Kapitel 1
Zahlen

Die klassische Algebra der Ägypter, Babylonier und Griechen beschäftigte sich vorwiegend mit dem Lösen von Gleichungen. Im Zentrum der Untersuchungen der modernen Algebra liegen hingegen algebraische Operationen, wie zum Beispiel die Addition und die Multiplikation ganzer Zahlen. Das Ziel dieses Kapitels besteht darin, die wichtigsten Grundbegriffe der Algebra darzustellen. Dazu ist es notwendig, sich in eine abstrakte Begriffswelt zu begeben. Um dies zu erleichtern, beginnen wir mit einem Studium der grundlegenden Eigenschaften ganzer Zahlen. Besonderer Wert wird auch auf die Vermittlung wichtiger Beweistechniken gelegt. Die Bildung von Äquivalenzklassen ist eine fundamentale mathematische Konstruktionsmethode und wird daher ausführlich erläutert. Viele der hier vorgestellten praktischen Anwendungen beruhen darauf. Als informatikbezogene Anwendung wird am Ende des Kapitels erläutert, wie die Grundbegriffe der Algebra für sinnvolle und praxisrelevante Prüfzeichen- und Chiffrierverfahren eingesetzt werden.

1.1 Rechnen mit ganzen Zahlen

Die ganzen Zahlen dienen als Modell für alle weiteren algebraischen Strukturen, die wir in diesem Kapitel untersuchen. Als Vorbereitung auf die axiomatische Einführung abstrakterer Begriffe konzentrieren wir uns auf die grundlegenden Eigenschaften der Rechenoperationen mit ganzen Zahlen. Außerdem lernen wir das Prinzip der vollständigen Induktion und den Euklidischen Algorithmus kennen. Das sind wichtige Werkzeuge für den Alltagsgebrauch eines Informatikers.
Auf eine axiomatische Einführung der natürlichen Zahlen wird hier bewusst verzichtet. Der interessierte Leser findet eine solche in [EbZ].
Für die Gesamtheit aller ganzen Zahlen hat sich das Symbol $\mathbb{Z}$ eingebürgert:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} .$$

Die Summe, das Produkt und die Differenz (jedoch nicht der Quotient) zweier ganzer Zahlen ist stets eine ganze Zahl. Die Addition und die Multiplikation sind die Operationen auf die sich das algebraische Studium der ganzen Zahlen gründet. Wir listen hier in aller Ausführlichkeit ihre wesentlichen Eigenschaften auf. Das hilft uns später, abstraktere Begriffe wie Gruppe, Ring und Körper besser zu verstehen. Für beliebige ganze Zahlen $a, b, c \in \mathbb{Z}$ gilt:

Kommutativgesetz der Addition	$a + b = b + a$	(1.1)
Assoziativgesetz der Addition	$(a + b) + c = a + (b + c)$	(1.2)
Gesetz vom additiven neutralen Element	$a + 0 = a$	(1.3)
Gesetz vom additiven inversen Element	$a + (-a) = 0$	(1.4)
Kommutativgesetz der Multiplikation	$a \cdot b = b \cdot a$	(1.5)
Assoziativgesetz der Multiplikation	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(1.6)
Gesetz vom multipl. neutralen Element	$1 \cdot a = a$	(1.7)
Distributivgesetz	$a \cdot (b + c) = a \cdot b + a \cdot c$	(1.8)

Das Gesetz vom inversen Element (1.4) ist folgendermaßen zu lesen:

Zu jeder ganzen Zahl a gibt es eine ganze Zahl $-a$, für die $a + (-a) = 0$ ist.

Es wird hier nicht gesagt, dass $-a$ durch die gegebene Zahl a eindeutig festgelegt ist. Ein erstes Indiz dafür, welches Potenzial in diesen acht Gesetzen steckt ist, dass sie die Eindeutigkeit von $-a$ erzwingen. Das sehen wir wie folgt: Wenn wir annehmen, dass $x, y \in \mathbb{Z}$ Zahlen sind, für die $a + x = 0$ und $a + y = 0$ gilt, dann folgt mit (1.3), (1.2) und (1.1)

$$x = x + 0 = x + (a + y) = (x + a) + y = 0 + y = y\,.$$

Wir haben also unter alleiniger Benutzung der Gesetze (1.1), (1.2) und (1.3) gezeigt, dass die Gleichung $a + x = 0$ höchstens eine Lösung besitzen kann. Das Gesetz (1.4) beinhaltet nun die Aussage, dass es eine solche Lösung tatsächlich gibt. Ein weiteres Beispiel der ausschließlichen Benutzung der Gesetze (1.1)–(1.8) ist die folgende Herleitung der wohlbekannten Gleichung $(-1) \cdot (-1) = 1$:

$$\begin{aligned}
1 &= 1 + 0 \cdot (-1) && \text{wegen (1.3)}\\
&= 1 + \big(1 + (-1)\big) \cdot (-1) && \text{wegen (1.4)}\\
&= 1 + \big(1 \cdot (-1) + (-1) \cdot (-1)\big) && \text{wegen (1.8)}\\
&= \big(1 + (-1)\big) + (-1) \cdot (-1) && \text{wegen (1.2) und (1.7)}\\
&= (-1) \cdot (-1) && \text{wegen (1.3) und (1.4).}
\end{aligned}$$

Bei der ersten Umformung benutzen wir, dass für alle ganzen Zahlen a die Gleichung $0 \cdot a = 0$ gilt. Um dies aus den Grundregeln abzuleiten, bemerken wir zunächst, dass die Gleichungen $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ aus

(1.3) und (1.8) folgen. Nach Addition von $-(a \cdot 0)$ ergibt sich daraus, unter Benutzung von (1.4) und (1.2), die Gleichung $0 = a \cdot 0$. Kommutativität der Multiplikation (1.5) liefert schließlich $0 \cdot a = 0$.
Derartig elementare Rechnungen sind wichtig, weil wir sie auf abstraktem Niveau wiederholen können. Im Verlauf dieses Kapitels werden wir lernen, mit mathematischen Strukturen umzugehen, bei denen nur noch die algebraischen Operationen an unsere konkrete Erfahrung mit ganzen Zahlen angelehnt sind, nicht aber die Objekte, mit denen wir operieren. In Beweisen können wir dann ausschließlich auf Grundregeln wie (1.1)–(1.8) zurückgreifen. Diese werden als Axiome (das heißt zu Beginn vorgegebene, charakteristische Eigenschaften) der betrachteten Struktur bezeichnet.
Die Fähigkeit, Argumentationen auf der Grundlage einer kleinen Zahl klar vorgegebener Regeln zu führen, ist für die exakten Wissenschaften so wichtig, dass sie von Anfang an und kontinuierlich trainiert werden muss. Wenn Sie die bisher angegebenen Beweise elementarer Aussagen nur überflogen haben, dann empfehlen wir Ihnen deshalb, dass Sie sich vor dem Weiterlesen nochmals etwas intensiver damit beschäftigen.

Solche Begriffe wie *Teiler* und *Primzahl* sind dem Leser vermutlich bereits vertraut. Wir werden sie hier kurz wiederholen, um von vornherein mit klaren und einheitlichen Begriffen zu operieren. Eine derartige Vorgehensweise ist in Mathematik und Informatik von prinzipieller Wichtigkeit, um Missverständnisse, nicht funktionierende Software oder gar Milliardenverluste zu vermeiden.
Eine ganze Zahl b heißt *Teiler* der ganzen Zahl a, falls es eine ganze Zahl c gibt, so dass $bc = a$ gilt. Wir schreiben dann $b \mid a$ (sprich: b teilt a).
So hat zum Beispiel $a = 6$ die Teiler $-6, -3, -2, -1, 1, 2, 3, 6$. Die Zahl $a = 0$ ist die einzige ganze Zahl, die unendlich viele Teiler besitzt. Entsprechend unserer Definition ist sie durch jede ganze Zahl teilbar. Jede ganze Zahl a hat mindestens die Teiler $-a, -1, 1, a$, und wenn $a \neq \pm 1, 0$ ist, sind dies vier verschiedene Teiler. Außer $a = 0$ besitzt keine ganze Zahl den Teiler 0.
Wir nennen eine Zahl $a \in \mathbb{Z}$ *zusammengesetzt*, wenn es ganze Zahlen $b \neq \pm 1$, $c \neq \pm 1$ gibt, so dass $a = bc$. Eine von ± 1 verschiedene Zahl, die nicht zusammengesetzt ist, nennt man *Primzahl*. Da $0 = 0 \cdot 2$ gilt, ist 0 zusammengesetzt, also keine Primzahl. Da $2 = 1 \cdot 2$ und $2 = (-1) \cdot (-2)$ bis auf die Reihenfolge der Faktoren die einzigen Darstellungen von $a = 2$ als Produkt zweier ganzer Zahlen sind, ist 2 eine Primzahl.
Eine Zahl c heißt *gemeinsamer Teiler* von a und b falls $c \mid a$ und $c \mid b$. Wir nennen zwei Zahlen *teilerfremd*, wenn 1 und -1 die einzigen gemeinsamen Teiler dieser Zahlen sind.

Definition 1.1.1. Seien $a \neq 0$, $b \neq 0$ ganze Zahlen. Wir nennen eine positive ganze Zahl $d > 0$ *größten gemeinsamen Teiler* von a und b, wenn die folgenden beiden Bedingungen erfüllt sind:

(i) (gemeinsamer Teiler) $d \mid a$ und $d \mid b$;
(ii) (Maximalität) Für jedes $c \in \mathbb{Z}$ gilt: Wenn $c \mid a$ und $c \mid b$, dann gilt $c \mid d$.

Wenn diese Eigenschaften erfüllt sind, schreiben wir $d = \mathrm{ggT}(a, b)$.

Beachten Sie hier, dass die Bedingung (ii) *nicht* lautet „d ist die größte ganze Zahl, die (i) erfüllt“. Vergleichen Sie dies jedoch mit Aufgabe 1.2.
Diese Definition führt zu unseren ersten mathematischen Problemen:

> Gibt es für beliebige $a, b \in \mathbb{Z}$ stets einen größten gemeinsamen Teiler?
> Wenn ja, ist dieser dann eindeutig bestimmt?
> Wie kann man ihn berechnen?

Die Antworten sind Ihnen vermutlich bekannt. Wir wollen diese Fragen hier jedoch nicht nur beantworten, sondern unsere Antworten auch begründen. Wir werden die Existenz und Eindeutigkeit des größten gemeinsamen Teilers *beweisen*. Die Existenz werden wir mit Hilfe des Euklidischen Algorithmus nachweisen, der uns außerdem ein effektives Mittel für seine Berechnung in die Hand gibt. Ohne eine Berechnungsmethode zu kennen und ohne den Nachweis der Existenz geführt zu haben, werden wir zunächst die Eindeutigkeit des größten gemeinsamen Teilers beweisen.

Satz 1.1.2 *Zu gegebenen ganzen Zahlen $a \neq 0, b \neq 0$ gibt es höchstens einen größten gemeinsamen Teiler.*

Beweis. Angenommen d und d' seien größte gemeinsame Teiler von a und b im Sinne von Definition 1.1.1. Dann gilt

(1) $d \mid a$ und $d \mid b$;
(2) $d' \mid a$ und $d' \mid b$;
(3) Wenn $c \in \mathbb{Z}$, so dass $c \mid a$ und $c \mid b$, dann gilt $c \mid d$ und $c \mid d'$.

Aus (1) und (3) mit $c = d$ ergibt sich $d \mid d'$. Ebenso folgt aus (2) und (3) mit $c = d'$, dass $d' \mid d$ gilt. Daher gibt es ganze Zahlen r, s mit $d' = d \cdot r$ und $d = d' \cdot s$. Das heißt $d = d \cdot r \cdot s$ und somit $r \cdot s = 1$. Also muss $r = s = 1$ oder $r = s = -1$ gelten. Da aber d und d' positive ganze Zahlen sind, ist $r = s = 1$ und wir erhalten $d = d'$. □

Der *Euklidische*[1] *Algorithmus* ist einer der ältesten und grundlegendsten Algorithmen der Mathematik. Uns dient er hier sowohl als Beweistechnik als auch als Methode für konkrete Rechnungen. Sein mathematisches Kernstück ist die *Division mit Rest*. Darunter verstehen wir die folgende Eigenschaft ganzer Zahlen, die sich nicht aus den Grundregeln (1.1)–(1.8) ergibt, da die Ordnungsrelation $<$ darin auftritt:

> Wenn $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann gibt es ganze Zahlen r und n,
> so dass $\quad a = nb + r \quad$ und $\quad 0 \leq r < |b| \quad$ gilt.

[1] Euklid von Alexandria wirkte um 300 v.u.Z. in Alexandria, genaue Lebensdaten und sichere Information, ob es sich wirklich um eine einzelne Person handelt, sind nicht bekannt. Vgl. Fußnote auf Seite 76.

Die Zahl r heißt *Rest von a bei Division durch b*. Hier und im Folgenden bezeichnet $|b|$ den Betrag der ganzen Zahl b, das heißt $|b| = b$ wenn $b \geq 0$ und $|b| = -b$ wenn $b \leq 0$. Verallgemeinerungen des hier vorgestellten Euklidischen Algorithmus, etwa für Polynome oder Gaußsche ganze Zahlen, beruhen jeweils auf einer entsprechend angepassten Version der Division mit Rest.

Der Euklidische Algorithmus

Als Eingabedaten seien zwei positive ganze Zahlen a, b mit $a > b$ gegeben. Am Ende wird $\mathrm{ggT}(a, b)$ ausgegeben.
Jeder Schritt des Algorithmus besteht aus einer Division mit Rest, gefolgt von einem Test, in dem entschieden wird, ob das Ende bereits erreicht wurde.

Initialisierung: $A := a$, $B := b$
Division: Bestimme $N \in \mathbb{Z}$, so dass $0 \leq A - N \cdot B < B$.
$C := A - N \cdot B$ ist der Rest von A bei Division durch B.
Test: Wenn $C = 0$, dann Ausgabe von $\mathrm{ggT}(a, b) := B$ und stopp.
Wenn $C > 0$, dann Division mit Rest für $A := B$, $B := C$.

Wie bei jedem Algorithmus sind zunächst folgende Fragen zu klären:

Endet dieser Algorithmus stets nach endlich vielen Schritten?
Liefert er wirklich den größten gemeinsamen Teiler?

Um diese Fragen zu beantworten, schauen wir uns den Algorithmus Schritt für Schritt an. Wir setzen $a_1 := a$, $b_1 := b$. Bei jedem Schritt wird ein neues Paar von Zahlen (a_k, b_k) produziert. Das neue Paar (a_k, b_k) ergibt sich für jedes $k \geq 1$ aus dem vorherigen durch folgende Formeln:

$$\begin{aligned} b_{k+1} &= a_k - n_k b_k \\ a_{k+1} &= b_k \ . \end{aligned}$$

Hier ist n_k eine geeignete ganze Zahl und es gilt stets $0 \leq b_{k+1} < b_k$. Nach dem k-ten Schritt liegt uns das Paar (a_{k+1}, b_{k+1}) vor. Nach dem N-ten Schritt stoppt der Algorithmus genau dann, wenn $b_{N+1} = 0$ gilt. In diesem Fall ist $0 = a_N - n_N \cdot b_N$ und für die Korrektheit des Algorithmus wäre zu beweisen, dass $b_N = \mathrm{ggT}(a, b)$ gilt. Schauen wir uns zunächst ein Beispiel an.

k	(a_k, b_k)	$a_k - n_k b_k = b_{k+1}$
1	$(287, 84)$	$287 - 3 \cdot 84 = 35$
2	$(84, 35)$	$84 - 2 \cdot 35 = 14$
3	$(35, 14)$	$35 - 2 \cdot 14 = 7$
4	$(14, 7)$	$14 - 2 \cdot 7 = 0$

Wir haben hier $N = 4$, $b_4 = 7$ und es gilt tatsächlich $\mathrm{ggT}(287, 84) = 7$.

Bemerkung 1.1.3. Pro Schritt produziert der Algorithmus nicht zwei, sondern nur eine neue Zahl, nämlich b_{k+1}. Wenn wir $b_0 := a_1$ setzen, dann

können wir die Berechnung in jedem Schritt des Algorithmus auch in der Form

$$b_{k+1} = b_{k-1} - n_k b_k$$

schreiben. Dabei soll wieder $0 \leq b_{k+1} < b_k$ gelten. Der Algorithmus terminiert, sobald $b_{k+1} = 0$ ist.

Da $b_1 > b_2 > \ldots > b_n \geq 0$ und die b_i ganze Zahlen sind, ist nach maximal b_1 Schritten sicher die Bedingung $b_{k+1} = 0$ erfüllt. Die *Endlichkeit* des Algorithmus ist damit garantiert.
Die *Korrektheit* des Euklidischen Algorithmus wird mittels vollständiger Induktion bewiesen. Da diese Beweistechnik häufig verwendet wird und hier zum ersten Mal auftritt, stellen wir sie sehr ausführlich dar.

Satz 1.1.4 *Der Euklidische Algorithmus berechnet den größten gemeinsamen Teiler.*

Beweis. Sei N die Zahl der Schritte im Euklidischen Algorithmus, das heißt

$$0 = a_N - n_N b_N \quad \text{und} \quad b_1 > b_2 > \ldots > b_N > b_{N+1} = 0\,.$$

Zu zeigen ist $b_N = \mathrm{ggT}(a_1, b_1)$. Die Induktion wird über N, die Anzahl der Schritte, durchgeführt.
Induktionsanfang: Als erstes beweisen wir den Satz für den Fall $N = 1$. Dazu müssen wir prüfen, ob b_1 die Bedingungen der Definition 1.1.1 erfüllt. Wegen $N = 1$ gilt $a_1 = n_1 \cdot b_1$ und somit $b_1 \mid a_1$. Zusammen mit $b_1 \mid b_1$ ist das gerade die Bedingung (i) der Definition. Wenn eine ganze Zahl c Teiler von a_1 und b_1 ist, dann gilt offenbar $c \mid b_1$, also ist auch die Bedingung (ii) erfüllt. Damit haben wir gezeigt, dass $b_1 = \mathrm{ggT}(a_1, b_1)$, wenn $N = 1$ ist.
Induktionsschritt: Wir setzen voraus, dass die Behauptung des Satzes für einen festen Wert $N \geq 1$ wahr ist und wollen daraus schließen, dass sie auch für $N + 1$ gilt.
Voraussetzung. Für jedes Zahlenpaar (a, b), für welches der Euklidische Algorithmus nach N Schritten terminiert (d.h. $0 = a_N - n_N b_N$), liefert uns der Algorithmus den größten gemeinsamen Teiler, d.h. es gilt $b_N = \mathrm{ggT}(a, b)$.
Behauptung. Für jedes Zahlenpaar (a, b), für welches der Euklidische Algorithmus nach $N + 1$ Schritten terminiert, liefert uns dieser Algorithmus den größten gemeinsamen Teiler.
Beweis. Sei $(a, b) = (a_1, b_1)$ ein Paar positiver ganzer Zahlen mit $a > b$, so dass der Euklidische Algorithmus nach $N+1$ Schritten terminiert. Dann endet der Euklidische Algorithmus für das Paar (a_2, b_2) bereits nach N Schritten. Wir können daher die Induktionsvoraussetzung auf das Paar (a_2, b_2) anwenden und erhalten $b_{N+1} = \mathrm{ggT}(a_2, b_2)$. Man beachte hier die verschobene Nummerierung. Der Erste Schritt des Algorithmus liefert uns die Gleichungen

$$\begin{aligned} b_2 &= a_1 - n_1 b_1 \\ a_2 &= b_1 \ , \end{aligned} \tag{1.9}$$

oder äquivalent dazu

$$\begin{aligned} a_1 &= b_2 + n_1 a_2 \\ b_1 &= a_2 \ . \end{aligned} \tag{1.10}$$

Wir setzen zur Abkürzung $d = b_{N+1} = \mathrm{ggT}(a_2, b_2)$. Dann gilt $d \mid a_2$ und $d \mid b_2$. Mit Hilfe von (1.10) ergibt sich daraus $d \mid a_1$ und $d \mid b_1$. Daher erfüllt d die Bedingung (i) aus Definition 1.1.1 des größten gemeinsamen Teilers von a_1 und b_1. Wenn nun c ein gemeinsamer Teiler von a_1 und b_1 ist, dann folgt aus (1.9) $c \mid a_2$ und $c \mid b_2$. Da $d = \mathrm{ggT}(a_2, b_2)$ hat dies $c \mid d$ zur Folge. Damit erfüllt d in der Tat die definierenden Eigenschaften des größten gemeinsamen Teilers von a_1 und b_1. Also $d = \mathrm{ggT}(a_1, b_1)$, was die Behauptung war. □

Somit ist die Korrektheit und die Endlichkeit des Euklidischen Algorithmus bewiesen. Mit Hilfe dieses Algorithmus lässt sich der größte gemeinsame Teiler zweier ganzer Zahlen relativ schnell berechnen. Wenn die Zahlen zu groß werden, stößt er jedoch an seine Grenzen und um in akzeptabler Zeit ein Ergebnis zu erhalten, sind weitere Ideen notwendig. Einige davon werden wir am Ende dieses Kapitels kennenlernen.
Von mathematischem Interesse ist der Euklidische Algorithmus für uns aber auch deshalb, weil er die Existenz des größten gemeinsamen Teilers liefert. Darüber hinaus kann er für weitere interessante Anwendungen genutzt werden, von denen wir uns eine zunächst an einem Beispiel anschauen.

Beispiel 1.1.5. Der Euklidische Algorithmus für das Paar (104,47) lautet

k	(a_k, b_k)	$a_k - n_k b_k = b_{k+1}$
1	$(104, 47)$	$104 - 2 \cdot 47 = 10$
2	$(47, 10)$	$47 - 4 \cdot 10 = 7$
3	$(10, 7)$	$10 - 1 \cdot 7 = 3$
4	$(7, 3)$	$7 - 2 \cdot 3 = 1$
5	$(3, 1)$	$3 - 3 \cdot 1 = 0$

Nun setzen wir, mit dem größten gemeinsamen Teiler 1 beginnend, die Rechenergebnisse rückwärts wieder ein. Zur besseren Übersicht sind die Zahlen b_k unterstrichen.

$$\begin{aligned} 1 &= \underline{7} - 2 \cdot \underline{3} \\ &= \underline{7} - 2 \cdot (\underline{10} - 1 \cdot \underline{7}) && = 3 \cdot \underline{7} - 2 \cdot \underline{10} \\ &= 3 \cdot (\underline{47} - 4 \cdot \underline{10}) - 2 \cdot \underline{10} && = 3 \cdot \underline{47} - 14 \cdot \underline{10} \\ &= 3 \cdot \underline{47} - 14 \cdot (\underline{104} - 2 \cdot \underline{47}) && = (-14) \cdot \underline{104} + 31 \cdot \underline{47} \ . \end{aligned}$$

Wir haben damit den größten gemeinsamen Teiler $d = 1$ der beiden Zahlen $a = 104$ und $b = 47$ in der Gestalt $d = r \cdot a + s \cdot b$ dargestellt. Dabei sind

$r = -14$ und $s = 31$ ganze Zahlen. Dies ist ganz allgemein möglich und man kann damit sogar den größten gemeinsamen Teiler charakterisieren.

Satz 1.1.6 *Seien $a \neq 0$, $b \neq 0$ ganze Zahlen. Eine Zahl $d > 0$ ist genau dann der größte gemeinsame Teiler von a und b, wenn die folgenden beiden Bedingungen erfüllt sind:*

(1) *Es gibt ganze Zahlen r, s, für die $d = ra + sb$ gilt.*
(2) *Jede ganze Zahl der Gestalt $ra + sb$ ist durch d teilbar.*

Beweis. Weil die Behauptung besagt, dass zwei unterschiedliche Charakterisierungen des größten gemeinsamen Teilers äquivalent sind, muss der Beweis aus zwei Teilen bestehen.
Teil I. Es ist zu zeigen, dass $\mathrm{ggT}(a, b)$ die Bedingungen (1) und (2) erfüllt.
Teil II. Umgekehrt muss gezeigt werden, dass eine Zahl d, welche die Bedingungen (1) und (2) erfüllt, auch die Bedingung (i) und (ii) aus Definition 1.1.1 erfüllt, woraus sich dann $d = \mathrm{ggT}(a, b)$ ergibt.
Beweis von I. Ohne Beschränkung der Allgemeinheit können wir $a \geq b > 0$ annehmen, denn $\mathrm{ggT}(-a, b) = \mathrm{ggT}(a, -b) = \mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$. Sei $d = \mathrm{ggT}(a, b)$. Da d gemeinsamer Teiler von a und b ist, gilt $d \mid ra + sb$ für beliebige ganze Zahlen $r, s \in \mathbb{Z}$. Die Eigenschaft (2) wird also von d erfüllt. Zum Beweis von (1) führen wir wieder eine Induktion über N, die Anzahl der Schritte im Euklidischen Algorithmus, durch.
Induktionsanfang: Falls $N = 1$, so ist $d = b = b_1$ und $a = a_1 = n_1 b_1$. Damit können wir $r = 0$, $s = 1$ wählen um $d = ra + sb$ zu erhalten.
Induktionsschritt: Wenn der Euklidische Algorithmus für $(a, b) = (a_1, b_1)$ aus $N+1$ Schritten besteht, so sind es für (a_2, b_2) nur N Schritte. Wir können also die Induktionsvoraussetzung auf (a_2, b_2) anwenden. Diese besagt, dass es ganze Zahlen r', s' gibt, für die $d = r'a_2 + s'b_2$ gilt. Außerdem gelten wieder die Gleichungen (1.9) und (1.10) und, wie gewünscht, erhalten wir

$$d = r'b_1 + s'(a_1 - n_1 b_1) = s'a_1 + (r' - s'n_1)b_1 \ .$$

Beweis von II. Sei nun $d = ra + sb > 0$ eine ganze Zahl, welche die Bedingung (2) erfüllt. Außerdem sei $d' = \mathrm{ggT}(a, b)$. Nach dem bereits gezeigten Teil I gibt es $r', s' \in \mathbb{Z}$ mit $d' = r'a + s'b$ und d' erfüllt die Bedingung (2). Da $d = ra + sb$ folgt daraus $d' \mid d$. Weil $d' = r'a + s'b$ und d nach Voraussetzung die Bedingung (2) erfüllt, folgt $d \mid d'$. Daraus ergibt sich, wie bereits zuvor, $d = d'$. □

Das bisher erworbene Verständnis über den größten gemeinsamen Teiler wenden wir nun an, um eine nützliche Charakterisierung von Primzahlen zu geben.

Satz 1.1.7 (a) *Für $a, b, c \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$ und $a \mid bc$ gilt stets $a \mid c$.*
(b) *Eine Zahl $p \neq 0, 1, -1$ ist genau dann eine Primzahl, wenn folgende Bedingung erfüllt ist: Für beliebige ganze Zahlen a, b folgt aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$.*

Beweis. (a) Da $\mathrm{ggT}(a, b) = 1$, gibt es nach Satz 1.1.6 ganze Zahlen r, s mit $ra + sb = 1$. Also ist $c = c \cdot (ra + sb) = a \cdot rc + bc \cdot s$. Da wir $a \mid bc$ vorausgesetzt haben, folgt daraus $a \mid c$.
(b) Der Beweis der behaupteten Äquivalenz zweier Eigenschaften zerfällt erneut in zwei Teile:
Teil I. Zunächst nehmen wir an, dass die Zahl p die Bedingung erfüllt, dass aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$ folgt. Es ist zu zeigen, dass p eine Primzahl im Sinne unserer Definition auf Seite 5 ist. Dazu nehmen wir an, dass p als Produkt $p = ab$ geschrieben werden kann. Dann gilt $p \mid ab$, also nach Voraussetzung $p \mid a$ oder $p \mid b$. Wir können annehmen $b = rp$. Der Fall $p \mid a$ erledigt sich in gleicher Weise. Wir erhalten $p = ab = arp$, woraus, wegen $p \neq 0$, $ar = 1$ folgt. Daher muss $a = r = 1$ oder $a = r = -1$ gelten. Also ist p eine Primzahl.
Teil II. Sei nun p eine Primzahl. Wir haben zu zeigen, dass aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$ folgt. Seien dazu a, b ganze Zahlen, für die $p \mid ab$ gilt. Wir nehmen an p ist kein Teiler von a, sonst wären wir ja fertig. Da p eine Primzahl ist, hat p nur die beiden positiven Teiler 1 und p. So kann $\mathrm{ggT}(p, a)$ nur 1 oder p sein. Da aber p kein Teiler von a ist, muss $\mathrm{ggT}(p, a) = 1$ sein. Wir können nun Teil (a) des Satzes 1.1.7 anwenden und erhalten $p \mid b$. □

Unter Benutzung dieser Charakterisierung von Primzahlen können wir jetzt den folgenden Satz beweisen. Er bringt zum Ausdruck, dass die Primzahlen die Grundbausteine der ganzen Zahlen bezüglich ihrer multiplikativen Struktur sind.

Satz 1.1.8 (Eindeutige Primfaktorzerlegung) *Jede ganze Zahl $n \neq 0$ lässt sich auf genau eine Weise in der Form $n = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$ schreiben, wobei $u = \pm 1$ das Vorzeichen von n ist und $1 < p_1 \leq p_2 \leq \cdots \leq p_k$ Primzahlen sind. Der Fall $k = 0$ ist dabei auch zugelassen und wir meinen dann $n = u$.*

Beweis. Wenn $n < 0$ ist, wählen wir $u = -1$, sonst sei $u = 1$. Es genügt, den Fall $n > 0$ zu untersuchen, der Rest lässt sich durch Multiplikation mit (-1) darauf zurückführen. Zu beweisen ist für jede ganze Zahl $n \geq 2$ die Existenz und Eindeutigkeit einer Darstellung $n = p_1 \cdot \ldots \cdot p_k$ mit Primzahlen $1 < p_1 \leq \cdots \leq p_k$. Die Beweise werden wieder induktiv geführt.
Existenzbeweis: (Vollständige Induktion über n.)
Induktionsanfang: $n = 2$. Da $p_1 = 2$ eine Primzahl ist, sind wir fertig.

Induktionsschritt: Wir nutzen eine leicht veränderte Version des Prinzips der vollständigen Induktion. Die Induktionsvoraussetzung umfasst hier die Gültigkeit der zu beweisenden Aussage für alle Werte $n \leq N$. Daraus ist die Gültigkeit der Aussage für $n = N + 1$ abzuleiten. Das heißt, wir setzen voraus, dass jede ganze Zahl n mit $2 \leq n \leq N$ eine Darstellung als Produkt von Primzahlen besitzt.
Wir wollen dies nun für die Zahl $N+1$ zeigen. Wenn $N+1$ eine Primzahl ist, dann setzen wir $p_1 = N + 1$ und sind fertig. Wenn $N + 1$ keine Primzahl ist, so gibt es nach der Definition des Begriffes der Primzahl ganze Zahlen $a \geq 2$, $b \geq 2$, für die $N + 1 = ab$ gilt. Da a und b kleiner als $N + 1$ sind, lassen sich beide Zahlen nach Induktionsvoraussetzung als Primzahlprodukt schreiben. Damit ist die Existenzaussage bewiesen.
Eindeutigkeitsbeweis: (Induktion über k, die Anzahl der Primfaktoren.)
Induktionsanfang: $k = 1$ bedeutet hier, dass $n = p_1$ eine Primzahl ist. Wenn außerdem $p_1 = n = p'_1 \cdot \ldots \cdot p'_r$ gilt, dann muss $r = 1$ und $p_1 = p'_1$ gelten. Dies folgt aus der Definition des Begriffes der Primzahl.
Induktionsschritt: Wir nehmen an, dass jede Darstellung mit k Faktoren eindeutig ist, also wenn $n = p_1 \cdot \ldots \cdot p_k$ mit Primzahlen $p_1 \leq \cdots \leq p_k$ und $n = p'_1 \cdot \ldots \cdot p'_r$ mit Primzahlen $p'_1 \leq \cdots \leq p'_r$ geschrieben werden kann, dann ist $k = r$ und $p_i = p'_i$.
Sei n eine Zahl mit $k+1$ Primfaktoren, also $n = p_1 \cdot \ldots \cdot p_{k+1}$ mit Primzahlen $p_1 \leq \cdots \leq p_{k+1}$. Wenn $n = p'_1 \cdot \ldots \cdot p'_r$ eine weitere Zerlegung von n in Primfaktoren $p'_1 \leq \cdots \leq p'_r$ ist, dann gilt $p_{k+1} \mid p'_1 \cdot \ldots \cdot p'_r$. Wegen Satz 1.1.7 ergibt sich daraus $p_{k+1} \mid p'_i$ für ein i. Da beides positive Primzahlen sind, muss $p_{k+1} = p'_i$ gelten. Daher ist $p_1 \cdot \ldots \cdot p_k = \underbrace{p'_1 \cdot \ldots \cdot p'_{i-1} \cdot p'_{i+1} \cdot \ldots \cdot p'_r}_{r-1 \text{ Faktoren}}$ und die Induktionsvoraussetzung liefert $k = r - 1$ und $p_j = p'_j$ für $j < i$ bzw. $p_j = p'_{j+1}$ für $j \geq i$. Da $p_{k+1} \geq p_k$ gilt, ist $p'_i \geq p'_r$. Da wir $p'_i \leq p'_r$ vorausgesetzt hatten, gilt $p'_i = p'_r$ und wir können $i = r$ wählen. Es folgt dann $k + 1 = r$ und $p_j = p'_j$ für alle j. □

Zum Abschluss dieses Abschnittes beweisen wir einen sehr wichtigen Satz, der bereits vor über 2000 Jahren im antiken Griechenland bekannt war – der Beweis ist bereits bei Euklid[2] zu finden.

Satz 1.1.9 *Es gibt unendlich viele verschiedene Primzahlen.*

Beweis. Der Beweis wird *indirekt* geführt, das bedeutet, wir nehmen an, dass das (streng mathematische) Gegenteil der Behauptung wahr wäre. Daraus versuchen wir durch logische Schlüsse einen Widerspruch herzuleiten. Wenn uns das gelingt, muss unsere Annahme (nämlich, dass die Behauptung des Satzes nicht gelten würde) falsch sein. Die Behauptung des Satzes ist dann

[2] Vgl. Fußnote auf Seite 6.

bewiesen. Dies ist ein zweites wichtiges Beweisprinzip, welches wir häufig benutzen werden. Die Theorie dazu befindet sich im Kapitel 6: Satz 6.1.1 und nachfolgende Erläuterungen.
Nun zum Beweis: Wir nehmen an, es gäbe nur endlich viele Primzahlen. Dies seien die Zahlen $p_1, p_2, \ldots, p_n$. Nun untersuchen wir die Zahl $a := 1 + \prod_{i=1}^{n} p_i$. Da wir (nach Satz 1.1.8) diese Zahl in Primfaktoren zerlegen können und $a > 1$ ist (da uns ja $p_1 = 2$ schon als Primzahl bekannt ist), gibt es eine Primzahl $p > 1$, welche a teilt. Diese muss, wegen unserer Annahme der Endlichkeit, unter den Zahlen $p_1, \ldots, p_n$ vorkommen. Daher teilt p das Produkt $\prod_{i=1}^{n} p_i$ und somit auch $1 = a - \prod_{i=1}^{n} p_i$. Dies ist aber für eine Zahl $p > 1$ nicht möglich. Damit haben wir den gewünschten Widerspruch erhalten und der Beweis ist vollständig. □

Für die angekündigten Anwendungen in der Kryptographie (siehe Abschnitt 1.5) werden wir die folgende zahlentheoretische Funktion benötigen.

Definition 1.1.10. Für jede positive ganze Zahl n bezeichnet $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen k, für die $1 \leq k < n$ gilt. Diese Funktion φ heißt *Eulerfunktion*[3] oder Eulersche φ-Funktion.
In Kurzschreibweise: $\varphi(n) = |\{k \mid 1 \leq k < n,\ \mathrm{ggT}(k,n) = 1\}|$. Hier und im Folgenden wird durch $|A|$ die Kardinalität, also die Anzahl der Elemente, einer Menge A bezeichnet, vgl. Beispiel 6.3.15.

Die im folgenden Satz zusammengefassten Eigenschaften erleichtern die Berechnung der Werte der Eulerfunktion.

Satz 1.1.11 *Sei p eine Primzahl und seien k, m, n positive ganze Zahlen. Dann gilt:*

(1) $\varphi(p) = p - 1$;
(2) $\varphi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}$;
(3) *Wenn* $\mathrm{ggT}(m,n) = 1$, *dann ist* $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis. Die Aussage (1) ist klar, da unter den Zahlen $1, 2, \ldots, p-1$ keine durch p teilbar ist.
Es ist genau dann $\mathrm{ggT}(a, p^k) \neq 1$, wenn $p \mid a$ gilt. Unter den Zahlen $1, 2, \ldots, p^k$ sind genau die folgenden p^{k-1} Vielfachen von p enthalten: $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. Also bleiben $p^k - p^{k-1}$ Zahlen, die zu p^k teilerfremd sind.
Den Beweis von (3) können wir leicht führen, wenn wir einige Grundbegriffe der Gruppentheorie kennengelernt haben (siehe Satz 1.3.34). Daher verzichten wir an dieser Stelle auf einen Beweis. Dem Leser wird jedoch empfohlen, einen Beweis mit elementaren Mittels selbst auszuarbeiten. □

[3] Leonard Euler (1707–1783), Schweizer Mathematiker.

Beispiel 1.1.12. (i) $\varphi(2) = 1$, $\varphi(4) = 2$, $\varphi(8) = 4$, $\varphi(2^n) = 2^{n-1}$.
(ii) $\varphi(3) = 2$, $\varphi(9) = 6$, $\varphi(27) = 18$, $\varphi(3^n) = 2 \cdot 3^{n-1}$.
(iii) $\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$. Unter den Zahlen $1, 2, 3, 4, 5, 6$ sind nur 1 und 5 teilerfremd zu 6.
(iv) $\varphi(12) = \varphi(2^2) \cdot \varphi(3) = 2 \cdot 2 = 4$ und die zu 12 teilerfremden Zahlen sind $1, 5, 7, 11$.
(v) $\varphi(18) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 3 \cdot 2 = 6$ und wir finden $1, 5, 7, 11, 13, 17$ als Zahlen, die zu 18 teilerfremd sind.

Auf der Grundlage von Satz 1.1.11 ist es sehr leicht, für jede ganze Zahl, deren Primfaktorzerlegung uns bekannt ist, den Wert der Eulerfunktion zu bestimmen. Die Faktorisierung einer Zahl in Primfaktoren ist jedoch ein rechenaufwändiges Problem und somit auch die Berechnung von φ. Man könnte zwar mit dem Euklidischen Algorithmus für jede Zahl k zwischen 1 und n testen, ob sie zu n teilerfremd ist oder nicht, aber auch dies ist ziemlich rechenaufwändig. Diese Schwierigkeit ist die Grundlage des RSA-Verfahrens, das im Abschnitt 1.5 behandelt wird.

Aufgaben

Übung 1.1. Berechnen Sie mit Hilfe des Euklidischen Algorithmus für jedes der folgenden Zahlenpaare (a, b) den größten gemeinsamen Teiler d und finden Sie ganze Zahlen r, s, so dass $d = ra + sb$ gilt.

(i) $(12345, 54321)$ (ii) $(338169, 337831)$ (iii) $(98701, 345)$

Übung 1.2. Beweisen Sie, dass Definition 1.1.1 für $d > 0$ äquivalent ist zu

(i) $d \mid a$ und $d \mid b$;
(ii') Für $c \in \mathbb{Z}$ gilt: Wenn $c \mid a$ und $c \mid b$, dann gilt auch $c \leq d$.

Übung 1.3. Benutzen Sie vollständige Induktion zum Beweis der folgenden Formel:

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 .$$

Übung 1.4. Versuchen Sie mittels vollständiger Induktion die folgenden beiden Formeln für jede ganze Zahl $n \geq 0$ zu beweisen. Dabei ist $q \neq 1$ eine reelle Zahl und wir setzen stets $q^0 = 1$ (auch für $q = 0$).

$$\sum_{k=0}^{n} q^k = \frac{q^{n+1} - q^2 + q - 1}{q - 1} + q, \qquad \sum_{k=0}^{n} q^k = \frac{q^{n+1} - q^2 + q - 1}{q - 1}$$

Welche Formel ist richtig? Welcher Schritt im Beweis funktioniert nicht?

Übung 1.5. Wir definieren hier für ganze Zahlen $n \geq 0$ und k die Symbole $\binom{n}{k}$ durch folgende rekursive Vorschrift (Pascalsches[4] Dreieck, siehe S. 283):

- $\binom{0}{0} = 1$,
- wenn $k < 0$ oder $k > n$, dann ist $\binom{n}{k} = 0$ und
- wenn $0 \leq k \leq n$, dann ist $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Beweisen Sie unter Benutzung dieser Definition und mittels vollständiger Induktion für $n \geq 0$ und beliebige reelle Zahlen a, b die *binomische Formel*:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} .$$

Übung 1.6. Zeigen Sie mittels vollständiger Induktion und unter Benutzung der Definition in Aufgabe 1.5 für $0 \leq k \leq n$ die folgende explizite Formel:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} ,$$

wobei $0! := 1$ und $n! := n \cdot (n-1)!$ rekursiv definiert ist. Benutzen Sie diese Formel, um zu zeigen, dass $p \mid \binom{p}{k}$ für jede Primzahl p und $1 \leq k \leq p-1$ gilt.

Übung 1.7. Benutzen Sie die Methode der vollständigen Induktion, um zu beweisen, dass für jedes $n > 1$, für jede Primzahl p und für beliebige ganze Zahlen $a_1, \ldots, a_n$ folgendes gilt:

Wenn $p \mid a_1 \cdot \ldots \cdot a_n$, dann gibt es ein i mit $1 \leq i \leq n$ und $p \mid a_i$.

Sie können dafür den Satz 1.1.7 benutzen, in dem der Fall $n = 2$ behandelt wurde.

Übung 1.8. Beweisen Sie, dass $\sqrt{26}$ irrational ist, das heißt, sich nicht als Quotient zweier ganzer Zahlen darstellen lässt.

Übung 1.9. (a) Beweisen Sie (ohne die allgemeinere Eigenschaft (3) aus Satz 1.1.11 zu benutzen), dass für Primzahlen $p \neq q$ stets gilt:
$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
(b) Berechnen Sie: $\varphi(101), \varphi(141), \varphi(142), \varphi(143), \varphi(169), \varphi(1024)$.
(c) Für welche Zahlen n gilt $n = 2 \cdot \varphi(n)$?

Übung 1.10. Gilt für jede ungerade Zahl n, dass das um eins verminderte Quadrat dieser Zahl, also $n^2 - 1$, durch 8 teilbar ist? Beweisen Sie Ihre Antwort.

[4] Blaise Pascal (1623–1662), französischer Mathematiker.

1.2 Restklassen

Abstraktion ist eine wichtige Methode zur Beschreibung und Analyse komplexer Situationen. Das betrifft sowohl mathematische Sachverhalte als auch Gegenstände und Vorgänge der realen Welt. Bei einer Abstraktion ignoriert man einige als unwesentlich betrachtete Merkmale und konzentriert sich dadurch auf eine geringere Zahl einfacher strukturierter Aspekte. Dabei können jedoch bestimmte Vorgänge oder Gegenstände ununterscheidbar werden, obwohl sie in Wirklichkeit verschieden sind. Wenn wir zum Beispiel von Bäumen sprechen und es uns dabei vor allem darauf ankommt, diese von Blumen, Steinen, Tieren und Wolken zu unterscheiden, dann haben wir bereits abstrahiert. Wir unterscheiden in diesem Moment nicht zwischen Ahorn, Birke, Buche, Eiche, Kiefer, Lärche und Weide oder gar konkreten Exemplaren solcher Gewächse.

Um Abstraktionen mit mathematischer Präzision durchführen zu können, wird die Sprache der *Mengen*, *Relationen* und *Abbildungen* benutzt. Eine Einführung in diese mathematischen Grundbegriffe befindet sich im Kapitel 6, in den Abschnitten 6.2 und 6.3. Die Zusammenfassung verschiedener Objekte deren wesentliche Merkmale übereinstimmen, wird in der Mathematik durch die Bildung von Äquivalenzklassen realisiert. Wir werden diese Methode in diesem Abschnitt am Beispiel der Restklassen ganzer Zahlen illustrieren.
Der Nutzen dieser Begriffsbildungen zeigt sich dann in den Anwendungen: Wir beweisen einige Teilbarkeitsregeln und beschäftigen uns mit Prüfziffern als Mittel zur Erkennung von Datenübertragungsfehlern.
Bevor wir die allgemeine Definition geben, betrachten wir ein Beispiel. Hierzu stellen wir uns vor, dass wir uns nur dafür interessieren, ob das Ergebnis einer Rechenoperation gerade oder ungerade ist. Wir benutzen dazu die folgende Schreibweise für ganze Zahlen a:

$$\begin{aligned} a &\equiv 0 \mod 2, \quad && \text{wenn } a \text{ gerade,} \\ a &\equiv 1 \mod 2, && \text{wenn } a \text{ ungerade.} \end{aligned}$$

Für $a = 17\ 601\ 000$ und $b = 317\ 206\ 375$ gilt $a \equiv 0 \mod 2$ und $b \equiv 1 \mod 2$. Diese Schreibweise drückt aus, dass a den Rest 0 und b den Rest 1 bei Division durch 2 lässt.
Um zu entscheiden, welche Reste $a + b$ und $a \cdot b$ bei Division durch 2 lassen, muss man die Summe oder das Produkt nicht wirklich ausrechnen. Wir erhalten leicht $a + b \equiv 1 \mod 2$ und $a \cdot b \equiv 0 \mod 2$. Wir bekommen dieses Resultat, indem wir die gewünschte Rechenoperation mit den Resten $0, 1$ durchführen:

$$\begin{aligned} a + b \equiv 0 + 1 &\equiv 1 \mod 2 \quad \text{und} \\ a \cdot b \equiv 0 \cdot 1 &\equiv 0 \mod 2\,. \end{aligned}$$

Das ist wesentlich schneller als die Rechnung mit den großen Zahlen a, b. Wir erhalten das gleiche Resultat, wenn wir a durch eine beliebige andere gerade Zahl und b durch eine beliebige ungerade Zahl ersetzen. Wir können also mit den Resten, oder besser den Restklassen rechnen. Um dies zu formalisieren, bezeichnen wir mit $[0]$ die Menge aller geraden Zahlen und mit $[1]$ die Menge aller ungeraden Zahlen. Diese Mengen nennt man *Restklassen*.
Es gilt $a \in [0]$, $b \in [1]$ und unsere Rechnung hat jetzt die folgende einfache Form: $a+b \in [0+1] = [1]$ und $a \cdot b \in [0 \cdot 1] = [0]$. Das führt uns dazu, Summe und Produkt der Restklassen $[0], [1]$ folgendermaßen zu definieren:

$$[0] + [0] = [0], \qquad [0] + [1] = [1] + [0] = [1], \qquad [1] + [1] = [0],$$
$$[0] \cdot [0] = [0] \cdot [1] = [1] \cdot [0] = [0], \qquad [1] \cdot [1] = [1] \, .$$

Es ist leicht nachzuprüfen, dass diese Addition und Multiplikation der Restklassen $[0], [1]$ die Grundgesetze (1.1)–(1.8) des Rechnens mit ganzen Zahlen erfüllen. Für das Rechnen mit Resten gelten dieselben Regeln wie beim Rechnen mit ganzen Zahlen.
Um dieses Beispiel zu verallgemeinern, benutzen wir den Begriff der Äquivalenzrelation (Definition 6.3.12). Im obigen Beispiel liegen zwei ganze Zahlen in derselben Restklasse, wenn sie entweder beide gerade oder beide ungerade sind. Da zwei Zahlen genau dann dieselbe Parität haben, wenn ihre Differenz gerade ist, ist die zugehörige Äquivalenzrelation $\sim$ durch $a \sim b \iff 2 \mid a-b$ gegeben. Üblicherweise schreibt man in dieser Situation $a \equiv b \mod 2$ statt $a \sim b$, also

$$a \equiv b \mod 2 \quad \iff \quad 2 \mid a - b \, .$$

Wenn wir die Zahl 2 durch eine beliebige ganze Zahl $n \geq 0$ ersetzen, erhalten wir die folgende Definition.

Definition 1.2.1. $a \equiv b \mod n \iff n \mid a - b$.

Dadurch ist auf der Menge $\mathbb{Z}$ aller ganzen Zahlen eine Äquivalenzrelation definiert. Wenn $a \equiv b \mod n$, dann sagen wir: *a ist kongruent b modulo n.*
Unter Benutzung der Division mit Rest erhalten wir $a = r_a + k_a \cdot n$ und $b = r_b + k_b \cdot n$, wobei $k_a, k_b \in \mathbb{Z}$ und $0 \leq r_a < n$, $0 \leq r_b < n$. Dann ist $a - b = (r_a - r_b) + (k_a - k_b) \cdot n$ und es ergibt sich

$$a \equiv b \mod n \iff r_a = r_b \, .$$

Daher ist a genau dann kongruent b modulo n, wenn a und b den gleichen Rest bei Division durch n lassen. Die Äquivalenzklassen dieser Äquivalenzrelation nennen wir *Restklassen* modulo n. Die Restklasse modulo n, in der $a \in \mathbb{Z}$ enthalten ist, wird mit $[a]_n$, oder wenn keine Verwechslungen möglich sind mit $[a]$, bezeichnet. Für festes $n \geq 0$ liegt nach Satz 6.3.16 jede ganze Zahl in genau einer Restklasse modulo n. Jedes Element $b \in [a]$ heißt *Repräsentant* der Restklasse $[a]$. Wenn b ein Repräsentant von $[a]$ ist, dann gilt $[a] = [b]$. Die

Menge aller Restklassen modulo n bezeichnen wir mit $\mathbb{Z}/n\mathbb{Z}$, vgl. Definition 6.3.13.

Bemerkung 1.2.2. Wenn $n > 0$ ist, dann gibt es genau n verschiedene Restklassen modulo n, dies sind $[0], [1], \ldots, [n-1]$, d.h.

$$\mathbb{Z}/n\mathbb{Z} = \big\{[0], [1], \ldots, [n-1]\big\} .$$

Man nennt daher die Zahlen $0, 1, 2, \ldots, n-2, n-1$ ein *vollständiges Restsystem* modulo n. Da $[a]_n = [a+kn]_n$ für beliebiges $k \in \mathbb{Z}$, gibt es auch andere vollständige Restsysteme, z.B. ist nicht nur $0, 1, 2$ sondern auch $-1, 0, 1$ ein vollständiges Restsystem modulo 3.
Im Fall $n = 0$ treffen wir eine völlig andere Situation an, denn $a \equiv b \mod 0$ ist äquivalent zu $a = b$. Daher ist in jeder Restklasse modulo 0 genau eine Zahl enthalten und es gibt unendlich viele solche Restklassen: $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

Wie im Fall $n = 2$ möchten wir ganz allgemein mit den Restklassen modulo n rechnen.

Definition 1.2.3. Auf der Menge $\mathbb{Z}/n\mathbb{Z}$ definieren wir eine Addition und eine Multiplikation durch $[a] + [b] := [a + b]$ und $[a] \cdot [b] := [a \cdot b]$.

Dies besagt, dass wir Restklassen addieren oder multiplizieren, indem wir diese Operationen mit Repräsentanten dieser Restklassen durchführen. Um zu klären, ob eine solche Definition sinnvoll ist, müssen wir beweisen, dass wir stets dasselbe Resultat erhalten, ganz gleich welche Repräsentanten wir gewählt haben. Es ist daher zu zeigen, dass aus $[a] = [a']$ und $[b] = [b']$ stets $[a] + [b] = [a'] + [b']$ und $[a] \cdot [b] = [a'] \cdot [b']$ folgt. Da, wie leicht einzusehen ist, die Addition und die Multiplikation von Restklassen kommutativ sind, ergibt sich dies aus zweimaliger Anwendung der Implikation

$$[a] = [a'] \quad \Longrightarrow \quad [a] + [b] = [a'] + [b] \quad \text{und} \quad [a] \cdot [b] = [a'] \cdot [b].$$

Um dies zu beweisen, bemerken wir zuerst, dass $[a] = [a']$ genau dann gilt, wenn $a \equiv a' \mod n$, das heißt $a' = a + kn$ für ein $k \in \mathbb{Z}$. Daraus erhalten wir $a' + b = a + kn + b$ und somit

$$[a'] + [b] = [a' + b] = [a + kn + b] = [a + b] = [a] + [b].$$

Ebenso ergibt sich $a' \cdot b = (a + kn) \cdot b = a \cdot b + kb \cdot n$ und

$$[a'] \cdot [b] = [a' \cdot b] = [a \cdot b + kb \cdot n] = [a \cdot b] = [a] \cdot [b].$$

Für die Zukunft halten wir fest: Wenn wir mathematische Operationen oder Abbildungen auf Mengen von Äquivalenzklassen definieren, dann müssen wir immer sicherstellen, dass die Definition nicht von der Wahl der Repräsentanten abhängt. Man spricht dann von *Wohldefiniertheit* der Operation oder Abbildung.

Der folgende Satz sagt, dass das Rechnen mit Restklassen genauso funktioniert wie mit ganzen Zahlen.

Satz 1.2.4 *Die Gesetze* (1.1)–(1.8) *für das Rechnen in* $(\mathbb{Z}, +, \cdot)$ *gelten auch in* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Beweis. Wenn wir [0], [1] als neutrale Elemente für die Addition bzw. Multiplikation verwenden und $-[a] := [-a]$ setzen, dann ergeben sich diese Gesetze unmittelbar aus denen, die wir für $\mathbb{Z}$ formuliert hatten, indem wir dort a, b, c durch $[a], [b], [c]$ ersetzen. □

Bemerkung 1.2.5. Jeder ist gewissen Rechnungen modulo n bereits im realen Leben begegnet. Zum Beispiel bei der Uhrzeit. Der Stundenzeiger jeder analogen Uhr zeigt uns Zahlen modulo 12 an. Überlegungen wie diese sind jedem vertraut: Jetzt ist es 10 Uhr, also ist es in 3 Stunden 1 Uhr. In mathematischer Sprache: $10 + 3 \equiv 1 \mod 12$. Ebenso sind wir daran gewöhnt, dass der Minutenzeiger modulo 60 rechnet.

Bevor wir weitere, etwas verstecktere Beispiele des Rechnens in $\mathbb{Z}/n\mathbb{Z}$ aus dem Alltagsleben kennenlernen, befassen wir uns mit der Division in $\mathbb{Z}/nZ$. Dabei werden wir Erkenntnisse aus Abschnitt 1.1 aus einem neuen Blickwinkel betrachten und die mathematischen Grundlagen für die angekündigten Anwendungen bereitstellen.
Bei der Division in $\mathbb{Z}/n\mathbb{Z}$ geht es darum, für gegebene $a, b \in \mathbb{Z}$ die Gleichung $a \cdot x \equiv b \mod n$ zu lösen. Es ist sinnvoll, zunächst die einfachere Gleichung

$$a \cdot x \equiv 1 \mod n \tag{1.11}$$

zu studieren. Unter Benutzung des Euklidischen Algorithmus haben wir im Satz 1.1.6 gezeigt, dass es genau dann ganze Zahlen r, s mit $ra + sn = 1$ gibt, wenn $\mathrm{ggT}(a, n) = 1$ gilt. Mit Hilfe von Kongruenzen und Restklassen kann man diesen Sachverhalt folgendermaßen[5] ausdrücken

$$\begin{aligned} \mathrm{ggT}(a,n) = 1 &\iff \exists\, r \in \mathbb{Z} : r \cdot a \equiv 1 \mod n \\ &\iff \exists\, [r] \in \mathbb{Z}/n\mathbb{Z} : [r] \cdot [a] = [1]\,. \end{aligned}$$

Der Euklidische Algorithmus liefert also eine Methode, mit der wir Gleichungen der Form (1.11) lösen können. Die Eindeutigkeit einer solchen Lösung wird im folgenden Satz geklärt.

Satz 1.2.6 *Wenn* a, n *teilerfremde ganze Zahlen sind, dann gibt es genau eine Restklasse* $[r] \in \mathbb{Z}/n\mathbb{Z}$ *mit* $[r] \cdot [a] = [1]$, *d.h.* $r \cdot a \equiv 1 \mod n$.

[5] Der Existenzquantor $\exists$ und der Allquantor $\forall$ sind in Abschnitt 6.1 ab S. 360 erklärt.

Beweis. Die Existenz haben wir bereits gezeigt (Satz 1.1.6). Angenommen, für $r, r' \in \mathbb{Z}$ gilt $r \cdot a \equiv 1 \mod n$ und $r' \cdot a \equiv 1 \mod n$. Dann folgt $ra \equiv r'a \mod n$ und somit $n \mid a(r - r')$. Da nach Voraussetzung $\mathrm{ggT}(a, n) = 1$, liefert Satz 1.1.7, dass n ein Teiler von $r - r'$ ist. Damit ist $r \equiv r' \mod n$ also $[r] = [r']$. □

Beispiel 1.2.7. Wenn $n = 11$ und $a = 3$ ist, dann erhalten wir mittels Euklidischem Algorithmus: $\underline{11} - 3 \cdot \underline{3} = \underline{2}$ und $\underline{3} - \underline{2} = 1$. Rückwärts Einsetzen ergibt $1 = \underline{3} - \underline{2} = \underline{3} - (\underline{11} - 3 \cdot \underline{3}) = 4 \cdot \underline{3} - 1 \cdot \underline{11}$. Daraus erhalten wir $4 \cdot 3 \equiv 1 \mod 11$, das heißt $[3] \cdot [4] = [1]$ in $\mathbb{Z}/11\mathbb{Z}$. Ebenso erhält man $[1] \cdot [1] = [2] \cdot [6] = [3] \cdot [4] = [5] \cdot [9] = [7] \cdot [8] = [10] \cdot [10] = [1]$ in $\mathbb{Z}/11\mathbb{Z}$. Die Restklasse $[0] \in \mathbb{Z}/11\mathbb{Z}$ ist die einzige, die dabei nicht auftritt. Die Gleichung $x \cdot [0]_n = [1]_n$ hat für kein $n \geq 2$ eine Lösung $x \in \mathbb{Z}/n\mathbb{Z}$.

Wenn n eine Primzahl ist, ergibt sich als Spezialfall aus Satz 1.2.6:

Folgerung 1.2.8. *Wenn $a \in \mathbb{Z}$ und n eine Primzahl ist, so dass $[a] \neq [0] \in \mathbb{Z}/n\mathbb{Z}$, dann gibt es genau ein $[r] \in \mathbb{Z}/n\mathbb{Z}$, für das $[r] \cdot [a] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$ gilt.*

Falls n eine Primzahl und $[a] \neq [0]$ in $\mathbb{Z}/n\mathbb{Z}$ ist, genügt das, um jede Gleichung der Gestalt

$$ax \equiv b \mod n \tag{1.12}$$

zu lösen. Dazu schreiben wir die Kongruenz (1.12) in der Form $[a] \cdot [x] = [b]$ und erhalten unter Benutzung von $[r] \cdot [a] = [1]$

$$[r] \cdot [b] = [r] \cdot ([a] \cdot [x]) = ([r] \cdot [a]) \cdot [x] = [x] \, .$$

Also ist $[x] = [r \cdot b]$ die gesuchte und einzige Lösung. Die Menge aller ganzzahligen Lösungen der Kongruenz (1.12) ist daher $[r \cdot b]_n = \{rb + kn \mid k \in \mathbb{Z}\}$.

Falls n keine Primzahl ist, dann gibt es zu jeder Lösung $x \in \mathbb{Z}$ der Kongruenz (1.12) eine ganze Zahl $s \in \mathbb{Z}$, so dass $ax + sn = b$ gilt. Aus Satz 1.1.6 erhalten wir, dass dies genau dann möglich ist, wenn $d = \mathrm{ggT}(a, n)$ ein Teiler von b ist. Das ist die Lösbarkeitsbedingung für die Kongruenz (1.12). Wenn sie erfüllt ist, dann sind $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ und $n' = \frac{n}{d}$ ganze Zahlen und $x \in \mathbb{Z}$ ist genau dann Lösung von (1.12), wenn

$$a'x \equiv b' \mod n' \, .$$

Da $\mathrm{ggT}(a', n') = 1$, finden wir mit der oben angegebenen Methode alle Lösungen dieser Kongruenz und damit auch die von (1.12).

Erste Anwendungen der Rechenoperationen in $\mathbb{Z}/n\mathbb{Z}$ betreffen die Bestimmung von Endziffern sehr großer Zahlen und Teilbarkeitsregeln.

Beispiel 1.2.9. Mit welcher Ziffer endet die Zahl 9^{99}?

Die letzte Ziffer d einer Zahl $a \in \mathbb{Z}$ ist dadurch charakterisiert, dass $0 \leq d \leq 9$ und dass es eine ganze Zahl k gibt, für die $a = 10k + d$ gilt. Daher ist $d \equiv a \mod 10$.
Da $9 \equiv -1 \mod 10$, erhalten wir $9^{99} \equiv (-1)^{99} \equiv -1 \mod 10$. Da $d = 9$ die einzige Ziffer ist, die kongruent -1 modulo 10 ist, endet 9^{99} auf 9. Es ist kein Problem, dies mit einem Taschenrechner nachzuprüfen.
Wie sieht es jedoch bei $9^{(9^9)}$ oder bei $9^{(10^{11})}$ aus? Da versagt eine direkte Rechnung mit einem gewöhnlichen Taschenrechner. Die Rechnung mit Kongruenzen kann aber wieder im Kopf durchgeführt werden.
Zunächst bemerken wir, dass der Exponent 9^9 ungerade ist, da $9 \equiv 1 \mod 2$ und somit $9^9 \equiv 1^9 \equiv 1 \mod 2$. Damit erhalten wir nun $9^{(9^9)} \equiv (-1)^{(9^9)} \equiv -1 \mod 10$ und auch $9^{(9^9)}$ endet mit der Ziffer 9.
In analoger Weise sehen wir, dass $10^{11} \equiv 0^{11} \equiv 0 \mod 2$, der Exponent also gerade ist, woraus wir $9^{(10^{11})} \equiv (-1)^{(10^{11})} \equiv 1 \mod 10$ erhalten. Daraus schließen wir, dass $9^{(10^{11})}$ mit der Ziffer 1 endet.
Mit geringem Mehraufwand kann man auf diese Weise per Hand die letzten zwei oder drei Ziffern all dieser relativ großen Zahlen bestimmen. Effektiver geht das mit dem kleinen Satz von Fermat, Satz 1.3.24. Weitere Methoden, die das Rechnen mit großen Zahlen erleichtern, werden wir nach Satz 1.4.23 kennenlernen, siehe Bemerkung 1.4.26.

Beispiel 1.2.10 (Teilbarkeit durch 3). Viele kennen die 3-er Regel: Eine ganze Zahl ist genau dann durch drei teilbar, wenn ihre Quersumme durch drei teilbar ist. Als *Quersumme* einer Zahl bezeichnet man die Summe ihrer Ziffern.
Unter Verwendung von Kongruenzen lässt sich die Richtigkeit dieser Regel sehr elegant beweisen. Da eine Zahl a genau dann durch 3 teilbar ist, wenn $a \equiv 0 \mod 3$ gilt, genügt es zu zeigen, dass jede ganze Zahl kongruent ihrer Quersumme modulo 3 ist.
Wenn eine Zahl a die Ziffern $a_k a_{k-1} \dots a_1 a_0$ hat, dann ist $a = \sum_{i=0}^{k} a_i 10^i$ und $\sum_{i=0}^{k} a_i$ ist die Quersumme dieser Zahl. Da $10 \equiv 1 \mod 3$ ergibt sich

$$a = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i \equiv \sum_{i=0}^{k} a_i \mod 3 \,.$$

Damit ist die 3-er Regel bewiesen. Da $10 \equiv 1 \mod 9$, gilt die gleiche Regel auch für Teilbarkeit durch 9.

Beispiel 1.2.11 (Teilbarkeit durch 11). Da $10 \equiv -1 \mod 11$ folgt aus $a = \sum_{i=1}^{k} a_i 10^i$ die Kongruenz $a \equiv \sum_{i=1}^{k} (-1)^i a_i \mod 11$. Daraus sehen wir, dass a genau dann durch 11 teilbar ist, wenn die *alternierende Quersumme* von a durch 11 teilbar ist.
Zum Beispiel ist 317 206 375 nicht durch 11 teilbar, da die alternierende Quersumme $3 - 1 + 7 - 2 + 0 - 6 + 3 - 7 + 5 = 2$ nicht durch 11 teilbar ist.

Nach dem gleichen Muster lassen sich weitere, zum Teil weniger bekannte Teilbarkeitsregeln herleiten und beweisen. Unsere Beweise beruhen stets auf einer Kongruenz der Gestalt $10^r \equiv \pm 1 \mod n$. Das funktioniert für solche n, die Teiler einer Zahl der Gestalt $10^r \pm 1$ sind.

Beispiel 1.2.12 (Teilbarkeit durch 101). Die Zahl 101 ist eine Primzahl und es gilt $100 \equiv -1 \mod 101$. Zur Beschreibung einer Teilbarkeitsregel teilen wir deshalb die Ziffern einer Zahl a in Zweiergruppen. Wir beginnen dabei am Ende der Zahl. Wenn $A_k, A_{k-1}, \ldots, A_1, A_0$ diese Zweiergruppen sind, dann ist $0 \le A_i \le 99$ und $a = \sum_{i=1}^{k} A_i 10^{2i}$. Damit ergibt sich

$$a \equiv \sum_{i=1}^{k} (-1)^i A_i \mod 101 \,.$$

Also ist a genau dann durch 101 teilbar, wenn die alternierende Summe der am Ende beginnend gebildeten 2-er Gruppen durch 101 teilbar ist.
Die 2-er Gruppen unserer Beispielzahl 317 206 375 lauten $A_4 = 03, A_3 = 17, A_2 = 20, A_1 = 63, A_0 = 75$. Da $3 - 17 + 20 - 63 + 75 = 18$ nicht durch 101 teilbar ist, ist auch 317 206 375 nicht durch 101 teilbar.

Beispiel 1.2.13 (Teilbarkeit durch 7 und 13). Der Ausgangspunkt ist die Gleichung $1001 = 7 \cdot 11 \cdot 13$. Daraus erhalten wir $1000 \equiv -1 \mod 7$ und $1000 \equiv -1 \mod 13$. Daher können wir die Teilbarkeit durch 7 und 13 durch Betrachtung der alternierenden Summe der 3-er Gruppen (am Ende beginnend) testen.
Für die uns bereits vertraute Zahl 317 206 375 erhalten wir als alternierende Summe der Dreiergruppen $317 - 206 + 375 = 486$. Da $486 \equiv -4 \mod 7$ und $486 \equiv 5 \mod 13$ gilt, ist weder 13 noch 7 ein Teiler von 317 206 375.

Bei der Übermittlung von Informationen können Fehler oder Datenverluste auftreten. Oft ist es wichtig, dass solche Fehler erkannt oder sogar korrigiert werden. Bei der menschlichen Sprache erlernen wir diese Fähigkeit frühzeitig, wodurch es uns oft möglich ist, auch mit einer Person zu kommunizieren, die nuschelt oder einen unvertrauten Dialekt spricht. Wenn es sich bei der übermittelten Information jedoch um eine Zahl handelt, zum Beispiel eine Kontonummer, Artikelnummer, Kreditkartennummer oder Ähnliches, dann ist es für ein menschliches Wesen nicht so einfach, Fehler zu erkennen. Das Anhängen einer sogenannten Prüfziffer ist die einfachste Methode, eine Fehlererkennung zu ermöglichen. In den folgenden beiden Beispielen werden zwei weltweit praktizierte Prüfzifferverfahren vorgestellt. In beiden Fällen wird die Prüfziffer durch eine Rechnung modulo n bestimmt. Im Kapitel 2.5 werden wir uns mit Methoden beschäftigen, die eine Korrektur von Fehlern ermöglicht.

Beispiel 1.2.14 (EAN – European Article Number). In vielen Supermärkten werden an der Kasse die auf den Waren aufgedruckten Strichcodes gelesen, woraus dann die Rechnung für den Kunden und eine Übersicht

über den Lagerbestand erstellt wird. Der Strichcode spiegelt in einer bestimmten Weise die 13-stellige EAN wieder. Davon tragen die ersten 12 Ziffern $a_1, \ldots, a_{12}$ die Information, die 13. Ziffer a_{13} ist eine Prüfziffer. Die ersten 12 Ziffern sind in drei Gruppen unterteilt. Die erste Zifferngruppe ist eine Länderkennung, sie umfasst die ersten drei Ziffern. Die Nummern 400–440 sind Deutschland, 760–769 der Schweiz und Liechtenstein und 900–919 Österreich zugeordnet. Aus den ersten drei Ziffern kann man in der Regel nur auf den Firmensitz des Herstellers schließen, nicht aber auf das Land in dem der Artikel tatsächlich hergestellt wurde.
Die zweite Gruppe besteht meist aus vier, manchmal aber auch aus fünf oder sechs Ziffern. Sie codiert das produzierende Unternehmen, welches die verbleibenden Ziffern als Artikelnummer frei vergeben kann. Bei der EAN

sieht die Einteilung in Zifferngruppen folgendermaßen aus:

$$\underbrace{\underset{a_1}{4}\ \underset{a_2}{3}\ \underset{a_3}{9}}_{\text{Land}} \quad \underbrace{\underset{a_4}{9}\ \underset{a_5}{1}\ \underset{a_6}{4}\ \underset{a_7}{8}}_{\text{Hersteller}} \quad \underbrace{\underset{a_8}{4}\ \underset{a_9}{0}\ \underset{a_{10}}{5}\ \underset{a_{11}}{5}\ \underset{a_{12}}{0}}_{\text{Artikel}} \quad \underbrace{\underset{a_{13}}{8}}_{\text{Prüfziffer}}$$

Bereits 1973 wurde in den USA ein 12-stelliger Produktcode eingeführt, der kurz darauf in Europa zur EAN erweitert wurde. Seit die 13-stellige EAN auch in Nordamerika verwendet wird, spricht man von der *International Article Number*. Die Prüfziffer ergibt sich aus den ersten 12 Ziffern wie folgt:

$$a_{13} \equiv -(a_1 + 3a_2 + a_3 + 3a_4 + \cdots + 3a_{12}) \mod 10.$$

Jede gültige EAN muss daher die folgende Prüfgleichung erfüllen:

$$a_1 + 3a_2 + a_3 + 3a_4 + \cdots + a_{11} + 3a_{12} + a_{13} \equiv 0 \mod 10. \tag{1.13}$$

Im obigen Beispiel gilt tatsächlich

$$\underline{4} + 3 \cdot \underline{3} + \underline{9} + 3 \cdot \underline{9} + \underline{1} + 3 \cdot \underline{4} + \underline{8} + 3 \cdot \underline{4} + \underline{0} + 3 \cdot \underline{5} + \underline{5} + 3 \cdot \underline{0} + \underline{8} \equiv 0 \mod 10.$$

Wenn genau eine der 13 Ziffern fehlt oder unleserlich ist, dann lässt sie sich mit Hilfe der Prüfgleichung (1.13) rekonstruieren. Das ist offensichtlich, wenn die fehlende Ziffer mit Faktor 1 in der Prüfgleichung auftritt. Wenn sie mit dem Faktor 3 versehen ist, dann nutzen wir die Kongruenz $3 \cdot 7 \equiv 1 \mod 10$ um sie zu bestimmen.

Beispiel 1.2.15 (ISBN – International Standard Book Number). Alle im Handel erhältlichen Bücher sind heutzutage mit einer ISBN versehen. Von 1972 bis Ende 2006 bestand sie aus zehn Zeichen, heute ist sie 13-stellig.

Zur Unterscheidung dieser beiden Typen spricht man von der ISBN-10 und der ISBN-13. Jeder ISBN-10 ist in eindeutiger Weise eine ISBN-13 zugeordnet, nicht aber umgekehrt.
Die ISBN-13 eines Buches ist identisch mit seiner EAN. Die Prüfziffer wird nach der Vorschrift im Beispiel 1.2.14 bestimmt. Bei der ISBN-10 erfolgt die Berechnung des Prüfzeichens auf eine mathematisch interessantere Art.
Ähnlich zur Struktur der EAN, sind die 10 Zeichen einer ISBN-10 in vier Gruppen unterteilt. Die einzelnen Gruppen repräsentieren das Land bzw. den Sprachraum, den Verlag, eine verlagsinterne Nummer des Buches, sowie das Prüfzeichen. Details sind durch die Norm DIN ISO 2108 geregelt. Die erste Zifferngruppe besteht oft nur aus einer, kann aber bis zu fünf Ziffern umfassen. Der deutsche Sprachraum entspricht der Ziffer 3. In der ISBN dieses Buches finden Sie die Verlagsnummer 540 des Springer-Verlags vor. Auch die Verlagsnummern können aus unterschiedlich vielen Ziffern bestehen.
Wenn wir die einzelnen Zeichen einer ISBN-10, von links beginnend, mit $a_1, a_2, \ldots, a_9, a_{10}$ bezeichnen, dann lautet die Prüfgleichung:

$$\sum_{i=1}^{10} i \cdot a_i \equiv 0 \mod 11 \,. \tag{1.14}$$

Da $10 \cdot a_{10} \equiv -a_{10} \mod 11$, ist der Wert des Prüfzeichens a_{10} gleich der kleinsten nicht-negativen ganzen Zahl, die kongruent $\sum_{i=1}^{9} i \cdot a_i$ modulo 11 ist. Der mögliche Wert 10 wird in Anlehnung an die entsprechende römische Ziffer durch das Symbol `X` wiedergegeben. Daher sprechen wir von einem Prüfzeichen statt von einer Prüfziffer. Das Symbol `X` ist nur als Prüfzeichen, also an der letzten Stelle und auch nur bei der ISBN-10 zugelassen.
Für die ISBN `3-528-77217-4` erhalten wir

$$\underline{3} + 2 \cdot \underline{5} + 3 \cdot \underline{2} + 4 \cdot \underline{8} + 5 \cdot \underline{7} + 6 \cdot \underline{7} + 7 \cdot \underline{2} + 8 \cdot \underline{1} + 9 \cdot \underline{7} \equiv 4 \mod 11$$

und das ist tatsächlich die angegebene Prüfziffer.
Um aus einer ISBN-10 die zugehörige ISBN-13 zu gewinnen, wird zuerst das Prüfzeichen entfernt, dann das Präfix 978 vorangestellt und schließlich nach den Regeln der EAN die neue Prüfziffer berechnet. In unserem Beispiel:

$$9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 5 + 3 \cdot 2 + 8 + 3 \cdot 7 + 7 + 3 \cdot 2 + 1 + 3 \cdot 7 \equiv 2 \mod 10.$$

Damit erhalten wir 8 als neue Prüfziffer und die zu `3-528-77217-4` gehörige ISBN-13 lautet `9783528772178`. Auf Büchern, die vor dem 1. Januar 2007 gedruckt wurden, sind in der Regel beide Nummern vorzufinden:

Außer 978 ist auch das Präfix 979 im Gebrauch, wodurch sich die Zahl der prinzipiell möglichen Buchnummern verdoppelt. Die ISBN-13, die gleichzeitig auch die EAN darstellt, gibt ein Beispiel dafür, dass aus den ersten drei Ziffern einer EAN nicht das Herkunftsland des Artikels bestimmt werden kann, es sei denn, man ist der Ansicht, dass alle Bücher aus „Buchland“ kommen.

Aufgaben

Übung 1.11. Zeigen Sie, dass $\sum_{k=1}^{2000} k^{13} = 1^{13} + 2^{13} + \cdots + 1999^{13} + 2000^{13}$ durch 2001 teilbar ist.

Übung 1.12. Vor geraumer Zeit empfahl mir ein guter Freund zwei Bücher. Aus Bequemlichkeit sandte er mir lediglich die folgenden beiden ISBN-10: `3-423-62015-3` und `3-528-28783-6`. Beim Versuch diese Bücher zu kaufen, musste ich leider feststellen, dass eine der beiden Nummern fehlerhaft war. Überprüfen Sie unter Benutzung der Prüfgleichung (1.14) die Gültigkeit beider ISBN's. Geben Sie alle Möglichkeiten an, die fehlerhafte ISBN-10 an genau einer Stelle so zu verändern, dass die Prüfgleichung erfüllt ist. Übertragen Sie die so gefundenen korrigierten ISBN-10 in das ISBN-13-Format und ermitteln Sie (z.B. mit Hilfe einer Internetrecherche) welche davon tatsächlich zu einem Buch gehört.

1.3 Gruppen

Zu Beginn des vorigen Abschnittes haben wir die Wichtigkeit der Methode der Abstraktion hervorgehoben. Als wichtigstes Beispiel eines Abstraktionsprozesses diente uns dort der Übergang von ganzen Zahlen zu Restklassen. Wir nehmen nun den scheinbar wenig spektakulären Satz 1.2.4 als Ausgangspunkt für unsere weiteren Überlegungen. Er sagt, dass die Grundgesetze des Rechnens beim Übergang zu Restklassen nicht verloren gehen. In diesem Sinne gehören die Axiome (1.1)–(1.8) zu den wesentlichen Merkmalen, welche sich bei der Abstraktion herauskristallisiert haben. Auf dem neuen Abstraktionsniveau, auf das wir uns in diesem Abschnitt begeben, sind solche Rechengesetze das Einzige, was wir noch als wesentlich betrachten wollen. Die

Konzentration auf Rechengesetze, oder allgemeiner auf strukturelle Eigenschaften algebraischer Operationen, gehört zu den wichtigsten Charakteristiken der modernen Algebra. Als erstes Beispiel werden wir den Begriff der *Gruppe* kennenlernen und studieren. Weitere Begriffe wie *Ring* und *Körper* bilden den Gegenstand von Abschnitt 1.4. Wie bereits zuvor beschränken wir uns auch hier nicht auf abstrakte Definitionen, sondern illustrieren die eingeführten Begriffe durch viele konkrete Beispiele bis hin zu Anwendungen aus dem Alltag.

Definition 1.3.1. Eine nichtleere Menge G zusammen mit einer Abbildung $* : G \times G \to G$, die jedem Paar $(a, b) \in G \times G$ ein Element $a * b \in G$ zuordnet, heißt *Gruppe*, wenn Folgendes gilt:

$$\text{(Assoziativgesetz)} \ \forall\, a, b, c \in G : \qquad a * (b * c) = (a * b) * c. \tag{1.15}$$

$$\text{(neutrales Element)} \ \exists\, e \in G \, \forall\, a \in G : \qquad e * a = a. \tag{1.16}$$

$$\text{(inverses Element)} \ \forall\, a \in G \, \exists\, a' \in G : \qquad a' * a = e. \tag{1.17}$$

Wenn zusätzlich noch das

$$\text{(Kommutativgesetz)} \ \forall\, a, b \in G : \qquad a * b = b * a, \tag{1.18}$$

gilt, dann nennen wir G eine *abelsche*[6] *Gruppe*.

Zur Vermeidung von Unklarheiten sprechen wir oft von der „Gruppe $(G, *)$“ und nicht nur von der „Gruppe G“. Das Symbol $*$ dient uns zur allgemeinen Bezeichnung der Verknüpfung in einer Gruppe. In Beispielen ersetzen wir nicht nur G durch eine konkrete Menge, sondern oft auch den $*$ durch eines der gebräuchlichen Verknüpfungssymbole wie etwa $+, \cdot, \circ$ oder $\times$.
Wenn $+$ als Verknüpfungsymbol verwendet wird sprechen wir von einer *additiven Gruppe*. Dann schreiben wir 0 statt e und das additive Inverse a' von a bezeichnen wir mit $-a$.
Wenn $\cdot$ als Verknüpfungsymbol verwendet wird, sprechen wir von einer *multiplikativen Gruppe*. In diesem Fall wird das neutrale Element durch 1 statt durch e bezeichnet. Für das multiplikative Inverse hat sich die Bezeichnung a^{-1} eingebürgert.

Beispiel 1.3.2. (i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind abelsche Gruppen. Hier und im Folgenden bezeichnet $\mathbb{Q}$ die Menge der rationalen Zahlen, $\mathbb{R}$ die Menge der reellen Zahlen und $\mathbb{C}$ die Menge der komplexen Zahlen, vgl. Beispiel 1.4.20 und Abschnitt 3.1.
(ii) Aus Satz 1.2.4 ergibt sich, dass $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe ist.
(iii) $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen. Die Zahl 0 mussten wir wegen (1.17) entfernen, da sie kein multiplikatives Inverses besitzt.

[6] Niels Henrik Abel (1802–1829), norwegischer Mathematiker.

(iv) Im Gegensatz dazu ist $(\mathbb{Z} \smallsetminus \{0\}, \cdot)$ *keine* Gruppe, denn keine von ± 1 verschiedene ganze Zahl hat ein multiplikatives Inverses in $\mathbb{Z}$. Die größte multiplikative Gruppe, die nur ganze Zahlen enthält, ist daher $\{1, -1\}$.

(v) Aus Satz 1.2.6 folgt, dass $(\mathbb{Z}/n\mathbb{Z})^* := \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1\}$ eine Gruppe bezüglich Multiplikation ist.

(vi) Auf dem kartesischen Produkt $G \times H$ (siehe Abschnitt 6.2) zweier Gruppen $(G, *)$ und $(H, \cdot)$ erhalten wir die Struktur einer Gruppe $(G \times H, \circ)$ indem wir $(g, h) \circ (g', h') := (g * g', h \cdot h')$ definieren. Das ist jedem von der additiven Gruppe $\mathbb{R}^2$ – Vektoren in der Ebene – vertraut.

Beispiel 1.3.3. Als Verknüpfung der *symmetrischen Gruppe* einer Menge M

$$\mathrm{sym}(M) := \{f : M \to M \mid f \text{ ist eine bijektive}^7 \text{Abbildung}\}$$

verwenden wir die Komposition von Abbildungen. Wenn $f, g : M \to M$ zwei Abbildungen sind, dann ist ihre Komposition $f \circ g : M \to M$ für alle $m \in M$ durch $(f \circ g)(m) := f\big(g(m)\big)$ definiert.
Das neutrale Element ist die *identische Abbildung* $\mathrm{Id}_M : M \to M$, die durch $\mathrm{Id}_M(m) = m$ gegeben ist. Die zu $f : M \to M$ inverse Abbildung $g = f^{-1}$ hat folgende Beschreibung. Da f bijektiv ist, gibt es zu jedem $m \in M$ genau ein $n \in M$ mit $f(n) = m$. Die inverse Abbildung ist dann durch $g(m) := n$ gegeben. Sie ist durch $g \circ f = f \circ g = \mathrm{Id}_M$ charakterisiert.
Wenn M eine endliche Menge mit n Elementen ist, können wir durch Nummerierung der Elemente die Menge M mit $\{1, 2, \ldots, n\}$ identifizieren. In dieser Situation hat sich die Bezeichnung $\mathfrak{S}_n$ für die Gruppe $(\mathrm{sym}(M), \circ)$ eingebürgert. Die Elemente von $\mathfrak{S}_n$ nennt man Permutationen. Jede Permutation $\sigma \in \mathfrak{S}_n$ ist eine Bijektion

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

und eine solche lässt sich durch Angabe einer Wertetabelle beschreiben. Dazu werden einfach die Zahlen $1, 2, \ldots, n$ und deren Bilder unter der Abbildung $\sigma \in \mathfrak{S}_n$ in zwei Zeilen übereinander angeordnet

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} .$$

Die Gruppe $\mathfrak{S}_3$ besteht aus den folgenden sechs Elementen

$$\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} .$$

Die Anzahl der Elemente der Gruppe $\mathfrak{S}_n$ beträgt $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. Die Zahl $n!$, ausgesprochen als „n Fakultät“, ist mathematisch exakter rekursiv definiert: man setzt $0! := 1$ und $n! := n \cdot (n-1)!$ für alle $n \geq 1$.

[7] Siehe Definition 6.3.3.

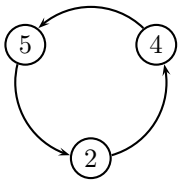
Durch die folgende Rechnung erkennen wir, dass $\mathfrak{S}_3$ *nicht* abelsch ist:

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\neq\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\ .$$

Besonders für größere n ist die Benutzung von Wertetabellen ziemlich aufwändig. Es ist dann günstiger, die platzsparendere *Zyklenschreibweise* zu verwenden. Um die Zerlegung einer Permutation σ in ein Produkt von Zyklen zu bestimmen, startet man mit irgendeinem Element $k \in \{1,\dots,n\}$ und schreibt die iterierten Bilder dieser Zahl hintereinander in eine Liste $(k,\sigma(k),\sigma(\sigma(k)),\dots)$. Die Liste wird mit einer schließenden Klammer beendet, sobald man wieder auf das Startelement k trifft. So ist zum Beispiel

$$\begin{pmatrix}1&2&3&4&5&6\\1&4&3&5&2&6\end{pmatrix}=(2\,4\,5)=(4\,5\,2)=(5\,2\,4)\ .$$

Diesen Zyklus kann man sich etwa wie im folgenden Bild vorstellen:



Jede durch die Permutation σ nicht veränderte Zahl k, d.h. $k=\sigma(k)$, wird nicht aufgeschrieben. Jedes von σ veränderte Element der Menge $\{1,\dots,n\}$ muss jedoch betrachtet werden. Im Allgemeinen werden wir daher ein Produkt mehrerer Zyklen erhalten:

$$\begin{pmatrix}1&2&3&4&5&6\\6&4&3&5&2&1\end{pmatrix}=(1\,6)\circ(2\,4\,5)\ .$$

Der Vorteil der effektiveren Schreibweise wird mit einer Mehrdeutigkeit erkauft. So kann zum Beispiel der Zyklus $(1\,2)$ jeder der folgenden Wertetabellen entsprechen:

$$\begin{pmatrix}1&2\\2&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6\\2&1&3&4&5&6\end{pmatrix},\ \text{etc.}$$

je nachdem in welchem $\mathfrak{S}_n$ wir gerade arbeiten. Das ist jedoch nicht weiter dramatisch, da $\mathfrak{S}_{n-1}$ auf natürliche Weise als Untergruppe in $\mathfrak{S}_n$ enthalten ist, siehe Beispiel 1.3.14.
Die sechs Elemente der Gruppe $\mathfrak{S}_3$ haben in Zyklenschreibweise die Gestalt

$$\mathrm{Id} = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \quad (1\,2) = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \quad (1\,3) = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix},$$
$$(2\,3) = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \quad (1\,2\,3) = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \quad (1\,3\,2) = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}.$$

Alle Elemente dieser Gruppe sind einfache Zyklen. Ab $n \geq 4$ gibt es Elemente in $\mathfrak{S}_n$, die keine einfachen Zyklen sind, zum Beispiel $(12)(34) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & \cdots \\ 2 & 1 & 4 & 3 & \cdots \end{smallmatrix}\right)$.

Beispiel 1.3.4. Obwohl wir uns dem Gruppenbegriff durch Abstraktion von den ganzen Zahlen genähert haben, liegt sein historischer Ursprung in der Geometrie. Viele Menschen sind von Symmetrien in Natur, Kunst und Wissenschaft fasziniert. Das mathematische Studium von Symmetrien führt unausweichlich zum Begriff der *Symmetriegruppe*. Die elementarsten Beispiele erhält man als Menge aller Symmetrien einer ebenen Figur wie etwa eines Kreises oder eines Dreiecks. Unter einer Symmetrie wollen wir hier eine Kongruenztransformation einer solchen Figur verstehen, also eine Verschiebung, Drehung oder Spiegelung, unter der diese Figur auf sich selbst abgebildet wird.
Die Menge aller Symmetrien eines regelmäßigen ebenen n-Ecks ($n \geq 3$) bezeichnet man mit D_n. Sie heißt *Diedergruppe* (auch *Di-edergruppe* oder *Diëdergruppe*). Zur Illustration betrachten wir hier den Fall $n = 5$ (Abb. 1.1).

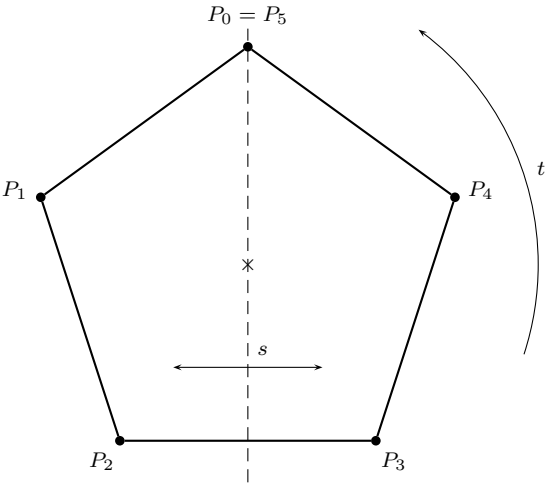


Abb. 1.1 Geometrische Bedeutung der Gruppe D_5

Es gibt keine Verschiebung, welche ein Fünfeck in sich selbst überführt. Als Symmetrien kommen also nur Drehungen und Spiegelungen in Frage. Jede Drehung mit Zentrum im Mittelpunkt des Fünfecks um einen Winkel der

Größe $k \cdot \frac{2\pi}{5}, k \in \mathbb{Z}$, bildet das Fünfeck auf sich selbst ab. Mit $t \in D_5$ bezeichnen wir die Drehung um $\frac{2\pi}{5}$ entgegen dem Uhrzeigersinn. Die weiteren Drehungen sind dann t^2, t^3, t^4 und $t^5 = \mathrm{Id}$.
Jede Kongruenztransformation ist durch ihr Wirken auf der Menge der Eckpunkte $\{P_0, P_1, P_2, P_3, P_4\}$ vollständig festgelegt. Daher ist $t \in D_5$ durch $t(P_i) = P_{i+1}$ gegeben, wobei wir die Indizes als Elemente von $\mathbb{Z}/5\mathbb{Z}$ auffassen, also $P_5 = P_0$ setzen. Diese bequeme Vereinbarung nutzen wir auch im Folgenden.
Als weitere Symmetrien kommen noch die Spiegelungen an den Verbindungsgeraden des Mittelpunktes mit den Eckpunkten des Fünfecks in Betracht. Sei zum Beispiel s die Spiegelung an der Achse durch P_0, siehe Abb. 1.1. Dann gilt $s(P_i) = P_{5-i}$ und s, st, st^2, st^3, st^4 ist eine komplette Liste aller Spiegelungen, die das Fünfeck auf sich selbst abbilden. Das ergibt:

$$D_5 = \{1, t, t^2, t^3, t^4, s, st, st^2, st^3, st^4\} .$$

Offenbar gilt $t^5 = 1$ und $s^2 = 1$. Außerdem prüft man durch Berechnung der Wirkung auf den Eckpunkten die Identität $tst = s$ leicht nach. Aus ihr folgt $ts = st^{-1}$ und wegen $t^{-1} = t^4$ sehen wir daraus, dass D_5 nicht abelsch ist. Ausgehend von diesen Relationen kann man alle Produkte in D_5 berechnen. Für allgemeines $n \geq 3$ ist die Beschreibung von D_n analog. Die Gruppe D_n besteht aus den $2n$ Elementen $1, t, t^2, \ldots, t^{n-1}, s, st, st^2, \ldots, st^{n-1}$. Jedes beliebige Produkt lässt sich unter Verwendung der Relationen $t^n = 1, s^2 = 1$ und $tst = s$ berechnen.

Satz 1.3.5 *In jeder Gruppe $(G, *)$ gilt:*

(a) *Es gibt genau ein neutrales Element $e \in G$.*
(b) *Für alle $a \in G$ gilt $a * e = a$.*
(c) *Zu jedem $a \in G$ gibt es genau ein a' mit $a' * a = e$.*
(d) *Wenn $a' * a = e$, dann gilt auch $a * a' = e$.*
(e) *In G kann man kürzen, das heißt aus $a * b = a * c$ folgt stets $b = c$ und aus $b * a = c * a$ folgt stets $b = c$.*

Beweis. Wir beginnen mit (d). Sei a'' ein inverses Element zu a', welches nach (1.17) in Definition 1.3.1 existiert und $a'' * a' = e$ erfüllt. Wir erhalten

$$\begin{aligned} a * a' &\underset{(1.16)}{=} e * (a * a') = (a'' * a') * (a * a') \\ &\underset{(1.15)}{=} a'' * \big((a' * a) * a'\big) \underset{(1.17)}{=} a'' * (e * a') \\ &\underset{(1.16)}{=} a'' * a' = e, \qquad \text{wie gewünscht.} \end{aligned}$$

Damit folgt (b): $a * e \underset{(1.17)}{=} a * (a' * a) \underset{(1.15)}{=} (a * a') * a \underset{(d)}{=} e * a \underset{(1.16)}{=} a.$

Als Nächstes zeigen wir (a). Dazu nehmen wir an, dass $\bar{e}$ ein weiteres neutrales Element ist. Das heißt nach (1.16), dass für jedes $a \in G$ die Gleichung $\bar{e} * a = a$ erfüllt ist, insbesondere $e = \bar{e} * e$. Wenn wir in (b) $a = \bar{e}$ einsetzen, erhalten wir $\bar{e} * e = \bar{e}$ und somit die gewünschte Eindeutigkeit $e = \bar{e}$.
Nun können wir (c) beweisen. Wenn $\bar{a}'$ ein weiteres Inverses zu a ist, dann gilt $\bar{a}' * a = e$. Es ergibt sich $\bar{a}' \underset{(b)}{=} \bar{a}' * e \underset{(d)}{=} \bar{a}' * (a * a') \underset{(1.15)}{=} (\bar{a}' * a) * a' = e * a' \underset{(1.16)}{=} a'$.
Schließlich folgt (e) durch Multiplikation mit a' von links (bzw. rechts). □

Bemerkung 1.3.6. Die Aussage (d) in Satz 1.3.5 besagt *nicht*, dass die Gruppe G abelsch ist. Sie besagt nur, dass ein von links zu multiplizierendes Inverses mit dem von rechts zu multiplizierenden Inversen übereinstimmt.

Bemerkung 1.3.7. Aus Satz 1.3.5 (c) folgt $(a^{-1})^{-1} = a$ und $(a * b)^{-1} = b^{-1} * a^{-1}$ in jeder multiplikativ geschriebenen Gruppe.

Definition 1.3.8. (1) Eine nichtleere Teilmenge $U \subset G$ einer Gruppe $(G, *)$ heißt *Untergruppe* von G, wenn für alle $a, b \in U$ stets $a * b \in U$ und $a^{-1} \in U$ gilt.
(2) Eine Abbildung $f : G \to H$ zwischen zwei Gruppen $(G, *)$ und $(H, \circ)$ heißt *Gruppenhomomorphismus*, wenn für alle $a, b \in G$ stets $f(a * b) = f(a) \circ f(b)$ gilt.
(3) Ein bijektiver[8] Gruppenhomomorphismus heißt *Isomorphismus*. Wenn es hervorzuheben gilt, dass $f : G \to H$ ein Isomorphismus ist, dann schreiben wir $f : G \xrightarrow{\sim} H$.

Bemerkung 1.3.9. Wenn $U \subset G$ eine Untergruppe ist, dann ist $(U, *)$ eine Gruppe, wobei $*$ die Einschränkung der Verknüpfung $*$ von G auf U ist.

Bemerkung 1.3.10. Da jede Untergruppe $U \subset G$ nichtleer ist, gibt es mindestens ein Element $a \in U$. Die Definition besagt, dass damit auch $a^{-1} \in U$ und $e = a^{-1} * a \in U$ sein muss. Daher ist das neutrale Element $e \in G$ in jeder Untergruppe enthalten. Man kann also in Definition 1.3.8 die Bedingung $U \neq \emptyset$ durch die gleichwertige Forderung $e \in U$ ersetzen.

Bemerkung 1.3.11. Wenn $f : (G, *) \to (H, \circ)$ ein Gruppenhomomorphismus ist und $e_G \in G$, $e_H \in H$ die neutralen Elemente bezeichnen, dann gilt $f(e_G) = e_H$, denn $e_H \circ f(e_G) = f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G)$, woraus wegen Satz 1.3.5 (e) $e_H = f(e_G)$ folgt.
Ferner gilt $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$, was wegen der Eindeutigkeit des Inversen, Satz 1.3.5 (c), aus $e_H = f(e_G) = f(a^{-1} * a) = f(a^{-1}) \circ f(a)$ folgt.

Bemerkung 1.3.12. Wenn $f : G \to H$ ein Isomorphismus ist, dann ist auch $f^{-1} : H \to G$ ein Isomorphismus.

Beispiel 1.3.13. $2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ ist Untergruppe von $(\mathbb{Z}, +)$. Die ungeraden Zahlen $\{2n + 1 \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ bilden keine Untergruppe, zum Beispiel weil 0 nicht darin enthalten ist.

[8] Siehe Definition 6.3.3.

Beispiel 1.3.14. Die Abbildung $f : \mathfrak{S}_n \to \mathfrak{S}_{n+1}$, die durch

$$f(\sigma)(k) := \begin{cases} \sigma(k) & 1 \le k \le n \\ n+1 & k = n+1 \end{cases}$$

definiert ist, ist ein Gruppenhomomorphismus. In der Sprache der Wertetabellen operiert dieser Homomorphismus wie folgt, wenn wir $i_k = \sigma(k)$ setzen:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 \\ i_1 & i_2 & i_3 & \dots & i_n & n+1 \end{pmatrix} .$$

Wenn wir f auf Zyklen anwenden, sehen wir keine Veränderung in der Schreibweise, es ändert sich nur die Interpretation. Das Bild der Abbildung f ist die Untergruppe $f(\mathfrak{S}_n) = U_n := \{\sigma' \in \mathfrak{S}_{n+1} \mid \sigma'(n+1) = n+1\} \subset \mathfrak{S}_{n+1}$ und f definiert einen Isomorphismus $f : \mathfrak{S}_n \xrightarrow{\sim} U_n$. Daher können wir $\mathfrak{S}_n$ als Untergruppe von $\mathfrak{S}_{n+1}$ auffassen. Dadurch ist die scheinbar ungenaue Zyklenschreibweise mathematisch gerechtfertigt, bei der z.B. $(1\,2)$ als Element in jedem $\mathfrak{S}_n$ aufgefasst werden kann.

Beispiel 1.3.15. Da eine Kongruenztransformation eines regelmäßigen ebenen n-Ecks ($n \ge 3$) durch die Bildpunkte der Ecken des n-Ecks festgelegt ist, können wir, nachdem wir die Ecken nummeriert haben, $D_n \subset \mathfrak{S}_n$ als Untergruppe auffassen.

Beispiel 1.3.16. Die Drehungen $\{1, t, t^2, t^3, t^4\} \subset D_5$ bilden eine Untergruppe. Allgemeiner, wenn $(G, *)$ eine Gruppe und $g \in G$ irgendein Element ist, dann ist die Teilmenge

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\dots, g^{-3}, g^{-2}, g^{-1}, e_G, g, g^2, g^3, \dots\}$$

stets Untergruppe von G.

Definition 1.3.17. Eine Gruppe G heißt *zyklisch*, wenn es ein $g \in G$ gibt, so dass $\langle g \rangle = G$ ist. Wir sagen dann, *g erzeugt die Gruppe G.*

Für jedes $n \in \mathbb{Z}$ ist $\langle n \rangle = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ eine zyklische Untergruppe von $(\mathbb{Z}, +)$ mit Erzeuger n. Hier ist zu beachten, dass wir wegen der additiven Schreibweise kn statt n^k schreiben.

Satz 1.3.18 *Zu jeder Untergruppe $U \subset \mathbb{Z}$ von $(\mathbb{Z}, +)$ gibt es ein $n \in \mathbb{Z}$ mit $U = n\mathbb{Z}$.*

Beweis. Sei $U^+ := \{k \in U \mid k \ge 1\}$. Wenn $U^+ = \emptyset$, dann ist $U = \{0\}$, denn mit $k \in U$ ist auch $-k \in U$. In diesem Fall folgt die Behauptung mit $n = 0$. Sei nun $U^+ \neq \emptyset$. Dann gibt es eine kleinste Zahl $n \in U^+$. Jedes $a \in U$ lässt sich als $a = r + s \cdot n$ mit ganzen Zahlen r, s schreiben, so dass $0 \le r < n$

(Division mit Rest). Da die Untergruppe U sowohl a als auch n enthält, ist auch $r = a - sn \in U$. Da n das kleinste Element von U^+ und $r < n$ ist, folgt $r \notin U^+$. Daher ist $r = 0$ und somit $a = s \cdot n$. Daraus ergibt sich $U = n\mathbb{Z}$. □

Beispiel 1.3.19. Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(k) := n \cdot k$ (fixiertes n) ist ein Gruppenhomomorphismus, denn $f(k + l) = n \cdot (k + l) = n \cdot k + n \cdot l = f(k) + f(l)$.
Die durch $f(k) := k^2$ definierte Abbildung ist hingegen kein Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ der additiven Gruppen, denn $f(2) = 4 \neq 1 + 1 = f(1) + f(1)$.
Wenn $(G, *)$ eine Gruppe ist und $a \in G, (a \neq e)$, dann ist durch $f(g) := a * g$ kein Gruppenhomomorphismus $f : G \to G$ definiert, da $f(e) = a * e = a \neq e$.

Wenn $U \subset G$ eine Untergruppe einer Gruppe $(G, *)$ ist, dann liefert uns die folgende Definition eine Äquivalenzrelation (siehe Abschnitt 6.3) auf der Menge G:

$$a \sim b \iff a^{-1} * b \in U \,. \tag{1.19}$$

Reflexivität: Da $U \subset G$ eine Untergruppe ist, gilt $a^{-1} * a = e \in U$ für alle $a \in G$. Daher folgt $a \sim a$.

Symmetrie: Wenn $a \sim b$, dann gilt $a^{-1} * b \in U$ und somit $(a^{-1} * b)^{-1} \in U$. Unter Verwendung von Bemerkung 1.3.7 folgt daraus $(a^{-1} * b)^{-1} = b^{-1} * (a^{-1})^{-1} = b^{-1} * a \in U$, also $b \sim a$.

Transitivität: Wenn $a \sim b$ und $b \sim c$, dann gilt $a^{-1} * b \in U$ und $b^{-1} * c \in U$. Also ist $a^{-1} * c = (a^{-1} * b) * (b^{-1} * c) \in U$ und damit $a \sim c$.

Aus der Definition folgt unmittelbar, dass die Äquivalenzklassen die Beschreibung $[a] = a * U := \{a * b \mid b \in U\}$ besitzen. Die Abbildung $U \to a * U$, die b auf $a * b$ abbildet, ist bijektiv, ihr Inverses bildet c auf $a^{-1} * c$ ab.
Die Mengen $a * U$ nennt man *Linksnebenklassen*. Für die Äquivalenzklassenmenge $G/\sim$ schreiben wir G/U und nennen sie die *Menge der Linksnebenklassen*. Den Spezialfall $U = n\mathbb{Z} \subset G = \mathbb{Z}$ haben wir ausführlich im Abschnitt 1.2 studiert.

Satz 1.3.20 (Lagrange[9]) *Wenn $(G, *)$ eine endliche Gruppe und $U \subset G$ eine Untergruppe von G ist, dann gilt:*

$$|G| = |U| \cdot |G/U| \,.$$

Beweis. Da die Abbildung $U \to a * U$, die $b \in U$ auf das Element $a * b \in a * U$ abbildet, bijektiv ist, haben alle Nebenklassen die gleiche Zahl von Elementen, nämlich $|U|$. Da nach Satz 6.3.16 jedes Element aus G in genau einer Nebenklasse liegt, ist die Zahl der Elemente von G gleich der Zahl der Nebenklassen $|G/U|$ multipliziert mit $|U|$. □

[9] Joseph Louis Lagrange (1736–1813), französisch-italienischer Mathematiker.

Definition 1.3.21. (1) Die Anzahl der Elemente $\mathrm{ord}(G) := |G|$ einer Gruppe G heißt *Ordnung der Gruppe G.*
(2) Für jedes Element $g \in G$ einer Gruppe G heißt $\mathrm{ord}(g) := \mathrm{ord}(\langle g \rangle)$ *Ordnung des Elements g.*

Obwohl diese Definition auch für Gruppen mit unendlich vielen Elementen gültig ist, werden wir uns hier vorrangig mit Ordnungen in endlichen Gruppen befassen. Die Ordnung eines Elements einer endlichen Gruppe ist stets eine positive ganze Zahl. Die Definition der Ordnung eines Elements $g \in G$ übersetzt sich in

$$\mathrm{ord}(g) = m \iff \langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\} .$$

Insbesondere gilt $\mathrm{ord}(g) = 1 \iff g = e$. Die Ordnung von $g \in G$ ist die kleinste positive ganze Zahl m, für die $g^m = e$ ist. Im Fall einer additiven Gruppe ist $\mathrm{ord}(g) = \min\{k \geq 1 \mid k \cdot g = 0\}$.

Beispiel 1.3.22. (i) $\mathrm{ord}(\mathbb{Z}) = \infty$, $\mathrm{ord}(\mathfrak{S}_n) = n!$, $\mathrm{ord}(D_n) = 2n$.
(ii) In $(\mathbb{Z}, +)$ gilt: $\mathrm{ord}(0) = 1$ und $\mathrm{ord}(n) = \infty$ für $n \neq 0$.
(iii) Sei $[0] \neq [a] \in (\mathbb{Z}/n\mathbb{Z}, +)$, dann ist $\mathrm{ord}([a]) = n/\mathrm{ggT}(a, n)$. Wenn n eine Primzahl ist, gilt folglich für $[a] \neq [0]$ stets $\mathrm{ord}([a]) = n$ in $(\mathbb{Z}/n\mathbb{Z}, +)$.

Satz 1.3.23 *Sei $(G, *)$ eine endliche Gruppe.*

(1) *Wenn $U \subset G$ Untergruppe ist, so ist* $\mathrm{ord}(U)$ *ein Teiler von* $\mathrm{ord}(G)$.
(2) *Für jedes $g \in G$ ist* $\mathrm{ord}(g)$ *ein Teiler von* $\mathrm{ord}(G)$.
(3) *Für alle $g \in G$ gilt $g^{\mathrm{ord}(G)} = e$.*

Beweis. Die Aussage (1) ergibt sich unmittelbar aus dem Satz 1.3.20 unter Benutzung des neu eingeführten Begriffes der Ordnung. Aussage (2) ergibt sich aus (1), denn $\mathrm{ord}(g) = \mathrm{ord}(\langle g \rangle)$.
Da es nach (2) eine ganze Zahl k gibt, für die $\mathrm{ord}(G) = k \cdot \mathrm{ord}(g)$ gilt, ergibt sich $g^{\mathrm{ord}(G)} = g^{k \cdot \mathrm{ord}(g)} = \left(g^{\mathrm{ord}(g)}\right)^k = e^k = e$. □

Zur Anwendung dieses Satzes auf die multiplikative Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ erinnern wir uns an die Eulerfunktion (Definition 1.1.10):

$$\varphi(n) = \left|\left\{k \in \mathbb{Z} \middle| 1 \leq k < n, \mathrm{ggT}(k, n) = 1\right\}\right| = \mathrm{ord}\left((\mathbb{Z}/n\mathbb{Z})^*\right) .$$

Satz 1.3.24 (kleiner Satz von Fermat[10]) (1) *Für jede Primzahl p und jede ganze Zahl a, die nicht durch p teilbar ist, gilt: $a^{p-1} \equiv 1 \mod p$.*
(2) *Wenn a, n teilerfremde ganze Zahlen sind, dann gilt $a^{\varphi(n)} \equiv 1 \mod n$.*

[10] Pierre de Fermat (1601–1665), französischer Mathematiker.

Beweis. Da $\varphi(p) = p-1$ für jede Primzahl p und $\varphi(n) = \operatorname{ord}((\mathbb{Z}/n\mathbb{Z})^*)$, folgt die Behauptung aus Satz 1.3.23 (3). □

Beispiel 1.3.25. (i) Wenn $\operatorname{ggT}(a, 10) = 1$, dann ist $a^4 \equiv 1 \mod 10$, da $\varphi(10) = \varphi(5) \cdot \varphi(2) = 4$. Mit anderen Worten: die vierte Potenz jeder ungeraden Zahl, die nicht auf 5 endet, hat als letzte Ziffer eine 1. Aus dieser Kongruenz ergibt sich auch, dass für jede ganze Zahl a, die zu 10 teilerfremd ist, die letzte Ziffer einer beliebigen Potenz a^m gleich der letzten Ziffer von a^r ist, sobald $r \equiv m \mod 4$. Dies ergibt sich aus $m = 4k + r$ und $a^m \equiv a^{4k+r} \equiv (a^4)^k \cdot a^r \equiv 1^k \cdot a^r \equiv a^r \mod 10$.

(ii) Ebenso lässt sich der Rechenaufwand für die Bestimmung von zwei oder mehr Endziffern großer Zahlen verringern. Bei der Berechnung der letzten zwei Ziffern kann man wegen $\varphi(100) = \varphi(5^2 \cdot 2^2) = 5 \cdot 4 \cdot 2 = 40$ die Exponenten modulo 40 reduzieren. Da $9^9 \equiv 9 \mod 40$, folgt zum Beispiel $9^{(9^9)} \equiv 9^9 \mod 100$. Ohne technische Hilfsmittel berechnet man leicht $9^9 \equiv 89 \mod 100$. Die letzten beiden Ziffern von $9^{(9^9)}$ lauten also 89.

Als Nächstes werden wir den Prozess der Vererbung der Addition von $\mathbb{Z}$ auf $\mathbb{Z}/n\mathbb{Z}$ (Definition 1.2.3) für Gruppen verallgemeinern.

Satz 1.3.26 *Sei $(G, *)$ eine abelsche Gruppe und $U \subset G$ eine Untergruppe. Dann ist auf der Menge der Linksnebenklassen G/U durch $[a] * [b] := [a * b]$ die Struktur einer abelschen Gruppe definiert.*

Beweis. Das Hauptproblem ist hier, ebenso wie bei Satz 1.2.4, die Wohldefiniertheit. Dazu ist zu zeigen, dass aus $[a] = [a']$ und $[b] = [b']$ stets $[a' * b'] = [a * b]$ folgt. Entsprechend der in (1.19) gegebenen Definition bedeuten $[a] = [a']$ und $[b] = [b']$, dass es $r, s \in U$ gibt, so dass $a' = a * r$ und $b' = b * s$ gilt. Damit ergibt sich $a' * b' = (a * r) * (b * s) = a * (r * b * s) = a * (b * r * s)$. Für die letzte Gleichung haben wir benutzt, dass G abelsch ist. Da U eine Untergruppe ist, gilt $r * s \in U$ und es folgt $a' * b' = (a * b) * (r * s) \in (a * b) * U$, also tatsächlich $[a' * b'] = [a * b]$. Die Gruppeneigenschaften übertragen sich nun unmittelbar von G auf G/U. □

Da die Gruppen $\mathfrak{S}_n$ und D_n nicht abelsch sind, entsteht die Frage, ob für solche Gruppen die Vererbung der Gruppenstruktur auf Linksnebenklassenmengen ebenfalls möglich ist. Als Beispiel betrachten wir die Untergruppe $\{1, s\} \subset D_5$. Sie besitzt die folgenden $5 = \operatorname{ord}(D_5)/2$ Nebenklassen

$$[1] = \{1, s\},\ [t] = \{t, ts\},\ [t^2] = \{t^2, t^2 s\},\ [t^3] = \{t^3, t^3 s\},\ [t^4] = \{t^4, t^4 s\}\ .$$

Um die Gruppenstruktur wie in Satz 1.3.26 vererben zu können, ist es wegen $[t] = [ts]$ notwendig, dass auch $[t^2] = [t] \cdot [t] = [ts] \cdot [t] = [tst]$ gilt. Da $tst = s$ ist, müsste dann $[t^2] = [s]$ sein. Ein Blick auf die Liste der fünf Nebenklassen verrät, dass t^2 und s in verschiedenen Nebenklassen liegen. Die

Gruppenstruktur vererbt sich daher *nicht* auf $D_5/\{1, s\}$. Beim Umgang mit nicht-abelschen Gruppen ist also Vorsicht geboten.
Bei genauerer Betrachtung des Beweises von Satz 1.3.26 sehen wir, dass nur an einer Stelle benutzt wurde, dass G abelsch ist, nämlich beim Beweis von $a * (r * b * s) \in (a * b) * U$. Diesen Beweisschritt kann man jedoch auch ausführen, wenn es ein Element $r' \in U$ gibt, so dass $r * b = b * r'$, denn dann folgt $a * (r * b * s) = a * (b * r' * s) \in (a * b) * U$.
Eine Untergruppe $U \subset G$, welche die Eigenschaft hat, dass für jedes $b \in G$ und jedes $r \in U$ ein $r' \in U$ mit $r * b = b * r'$ existiert, nennt man einen *Normalteiler*. Mit anderen Worten: Eine Untergruppe $U \subset G$ ist genau dann Normalteiler, wenn $b * U = U * b$ für alle $b \in G$. Mit dem gleichen Beweis wie von Satz 1.3.26 erhalten wir nun, dass sich die Gruppenstruktur von G auf G/U vererbt, sobald $U \subset G$ ein Normalteiler ist.
Wenn G abelsch ist, dann ist jede Untergruppe $U \subset G$ ein Normalteiler, da stets $r * b = b * r$. In nicht-abelschen Gruppen gibt es im Allgemeinen jedoch Untergruppen, die nicht Normalteiler sind. Zum Beispiel ist $\{1, s\} \subset D_5$ kein Normalteiler, da $ts \notin \{t, st\}$ in D_5.

Bemerkung 1.3.27. Wenn $U \subset G$ Normalteiler, dann ist für jedes $a \in U$ die Nebenklasse $[a] \in G/U$ das neutrale Element der Gruppe G/U.

Die Begriffe *Untergruppe* und *Homomorphismus* sind die wichtigsten Werkzeuge zur Untersuchung von Gruppen, die wir bisher kennengelernt haben. Im Folgenden beschäftigen wir uns damit, wie sie miteinander zusammenhängen. Als wichtigstes Resultat werden wir den Homomorphiesatz beweisen. Er erlaubt uns, unter geeigneten Voraussetzungen präzise Information über die Struktur bestimmter Gruppen herauszufinden.

Definition 1.3.28. Für jeden Gruppenhomomorphismus $f : G \to H$ heißt

$$\ker(f) := \{g \in G \mid f(a) = e_H\} \subset G \text{ der } \textit{Kern} \text{ von } f \text{ und}$$
$$\mathrm{im}(f) := \{f(a) \mid a \in G\} \subset H \text{ das } \textit{Bild} \text{ von } f.$$

Bemerkung 1.3.29. Ein Gruppenhomomorphismus $f : G \to H$ ist genau dann surjektiv, wenn $\mathrm{im}(f) = H$.

Satz 1.3.30 *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(1) $\ker(f) \subset G$ *ist eine Untergruppe.*
(2) $\mathrm{im}(f) \subset H$ *ist eine Untergruppe.*
(3) f *ist genau dann injektiv*[11]*, wenn* $\ker(f) = \{e_G\}$.

[11] Siehe Definition 6.3.3.

Beweis. (1) Da $f(e_G) = e_H$, ist $e_G \in \ker(f)$ und damit $\ker(f) \neq \emptyset$. Wenn $a, b \in \ker(f)$, dann ist $f(a) = e_H$ und $f(b) = e_H$. Daraus ergibt sich $f(a*b) = f(a) * f(b) = e_H * e_H = e_H$ und $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$. Also gilt $a * b \in \ker(f)$ und $a^{-1} \in \ker(f)$, das heißt $\ker(f)$ ist Untergruppe von G.
(2) Da $G \neq \emptyset$, ist auch $\mathrm{im}(f) \neq \emptyset$. Wenn $a' = f(a) \in \mathrm{im}(f)$ und $b' = f(b) \in \mathrm{im}(f)$, dann ist $a' * b' = f(a) * f(b) = f(a * b) \in \mathrm{im}(f)$ und $(a')^{-1} = f(a)^{-1} = f(a^{-1}) \in \mathrm{im}(f)$. Somit ist $\mathrm{im}(f)$ eine Untergruppe von H.
(3) Wenn f injektiv ist, dann ist $\ker(f) = \{e_G\}$. Wenn umgekehrt $\ker(f) = \{e_G\}$ und $f(a) = f(b)$, dann folgt $e_H = f(a) * f(b)^{-1} = f(a * b^{-1})$, d.h. $a * b^{-1} \in \ker(f) = \{e_G\}$. Damit ist $a * b^{-1} = e_G$, d.h. $a = b$, und f ist injektiv. □

Bemerkung 1.3.31. Für jeden Gruppenhomomorphismus $f : G \to H$ ist $\ker(f) \subset G$ ein *Normalteiler*, denn für $a \in G$, $b \in \ker(f)$ ist $f(a * b * a^{-1}) = f(a) * f(b) * f(a)^{-1} = f(a) * f(a)^{-1} = e_H$, also $a * b * a^{-1} \in \ker(f)$ und somit $a * b = b' * a$ für ein $b' \in \ker(f)$.

Satz 1.3.32 (Homomorphiesatz) *Sei $f : G \to H$ ein Gruppenhomomorphismus und $G/\ker(f)$ mit der von G vererbten Gruppenstruktur versehen. Dann ist die durch $\bar{f}\big([a]\big) := f(a)$ definierte Abbildung ein Isomorphismus*

$$\bar{f} : G/\ker(f) \longrightarrow \mathrm{im}(f) \ .$$

Beweis. Nach Bemerkung 1.3.31 ist $\ker(f) \subset G$ stets Normalteiler, also wird die Gruppenstruktur von G auf $G/\ker(f)$ vererbt. Die Wohldefiniertheit von $\bar{f}$ sehen wir wie folgt: Sei $[a] = [a'] \in G/\ker(f)$, dann gibt es ein $b \in \ker(f) \subset G$ mit $a' = a * b$. Damit erhalten wir $f(a') = f(a * b) = f(a) * f(b) = f(a) * e_H = f(a)$, wie gewünscht. Aus der Definition von $\bar{f}$ folgt sofort, dass $\bar{f}$ ein surjektiver Gruppenhomomorphismus ist. Für den Beweis der Injektivität betrachten wir $[a] \in \ker(\bar{f}) \subset G/\ker(f)$. Dann ist $f(a) = \bar{f}([a]) = e_H$, d.h. $a \in \ker(f)$ und somit $[a] = e_{G/\ker(f)}$. Wegen Satz 1.3.30 (3) ist $\bar{f}$ injektiv und daher ein Isomorphismus. □

Als erste Anwendung erhalten wir den folgenden Satz.

Satz 1.3.33 *Sei G eine Gruppe und $g \in G$ ein Element der Ordnung n. Dann gibt es einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$.*

Beweis. Durch $f(k) := g^k$ ist ein Homomorphismus $f : \mathbb{Z} \to G$ definiert. Offenbar ist $\mathrm{im}(f) = \langle g \rangle$ und $\ker(f) = n\mathbb{Z}$, wobei $n = \mathrm{ord}(g)$. Daher ist nach Satz 1.3.32 die induzierte Abbildung $\bar{f} : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ ein Isomorphismus. □

Als weitere Anwendung des Homomorphiesatzes können wir nun die bereits im Satz 1.1.11 angekündigte Formel für die Eulersche φ-Funktion beweisen.

Für Anwendungen praktischer Art ist allerdings der im Abschnitt 1.4 gegebene konstruktive Beweis von größerer Bedeutung, vgl Satz 1.4.23.

Satz 1.3.34 *Wenn m, n zwei teilerfremde ganze Zahlen sind, dann ist der durch $f\big([a]_{mn}\big) := \big([a]_m, [a]_n\big)$ gegebene Gruppenhomomorphismus*

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

ein Isomorphismus. Er bildet die Menge $(\mathbb{Z}/mn\mathbb{Z})^* \subset \mathbb{Z}/mn\mathbb{Z}$ bijektiv auf $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ ab. Insbesondere gilt $\varphi(mn) = \varphi(m)\varphi(n)$, falls $\mathrm{ggT}(m, n) = 1$.

Beweis. Sei $g : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ der durch $g(a) := \big([a]_m, [a]_n\big)$ definierte Gruppenhomomorphismus. Dann ist

$$\ker(g) = \{a \in \mathbb{Z} \mid a \equiv 0 \mod m \text{ und } a \equiv 0 \mod n\} .$$

Daraus sehen wir $mn\mathbb{Z} \subset \ker(g)$. Es gilt aber auch $\ker(g) \subset mn\mathbb{Z}$, denn jedes $a \in \ker(g)$ ist durch m und n teilbar. Das heißt, es gibt $k \in \mathbb{Z}$, so dass $a = kn$ ist und da $\mathrm{ggT}(m, n) = 1$ folgt dann $m \mid k$ aus Satz 1.1.7. Damit ist a durch mn teilbar und somit $\ker(g) \subset mn\mathbb{Z}$, also schließlich $\ker(g) = mn\mathbb{Z}$. Der Homomorphiesatz besagt dann, dass g einen Isomorphismus $\bar{g} : \mathbb{Z}/mn\mathbb{Z} \to \mathrm{im}(g)$ induziert. Das zeigt, dass $\mathrm{ord}(\mathrm{im}(\bar{g})) = \mathrm{ord}\,(\mathbb{Z}/mn\mathbb{Z}) = mn$ gilt. Weil $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ ebenfalls von Ordnung mn ist, muss $\mathrm{im}(\bar{g}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ gelten, und es folgt, dass $f = \bar{g}$ ein Isomorphismus ist.
Für die Aussage über $(\mathbb{Z}/mn\mathbb{Z})^*$ wechseln wir von der additiven zur multiplikativen Struktur von $\mathbb{Z}/mn\mathbb{Z}$. Obwohl wir erst im Abschnitt 1.4, bei der Beschäftigung mit Ringen, Addition und Multiplikation gleichzeitig betrachten werden, können wir bereits an dieser Stelle einen direkten Beweis geben. Wir benutzen dazu, dass für $[a] \in \mathbb{Z}/n\mathbb{Z}$ die Eigenschaft $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ zu $\mathrm{ggT}(a, n) = 1$ äquivalent ist[12]. Daher ist $f\big([a]_{mn}\big) = \big([a]_m, [a]_n\big)$ genau dann in $\big(\mathbb{Z}/m\mathbb{Z}\big)^* \times \big(\mathbb{Z}/n\mathbb{Z}\big)^*$ enthalten, wenn $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ggT}(a, n) = 1$ gilt. Für solche a gibt es ganze Zahlen r, s, r', s', so dass $ra + sn = 1$ und $r'a + s'm = 1$. Daraus erhalten wir $ram + smn = m$ und $1 = r'a + s'(ram + smn) = (r' + s'rm)a + (s's)mn$. Somit ist $\mathrm{ggT}(a, mn) = 1$, d.h. $[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$. Also ist $f\big((\mathbb{Z}/mn\mathbb{Z})^*\big) = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ und wegen der Injektivität von f folgt die Behauptung. □

Bemerkung 1.3.35. Man kann zeigen, dass jede endliche abelsche Gruppe isomorph zu einer Gruppe der Gestalt

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

[12] Beispiel 1.3.2 (v), Seite 26

ist. Durch Anwendung von Satz 1.3.34 kann man immer erreichen, dass die n_i Primzahlpotenzen sind.

Zum Abschluss dieses Abschnittes wenden wir uns nochmals der Fehlererkennung zu. Wir beginnen mit einer genaueren Analyse der Güte der Prüfzeichen bei EAN und ISBN, die wir am Ende von Abschnitt 1.2 betrachtet hatten. Anschließend benutzen wir den in diesem Abschnitt eingeführten Begriff der Gruppe, um diese Beispiele zu verallgemeinern. Das erlaubt es uns schließlich, die Prüfgleichung, die bei der Nummerierung ehemaliger deutscher Banknoten verwendet wurde, zu verstehen.
Sowohl EAN als auch ISBN-13 bestehen aus 13 Ziffern $a_1, \ldots, a_{13}$, welche die Prüfgleichung $\sum_{i=1}^{13} w_i a_i \equiv 0 \mod 10$ erfüllen. Dabei haben wir $w_i = 2 + (-1)^i$ gesetzt, oder im Klartext

$$w_i = \begin{cases} 1 & \text{falls } i \text{ ungerade,} \\ 3 & \text{falls } i \text{ gerade.} \end{cases}$$

Eine ISBN-10 besteht dagegen aus 10 Zeichen $a_1, \ldots, a_{10}$, die aus der Menge $\{0, 1, \ldots, 9, X\}$ sind. Das Symbol X wird als $[10] \in \mathbb{Z}/11\mathbb{Z}$ interpretiert und ist nur als a_{10} zugelassen. Die Prüfgleichung lautet $\sum_{i=1}^{10} i a_i \equiv 0 \mod 11$.
In beiden Situationen finden wir eine Prüfgleichung der Gestalt

$$\sum_{i=1}^{k} w_i a_i \equiv c \mod n \tag{1.20}$$

vor, wobei die a_i Repräsentanten von Elementen von $\mathbb{Z}/n\mathbb{Z}$ sind, die mit sogenannten „Gewichten“ $w_i \in \mathbb{Z}$ zu multiplizieren sind.
Wir können ganz allgemein mit einem endlichen Alphabet starten und Prüfgleichungen für Worte fester Länge untersuchen. Dazu werden die Elemente des Alphabets nummeriert, wodurch wir eine Bijektion zwischen einem n Symbole enthaltenden Alphabet und $\mathbb{Z}/n\mathbb{Z}$ erhalten. Wenn die Wortlänge gleich k ist, dann wählen wir k Gewichte $[w_i] \in \mathbb{Z}/n\mathbb{Z},\ i = 1, \ldots, k$ und fixieren ein Element $[c] \in \mathbb{Z}/n\mathbb{Z}$. In dieser Situation messen wir die Güte der Prüfgleichung (1.20) durch die Zahl der Fehler, die durch sie erkannt werden. Bei der manuellen Übermittlung von Daten sind typische Fehler:

Einzelfehler: Genau eines der a_i ist falsch.
Transposition: Zwei benachbarte Symbole a_i und a_{i+1} sind vertauscht.

Um festzustellen, ob die Prüfgleichung (1.20) diese Fehler erkennt, nehmen wir an, das korrekte Wort lautet $a_1 a_2 \ldots a_k$ und das möglicherweise fehlerhaft übermittelte ist $b_1 b_2 \ldots b_k$.
Über das korrekte Wort, welches uns als Empfänger des Wortes $b_1 b_2 \ldots b_k$ ja nicht wirklich bekannt ist, wissen wir lediglich, dass die Prüfgleichung

$$\sum_{i=1}^{k} w_i a_i \equiv c \mod n$$

gilt. Als weitere Information können wir die Summe $\sum_{i=1}^{k} w_i b_i$ berechnen. Deshalb kennen wir auch die *Diskrepanz*

$$\delta := \sum_{i=1}^{k} w_i(a_i - b_i) \equiv c - \sum_{i=1}^{k} w_i b_i \mod n\ .$$

Bei Vorliegen eines Einzelfehlers bzw. einer Transposition heißt das konkret:

Einzelfehler: Wenn nur a_j falsch ist, dann ist $\delta \equiv w_j(a_j - b_j) \mod n$;
Transposition: Wenn $b_{j+1} = a_j$ und $b_j = a_{j+1}$, ansonsten aber alles korrekt übermittelt wurde, dann ist $\delta \equiv (w_j - w_{j+1}) \cdot (a_j - a_{j+1}) \mod n$.

Ein Fehler wird erkannt, wenn die Prüfsumme $\sum_{i=1}^{k} w_i b_i$ nicht kongruent c modulo n ist, also genau dann, wenn die Diskrepanz δ von Null verschieden ist. Das führt auf folgende Bedingungen zur Fehlererkennung:

Einzelfehler: Ein Fehler liegt vor, wenn $[a_j] \neq [b_j]$. Er wird erkannt, wenn dies $[w_j] \cdot ([a_j] - [b_j]) \neq [0]$ zur Folge hat.
Transposition: Ein Fehler liegt vor, wenn $[a_j] \neq [a_{j+1}]$. Er wird erkannt, wenn dann auch $([w_j] - [w_{j+1}])([a_j] - [a_{j+1}]) \neq [0]$ gilt.

Um jeden Einzelfehler erkennen zu können, muss $[w_j]$ ein multiplikatives Inverses besitzen, das heißt $[w_j] \in (\mathbb{Z}/n\mathbb{Z})^*$. Diese Bedingung ist für EAN und ISBN-10 erfüllt.
Zur Erkennung aller Transpositionen muss $[w_j] - [w_{j+1}] \in (\mathbb{Z}/n\mathbb{Z})^*$ sein. Bei der EAN ist jedoch $[w_j] - [w_{j+1}] = \pm[2] \notin (\mathbb{Z}/10\mathbb{Z})^*$, denn $\mathrm{ggT}(\pm 2, 10) = 2$. Daher werden Transpositionen zweier Zahlen, deren Differenz fünf ist, durch die Prüfsumme nicht erkannt. Die Übermittlung von 61 statt 16 bleibt zum Beispiel unbemerkt. Dagegen wird die fehlerhafte Übermittlung von 26 statt 62 erkannt. Bei der ISBN-10 ist $w_j = j$, also $[w_j] - [w_{j+1}] = [-1] \in (\mathbb{Z}/11\mathbb{Z})^*$. Damit werden in diesem Fall alle Transpositionen erkannt.
Daran sehen wir, dass die Prüfgleichung der inzwischen abgeschafften ISBN-10 derjenigen der EAN und der neuen ISBN-13 bei der Fehlererkennung überlegen war. Beim maschinellen Lesen von Strichcodes sind allerdings Transpositionsfehler von untergeordneter Bedeutung, so dass diese Schwäche kaum praktische Relevanz haben sollte.
Der Nachteil der Prüfgleichung der ISBN-10 war die Notwendigkeit der Einführung eines elften Symbols „`X`“. Wenn wir ein Alphabet mit zehn Symbolen bevorzugen, dann führt uns die geschilderte Methode auf eine Prüfgleichung in $\mathbb{Z}/10\mathbb{Z}$. Da $(\mathbb{Z}/10\mathbb{Z})^* = \{\pm 1, \pm 3\}$, sind auf diese Weise keine wesentlichen Verbesserungen der EAN möglich. Um bessere Fehlererkennung zu erreichen, kann man versuchen, die additive Gruppe $\mathbb{Z}/10\mathbb{Z}$ durch eine andere Gruppe zu ersetzen. Man kann zeigen, dass jede Gruppe der Ordnung 10 zu $\mathbb{Z}/10\mathbb{Z}$ oder D_5 isomorph ist.

Doch zunächst sei ganz allgemein $(G, *)$ eine Gruppe mit n Elementen und $c \in G$ fixiert. Statt einer Multiplikation mit Gewichten w_i erlauben wir nun beliebige Permutationen $\sigma_i \in \mathrm{sym}(G)$, $1 \le i \le k$. Das führt zur Prüfgleichung

$$\sigma_1(a_1) * \sigma_2(a_2) * \ldots * \sigma_k(a_k) = c\,.$$

Zur Vereinfachung der Analyse wählen wir eine einzige Permutation $\sigma \in \mathrm{sym}(G)$ und setzen $\sigma_i := \sigma^i \in \mathrm{sym}(G)$ für $1 \le i \le k$. Bei korrektem Wort $a_1 \ldots a_k$ und empfangenem Wort $b_1 \ldots b_k$ ist dann

$$c = \sigma^1(a_1) * \sigma^2(a_2) * \ldots * \sigma^k(a_k) \;\text{ und }\; \widetilde{c} = \sigma^1(b_1) * \sigma^2(b_2) * \ldots * \sigma^k(b_k)\,.$$

Die Diskrepanz ist nun $\delta = c * \widetilde{c}^{-1} \in G$. Ein Fehler wird erkannt, wenn $\delta \neq e$.

Satz 1.3.36 *Eine Prüfgleichung der Form $\prod_{i=1}^{k} \sigma^i(a_i) = c$ erkennt alle Einzelfehler. Wenn für $x \neq y \in G$ stets $x * \sigma(y) \neq y * \sigma(x)$ gilt, dann werden auch alle Transpositionen erkannt.*

Beweis. Da $\delta = \sigma^1(a_1) * \sigma^2(a_2) * \ldots * \sigma^k(a_k) * \sigma^k(b_k)^{-1} * \ldots * \sigma^2(b_2)^{-1} * \sigma^1(b_1)^{-1}$, kann ein Einzelfehler an Position j nur dann unerkannt bleiben, wenn $e = \sigma^j(a_j) * \sigma^j(b_j)^{-1}$, also $\sigma^j(a_j) = \sigma^j(b_j)$ gilt. Da σ^j bijektiv ist, ist das nur möglich, wenn $a_j = b_j$, also überhaupt kein Fehler vorliegt. Damit ist die Erkennung aller Einzelfehler gesichert.
Wenn an den Positionen i und $i+1$ statt (a, b) das Paar (b, a) übermittelt wurde, dann wird dies durch die Prüfgleichung genau dann erkannt, wenn $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ gilt. Mit $x := \sigma^i(a) \neq \sigma^i(b) =: y$ folgt dies aus der Voraussetzung $x * \sigma(y) \neq y * \sigma(x)$. □

Beispiel 1.3.37. Sei jetzt $G = D_5 = \{1, t, t^2, t^3, t^4, s, st, st^2, st^3, st^4\}$. Wir nummerieren die Elemente dieser Gruppe, indem wir jede der Ziffern $0, \ldots, 9$ in der Form $5i + j$ schreiben und dann dem Element $t^j s^i \in D_5$ zuordnen. Das führt zu folgender Tabelle

0	1	2	3	4	5	6	7	8	9
1	t	t^2	t^3	t^4	s	st^4	st^3	st^2	st

Dadurch kann die Permutation

$$\sigma = (0\,1\,5\,8\,9\,4\,2\,7) \circ (3\,6) = \begin{pmatrix} 0&1&2&3&4&5&6&7&8&9 \\ 1&5&7&6&2&8&3&0&9&4 \end{pmatrix} \in \mathfrak{S}_{10}$$

als Permutation der Elemente der Gruppe D_5 aufgefasst werden. Man erhält

x	1	t	t^2	t^3	t^4	s	st	st^2	st^3	st^4
$\sigma(x)$	t	s	st^3	st^4	t^2	st^2	t^4	st	1	t^3

Es gilt tatsächlich $x\sigma(y) \neq y\sigma(x)$ für $x \neq y \in D_5$, siehe Aufgabe 1.23.

Die im Beispiel 1.3.37 beschriebene Permutation wurde tatsächlich bei der Prüfgleichung für die Nummern auf den seit Herbst 1990 ausgegebenen und bis zur Einführung des Euro-Bargelds zu Beginn des Jahres 2002 in Umlauf befindlichen DM-Banknoten angewandt.
Die elfstelligen Nummern auf diesen Banknoten hatten an den Stellen 1, 2 und 10 einen Buchstaben statt einer Ziffer. Die Buchstaben entsprachen Ziffern nach folgendem Schema:

Ziffer	0	1	2	3	4	5	6	7	8	9
Buchstabe	A	D	G	K	L	N	S	U	Y	Z

Die benutzte Prüfgleichung lautete

$$a_{11} \prod_{i=1}^{10} \sigma^i(a_i) = 1 \, .$$

Aus Satz 1.3.36 erhalten wir, dass dadurch alle Einzelfehler und Transpositionen erkannt werden konnten. Da an der Position 10 ein Buchstabe und an Position 11 eine Ziffer verwendet wurde, ist es nicht nötig, den Beweis an die leicht veränderte Prüfgleichung anzupassen.

Abb. 1.2 Eine ehemalige 10-DM Banknote mit Nummer `DS1170279G9` vom 1. 10. 1993

Beispiel 1.3.38. Um festzustellen, ob die Nummer der in Abb. 1.2 abgebildeten 10 DM Banknote wirklich die Prüfgleichung erfüllt, gehen wir folgendermaßen vor: Zuerst ersetzen wir `D` durch 1, `S` durch 6 und `G` durch 2. Dann wenden wir die entsprechende Potenz σ^i von σ an. Die Rechnung vereinfacht sich, wenn wir $\sigma^8 = \mathrm{Id}$ benutzen. Schließlich ersetzen wir die so erhaltenen Ziffern durch ihre entsprechenden Elemente in D_5 und bilden deren Produkt. Auf diese Weise erhalten wir Tabelle 1.1. Unter Verwendung

Position i	1	2	3	4	5	6	7	8	9	10	11
Ziffer a	1	6	1	1	7	0	2	7	9	2	9
Potenz von σ	σ	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7	Id	σ	σ^2	Id
$\sigma^i(a)$	5	6	9	4	9	2	4	7	4	0	9
Element in D_5	s	st^4	st	t^4	st	t^2	t^4	st^3	t^4	1	st

Tabelle 1.1 Überprüfung der Nummer einer ehemaligen Banknote

von $st^k st^k = 1$ und $tst = s$ ergibt sich $s \cdot st^4 \cdot st \cdot t^4 \cdot st \cdot t^2 \cdot t^4 \cdot st^3 \cdot t^4 \cdot 1 \cdot st = s\left(st^4 \cdot st^4\right) t\left(st^7 \cdot st^7\right) st = 1$, die Prüfgleichung ist erfüllt.

Die Verwendung von Prüfziffern erlaubt uns, Einzelfehler zu erkennen. Eine Korrektur ist in der Regel jedoch nur dann möglich, wenn bekannt ist, an welcher Stelle der Fehler auftrat. Im Normalfall muss man sich mit der Erkenntnis der Fehlerhaftigkeit begnügen. Dies ist in Situationen ausreichend, in denen die Originalquelle leicht erreichbar ist, wie etwa bei einer fehlerhaft gescannten EAN an der Kasse eines Supermarktes. Im Fall der Banknotennummern genügt die Feststellung der Fehlerhaftigkeit, eine Korrektur ist nicht nötig.
Bei der Übertragung von Daten innerhalb von oder zwischen Computern über ein Netzwerk ist eine Fehlerkorrektur jedoch nötig und erwünscht. Wir befassen uns mit fehlerkorrigierenden Codes im Abschnitt 2.5.
Wir wollen schließlich durch ein letztes Beispiel zeigen, wie ein in den achtziger Jahren des letzten Jahrhunderts weltweit verbreitetes Spielzeug der Mathematik ernsthafte Probleme stellen kann. Im Jahr 1975 ließ der ungarische Professor für Architektur Erno Rubik den sogenannten Zauberwürfel (Abb. 1.3) patentieren. Von diesem Würfel wurden mehr als 100 Millionen Exemplare verkauft. Noch heute kann man ihn in den Geschäften finden.

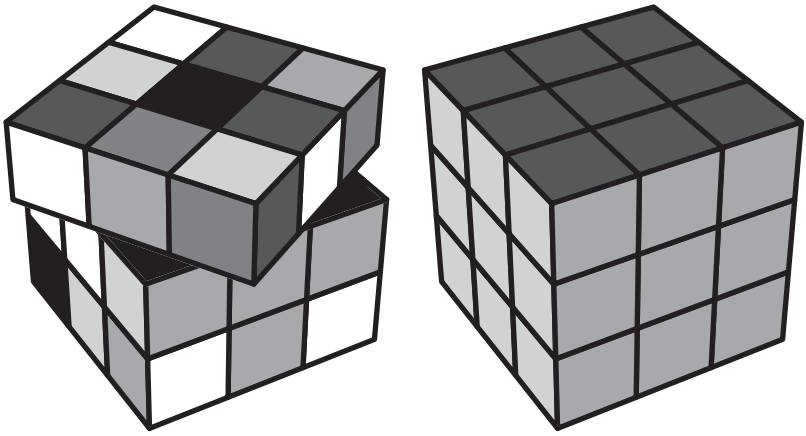


Abb. 1.3 Der Rubik-Würfel

Der Würfel besteht aus 26 zusammenhängenden kleinen farbigen Würfeln, die sich schichtweise in einer Ebene gegeneinander drehen lassen. Dadurch werden die einzelnen Würfel umgeordnet.
Bei den kleinen Würfeln gibt es 8 Ecksteine, deren 3 Außenflächen mit 3 verschiedenen Farben versehen sind. Es gibt 12 Kantensteine mit 2 verschiedenen Farben und 6 Mittelsteine, die jeweils eine der Farben blau, rot, gelb, grün, braun und weiß haben. Die kleinen Würfel sind so gefärbt, dass der Würfel in einer Stellung (Grundstellung) auf jeder Seite eine einheitliche Farbe besitzt. Mathematisch gesehen kann der Würfel als Permutationsgruppe W aufgefasst werden. Auf den 6 Seiten des Würfels gibt es durch die Unterteilung in die kleinen Würfel je 9 farbige Quadrate (insgesamt 54). Die 6 Quadrate der Mittelsteine gehen bei den Drehungen des Würfels in sich über, so dass man das Verdrehen des Würfels als Permutation der 48 („beweglichen“) Quadrate auffassen kann. Das ergibt eine Untergruppe der Permutationsgruppe $\mathfrak{S}_{48}$. Sie hat die Ordnung $\frac{1}{12} \cdot 8! \cdot 3^8 \cdot 12! \cdot 2^{12} \approx 4{,}3 \cdot 10^{19}$. Diese Untergruppe wird durch 6 Permutationen V, H, R, L, O, U erzeugt, die den Drehungen der 6 Seiten (Vorderseite, Hinterseite, rechte Seite, linke Seite, obere Seite, untere Seite) um 90 Grad entsprechen. Sei $B_0 = \{V, H, R, L, O, U\}$, dann ist $W = \langle B_0 \rangle$. Oft versteht man unter einer einzelnen Drehung auch die Drehung einer Seite um 180 oder 270 Grad. Daher setzen wir $B = \{D^k \mid D \in B_0, k = 1, 2, 3\}$.
Wenn man den Würfel als Spielzeug benutzt, kommt es darauf an, ihn aus einer beliebig verdrehten Stellung in möglichst kurzer Zeit in die Grundstellung zurückzudrehen. Das ist gar nicht so einfach. Es gab regelrechte Wettbewerbe und die Besten schafften das durchschnittlich in weniger als einer Minute. Der Weg zur Grundstellung ist natürlich nicht eindeutig bestimmt. Mathematisch stellt sich die Frage nach der folgenden Schranke:

$$M := \min\{k \mid \forall \sigma \in W \ \exists \sigma_1, \ldots, \sigma_k \in B, \text{ so dass } \sigma = \sigma_1 \circ \ldots \circ \sigma_k\} ,$$

d.h. M ist die kleinstmögliche Zahl, für die sich der Würfel aus jeder beliebigen Stellung mit höchstens M Drehungen wieder in Grundstellung bringen lässt. Anfang der achtziger Jahre wurde gezeigt, dass $18 \leq M \leq 52$ ist. Bis heute ist die Zahl M nicht bekannt. Man weiß jetzt, dass $20 \leq M \leq 22$ gilt. Dieses Ergebnis geht auf Tomas Rokicki (USA) zurück, der das Problem auf aufwändige Rechnungen mit Nebenklassen einer geeigneten Untergruppe von W zurückführte, die er dann von Computern durchführen ließ, siehe [Rok].

Aufgaben

Übung 1.13. Zeigen Sie, dass die durch $f(x, y) := x - y$ gegebene Abbildung $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ein Gruppenhomomorphismus bezüglich der additiven Gruppenstruktur (vgl. Bsp. 1.3.2 (vi)) ist. Bestimmen Sie $\ker(f)$ und $\mathrm{im}(f)$.

Übung 1.14. Bestimmen Sie die Ordnung von jedem der sechs Elemente der symmetrischen Gruppe $\mathfrak{S}_3$.

Übung 1.15. Zeigen Sie: $\operatorname{ord}([a]) = n/\operatorname{ggT}(a,n)$ für $[0] \neq [a] \in (\mathbb{Z}/n\mathbb{Z}, +)$.

Übung 1.16. (a) Welche der Gruppen $D_5, \mathfrak{S}_3, \mathbb{Z}/5\mathbb{Z}, (\mathbb{Z}/5\mathbb{Z})^*$ ist zyklisch?
(b) Beweisen Sie, dass jede endliche Gruppe, deren Ordnung eine Primzahl ist, eine zyklische Gruppe ist.

Übung 1.17. Zeigen Sie, dass die durch $g([a]) := [7^a]$ definierte Abbildung $g : \mathbb{Z}/16\mathbb{Z} \to (\mathbb{Z}/17\mathbb{Z})^*$ ein Isomorphismus von Gruppen ist.

Übung 1.18. Sei $f : G \to H$ ein Gruppenisomorphismus. Beweisen Sie, dass für jedes Element $a \in G$ stets $\operatorname{ord}(a) = \operatorname{ord}(f(a))$ gilt. Gilt dies auch für beliebige Gruppenhomomorphismen?

Übung 1.19. Beweisen Sie, dass es keinen Isomorphismus zwischen den Gruppen $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gibt. Gibt es einen Isomorphismus zwischen $\mathbb{Z}/6\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?

Übung 1.20. Sei $(G, *)$ eine Gruppe und $g \in G$ irgendein Element. Beweisen Sie, dass die durch $K(x) = g * x * g^{-1}$ gegebene Abbildung $K : G \to G$ ein Isomorphismus von Gruppen ist.

Übung 1.21. Sei $U \subset G$ eine Untergruppe einer endlichen Gruppe G, so dass $\operatorname{ord}(G) = 2\operatorname{ord}(U)$. Zeigen Sie, dass $U \subset G$ ein Normalteiler ist.

Übung 1.22. Geben Sie sämtliche Untergruppen der symmetrischen Gruppe $\mathfrak{S}_3$ an, und bestimmen Sie diejenigen unter ihnen, die Normalteiler sind.

Übung 1.23. Zeigen Sie, dass die im Beispiel 1.3.37 angegebene Permutation σ tatsächlich die im Satz 1.3.36 für die Erkennung von Transpositionsfehlern angegebene Bedingung erfüllt.

Übung 1.24. Überprüfen Sie, ob `GL0769947G2` eine gültige Nummer für eine ehemalige DM-Banknote sein könnte.

Übung 1.25. Bestimmen Sie die fehlende letzte Ziffer der Nummer einer ehemaligen DM-Banknote `DY3333333Z?`.

Übung 1.26. Sei $(G, *)$ eine Gruppe mit neutralem Element $e \in G$. Wir nehmen an, dass für jedes $a \in G$ die Gleichung $a * a = e$ gilt. Beweisen Sie, dass G eine abelsche Gruppe ist.

1.4 Ringe und Körper

In den Abschnitten 1.2 und 1.3 wurde die Methode der Abstraktion anhand des konkreten Beispiels der Restklassen ganzer Zahlen und des allgemeinen Begriffes der Gruppe illustriert. Ein Vergleich der Gruppenaxiome (Def. 1.3.1) mit der Liste der Eigenschaften ganzer Zahlen im Abschnitt 1.1 zeigt jedoch, dass der Gruppenbegriff nicht alle Aspekte des Rechnens mit ganzen Zahlen reflektiert. Wir benötigen eine mathematische Struktur mit zwei Rechenoperationen: einer Addition *und* einer Multiplikation. Das führt uns zu den Begriffen *Ring* und *Körper*. Diese Begriffe umfassen sowohl die uns vertrauten Zahlbereiche als auch Polynomringe. Letztere besitzen verblüffend große strukturelle Ähnlichkeit zum Ring der ganzen Zahlen.
Als Anwendung werden wir im folgenden Abschnitt 1.5 erste Schritte in der Kryptographie unternehmen.

Definition 1.4.1. Eine nichtleere Menge K, auf der zwei Verknüpfungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$ gegeben sind, heißt *Körper*, wenn

$$(K, +) \text{ eine abelsche Gruppe mit neutralem Element } 0 \in K \text{ ist,} \tag{1.21}$$

$$(K^*, \cdot) \text{ eine abelsche Gruppe ist, wobei } K^* := K \smallsetminus \{0\}, \text{ und das} \tag{1.22}$$

$$\text{Distributivgesetz gilt: } \forall\, a, b, c \in K : \quad a \cdot (b + c) = a \cdot b + a \cdot c. \tag{1.23}$$

Beispiel 1.4.2. (i) $\mathbb{R}, \mathbb{Q}$ sind Körper, aber $\mathbb{Z}$ ist kein Körper.
(ii) $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper, falls p eine Primzahl ist. Um ihn von der additiven Gruppe $\mathbb{Z}/p\mathbb{Z}$ zu unterscheiden, wird er mit $\mathbb{F}_p$ bezeichnet.

In jedem Körper K bezeichnet $1 \in K^*$ das neutrale Element der multiplikativen Gruppe $(K^*, \cdot)$. Da $0 \notin K^*$, muss stets $0 \neq 1$ gelten.
Mit den gleichen Beweisen wie zu Beginn von Abschnitt 1.1 erhält man folgende Aussagen in einem beliebigen Körper K:

$$\text{Für alle } a \in K \text{ gilt } 0 \cdot a = 0. \tag{1.24}$$

$$\text{Aus } a \cdot b = 0 \text{ folgt } a = 0 \text{ oder } b = 0. \tag{1.25}$$

$$\text{Für } a, b \in K \text{ gilt } a \cdot (-b) = -(a \cdot b) \text{ und } (-a) \cdot (-b) = a \cdot b. \tag{1.26}$$

Wenn n keine Primzahl ist, dann ist $\mathbb{Z}/n\mathbb{Z}$ *kein* Körper, denn die Eigenschaft (1.25) ist für zusammengesetztes n verletzt. Zum Beispiel gilt $[2] \cdot [3] = [0]$ in $\mathbb{Z}/6\mathbb{Z}$. Echte Teiler von n haben kein multiplikatives Inverses modulo n und somit ist $(\mathbb{Z}/n\mathbb{Z}) \smallsetminus \{[0]\}$ keine Gruppe bezüglich der Multiplikation. Daher ist es notwendig, den etwas allgemeineren Begriff des Ringes einzuführen.

Definition 1.4.3. Eine Menge R, auf der zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ gegeben sind, heißt kommutativer *Ring* mit Eins, wenn folgende Bedingungen erfüllt sind:

$(R, +)$ ist eine abelsche Gruppe mit neutralem Element $0 \in R$. (1.27)

Die Multiplikation in R ist assoziativ, kommutativ und es gibt ein neutrales Element $1 \in R$. (1.28)

Das Distributivgesetz gilt. (1.29)

Wenn im Folgenden von einem *Ring* die Rede ist, dann meinen wir stets einen kommutativen Ring mit Eins. In anderen Lehrbüchern wird bei dem Begriff des Ringes mitunter in (1.28) auf die Kommutativität der Multiplikation oder auf die Existenz eines neutralen Elements $1 \in R$ verzichtet.
Die Menge aller 2×2-Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit ganzzahligen Einträgen $a, b, c, d \in \mathbb{Z}$ bilden einen Ring bezüglich der gewöhnlichen Addition von Matrizen und der Matrizenmultiplikation (Def. 2.2.22) als Produkt. Die Einheitsmatrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ ist das Einselement dieses Ringes und die Matrix, deren Einträge sämtlich gleich Null sind, ist das Nullelement dieses Ringes. Da

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} ,$$

ist dieser Ring *nicht* kommutativ. Er wird also in diesem Buch nicht weiter auftauchen.
Der einzige Unterschied zwischen den Definitionen der Begriffe Ring und Körper ist, dass für einen Ring nicht gefordert wird, dass zu jedem $r \in R$ mit $r \neq 0$ ein multiplikatives Inverses existiert. Allerdings ist deshalb in einem Ring nicht mehr automatisch $1 \neq 0$. Wenn jedoch in einem Ring $0 = 1$ gilt, dann sind alle Elemente dieses Ringes gleich 0. Mit anderen Worten: Der einzige Ring, in dem $0 = 1$ ist, ist der *Nullring* $R = \{0\}$. In jedem anderen Ring gilt $1 \neq 0$. In allen Ringen gelten weiterhin (1.24) und (1.26). Die Aussage (1.25) gilt in allgemeinen Ringen jedoch nicht.

Beispiel 1.4.4. (i) Jeder Körper, insbesondere $\mathbb{R}$ und $\mathbb{Q}$, aber auch die Menge der ganzen Zahlen $\mathbb{Z}$ sind Ringe.
(ii) Für jedes $n \in \mathbb{Z}$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Ring.
(iii) Wenn R und R' Ringe sind, dann ist das kartesische Produkt $R \times R'$ mit den Verknüpfungen

$$(r, r') + (s, s') := (r + s, r' + s')$$
$$(r, r') \cdot (s, s') := (r \cdot s, r' \cdot s')$$

ebenfalls ein Ring. Selbst wenn R und R' Körper sind, ist $R \times R'$ kein Körper. Das liegt daran, dass stets $(1, 0) \cdot (0, 1) = (0, 0) = 0$ gilt.

Beispiel 1.4.5 (Polynomringe). Sei R ein Ring. Dann definieren wir den Polynomring $R[X]$ wie folgt. Die zugrunde liegende Menge enthält alle Polynome in der Unbestimmten X mit Koeffizienten aus dem Ring R:

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; n \geq 0, a_i \in R \right\}.$$

Ein Polynom ist somit ein formaler Ausdruck, in dem die „Unbestimmte“ X auftritt. Zwei solche Ausdrücke sind genau dann gleich, wenn ihre Koeffizienten a_i übereinstimmen. Polynome sind *nicht* dasselbe wie Polynomfunktionen, die man durch das Einsetzen von Elementen $x \in K$ für X aus Polynomen erhält, vgl. Aufgabe 1.35. Die Addition ist komponentenweise definiert:

$$\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} b_j X^j := \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i$$

wobei wir $a_i = 0$ für $i > n$ und $b_j = 0$ für $j > m$ setzen.
Die Multiplikation ist so definiert, dass $aX^i \cdot bX^j = (a \cdot b)X^{i+j}$ ist und das Distributivgesetz gilt. Ausführlicher bedeutet das:

$$\left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{j=0}^{m} b_j X^j \right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k \,.$$

Konkret erhalten wir für $X^2+1, 2X-3 \in \mathbb{Z}[X]$ folgende Summe und Produkt:

$$\begin{aligned} (X^2+1) \cdot (2X-3) &= 2X^3 - 3X^2 + 2X - 3, \text{ sowie} \\ (X^2+1) + (2X-3) &= X^2 + 2X - 2 \,. \end{aligned}$$

Jedem Polynom ist sein *Grad* zuordnet. Wenn

$$f = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + \ldots + a_{n-1} X^{n-1} + a_n X^n$$

und $a_n \neq 0$, dann heißt $\deg(f) := n$ der Grad des Polynoms f. Es ist zweckmäßig dem Nullpolynom den Grad $-\infty$ zuzuordnen. Wenn $\deg(f) = n$, dann nennen wir a_n den *Leitkoeffizienten* von f und $a_n X^n$ den *Leitterm* des Polynoms f.

Definition 1.4.6. (1) Sei R ein Ring und $R' \subset R$ eine Teilmenge, so dass R' Untergruppe bezüglich der Addition ist, $1 \in R'$ und für $a, b \in R'$ stets $a \cdot b \in R'$ gilt. Dann heißt R' *Unterring* von R.
(2) Ein Unterring $L \subset K$ eines Körpers K heißt *Teilkörper*, wenn für jedes $0 \neq a \in L$ auch $a^{-1} \in L$ ist.
(3) Eine Abbildung $f : R \to R'$ zwischen zwei Ringen R und R' heißt *Ringhomomorphismus*, falls $f(1) = 1$ ist und $f(a+b) = f(a) + f(b)$ und $f(a \cdot b) = f(a) \cdot f(b)$ für alle $a, b \in R$ gilt. Wenn R und R' Körper sind, dann spricht man auch von einem *Körperhomomorphismus*.

Beispiel 1.4.7. (i) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ sind Unterringe, $\mathbb{Q} \subset \mathbb{R}$ ist Teilkörper.

(ii) $R \subset R[X]$ ist Unterring.
(iii) Für fixiertes $a \in R$ ist die durch $f_a(h) := h(a)$ definierte Abbildung $f_a : R[X] \to R$ ein Ringhomomorphismus. Wenn $h = \sum_{i=0}^{n} a_i X^i$, dann ist $h(a) := \sum_{i=0}^{n} a_i a^i \in R$. Wir nennen f_a den *Einsetzungshomomorphismus.*
(iv) $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit $f(a) := [a]$ ist ein Ringhomomorphismus.
(v) $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ ist ein Unterring.
(vi) Die Abbildung $\mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X]$, bei der jeder Koeffizient durch seine Restklasse ersetzt wird, ist ein Ringhomomorphismus. Allgemeiner ist für jeden Ringhomomorphismus $f : R \to R'$ ein Ringhomomorphismus $R[X] \to R'[X]$ definiert, indem f auf die Koeffizienten angewendet wird.

Der Polynomring $K[X]$ über einem Körper K weist viel Ähnlichkeit mit dem in Abschnitt 1.1 studierten Ring der ganzen Zahlen auf. Die Ursache dafür besteht im Vorhandensein eines Euklidischen Algorithmus für Polynome, der auf der folgenden *Division mit Rest* basiert.

Satz 1.4.8 *Zu gegebenen Polynomen $f, g \in K[X]$ mit $\deg(f) \geq \deg(g)$ gibt es ein $h \in K[X]$, so dass $\deg(f - gh) < \deg(g)$ gilt.*

Beweis. Der Beweis erfolgt per Induktion über $k := \deg(f) - \deg(g) \geq 0$. Der Induktionsanfang ($k = 0$) und der Induktionsschritt (Schluss von k auf $k+1$) ergeben sich aus der folgenden Überlegung, bei der $k \geq 0$ beliebig ist. Sei $f = aX^{n+k} + \ldots$ und $g = bX^n + \ldots$, wobei nur die Terme höchsten Grades (Leitterme) aufgeschrieben sind. Die Leitkoeffizienten sind $a \neq 0$ und $b \neq 0$. Es gilt also $\deg(f) = n + k$ und $\deg(g) = n$. Dann ist

$$\deg\left(f - \left(\tfrac{a}{b} \cdot X^k\right) \cdot g\right) < n + k = \deg(f),$$

denn der Leitterm von f wird durch Subtraktion von $\left(\frac{a}{b} X^k\right) g$ entfernt. □

Beispiel 1.4.9. (i) Sei $f = X^3 + 1$ und $g = X - 1$. Die Leitterme von f und g sind X^3 bzw. X. Daher müssen wir g mit X^2 multiplizieren. Wir erhalten $f - X^2 g = X^3 + 1 - X^2(X - 1) = X^2 + 1$. Da dies vom Grad $2 > \deg(g)$ ist, müssen wir fortfahren und nun Xg subtrahieren. Der Faktor X ergibt sich wieder als Quotient der Leitterme. Damit erhalten wir $f - (X^2 + X)g = X^2 + 1 - X(X - 1) = X + 1$. Dieses Ergebnis hat Grad $1 \geq \deg(g)$ und somit ist ein weiterer Schritt notwendig. Wir subtrahieren nun g und erhalten schließlich $f - (X^2 + X + 1)g = X + 1 - (X - 1) = 2$.
(ii) Sei $f = X^3 - 3X^2 + 2X$ und $g = X^2 - 1$. Die Leitterme sind hier X^3 und X^2, daher subtrahieren wir zunächst Xg von f und erhalten $f - Xg = -3X^2 + 3X$. Nun ist $3g$ zu addieren und wir erhalten $f - (X - 3)g = 3X - 3$.

Der Euklidische Algorithmus in Polynomringen

Als Eingabedaten seien zwei Polynome $f, g \in K[X]$ mit $\deg(f) \geq \deg(g)$ gegeben. Am Ende wird $\mathrm{ggT}(f, g)$ ausgegeben.
Jeder Schritt des Algorithmus besteht aus einer Division mit Rest, gefolgt von einem Test, in dem entschieden wird, ob das Ende bereits erreicht wurde. Um die Division mit Rest stets ausführen zu können, setzen wir voraus, dass K ein Körper ist.

Initialisierung: $A := f$, $B := g$
Division: Bestimme $N \in K[X]$, so dass $\deg(A - N \cdot B) < \deg(B)$.
$C := A - N \cdot B$ ist der Rest von A bei Division durch B.
Test: Wenn $C = 0$, dann Ausgabe von $\mathrm{ggT}(a, b) := B$ und stopp.
Wenn $C \neq 0$, dann Division mit Rest für $A := B$, $B := C$.

Der Ausgabewert ist, bis auf die Normierung des Leitkoeffizienten, der größte gemeinsame Teiler von f und g. Die Definition des Begriffes *größter gemeinsamer Teiler* lässt sich fast wörtlich aus $\mathbb{Z}$ auf Polynomringe übertragen. Der wesentliche Unterschied besteht darin, dass wir die Normierung „$d > 0$“ durch „Leitkoeffizient ist gleich 1“ zu ersetzen haben. Wie bereits in Abschnitt 1.1 beginnen wir mit den Definitionen der Begriffe Teilbarkeit und größter gemeinsamer Teiler.

Definition 1.4.10. Ein Element b eines Ringes R heißt *Teiler* des Elements $a \in R$, falls es ein $c \in R$ gibt, so dass $b \cdot c = a$ gilt. Wir schreiben dann $b \mid a$.

Definition 1.4.11. Seien $f, g \in K[X]$ von Null verschiedene Polynome. Ein Polynom $d \in K[X]$ heißt genau dann *größter gemeinsamer Teiler* von f und g, wenn die folgenden drei Bedingungen erfüllt sind:

(i) (Normierung) Der Leitkoeffizient von d ist gleich 1.
(ii) (gemeinsamer Teiler) $d \mid f$ und $d \mid g$.
(iii) (Maximalität) $\forall\, c \in K[X]$: Wenn $c \mid f$ und $c \mid g$, dann gilt $c \mid d$.

Beispiel 1.4.12. (i) Wir bestimmen den größten gemeinsamen Teiler von

$$f = X^4 - 1 \text{ und } g = X^3 - 1\,.$$

Es sind zwei Divisionen mit Rest durchzuführen:

$$(X^4 - 1) - X \cdot (X^3 - 1) = X - 1$$
$$(X^3 - 1) - (X^2 + X + 1)(X - 1) = 0\,.$$

Das ergibt: $\mathrm{ggT}(X^4 - 1, X^3 - 1) = X - 1$.
(ii) Für $f = X^3 - 3X^2 + 2X$ und $g = X^2 - 1$ erhalten wir

$$f - (X - 3)g = 3X - 3 \quad \text{und}$$
$$(X^2 - 1) - \frac{1}{3}(X + 1)(3X - 3) = 0\,.$$

Damit ist $\mathrm{ggT}(X^3 - 3X^2 + 2X, X^2 - 1) = X - 1$, denn das Polynom $3X - 3$ ist noch durch 3 zu teilen, um den Leitkoeffizienten zu normieren.

Der Beweis, dass dieser Algorithmus stets nach endlich vielen Schritten endet und tatsächlich den größten gemeinsamen Teiler berechnet, ist fast wörtlich derselbe wie für den Euklidischen Algorithmus in $\mathbb{Z}$. Daher wird er hier weggelassen. Alle Eigenschaften der ganzen Zahlen, die mit Hilfe des Euklidischen Algorithmus bewiesen wurden, lassen sich auch für Polynomringe $K[X]$ mit Koeffizienten in einem Körper K beweisen. Die Beweise übertragen sich aus Abschnitt 1.1 fast wörtlich.

Satz 1.4.13 (1) *Für $f, g, h \in K[X]$ gilt genau dann $h = \mathrm{ggT}(f, g)$, wenn es Polynome $r, s \in K[X]$ gibt, so dass $h = rf + sg$ und wenn jedes andere Polynom dieser Gestalt durch h teilbar ist.*

(2) *Wenn $f, g, h \in K[X]$ Polynome sind, für die $\mathrm{ggT}(f, h) = 1$ und $f \mid g \cdot h$ gilt, dann folgt $f \mid g$.*

(3) *Ein Polynom f heißt* irreduzibel*, wenn aus $f = g \cdot h$ stets $g \in K$ oder $h \in K$ folgt. Dies ist äquivalent dazu, dass aus $f \mid gh$ stets $f \mid g$ oder $f \mid h$ folgt.*

(4) *Jedes Polynom $0 \neq f \in K[X]$ hat eine, bis auf die Reihenfolge eindeutige, Darstellung $f = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$, wobei $u \in K^*$ und $p_i \in K[X]$ irreduzible Polynome mit Leitkoeffizient 1 sind.*

Da der Ring $K[X]$ in seiner Struktur dem Ring $\mathbb{Z}$ so sehr ähnlich ist, entsteht die Frage, ob es auch für Polynomringe möglich ist, auf Restklassenmengen in ähnlicher Weise wie auf $\mathbb{Z}/n\mathbb{Z}$ eine Ringstruktur zu definieren. Das führt allgemeiner auf die Frage, für welche Teilmengen $I \subset R$ eines beliebigen Ringes R sich die beiden Rechenoperationen $+$ und $\cdot$ auf R/I vererben. Dafür ist nicht ausreichend, dass Summen und Produkte von Elementen aus I stets in I sind. Eine Analyse des Wohldefiniertheitsproblems führt auf die folgende Definition.

Definition 1.4.14. Sei R ein Ring und $I \subset R$ eine nichtleere Teilmenge. Wir nennen I ein *Ideal*[13], falls die folgenden beiden Bedingungen erfüllt sind:

$$\text{Für alle } a, b \in I \text{ gilt } a + b \in I. \tag{1.30}$$

$$\text{Für alle } r \in R \text{ und } a \in I \text{ gilt } r \cdot a \in I. \tag{1.31}$$

Aus (1.30) und (1.31) folgt, dass $I \subset R$ ist eine Untergruppe bezüglich der Addition ist.

[13] Der deutsche Mathematiker Richard Dedekind (1831–1916) führte den Begriff des Ideals ein, um für bestimmte Erweiterungen des Ringes der ganzen Zahlen eine Verallgemeinerung der in der Formulierung von Satz 1.1.8 dort nicht mehr gültigen eindeutigen Primfaktorzerlegung zu erhalten.

Beispiel 1.4.15. (i) Die Ideale in $\mathbb{Z}$ sind genau die Teilmengen $n\mathbb{Z} \subset \mathbb{Z}$. Jede Untergruppe von $(\mathbb{Z}, +)$ ist nach Satz 1.3.18 von der Gestalt $n\mathbb{Z}$. Da für $r \in \mathbb{Z}$ und $a = ns \in n\mathbb{Z}$ stets $r \cdot a = nrs \in n\mathbb{Z}$ gilt, sind die Mengen $n\mathbb{Z}$ tatsächlich Ideale.

(ii) Wenn $a_1, \ldots, a_k \in R$ beliebige Elemente sind, dann ist

$$\langle a_1, \ldots, a_k \rangle := \left\{ \sum_{i=1}^{k} r_i a_i \;\middle|\; r_i \in R \right\} \subset R$$

ein Ideal. Für $k = 1$ erhalten wir $\langle a \rangle = a \cdot R = \{ra \mid r \in R\}$. Dies verallgemeinert die Ideale $n\mathbb{Z} \subset \mathbb{Z}$. Ideale der Gestalt $\langle a \rangle$ heißen *Hauptideale*.

(iii) Stets ist $\langle 1 \rangle = R$ ein Ideal. Es ist das einzige Ideal, das ein Unterring ist.

Satz 1.4.16 *Sei R ein Ring, $I \subset R$ ein Ideal. Dann wird auf der additiven Gruppe R/I durch $[a] \cdot [b] := [a \cdot b]$ die Struktur eines Ringes definiert.*

Beweis. Um die Wohldefiniertheit der Multiplikation einzusehen, starten wir mit $r, s \in I$ und betrachten $a' = a + r$, $b' = b + s$. Dann ist $a' \cdot b' = (a+r)\cdot(b+s) = ab+as+rb+rs$. Wegen (1.30) und (1.31) ist $as+br+rs \in I$. Das heißt $[a'b'] = [ab]$, die Multiplikation auf R/I ist also wohldefiniert. Die Ringeigenschaften übertragen sich nun leicht. □

Satz 1.4.17 *Wenn K ein Körper ist, dann ist $K[X]$ ein* Hauptidealring. *Das heißt, für jedes Ideal $I \subset K[X]$ gibt es ein $f \in K[X]$, so dass $I = \langle f \rangle$.*

Beweis. Der Beweis ist analog zum Beweis von Satz 1.3.18. Sei $I \subset K[X]$ ein Ideal. Wenn $I = \{0\}$, dann können wir $f = 0$ wählen und sind fertig. Sei von nun an $I \neq \{0\}$. Da für $g \neq 0$ der Grad $\deg(g) \geq 0$ stets eine nicht-negative ganze Zahl ist, gibt es mindestens ein Element $f \in I$ von minimalem Grad. Das heißt, für jedes $0 \neq g \in I$ ist $\deg(f) \leq \deg(g)$. Jedes $0 \neq g \in I$ lässt sich als $g = r + h \cdot f$ mit $r, h \in K[X]$ schreiben, so dass $\deg(r) < \deg(f)$ (Division mit Rest). Da I ein Ideal ist, muss $r = g - hf \in I$ sein. Wegen der Minimalität des Grades von f folgt $r = g - hf = 0$, d.h. $g \in \langle f \rangle$ und somit $I = \langle f \rangle$. □

Definition 1.4.18. (1) Ein Element $a \in R$ eines Ringes R heißt *Nullteiler*, wenn ein $0 \neq b \in R$ mit $a \cdot b = 0$ existiert.

(2) Ein Element $a \in R$ heißt *Einheit*, wenn ein $b \in R$ mit $a \cdot b = 1$ existiert.

(3) Ein Ring R heißt *nullteilerfrei*, wenn $0 \in R$ der einzige Nullteiler ist.

Bei der Benutzung dieser Begriffe ist Vorsicht geboten, denn für jedes $a \in R$ gilt $a \mid 0$, auch wenn a kein Nullteiler ist. Ein Ring R ist genau dann nullteilerfrei, wenn aus $a \cdot b = 0$ stets $a = 0$ oder $b = 0$ folgt. Das heißt, dass

wir in nullteilerfreien Ringen wie gewohnt kürzen können: Falls $c \neq 0$, dann folgt aus $a \cdot c = b \cdot c$ in nullteilerfreien Ringen $a = b$. In einem Ring, der echte Nullteiler hat, kann man so nicht schließen.

Beispiel 1.4.19. (i) Die Einheiten eines Ringes sind genau die Elemente, die ein multiplikatives Inverses besitzen. Daher ist die Menge aller Einheiten

$$R^* := \{a \in R \mid a \text{ ist Einheit in } R\}$$

eine multiplikative Gruppe.
Es gilt $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1\}$. Für jeden Körper K ist $K^* = K \setminus \{0\}$. Ein Ring R ist genau dann Körper, wenn $R^* = R \setminus \{0\}$.

(ii) Wenn $n \geq 2$, dann ist in $\mathbb{Z}/n\mathbb{Z}$ jedes Element entweder Nullteiler oder Einheit (vgl. Aufg. 1.32), denn

$$[a] \in \mathbb{Z}/n\mathbb{Z} \quad \text{ist Nullteiler} \quad \Longleftrightarrow \quad \mathrm{ggT}(a,n) \neq 1\,, \tag{1.32}$$

$$[a] \in \mathbb{Z}/n\mathbb{Z} \quad \text{ist Einheit} \quad \Longleftrightarrow \quad \mathrm{ggT}(a,n) = 1\,. \tag{1.33}$$

(iii) Der einzige Nullteiler in $\mathbb{Z}$ ist 0, also ist $\mathbb{Z}$ nullteilerfrei. Außerdem gilt $\mathbb{Z}^* = \{1, -1\}$. In dem Ring $\mathbb{Z}$ ist somit jedes von $0, 1$ und -1 verschiedene Element weder Nullteiler, noch Einheit.

(iv) Für beliebige Ringe R, S gilt $(R \times S)^* = R^* \times S^*$.

Beispiel 1.4.20 (Komplexe Zahlen). Der Körper $\mathbb{C}$ der komplexen Zahlen spielt eine wichtige Rolle bei der Lösung nichtlinearer Gleichungen. Das liegt daran, dass der Prozess des Lösens von Polynomgleichungen in $\mathbb{C}$ – zumindest theoretisch – immer erfolgreich abgeschlossen werden kann, wogegen dies in den kleineren Körpern $\mathbb{Q}$ und $\mathbb{R}$ nicht immer möglich ist. Als Prototyp einer solchen Polynomgleichung dient $X^2 + 1 = 0$. Obwohl die Koeffizienten dieser Gleichung aus $\mathbb{Q}$ sind, hat sie weder in $\mathbb{Q}$ noch in $\mathbb{R}$ eine Lösung. Die beiden Lösungen dieser Gleichung sind erst in $\mathbb{C}$ zu finden.
Die additive Gruppe von $\mathbb{C}$ ist die Menge $\mathbb{R} \times \mathbb{R}$ aller Paare reeller Zahlen. Die Addition ist komponentenweise definiert und die Multiplikation ist durch die folgende Formel gegeben

$$(a,b) \cdot (a',b') := (aa' - bb', ab' + ba')\,.$$

Man sieht leicht ein, dass $0 = (0,0)$ und $1 = (1,0)$ gilt, womit man die in der Definition eines Körpers geforderten Eigenschaften leicht nachrechnen kann. Der interessanteste Teil dieser recht ermüdenden Rechnungen ist die Angabe eines multiplikativen Inversen für $(a,b) \neq (0,0)$:

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)\,.$$

Zur Vereinfachung ist es üblich $\mathrm{i} = (0,1)$ zu schreiben. Statt (a,b) wird dann $a + b\mathrm{i}$ geschrieben. Dadurch lässt sich die oben angegebene Definition der

Multiplikation durch die Gleichung $\mathrm{i}^2 = -1$ charakterisieren. Die vollständige Formel ergibt sich damit aus dem Distributivgesetz. Der Betrag einer komplexen Zahl $|a+b\mathrm{i}| = \sqrt{a^2+b^2}$ ist der Abstand des Punktes (a,b) vom Ursprung $(0,0)$ in der reellen Ebene.
Durch die Abbildung $x \mapsto (x,0)$ wird $\mathbb{R} \subset \mathbb{C}$ Teilkörper. Dies wird durch die Schreibweise $(x,0) = x + 0 \cdot \mathrm{i} = x$ direkt berücksichtigt. Hier ein Rechenbeispiel:

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

Die graphische Darstellung[14] der komplexen Zahlen in der reellen Ebene und die geometrische Interpretation der Addition und Multiplikation (Abb. 1.4) sind nützliche Hilfsmittel. Dadurch lässt sich die algebraische Struktur, die wir dadurch auf den Punkten der reellen Ebene erhalten, zur Lösung von Problemen der ebenen Geometrie anwenden.

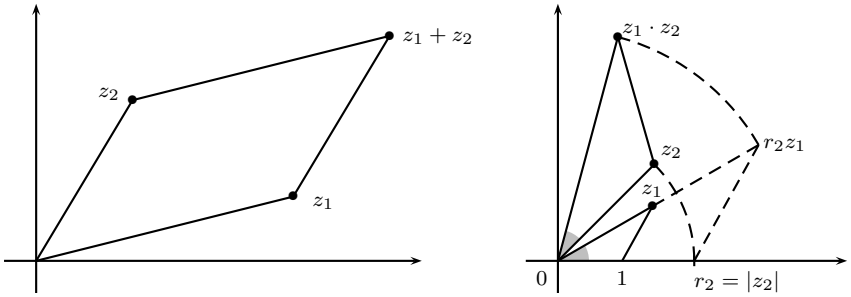


Abb. 1.4 Addition und Multiplikation komplexer Zahlen

Die wichtigste Eigenschaft des Körpers $\mathbb{C}$ ist im folgenden Satz festgehalten, den wir hier ohne Beweis angeben.

Satz 1.4.21 (Fundamentalsatz der Algebra) *Jedes von Null verschiedene Polynom $f \in \mathbb{C}[X]$ lässt sich als Produkt linearer Polynome schreiben:*

[14] Die früheste, heute bekannte Publikation der Idee, komplexe Zahlen durch Punkte einer Ebene zu repräsentieren, erschien im Jahre 1799. Sie stammt von dem norwegisch-dänischen Mathematiker Caspar Wessel (1745–1818), blieb aber damals weitgehend unbemerkt. Zum Allgemeingut wurde diese Idee durch ein kleines Büchlein, welches im Jahre 1806 vom Schweizer Buchhalter und Amateurmathematiker Jean-Robert Argand (1768–1822) in Paris veröffentlicht wurde. In der englischsprachigen Literatur spricht man daher von der *Argand Plane*, in der französischen dagegen manchmal von der *plan de Cauchy*. Der deutsche Mathematiker Carl Friedrich Gauss (1777–1855) trug durch eine Publikation im Jahre 1831 zur Popularisierung dieser Idee bei. Daher spricht man in der deutschsprachigen Literatur von der *Gaußschen Zahlenebene*.

$$f = c \cdot (X - a_1) \cdot (X - a_2) \cdot \ldots \cdot (X - a_n) \, .$$

Dabei ist $c \in \mathbb{C}^*$ der Leitkoeffizient, $n = \deg(f)$ der Grad und die $a_i \in \mathbb{C}$ sind die Nullstellen von f.

Eine komplexe Zahl $a \in \mathbb{C}$ ist genau dann *Nullstelle* von f, wenn $f(a) = 0$ gilt. Jedes Polynom $f \in \mathbb{C}[X]$ von positivem Grad hat mindestens eine Nullstelle in $\mathbb{C}$. Für Teilkörper von $\mathbb{C}$ ist dies nicht der Fall.
Bevor wir uns den versprochenen Anwendungen der bisher entwickelten Theorie zuwenden können, müssen noch zwei sehr nützliche Werkzeuge behandelt werden. Es handelt sich um den Homomorphiesatz und um den Chinesischen Restsatz.

Satz 1.4.22 (Homomorphiesatz für Ringe) *Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Dann ist $\ker(\varphi) \subset R$ ein Ideal, $\operatorname{im}(\varphi) \subset R'$ ein Unterring und die durch $\overline{\varphi}\big([r]\big) := \varphi(r)$ definierte Abbildung*

$$\overline{\varphi} : R/\ker(\varphi) \to \operatorname{im}(\varphi)$$

ist ein Isomorphismus von Ringen.

Beweis. Um zu sehen, dass $\ker(\varphi) \subset R$ ein Ideal ist, betrachten wir $a, b \in \ker(\varphi)$. Das heißt $\varphi(a) = \varphi(b) = 0$ und somit $\varphi(a+b) = \varphi(a) + \varphi(b) = 0$, also $a + b \in \ker(\varphi)$. Wenn $a \in \ker(\varphi)$ und $r \in R$, dann ist $\varphi(ra) = \varphi(r) \cdot \varphi(a) = 0$ und es ergibt sich $ra \in \ker(\varphi)$. Daher ist $\ker(\varphi) \subset R$ ein Ideal.
Nun zeigen wir, dass $\operatorname{im}(\varphi) \subset R'$ ein Unterring ist. Nach Satz 1.3.30 ist $\operatorname{im}(\varphi) \subset R'$ eine additive Untergruppe. Aus $\varphi(1) = 1$ folgt $1 \in \operatorname{im}(\varphi)$. Da sich aus $\varphi(a) \in \operatorname{im}(\varphi)$ und $\varphi(b) \in \operatorname{im}(\varphi)$ auch $\varphi(a) \cdot \varphi(b) = \varphi(ab) \in \operatorname{im}(\varphi)$ ergibt, folgt schließlich, dass $\operatorname{im}(\varphi)$ ein Unterring von R' ist.
Wir wissen aus Satz 1.3.32, dass $\overline{\varphi}$ ein wohldefinierter Isomorphismus der additiven Gruppen ist. Da $\overline{\varphi}\big([a] \cdot [b]\big) = \overline{\varphi}\big([ab]\big) = \varphi(ab) = \varphi(a) \cdot \varphi(b) = \overline{\varphi}\big([a]\big) \cdot \overline{\varphi}\big([b]\big)$ und $\overline{\varphi}\big([1]\big) = \varphi(1) = 1$, ist $\overline{\varphi}$ ein Ringisomorphismus. □

Satz 1.4.23 (Chinesischer[15] Restsatz) *Seien $m_1, \ldots, m_k$ paarweise teilerfremde ganze Zahlen, sei $m := m_1 \cdot \ldots \cdot m_k$ deren Produkt und seien $a_1, \ldots, a_k$ ganze Zahlen. Dann gibt es eine Lösung $x \in \mathbb{Z}$ der simultanen Kongruenzen:*

$$x \equiv a_1 \mod m_1, \qquad x \equiv a_2 \mod m_2, \qquad \ldots \qquad x \equiv a_k \mod m_k$$

und dieses x ist eindeutig bestimmt modulo m.

Beweis. Die Beweisidee besteht darin, das Problem in einfachere Teilprobleme zu zerlegen, aus deren Lösung wir die gesuchte Lösung x zusammensetzen können. Wir bestimmen zunächst ganze Zahlen $x_1, \ldots, x_k$, für die

$$x_i \equiv \begin{cases} 1 & \mod m_i \\ 0 & \mod m_j, \quad \text{falls } j \neq i, \end{cases} \tag{1.34}$$

gilt. Aus solchen x_i ergibt sich dann $x = \sum_{i=1}^{k} x_i a_i \mod m$ als Lösung der gegebenen simultanen Kongruenzen. Da die Differenz zweier Lösungen durch sämtliche m_i teilbar ist und die m_i paarweise teilerfremd sind, folgt die behauptete Eindeutigkeit.
Da die m_i paarweise teilerfremd sind, gilt für eine ganze Zahl x_i genau dann $x_i \equiv 0 \mod m_j$ für alle $j \neq i$, wenn x_i durch $p_i := \prod_{j \neq i} m_j = \frac{m}{m_i}$ teilbar ist. Weil p_i und m_i teilerfremd sind, liefert uns der Euklidische Algorithmus ganze Zahlen r und s, so dass $rp_i + sm_i = 1$. Die Zahl $x_i := rp_i = rm/m_i$ ist dann eine Lösung der simultanen Kongruenzen (1.34). □

Folgerung 1.4.24. *Seien $m_1, \ldots, m_k$ paarweise teilerfremde ganze Zahlen, d.h. $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$, und sei $m := m_1 \cdot \ldots \cdot m_k$. Dann gilt:*

(a) *Durch die Zuordnung $[a]_m \mapsto ([a]_{m_1}, \ldots, [a]_{m_k})$ ist ein Isomorphismus von Ringen definiert:*

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z} \,.$$

(b) *Der Isomorphismus aus (a) induziert einen Isomorphismus abelscher Gruppen*

$$(\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/m_k\mathbb{Z})^* \,.$$

Insbesondere gilt für die Eulersche φ-Funktion: $\varphi(m) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)$.

Beweis. Der Teil (a) ist lediglich eine andere Formulierung von 1.4.23. Statt des angegebenen konstruktiven Beweises kann man (a) aber auch per Induktion aus Satz 1.3.34 gewinnen. Dazu muss man noch bemerken, dass für beliebige $k \in \mathbb{Z}$ stets $[ab]_k = [a]_k \cdot [b]_k$ und $[1]_k = 1$ im Ring $\mathbb{Z}/k\mathbb{Z}$ gilt, und dass somit der Gruppenhomomorphismus in Satz 1.3.34 sogar ein Ringisomorphismus ist.
Da nach Beispiel 1.4.19 (iv) für beliebige Ringe R_i die Einheitengruppe von $R = R_1 \times \ldots \times R_k$ gleich $R^* = R_1^* \times \ldots \times R_k^*$ ist, folgt (b) aus (a). □

[15] In einem chinesischen Mathematiklehrbuch, welches vermutlich etwa im dritten Jahrhundert u.Z. geschrieben wurde, wird nach einer Zahl x gefragt, welche die drei Kongruenzen $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$ und $x \equiv 2 \mod 7$ erfüllt. Die Lösung wurde dort mit der gleichen Methode ermittelt, die auch dem hier angegebenen Beweis zugrunde liegt. Es handelt sich dabei um die früheste bekannte Quelle, in der ein solches Problem behandelt wurde, daher der Name des Satzes.

Es folgt ein Anwendungsbeispiel für den Chinesischen Restsatz.

Beispiel 1.4.25 (Die defekte Waschmaschine). Es war einmal ein Haus, in dem sieben Personen wohnten. Jede von ihnen besaß eine Waschmaschine. All diese Waschmaschinen befanden sich im Waschraum im Keller des Hauses. Eines Tages stellte sich heraus, dass eine der Maschinen defekt ist. Da sich die Mieter jedoch sehr gut verstanden und in unterschiedlichen Abständen ihre Wäsche wuschen, einigten sie sich darauf, dass jeder eine jede der noch funktionierenden Waschmaschinen benutzen darf. Ein Problem war erst dann zu erwarten, wenn alle am selben Tag ihre Wäsche waschen wollten.
Die Mieter einigten sich an einem Sonntag auf dieses liberale Nutzungsverhalten. Dabei stellten sie überrascht fest, dass jeder von ihnen für die kommende Woche einen anderen Tag als Waschtag eingeplant hatte. Von da an wollte jede dieser sieben Personen in regelmäßigen Abständen seine Wäsche waschen. Die Häufigkeit der Waschmaschinenbenutzung ist aus Tabelle 1.2 zu ersehen,

Wochentag	Mo	Di	Mi	Do	Fr	Sa	So
Häufigkeit	2	3	4	1	6	5	7
Person	P_1	P_2	P_3	P_4	P_5	P_6	P_7

Tabelle 1.2 Häufigkeit der Waschmaschinenbenutzung

in der diese Häufigkeit dem Wochentag zugeordnet ist, an dem die betreffende Person in der ersten Woche ihre Wäsche zu waschen beabsichtigte. So wäscht zum Beispiel der Mieter der am Montag wäscht jeden zweiten Tag seine Wäsche, danach dann am Mittwoch, am Freitag, am Sonntag u.s.w.

> Wie lange hatten die Hausbewohner Zeit, die Waschmaschine reparieren zu lassen, ohne dass jemand seinen Rhythmus ändern musste?

Zur Beantwortung dieser Frage gilt es herauszufinden, wann erstmalig alle Mieter am selben Tag waschen wollten. Dazu nummerieren wir die Tage fortlaufend, beginnend mit 1 am Montag nach der Zusammenkunft der Mieter. Die Mieter bezeichnen wir mit $P_1, P_2, \ldots, P_7$, so dass P_i am Tag i wäscht. Die Waschhäufigkeit m_i von P_i ist der Eintrag in der mittleren Zeile von Tabelle 1.2. Die Person P_i wäscht somit genau dann am Tag mit der Nummer x, wenn $x \equiv i \mod m_i$ gilt. Zur Lösung des Problems suchen wir daher die kleinste ganze Zahl $x > 0$, welche sämtliche der folgenden Kongruenzen erfüllt:

$$x \equiv 1 \mod 2 \quad x \equiv 2 \mod 3 \quad x \equiv 3 \mod 4 \quad x \equiv 4 \mod 1$$
$$x \equiv 5 \mod 6 \quad x \equiv 6 \mod 5 \quad x \equiv 7 \mod 7\,.$$

Dies können wir vereinfachen. Da für jedes $x \in \mathbb{Z}$ die Kongruenz $x \equiv 4 \mod 1$ erfüllt ist, können wir sie streichen. Da $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ nach dem Chinesische Restsatz, ist $x \equiv 5 \mod 6$ äquivalent zu den zwei Kongruenzen $x \equiv 1 \mod 2$ und $x \equiv 5 \mod 3$. Da $5 \equiv 2 \mod 3$, treten beide Kongruenzen bereits auf, wir können somit $x \equiv 5 \mod 6$ ersatzlos streichen. Da schließlich

eine Zahl x, für die $x \equiv 3 \mod 4$ gilt, ungerade ist, können wir die Kongruenz $x \equiv 1 \mod 2$ ebenfalls streichen. Es verbleiben die folgenden Kongruenzen:

$$\begin{aligned} x &\equiv 2 \mod 3 & \qquad x &\equiv 3 \mod 4 \\ x &\equiv 1 \mod 5 & \qquad x &\equiv 0 \mod 7\,. \end{aligned} \tag{1.35}$$

Da $3 \cdot 4 \cdot 5 \cdot 7 = 420$, verspricht uns der Chinesische Restsatz eine Lösung, die modulo 420 eindeutig bestimmt ist. Zu beachten ist hier, dass $3, 4, 5, 7$ tatsächlich paarweise teilerfremd sind. Das war bei den ursprünglichen Werten $2, 3, 4, 1, 6, 5, 7$ nicht der Fall, ist aber eine wichtige Voraussetzung für die Anwendung des Chinesischen Restsatzes.
Wenn wir die Methode des Beweises von Satz 1.4.23 auf die Kongruenzen (1.35) aus dem Waschmaschinenproblem anwenden, dann rechnen wir mit den Zahlen $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$ und $a_1 = 2, a_2 = 3, a_3 = 1, a_4 = 0$. Es ergibt sich $m = m_1 m_2 m_3 m_4 = 420$ und $p_1 = 140, p_2 = 105, p_3 = 84, p_4 = 60$. Der Euklidische Algorithmus liefert uns die folgenden Ausdrücke der Gestalt $rp_i + sm_i = 1$:

$$\begin{aligned} i = 1: &\quad 2 \cdot 140 - 93 \cdot 3 = 1 &\quad\Longrightarrow\quad & x_1 = 280 \\ i = 2: &\quad 1 \cdot 105 - 26 \cdot 4 = 1 &\quad\Longrightarrow\quad & x_2 = 105 \\ i = 3: &\quad 4 \cdot\ 84 - 67 \cdot 5 = 1 &\quad\Longrightarrow\quad & x_3 = 336 \\ i = 4: &\quad 2 \cdot\ 60 - 17 \cdot 7 = 1 &\quad\Longrightarrow\quad & x_4 = 120 \end{aligned}$$

Wenn man die Gleichung $rp_i + sm_i = 1$ als Kongruenz $rp_i \equiv 1 \mod m_i$ schreibt und p_i durch Reduktion modulo m_i verkleinert, dann verringert sich der Rechenaufwand ein wenig. Die Ergebnisse x_i ändern sich dadurch jedoch nicht. Als Lösung der simultanen Kongruenzen (1.35) ergibt sich

$$x = \sum_{i=1}^{4} a_i x_i = 2 \cdot 280 + 3 \cdot 105 + 1 \cdot 336 + 0 \cdot 120 = 1211\,.$$

Die allgemeine Lösung hat daher die Gestalt $1211 + n \cdot 420$ mit $n \in \mathbb{Z}$ und die kleinste positive Lösung ist $1211 - 2 \cdot 420 = 371$. Die Hausbewohner haben also 371 Tage – mehr als ein Jahr – Zeit, die Waschmaschine reparieren zu lassen, vorausgesetzt keine weitere Waschmaschine fällt aus und keiner der Mieter ändert seinen Waschrhythmus.

Eine genaue Betrachtung des oben beschriebenen Algorithmus zur Lösung simultaner Kongruenzen zeigt, dass in jeder Teilaufgabe mit den relativ großen Zahlen p_i gerechnet wird. Wenn eine hohe Anzahl von Kongruenzen vorliegt kann dies durchaus zu beträchtlichem Rechenaufwand führen. Durch eine schrittweise Berechnung der Lösung x kann man hier eine Verbesserung erreichen. Die Idee besteht darin, dass man induktiv aus der allgemeinen Lösung

der ersten t Kongruenzen die allgemeine Lösung der ersten $t+1$ Kongruenzen bestimmt.
Als Induktionsanfang können wir $x = a_1$ wählen. Sei x_t eine Lösung der ersten t Kongruenzen: $x_t \equiv a_i \mod m_i$ für $1 \leq i \leq t$. Dann gilt für jede Lösung x_{t+1} der ersten $t+1$ Kongruenzen

$$x_{t+1} = x_t + y \cdot m_1 \cdot \ldots \cdot m_t \qquad \text{und} \qquad x_{t+1} \equiv a_{t+1} \mod m_{t+1} .$$

Um x_{t+1} zu bestimmen, müssen wir alle ganzen Zahlen y ermitteln, für die

$$x_t + y m_1 \cdot \ldots \cdot m_t \equiv a_{t+1} \mod m_{t+1}$$

gilt. Die Lösung ist

$$y \equiv (a_{t+1} - x_t) \cdot (m_1 \cdot \ldots \cdot m_t)^{-1} \mod m_{t+1} .$$

Das Inverse $(m_1 \cdot \ldots \cdot m_t)^{-1}$ existiert in $\mathbb{Z}/m_{t+1}\mathbb{Z}$, da die m_i paarweise teilerfremd sind. Mit diesem y erhalten wir dann x_{t+1}.
Die Lösung der simultanen Kongruenzen (1.35) ergibt sich mit diesem Algorithmus wie folgt:

$$\begin{aligned}
x_1 &= 2 && y \equiv (a_2 - x_1) m_1^{-1} \mod m_2 \\
& && y \equiv (3-2)3^{-1} \mod 4 \\
& && y \equiv 3 \mod 4 \\
x_2 &= x_1 + 3y = 11 && y \equiv (a_3 - x_2)(m_1 m_2)^{-1} \mod m_3 \\
& && y \equiv (1-11)12^{-1} \mod 5 \\
& && y \equiv 0 \mod 5 \\
x_3 &= x_2 + 12y = 11 && y \equiv (a_4 - x_3)(m_1 m_2 m_3)^{-1} \mod m_4 \\
& && y \equiv (0-11)60^{-1} \mod 7 \\
& && y \equiv 6 \mod 7 \\
x_4 &= x_3 + 60y = 371 && \Longrightarrow \quad x = 371 .
\end{aligned}$$

Bemerkung 1.4.26. Beim Rechnen mit sehr großen ganzen Zahlen kommt der Chinesische Restsatz in der Informatik zur Anwendung. Nehmen wir an, ein polynomialer Ausdruck $P(a_1, \ldots, a_r)$ soll für konkret gegebene, aber sehr große $a_i \in \mathbb{Z}$ berechnet werden. Bei bekanntem Polynom P kann man zunächst leicht eine obere Schranke für das Ergebnis berechnen. Sei $m \in \mathbb{Z}$ so, dass $|P(a_1, \ldots, a_r)| < m/2$ gilt. Dann genügt es, die Rechnung in $\mathbb{Z}/m\mathbb{Z}$ durchzuführen. Wenn m sehr groß ist, mag das noch keine bemerkenswerte Verbesserung bringen. An dieser Stelle kann der Chinesischen Restsatz helfen. Dazu wählen wir relativ kleine paarweise teilerfremde Zahlen m_i, deren Produkt $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ sich als Schranke wie zuvor eignet. Bei der Berechnung von $P(a_1, \ldots, a_r) \mod m_i$ treten nun keine sehr großen Zahlen mehr auf. Mit Hilfe des obigen Algorithmus zur Lösung simultaner Kongruen-

zen können wir aus diesen Zwischenergebnissen dann $P(a_1,\dots,a_r) \mod m$ ermitteln. Da $|P(a_1,\dots,a_r)| < \frac{m}{2}$, ist $P(a_1,\dots,a_r)$ gleich dem eindeutig bestimmten Repräsentanten dieser Restklasse im Intervall $\left(-\frac{m}{2},\frac{m}{2}\right)$. Auf diese Weise ist es sogar möglich, dass die Berechnung der k verschiedenen Werte $P(a_1,\dots,a_r) \mod m_i$ parallel durchgeführt wird, wodurch ein weiterer Zeitgewinn erzielt werden kann. Diese Methode kommt zum Beispiel in der Kryptographie zum Einsatz, wo momentan mit Zahlen, die mehr als 200 Dezimalstellen besitzen, gerechnet wird.

Zum Abschluss dieses Abschnittes wenden wir uns einem sowohl theoretisch als auch praktisch sehr nützlichen Resultat zu. Mit seiner Hilfe kann man Multiplikationen im Körper $\mathbb{F}_p$ für große Primzahlen p wesentlich schneller ausführen. Bei der Implementierung mancher Programmpakete der Computeralgebra macht man sich dies tatsächlich zu Nutze.

Satz 1.4.27 *$\mathbb{F}_p^*$ ist eine zyklische Gruppe.*

Beweis. Der Beweis besteht aus fünf Schritten.
SCHRITT 1: *Sei G eine zyklische Gruppe, $m = \operatorname{ord}(G)$ und $d > 0$ ein Teiler von m. Dann ist die Anzahl der Elemente von Ordnung d in G gleich $\varphi(d)$.*
Nach Satz 1.3.33 ist G isomorph zur additiven Gruppe $\mathbb{Z}/m\mathbb{Z}$. Es sind also die Elemente von Ordnung d in dieser Gruppe zu zählen. Aus Beispiel 1.3.22 (iii) (siehe auch Aufgabe 1.15) ist bekannt, dass ein Element $[a] \in \mathbb{Z}/m\mathbb{Z}$ genau dann die Ordnung d hat, wenn $\operatorname{ggT}(a,m) = \dfrac{m}{d}$. Dies ist genau dann der Fall, wenn wir $a = b \cdot \dfrac{m}{d}$ mit einem zu d teilerfremden $b \in \mathbb{Z}$ schreiben können. Daher gibt es ebenso viele Restklassen $[a] \in \mathbb{Z}/m\mathbb{Z}$ der Ordnung d wie es Elemente $[b] \in (\mathbb{Z}/d\mathbb{Z})^*$ gibt. Die Behauptung folgt nun aus $\operatorname{ord}\left((\mathbb{Z}/d\mathbb{Z})^*\right) = \varphi(d)$.
SCHRITT 2: *Für jede ganze Zahl $m \geq 1$ ist $m = \sum_{d|m} \varphi(d)$, wobei sich die Summation über alle positiven Teiler von m erstreckt.*
Da nach Satz 1.3.23 $\operatorname{ord}([a])$ Teiler von $m = \operatorname{ord}\left(\mathbb{Z}/m\mathbb{Z}\right)$ ist, folgt diese Gleichung aus Schritt 1, indem man die m Elemente von $\mathbb{Z}/m\mathbb{Z}$ nach ihrer Ordnung gruppiert zählt.
SCHRITT 3: *Ein Polynom $f \in K[X]$ vom Grad $n \geq 1$ hat höchstens n Nullstellen im Körper K.*
Sei $0 \neq f \in K[X]$ und $a \in K$. Wenn wir f durch $X - a$ mit Rest dividieren (Satz 1.4.8), erhalten wir $h \in K[X]$ und $r \in K$, so dass $f - h \cdot (X - a) = r$. Wenn a eine Nullstelle von f ist, dann folgt $r = 0$ durch Einsetzen von a für X, das heißt $f = h \cdot (X - a)$. Da K nullteilerfrei ist, ergibt sich daraus mittels vollständiger Induktion: Wenn $a_1,\dots,a_k$ paarweise verschiedene Nullstellen von $f \in K[X]$ sind, dann gibt es ein Polynom $g \in K[X]$, so dass $f = (X-a_1)\cdot\ldots\cdot(X-a_k)\cdot g$ gilt. Da K ein Körper ist, addieren sich die Grade von Polynomen bei der Multiplikation. Daher gilt $n = \deg(f) = k + \deg(g) \geq k$.

Das Polynom f kann also höchstens $n = \deg(f)$ verschiedene Nullstellen in K besitzen.
SCHRITT 4: *Die Gruppe $\mathbb{F}_p^*$ enthält höchstens $\varphi(d)$ Elemente der Ordnung d.* Sei $U_d := \{a \in \mathbb{F}_p^* \mid a^d = 1\} \subset \mathbb{F}_p^*$ und $G_d := \{a \in \mathbb{F}_p^* \mid \mathrm{ord}(a) = d\} \subset \mathbb{F}_p^*$. Dann ist $U_d \subset \mathbb{F}_p^*$ Untergruppe und $G_d \subset U_d$ Teilmenge. Die Menge U_d enthält genau die Nullstellen des Polynoms $X^d - 1$ in $\mathbb{F}_p$ und deshalb folgt aus Schritt 3 die Ungleichung $\mathrm{ord}(U_d) \leq d$. Wenn $G_d = \emptyset$, dann ist die behauptete Aussage klar. Wenn es wenigstens ein Element g in G_d gibt, dann erzeugt dieses eine Untergruppe $\langle g \rangle \subset U_d$ der Ordnung d. Wegen $\mathrm{ord}(U_d) \leq d$ folgt daraus $\langle g \rangle = U_d$, diese Gruppe ist also zyklisch. Die Menge G_d besteht genau aus den Elementen der Ordnung d der zyklischen Gruppe U_d, sie enthält somit nach Schritt 1 genau $\varphi(d)$ Elemente.
SCHRITT 5: *Die Gruppe $\mathbb{F}_p^*$ ist zyklisch.*
Wir zählen nun die $m := p - 1$ Elemente der Gruppe $\mathbb{F}_p^*$ nach ihrer Ordnung gruppiert. Das ergibt $m = \sum_{d|m} |G_d|$. Aus Schritt 4 erhalten wir $|G_d| \leq \varphi(d)$, woraus wir unter Benutzung von Schritt 2 die Ungleichungskette

$$m = \sum_{d|m} |G_d| \leq \sum_{d|m} \varphi(d) = m$$

erhalten. Das ist nur möglich, wenn jede der Ungleichungen $|G_d| \leq \varphi(d)$ eine Gleichung ist. Insbesondere muss $|G_m| = \varphi(m) \geq 1$ sein, das heißt, in der multiplikativen Gruppe $\mathbb{F}_p^*$ gibt es ein Element der Ordnung $m = p - 1$. □

Bemerkung 1.4.28. Der gleiche Beweis zeigt, dass für jeden endlichen Körper K die multiplikative Gruppe K^* zyklisch ist.

Beispiel 1.4.29. $\mathbb{F}_5^*$ ist eine zyklische Gruppe der Ordnung 4. Da $\varphi(4) = 2$ ist, gibt es zwei Erzeuger. Dies sind [2] und [3], denn

$$\begin{aligned} [2]^1 &= [2], & [2]^2 &= [4], & [2]^3 &= [3] \\ [3]^1 &= [3], & [3]^2 &= [4], & [3]^3 &= [2]\,. \end{aligned}$$

Dagegen sind [1] und [4] keine Erzeuger. Es gilt $\mathrm{ord}([1]) = 1$ und $\mathrm{ord}([4]) = 2$.

Folgerung 1.4.30. *Für jede ganze Zahl $e \geq 1$ und jede Primzahl $p > 2$ ist $(\mathbb{Z}/p^e\mathbb{Z})^*$ eine zyklische Gruppe.*

Beweis. Der Fall $e = 1$ wurde in Satz 1.4.27 behandelt. Sei nun $e \geq 2$ und $w \in \mathbb{Z}$ eine ganze Zahl, so dass $[w]_p$ ein Erzeuger der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ ist. Wir werden zeigen, dass

$$z := w^{p^{e-1}} \cdot (1 + p) \mod p^e$$

ein Element der Ordnung $(p-1)p^{e-1}$ in $(\mathbb{Z}/p^e\mathbb{Z})^*$ ist. Daraus folgt die Behauptung, denn $\operatorname{ord}(\mathbb{Z}/p^e\mathbb{Z})^* = (p-1)p^{e-1}$. Nach Satz 1.3.23 (2) kommen nur Zahlen der Gestalt $k \cdot p^j$ mit $k \mid p-1$ und $0 \le j \le e-1$ als Ordnung von z in Frage.
Nach dem kleinen Satz von Fermat (Satz 1.3.24) gilt $w^p \equiv w \mod p$, woraus $z^{kp^j} \equiv w^{p^{j+e-1}k} \equiv w^k \mod p$ folgt. Weil $[w]_p$ die Ordnung p hat, ist somit $z^{kp^j} \not\equiv 1 \mod p$ für $0 < k < p-1$. Daher gilt auch $z^{kp^j} \not\equiv 1 \mod p^e$ und es folgt $\operatorname{ord}(z) = (p-1)p^j$ für ein $0 \le j \le e-1$.
Wegen Satz 1.3.23 (3) gilt $w^{p^{e-1}(p-1)} \equiv 1 \mod p^e$, woraus wir $z^{(p-1)p^j} \equiv (1+p)^{(p-1)p^j} \mod p^e$ erhalten. Die Behauptung der Folgerung folgt daher, wenn wir per Induktion über $e \ge 2$ gezeigt haben, dass

$$(1+p)^{(p-1)p^{e-2}} \not\equiv 1 \mod p^e \tag{1.36}$$

gilt. Dabei werden wir benutzen, dass wegen Satz 1.3.23 (3) für alle $e \ge 1$ gilt:

$$(1+p)^{(p-1)p^{e-1}} \equiv 1 \mod p^e \,. \tag{1.37}$$

Für den Induktionsanfang bei $e = 2$ verwenden wir die Binomische Formel (vgl. Aufgabe 1.5) und erhalten

$$(1+p)^{p-1} = 1 + (p-1)p + \binom{p-1}{2}p^2 + \ldots + p^{p-1} \equiv 1 - p \not\equiv 1 \mod p^2 \,.$$

Die Voraussetzung für den Induktionsschritt ist die Gültigkeit von (1.36) für ein festes $e \ge 2$. Wir haben zu zeigen, dass $(1+p)^{(p-1)p^{e-1}} \not\equiv 1 \mod p^{e+1}$ gilt. Nach (1.37) besagt die Voraussetzung gerade, dass es eine ganze Zahl c mit $c \not\equiv 0 \mod p$ gibt, so dass $(1+p)^{(p-1)p^{e-2}} = 1 + cp^{e-1}$ gilt.
Die Binomische Formel ergibt hier

$$\begin{aligned}(1+p)^{(p-1)p^{e-1}} &= \left(1+cp^{e-1}\right)^p = \sum_{k=0}^{p}\binom{p}{k}c^k p^{k(e-1)} \\ &= 1 + cp^e + \binom{p}{2}c^2p^{2(e-1)} + \ldots + c^p p^{p(e-1)} \,.\end{aligned}$$

Da $\binom{p}{k}$ für $1 \le k \le p-1$ durch p teilbar ist (vgl. Aufgabe 1.6), und für $e \ge 2$ die Ungleichungen $1 + k(e-1) \ge e+1$ und $p(e-1) \ge e+1$ gelten, ist $\binom{p}{k}c^k p^{k(e-1)}$ für $1 \le k \le p$ durch p^{e+1} teilbar. Daraus folgt

$$(1+p)^{(p-1)p^{e-1}} \equiv 1 + cp^e \not\equiv 1 \mod p^{e+1} \,,$$

da $c \not\equiv 0 \mod p$. Damit ist (1.36) für alle $e \ge 2$ bewiesen. □

Aufgaben

Übung 1.27. Bestimmen Sie den größten gemeinsamen Teiler der Polynome $f = X^5 - X^3 - X^2 + 1 \in \mathbb{Q}[X]$ und $g = X^3 + 2X - 3 \in \mathbb{Q}[X]$.

Übung 1.28. Dividieren Sie $f = X^5 + X^3 + X^2 + 1$ durch $g = X + 2$ mit Rest in $\mathbb{F}_3[X]$.

Übung 1.29. Beweisen Sie, dass die Menge $I = \{f \in \mathbb{Z}[X] \mid f(1) = 0\}$, aller Polynome $f \in \mathbb{Z}[X]$, die $1 \in \mathbb{Z}$ als Nullstelle haben, ein Ideal ist. Ist I ein Hauptideal?

Übung 1.30. Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom (vgl. 1.4.13). Beweisen Sie, dass der Ring $K[X]/\langle f \rangle$ ein Körper ist.

Übung 1.31. Beweisen Sie, dass $\mathbb{F}_2[X]/\langle X^2+X+1 \rangle$ ein Körper ist. Wie viel Elemente enthält dieser Körper? Beschreiben Sie die multiplikative Gruppe dieses Körpers. Ist sie zyklisch?

Übung 1.32. Beweisen Sie für jede ganze Zahl $n > 1$, dass jedes Element des Ringes $\mathbb{Z}/n\mathbb{Z}$ entweder eine Einheit oder ein Nullteiler ist.

Übung 1.33. Bestimmen sie die kleinste positive ganze Zahl x, welche das folgende System simultaner Kongruenzen erfüllt:

$$x \equiv 2 \mod 7, \qquad x \equiv 3 \mod 8, \qquad x \equiv 4 \mod 9.$$

Zusatz: Denken Sie sich eine möglichst realistische Textaufgabe (aus dem Alltagsleben oder aus Wissenschaft und Technik) aus, die auf ein System simultaner Kongruenzen führt.

Übung 1.34. Bestimmen Sie alle ganzen Zahlen x, welche das folgende System simultaner Kongruenzen erfüllen:

$$x \equiv 5 \mod 7, \qquad x \equiv 7 \mod 11, \qquad x \equiv 11 \mod 13.$$

Übung 1.35. Finden Sie für jede Primzahl p ein Polynom $0 \neq f \in \mathbb{F}_p[X]$, welches *jedes* Element des Körpers $\mathbb{F}_p$ als Nullstelle hat.
Finden Sie ein Polynom vom Grad 2 in $\mathbb{F}_5[X]$, welches in $\mathbb{F}_5$ *keine* Nullstelle besitzt. Versuchen Sie das auch für alle anderen Körper $\mathbb{F}_p$!

Übung 1.36. Sei K ein Körper und $\mathbb{N}_+ := \{n \in \mathbb{Z} \mid n > 0\}$. Auf der Menge $I(K) := \{f \mid f : \mathbb{N}_+ \to K \text{ ist eine Abbildung}\}$ definieren wir eine Addition und eine Multiplikation wie folgt:

$$(f+g)(n) := f(n) + g(n) \quad \text{und} \quad (f \cdot g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Dabei erstreckt sich die Summe über alle positiven Teiler von n. Das Element $e \in I(K)$ sei durch $e(1) = 1$ und $e(n) = 0$ für $n > 1$ gegeben. Zeigen Sie:

(a) $I(K)$ ist ein Ring mit dem Einselement e.
(b) $f \in I(K)$ ist genau dann eine Einheit, wenn $f(1) \in K^*$.
(c) Sei $u \in I(K)$ durch $u(n) = 1$ für alle $n \in \mathbb{N}_+$ gegeben und φ wie üblich die Eulerfunktion. Berechnen Sie das Produkt $u \cdot \varphi$ in $I(K)$.

Übung 1.37. Geben Sie alle Erzeuger der multiplikativen Gruppe $\mathbb{F}_{17}^*$ an und berechnen Sie die Ordnung jedes Elements dieser Gruppe.

Übung 1.38. Bestimmen Sie die Nullstellen $a, b \in \mathbb{C}$ des Polynoms

$$2X^2 - 2X + 5$$

und berechnen Sie die komplexen Zahlen $a + b, a \cdot b, a - b$ und $\frac{a}{b}$.

1.5 Kryptographie

Kryptographie ist die Wissenschaft von der Verschlüsselung von Nachrichten. Dabei geht es darum, aus einem gegebenen Klartext ein sogenanntes Kryptogramm (Geheimtext) zu erzeugen, aus dem nur ein bestimmter Personenkreis – die rechtmäßigen Empfänger – den gegebenen Klartext rekonstruieren kann. Statt „verschlüsseln“ bzw. „Rekonstruktion des Klartextes“ sagt man auch *chiffrieren* bzw. *dechiffrieren*.
Wir konzentrieren uns in diesem Abschnitt auf die einfachsten mathematischen Grundlagen der Kryptographie. Nach einer kurzen Erwähnung klassischer Chiffrierverfahren und einer knappen Erläuterung des Diffie-Hellman-Schlüsselaustausches widmen wir uns hauptsächlich der Beschreibung des RSA-Verfahrens. Dabei kommen Kenntnisse aus den vorigen Abschnitten zur Anwendung.
Die Verschlüsselung von Informationen ist bei jeder Übermittlung von vertraulichen Daten über ein öffentlich zugängliches Datennetzwerk notwendig. Wenn Sie zum Beispiel bei einer online-Buchhandlung ein Buch kaufen möchten und dies mit Ihrer Kreditkarte bezahlen, dann muss gesichert sein, dass Unbefugte nicht an ihre Kreditkartendaten kommen. Außerdem gibt es seit Jahrtausenden im militärischen Bereich ein starkes Bedürfnis nach geheimer Übermittlung von Nachrichten.
Durch den griechischen Historiker Plutarch (ca. 46–120 u.Z.) ist es überliefert, dass bereits vor etwa 2500 Jahren die Regierung von Sparta zur Übermittlung geheimer Nachrichten an ihre Generäle folgende Methode benutzte:
Sender und Empfänger besaßen identische zylinderförmige Holzstäbe, sogenannte Skytale. Zur Chiffrierung wurde ein schmales Band aus Pergament spiralförmig um den Zylinder gewickelt. Dann wurde der Text parallel zur Achse des Stabes auf das Pergament geschrieben. Der Text auf dem abgewickelten Band schien dann völlig sinnlos. Nach dem Aufwickeln auf seine Skytale konnte der Empfänger den Text jedoch ohne große Mühe lesen. Hierbei

handelt es sich um eine *Permutationschiffre*: Die Buchstaben des Klartextes werden nach einer bestimmten Regel permutiert.
Eine weitere, seit langem bekannte Methode der Chiffrierung ist die *Verschiebechiffre*. Dabei werden die Buchstaben des Klartextes nach bestimmten Regeln durch andere Buchstaben ersetzt. Die älteste bekannte Verschiebechiffre wurde von dem römischen Feldherrn und Diktator Julius Cäsar (100–44 v.u.Z.) benutzt. Es existieren vertrauliche Briefe von Cäsar an Cicero, in denen diese Geheimschrift benutzt wird.
Die Methode ist denkbar einfach. Jeder Buchstabe wird durch den Buchstaben des Alphabets ersetzt, der drei Stellen weiter links im Alphabet steht. Zur praktischen Realisierung schreibt man das Alphabet jeweils gleichmäßig auf zwei kreisförmige Pappscheiben unterschiedlichen Radius (Abb. 1.5). Die Scheiben werden an ihren Mittelpunkten drehbar miteinander verbunden. Für Cäsars Chiffre muss man einfach das „A“ der einen Scheibe mit dem „D“ der anderen in Übereinstimmung bringen. Dadurch erhält man eine Tabel-

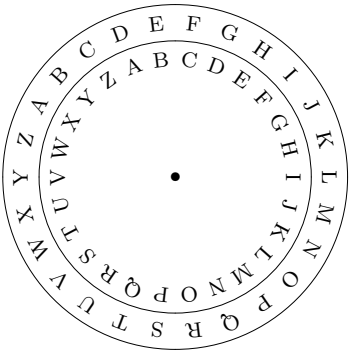


Abb. 1.5 Cäsars Chiffre

le, mit der man chiffrieren und dechiffrieren kann. Mit dem heutigen Wissen bietet eine solche Chiffrierung keinerlei Sicherheit mehr. Weitere Verfahren dieser Art findet man zum Beispiel im Buch von A. Beutelspacher [Beu]. Ein sehr schönes Beispiel einer Kryptoanalyse eines chiffrierten Textes, bei der die Buchstaben des Alphabets durch andere Zeichen ersetzt wurden, kann man in der Kurzgeschichte „Der Goldkäfer“ des amerikanischen Autors E.A. Poe (1809–1849) nachlesen.
Die Sicherheit der bisher beschriebenen Verfahren ist nach heutigen Maßstäben sehr gering. Ein bekanntes Verfahren, welches perfekte Sicherheit bietet, geht auf Vigenère[16] zurück. Anstelle einer festen Regel benutzt es für die Ersetzung der Klartextbuchstaben eine zufällige und beliebig lange Buchstabenfolge, einen sogenannten Buchstabenwurm. Die Sicherheit dieses Verfahrens hängt davon ab, dass Sender und Empfänger irgendwann

[16] Blaise de Vigenère (1523–1596), französischer Diplomat.

über einen sicheren Kanal den Schlüssel und damit die Details für den Algorithmus, ausgetauscht haben. Dies kann beispielsweise durch persönliche Übergabe erfolgen. Für die Anwendung in Computernetzwerken ist dies jedoch nur unter besonderen Umständen praktikabel. Für den Alltagsgebrauch, wie zum Beispiel beim online-Buchkauf, benötigt man andere Methoden für den Schlüsselaustausch.
Moderne Methoden beruhen auf einer bahnbrechenden Idee, die erstmals 1976 von Diffie und Hellman [DH] veröffentlicht wurde. Sie besteht darin, sogenannte *Einwegfunktionen* zu benutzen. Das sind Funktionen, die leicht berechenbar sind, deren inverse Abbildung aber nur für den Besitzer von Zusatzinformationen leicht zu berechnen ist. Ohne Zusatzinformation ist die Berechnung des Inversen so aufwändig und langwierig, dass praktisch Sicherheit gegeben ist, zumindest für eine begrenzte Zeit.
Beispiele solcher Einwegfunktionen sind das *Produkt zweier Primzahlen* und die *diskrete Exponentialabbildung* $\mathbb{Z}/\varphi(n)\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^*$, die bei vorgegebener Basis s durch $x \mapsto s^x$ definiert ist. Für sehr große ganze Zahlen ist die Berechnung der Inversen – die *Faktorisierung in Primzahlen* bzw. der *diskrete Logarithmus* – sehr zeitaufwändig.
Der Schlüsselaustausch nach Diffie-Hellman geschieht wie folgt: Die Personen **A** und **B** wollen einen Schlüssel in Form eines Elements von $\mathbb{Z}/p\mathbb{Z}$ vereinbaren, ohne dass ein Dritter dies in Erfahrung bringen kann. Dazu wird eine große Primzahl p und eine ganze Zahl $0 < s < p$ öffentlich ausgetauscht. Nun wählt **A** eine ganze Zahl $a \in \mathbb{Z}$ und **B** eine ganze Zahl $b \in \mathbb{Z}$, so dass $0 < a, b < p - 1$. Diese Information wird von beiden geheim gehalten. Dann berechnet **A** den Wert $s^a \mod p$ in $\mathbb{Z}/p\mathbb{Z}$ und übermittelt ihn **B**. Ebenso sendet **B** den Wert $s^b \mod p$ an **A**. Schließlich berechnen beide den gleichen Wert $(s^b)^a \equiv s^{a \cdot b} \equiv (s^a)^b \mod p$. Auf diese Weise ist beiden Personen (und keinem Dritten) der gemeinsame Schlüssel $s^{a \cdot b} \mod p$ in $\mathbb{Z}/p\mathbb{Z}$ bekannt.
Zur praktischen Anwendung würde die Online-Buchhandlung eine Primzahl p, eine ganze Zahl $0 < s < p$ und $s^b \mod p$ veröffentlichen. Es ist günstig, wenn s ein Erzeuger der multiplikativen Gruppe $\mathbb{F}_p^*$ ist. Die Zahl b bleibt geheim und ist nur dem Buchhändler bekannt. Für die Sicherheit der Daten ist die Einweg-Eigenschaft des diskreten Logarithmus entscheidend.
Der Kunde wählt nun zufällig eine Zahl a und berechnet $(s^b)^a \mod p$ in $\mathbb{Z}/p\mathbb{Z}$, das ist der Schlüssel für seine Transaktion. Diesen benutzt er, um mit Hilfe eines vom Buchhändler bekanntgegebenen Verfahrens seine Daten zu chiffrieren. In der von Taher ElGamal im Jahre 1985 veröffentlichten Arbeit [EG] wurde als Chiffrierverfahren einfach die Multiplikation mit dem Schlüssel in $\mathbb{Z}/p\mathbb{Z}$ vorgeschlagen, dies wird heute als *ElGamal-Verfahren* bezeichnet. Die Chiffrierung kann jedoch auch auf jede andere, vorher vereinbarte Art erfolgen. Zusätzlich zum chiffrierten Text übermittelt er auch $s^a \mod p$, woraus der Buchhändler den Schlüssel $(s^a)^b \mod p$ berechnen kann.

Die Vorgehensweise beim *RSA-Verfahren* ist eine völlig andere. Es beruht darauf, dass die Produktabbildung $\{\text{Primzahl}\} \times \{\text{Primzahl}\} \to \mathbb{Z}$ eine Einwegfunktion ist. Es ist nach seinen Entdeckern R. Rivest, A. Shamir, L. Adle-

man [RSA] benannt. Das Grundprinzip ist das Folgende: Zu einer natürlichen Zahl n wird ein öffentlicher Schlüssel $e \in \mathbb{Z}$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$ gewählt. Durch das Lösen der Gleichung $[e] \cdot [d] = 1$ in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ wird der geheime Schlüssel $d \in \mathbb{Z}$ bestimmt.
Jeder, der das Paar (n, e) kennt, kann eine Nachricht chiffrieren. Dies geschieht, indem eine Kongruenzklasse $m \in \mathbb{Z}/n\mathbb{Z}$ zu $m^e \in \mathbb{Z}/n\mathbb{Z}$ verschlüsselt wird. Um dies zu dechiffrieren benutzt man den Satz 1.3.24. Er liefert $(m^e)^d = m^{e \cdot d} = m$ in $\mathbb{Z}/n\mathbb{Z}$. Dazu ist die Kenntnis der Zahl d nötig. Daher muss man d geheim halten, wogegen die Zahlen n und e öffentlich bekanntgegeben werden.
Die Sicherheit dieses Verfahrens beruht darauf, dass die Berechnung von d bei Kenntnis von n und e ohne weitere Zusatzinformationen ein sehr aufwändiges Problem ist. Die Methoden von Abschnitt 1.2 erlauben uns, den geheimen Schlüssel d mit Hilfe des Euklidischen Algorithmus zu berechnen. Dazu muss allerdings auch die Zahl $\varphi(n)$ bekannt sein. Wenn die Faktorisierung von n in ein Produkt von Primzahlen bekannt ist, dann ist die Berechnung von $\varphi(n)$ mit Hilfe von Satz 1.3.34 oder Folgerung 1.4.24 sehr leicht. Für große n (das heißt momentan mit 200 bis 400 Dezimalstellen) ist das Auffinden der Zerlegung in Primfaktoren ein sehr aufwändiges Problem.
Zur praktischen Durchführung beschafft man sich zunächst zwei verschiedene, relativ große Primzahlen p und q. Dann berechnet man $n = pq$ und $\varphi(n) = (p-1)(q-1)$. Letzteres ist die Geheiminformation, die man nicht preisgeben darf und die nach der Berechnung von d nicht mehr benötigt wird.
Vor einigen Jahren galten dabei 100-stellige Primzahlen als hinreichend sicher. Man muss allerdings mit der Entwicklung von Technik und Algorithmen ständig Schritt halten. Heute ist es kein Problem, eine 430-Bit Zahl innerhalb einiger Monate mit einem einzigen PC zu faktorisieren. Durch die Entwicklung der Hardware und durch die Entdeckung besserer Algorithmen zur Faktorisierung großer Zahlen wird die Größe der Zahlen, die in erträglicher Zeit faktorisierbar sind, in naher Zukunft wachsen. Wer Verantwortung für Datensicherheit übernimmt, sollte sich daher regelmäßig über den aktuellen Stand der Entwicklung informieren.
Die Firma RSA-Security hatte im Jahre 1991 eine Liste von Zahlen veröffentlicht, für deren Faktorisierung Preisgelder in unterschiedlicher Höhe ausgesetzt wurden („Factoring Challenge“). Im Jahre 2001 wurde diese Liste wegen der rasanten Erfolge durch eine neue ersetzt. Die größte Zahl auf dieser Liste heißt `RSA-2048`. Sie hat 2048 Ziffern in Binärdarstellung und 617 Dezimalziffern. Es war ein Preisgeld in Höhe von 200 000 US$ auf ihre Faktorisierung ausgesetzt. Sämtliche Zahlen dieser Liste sind Produkt zweier Primzahlen.
Die Faktorisierung der 129-stelligen Zahl `RSA-129` im April 1994 hatte damals das öffentliche Interesse auf diese sogenannten RSA-Zahlen gelenkt. Diese Zahl wurde im Jahre 1977 von R. Rivest, A. Shamir, und L. Adleman zur Verschlüsselung einer der ersten Nachrichten mit dem RSA-Verfahren benutzt. Zur Zeit der Veröffentlichung der verschlüsselten Nachricht glaubte man, dass es Millionen von Jahren dauern wird, bis diese Nachricht ent-

schlüsselt sein wird. Die 1994 gefundene Entschlüsselung lautete: „The magic words are squeamish ossifrage“ [Fr].
Die Faktorisierung dieser 129-stelligen Zahl gelang unter anderem durch Parallelisierung der Rechnung, einer Idee, der wir bereits in Bemerkung 1.4.26 begegnet sind.
Anfang Dezember 2003 wurde bekanntgegeben, dass eine weitere Zahl aus der erwähnten Liste faktorisiert wurde. Es handelte sich dabei um `RSA-576`, deren Faktorisierung mit 10 000 US$ dotiert war. Die Binärdarstellung dieser Zahl besitzt 576 Ziffern. In Dezimaldarstellung handelt es sich um die 174-ziffrige Zahl

188198812920607963838697239461650439807163563379417382700763355642298885971523466548531906060650474304531738801130339671619969232120573403187955065699622130516875930765025705967161996923212057340318795506569962213051687593076502570591

Die Faktorisierung wurde von einem von Prof. Jens Franke (Mathematisches Institut der Universität Bonn) geleiteten Team durchgeführt. Diese Zahl konnte unter Benutzung eines Algorithmus aus der algebraischen Zahlentheorie, den man das Zahlkörpersieb nennt, in zwei Primzahlen mit je 87 Ziffern zerlegt werden. Dadurch wurde deutlich, dass nunmehr keine Hochleistungsrechner mehr nötig sind, um solch eine Aufgabe zu lösen: Die wesentlichen Rechnungen wurden auf gewöhnlichen PC's, die in besonderer Weise vernetzt waren, durchgeführt und dauerten etwa 3 Monate.
Die Bonner Gruppe um J. Franke hat dann im Mai 2005 die Zahl `RSA-200` (200 Ziffern im Dezimalsystem, siehe Abb. 1.6) und im November 2005 auch die 193-ziffrige Zahl `RSA-640` faktorisiert. Auf die letztere war ein Preisgeld von 20 000 US$ ausgesetzt. Obwohl damit noch nicht das Ende der Liste der Firma RSA-Security erreicht war, wurde der Wettbewerb um die Faktorisierung dieser Zahlen im Frühjahr 2007 für beendet erklärt.

27997833911221327870829467638722601621070446786955
42853756000992932612840010760934567105295536085606
18223519109513657886371059544820065767750985805576
13579098734950144178863178946295187237869221823983
=
35324619344027701212726049781984643686711974001976
25023649303468776121253679423200058547956528088349
×
79258699544783330333470858414800596877379758573642
19960734330341455767872818152135381409304740185467

Abb. 1.6 Faktorisierung von `RSA-200`

Die Electronic Frontier Foundation[17] hat einen Preis von 100 000 US$ für diejenigen ausgesetzt, die eine Primzahl mit mehr als 10 000 000 Ziffern finden. Solche Zahlen wurden im Sommer 2008 gefunden. Wer eine Primzahl mit mindestens 10^8 Ziffern findet, auf den warten nun 150 000 US$. Die größte bisher gefundene Primzahl hat 12 978 189 Ziffern. Das ist die Zahl $2^{43112609} - 1$. Es handelt sich dabei um eine sogenannte Mersenne-Primzahl[18], d.h. eine Primzahl der Form $M_n := 2^n - 1$. Es ist leicht zu sehen, dass $2^n - 1$ nur Primzahl sein kann, wenn n selbst eine Primzahl ist. Mersenne behauptete, dass für $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ die Zahl M_n eine Primzahl ist. Für M_{67} und M_{257} erwies sich das später als falsch. So fand F. Cole[19] die Faktoren von M_{67}. Bis heute sind 46 Mersenne-Primzahlen bekannt. Es ist auch nicht klar, ob es unendlich viele gibt. Die Mersenne-Zahlen kann man verallgemeinern und Zahlen vom Typ $\frac{b^n-1}{b-1}$ betrachten. Diese Zahlen zeichnen sich dadurch aus, dass sie in der b-adischen Darstellung (vgl. Kapitel 3.4) genau n Einsen haben. Insbesondere hat $2^n - 1$ im Dualsystem genau n Einsen. Wenn $b = 10$ ist, erhält man eine sogenannte *Repunit*[20] $R_n := \frac{10^n-1}{9}$. Die Zahl R_{1031} wurde im Jahre 1986 von H. Williams und H. Dubner als Primzahl identifiziert. Sie besteht aus 1031 Ziffern, die alle gleich 1 sind, siehe [WD].

Mancher Leser mag sich fragen, wie man die bisher besprochene Verschlüsselung von Elementen aus $\mathbb{Z}/n\mathbb{Z}$ auf die Verschlüsselung realer Texte anwenden kann. Eine mögliche Antwort ist die Folgende.
Der aus Schriftzeichen bestehende Klartext wird zunächst in eine Zahl umgewandelt. Dazu kann man den ASCII-Code benutzen. ASCII ist eine Abkürzung für American Standard Code for Information Interchange. Dieser Code, der zu Beginn der 1960-er Jahre entwickelt wurde, ordnet jedem Buchstaben des englischen Alphabets und einigen Sonderzeichen eine 7-Bit Zahl zu. In der heutigen Zeit stehen normalerweise 8 Bits zur Speicherung und Verarbeitung von 7-Bit ASCII-Zeichen zur Verfügung. Das zusätzliche Bit könnte als Paritätsbit zur Fehlererkennung genutzt werden (vgl. Beispiel 2.5.6), es wird jedoch heute meist mit Null belegt.
Auf den ASCII-Code bauen viele andere Codierungen auf, die zur Digitalisierung anderer Zeichen in nicht-englischen Sprachräumen entwickelt wurden. Das gilt auch für den in den 1990-er Jahren entwickelten Unicode-Standard, der die Codierungsvielfalt abgelöst hat. Der Unicode-Standard erlaubt die Codierung tausender Symbole und Schriftzeichen aus verschiedensten Kulturen der Welt.
Die 26 Großbuchstaben entsprechen im ASCII-Code den in Tabelle 1.3 angegebenen Dezimal- bzw. Hexadezimalzahlen. Durch Addition von 32 (bzw. 20 hexadezimal) ergibt sich der Wert des entsprechenden Kleinbuchstabens.

[17] `www.eff.org`

[18] Marin Mersenne (1588–1648), französischer Mathematiker und Theologe.

[19] Frank Nelson Cole (1861–1926), US-amerikanischer Mathematiker.

[20] aus dem Englischen von *repeated unit*.

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M
ASCII (dezimal)	65	66	67	68	69	70	71	72	73	74	75	76	77
ASCII (hex)	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D

Buchstabe	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ASCII (dezimal)	78	79	80	81	82	83	84	85	86	87	88	89	90
ASCII (hex)	4E	4F	50	51	52	53	54	55	56	57	58	59	5A

Tabelle 1.3 ASCII-Code für Großbuchstaben

Da beim RSA-Verfahren in $\mathbb{Z}/n\mathbb{Z}$ gerechnet wird, muss der Text in entsprechende Abschnitte zerlegt werden, so dass die durch die ASCII-Codierung entstehende Zahl kleiner als n ist.
Um mittelfristige Datensicherheit zu gewährleisten, wird heute empfohlen, dass bei praktischer Anwendung des RSA-Verfahrens, die Zahl n mindestens eine 2048-Bit Zahl ist. Diese haben bis zu 617 Ziffern in Dezimaldarstellung. Der zu verschlüsselnde Text ist dann in Blöcke zu je 256 Zeichen zu zerlegen, da $8 \cdot 256 = 2048$. Jeder so gewonnene Textblock wird mit Hilfe des ASCII-Codes in eine Zahl $0 < m < n$ übersetzt, die zur Verschlüsselung zur e-ten Potenz erhoben wird: $m^e \mod n$.
Der Empfänger der Nachricht, der als Einziger den geheimen Schlüssel d kennt, dechiffriert diese Nachricht, indem er zunächst jede der empfangenen Zahlen in die d-te Potenz modulo n erhebt. Als Binärzahl geschrieben sind die 8-er Blöcke der so erhaltenen Zahlen dann der ASCII-Code der Zeichen der ursprünglichen Textblöcke.

Beispiel 1.5.1. Sei $p = 1373$ und $q = 2281$, dann ist $n = pq = 3131813$ und $\varphi(n) = 3128160$. Da $2^{21} = 2097152 < n$ können wir drei 7-Bit ASCII Symbole am Stück verarbeiten. Zur Chiffrierung der drei Zeichen `R S A` können wir deren Hexadezimalwerte `52 53 41` aus Tabelle 1.3 als Folge von 7-Bit Zahlen schreiben: `1010010 1010011 1000001`. Für die Rechnung per Hand ist es jedoch einfacher mit den Dezimalwerten `82 83 65` zu rechnen. Die obige 21-Bit Zahl hat den Wert $82 \cdot 2^{14} + 83 \cdot 2^7 + 65 = 1354177$. Wird der öffentliche Schlüssel $e = 491$ benutzt, dann ist $1354177^{491} \mod 3131813$ zu berechnen. Dies ist kongruent 992993 modulo 3131813. Da $992993 = 60 \cdot 2^{14} + 77 \cdot 2^7 + 97$, besteht der verschlüsselte Text aus den Zeichen der ASCII-Tabelle mit den Nummern `60 77 97`, das sind: `< M a`. Wir hatten Glück, dass die Chiffrierung auf druckbare Zeichen geführt hat. Die Zeichen mit den Nummern 0–31 und 127 in der ASCII-Tabelle sind nicht-druckbare Sonderzeichen, daher wird man auf dem hier begangenen Weg nicht immer zu einem druckbaren verschlüsselten Text gelangen. Das ist kein Mangel, denn allein aus den Zahlenwerten lässt sich der Originaltext mit Hilfe des geheimen Schlüssels rekonstruieren. Eine Betrachtung des Textes in verschlüsselter Form ist in der Regel wenig informativ.
Da wir die Zerlegung von n in Primfaktoren und daher auch $\varphi(n)$ kennen, können wir Hilfe des Euklidischen Algorithmus den geheimen Schlüssel $d =$

6371 bestimmen. Es ist eine nützliche Übung, die Dechiffrierung von `< M a` mit dieser Zahl d konkret durchzuführen.

Mit Hilfe des RSA-Verfahrens kann man auch eine sogenannte digitale Unterschrift erzeugen. Zu diesem Zweck muss der Absender **A** der Nachricht einen öffentlichen Schlüssel bekanntgegeben haben. Wenn (n_A, e_A) der öffentliche Schlüssel und d_A der geheime Schlüssel von **A** sind, dann wird eine unverschlüsselte Nachricht m durch Anhängen von $m^{d_A} \mod n_A$ unterschrieben. Jeder kann jetzt durch Berechnung von $\left(m^{d_A}\right)^{e_A} \mod n_A$ feststellen, ob der angehängte chiffrierte Teil tatsächlich mit dem gesendeten Klartext übereinstimmt. In der Realität wird nicht die gesamte Nachricht, sondern nur der Wert einer Hashfunktion chiffriert (vgl. Seite 312).
Wenn auch der Empfänger **E** einen öffentlichen Schlüssel (n_E, e_E) bekanntgegeben hat, dann kann **A** ihm eine elektronisch unterschriebene und chiffrierte Nachricht senden. Dies geschieht, indem zuerst der Klartext wie beschrieben signiert und anschließend mit dem öffentlichen Schlüssel von **E** chiffriert wird. Der Empfänger geht nun umgekehrt vor. Zuerst dechiffriert er die Nachricht mit Hilfe seines geheimen Schlüssels d_E, dann prüft er die Unterschrift durch Anwendung des öffentlichen Schlüssels von **A**.
In der modernen Kryptographie werden heute algebraische Strukturen verwendet, die weit über den Rahmen dieses einführenden Kapitels hinausgehen. Zum Beispiel basiert die Verwendung von *elliptischen Kurven* auf Methoden der algebraischen Geometrie. Wer interessiert ist, findet in [Bau], [Beu], [Ko1], [Ko2], [BSW] und [We] Material unterschiedlichen Schwierigkeitsgrades für das weitere Studium.
Zum Abschluss dieses Abschnittes möchten wir nochmals die Warnung aussprechen, dass wir uns hier auf die Darlegung der mathematischen Grundideen der modernen Kryptographie beschränkt haben. In der angegebenen Form weisen die beschriebenen Verfahren beträchtliche Sicherheitslücken auf. Um wirkliche Datensicherheit zu erreichen, ist eine genaue Analyse der bekannten Angriffe auf die benutzten Kryptosysteme notwendig.

Aufgaben

Übung 1.39. Bestimmen Sie den geheimen Schüssel d für jedes der folgenden Paare (n, d) von öffentlichen RSA-Schlüsseln:
(i) $(493, 45)$ (ii) $(10201, 137)$ (iii) $(13081, 701)$ (iv) $(253723, 1759)$

Übung 1.40. Sei $p = 31991$ und $s = 7$.

(a) Sei $a = 27$ und $b = 17$. Bestimmen Sie $s^a \mod p$, $s^b \mod p$ und den Diffie-Hellman Schlüssel $s^{a \cdot b} \mod p$.
(b) Versuchen Sie den Schlüssel zu finden, den zwei Personen durch Austausch der beiden Zahlen 4531 und 13270 vereinbart hatten.

Übung 1.41. Mit dem öffentlichen RSA-Schlüssel $(n, e) = (9119, 17)$ sollen Nachrichten chiffriert werden. In diesen Texten werden nur solche Zeichen zugelassen, deren ASCII-Code einen Dezimalwert zwischen 32 und 90 hat. Der Nachrichtentext wird in Paare von Zeichen zerlegt. Die zweiziffrigen Dezimaldarstellungen dieser beiden Zeichen werden jeweils zu einer vierstelligen Dezimalzahl nebeneinandergestellt. Auf diese Weise wird aus dem Buchstabenpaar `BK` die Dezimalzahl $m = 6675$.
Die Chiffrierung erfolgt nach dem RSA-Verfahren durch die Berechnung von $m^e \mod n$. Für $m = 6675$ erhält man $4492 \mod 9119$. An den Empfänger der verschlüsselten Nachricht wird nicht diese Zahl, sondern die entsprechende ASCII-Zeichenkette übermittelt. Im Fall von 4492 finden wir in der ASCII-Tabelle zu den Dezimalzahlen 44 und 92 die Symbole `,\`
Finden Sie den aus 6 Buchstaben bestehenden Klartext, der mit diesem Verfahren zu dem Geheimtext `+TT&@/` wurde.

http://www.springer.com/978-3-540-89106-2

Mathematik für Informatiker
Algebra, Analysis, Diskrete Strukturen
Kreussler, B.; Pfister, G.
2009, XII, 457 S., Softcover
ISBN: 978-3-540-89106-2