil zu je drei von 0 verschiedenen Zahlen a, b, c, welche der Bedingung (1) genügen, stets ein, und zwar genau ein, rechtwinkliges Dreieck mit den Seitenlängen a, b, c existiert.

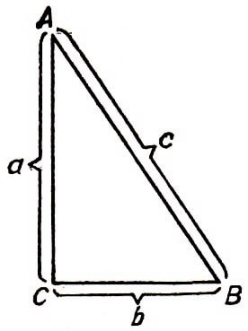


Abb. 1

Trägt man nämlich Strecken der Länge a und b auf den Schenkeln eines rechten Winkels ab, wie dies Abbildung 1 zeigt, und verbindet man ihre Endpunkte A und B durch eine gerade Linie, so gilt nach dem Satz des Pythagoras $AB^2 = a^2 + b^2 = c^2$, also $AB = c$.

Dass das Dreieck ABC bei gegebenen a, b, c eindeutig bestimmt ist, ergibt sich aus dem Satz, dass Dreiecke kongruent sind, wenn sie in den drei Seiten übereinstimmen. Nun beschäftigen wir uns mit pythagoreischen Tripeln $\{a, b, c\}$, das sind ganze Zahlen a, b, c, die der Gleichung (1) genügen.

Ist $c = 0$, so muss $a = b = 0$ gelten. Daher brauchen wir nur den Fall $c \neq 0$ zu untersuchen. Dann ergibt sich aus (1)

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \tag{2}$$

Nun setzen wir $\frac{a}{c} = x$ und $\frac{b}{c} = y$, so dass (2) die Gestalt

$$x^2 + y^2 = 1 \tag{3}$$

annimmt. Wenn es uns gelingt, alle rationalen (nicht nur die ganzzahligen) Lösungen der Gleichung (3) zu finden, haben wir damit die Lösung des Problems der pythagoreischen Tripel erhalten. Ist nämlich $\{x, y\}$ eine Lösung der Gleichung (3), so ist jedes Tripel $\{\alpha x, \alpha y, \alpha\}$ mit von 0 verschiedenem ganzzahligem α, für welches x und y ganzzahlig werden, ein pythagoreisches Tripel:
Die Identität $\alpha^2 x^2 + \alpha^2 y^2 = \alpha^2$ ergibt sich aus (3) durch Multiplikation mit α^2. Daher betrachten wir sämtliche rationalen Lösungen der Gleichung (3).
Zunächst ist diese Gleichung mit der folgenden äquivalent:

$$x^2 = 1 - y^2 \tag{3'}$$

Nimmt man aus der Menge aller Lösungen dieser Gleichung die Lösungen $x = 0$, $y = \pm 1$ heraus, so bilden alle verbleibenden Lösungen die Menge der Lösungen der Gleichung

$$\frac{x}{1-y} = \frac{1+y}{x} \tag{4}$$

Nun setzen wir

$$\frac{x}{1-y} = u \quad , \quad \frac{1+y}{x} = v \tag{5}$$

Die Zahlen u und v sind offenbar ebenfalls rationale Zahlen, wenn x und y rationale Zahlen sind, und x und y ergeben sich aus u und v gemäß

$$x = \frac{2u}{uv+1} \qquad , \qquad y = \frac{uv-1}{uv+1} \tag{6}$$

Dass die Gleichungen (6) gelten, kann der Leser leicht verifizieren, indem er das System (5) nach x und y auflöst. Mit Hilfe von (6) lässt sich (4) in der Form

$$u = v \tag{7}$$

schreiben. Ist $\{x = x_0, y = y_0\}$ eine Lösung der Gleichung (4), so ist

$$\left\{u_0 = \frac{x_0}{1-y_0}, v_0 = \frac{1+y_0}{x_0}\right\}$$

eine Lösung der Gleichung(7),und umgekehrt, ist $\{u_0, v_0\}$ eine Lösung der Gleichung (7), so ist (vgl. die Formeln (6))

$$\left\{x_0 = \frac{2v_0}{u_0v_0+1}, y_0 = \frac{u_0v_0-1}{u_0v_0+1}\right\}$$

eine Lösung der Gleichung (4)
Nun ergeben sich alle Lösungen der Gleichung (7) folgendermaßen:

Man muss für u und v dieselben rationalen Zahlen wählen. Daher werden alle Lösungen der Gleichung (4) durch die Formeln (6) geliefert, wenn $u = v = t$ gesetzt wird, wobei t eine beliebige rationale Zahl ist:

$$x = \frac{2t}{t^2+1} \qquad , \qquad y = \frac{t^2-1}{t^2+1} \tag{8}$$

Es sei $t = \frac{m}{n}$ ein unkürzbarer Bruch (also $(m, n) = 1$). Dann nimmt das System (8) folgende Gestalt an:

$$x = \frac{2mn}{m^2+n^2} \qquad , \qquad y = \frac{m^2-n^2}{m^2+n^2} \tag{9}$$

Dies sind sämtliche rationalen Zahlen x und y, die der Gleichung (3') genügen. Lassen wir m und n beliebige ganzzahlige Werte annehmen, außer $m = n = 0$, so erhalten wir Lösungen der Gleichung (3'). Für $m = 0$, $n = 1$ erhalten wir die Lösung $\{x = 0, y = -1\}$ und für $m = 1$, $n = 0$ die Lösung $\{x = 0, y = 1\}$.
Beide Lösungen mussten wir zunächst ausschließen, da anderenfalls die Gleichungen (3') und (4) nicht äquivalent sind. Nachträglich stellen wir fest, dass die Formeln (9) auch diese Lösung der Gleichung (3') liefern. Somit ist für alle ganzzahligen m und n, von $m = n = 0$ abgesehen, das Zahlentripel

$$\{2mn, m^2-n^2, m^2+n^2\} \tag{10}$$

ein pythagoreisches Tripel. Überdies ist, wie schon gesagt, auch jedes Tripel ganzer Zahlen

$$2\alpha mn, \qquad \alpha(m^2-n^2), \qquad \alpha(m^2+n^2) \tag{11}$$

wobei α eine beliebige zulässige rationale Zahl bedeutet (insbesondere auch $\alpha = 0$), ein pythagoreisches Tripel. Wir erinnern daran, dass wir von der Gleichung (1) ausgegangen sind, dann nacheinander von (1) über die Gleichungen (2)-(8) zu (9), also zur Formel

$$\frac{a}{c} = \frac{2mn}{m^2+n^2} \qquad , \qquad \frac{b}{c} = \frac{m^2-n^2}{m^2+n^2} \tag{9'}$$

gelangt sind.
Nun setzen wir $a = 2mn\rho_1$, $b = (m^2-n^2)\rho_2$, $c = (m^2+n^2)\alpha$, für irgendwelche rationalen Zahlen ρ_1, ρ_2, α. Dann folgt aus der ersten Formel von (9') die Beziehung $\rho_1/\alpha = 1$ und aus der zweiten $\rho_2/\alpha = 1$, also (10').

Es muss noch geklärt werden, wie in (10') der Nenner der rationalen Zahl beschaffen sein muss, damit die Zahlen in (10') ganze Zahlen sind. Da die Zahl $2mn\alpha$ eine ganze Zahl sein soll, können die Teiler dieses Nenners nur Teiler der Zahlen m, n und 2 sein. Andererseits müssen, da $(m^2-n^2)\alpha$ eine ganze Zahl sein soll, die Teiler des Nenners von α Teiler der Zahl m^2-n^2 sein; weil aber unter diesen wegen $(m,n) = 1$ keine Teiler von m und n vorkommen, ist α entweder eine ganze Zahl oder eine rationale Zahl mit dem Nenner 2. In diesem Fall müssen die Zahlen m und n beide ungerade sein.
Damit haben wir folgenden Satz bewiesen:

Satz. Ein Tripel $\{a,b,c\}$ ganzer Zahlen ist genau dann pythagoreisch, wenn es die Gestalt $\{2\alpha mn, \alpha(m^2-n^2), \alpha(m^2+n^2)\}$ hat, wobei m und n teilerfremde Zahlen sind und α eine beliebige ganze Zahl ist; sind m und n ungerade, so braucht α nicht ganzzahlig zu sein, sondern darf eine Zahl der Gestalt $k/2$ sein, wobei k eine beliebige ungerade ganze Zahl ist.

Setzen wir beispielsweise $m = 2$, $n = 1$, $\alpha = 1$, so erhalten wir das pythagoreische Tripel $\{4,3,5\}$; für dieselben m und n ergeben sich für $\alpha = 3$ und $\alpha = 5$ die pythagoreischen Tripel $\{12,9,15\}$ und $\{20,15,25\}$.

Im alten Ägypten wurden pythagoreische Tripel zur Konstruktion rechter Winkel benutzt. Sind die Zahlen a,b,c durch die Beziehung (1) verknüpft, so ist das Dreieck mit den Seitenlängen a,b,c rechtwinklig.
Ein Dreieck lässt sich aus seinen drei Seiten leicht mit Zirkel und Lineal konstruieren: Um die Endpunkte von c werden mit den Radien a und b Bogen geschlagen, und deren Schnittpunkt wird mit den Endpunkten von c verbunden.
In der Praxis waren die Strecken a,b,c Stücke einer Schnur, deren Längen sich wie die Zahlen eines pythagoreischen Tripels verhielten, etwa wie 3:4:5.

Übungen

1. Man bestimme alle ganzen Zahlen zu mit der Eigenschaft, dass der Ausdruck $x^3 + 2x + 7$ bei Division durch 5 den Rest 2 liefert.

2. Es sei $m > 1$ eine natürliche Zahl und $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ ein Polynom mit den ganzzahligen Koeffizienten $a_0, a_1, ..., a_n$. Man beweise: Ist x ganzzahlig, so hängt der Rest bei der Division von $f(x)$ durch m nur davon ab, welchen Rest x bei Division durch m lässt.

3. Man beweise, dass $d = (a, b)$ und $-d$ die einzigen gemeinsamen Teiler von a und b sind, die als Linearkombination der Zahlen a und b darstellbar sind.

4. Man beweise, dass die Zahl der Schritte im Euklidischen Algorithmus beliebig groß sein kann.

5. Man bestimme $d = (a, b)$ und stelle d in der Gestalt $\alpha a + \beta b$ dar für $a = 127$, $b = 211$; $a = 111111$, $b = 111$; $a = 191$, $b = 291$.

6. Man beweise, dass $(a, b) = (a, a + b) = (a, a - b)$ gilt.

7. Man bestimme alle ganzzahligen Lösungen der Gleichungen
α) $2x + 3y = 5$;
β) $10x + 2y = 5$;
γ) $121x + 1331y = 11$.

8. Man beweise: Ist p Primzahl, so ist $\sqrt{p}$ irrational.

9. Man bestimme alle pythagoreischen Tripel $\{a, b, c\}$, für welche $|c| < 100$ ist.

2 Die Arithmetik der Gaußschen Zahlen

2.1 Gaußsche Zahlen und ganze Gaußsche Zahlen

Eine naheliegende 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 1. 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 kurz 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 wollen wir 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 $\gamma = \alpha/\beta$ eine Gaußsche Zahl ist.
Es ist nämlich

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

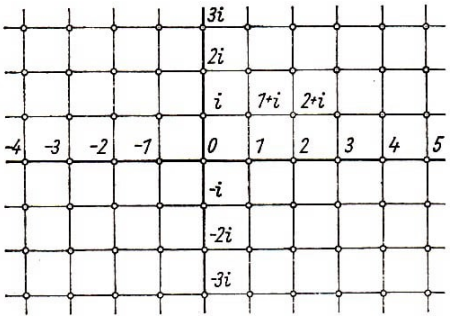
Die Zahlen $\frac{ac+bd}{c^2+d^2}$ und $\frac{bc-ad}{c^2+d^2}$ - Real- und Imaginärteil der Zahl γ - sind rationale Zahlen. Daher ist γ eine Gaußsche Zahl.

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. 2). Sie liegen auf den Eckpunkten eines Netzes von Quadraten der Kantenlänge 1, das die ganze komplexe Ebene bedeckt.

Abb. 2



Aus der Theorie der komplexen Zahlen benötigen wir die Begriffe Norm und Betrag einer komplexen Zahl. Als Norm der komplexen Zahl $\alpha = x + iy$ 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 auch 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.

Bemerkung. 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.

Nicht jede positive ganze Zahl ist Norm einer ganzen Gaußschen Zahl. Es gilt nämlich folgender Satz:

Satz 1. 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.
Ist umgekehrt $c = x^2 + y^2$, wobei x und y ganze rationale Zahlen sind, dann ist ebenso $c = N(x + yi)$, 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 $x^2 = 4m^2$ und $y^2 = 4(n^2+n)+1$, 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 übergeben 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 $N(\alpha)$ und $N(\beta)$ ganze rationale Zahlen sind, eine notwendige Bedingung dafür, dass β durch α teilbar ist.

Im Ring der ganzen rationalen Zahlen gibt es nur zwei Zahlen, welche Teiler aller ganzen Zahlen sind, nämlich $+1$ und -1. Im Ring der ganzen Gaußschen Zahlen hat man vier solche Zahlen, nämlich $+1$, -1, $+$i, -i. Man sieht leicht, dass die vier genannten Zahlen wirklich diese Eigenschaft haben. Es ist nämlich

$$\alpha = \alpha \cdot 1, \qquad \alpha = (-\alpha) \cdot (-1), \qquad \alpha = (\alpha i) \cdot i, \qquad \alpha = (\alpha i) \cdot (-i)$$

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 nennt man solche Zahlen Teiler der Einheit oder einfach 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 offensichtlich, 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 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 2. Eine von null verschiedene 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 ganze Gaußsche 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 α_i nicht notwendig voneinander verschiedene Primzahlen. Eine solche Zerlegung ist im folgenden 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_j, so haben beide Zerlegungen die gleiche Anzahl von Faktoren, $k = l$, und die Zerlegungen (4) und (5) unterscheiden sich höchstem 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: Ist etwa

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

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

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

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_1, π_2, π_3 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 besagt, 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.

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

Definition 3. Zwei ganze Gaußsche Zahlen heißen assoziiert, wenn sie sich um eine Einheit als Faktor 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 $(i = 1, 2, ..., k)$ 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_l zu der entsprechenden Primzahl π_j assoziiert ist.

Wir wollen den Beweis des Hauptsatzes skizzieren. Er wird fast genauso geführt, wie der Beweis der entsprechenden Behauptung für ganze rationale Zahlen. Aus diesem Grunde werden 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 $\alpha = 1, -1, i, -1$; die Zahl α ist in ein Produkt einer leeren Menge von Primzahlen zerlegbar.

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

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 $\rho = \pi_1 \cdot \pi_2 \cdot ... \cdot \pi_k$ und $\tau = \sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_l$. Dann ist aber

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

eine Zerlegung für α.

Den Beweis der Behauptung über die Eindeutigkeit kann man mit Hilfe von Eigenschaften führen, die im Ring der ganzen Gaußschen Zahlen für den größten gemeinsamen Teiler und für teilerfremde Zahlen gelten. Der Schlüssel des Beweises ist die Tatsache, dass auch im Ring 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 stets ganze Gaußsche Zahlen γ und ρ, wobei $N(\rho) < N(\beta)$ ist derart, dass

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

ist.

Bemerkung. Die Zahl γ wird Quotient, die Zahl ρ Rest bei der Division von α durch β genannt. In Satz 1 wurden diese Begriffe für die ganzen rationalen Zahlen eingeführt; dabei musste der Rest nichtnegativ sein ($r \geq 0$).
Diese Forderung ist aber nicht wesentlich. Sieht man von ihr ab und verlangt nur $|r| < |b|$, so ist die Definition des Quotienten bzw. des Restes bei Gaußschen Zahlen eine naheliegende Verallgemeinerung der Definition bei ganzen rationalen Zahlen.

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. 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.

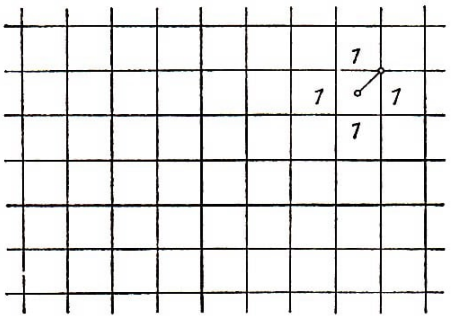


Abb. 3

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. 3).
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 $\tau = \alpha/\beta$ 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 von null verschiedener ganzer Gaußscher Zahlen α, β, indem man für die Zahl $\delta \neq 0$ mit kleinster Norm aus der Menge der Zahlen der Gestalt $\alpha\xi + \beta\eta$ (ξ 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.

2.2 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.

Bemerkung. 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 $5=(2+i)\cdot(2-i)$.

Beweis. Wegen $N(\alpha)=\alpha\cdot\overline{\alpha}$ teilt jede ganze Gaußsche Zahl ihre Norm.
Es sei jetzt π eine Gaußsche Primzahl, dann gilt $\pi|N(\pi)$. Wir nehmen an, $N(\pi)=p_1\cdot\cdot p_2...p_r$ sei eine Zerlegung der Zahl $N(\pi)$ in ein Produkt rationaler Primzahlen; dann gilt also $\pi \mid p_1\cdot p_2...p_r$; folglich teilt pi 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 1 bewiesen.

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

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

Der zweite Fall bedeutet, dass π Einheit ist und dass eine der Gleichungen $\pi=p$, $\pi=-p$, $\pi=ip$, $\pi=-pi$ 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 in Kap. III, § 3, beweisen.

Alle ungeraden rationalen Primzahlen, die nicht die Gestalt $4n + 1$, also die Gestalt $4n+3$ haben, bilden 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.
(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.)

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

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

Für die Normen ergibt sich

$$N(\alpha) = t = N(\sigma_1^{a_1})...N(\sigma_l^{a_l}) \cdot N(\rho_1^{b_1})...N(\rho_s^{b_s}) = p_1^{a_1}...p_l^{a_l} \cdot q_1^{2b_1}...q_s^{2b_s} \tag{8}$$

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 $4n+3$ und $a_1, ..., a_l, b_1, ..., b_s$ ganze nicht negative Zahlen sind.

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

$$\alpha = \sigma_1^{a_1} ... \sigma_l^{a_l} \cdot \rho_1^{b_1} ... \rho_s^{b_s}$$

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 2. 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.

Bemerkung. 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.

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. 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: Nicht in allen den Gaußschen Zahlen ähnlichen Arithmetiken gilt der Satz von der Eindeutigkeit der Zerlegung einer Zahl in ein Produkt von Primzahlen. Wir geben ein Beispiel einer solchen "Arithmetik".

Wir betrachten komplexe Zahlen der Gestalt

$$\alpha = x + y\sqrt{-5} \tag{9}$$

wobei x und y ganze rationale Zahlen sind. Es ist leicht zu sehen, dass Summe, Differenz und Produkt von Zahlen der Gestalt (9) wieder von dieser Gestalt sind.
Wir wollen die Menge aller Zahlen der Gestalt (9) 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 (9) 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 jedoch $N(\xi \cdot \eta) = N(\xi)N(\eta)$ gilt, ist $N(\alpha)|N(\beta)$ eine notwendige (doch im allgemeinen nicht hinreichende) Bedingung dafür, dass β durch α teilbar ist.

Analog wie im Fall der ganzen Gaußschen Zahlen lassen sich die Begriffe Einheit und Primzahl auf Γ übertragen. 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

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

in Γ Primzahlen sind. Es ist nämlich

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

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

$$x^2 + 5y^2 = 2 \qquad \text{und} \qquad x^2 + 5y^2 = 3$$

keine ganzzahligen Lösungen haben.
Die betrachteten vier Zahlen sind also Primzahlen in Γ. Nun gilt aber, wie man leicht sieht,

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

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 auftauchen, dass der Hauptsatz der elementaren Zahlentheorie in einigen wichtigen Zahlenbereichen nicht gilt, von Kummer selbst sowie von anderen bekannten Mathematikern, wie R. Dedekind, E. Solotrew, L. Kronecker und anderen erfolgreich überwunden. Es entstand eine umfangreiche neue Disziplin in der Mathematik, die Theorie der algebraischen

Zahlen.

Übungen

1. Man dividiere die ganze Gaußsche Zahl a durch die ganze Gaußsche Zahl b:
a) $a = 2 + 3i$, $b = 1 - i$; b) $a = 1 + i$, $b = 2 + i$.

2. Man zerlege die folgenden ganzen Gaußschen Zahlen in Primfaktoren:
a) $1 + i$; b) $2 + 5i$; c) 5; d) 10.

3. Lassen sich die folgenden ganzrationalen Zahlen als Summe von Quadraten ganzrationaler Zahlen darstellen?
a) 197; b) 1472; c) 111112.

4. Man beweise, dass für die komplexen Zahlen der Gestalt $a+b\sqrt{-2}$ mit ganzrationalen a und b der Hauptsatz der elementaren Zahlentheorie gilt.

5. Man beweise, dass im Ring der Zahlen der Gestalt $a + b\sqrt{-5}$ mit ganzrationalen a und b die Zahlen 7, $1 + 2\sqrt{-5}$ und $1 - \sqrt{-5}$ Primzahlen sind.

3 Endliche Arithmetiken

Mit ersten Anwendungen der Division mit Rest haben wir uns beim Beweis des Hauptsatzes der elementaren Zahlentheorie und der Auflösung einfacher diophantischer Gleichungen bekannt gemacht. Jetzt werden wir uns der wichtigsten Konstruktion zuwenden, die mit der Division ganzer Zahlen zusammenhängt, den Restklassen.

Der Grundgedanke ist der folgende. Bei der Division ganzer Zahlen durch eine natürliche Zahl $n \geq 1$ gibt es immer nur die n verschiedenen Reste $0, 1, 2, ..., n-1$. Daher kann man die unendliche Menge der ganzen Zahlen in endlich viele (in n) Teilmengen einteilen, die sämtlich jeweils diejenigen Zahlen enthalten, welche bei Division durch n denselben Rest lassen.

Diese Teilmengen werden Restklassen nach dem Modul n genannt. Es zeigt sich, dass man auf sie in natürlicher Weise die gewöhnlichen Grundrechenarten Multiplikation, Addition und Subtraktion übertragen kann. Dies führt zu einer neuen interessanten "Arithmetik", einer sogenannten endlichen Arithmetik.

3.1 Restklassen

Der Kürze halber vereinbaren wir, wenn nichts anderes gesagt wird, von jetzt an unter "Zahl" eine "ganze Zahl" zu verstehen. Die Menge dieser Zahlen ist ein Ring, der üblicherweise mit $\mathbb{Z}$ bezeichnet wird.

Definition 1. Es sei $n \geq 1$ eine ganze Zahl. Die Zahlen x und y heißen kongruent nach dem Modul n oder kongruent modulo n, in Zeichen

$$x \equiv y (\mathrm{mod}\, n) \qquad \text{oder} \qquad y \equiv x (\mathrm{mod}\, n)$$

wenn die Differenz $x - y$ durch n teilbar ist.
Sind x und y nicht kongruent modulo n, so schreiben wir

$$x \not\equiv y (\mathrm{mod}\, n) \qquad \text{oder} \qquad y \not\equiv x (\mathrm{mod}\, n)$$

Beispielsweise ist 12 $\equiv$ 15 (mod 3), da 12 - 15 = -3 durch 3 teilbar ist, und 21 $\not\equiv$ 10 (mod 5), da 21 - 10 = 11 nicht durch 5 teilbar ist.

Es sei $n = 3$. Wie sieht die Menge aller Zahlen aus $\mathbb{Z}$ aus, die zu 5 kongruent modulo 3 sind?
Zunächst gehört die Zahl 5 selbst zu dieser Menge denn es ist $5 \equiv 5 (\mathrm{mod}\, 3)$. Ferner ist, wenn $x \equiv 5 (\mathrm{mod}\, 3)$ gilt, $x - 5 = 3k$ für ein k aus $\mathbb{Z}$, also $x = 5 + 3k$.

Umgekehrt ist für jedes k aus $\mathbb{Z}$ die Zahl $x = 5 + 3k$ zu 5 modulo 3 kongruent, da zu $x - 5 = 3k$, also durch 3 teilbar ist. Lassen wir k in $x = 5 + 3k$ alle ganzen Zahlen durchlaufen, so erhalten wir die Menge aller Zahlen, die zu 5 kongruent modulo 3 sind. Diese Menge, die wir mit **5** bezeichnen, ist eine unendliche Menge.
Für $k = ..., -3, -2, -1, 0, 1, 2, 3, ...$ erhalten wir die Elemente

$$..., -4, -1, 2, 5, 8, 11, ...$$

Definition 2. Die Menge **X** aller derjenigen Zahlen aus $\mathbb{Z}$, die zu einer Zahl x modulo n kongruent sind, wird die Restklasse der Zahl x modulo n genannt und mit x (mod n) bezeichnet; bei bekanntem festen n schreiben wir auch **x** oder $\overline{x}$. Eine Zahl aus **X** wird ein Rest der Zahl x modulo n oder auch ein Repräsentant der Klasse **X** genannt.

So wurde im obigen Beispiel die Restklasse der Zahl 5 modulo 3 mit 5 (mod 3) bezeichnet. Offenbar ist 8 (mod 3) = 5 (mod 3), und allgemein ist die Restklasse **x** $= x(\mathrm{mod}\,3)$ jedes Repräsentanten x aus 5 (mod 3) gleich 5 (mod 3).

Satz 1. Es sei $x = qn + r$, $0 \leq r < n$. Dann gilt $x(\mathrm{mod}\,n) = r(\mathrm{mod}\,n)$.

Beweis. Jede Zahl z, die modulo n zu x kongruent ist, ist modulo n auch zu r kongruent; ist nämlich $z - x = kn$, so ist $z - r = z - x + qn = kn + qn = (k + q)n$.
Und umgekehrt, ist $z - r = kn$, so ist $z - x = r + kn - qn - r = (k - q)n$.

Der Rest r bei der Division einer Zahl x durch n wird kanonischer Repräsentant der Klasse **x**$(\mathrm{mod}\,n)$ genannt. Bei dem oben betrachteten Beispiel der Klasse **5**$(\mathrm{mod}\,3)$ ist daher 2 der kanonische Repräsentant.

Folgerung. Alle möglichen Restklassen modulo n sind

$$\mathbf{0}(\mathrm{mod}\,n), \mathbf{1}(\mathrm{mod}\,n), ..., \mathbf{(n\text{-}1)}(\mathrm{mod}\,n)$$

also **0**, **1**, ..., **n-1**.
Die Zahlen $0, 1, 2, ..., n-1$ bilden nämlich die Menge aller möglichen Reste bei Division durch n, so dass es keine anderen Restklassen als **0**, **1**, ... , **n-1** geben kann. Stimmen aber etwa einige dieser Klassen überein?

Wäre **a** $=$ **b**, wobei a und b verschiedene Reste bei Division durch n sind, so müsste für ein bestimmtes k die Gleichung $a - b = kn$ erfüllt sein, was für $k \neq 0$ unmöglich ist, da $|a - b| < n$, aber $|kn| \geq n$ gilt. Daher ist dann $a = b$, und alle Klassen **0**, **1**, **2**, ..., **n-1** sind tatsächlich verschieden.

Im folgenden bezeichnen wir die Menge der Restklassen modulo n mit Z_n.

Übungen

1. Man beweise: Gehört eine ganze Zahl a zwei Restklassen **X** modulo n and **Y** modulo n an, so ist **X** $=$ **Y**.

Hinweis: Man beachte, dass aus $x \equiv a(\mathrm{mod}\,n)$ and $y \equiv a(\mathrm{mod}\,n)$ die Beziehung $x \equiv y(\mathrm{mod}\,n)$, also **x**$(\mathrm{mod}\,n) =$ **y**$(\mathrm{mod}\,n)$ folgt.

2. Man beweise: Sind m und l natürliche Zahlen und ist $n = ml$, so besteht jede Restklasse modulo m aus l Restklassen modulo n.

3.2 Restklassenarithmetik

Bei der Untersuchung der Teilbarkeit der ganzrationalen und der ganzen Gaußschen Zahlen haben wir benutzt, dass diese Zahlbereiche einen Ring bilden, d.h., dass Summe, Differenz und Produkt je zweier Zahlen einer dieser Mengen wieder dieser Menge

angehören und dass diese Operationen bestimmten Gesetzen gehorchen, dem Kommutativgesetz, dem Assoziativgesetz und dem Distributivgesetz.
Die Ringeigenschaften der ganzen Zahlen bilden die Arithmetik der ganzen Zahlen.

Im vorhergehenden Paragraphen haben wir uns mit der Arithmetik der ganzen Gaußschen Zahlen bekannt gemacht. Jetzt führen wir arithmetische Operationen auf der Menge Z_n ein und lernen die Arithmetik der Restklassen kennen.

Definition 3. Unter der Summe der beiden Restklassen **x** und **y** modulo n verstehen wir die Restklasse **x + y**, in Zeichen

$$\mathbf{x} + \mathbf{y} = \mathbf{x} + \mathbf{y}$$

Dabei müssen wir uns über etwas klarwerden. Die Klassen **x** und **y** sind Mengen, sogar unendliche Mengen. Die Repräsentanten x und y, mit deren Hilfe wir die Summe **x** + **y** definiert haben, sind innerhalb ihrer Klassen mit allen übrigen Repräsentanten gleichberechtigt; wenn daher Definition 3 keinerlei Widersprüche enthalten soll, so muss folgendes gelten:

Wenn wir in **x** und **y** andere Repräsentanten, etwa x' und y' wählen, so müssen wir als Klasse **x' + y'** wieder dieselbe Klasse **x+y** erhalten, d. h., es muss die Identität **x' + y'** = **x+ y** erfüllt sein (wäre **x' + y'** $\neq$ **x + y**, so wäre die Definition nicht widerspruchsfrei: **x' + y'** $= x' + y' = x + y =$ **x + y**, entgegen **x' + y'** $\neq$ **x + y**).
Mit dem Nachweis, dass diese Identität wirklich besteht, ist bewiesen, dass die Definition der Summe korrekt ist.

Es seien also r_x und r_y die Reste bei der Division der Zahlen x bzw. y durch n. Dann besteht die Klasse **x+y** aus allen denjenigen Zahlen, die bei der Division durch n denselben Rest lassen wie $r_x + r_y$.
Andererseits besteht die Klasse **x'+ y'** aus denselben Zahlen, weil die Reste bei der Division der Zahlen x' und y' durch n ja r_x und r_y sind. Damit ist bewiesen, dass Definition 3 korrekt ist.

Wir betrachten einige Beispiele. Es sei $n = 2$. Dann gibt es nur die beiden Restklassen **0** und **1**. Ihre Addition ist sehr einfach:

$$\mathbf{0} + \mathbf{0} = \mathbf{0}, \qquad \mathbf{1} + \mathbf{0} = \mathbf{0} + \mathbf{1} = \mathbf{1}, \qquad \mathbf{1} + \mathbf{1} = \mathbf{0}$$

Zweckmäßigerweise schreibt man dies in Form einer Tabelle. Man hat sie folgendermaßen zu lesen. Angenommen, wir hätten die Summe **0** + **1** zu bestimmen.
In der linken Spalte suchen wir den ersten Summanden (also die **0**) auf, und in der oberen Zeile den zweiten (also die **1**). Im Schnittpunkt derjenigen Zeile, in der der erste Summand steht, und derjenigen Spalte, in der der zweite Summand steht, findet sich die Summe **1**. Wir nennen diese Tabelle die Additionstabelle für Z_2

Tabelle 1. Addition in Z_2

	0	1
0	0	1
1	1	0

Tabelle 2. Addition in Z_3

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Nun sei $n = 3$. Dann gibt es die Restklassen **0**, **1**, **2**. Tabelle 2 stellt die entsprechende Additionstabelle der.
Der Leser möge diese Tabelle sowie die folgenden Tabellen (nächste Seite) für $n = 7$ und $n = 10$ nachprüfen.

Somit wird die Addition von Restklassen in Z_n durch die Addition von Repräsentanten dieser Klassen definiert. Analog werden Subtraktion und Multiplikation definiert.

Definition 4. Unter der Differenz zweier Restklassen **x** und **y** modulo n verstehen wir die Restklasse **x-y**, in Zeichen

$$\mathbf{x} - \mathbf{y} = \mathbf{x} \text{ - } \mathbf{y}$$

Tabelle 1. Addition in Z_7

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabelle 2. Addition in Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Definition 5. Unter dem Produkt zweier Restklassen **x** und **y** modulo n verstehen wir die Klasse **xy**, in Zeichen

$$\mathbf{xy} = \mathbf{xy} \qquad \text{oder} \qquad \mathbf{x} \cdot \mathbf{y} = \mathbf{xy}$$

Der Leser hat sicherlich bemerkt, dass ebenso wie bei Definition 3 auch bei den Definitionen 4 und 5 geprüft werden muss, ob sie korrekt sind. Der Beweis der entsprechenden Identitäten, **x'** - **y'** = **x** - **y** und **x'y'** = **xy** ist nicht schwer.

Den ersten überlassen wir dem Leser als Übungsaufgabe, der zweite verläuft folgendermaßen: Es ist **x'** $= x + k_x n$ und **y'** $= y + k_y n$, mit ganzzahligen k_x und k_y. Dann ist $x'y' = xy + n(xk_y + yk_x + k_x k_y n)$. Daher ist

$$\mathbf{x'y'} = \mathbf{xy} (\mathrm{mod}\, n)$$

Die Additionstabellen (vgl. Tabelle 1 bis 4) eignen sich nicht nur zur Beschreibung der Addition, sondern auch zur Beschreibung der Subtraktion.
Das hängt mit folgender einfachen Beobachtung zusammen: Ist **a** = **b** - **c**, so ist **b** = **a** + **c**. Addieren wir nämlich auf beiden Seiten der Identität **a** = **b** - **c** die Klasse **c**, so erhalten wir

$$\mathbf{a} + \mathbf{c} = (\mathbf{b} - \mathbf{c}) + \mathbf{c}$$

Offenbar ist $\mathbf{b}-\mathbf{c} = \mathbf{b}+(-\mathbf{c})$ (und beide Seiten bezeichnen die Restklasse **b** -**c**$(\mathrm{mod}\, n)$). Daher ist $(\mathbf{b}-\mathbf{c})+\mathbf{c} = (\mathbf{b}+(-\mathbf{c}))+\mathbf{c}$. Für je drei Klassen **x**,**y**,**z** gilt aber das Assoziativgesetz

$$(\mathbf{x}+\mathbf{y})+\mathbf{z} = \mathbf{x}+(\mathbf{y}+\mathbf{z})$$

(jede der beiden Seiten der Identität bezeichnet die Restklasse **x + y + z**$(\mathrm{mod}\, n)$). Daher ist

$$(\mathbf{b}+(-\mathbf{c}))+\mathbf{c} = \mathbf{b}+(-\mathbf{c}+\mathbf{c}) = \mathbf{b}+0 = \mathbf{b} \qquad \text{also} \qquad \mathbf{a}+\mathbf{c} = \mathbf{b}$$

Um also in einer Additionstabelle die Differenz **a** - **b** zu finden, sucht man in der linken Spalte den Subtrahenden **b**, dann in der betreffenden Zeile der Tabelle den Minuenden **a**, und dann steht die Differenz **a** - **b** über der Spalte, in der **a** steht. So ergibt sich aus Tabelle 3 leicht, dass 4 (mod 7) - 6 (mod 7) = 5 (mod 7) ist, und aus Tabelle 4, dass 4 (mod 10) - 6 (mod 10) = 8 (mod 10) und 6 (mod 10) - 4 (mod 10) = 2 (mod 10) ist.

Auch für die Multiplikation in Z_n schreibt man zweckmäßigerweise Tabellen auf, die den Additionstabellen analog sind; hier steht natürlich an der Stelle, an der dort die Summe stand, das Produkt.

Tabelle 5. Multiplikation in Z_2

	0	1
0	0	0
1	0	1

Tabelle 6. Multiplikation in Z_3

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabelle 7. Multiplikation in Z_7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tabelle 8. Multiplikation in Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Restklassen in Z_n können also addiert, subtrahiert und multipliziert werden. Das Kommutativgesetz, das Assoziativgesetz und das Distributivgesetz, die bei der Addition und Multiplikation von Zahlen gelten, lassen sich auf Restklassen übertragen. Die Beweise der entsprechenden Gesetze überlassen wir dem Leser.
Die Menge Z_n mit den oben eingeführten Operationen Addition, Subtraktion und Multiplikation ist ein Ring, der sogenannte Restklassenring modulo n. Die Elemente 0 und

1 nennt man die Null und die Eins des Ringes Z_n.

Schließlich wenden wir uns der Division im Ring Z_n zu. Es sei $\mathbf{a} = a \pmod n$ und $\mathbf{b} = b \pmod n$; wir sagen, die Klasse **b** teile die Klasse **a**, in Zeichen $\mathbf{b}|\mathbf{a}$, wenn eine Klasse $\mathbf{c} = c \pmod n$ existiert derart, dass $\mathbf{a} = \mathbf{b} \cdot \mathbf{c}$ ist.
Ist beispielsweise $n = 10$ (vgl. Tab.8), so teilt die Klasse **2** die Klasse **4**, und die Klasse **4** teilt die Klasse **6**. Im Fall $\mathbf{b} \mid \mathbf{a}$ sagen wir auch, **b** sei ein Teiler der Klasse **a**.

Im Ring $\mathbb{Z}$ der ganzen Zahlen sind Teiler der Zahl 0 alle ganzen Zahlen x, da $x \cdot 0 = 0$ für jedes x gilt, und Teiler der Zahl 1 nur die Zahlen 1 und -1.
Natürlich teilen auch im Ring Z_n alle Klassen **x** die Klasse **0**, und die Klassen **1** und. **-1** teilen **1**. Im Unterschied zum Ring Z besitzt der Ring Z_n für gewisse n Eigenschaften, die $\mathbb{Z}$ nicht besitzt.

So ist beispielsweise im Ring $\mathbb{Z}$ die Gleichung $xy = 0$ nur dann erfüllt, wenn mindestens eine der Zahlen x oder y gleich 0 ist. Im Ring Z_n gilt aber $\mathbf{2} \cdot \mathbf{5} = \mathbf{0}$, obwohl weder $\mathbf{2} = \mathbf{0}$ noch $\mathbf{5} = \mathbf{0}$ gilt.
Ferner sind im Ring $\mathbb{Z}$ Teiler der Zahl 1 nur die Zahlen 1 und -1, während im Ring Z_n die Klasse **1** durch die vier Elemente **1**, **3**, **7**, **9** teilbar ist, weil $\mathbf{1} = \mathbf{1}\cdot\mathbf{1} = \mathbf{3}\cdot\mathbf{7} = \mathbf{7}\cdot\mathbf{3} = \mathbf{9}\cdot\mathbf{9}$ ist.

Schließlich gilt im Ring $\mathbb{Z}$ die sogenannte Kürzungsregel, d.h., aus $ax = ay$ und $a \neq 0$ folgt stets $x = y$, die nicht in jedem Restklassenring Z_n gilt. In Z_{10} folgt beispielsweise aus $\mathbf{2} \cdot \mathbf{7} = \mathbf{2} \cdot \mathbf{2}$ und $\mathbf{2} \neq \mathbf{0}$ keinesfalls $\mathbf{7} = \mathbf{2}$.

Wir beweisen nun den in diesem Zusammenhang grundlegenden Satz über den Ring Z_n. Zunächst führen wir zwei Begriffe ein:

Eine Klasse **x** des Ringes Z_n wird Nullteiler genannt, wenn $\mathbf{x} \neq \mathbf{0}$ ist und eine Klasse $\mathbf{y} \neq \mathbf{0}$ in Z_n existiert mit $\mathbf{xy} = \mathbf{0}$.

Eine Klasse **x** aus Z_n wird Teiler des Einselementes genannt, wenn eine Klasse **y** in Z_n existiert, für welche $\mathbf{x} \cdot \mathbf{y} = \mathbf{1}$ gilt. Teiler des Einselementes werden auch reziproke oder invertierbare Elemente genannt.

Satz 2. Eine Klasse **x** des Ringes Z_n ist genau dann ein Teiler des Einselementes, wenn die Zahlen x und y teilerfremd sind.
(2) Eine Klasse **x** des Ringes Z_n ist genau dann ein Teiler des Einselementes, wenn sie kein Nullteiler ist.

Es sei bemerkt, dass der ggT der ganzen Zahlen x und n nicht von der Wahl des Repräsentanten in der Klasse **x** abhängt. Ist nämlich $x' \equiv x \pmod n$, so ist $x' = x+kn$, und jeder (insbesondere der größte) gemeinsame Teiler von x und n ist gemeinsamer Teiler von x' und n.
Daher gilt $(x, n) \mid (x', n)$ und auch umgekehrt $(x', n) \mid (x, n)$. Somit ist die Formulierung von Satz 2 (Teil 1) korrekt.

Beweis (1). Es seien x und n teilerfremd. Nach Satz 3 von Kapitel I bedeutet dies, dass $xs + nt = 1$ für gewisse s und t aus $\mathbb{Z}$ gilt. Durch Übergang zu den Resten modulo n

erhalten wir dann

$$\mathbf{xs} + \mathbf{nt} = \mathbf{1} \qquad \text{oder} \qquad xs(\mathrm{mod}\, n) + nt(\mathrm{mod}\, n) \equiv 1(\mathrm{mod}\, n)$$

also $\mathbf{xs} = \mathbf{1}$, da $\mathbf{nt} = \mathbf{0t} = \mathbf{0}$ gilt. Somit ist **x** in Z_n Teiler des Einselelementes.
Gilt umgekehrt $\mathbf{xs} = \mathbf{1}$ in Z_n für eine Klasse **s**, so ist $xs - 1 = 0 \pmod{n}$, also $xs - 1 = k \cdot n$. Das heißt aber, dass x und n teilerfremd sind.

(2) Es sei **x** kein Nullteiler; wir betrachten den größten gemeinsamen Teiler d von x und n. Dann gilt

$$d = xs + nt$$

für gewisse s und t aus $\mathbb{Z}$, und es ist $n = d \cdot n'$. Ist $d = 1$, so ist nach dem oben Bewiesenen **x** ein Teiler des Einselementes in Z_n. Wäre aber $d \neq 1$, so wäre $\mathbf{n'} \neq \mathbf{0}$, und wegen $x = x' \cdot d$ würde

$$\mathbf{xn'} = \mathbf{x'd} \cdot \ \mathbf{n'} = \mathbf{x'} \cdot \mathbf{n} = \mathbf{0} \tag{1}$$

gelten, d.h., **x** wäre im Widerspruch zur Voraussetzung Nullteiler. Daher ist $\mathbf{d} = \mathbf{1}$ und **x** Teiler des Einselementes in Z_n.
Umgekehrt sei **x** ein Teiler des Einselementes in Z_n. Dann gibt es ein Element **y** aus Z_n mit $\mathbf{xy} = \mathbf{1}$. Wäre $\mathbf{xz} = \mathbf{0}$ für $\mathbf{z} \neq \mathbf{0}$, so würde aus dieser Gleichung $\mathbf{yzx} = \mathbf{y0} = \mathbf{0}$ folgen, also $(\mathbf{yx}) \cdot \mathbf{z} = \mathbf{0}$ oder $\mathbf{1} \cdot \mathbf{z} = \mathbf{0}$ im Widerspruch zu $\mathbf{z} \neq \mathbf{0}$. Daher ist $\mathbf{xz} \neq \mathbf{0}$, womit der Satz bewiesen ist.

Folgerung 1. Eine Klasse $\mathbf{x} \neq \mathbf{0}$ aus Z_n ist genau dann Nullteiler, wenn die Zahlen x und n nicht teilerfremd sind.

Folgerung 2. In einem Ring Z_n (für eine Primzahl p) gibt es keine Nullteiler.

Da nämlich jede der Zahlen $1, 2, ..., p-1$ zu p teilerfremd ist, wenn p eine Primzahl ist, sind die Klassen $\mathbf{1}, \mathbf{2}, ..., \mathbf{p\text{-}1}$ in Z_n Teiler des Einselementes von Z_p.

Zum Schluss dieses Abschnitts bringen wir noch zwei Sätze, welche sich aus den "ungewöhnlichen"Eigenschaften der endlichen Arithmetik ergeben.

Satz 3. Ist p eine Primzahl und $\mathbf{a} = a \pmod{p}$, $\mathbf{b} = b \pmod{p}$, so ist

$$(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$$

Beweis. Wir erinnern an die binomische Formel für beliebige ganze Zahlen x und y:

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y + ... + \binom{p}{k} x^{p-k}y^k + ... \binom{p}{p-1} xy^{p-1} + y^p$$

wobei bekanntlich für $k = 1, 2, ..., p-1$

$$\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{1 \cdot 2 \cdot ... \cdot k}$$

gilt.

Der Binomialkoeffizient $\binom{p}{k}$ ist für jedes k durch p teilbar, da p als Primzahl zu jeder der Zahlen $1, 2, ..., k$ für $k < p$ teilerfremd ist. Daher lässt sich die Differenz $(x+y)^p - x^p - y^p$ als Summe von Zahlen darstellen, von denen jede durch p teilbar ist.
Somit ist $(x + y)^p \equiv (x^p + y^p)$ (mod p), so dass wir für $x = a$ und $y = b$ tatsächlich die Beziehung

$$(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$$

erhalten.
Nicht weniger interessant ist folgender Satz, der unter dem Namen kleiner Fermatscher Satz bekannt ist:

Satz 4. Ist p eine Primzahl und $\mathbf{x} = x$ (mod p), so ist $\mathbf{x}^p = x$.

Beweis. Ist $\mathbf{x} = 0$, so ist nichts zu beweisen. Es sei also $\mathbf{x} \neq \mathbf{0}$. Das bedeutet, dass die Zahl x nicht durch p teilbar ist. Da p Primzahl ist, sind x und p teilerfremd. Daher sind die Klassen $\mathbf{x}, \mathbf{2x}, ..., \mathbf{(p\text{-}1)x}$ paarweise verschieden; denn $\mathbf{lx} = \mathbf{kx}$ würde bedeuten, dass $\mathbf{l} = \mathbf{k}$ ist (nach Satz 2 dieses Kapitels ist das Element $\mathbf{x}$ ein Teiler des Einselementes, und wenn $\mathbf{xy} = \mathbf{1}$ ist, erhalten wir durch Multiplikation der Gleichung $\mathbf{lx} = \mathbf{kx}$ mit $\mathbf{y}$ die Beziehung $\mathbf{l} = \mathbf{k}$).

Dies ist aber nicht möglich, wenn $0 < l$, $k < p$ und $l \neq k$ ist. Somit sind die Klassen $\mathbf{x}, \mathbf{2x}, ..., \mathbf{(p\text{-}1)x}$ nichts anderes als die Klassen $\mathbf{1}, \mathbf{2}, ..., \mathbf{(p\text{-}1)}$, wenn auch eventuell in anderer Reihenfolge, so dass die Produkte $\mathbf{x} \cdot \mathbf{2x} ... \mathbf{(p\text{-}1)x}$ und $\mathbf{1} \cdot \mathbf{2} ... \mathbf{(p\text{-}1)}$ übereinstimmen müssen.
Daher ist $\mathbf{1} \cdot \mathbf{2} ... \mathbf{(p\text{-}1)}\mathbf{x}^{p-1} = \mathbf{1} \cdot \mathbf{2} ... \mathbf{(p\text{-}1)}$. Kürzen wir durch $\mathbf{1} \cdot \mathbf{2} ... \mathbf{(p\text{-}1)}$, so ergibt sich $\mathbf{x}^{p-1} = \mathbf{1}$, durch Multiplikation mit x also $\mathbf{x}^p = \mathbf{x}$, und der Satz ist bewiesen.

Die Menge der von $\mathbf{0}$ verschiedenen Restklassen $\mathbf{1}$, $\mathbf{2}$, ..., $\mathbf{p\text{-}1}$ nach einem Primzahlmodul p besitzt viele interessante Eigenschaften. Eine davon ist folgende:

Unter diesen Klassen gibt es immer eine solche Klasse $\mathbf{a}$ derart, dass jede andere Klasse eine Potenz von ihr ist, d.h., zu jeder Klasse x existiert eine natürliche Zahl t mit $\mathbf{a}^t = \mathbf{x}$.

Übungen

1. Anhand von Tabelle 7 bestimme man zu jedem $\mathbf{x}$ aus Z_n eine reziproke Klasse, d.h. ein $\mathbf{y}$ mit $\mathbf{xy} = \mathbf{1}$.

2. Man beweise: Ist eine Klasse $\mathbf{x}$ des Ringes Z_n ein Teiler des Einselementes, so existiert genau eine Klasse $\mathbf{y}$, für welche $\mathbf{xy} = \mathbf{1}$ ist. (Man nehme das Gegenteil an, dass eine Gleichung $\mathbf{1} = \mathbf{xy}_1 = \mathbf{xy}_2$ existiere, und multipliziere dann die letzte mit $\mathbf{y}_1$ bzw. mit $\mathbf{y}_2$.)

3. Man beweise, dass man durch ein Element $\mathbf{a} \neq \mathbf{0}$ des Ringes Z_n genau dann kürzen kann (d.h., dass aus $\mathbf{ax} = \mathbf{ay}$ die Beziehung $\mathbf{x} = \mathbf{y}$ folgt), wenn $\mathbf{a}$ ein Teiler des Einselementes ist.

Hinweis. Dass die Bedingung hinreichend ist, ist fast trivial; dass sie notwendig ist, beweise man indirekt: Ist $\mathbf{a}$ kein Teiler des Einselementes, so ist $\mathbf{ab} = \mathbf{0}$ für ein gewisses

$\mathbf{b} \neq \mathbf{0}$ aus Z_n; danach stelle man $\mathbf{b}$ in der Gestalt $\mathbf{x} - \mathbf{y}$ für $\mathbf{x} \neq \mathbf{y}$ aus Z_n dar und betrachte die Identität $\mathbf{a}(\mathbf{x} - \mathbf{y}) = \mathbf{0}$.

4. Man stelle die Additions- und die Multiplikationstabelle für Z_8 auf und bestimme in diesem Ring alle Nullteiler und alle Teiler des Einselementes.

5. Es sei N eine beliebige natürliche Zahl und r die Anzahl der zu N teilerfremden unter den Zahlen $1, 2, ..., N-1$. Man beweise, dass für jede zu N teilerfremde ganze Zahl a im Ring Z_n die Beziehung $\mathbf{a}^r = \mathbf{1}$ gilt (Satz von Euler).
In der Zahlentheorie wird diese Zahl r mit $\varphi(N)$ bezeichnet.

3.3 Diophantische Gleichungen und Reste

Jetzt können wir zur Untersuchung von diophantischen Gleichungen eines allgemeineren als des in Kapitel I betrachteten Typs übergehen.

Zunächst führen wir den Begriff eines ganzzahligen Polynoms in n Unbestimmten ein. Wir nennen $x_1, ..., x_n$ unabhängige Veränderliche (Unbestimmte), wenn jede von ihnen ganzzahlige Werte unabhängig von allen übrigen annimmt. Unter einem Monom der Veränderlichen $x_1, x_2, ..., x_n$ verstehen wir jeden Ausdruck der Gestalt

$$ax_1^{m_1}x_2^{m_2}...x_n^{m_n} \tag{1}$$

wobei die $m_1, m_2, ..., m_n$ ganze nichtnegative Zahlen sind und a eine beliebige ganze Zahl, der sogenannte Koeffizient des Monoms, ist.
Setzen wir für $x_1, x_2, ..., x_n$ in dem Monom ganze Zahlen ein, etwa $x_1 = a_1, x_2 = a_2, ..., x_n = a_n$, so geht das Monom in die bestimmte ganze Zahl $ax_1^{m_1}x_2^{m_2}...x_n^{m_n}$ über. Zwei Monome derselben Veränderlichen, $ax_1^{m_1}x_2^{m_2}...x_n^{m_n}$ und $bx_1^{k_1}x_2^{k_2}...x_n^{k_n}$ kann man multiplizieren, es ergibt sich wieder ein Monom nach der Regel

$$(ax_1^{m_1}x_2^{m_2}...x_n^{m_n}) \cdot (bx_1^{k_1}x_2^{k_2}...x_n^{k_n} = abax_1^{m_1+k_1}x_2^{m_2+k_2}...x_n^{m_n+k_n} \tag{2}$$

Natürlich bleibt (2) richtig, wenn wir $x_1, x_2, ..., x_n$ durch ganze Zahlen ersetzen.

Nun vereinbaren wir, was wir unter der Addition von Monomen verstehen. Unter der Summe der Monome $ax_1^{m_1}x_2^{m_2}...x_n^{m_n}$ und $bx_1^{k_1}x_2^{k_2}...x_n^{k_n}$ verstehen wir den Ausdruck

$$ax_1^{m_1}x_2^{m_2}...x_n^{m_n} + bx_1^{k_1}x_2^{k_2}...x_n^{k_n}$$

der für konkrete ganzzahlige Werte $x_1, x_2, ..., x_n$ etwa $x_1 = a_1, x_2 = a_2, ..., x_n = a_n$ den ganzzahligen Wert

$$aa_1^{a_1}a_2^{m_2}...a_n^{m_n} + ba_1^{k_1}a_2^{k_2}...a_n^{k_n}$$

annimmt. Jetzt ist es nicht schwer, die Summe endlich vieler Monome der Unbestimmten $x_1, x_2, ..., x_n$ zu definieren.

Definition 6. Unter einem ganzzahligen Polynom der Unbestimmten $x_1, x_2, ..., x_n$ verstehen wir jede Summe endlich vieler Monome der Unbestimmten $x_1, x_2, ..., x_n$. Die Koeffizienten der Summandenmonome werden die Koeffizienten des Polynoms genannt.

Ein Polynom in n Unbestimmten bezeichnen wir mit $f(x_1, x_2, ..., x_n)$.

So ist beispielsweise $f(x_1, x_2) = x_1 + x_2$ ein Polynom in zwei Unbestimmten; seine Koeffizienten sind gleich 1. Für das Polynom $g(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2^2$ ist charakteristisch, dass seine sämtlichen Werte (d.h. die Zahlen, die man erhält, wenn man x_1 und x_2 durch konkrete ganze Zahlen ersetzt) Quadratzahlen sind; es ist nämlich

$$g(x_1, x_2) = (x_1 + x_2)^2$$

Es versteht sich von selbst, dass die mehrfache Wiederholung des Wortes "ganzzahlig" in allen unseren Konstruktionen durch die Konkretheit unserer Ziele bedingt ist:
Wir haben ein Polynom in den n Unbestimmten $x_1, x_2, ..., x_n$ konstruiert, das für ganzzahlige Werte dieser Unbestimmten ganzzahlige Werte annimmt. Man könnte aber auch von reellen oder komplexen Polynomen in n Unbestimmten sprechen, nur muss man dann für die Koeffizienten der Monome reelle bzw. komplexe Zahlen wählen, und analog können die Unbestimmten $x_1, x_2, ..., x_n$ als Werte reelle bzw. komplexe Zahlen annehmen.

Überdies kann man Polynome in n Unbestimmten konstruieren, deren Koeffizienten Restklassen nach einem festen Modul m sind und deren Veränderliche Werte aus Z_m annehmen (solche Polynome werden wir verwenden). Ein solches Polynom nennen wir - im Unterschied zu einem ganzzahligen Polynom - ein Polynom über dem Ring der Restklassen modulo m.

Wir untersuchen den Zusammenhang zwischen ganzzahligen Polynomen und Polynomen über einem Restklassenring.
Es sei $f(x_1, x_2, ..., x_n)$ ein ganzzahliges Polynom von n Veränderlichen und m eine ganze positive Zahl. Den Unbestimmten $x_1, x_2, ..., x_n$ erteilen wir irgendwelche ganzzahligen Werte, $x_1 = a_1$, $x_2 = a_2$, ..., $x_n = a_n$; dann geht das Polynom in die Zahl $f(a_1, a_2, ..., a_n)$ über.
Mit $\mathbf{f}(x_1, x_2, ..., x_n)$ bezeichnen wir nun das Polynom über dem Restklassenring modulo m, das wir aus $f(x_1, x_2, ..., x_n)$ erhalten, wenn wir die Koeffizienten durch ihre Restklassen modulo m ersetzen. Dann ist, wie aus § 2 folgt,

$$\mathbf{f}(\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n) = \mathbf{f}(a_1, a_2, ..., a_n)$$

wobei $\mathbf{f}(\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n) = f(a_1, a_2, ..., a_n) \pmod m$ und $\mathbf{a}_i = a_i \pmod m$ $(i = 1, 2, ..., n)$ gilt. Wir nennen das Polynom $\mathbf{f}(x_1, x_2, ..., x_n)$ die Reduktion des Polynoms $f(x_1, x_2, ..., x_n)$ nach dem Modul m.

Beispielsweise ist für $m = 9$, $n = 2$ und $f(x_1; x_2) = 15x_1^3 + 9x_1^2x_2 + 8x_1x_2 + 11x_2^2$

$$\mathbf{f}(x_1, x_2) = \mathbf{6}x_1^3 + \mathbf{0}x_1^2x_2 + \mathbf{8}x_1x_2 + \mathbf{2}x_2^2 = \mathbf{6}x_1^3 + \mathbf{8}x_1x_2 + \mathbf{2}x_2^2$$

Definition 7. Unter einer diophantischen Gleichung in n Unbekannten verstehen wir eine Gleichung der Gestalt

$$f(x_1, x_2, ..., x_n) = 0 \tag{3}$$

wobei $f(x_1, x_2, ..., x_n) = 0$ ein ganzzahliges Polynom in n Unbekannten ist und die $x_1, x_2, ..., x_n$ nur ganzzahlige Werte annehmen.

Wir weisen auf folgendes hin. Ist $x_1 = a_1$, $x_2 = a_2$, ..., $x_n = a_n$ eine Lösung der diophantischen Gleichung (3), d.h., ist $f(a_1, a_2, ..., a_n) = 0$, so gilt

$$\mathbf{f}(\mathbf{a}_1, \mathbf{a}_2, ...\mathbf{a}_n) = 0 \tag{4}$$

für die Reduktion nach jedem Modul m. Daher kann, wenn für irgendein m die Identität (4) nicht für alle möglichen Reste $\mathbf{a}_1, \mathbf{a}_2$, ..., $\mathbf{a}_n$ nach dem Modul m erfüllt ist, die Gleichung (4) keine Lösung haben. Mit anderen Worten, es gilt

Satz 5. Eine Lösung der diophantischen Gleichung (3) kann nur dann existieren, wenn die Identität (4) für alle Moduln m und beliebige Reste $\mathbf{a}_i = a_i \pmod m$, $i = 1, 2, ..., n$, erfüllt ist.

Beispiele

1. Man untersuche, ob die diophantische Gleichung

$$x^2 + 21xy + 14yz - 3 = 0$$

lösbar ist. Die Reduktion dieser Gleichung modulo 7 lautet

$$x^2 = 3$$

Unter den Restklassen **0**, **1**, **2**, **3**, **4**, **5**, **6** modulo 7 sind wegen

$$\mathbf{0}^2 = \mathbf{0}, \mathbf{1}^2 = \mathbf{1}, \mathbf{2}^2 = \mathbf{4}, \mathbf{3}^2 = \mathbf{2}, \mathbf{4}^2 = \mathbf{2}, \mathbf{5}^2 = \mathbf{4}, \mathbf{6}^2 = \mathbf{1}$$

nur die Klassen **0**, **1**, **2**, **4** Quadratzahlen. Daher kann die Beziehung $x^2 = \mathbf{3}$ niemals erfüllt sein, so dass die gegebene Gleichung keine Lösung besitzt.

2. Man untersuche, ob die diophantische Gleichung

$$15x^2 - 7y^2 = 9$$

lösbar ist.
Es sei $x = m$, $y = n$ eine Lösung. Sind m und n durch 3 bzw. 9 teilbar, so sind m^2 und n^2 durch 9 teilbar. Dann sind auch die Zahlen $m^2/9$ und $n^2/9$ Quadratzahlen, wie sich aus dem Hauptsatz der elementaren Zahlentheorie ergibt. Daher ist $m^2 = 9m_1^2$ und $n^2 = 9n_1^2$. Dann nimmt die gegebene Gleichung die Gestalt

$$15m_1^2 - 7n_1^2 = 1$$

an, und die Reduktion modulo 5 liefert

$$-\mathbf{2}\mathbf{n}_1^2 = \mathbf{1}$$

Wegen $-\mathbf{2} \cdot \mathbf{2} = -\mathbf{4} = \mathbf{1}$ ergibt sich $\mathbf{n}_1^2 = \mathbf{2}$.
Unter den Resten modulo 5 sind aber nur **0**, **1** und **4** Quadratzahlen. Daher hat die ursprüngliche Gleichung keine Lösung.

Natürlich erhebt sich die Frage, ob die Bedingung, dass die Reduktion einer gegebenen diophantischen Gleichung nach allen möglichen Moduln lösbar ist, nicht auch dafür hinreichend ist, dass die diophantische Gleichung selbst eine Lösung hat. Im allgemeinen Fall ist die Antwort auf diese Frage negativ. Man kann beweisen, dass beispielsweise die diophantische Gleichung

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$$

die offenbar keine Lösung hat (weder 13 noch 17 noch 221 ist im Ring $\mathbb{Z}$ eine Quadratzahl), bei der Reduktion nach jedem Modul m unter den entsprechenden Restklassen eine Lösung besitzt. Unsere bisherigen Überlegungen reichen dafür nicht aus. Dazu ist eine eingehende Beschreibung der Teilmenge der Quadratzahlen im Ring der Restklassen nach dem Modul m erforderlich.
Wenigstens für Primzahlmoduln bringen wir hier einige Ergebnisse.

Es sei p eine von 2 verschiedene, also ungerade Primzahl; $-\frac{p-1}{2}$, ..., $-1, 0, 1$, ..., $\frac{p-1}{2}$ sind sämtliche Elemente von Z_p. Erheben wir jede dieser Zahlen ins Quadrat, so erhalten wir wegen

$$\begin{aligned} \mathbf{1} &= (-\mathbf{1})^2 \\ \mathbf{2}^2 &= (-\mathbf{2})^2 \\ &\dots \\ \left(\frac{\mathbf{p\text{-}1}}{2}\right)^2 &= \left(-\frac{\mathbf{p\text{-}1}}{2}\right)^2 \end{aligned}$$

höchstens $(\mathbf{p\text{-}1})/2$ von null und voneinander verschiedene Elemente von Z_p. Es sind alle Quadrate $\mathbf{1}^2, \mathbf{2}^2$, ..., $\left(\frac{\mathbf{p\text{-}1}}{2}\right)^2$ paarweise verschieden. Wäre $\alpha^2 = \beta^2$, so wäre $(\alpha + \beta)(\alpha - \beta) = 0$, also - da es in Z_p keine Nullteiler gibt - entweder $\alpha = \beta$ oder $\alpha = -\beta$; ersteres ist nicht möglich, da nach Voraussetzung α und β verschieden sind, das zweite ausgeschlossen, da α und β verschiedene Elemente der Menge **1**, **2**, ..., $\frac{\mathbf{p\text{-}1}}{2}$ sind. Daher gibt es in Z_p genau $\frac{p-1}{2}$ von Null verschiedene Quadrate.

Wann kommt unter diesen Elementen -1 vor? Nach dem kleinen Fermatschen Satz ist $\mathbf{a}^{p-1} = \mathbf{1}$ für alle $\mathbf{a} \neq \mathbf{0}$ aus Z_p. Ist **a** ein Quadrat, also $\mathbf{a} = \mathbf{b}^2$ für ein bestimmtes **b**, so ist

$$\mathbf{a}^{\frac{p-1}{2}} = (\mathbf{b}^2)^{\frac{p-1}{2}} = \mathbf{b}^{p-1} = \mathbf{1}$$

Allgemein ist $\mathbf{x}^{\frac{p-1}{2}}$ gleich **1** oder **-1**, je nachdem, ob **x** ein Quadrat ist oder nicht. Ist nämlich **x** ein Quadrat, so ist, wie wir schon gesehen haben, dies der Fall.
Ist aber **x** kein Quadrat, so ist $\mathbf{x}^{\frac{p-1}{2}} = \mathbf{r}$, aber schon $\mathbf{r}^2 = \mathbf{1}$ oder $\mathbf{r}^2 - \mathbf{1} = 0$. Letzteres ist aber wegen $r^2 - 1 = (r-1)(r+l)$ und der Tatsache, dass es in Z_p keine Nullteiler gibt, nur möglich für $r = \mathbf{1}$ oder $r = \mathbf{-1}$.

Wäre $r = \mathbf{1}$, so würde das Polynom $z^{\frac{p-1}{2}} - 1$ über Z_p öfter verschwinden als für $\frac{p-1}{2}$ Werte von z. Das ist jedoch aus folgendem Grunde unmöglich:
Es sei $f(z) = \mathbf{a}_0 z^n + \dots + \mathbf{a}_n$ ein beliebiges Polynom über Z_p und $f(\mathbf{c}) = \mathbf{0}$ für ein **c** aus Z_p; dann muss $f(z) = (z - \mathbf{c})g(z)$ sein, wobei $g(z)$ ein Polynom über Z_p ist. Dies

beweisen wir durch vollständige Induktion nach dem sogenannten Grad n des Polynoms $f(z)$.

Für $n = 1$ hat $f(z)$ die Gestalt $\mathbf{a}_0 z + \mathbf{a}_1$ und da $f(\mathbf{c}) = \mathbf{0}$, also $\mathbf{a}_0\mathbf{c} + \mathbf{a}_1 = \mathbf{0}$ ist, muss $f(z) = \mathbf{a}_0 z - \mathbf{a}_0\mathbf{c}$ sein. Daher ist $f(z) = (z - \mathbf{c})\mathbf{a}_0$.
Nun nehmen wir an, unsere Behauptung sei für alle Polynome aller Grade $t < n$ bewiesen. Das Polynom

$$\begin{aligned} g_1(z) &= f(z) - \mathbf{a}_0 z^{n-1}(z - \mathbf{c}) = \mathbf{a}_0 z^n + \mathbf{a}_1 z^{n-1} + ... + \mathbf{a}_n - \mathbf{a}_0 z^n + \mathbf{a}_0\mathbf{c} z^{n-1} \\ &= (\mathbf{a}_1 + \mathbf{a}_0 c) z^{n-1} + \mathbf{a}_2 z^{n-2} + ... + \mathbf{a}_n \end{aligned}$$

hat einen Grad, der kleiner als n ist, und verschwindet offensichtlich wegen $f(\mathbf{c}) = 0$ für $z = \mathbf{c}$. Nach der Induktionsannahme ist daher $g_1(z) = (z - \mathbf{c})g_2(z)$, also

$$f(z) = g_1(z) + \mathbf{a}_0 z^{n-1}(z - \mathbf{c}) = (z - \mathbf{c})(\mathbf{a}_0 z^{n-1} + g_2(z))$$

Damit ist die Behauptung bewiesen.

Aus ihr ergibt sich: Sind $\mathbf{c}_1, ..., \mathbf{c}_k$ verschiedene Elemente aus Z_p, für welche $f(\mathbf{c}_1) = ... = f(\mathbf{c}_k) = 0$ gilt, so ist $f(z) = (z - \mathbf{c}_1)...(z - \mathbf{c}_k)g(z)$. Da sich die Grade von Polynomen beim Multiplizieren addieren, können in dem Ausdruck $f(z) = (z - \mathbf{c}_1)...(z - \mathbf{c}_k)g(z)$ rechts nicht mehr Faktoren der Gestalt $(z - \mathbf{c}_i)$ stehen als der Grad des Polynoms $f(z)$ beträgt.
Daher kann das im vorigen Absatz erwähnte Polynom $z^{p-1} - 1$ nicht für mehr als $\frac{p-1}{2}$ Werte von z verschwinden.

Somit ist $x^{\frac{p-1}{2}} = -1$. Hieraus ergibt sich etwas prinzipiell Wichtiges. Ein Element **x** auch Z_p ist genau dann ein Quadrat, wenn $\mathbf{x}^{\frac{p-1}{2}} = 1$ ist, und genau dann kein Quadrat, wenn $\mathbf{x}^{\frac{p-1}{2}} = -1$ ist. Daher ist -1 ein Quadrat, wenn $(\text{-}\mathbf{1})^{\frac{p-1}{2}} = \mathbf{1}$ ist, und kein Quadrat, wenn $(\text{-}\mathbf{1})^{\frac{p-1}{2}} = \text{-}\mathbf{1}$ ist.
Die Zahl p ist ungerade, also entweder $p = 4k + 1$ oder $p = 4k - 1$. Im ersten Fall ist $(\text{-}\mathbf{1})^{\frac{p-1}{2}} = (\text{-}\mathbf{1})^{k-1} = \text{-}\mathbf{1}$ und -**1** kein Quadrat.
Eine weitere Behauptung: Sind x und y aus Z_p keine Quadrate, so ist xy ein Quadrat. Dies möge der Leser selbst beweisen.

In der diophantischen Gleichung $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ ist $221 = 13 \cdot 17$. Daher hat in der Reduktion nach einem Primzahlmodul diese Gleichung eine Lösung (denn wenigstens eine der Klassen 13, 17, $13 \cdot 17$ ist ein Quadrat).

Nun können wir die schon in Kapitel II formulierte Aussage beweisen:
Jede Primzahl p der Gestalt $p = 4k + 1$ mit ganzzahligem k ist die Norm einer ganzen Gaußschen Zahl (also als Summe zweier Quadrate ganzer Zahlen darstellbar) : $p = x^2 + y^2$.
Dies beweisen wir durch vollständige Induktion nach p.

Für $p = 4$ (die kleinste Primzahl der Gestalt $4k + 1$) ist offenbar $5 = 2^2 + 1^2$.
Nun nehmen wir an, die Behauptung sei für alle Primzahlen der Gestalt $4k+1$ bewiesen, die kleiner als eine Primzahl p derselben Gestalt sind. Im Ring Z_p ist, wie oben bewiesen wurde, die Klasse -**1** ein Quadrat, d.h., es gibt ein **x** aus Z_p mit $\mathbf{x}^2 + \mathbf{1} = \mathbf{0}$.

Dies bedeutet, dass im Ring $\mathbb{Z}$ der ganzen Zahlen $x^2 + y^2 = lp$ gilt, wobei x und y ganze Zahlen sind und die Restklasse von y die Klasse **1** ist. Da alle Quadrate in Z_p in der Folge

$$\mathbf{0}^2, \mathbf{1}^2, \mathbf{2}^2, ..., \left(\frac{\mathbf{p\text{-}1}}{\mathbf{2}}\right)^2$$

enthalten sind, können wir annehmen, dass $0 < x, y < p/2$ also $l < p$ ist. Schließlich setzen wir voraus, dass x und y teilerfremd sind (anderen- falls kürzen wir beide Seiten der Gleichung $x^2 + y^2 = lp$ durch gemeinsame Teiler).

Es sei $l = p_1 \cdot p_2 ... p_r$, die Pimzahlzerlegung von l in $\mathbb{Z}$. Da $(x, y) = 1$ und $x^2 + y^2$ durch p_j, $(j = 1, 2, ..., r)$ teilbar ist, ist die Klasse -**1** mod p_j ein Quadrat in Z_p, also $p_j = 4m_j + 1$ für eine ganze Zahl m_j $(j = 1, 2, ..., r)$.
Wegen $p_j < P$ ist nach Induktionsannahme

$$p_j = x_j^2 + y_j^2 = (x_j + iy_j)(x_j - iy_j) = t^{(j)} \cdot \bar{t}^{(j)}$$

wobei $t^{(j)}$ und $\bar{t}^{(j)}$ Primfaktoren im Ring der ganzen Gaußschen Zahlen und $\overline{a + bi} = a - bi$ die konjugiert-komplexe Zahl von $a + bi$ ist.

Daher ist

$$(x + iy)(x - iy) = pt^{(1)} ... t^{(r)} \overline{t^{(1)}} ... \overline{t^{(r)}}$$

Rechts steht ein Produkt aus Gaußschen Primzahlen. Auf Grund der Eindeutigkeit der Primzahlzerlegung im Ring der ganzen Gaußschen Zahlen können wir rechts und links durch die Primzahlen $t^{(1)} ... t^{(r)} \overline{t^{(1)}} ... \overline{t^{(r)}}$ kürzen.
Auf diese Weise erhalten wir die Darstellung der ganzen Primzahl p als Produkt Gaußscher Zahlen und ihrer konjugiert-komplexen Zahlen. Damit ist die Behauptung bewiesen.

Die Untersuchung diophantischer Gleichungen auf Lösbarkeit mit Hilfe von Restklassenringen hat in der Zahlentheorie vor allem deshalb große Bedeutung, weil sie es in vielen Fällen ermöglicht, den Ausgang von Versuchen zur Lösung diophantischer Aufgaben "vorherzusagen".

Wir beschließen dieses Kapitel mit einem Beispiel, wie man die Reduktion einer speziellen diophantischen Gleichung untersucht:

$$\mathbf{f}(x, y) = \mathbf{a}x^2 + \mathbf{b}xy + \mathbf{c}z^2 = \mathbf{0}$$

Unter dem Symbol $f_p(x, y)$ wollen wir die Reduktion des Polynoms $f(x, y)$ nach dem Modul p verstehen.

Satz 6. Es sei $p \neq 2$ eine Primzahl. Die Gleichung

$$f_p(x, y) = \mathbf{0}$$

hat genau dann eine von $x = y = \mathbf{0} = 0$ (mod p) verschiedene Lösung, wenn $\mathbf{b}^2 = \mathbf{a} \cdot \mathbf{c} = (b^2 - ac)$ (mod p) ein Quadrat im Ring Z_p ist.

Beweis. Es sei $\mathbf{b}^2 - \mathbf{a}\cdot\mathbf{c} = \mathbf{z}^2$; und $\mathbf{a} \neq \mathbf{0}$. Da bei den von $\mathbf{0}$ verschiedenen Restklassen nach einem Primzahlmodul eine Division möglich ist, können folgende Umformungen vorgenommen werden:

$$\mathbf{a}x^2 + 2\mathbf{b}xy + \mathbf{c}y^2 = \mathbf{a}\left(x - \frac{-\mathbf{b}+\mathbf{z}}{\mathbf{a}}y\right)\left(x - \frac{-\mathbf{b}-\mathbf{z}}{\mathbf{a}}y\right)$$

(Von ihrer Gültigkeit kann man sich unmittelbar überzeugen, wenn man sich auf die Definition der Operationen mit Monomen stützt.) Daher genügt es, eine Lösung der Gleichung

$$\left(x - \frac{\mathbf{z}-\mathbf{b}}{\mathbf{a}}y\right)\left(x + \frac{\mathbf{b}+\mathbf{z}}{\mathbf{a}}y\right) = 0$$

zu finden. Da es in einem Restklassenring nach einer Primzahl keinen Nullteiler gibt, kann man eine solche Lösung aus einer der beiden Gleichungen

$$x = \frac{-\mathbf{b}+\mathbf{z}}{\mathbf{a}}y \qquad , \qquad x = \frac{-\mathbf{b}-\mathbf{z}}{\mathbf{a}}y$$

erhalten.
Ist $\mathbf{a} = 0$, aber $\mathbf{c} \neq 0$, so kann man alles oben Gesagte leicht auch auf diesen Fall übertragen. Ist aber $\mathbf{a} = \mathbf{c} = 0$, so ist eine von 0 verschiedene Lösung der gegebenen Gleichung beispielsweise $x = \mathbf{1}$, $y = \mathbf{0}$.

Umgekehrt, sei $x = \mathbf{x}$, $y = \mathbf{y}$ eine Lösung mit $\mathbf{x} \neq \mathbf{0}$ oder $\mathbf{y} \neq \mathbf{0}$. Ist $\mathbf{a} = \mathbf{c} = \mathbf{0}$, so ist die Aussage trivial, denn $\mathbf{b}^2$ ist ein Quadrat. Es sei etwa $\mathbf{a} \neq \mathbf{0}$. Dann ist

$$\mathbf{0} = \mathbf{a}\mathbf{x}^2 + 2\mathbf{b}\mathbf{x}\mathbf{y} + \mathbf{c}\mathbf{y}^2 = \mathbf{a}\left(\mathbf{x}^2 + \frac{2\mathbf{b}}{\mathbf{a}}\mathbf{x}\mathbf{y} + \frac{\mathbf{c}}{\mathbf{a}}\mathbf{y}^2\right) = \mathbf{a}\left(\left(\mathbf{x} + \frac{\mathbf{b}}{\mathbf{a}}\mathbf{y}\right)^2 - \frac{\mathbf{b}^2 - \mathbf{a}\mathbf{c}}{\mathbf{a}^2}\mathbf{y}^2\right)$$

Daher ist

$$\left(\mathbf{x} + \frac{\mathbf{b}}{\mathbf{a}}\mathbf{y}\right)^2 = \frac{\mathbf{b}^2 - \mathbf{a}\mathbf{c}}{\mathbf{a}^2}\mathbf{y}^2$$

Wegen $\mathbf{a} \neq \mathbf{0}$ ist die Klasse $\mathbf{y}$ von $\mathbf{0}$ verschieden; wäre $\mathbf{y} = \mathbf{0}$, so wäre auch $\mathbf{x} = \mathbf{0}$. Das ist aber ein Widerspruch zur Voraussetzung. Daher ist

$$\mathbf{b}^2 - \mathbf{a}\cdot\mathbf{c} = \frac{\mathbf{a}^2}{\mathbf{y}^2}\left(\mathbf{x} + \frac{\mathbf{b}}{\mathbf{a}}\mathbf{y}\right)^2 = \left[\frac{\mathbf{a}}{\mathbf{y}}\left(\mathbf{x} + \frac{\mathbf{b}}{\mathbf{a}}\mathbf{y}\right)\right]^2$$

Damit ist der Satz bewiesen.

In die Voraussetzung war $p \neq 2$ aufgenommen werden. Das geschah nicht, weil der Satz für $p = 2$ falsch wäre. Im Fall $p = 2$ ist der Satz trivial, weil $\mathbf{f}_2(x, y) = \mathbf{a}x^2 + \mathbf{c}y^2 - \mathbf{ac}$ (mod 2) ein Quadrat im Ring Z_2 ist und $\mathbf{a}x^2 = \mathbf{c}y^2 = 0$ offensichtlich eine nichttriviale Lösung besitzt.

4 Zahlensysteme

Zum Aufschreiben von Zahlen benutzen wir gewöhnlich die Dezimalziffern 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. In diesem Kapitel untersuchen wir die Rolle der Zahl 10 bei der traditionellen Schreibweise der Zahlen und beschreiben alle möglichen Arten, die "Zehn" durch andere natürliche Zahlen zu ersetzen.
Besonders wichtig wurde in unserer Zeit diejenige Darstellung, bei der die Zwei die Rolle der Zehn übernimmt. In elektronischen Rechenautomaten wird meist nicht das Dezimalsystem, sondern das sogenannte Dualsystem verwendet.

4.1 Das Dezimalsystem

Unter dem Dezimalsystem versteht man das System der Zahlen, die in der üblichen Weise mit Hilfe der Dezimalziffern 0, 1, 2, ..., 9 geschrieben sind; jede dieser Ziffern bezeichnet eine bestimmte nichtnegative ganze Zahl.

Derartige Systeme zur Darstellung der Zahlen werden Positionssysteme genannt; dabei bezeichnet eine Ziffer verschiedene Zahlen, je nachdem, welchen Platz sie in der Darstellung besetzt. Natürlich könnte man an Stelle dieser Dezimalsymbole auch andere nehmen; wenn es aber wieder zehn Symbole wären und sie analog der traditionellen Ziffern benutzt würden, so müsste man das System dieser Zahlen wieder als Dezimalsystem bezeichnen.

Worin besteht die Rolle der Zahl 10? Sie besteht darin, dass wir eine Zahl mit Hilfe aller möglichen Reste schreiben, die bei der Division durch 10 entstehen; denn gerade wie Reste bei Division durch 10 verhalten sich die Dezimalziffern bei allen Rechenoperationen mit den Zahlen. Um das zu zeigen, untersuchen wir die Dezimaldarstellung einer Zahl näher:

Es sei zunächst N eine natürliche Zahl. Aus dem Algorithmus der Division mit Rest folgt, dass $N = 10q_0 + r_0$ ist, mit $0 \leq r_0 \leq 9$ und $0 \leq q_0 \leq N$ (ist beispielsweise $N = 6$, so ist $q_0 = 0$ und $r_0 = 6$).
Ist der Quotient q_0 positiv, so gilt entsprechend $q_0 = 10q_1 + r_1$, mit $0 \leq r_1 \leq 9$ und

$$N = 10q_0 + r_0 = 10^2 q_1 + 10r_1 + r_0$$

Ist $q_1 > 0$, so kann man das Verfahren fortsetzen und erhält

$$N = 10^3 q_2 + 10^2 r_2 + 10r_1 + r_0$$

Der Quotient q_2 wird kleiner als q_1, und q_1 kleiner als q_0, und q_0 war kleiner als N. Daher ergibt sich nach endlich vielen Schritten, sagen wir, nach n Schritten, $q_n = 0$ und

$$N = 10^n r_n + 10^{n-1} r_{n-1} + ... + 10r_1 + r_0 \tag{1}$$

Hierbei sind $r_0, ..., r_n$ nichtnegative ganze Zahlen, welche höchstens gleich 9 sind. Die Darstellung (1) wird die Dezimaldarstellung (oder auch Dezimalentwicklung) der Zahl N genannt.

Es sei

$$N = 10^{n'} r'_{n'} + 10^{n'-1} r'_{n'-1} + ... + 10r'_1 + r'_0 \qquad (1')$$

eine weitere derartige Darstellung. Dann gilt zunächst $r_0 = r'_0$, da sowohl r_0 als auch r'_0 der eindeutig bestimmte Rest von N bei der Division durch 10 ist. Daraus folgt

$$\frac{N - r_0}{10} = \frac{N - r'_0}{10}$$

woraus sich analog $r_1 = r'_1$ ergibt. So fortfahrend erhält man die Übereinstimmung der beiden Darstellungen.

Vereinbart man, dass das Symbol $a_n a_{n-1} ... a_0$ die aufgeschriebene Reihenfolge der Dezimalziffern $a_n, a_{n-1}, ..., a_0$ bedeutet, so lautet die Dezimaldarstellung der Zahl

$$N = r_n r_{n-1} ... r_0$$

Mit Hilfe von (1) lassen sich interessante Tatsachen herleiten. Einige davon führen wir hier an.

Satz 1. Die Differenz zwischen einer Zahl und der Summe ihrer Dezimalziffern (ihrer Quersumme) ist durch 9 teilbar.

Beweis. Die Zahl N sei in der Gestalt (1) dargestellt. Dann ist

$$\begin{aligned} N - (r_0 + ... + r_n) &= 10^n r_n + 10^{n-1} r_{n-1} + ... + 10r_1 + r_0 - r_n - r_{n-1} - ... - r_1 - r_0 \\ &= (10^n - 1) r_n + (10^{n-1} - 1) r_{n-1} + ... + (10 - 1) r_1 \end{aligned}$$

Nun ist aber $\mathbf{10}$ (mod 9) = $\mathbf{1}$ (mod 9), so dass auch 10^n (mod 9) $\equiv 1$ (mod 9) gilt; daher ist auch N (mod 9) $\equiv (r_n + ... + r_0)$ (mod 9), also $N - (r_n + ... + r_0) \equiv 0$ (mod 9). Damit ist Satz 1 bewiesen.

Folgerung. Ist die Quersumme einer Zahl durch 9 teilbar, so ist auch die Zahl selbst durch 9 teilbar.
Umgekehrt, ist eine Zahl durch 9 teilbar, so ist auch ihre Quersumme ein Vielfaches von 9.

Ist nämlich M die Quersumme einer durch 9 teilbaren Zahl N, so folgt aus $N \equiv M$ (mod 9) unmittelbar $M \equiv 0$ (mod 9). Analog, ist $N \equiv 0$ (mod 9), so ergibt sich aus $N \equiv M$ (mod 9) ebenso $M \equiv 0$ (mod 9).
Entsprechend lässt sich ein Kriterium für die Teilbarkeit einer Zahl durch 3 formulieren und beweisen.

Satz 2. Ist die Differenz zwischen der Summe der an den geradzahligen Stellen stehenden Dezimalziffern einer Zahl N und der Summe der Dezimalziffern an den ungeradzahligen Stellen durch 11 teilbar, so ist auch die Zahl N selbst durch 11 teilbar.
Auch die Umkehrung gilt: Ist N ein Vielfaches von 11, so ist die Differenz der Summen der Ziffern an den geradzahligen und an den ungeradzahligen Stellen durch 11 teilbar.

Beweis. Bekanntlich ist $10^{2k} \equiv 1$ (mod 11) und $10^{2k+1} \equiv 10$ (mod 11). Gehen wir in (1) zu Resten modulo 11 über, so erhalten wir

$$N \equiv r_0 + 10r_1 + r_2 + 10r_3 + ... \pmod{11} \qquad \text{also}$$

$$N \equiv (r_0 + r_2 + ...) + 10(r_1 + r_3 + ...) \pmod{11}$$

Wegen $(r_0 + r_2 + ...) \equiv (r1 + r3 + ...) \pmod{11}$ ist daher

$$N \equiv (r_1 + r_3 + ...) + 10(r_1 + r_3 + ...) \pmod{11} \equiv 11(r_1 + r_3 + ...) \equiv 0 \pmod{11}$$

Gilt umgekehrt $N \equiv 0$ (mod 11), so erhält man unter Berücksichtigung von $10 \equiv -1$ (mod 11) offenbar aus

$$(r_0 + r_2 + ...) + 10(r_1 + r_3 + ...) \equiv 0 \pmod{11}$$

die Beziehung

$$(r_0 + r_2 + ...) - (r_1 + r_3 + ...) \equiv 0 \pmod{11}$$

Wie wir sehen, stehen in der Dezimaldarstellung einer natürlichen Zahl die Ziffern genau in der Reihenfolge wie die Reste bei der Division durch 10. Für beliebige ganze Zahlen gilt das gleiche, nur steht vor einer negativen Zahl das Minuszeichen.

Nun gehen wir zu rationalen Zahlen über, zu unkürzbaren Brüchen der Gestalt $R = \frac{N}{M}$, wobei wir zunächst N und M als natürliche Zahlen voraussetzen; später betrachten wir auch negative rationale Zahlen. Unser nächstes Ziel besteht darin, für rationale Zahlen eine Darstellung der Gestalt (1) zu gewinnen, die für $M = 1$ in die Darstellung (1) übergeht.

Wir wollen annehmen, $R = \frac{N}{M}$ sei ein echter Bruch, es sei also $N < M$. Anderenfalls können wir den ganzen Teil abspalten, für den wir wie oben die Dezimaldarstellung erhalten können, so dass wir uns auf die Dezimaldarstellung echter Brüche beschränken können.

Es sei $10N = q_1M + a_1$, mit $0 \leq a_1 < M$. Dann ist $0 \leq q_1 < 9$, weil $10N < 10M$ gilt, und

$$R = \frac{N}{M} = \frac{10N}{10M} = \frac{q_1M + a_1}{10M} = 10^{-1}q_1 + 10^{-1}\frac{a_1}{M}$$

Ist $a_1 = 0$, so lautet die Dezimaldarstellung von R einfach

$$R = 10^{-1}q_1 \tag{2}$$

Ist $a_1 \neq 0$, so ist analog

$$\frac{a_1}{M} = 10^{-1}q_2 + 10^{-1}\frac{a_2}{M}$$

mit $0 \leq q_2 \leq 9$ und $0 \leq a_2 < M$. Für $a_2 = 0$ hat die gesuchte Dezimaldarstellung die Gestalt

$$R = 10^{-1}q_1 + 10^{-2}q_2$$

Ist $a_2 \neq 0$, so ist

$$\frac{a_2}{M} = 10^{-1}q_3 + 10^{-1}\frac{a_3}{M}$$

mit $0 \leq q_3 \leq 9$ und $0 \leq a_3 < M$ usw.
Nun sind zwei Fälle möglich: Entweder bricht das Verfahren nach endlich vielen Schritten ab, und wir erhalten einen endlichen Dezimalbruch

$$R = 0, q_{-1}q_{-2}...q_{-k} = q_{-1}10^{-1} + q_{-2}10^{-2} + ... + q_{-k}10^{-k} \tag{3}$$

oder das Verfahren bricht nicht ab. Da es aber bei der Division durch eine Zahl M höchstens M verschiedene Reste gibt, müssen sich die Reste a_k (also auch die Quotienten q_k) irgendwann zu wiederholen beginnen. Wir erhalten also einen unendlichen periodischen Dezimalbruch:

$$R = q_{-1}10^{-1} + q_{-2}10^{-2} + ... + q_{-k}10^{-k} + ...$$

Mit dem letzten Fall wollen wir uns nun etwas näher befassen, um die Länge der Periode zu bestimmen. Wir nehmen an, wir hätten für die Quotienten und Reste folgende Tabelle erhalten:

$$\begin{aligned} 10a_0 &= Mq_1 + a_1, \\ 10a_1 &= Mq_2 + a_2, \\ &... \\ 10a_{k-2} &= Mq_{k-1} + a_{k-1}, \\ 10a_{k-1} &= Mq_k + a_0 \end{aligned} \tag{4}$$

Hier haben wir der Einfachheit halber die Bezeichnungsweise so gewählt, dass die erste Ziffer der Periode (d.h. ein Quotient q_i den wir nach dem obigen Verfahren erhalten haben), die Nummer 1 hat; in der letzten Zeile der Tabelle erscheint zum zweiten Mal der Rest a_0, mit dem die Berechnung in (4) begonnen wurde.
Wir erinnern daran, dass die Reste $a_0, a_1, ..., a_{k-1}$ sämtlich von null verschieden sind, was man natürlich von den Ziffern q_i nicht sagen kann. Schematisch schreibt man bekanntlich den entsprechenden Ausschnitt in der Form

$$0, ...q_1q_2...q_{k-1}q_k...$$

Nachdem wir die Ziffer q_k hingeschrieben haben, ist die nächste Ziffer, die sich bei der Berechnung ergibt, wieder die Ziffer q_1. Daher beginnt die Periode des Bruches mit der Ziffer q_1 und endet mit q_k. Das sind k Ziffern. Nun betrachten wir (4) als Kongruenzen modulo M:

$$\begin{aligned} 10a_0 &\equiv a_1, \\ 10a_1 &\equiv a_2, \\ &... \\ 10a_{k-2} &\equiv a_{k-1}, \\ 10a_{k-1} &\equiv a_0 \end{aligned} \tag{5}$$

Setzen wir a_1 aus der ersten Kongruenz in die zweite ein, dann a_2 aus der zweiten in die dritte usw., so erhalten wir

$$10^k a_0 \equiv a_0 (\mathrm{mod}\, M)$$

Nun sind die beiden Fälle $(10, M) = 1$ und $(10, M) \neq 1$ möglich. Im ersten sind in der Gleichung $10N = Mq + a$ mit $0 \leq a < M$ die Zahlen a und M teilerfremd, da andererseits jeder ihrer gemeinsamen Teiler als zu 10 teilerfremde Zahl ein Teiler von M sein müsste, aber nach Voraussetzung $(N, M) = 1$ gilt.
Daher sind im Fall $(10, M) = 1$ alle Reste a_i zu M teilerfremd, insbesondere ist also $(a_0, M) = 1$. Das bedeutet, dass die Klasse $\mathbf{a}_0$ (mod M) ein Teiler des Einselementes ist; daher gilt

$$10^k \equiv 1 (\mathrm{mod}\, M)$$

Die Zahl k, für welche $10^k \equiv 1$ (mod M) gilt, ist die kleinste unter den natürlichen Zahlen n, für welche $10^n \equiv 1$ (mod M) ist. Wäre nämlich $10^n \equiv 1$ (mod M) für ein $n < k$, so ergäbe sich aus den Kongruenzen (5) die Beziehung

$$a_n \equiv 10^n a_0 \equiv a_0 (\mathrm{mod}\, M)$$

Wegen $0 < a_0 < M$, $0 < a_n < M$ bedeutet die Kongruenz $a_n \equiv a_0$ (mod M) die Identität $a_n = a_0$. Dies widerspricht aber der Tatsache, dass alle Reste $a_0, a_1, ..., a_{k-1}$ paarweise verschieden sind (darauf beruhten ja die Gleichungen (4)).

Nun betrachten wir den Fall $(10, M) \neq 1$. Es sei $M = 2^r 5^s M'$ und $(10, M') = 1$. Dann ist $R = \frac{N}{M} = \frac{N}{2^r 5^s M'}$. Wir erweitern den Bruch R mit Potenzen von 2 und 5 so, dass der Nenner die Gestalt $10^l M'$ annimmt (beispielsweise $\frac{29}{140} = \frac{29}{2^2 \cdot 5 \cdot 7} = \frac{2^0 \cdot 5 \cdot 29}{10^2 \cdot 7} = \frac{145}{10^2 \cdot 7}$).

So erhalten wir $R = 10^{-l} \frac{N'}{M'}$ mit $(M', N') = 1$ und $(M', 10) = 1$.

Nach dem oben, Bewiesenen ist die Periodenlänge des Bruches $R' = \frac{N'}{M'}$ gleich derjenigen kleinsten Zahl k, für welche $10^k \equiv 1$ (mod M') ist. Dann ist aber die Periode des Bruches $R = 10^{-l} \cdot R'$ dieselbe, beginnt jedoch erst l Stellen weiter rechts. Damit haben wir bewiesen:

Satz 3. Es sei $R = \frac{N}{M}$ und $M = 2^r 5^s M'$ mit $(N, M) = 1$ und $(10, M') = 1$. Dann ist die Periodenlänge von R gleich der kleinsten natürlichen Zahl k, für welche

$$10^k \equiv 1 (\mathrm{mod}\, M')$$

gilt.

Ehe wir beschreiben, wie man die Dezimalziffern rationaler Brüche erhält, die, wie im Fall natürlicher Zahlen, der Dezimalentwicklung

$$R = r_{-1} 10^{-1} + ... + r_{-n} 10^{-n} \tag{5}$$

mit $0 \leq r_{-t} \leq 9$ entsprechen, weisen wir auf folgenden Umstand hin, der uns die Eindeutigkeit der Darstellung (6) garantiert: Es gilt

$$10^{-s} = 9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + ... + 9 \cdot 10^{-s-n} + ...$$

(mit anderen Worten, es ist 0,0...01 = 0,0..0099...9...).

Beweis. Wegen $0 < 10^{-1} < 1$ liefert die Summenformel für geometrische Reihen

$$9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + ... = 9 \cdot 10^{-s}(10^{-1} + 10^{-2} + ...) = 9 \cdot 10^{-s} \cdot \frac{10^{-1}}{1 - 10^{-1}} = 10^{-s}$$

Daher ist

$$0, r_{-1}...r_{-k}99... = 0, r_{-1}...r_{-k} + 0, \underbrace{0...01}_{k \text{ Stellen}}$$

Nun können wir beschreiben, wie die Dezimalziffern eines echten Bruches R bestimmt werden.
Es sei

$$R = r_{-1} \cdot 10^{-1} + r_{-2} \cdot 10^{-2} + ... + r_{-k} \cdot 10^{-k} + ...$$

Dann ist r_{-1} der ganze Teil der Zahl $10R$, ferner r_{-2} der ganze Teil der Zahl $10(10R - r_{-1})$ usw., r_{-k} der ganze Teil der Zahl

$$10^r \cdot R - 10^{-k-1} \cdot r_{-1} - ... - 10r_{-k+1}$$

Wir wollen das an Beispielen erläutern.
Es sei $R = \frac{2}{3}$. Die Länge l der Periode dieses Bruches bei der Dezimaldarstellung ist gleich der kleinsten derjenigen Zahlen k, für welche $10^k \equiv 1$ (mod 3) ist. Offenbar ist $l = 1$.
Die Periode selbst ergibt sich leicht: $R = 0,666...$

Nun ein Beispiel für einen Bruch mit einer größeren Länge der Periode in Dezimalschreibweise: $R_l = \frac{1}{7}$. Wir bestimmen die kleinste Zahl l, für die $10^l \equiv 1$ (mod 7) ist, am einfachsten folgendermaßen.
Dabei lassen wir der Kürze halber jeweils das Symbol (mod 7) weg. Im Ring Z_7 gilt $10 \equiv 3$, also $10^n \equiv 3^n$, und das bedeutet

$$\begin{aligned}
3^1 &\equiv 3, \\
3^2 &\equiv 2, \\
3^3 &\equiv 3 \cdot 2 \equiv 6, \\
3^4 &\equiv 3 \cdot 6 \equiv 4, \\
3^5 &\equiv 3 \cdot 4 \equiv 5, \\
3^6 &\equiv 3 \cdot 5 \equiv 1.
\end{aligned}$$

Die Periodenlänge l ist gleich 6.

Übungen

1. Man bestimme die Periodenlänge des Bruches $R = \frac{1}{23}$ im Dezimalsystem.

2. Man beweise, dass es Dezimalbrüche mit beliebig großer Periodenlänge gibt.

Hinweis: Es sei N eine beliebige natürliche Zahl. Wir schreiben einen Dezimalbruch R in Schritten nach folgender Regel auf:

1. Schritt: 0,10;
2. Schritt: 0,101 100;
3. Schritt: 0,101100111000 usw. ...

Das tun wir so lange, bis die Zahl der Dezimalstellen die Zahl N übertrifft. Dann schreiben wir hinter den so erhaltenen Dezimalbruch dieselben Stellen wieder und wieder auf, usw. Wir erhalten so einen unendlichen periodischen Dezimalbruch. Dann muss nur noch gezeigt werden, dass seine Periode gleich dem aufgeschriebenen Teil ist.

Wir fassen zusammen: Jede rationale Zahl kann entweder als endlicher oder als unendlicher, dann aber notwendigerweise periodischer Dezimalbruch geschrieben werden (dessen ganzer Teil 0 oder eine von null verschiedene Zahl sein kann).

Auch die Umkehrung dieser Aussage ist richtig:
Jeder endliche oder unendliche periodische Dezimalbruch ist eine rationale Zahl. Für endliche Dezimalbrüche ist das klar, für periodische wird es folgendermaßen bewiesen: Den gegebenen periodischen Bruch können wir als Summe eines endlichen Dezimalbruches und eines Bruchs der Gestalt

$$\rho = 0, \underbrace{000...0}_{s} \overline{q_1...q_n} q_1...q_n$$

darstellen, mit $q_1...q_n$ als Periode. Wie schon gesagt, ist der erste Summand (der endliche Bruch) eine rationale Zahl. Setzen wir $q_1...q_n = q$, so lautet der zweite Summand

$$\rho = q \cdot 10^{-n-s} + q \cdot 10^{-2n-s} + ... = q \cdot 10^{-s}(10^{-n} + 10^{-2n} + 10^{-3n} + ...)$$

Wegen $0 < 10^{-n} < 1$ liefert die Summenformel für geometrische Reihen

$$10^{-n} + 10^{-2n} + 10^{-3n} + ... = \frac{10^{-n}}{1 - 10^{-n}} = \frac{1}{10^n - 1}$$

Somit ist ρ, also auch der gegebene periodische Dezimalbruch, eine rationale Zahl.

Unter irrationalen Zahlen verstehen wir unendliche nichtperiodische Dezimalbrüche der Form

$$R = 10^n a_n + ... + 10a_1 + a_0 + 10^{-1}a_{-1} + ... + 10^{-k}a_{-k} + ... \tag{7}$$

Im Rahmen dieses Bändchens wollen wir jedoch auf irrationale Zahlen nicht eingehen.

Es seien P und Q reelle Zahlen, in der Gestalt (7) geschrieben, und es sei $P \geq 0$, $Q \geq 0$. Wir suchen die Darstellung (7) der Zahl $P + Q$. Genau genommen können wir die Dezimaldarstellung der Zahl $P+Q$ nur durch schrittweises Erhöhen der Genauigkeit, mit der die Summanden P und Q gegeben sind, erhalten.
Da wir aber hier nicht die Arithmetik der reellen Zahlen entwickeln, sondern nur das Verhalten der Ziffern bei der Addition ableiten wollen, begnügen wir uns damit, P und Q als endliche Dezimalbrüche vorauszusetzen.

$$\begin{aligned} P &= 10^n p_n + ... + 10^r p_r + ... + p_0 + 10^{-1}p_{-1} + ... + 10^{-m}p_{-m} \\ Q &= 10^l q_l + ... + 10^r q_r + ... + q_0 + 10^{-1}q_{-1} + ... + 10^{-m}q_{-m} \end{aligned} \tag{8}$$

(von den Ziffern p_{-m} und q_{-m} soll mindestens eine von 0 verschieden sein).
In der Entwicklung (7) der Zahl $P+Q$ stehen bei 10^{-k} für $k > m$ Nullen. Bei 10^{-m} steht der Rest der Zahl $p_{-m}+q_{-m}$ nach Division durch 10; es sei $p_{-m}+q_{-m} = 10a_{-m}+b_{-m}$, $0 \leq b_{-m} \leq 9$.
Dann steht bei 10^{-m+1} der Rest der Zahl $p_{-m+1} + q_{-m+1}$ nach Division durch 10, addiert zum Quotienten a_{-m}, und wieder reduziert nach dem Modul 10, usw. Die Ziffern p_r und q_r erweisen sich so als Ergebnis der Addition der Restklassenarithmetik modulo 10.

Nun gehen wir zur Dezimaldarstellung der Zahl $P - Q$ über, wobei wir nicht annehmen, P und Q seien in der Gestalt (8) gegeben, aber das Verfahren der Addition im allgemeinen Fall als bekannt voraussetzen.

Es sei $10^n \leq Q < 10^{n+1}$ und $Q = 10^{n+1} - Q'$. Somit ist $P - Q = -10^{n+1} + P + Q'$, und die Dezimaldarstellung der Zahl $P-Q$ ergibt sich leicht aus der Dezimaldarstellung der Zahl $P + Q'$.
Es sei a_{n+1} die in der Entwicklung (7) bei 10^{n+1} stehende Ziffer. Ist $a_{n+1} \geq 1$, so ist das klar, ist aber $a_{n+1} = 0$, so hat man zwei Fälle zu betrachten: $10^{n+1} > P + Q'$ und $10^{n+1} < P + Q'$. Im ersten ist die Zahl $P + Q' - 10^{n+1}$ negativ, und ihre Dezimaldarstellung ergibt sich auf Grund der Darstellung

$$10^{n+1} = 9 \cdot 10^n + 9 \cdot 10^{n-1} + ... + 9 \cdot 10 + 9 + 9 \cdot 10^{-1} + 9 \cdot 10^{-2} + ... \qquad (9)$$

Von dieser Darstellung der Zahl $P + Q'$ kann man einfach stellenweise subtrahieren.
Der Fall $10^{n+1} < P + Q'$ und $a_{n+1} = 0$ wird folgendermaßen behandelt. Es sei a_{n+k} die von links der Zahl a_{n+1} nächst benachbarte von 0 verschiedene Ziffer (eine solche existiert wegen $10^{n+1} < P+Q'$). Dann kann man an Stelle des Summanden $a_{n+k} \cdot 10^{n+k}$ die Summe zweier Summanden schreiben: $(a_{n+k} - 1) \cdot 10^{n+k}$ und 10^{n+k}, von denen sich 10^{n+k} in einer zu (9) analogen Gestalt darstellen lässt.
Danach erhält man die Dezimaldarstellung der Zahl $P + Q' - 10^{n+k}$ entsprechend den bei der Addition erwähnten Vorschriften.

Schon am Beispiel dieser beiden Grundrechenarten mit Zahlen sehen wir, dass Dezimalziffern sich wie Reste bei der Division durch 10 verhalten. Multiplikation und Division reeller Zahlen in Dezimalschreibweise werden auf der Grundlage der Operationen Addition und Subtraktion definiert; wieder erweisen sich die Ziffern als der Arithmetik der Reste modulo 10 gehorchend.

4.2 Darstellung rationaler Zahlen im Positionssystem mit der Grundzahl N

Die Ergebnisse des vorhergehenden Paragraphen zeigen, dass eine Zahl und die Art ihrer Schreibweise (Formel (7)) im Grunde nur durch die Tradition verknüpft sind.
Wir haben mit einem Algorithmus zur Berechnung von Dezimalziffern begonnen, wobei wir von einer beliebigen natürlichen Zahl A ausgingen, und nicht davon, wie diese Zahl geschrieben ist.

Nun ersetzen wir die 10 durch eine andere, beliebige, festgewählte natürliche Zahl N und wiederholen, wenigstens in großen Zügen, die Konstruktion des vorhergehenden Paragraphen.

Zunächst brauchen wir Ziffern, das sind alle möglichen Reste, die bei der Division durch N auftreten, d.h. die Zahlen $0, 1, ..., N-1$. Ist $N = 1$ (das ist ja auch eine natürliche Zahl), so ist 0 die einzige Ziffer. Natürlich kann man mit Hilfe einer einzigen Ziffer nicht alle natürlichen Zahlen aufschreiben. Daher setzen wir $N \geq 2$ voraus.

Es sei A eine beliebige natürliche Zahl. Wir schreiben sie mit Hilfe der Reste bei Division durch N, d.h. mit Hilfe der Zahlen $0, 1, ..., N-1$. Dazu dividieren wir A durch N mit Rest:

$$A = Nq_0 + r_0, \qquad 0 \leq r_0 < N$$

Ist $q_0 = 0$, so ist

$$A = r_0$$

die gesuchte Darstellung der Zahl A in dem Positionssystem mit der Grundzahl N, oder kurz, in dem System mit der Grundzahl N. Ist aber $q_0 \neq 0$, so dividieren wir q_0 durch N mit Rest:

$$q_0 = Nq_1 + r_1, \qquad 0 \leq r_1 < N$$

Dann ist $A = N'q_1 + Nr_1 + r_0$.
Ist $q_1 = 0$, so lautet die gesuchte Darstellung der Zahl A

$$A = r_1 N + r_0$$

Ist aber $q_1 \neq 0$, so setzen wir das Verfahren fort; da $q_1 < q_0$ und $q_0 < A$ ist, nehmen die Quotienten q_0, q_1 usw. ab, bleiben aber ganze nichtnegative Zahlen. Daher erhalten wir nach endlich vielen Schritten den Quotienten $q_k = 0$ und damit eine Darstellung der natürlichen Zahl A im System mit der Grundzahl N:

$$A = r_k N^k + r_{k-1} N^{k-1} + ... + r_1 N + r_0 \tag{10}$$

wobei $r_0, r_1, ..., r_{k-1}$ ganze nichtnegative Zahlen sind, die $N-1$ nicht übertreffen; wir nennen sie die Ziffern im System mit der Grundzahl N.
Die Darstellung (10) einer natürlichen Zahl A ist eindeutig. Sei

$$A = r'_{k'} N^{k'} + r'_{k'-1} N^{k'-1} + ... + r'_1 N + r'_0 \tag{10'}$$

mit ganzen nichtnegativen $r' - k, r'_{k-1}, ..., r'_1, r'_0$, welche höchstens gleich $N-1$ sind, eine zweite Darstellung so würden r'_0 und r_0 als Reste bei Division der Zahl A durch N übereinstimmen, ebenso r'_1 und r_1 als Reste von $\frac{A-r_0}{N} = \frac{A-r'-0}{N}$ usw.

Beispiele

1. Man schreibe die Zahl $A = 722$ im Dualsystem auf.
Ziffern im Dualsystem sind 0 und 1. Wir müssen also $A = 722$ mit Hilfe der Zahlen 0 und 1 schreiben. Um die Reste r_0, r_1, ..., r_k bequem berechnen zu können, fertigen wir uns nacheinander eine Tabelle mit zwei Spalten an: Links sollen die Quotienten $q_0, q_1, ..., q_k$ stehen, rechts die Reste $r_0, r_1, ..., r_k$. Also

722	0
361	

somit ist $r_0 = 0$, $q_0 = 361$. Nächster Schritt:

722	0
361	1
180	

somit ist $r_1 = 1$, $q_1 = 180$. Weiter:

722	0
361	1
180	0
90	

also $r_2 = 0$, $q_2 = 90$. Und schließlich:

722	0
361	1
180	0
90	0
45	1
22	0
11	1
5	1
2	0
1	1
0	

Also lautet die Dualdarstellung von 722:

$$1011010010$$

(Die rechte Spalte der Tabelle (11) muss im Uhrzeigersinne um 90° gedreht werden, um die Antwort zu erhalten.)
Die Darstellung (10) lautet in unserem Fall

$$\begin{aligned} 722 &= 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^6 + 0 \cdot 2^8 + 1 \cdot 2^9 \\ &= 2^9 + 2^7 + 2^6 + 2^4 + 2^2 \end{aligned}$$

2. Man stelle $A = 722$ im System mit der Basis 12 (Duodezimalsystem) dar. Die Ziffern sind $0, 1, 2, ..., 11$. Die Berechnung der Reste $r_0, r_1, ...$ und der Quotienten $q_0, q_1, ...$ schreiben wir wieder in Gestalt einer Tabelle, analog (11):

722	2
60	0
5	5
0	

Die Darstellung von 722 im System mit der Basis 12 lautet also 502, d.h.

$$722 = 2 \cdot 12^0 + 0 \cdot 12 + 5 \cdot 12^2 = 5 \cdot 12^2 + 2$$

3. Man gebe die Zahl $A = 722$ im System mit der Grundzahl 722 an. Hier lautet die Tabelle (11)

722	0
1	1
0	

Daher hat 722 in diesem System die Gestalt 10, also $722 = 0 \cdot 722^0 + 1 \cdot 722$. Um diese 10 nicht mit der üblichen Zahl 10 zu verwechseln, schreiben wir sie **1 0**; das soll darauf hinweisen, dass 1 und 0 als Reste nach dem Modul 722 anzusehen sind.
Es ist interessant, folgende Tatsache festzuhalten: In einem System mit der Grundzahl N wird N in der Gestalt **1 0** geschrieben.

Nun wollen wir die umgekehrte Aufgabe lösen. Es sei eine natürliche Zahl A im System mit der Grundzahl N gegeben. Mit Hilfe von (10) können wir feststellen, wie sie im Dezimalsystem geschrieben aussieht. Dabei haben wir eine Reihe von Multiplikationen und Additionen auszuführen, aber keine Division mit Rest.
Dies erklärt sich daraus, dass wir in jedem Fall mit Zahlen operieren, die im traditionellen Dezimalsystem geschrieben sind - wir haben für kein anderes System Ziffern.
Beispielsweise lautet die Dualzahl **1 0 1 1 0 1 0 0 1 0** im Dezimalsystem $2^9 + 2^7 + 2^6 + 2^4 + 2^2 = 722$.

Würden wir aber versuchen, die Dezimaldarstellung dieser Zahl mit Hilfe des oben beschriebenen Verfahrens der Division mit Rest zu erhalten, so müssten wir **1 0 1 1 0 1 0 0 1 0** durch die Zahl 10 dividieren, die im Dualsystem **1 0 1 0** lautet. Zur Veranschaulichung führen wir die entsprechende Tabelle zur Berechnung der Reste bei der Division durch **1 0 1 0** hier an:

$$\begin{array}{l} 1011010010 : 1010 = 1001000 \\ \underline{-1010} \\ 1010 \\ \underline{1010} \\ 010 \end{array}$$

Daher ist der Quotient gleich **1 0 0 1 0 0 0**, der Rest **1 0**. Die nächste Etappe:

$$\begin{array}{l} 1001000 : 1010 = 111 \\ \underline{-1010} \\ 10000 \\ \underline{-1010} \\ 1100 \\ \underline{-1010} \\ 10 \end{array}$$

Der Quotient ist **1 1 1**, der Rest **1 0**. Schließlich vereinigen wir dies alles in der traditionellen Tabelle der Reste und Quotienten:

$$\begin{array}{r|l} \mathbf{1\,0\,1\,1\,0\,1\,0\,0\,1\,0} & \mathbf{1\,0} \\ \mathbf{1\,0\,0\,1\,0\,0\,0} & \mathbf{1\,0} \\ \mathbf{1\,1\,1} & \mathbf{1\,1\,1} \\ \mathbf{0} & \end{array}$$

Natürlich bedeutet $\overline{\underbrace{\mathbf{1\,1\,1}}\underbrace{\mathbf{1\,0}}_{2}\underbrace{\mathbf{1\,0}}_{2}}$ die Zahl 722, nur sind die Ziffern hier im Dualsystem geschrieben. (Darauf sollen die oberen Striche hinweisen.)

Dieses Beispiel, das die Art der Übertragung einer Zahl aus dem Dual- system in das Dezimalsystem zeigt, macht deutlich, dass die arithmetischen Operationen mit Zahlen in demjenigen System ausgeführt werden können, in dem sie geschrieben sind, ohne dass zum Dezimalsystem übergegangen werden muss.

Jetzt verallgemeinern wir unsere Überlegungen.

Es seien $A = a_n a_{n-1}...a_1 a_0$ und $B = b_m b_{m-1}...b_1 b_0$ im System mit der Grundzahl N dargestellte natürliche Zahlen, also $a_n, ..., a_0, b_m..., b_0$ Ziffern im System mit der Grundzahl N. Dann schreibt man die Addition $A + B$ am zweckmäßigsten

$$\begin{array}{rl} & a_n a_{n-1}...a_1 a_0 \\ + & b_m b_{m-1}...b_1 b_0 \\ \hline & \end{array}$$

Addieren wir a_0 und b_0, so erhalten wir $d_0 + c_0$, mit $0 \leq c_0 < N_1$ und $0 \leq d_0 \leq 1$; daher muss unter a_0 und b_0 in (12) die Ziffer c_0 geschrieben werden. Dann addieren wir a_1, b_1 und d_0 und stellen die Summe wieder in der Gestalt $d_1 + c_1$ dar, so dass in (12) unter a_1 und b_1 die Ziffer c_1 geschrieben werden muss, usw.

Beispiel. Es sei $N = 3$, $A =$ **2 1 1 1 0 0 1**, $B =$ **2 0 1 0 2 12** . Wir erhalten die Summe $A + B$

$$\begin{array}{r} \mathbf{2\,1\,1\,1\,0\,0\,1} \\ \mathbf{2\,0\,1\,0\,2\,1\,2} \\ \hline \mathbf{1\,1\,1\,2\,1\,2\,2\,0} \end{array}$$

Nun gehen wir zur Subtraktion über. Hier muss man zunächst feststellen, welche der Zahlen A, B die größere ist. Ist $n > m$, so ist, wie aus der Darstellung (10) folgt, $A > B$; für $n < m$ ist natürlich $A < B$. Im Fall $n = m$ muss man $\mathbf{a}_n$ und $\mathbf{b}_n$ vergleichen. Für $\mathbf{a}_n > \mathbf{b}_n$ ist natürlich $A > B$, im Fall $\mathbf{a}_n < \mathbf{b}_n$ offenbar $A < B$. Ist $\mathbf{a}_n = \mathbf{b}_n$, so muss man $\mathbf{a}_{n-1}$ und $\mathbf{b}_{n-1}$ vergleichen usw.
Stellt sich heraus, dass $\mathbf{a}_n = \mathbf{b}_n, \mathbf{a}_{n-1} = \mathbf{b}_{n-1}, ..., \mathbf{a}_0 = \mathbf{b}_0$ ist, so ist natürlich $A = B$. Beispielsweise ist für $N = 2$ die Zahl 101101001001 größer als die Zahl 101101000111.

Bei der Berechnung der Differenz $A - B$ muss man zunächst klären, ob $A \geq B$ oder $A < B$ gilt. Ist $A < B$, so muss man die Differenz $B - A$ berechnen und vor das Ergebnis ein Minuszeichen setzen. Jetzt nehmen wir $A \geq B$ an. Die Subtraktionsaufgabe $A - B$ schreiben wir wieder "spaltenweise" :

$$\begin{array}{rr} & a_n a_{n-1} ... a_2 a_1 a_0 \\ - & \quad b_m ... b_2 b_1 b_0 \\ \hline \end{array}$$

wobei unter jeder der Zeilen eine abgekürzte Schreibweise der rechten Seite der Formel (10) zu verstehen ist.
Ist $\mathbf{a}_0 \geq \mathbf{b}_0$„ so schreiben wir unter $\mathbf{a}_0$ und $\mathbf{b}_0$ die Ziffer $c_0 = a_0 - b_0$ (im System zur Basis N). Ist aber $a_0 < b_0$ und $a_1 > 0$, so "leihen" wir bei a_1 "eine Einheit" und setzen $c_0 = N + a_0 - b_0$.
Danach steht in der obigen Tabelle natürlich statt $\mathbf{a}_1$ die Ziffer $\overline{\mathbf{a}_1 - 1}$.

Ist aber $a_1 = 0$ und $a_2 > 0$, so muss man die "Einheit bei a_2 ausleihen", d.h. die Zahl in der Gestalt

$$\begin{aligned} A &= ... + (a_2 - 1)N + N^2 + a_0 = ... + (a_2 - 1)N^2 + N^2 - N + N + a_0 \\ &= ... + (a_2 - 1)N^2 + (N_1)N + N + a_0 \end{aligned}$$

darstellen. Dann ist $c_0 = N + a_0 - b_0$, und c_1, die unter a_1 und b_1 stehende Ziffer, ist gleich $N - a_1 - b_1$. Ist aber auch $a_2 = 0$, jedoch $a_3 > 0$, so muss man diese Überlegung wiederholen, also A in der Gestalt

$$\begin{aligned} A &= ... + a_3 N^3 + a_0 = ... + (a_3 - 1)N^3 + N^3 + a_0 \\ &= ... + (a_3 - 1)N^3 + N^3 - N^2 + N^2 - N + N + a_0 \\ &= ... + (a_3 - 1)N^3 + (N_1)N^2 + (N_1)N + N + a_0 \end{aligned}$$

darstellen. Im Fall $a_3 = 0$ weiß der Leser schon, was zu tun ist.

Beispiel. Es sei $N = 8$, $A =$ **7 2 4 1 3 5**, **B = 2 6 8 5 4 1 0**. Man bestimme $A - B$. Wegen $B > A$ haben wir so zu rechnen:

$$\begin{array}{rr} & \mathbf{2\ 6\ 3\ 5\ 4\ 1\ 0} \\ - & \quad \mathbf{7\ 2\ 4\ 1\ 3\ 5} \\ \hline & \mathbf{1\ 7\ 1\ 1\ 2\ 5\ 3} \end{array}$$

Die gesuchte Differenz ist also -**1 7 1 1 2 5 3**.

Bisher haben wir Addition und Subtraktion im System mit der Grundzahl N untersucht. Da Multiplikation und Division mit Rest sich darauf zurückführen lassen, verfügen wir jetzt über alles Nötige, um auch diese Operationen im System mit der Grundzahl N auszuführen zu können.

Wir betrachten jetzt den Bruch

$$R = r_{-1} \cdot 10^{-1} + r_2 \cdot 10^{-2} + ...$$

Wie die Dezimalziffern dieses Bruches zu berechnen sind, haben wir im vorigen Paragraphen beschrieben. Unser nächstes Ziel besteht nun darin, diesen Bruch R in der Gestalt

$$R = a_{-1} N^{-1} + a_{-2} N^{-2} + ...$$

darzustellen, wobei a_{-1}, a_{-2} Ziffern im System mit der Grundzahl N sind. Offenbar ist a_{-1} der ganze Teil der Zahl NR (natürlich ist $a_{-1} < N$, da $R < 1$, also $NR < N$ ist; daher ist a_{-1} eine Ziffer im System mit der Grundzahl N.
Analog ist a_{-2} der ganze Teil der Zahl $N(NR - a_{-1})$, d.h. der Zahl $N^2R - Na_{-1}$ allgemein also a_{-k} der ganze Teil der Zahl

$$N^{-k}R - Nk - 1a_{-1} - N^{k-2}a_{-2} - ... - Na_{-k+1}$$

Beispiel. Man stelle den Bruch $R = 0,0875$ im System mit der Grundzahl 9 dar. Die Zwischenergebnisse schreibt man auch hier zweckmäßigerweise in Tabellenform auf: Links stehen die Brüche, rechts die ganzen Teile des Produktes dieser Brüche mit $N = 9$.

0875	0
7875	7
0875	0
7875	7
0875	

Daher ist im System zur Basis 9 der endliche Dezimalbruch $R = 0,0875$ der unendliche periodische Dezimalbruch

$$0,\overline{07}07...$$

mit der Periodenlänge 2, der kleinsten natürlichen Zahl unter denjenigen Zahlen n, für welche $9^n \equiv 1 \pmod{M}$ ist; dabei ist M der Nenner des Bruches R, wenn man diesen als rationale Zahl schreibt: $R = \frac{7}{80}$, $M = 80$. Die Zahl 80 ist ja zu 9 teilerfremd.

Die Umwandlung eines endlichen Dezimalbruches in einen unendlichen periodischen Bruch in einem System zu einer anderen Grundzahl verdient besondere Aufmerksamkeit. Zunächst halten wir fest: Ist eine rationale Zahl $R = \frac{A}{B}$ (mit $(A, B) = 1$) ein unendlicher periodischer Dezimalbruch, so ist im System mit der Grundzahl B dieser Bruch endlich. Nach Satz 3 aus § 1 erhält man die Länge der Periode des Bruches R im Dezimalsystem folgendermaßen. Man stellt B in der Gestalt $2^r \cdot 5^s \cdot B'$ mit $(10, B') = 1$ dar, dann bestimmt man die kleinste natürliche Zahl n, für welche $10^n \equiv 1 \pmod{B'}$ ist. Es gilt

Satz 4. Es sei $N \geq 2$ eine natürliche Zahl und $R = \frac{A}{B}$ eine rationale Zahl, $(A, B) = 1$. Ferner sei $B = B'B''$ eine Darstellung der Zahl B mit $(B', N) = 1$ derart, dass jeder Primteiler des Faktors B'' ein Teiler von N ist.
Dann ist die Periodenlänge des Bruches R im System mit der Grundzahl N, welcher die Zahl R darstellt, die kleinste derjenigen natürlichen Zahlen n, für welche $N^n \equiv 1 \pmod{B'}$ ist.

Wir überlassen es dem Leser, den Beweis für diesen Satz unter Zugrundelegung des Beweises von Satz 3 selbständig zu finden.

Somit ist eine rationale Zahl im System mit der Grundzahl N ein endlicher oder ein unendlicher periodischer Bruch; eine irrationale Zahl aber ist in jedem System ein nicht-periodischer Bruch. Denn ließe sie sich in irgendeinem System als periodischer Bruch darstellen, so könnte man diesen durch eine Umformung der beschriebenen Art in einen

Quotienten zweier ganzer Zahlen umwandeln, was der Definition einer irrationalen Zahl widerspricht.

Endliche Brüche im System zur Basis N werden zweckmäßigerweise "spaltenweise" wie ganze Zahlen addiert und subtrahiert.

Jetzt betrachten wir Teilbarkeitskriterien. In Satz 1 dieses Kapitels steckt nämlich eine Information, die sich mit Erfolg auf Systeme mit der Basis N verallgemeinern lässt.

Satz 5. Die Differenz zwischen einer natürlichen Zahl A und der Summe ihrer Ziffern im System mit der Grundzahl N ist durch $N-1$ teilbar.

Zum Beweis brauchen wir nur die Darstellung (10) heranzuziehen, aus der sich folgendes ergibt:

$$A = (r_0 + ... + r_k) = r_k(N^k - 1) + r_{k-1}(N^{k-1} - 1) + ... + r_1(N - 1)$$

Bekanntlich ist aber $N^s - 1 = (N-1)(N^{s-1} + N^{s-2} + ... + N + 1)$, und damit ist alles bewiesen.

Somit ist eine Zahl A genau dann durch einen Teiler von $N-1$ teilbar, wenn dieser Teiler der Summe der Ziffern der Zahl A im System mit der Grundzahl N ist.
Stellt man beispielsweise eine Zahl A im System mit der Grundzahl B dar, so ergibt sich sofort, ob sie durch 7 teilbar ist: Man addiert ihre Ziffern und untersucht, ob diese Summe durch 7 teilbar ist.
Beispielsweise ist die Zahl **7 6 1 2 5** (im System mit der Basis 8) durch 7 teilbar, da die Ziffernsumme 21 durch 7 teilbar ist. Im Dezimalsystem geschrieben lautet diese Zahl 31829.

Für $N = 2$ ist die Aussage wegen $N - 1 = 1$ trivial. Daher ist im Sinne von Satz 5 das Dualsystem ungeeignet. Will man feststellen, ob eine im Dualsystem geschriebene Zahl durch irgendeine Zahl teilbar ist, so muss man entweder die Division mit Rest ausführen oder zu einem anderen System übergeben, in dem man die Antwort auf diese Frage einfacher erhält.

4.3 Systeme mit der Grundzahl N und mit der Grundzahl N^k

Solche Systeme haben im Zusammenhang mit den elektronischen Rechenautomaten eine größere Bedeutung erlangt.
Jede Dualzahl enthält nur die Ziffern 0 und 1. Da eine einfache Elektronenröhre (oder ein anderes elektronisches Element) zwei Zustände kennt, nämlich "stromdurchlässig" und "stromundurchlässig" ("eingeschaltet" oder "ausgeschaltet"), kann man dem ersten Zustand die Ziffer 1, dem zweiten die Ziffer 0 zuordnen.
Mit n solchen Ziffern kann man dann jede n-ziffrige Dualzahl darstellen. Auf diesem Prinzip beruht die Arbeitsweise von Elektronenrechnern; die Zahlen werden ins Dualsystem übertragen, und dann werden bestimmte Rechenoperationen ausgeführt.

An den Beispielen des vorigen Paragraphen hat der Leser erstens feststellen können, dass die Dualschreibweise schon bei relativ kleinen Zahlen viele Dualziffern erfordert:

Schon die Zahl 722 ist im Dualsystem zehnstellig. Daher werden die Zahlen nur vor ihrer Eingabe in die Maschine ins Dualsystem übertragen, dann aber so dargestellt, dass erstens weniger Stellen gebraucht werden, und zweitens, dass der Übergang zum Dualsystem direkter geschehen kann als im Dezimalsystem.

Beispielsweise sei $A = 30213$ eine Zahl im System mit der Grundzahl 4. Wie schreibt sie sich im Dualsystem? Nach (10) ist

$$A = 3\cdot 4^4+2\cdot 4^2+1\cdot 4+3 = (2+1)\cdot 2^8+2\cdot 2^4+1\cdot 2^2+2+1 = 2^9+2^8+2^5+2^2+2+1$$

Daher ist $A = \mathbf{1\,1\,0\,0\,1\,0\,0\,1\,1\,1}$ die Dualdarstellung. Mit anderen Worten, wir haben jede Ziffer der Zahl A im System mit der Grundzahl 4 in Dualziffern geschrieben und damit die Antwort erhalten. Dies lässt sich anhand des Resultates leicht verifizieren.

Wir führen nun die entsprechenden Überlegungen für den allgemeinen Fall durch:

$$A = a_{2n}\cdot 2^{2n} + a_{2n-1}\cdot 2^{2n-1} + ... + a_3\cdot 2^3 + a_2\cdot 2^2 + a_1\cdot 2 + a_0 \qquad (12)$$

dabei kann $a_{2n} = 0$ sein (wir brauchen eine gerade Anzahl von Ziffern), $a_0, a_1, ..., a_{2n}$ sind Dualziffern, d.h. die Zahlen 0 und 1.
Die Zahl $a_1\cdot 2 + a_0$ ist nicht größer als 3, kann also eine Ziffer im System mit der Grundzahl 4 sein. Nun betrachten wir die beiden folgenden Summanden:

$$a_3\cdot 2^3 + a_2\cdot 2^2 = (a_3\cdot 2 + a_2)\cdot 2^2$$

d.h., das ist eine Ziffer im System mit der Grundzahl 4, multipliziert mit 4. Das folgende Paar ist wieder eine solche Ziffer, multipliziert mit $2^4 = 4^2$ usw. Benutzen wir eine zur Darstellung (12) analoge Darstellung, so kommen wir zu folgender Regel:

Um von der Darstellung einer natürlichen Zahl A im System mit der Grundzahl N zur Darstellung im System mit der Grundzahl N^k überzugehen, muss man zunächst die Ziffern von A im System mit der Grundzahl N von rechts nach links in die Blöcke zu je k Ziffern einteilen und dann jede dieser k-stelligen Zahlen mit Hilfe von (10) als "einstellige" Zahl schreiben.

Den umgekehrten Übergang vollzieht man folgendermaßen: Jede Ziffer von A im System mit der Grundzahl N^k schreibt man als k-stellige Zahl im System mit der Grundzahl N. Auf diese Weise erhält man die Darstellung von A im System mit der Grundzahl N.

Bemerkung. Jede Ziffer im System mit der Grundzahl N^k schreibt sich mit höchstens k Ziffern im System mit der Grundzahl N, da N^k im System mit der Grundzahl N die Gestalt $\underbrace{10...0}_{k}$ hat. Wir vereinbaren, falls zur Darstellung einer Ziffer des Systems mit der Grundzahl N^k als Zahl im System mit der Grundzahl N nur $l < k$ Ziffern benötigt werden, dass diese Darstellung durch Voranstellen von $k-l$ Nullen ergänzt wird. Diese Festlegung steht im Einklang mit (10).

Statt eines Beweises, der nach Einführung entsprechender Bezeichnungen leicht zu erbringen ist, erläutern wir die Regel an zwei Beispielen.

Es sei $A =$ **9 7 5** im System mit der Grundzahl 27. Wir gehen zum System mit der Grundzahl 3 über. Für die 9 im System mit der Grundzahl 27 haben wir im System mit der Grundzahl 3 offenbar **1 0 0** zu schreiben, für 7 offenbar **0 2 1**, und für 5 schließlich **0 1 2**.
Die gesuchte Darstellung für **9 7 5** lautet also **1 0 0 0 2 1 0 1 2**.

Es sei $A =$ **7 8 10 15 10 9** eine Zahl im System mit der Grundzahl 16. Wir wollen sie in das System mit der Grundzahl 256 "übersetzen". Die Zahl **10 9** im System mit der Grundzahl 16 geht über in **169**, die Zahl **10 15** in **175**, die Zahl **7 8** in **120**. Im System mit der Grundzahl 256 haben wir also **120 175 169**.

5 Literatur

Basmakova, I. G., Diophant und diophantische Gleichungen, VEB Deutscher Verlag der Wissenschaften, Berlin / Birkhäuser-Verlag, Basel und Stuttgart 1974 (Übersetzung aus dem Russischen).

Chintschin, A. J., Die Elemente der Zahlentheorie, in: Enzyklopädie der Elementarmathematik, Bd. I, 8. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1978 (Übersetzung aus dem Russischen).

Dynkin, E. B., und W. A. Uspenski, Mathematische Unterhaltungen II: Aufgaben aus der Zahlentheorie, 5. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1977 (Übersetzung aus dem Russischen).

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

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

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

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

Koch, H., und H. Pieper, Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1976.

Krätzel, E., Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1981.

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

Sominski, I. S., Die Methode der vollständigen Induktion, 13. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1982 (Übersetzung aus dem Russischen).

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

Worobjow, N. N., Teilbarkeitskriterien, 3., ber. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1977 (Übersetzung aus dem Russischen).