Angewandte Mathematik

Studienbrief 3

FH University of Applied Sciences TECHNIKUM WIEN

Elemente der Zahlentheorie

Gerald und Susanne Teschl

Copyright Springer Verlag 2006–2023. Dieses Skriptum darf nur intern an der FH Technikum Wien verwendet werden.

Druckfehler/Feedback bitte an:
susanne.teschl@technikum-wien.at

WS 23/24

Studienbrief 3

Elemente der Zahlentheorie

Inhalt

3.1 Modulare Arithmetik oder das kleine Einmaleins auf endlichen Mengen

Erinnern Sie sich an die Division mit Rest aus Satz 2.50: Wenn $a \in \mathbb{Z}$ und $m \in \mathbb{N}$, so kann man a in der Form

$$a = q \cdot m + r$$

schreiben, wobei q und r aus $\mathbb{Z}$ eindeutig bestimmt sind durch die Festlegung $0 \leq r < m$. Diese Zahl r heißt Rest der Division und man verwendet dafür auch die Schreibweise mit dem Modulo-Operator: $r = a \bmod m$. Beispiel: $17 \bmod 5 = 2$, in Worten: „Der Rest der Division von 17 durch 5 ist 2“ oder kurz „17 modulo 5 ist 2“.

In diesem Studienbrief werden wir uns näher mit dem Rechnen mit Resten, der sogenannten modularen Arithmetik beschäftigen. Insbesondere werden wir es dabei nur mit ganzen Zahlen, also Elementen aus $\mathbb{Z}$, zu tun haben.

Modulare Arithmetik ist für viele Anwendungen in der Informatik wichtig, u.a. in der Kryptographie (z. B. RSA-Algorithmus) und Codierungstheorie. Denn immer, wenn man es mit einem endlichen Alphabet (durch Zahlen codiert) zu tun hat, stößt man unweigerlich auf Reste. Ein einfaches Beispiel: Das Alphabet {A, ..., Z} kann durch die Zahlen $\{0, 1, \ldots, 25\}$ dargestellt werden. Angenommen, eine Verschlüsselungsvorschrift lautet $y = x + 3$. Dann wird $x = 2$ (= Buchstabe C) zu $y = 2 + 3 = 5$ (Buchstabe F) verschlüsselt; $x = 25$ (Buchstabe Z) wird aber zu $y = 28$ verschlüsselt. Wir fallen also aus dem Alphabet heraus, es sei denn, wir beginnen bei 26 wieder mit A. Mathematisch formuliert nehmen wir den Rest modulo 26: $y = (x + 3) \bmod 26$. Damit ist $y = 28 \bmod 26 = 2$ (Buchstabe C).

Definition 3.1 Wenn zwei ganze Zahlen a und b bei Division durch $m \in \mathbb{N}$ denselben Rest haben, so sagt man, a und b sind **kongruent modulo** m. Man schreibt dafür $a \equiv b \pmod{m}$ oder auch einfach $a = b \pmod{m}$. Die Zahl m heißt **Modul**.

Also $17 = 22 \pmod 5$. Man kann bequem überprüfen, ob zwei Zahlen kongruent modulo m sind, indem man ihre Differenz betrachtet:

Satz 3.2 Zwei Zahlen a und b sind kongruent modulo m genau dann, wenn ihre Differenz ein Vielfaches von m ist, d.h., wenn $a - b = km$ mit $k \in \mathbb{Z}$ ist.
Mit anderen Worten: $a = b \pmod m$ bedeutet, dass a und b *bis auf ein Vielfaches von* m gleich sind.

Das ist leicht zu verstehen: $a = b \pmod m$ bedeutet ja, dass beide denselben Rest r bei Division durch m haben; das heißt, es gibt ganze Zahlen q_1 und q_2 mit $a = q_1 m + r$ und $b = q_2 m + r$. Das bedeutet aber, dass $a - b = (q_1 - q_2)m$, dass also $a - b$ ein Vielfaches von m ist.

Beispiel 3.3 (→CAS) Kongruente Zahlen
Richtig oder falsch?
a) $17 = 2 \pmod 5$ b) $17 = -3 \pmod 5$ c) $18 = 25 \pmod 6$

Lösung zu 3.3

a) Richtig, denn die Differenz $17 - 2 = 15$ ist ein Vielfaches von 5 (oder anders ausgedrückt: 17 und 2 haben bei Division durch 5 denselben Rest).
b) Richtig, denn $17 - (-3) = 17 + 3 = 20$ ist ein Vielfaches von 5.
c) Falsch, denn $25 - 18 = 7$ ist kein Vielfaches von 6.

■

Wir haben in Beispiel 3.3 gesehen, dass 17 kongruent modulo 5 sowohl zu 2, als auch zu -3 ist. Allgemein ist 17 ist kongruent modulo 5 zu allen Zahlen, die sich von 17 um ein Vielfaches von 5 unterscheiden. Man sagt, alle diese Zahlen liegen in der **Restklasse** R_2 zum Rest 2. Da bei Division durch 5 die Reste $r = 0, 1, 2, 3, 4$ auftreten können, gibt es fünf Restklassen $R_r = \{r + k \cdot 5 \mid k \in \mathbb{Z}\}$ modulo 5:

$$\begin{aligned}
R_0 &= \{k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \\
R_1 &= \{1 + k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \\
R_2 &= \{2 + k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \\
R_3 &= \{3 + k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} \\
R_4 &= \{4 + k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}
\end{aligned}$$

Allgemein gibt es m Restklassen modulo m, nämlich für jeden der Reste 0, 1, …, $m - 1$ genau eine Restklasse $R_r = \{r + k \cdot m \mid k \in \mathbb{Z}\}$.

Bei Rechnungen modulo m kann man in Summen und Produkten jederzeit eine Zahl durch irgendeine andere zu ihr kongruente Zahl (d.h. durch einen anderen **Vertreter** aus ihrer Restklasse) ersetzen:

Satz 3.4 Seien $a, b, c, d \in \mathbb{Z}$ und $m \in \mathbb{N}$. Wenn $a = b \pmod m$ und $c = d \pmod m$ gilt, dann folgt

$$\begin{aligned}
a + c &= b + d \pmod m \\
a \cdot c &= b \cdot d \pmod m.
\end{aligned}$$

Warum gelten die Rechenregeln aus Satz 3.4? Nun, $a = b \pmod m$ bedeutet gleicher Rest, also eine Darstellung der Form $a = qm + r_1$ und $b = pm + r_1$. Analog bedeutet $c = d \pmod m$ gleicher Rest, also $c = km + r_2$ und $d = hm + r_2$. Setzen wir das nun für a, b, c, d ein: $a + c = qm + r_1 + km + r_2 = (q + k)m + (r_1 + r_2)$, analog ist $b + d = pm + r_1 + hm + r_2 = (p + h)m + (r_1 + r_2)$. Wir sehen also, dass $a + c$ und $b + d$ denselben Rest bei Division durch m haben, kurz: $a + c = b + d \pmod m$. Analog geht die Überlegung für die Multiplikation.

Beispiel 3.5 Rechnen mit kongruenten Zahlen
Berechnen Sie den angegebenen Rest:
a) $(38 + 22) \bmod 9$ b) $(101 + 234) \bmod 5$ c) $(38 \cdot 22) \bmod 9$
d) $(101 \cdot 234) \bmod 5$ e) $(38 + 22 \cdot 17) \bmod 4$

Lösung zu 3.5

a) Natürlich können wir $38 + 22 = 60$ und dann den Rest von 60 bei Division durch 9 berechnen: $60 \bmod 9 = 6$. Alternative: Wir suchen den kleinsten Vertreter aus der Restklasse von 38, ebenso aus der Restklasse von 22 (das sind gerade die Reste 2 bzw. 4). Aus Satz 3.4 folgt dann: $38 + 22 = 2 + 4 = 6 \pmod 9$.

b) Wieder ersetzen wir die vorkommenden Zahlen durch ihre Reste modulo 5: $101+234 = 1+4 = 5 = 0 \,(\mathrm{mod}\, 5)$. Die Zahl $101+234 = 335$ hat bei Division durch 5 also den Rest 0.

c) Wegen $38 = 2 \,(\mathrm{mod}\, 9)$ und $22 = 4 \,(\mathrm{mod}\, 9)$ ist $38 \cdot 22 = 2 \cdot 4 = 8 \,(\mathrm{mod}\, 9)$. Wir konnten also recht mühelos berechnen, dass die Zahl $38 \cdot 22$ bei Division durch 9 den Rest 8 hat!

d) Wegen $101 = 1 \,(\mathrm{mod}\, 5)$ und $234 = 4 \,(\mathrm{mod}\, 5)$ ist $101 \cdot 234 = 1 \cdot 4 = 4 \,(\mathrm{mod}\, 5)$.

e) $38 + 22 \cdot 17 = 2 + 2 \cdot 1 = 4 = 0 \,(\mathrm{mod}\, 4)$.

■

Beispiel 3.6 Wochentagsformel
Welcher Wochentag war der 15.5.1955?
(Hinweise: (i) Der 1.1.1900 war ein Montag. (ii) Alle durch 4 teilbaren Jahre sind Schaltjahre, mit Ausnahme der durch 100 teilbaren, die nicht auch gleichzeitig durch 400 teilbar sind. Zum Beispiel war 1900 kein Schaltjahr, da es durch 100, nicht jedoch durch 400 teilbar ist; aber 2000 war ein Schaltjahr, weil es durch 400 teilbar ist.)

Lösung zu 3.6 Wir müssen die Anzahl der Tage, die zwischen dem 1.1.1900 und dem 15.5.1955 vergangen sind, berechnen und modulo 7 nehmen. Dann wissen wir den Wochentag (0 = Montag, 1 = Dienstag, usw.).

Beginnen wir mit den Tagen zwischen dem 1.1.1900 und dem 1.1.1955. Da ein Jahr 365 Tage hat, waren es $365 \cdot 55$ Tage (Schaltjahre noch nicht berücksichtigt). Da wir nur das Ergebnis modulo 7 brauchen, können wir $365 = 1 \,(\mathrm{mod}\, 7)$ und $55 = 6 \,(\mathrm{mod}\, 7)$ verwenden und erhalten $365 \cdot 55 = 1 \cdot 6 = 6 \,(\mathrm{mod}\, 7)$. Wegen $55 = 4 \cdot 13 + 3$ gab es dazwischen 13 Schaltjahre (1900 war kein Schaltjahr). Für jedes Schaltjahr müssen wir einen Tag dazurechnen, also kommen wir auf $6 + 13 = 19 = 5 \,(\mathrm{mod}\, 7)$. Der 1.1.1955 war also ein Samstag.

Nun zu den Tagen zwischen 1.1.1955 und 1.5.1955. Wir brauchen nur die Tage der Monate (Achtung beim Februar, falls es sich um ein Schaltjahr handelt)

Monat	1	2	3	4	5	6	7	8	9	10	11	12
Tage	31	28/29	31	30	31	30	31	31	30	31	30	31
Tage (mod 7)	3	0/1	3	2	3	2	3	3	2	3	2	3

zusammenzuzählen: $3+0+3+2 = 1 \,(\mathrm{mod}\, 7)$. Die Bilanz bisher (vom 1.1.1900 bis 1.5.1955) lautet dann: $5+1 = 6$. Der 1.5.1955 war somit ein Sonntag. Nehmen wir nun noch die 14 Tage seit Monatsbeginn (1.5.1955 bis 15.5.1955) dazu und zählen alles zusammen, so erhalten wir $5 + 1 + 14 = 20 = 6 \,(\mathrm{mod}\, 7)$. Der gesuchte Tag war also ein Sonntag! ■

Wenn man zuerst die Anzahl der Tage berechnet und erst am Ende modulo 7 rechnet, dann muss man schon ganz gut im Kopfrechnen sein. So ist es aber auch für ungeübte Kopfrechner zu schaffen! Analoges gilt für Computerprogramme; da kann es nämlich schnell passieren (z. B. in

der Kryptographie, wo mit großen Zahlen „modulo“ gerechnet wird), dass man einen Überlauf produziert, wenn man es ungeschickt angeht.

Modulorechnen wird auch bei Prüfziffern verwendet.

Vielleicht haben Sie schon einmal im Internet mit Ihrer Kreditkarte bezahlt und der Computer hat beim Absenden der Daten Ihre Kartennummer als ungültig zurückgewiesen. Bei Kontrolle der Nummer ist Ihnen dann aufgefallen, dass Sie bei der Eingabe zwei Ziffern vertauscht haben. Hätte der Computer diesen Fehler nicht sofort erkannt, so wären vermutlich einige Umstände auf Sie, den Verkäufer und die Kreditkartenfirma zugekommen. Wie aber hat der Computer erkannt, dass Sie zwei Ziffern vertauscht haben? Die Lösung ist einfach: Die letzte Ziffer einer Kreditkartennummer ist eine Prüfziffer, die mit modularer Arithmetik aus den übrigen Ziffern berechnet wird. Stimmt sie nicht, so wurde bei der Eingabe ein Fehler gemacht.

Beispiel 3.7 Prüfziffer
Auf Büchern findet sich eine dreizehnstellige *Internationale Standard-Buchnummer* (ISBN-13) der Form *abc-d-efghi-jkl-p*. Dabei ist *abc* je nach Buch 978 oder 979, d steht für die Sprache ($d = 3$ bedeutet zum Beispiel „deutschsprachig”), *efghi* kennzeichnet den Verlag und *jkl* den Buchtitel. Schließlich ist p die Prüfziffer, die

$$a + 3b + c + 3d + e + 3f + g + 3h + i + 3j + k + 3l + p = 0 \pmod{10}$$

erfüllen muss. Das Buch „Geheime Botschaften“ von S. Singh hat die ISBN-13 978-3-42333-071-*p*. Wie lautet die Prüfziffer p ($0 \leq p \leq 9$)?

Lösung zu 3.7 Die Prüfziffer p muss Lösung der Gleichung

$$9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 4 + 3 \cdot 2 + 3 + 3 \cdot 3 + 3 + 3 \cdot 0 + 7 + 3 \cdot 1 + p = 0 \pmod{10}$$

sein. Es muss also $82+p = 2+p = 0 \pmod{10}$ gelten. Somit ist $p = -2 = 8 \pmod{10}$, also $p = 8$. ■

3.1.1 Anwendung: Hashfunktionen

Modulare Arithmetik wird auch bei **Hashverfahren** verwendet. Eine **Hashfunktion** ist eine Funktion, die Datensätzen beliebiger Länge (beliebig viele Bit) Datensätze fester Länge (z. B. 128 Bit) zuordnet. Diese Datensätze fester Länge (also z. B. alle Dualzahlen der Länge 128) heißen **Hashwerte**. Hashverfahren werden in der Informatik zum Beispiel zum effizienten Speichern und Suchen von Datensätzen verwendet.

Betrachten wir folgendes Beispiel: Wir möchten Orte und zugehörige Vorwahlen so speichern, dass man zu einem gegebenen Ort möglichst schnell die zugehörige Vorwahl bekommt. Jeder Datensatz besteht aus zwei Teilen: Ort (das ist der Suchbegriff, der eingegeben wird) und Vorwahl. Der Teil, nach dem gesucht wird, in

unserem Fall der Ort, wird **Schlüssel** genannt. Der andere Teil des Datensatzes, in unserem Fall die Vorwahl, wird als **Wert** bezeichnet.

Die Idee ist, dass die Speicheradresse aus dem Schlüssel (Suchbegriff) selbst berechnet wird, sodass aufwendige Suchverfahren nicht notwendig sind. Dies geschieht durch eine Hashfunktion. Das ist in diesem Beispiel eine Abbildung H von der Menge K aller möglichen Schlüssel k (Orte) in die Menge A der verfügbaren Speicheradressen:

$$\begin{aligned} H:\ K &\to A = \{0, 1, \ldots, N-1\} \\ k &\mapsto H(k) \end{aligned}$$

Wir haben hier angenommen, dass es N Adressen gibt, die mit $0, \ldots, N-1$ durchnummeriert werden. Der Schlüssel k wird also unter der Adresse $H(k)$ (Hashwert des Schlüssels) abgelegt bzw. wieder gefunden.

Beispiel 3.8 Hashfunktion
Die möglichen Schlüssel k sind Zeichenketten, die Orte bedeuten. Die Hashfunktion sei

$$H(k) = \Big(\sum_i a_i\Big) \bmod N,$$

wobei a_i die Stelle des i-ten Buchstaben im Alphabet bezeichnet (Beispiel: Für $k = XYZ$ ist $a_1 = 24$, $a_2 = 25$ und $a_3 = 26$). Angenommen, es gibt $N = 7$ Speicheradressen. Berechnen Sie dann den Wert der Hashfunktion für folgende Schlüssel: WIEN, GRAZ, SALZBURG, DORNBIRN.

Lösung zu 3.8 Dem Ort WIEN entsprechen die Zahlen $23, 9, 5, 14$ (da W der 23. Buchstabe im Alphabet ist, I der 9. Buchstabe, usw.). Die Speicheradresse von WIEN ist daher $H(\text{WIEN}) = 23 + 9 + 5 + 14 = 51 = 2 \pmod 7$. Analog folgt $H(\text{GRAZ}) = 3$, $H(\text{SALZBURG}) = 1$, $H(\text{DORNBIRN}) = 3$. (Da hier immer modulo 7 gerechnet wird, lassen wir den Zusatz $(\bmod 7)$ weg, um Schreibarbeit zu sparen.) ■

Dieses Beispiel zeigt das typische Problem bei Hashverfahren: Den Schlüsseln GRAZ und DORNBIRN wird derselbe Speicherplatz zugeordnet. Man spricht von einer **Kollision**. In der Tat ist die Anzahl aller möglichen Schlüssel (hier alle möglichen Buchstabenkombinationen) in der Regel um ein Vielfaches größer als die Anzahl der verfügbaren Hashwerte (hier Speicheradressen). Daher legt man im Fall einer Kollision den Schlüssel auf einem um eine bestimmte Schrittweite m verschobenen Speicherplatz ab.

Zusammenfassend geht man daher wie folgt vor: Soll der Datensatz (k, v) bestehend aus Schlüssel k (für engl. *key* = Schlüssel) und Wert v (engl. *value* = Wert) abgelegt werden, so

- berechne den Hashwert $n = H(k)$.

- Ist der Speicherplatz n frei, so lege den Datensatz dort ab, sonst (Kollision) versuche den um m Plätze verschobenen Speicherplatz $n + m \pmod N$.

Soll zu einem gegebenen Schlüssel k der zugehörige Wert v gefunden werden, so

- berechne $n = H(k)$.
- Ist der dort liegende Schlüssel k_n gleich k, so ist das zugehörige v_n der gesuchte Wert. Andernfalls gehe auf den um m verschobenen Speicherplatz $n + m \pmod N$ und vergleiche erneut den Suchbegriff mit dem dort abgelegten Schlüssel.

Für die Fälle, dass beim Abspeichern kein freier Platz mehr gefunden wird, oder der Suchbegriff keinem Datensatz entspricht, müssen noch Abbruchbedingungen eingebaut werden, um Endlosschleifen zu vermeiden.

Beispiel 3.9 Hashtabelle
Gegeben seien folgende Paare aus Schlüsseln und Werten: (WIEN, 01), (GRAZ, 0316), (SALZBURG, 0662), (DORNBIRN, 05572). Die Hashfunktion sei wie im vorigen Beispiel definiert. Bei Auftreten einer Kollision soll um $m = 1$ Speicherplätze weitergegangen werden. Stellen Sie die Hashtabelle auf und suchen Sie den Wert von DORNBIRN.

Lösung zu 3.9 Aus dem letzten Beispiel wissen wir bereits, dass $H(\text{WIEN}) = 2$, $H(\text{GRAZ}) = 3$, $H(\text{SALZBURG}) = 1$ und $H(\text{DORNBIRN}) = 3$. Wir legen also die Datensätze für WIEN, GRAZ und SALZBURG auf die Speicherplätze 2, 3 bzw. 1. Da der Speicherplatz 3 bereits belegt ist, legen wir DORNBIRN auf dem Platz $3 + 1 = 4$ ab:

Speicherplatz (n)	Schlüssel (k_n)	Wert (v_n)
0		
1	SALZBURG	0662
2	WIEN	01
3	GRAZ	0316
4	DORNBIRN	05572
5		
6		

Um nach DORNBIRN zu suchen, berechnen wir zunächst $H(\text{DORNBIRN}) = 3$. Da $k_3 = \text{GRAZ} \neq \text{DORNBIRN}$, müssen wir 3 um 1 erhöhen. Nun ist $k_4 = \text{DORNBIRN}$ und $v_4 = 05572$ der gesuchte Wert. ■

In der Praxis sollten natürlich nicht zu viele Kollisionen auftreten, deshalb muss eine gute Hashfunktion die möglichen Schlüssel möglichst gleichmäßig auf die möglichen Speicherplätze verteilen. Als Faustregel gilt weiters, dass maximal 80% der verfügbaren Speicherplätze aufgefüllt werden sollten.

Die Wahrscheinlichkeit, dass *irgendeine* Kollision auftritt, ist übrigens recht hoch, wie das folgende **Geburtstagsparadoxon** zeigt: Nehmen wir an, Sie ordnen jeder Person in einem Raum ihren Geburtstag zu. Die Personen werden also gleichmäßig auf 365 Plätze verteilt (wir nehmen an, dass jeder Geburtstag gleich wahrscheinlich ist). Eine Kollision tritt auf, wenn *irgendwelche* zwei Personen darunter am gleichen Tag Geburtstag haben. Die Wahrscheinlichkeit dafür ist bei 23 Personen bereits über 50%! Wenn Sie also bei einer Party mit mindestens 23 Personen wetten, dass *irgendwelche* zwei Gäste am gleichen Tag Geburtstag haben, so sind Ihre Chancen zu gewinnen größer als 50%! Verteilt man n Schlüssel (Personen) auf N Plätze (Tage im Jahr), so ist die Wahrscheinlichkeit für mindestens eine Kollision (gemeinsamer Geburtstag) $P = 1 - \frac{N!}{(N-n)!N^n}$.

Hashfunktionen werden auch oft als Prüfziffern verwendet. Ein früher häufig verwendetes Verfahren ist der MD5-Algorithmus (Message Digest Version 5), der aus Daten beliebiger Länge eine 128-Bit Prüfziffer (=Hashwert) berechnet. Er wurde zum Beispiel gemeinsam mit einem Programmpaket veröffentlicht um nach dem Download durch Vergleich sicherstellen zu können, dass die Datei ohne Fehler heruntergeladen wurde. Der MD5-Algorithmus hat dabei noch eine weitere Eigenschaft: Während es bei klassischen Prüfziffern (z. B. ISBN) leicht möglich ist, Daten (gezielt) zu verändern, ohne die Prüfziffer zu ändern, ist dies hier um ein Vielfaches schwerer. Solche Hashfunktionen sind schwer zu finden und werden als **Einweg-Hashfunktionen** oder **digitaler Fingerabdruck** bezeichnet. Die Einweg-Eigenschaft ist entscheidend für Anwendungen in der Kryptographie (z. B. für die digitale Signatur). Statt des MD5-Algorithmus verwendet man heutzutage z.B. den Secure-Hash-Algorithmus (z.B. SHA-256, SHA-512), der die Einweg-Anforderung noch besser erfüllt.

3.2 Gruppen, Ringe und Körper

Fassen wir alle möglichen Reste, die bei der Division modulo m entstehen können, zu einer neuen Menge zusammen:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Äquivalent kann man $\mathbb{Z}_m$ auch als die Menge aller Restklassen modulo m definieren, da jede Restklasse $R_r = \{r + k \cdot m \mid k \in \mathbb{Z}\}$ ja eindeutig durch den zugehörigen Rest r bestimmt ist. In diesem Sinn steht z.B. der Rest $2 \in \mathbb{Z}_5$ stellvertretend für die gesamte zugehörige Restklasse $R_2 = \{2 + k \cdot 5 \mid k \in \mathbb{Z}\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$. Manchmal wird die Schreibweise $\mathbb{Z}/m\mathbb{Z}$ anstelle von $\mathbb{Z}_m$ verwendet.

Diese Menge von Resten hat, wie eingangs erwähnt, zum Beispiel die Bedeutung eines Alphabets: etwa $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ oder, für die Informatik besonders wichtig, $\mathbb{Z}_2 = \{0, 1\}$. In $\mathbb{Z}_m$ (also für die „Buchstaben des Alphabets“) kann man nun auf einfache Weise eine Addition und eine Multiplikation definieren, indem man als Ergebnis immer den Rest modulo m nimmt (und somit niemals aus dem Alphabet herausfällt). Zum Beispiel erhalten wir für $\mathbb{Z}_5$ folgende Additions- und

Multiplikationstabelle:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Zum Beispiel ist in der linken Tabelle $4+2=1 \pmod 5$, da $4+2=6$ und der Rest von 6 bei Division durch 5 gleich 1 ist. Rechte Tabelle: $2 \cdot 3 = 6 = 1 \pmod 5$. Wir addieren und multiplizieren also wie gewohnt in $\mathbb{Z}$ und berechnen dann den Rest modulo 5. Dadurch ist unser Ergebnis immer in $\mathbb{Z}_5$

Beispiel 3.10 Addition und Multiplikation in $\mathbb{Z}_m$
Berechnen Sie:
a) $3+5$ in $\mathbb{Z}_7$ b) $8+3$ in $\mathbb{Z}_{11}$ c) $3 \cdot 5$ in $\mathbb{Z}_7$ d) $8 \cdot 3$ in $\mathbb{Z}_{11}$

Lösung zu 3.10

a) $3+5=8=1 \pmod 7$, da der Rest von 8 bei Division durch 7 gleich 1 ist.
b) $8+3=11=0 \pmod{11}$, da der Rest von 11 bei Division durch 11 gleich 0 ist.
c) $3 \cdot 5 = 15 = 1 \pmod 7$
d) $8 \cdot 3 = 24 = 2 \pmod{11}$

■

Genau genommen rechnet auch jeder Computer mit Resten. Nehmen wir einfachheitshalber an, dass zur Speicherung nur zwei (Dezimal-)Stellen zur Verfügung stehen. Dann tritt z. B. bei der Addition $86 + 22$ ein Überlauf auf und das Ergebnis ist nicht 108, sondern 8. Der Computer rechnet hier also modulo 100. Es ist die Aufgabe des Programms, diesen Fehler zu erkennen und abzubrechen.

Andererseits ist es aber auch möglich, diesen Überlauf bewusst auszunutzen, um mit *negativen* Zahlen zu rechnen: Da $86 = -14 \pmod{100}$, verhält sich 86 bei Rechnungen modulo 100 gleich wie -14. So ist zum Beispiel $22+86=8 \pmod{100}$, ebenso wie $22-14=8 \pmod{100}$. In der Informatik verwendet man das, um negative ganze Zahlen abzuspeichern:

Stehen $n+1$ Bit zur Verfügung, so werden die ganzen Zahlen von -2^n bis 2^n-1 dadurch abgespeichert, dass man jede negative Zahl x zwischen -2^n und -1 mit der zugehörigen positiven Zahl y zwischen 2^n und $2^{n+1}-1$ identifiziert, die $x = y \pmod{2^{n+1}}$ erfüllt. Beispiel: Bei $n+1=4$ Bit werden die Zahlen $-2^3, \ldots, -1$ durch die Zahlen $2^3, \ldots, 2^4-1$ dargestellt. Zum Beispiel wird -4 durch 12 dargestellt, denn $-4 = 12 \pmod{16}$.

In Dualdarstellung lässt sich das leicht durchführen, indem man mit dem Betrag beginnt, $|-4| = 4 = (0100)_2$, alle Nullen und Einsen vertauscht, $(1011)_2 = (11)_{10}$ (**Einskomplement**), und dann eins hinzuaddiert, $(1100)_2 = (12)_{10}$ (**Zweikomplement**). Warum funktioniert das? Wenn ich zu einer Zahl ihr Einskomplement addiere erhalte ich die größtmögliche darstellbare Zahl (lauter 1 in der Binärdarstellung). Durch die Addition von eins wird der Überlauf provoziert und eine Zahl plus ihr Zweikomplement ist 0.

Wir sehen aus obiger Tabelle, dass $4+1=0 \pmod 5$. Man kann also 1 als Negatives zu 4 in $\mathbb{Z}_5$ betrachten.

Definition 3.11 Zu $e \in \mathbb{Z}_m$ ist das **Negative** oder **additive Inverse** jene Zahl $d \in \mathbb{Z}_m$, für die

$$e + d = 0 \pmod{m}$$

ist. Man schreibt für das additive Inverse wie gewohnt $-e$.

Ein additives Inverses gibt es zu jeder Zahl aus $\mathbb{Z}_m$ und es lässt sich auch leicht berechnen:

Satz 3.12 Zu jeder Zahl e aus $\mathbb{Z}_m$ gibt es genau ein additives Inverses $d \in \mathbb{Z}_m$:

$$d = m - e \quad \text{für} \quad e \neq 0 \qquad \text{und} \qquad d = 0 \quad \text{für} \quad e = 0.$$

Beispiel 3.13 **Additives Inverses in $\mathbb{Z}_m$**
Finden Sie das additive Inverse von $0, 1, 2, 3, 4$ in $\mathbb{Z}_5$.

Lösung zu 3.13 Das additive Inverse von 0 ist 0. Weiters ist das Negative zu 1 gleich $-1 = 5-1$ (oder $-1+5) = 4$. Weiters: $-2 = -2+5 = 3$, $-3 = -3+5 = 2$, $-4 = -4+5 = 1$. Probe: $0+0 = 0 \pmod 5$, $1+4 = 0 \pmod 5$, $2+3 = 0 \pmod 5$, $3+2 = 0 \pmod 5$, $4+1 = 0 \pmod 5$. ■

Eine kleine Anwendung des additiven Inversen ist die sogenannte Caesar-Verschlüsselung. Julius Caesar (100–44 v. Chr.) soll damit geheime Botschaften verschlüsselt haben:

Beispiel 3.14 **Caesar-Verschlüsselung**
Codieren Sie die Buchstaben des Alphabets zunächst gemäß A = 0, B = 1, ..., Z = 25 durch Zahlen und verschlüsseln Sie dann die Nachricht „KLEOPATRA“ nach der Vorschrift

$$y = x + e \pmod{26} \quad \text{mit dem Schlüssel } e = 3.$$

Wie wird wieder entschlüsselt?

Lösung zu 3.14 In Zahlen lautet KLEOPATRA: $10, 11, 4, 14, 15, 0, 19, 17, 0$. Verschlüsseln wir jede dieser Zahlen x gemäß $y = x + 3 \pmod{26}$:

x	10	11	4	14	15	0	19	17	0
$y = x + 3 \pmod{26}$	13	14	7	17	18	3	22	20	3

Wir erhalten die verschlüsselte Nachricht (in Zahlen) $13, 14, 7, 17, 18, 3, 22, 20, 3$, oder, wieder in Buchstaben: NOHRSDWUD.

Zum Entschlüsseln müssen wir $y = x + 3 \pmod{26}$ nach x auflösen, indem wir auf beiden Seiten -3 addieren, also $x = y - 3 = y + 23 \pmod{26}$. Zum Beispiel erhalten wir für $y = 13$ den Klartextbuchstaben $x = 13 + 23 = 36 = 10 \pmod{26}$ usw. Alternativ wäre hier der Rechengang $x = 13 - 3 = 10 \pmod{26}$ zulässig gewesen.

y	13	14	7	...	20	3
$x = y + 23 \pmod{26}$	10	11	4	...	17	0

■

Warnung: Dieses Verfahren bietet keinerlei Sicherheit, da es nur 25 Möglichkeiten für die Verschiebung gibt, es also leicht ist, alle Möglichkeiten durchzuprobieren. Das Knacken des Codes geht sogar noch schneller, wenn der Text lang genug ist: Da der häufigste Buchstabe im Deutschen das „E“ ist, liegt die Vermutung nahe, dass er auf den häufigsten Buchstaben im Geheimtext abgebildet wird. Und wenn wir die Verschlüsselung eines einzigen Buchstaben kennen, dann kennen wir bei der Caesar-Verschlüsselung bereits die gesamte Verschlüsselungsvorschrift.

Sie kennen die Caesar-Verschlüsselung vielleicht auch aus dem Internet als ROT13. Hier wird um genau 13 Stellen verschoben. Dadurch ergibt sich die spezielle Eigenschaft von ROT13, dass die gleiche Funktion zum Ver- und Entschlüsseln verwendet wird, denn: $13 = -13 \pmod{26}$, also $d = e$.

Nehmen wir uns nun die Multiplikation in $\mathbb{Z}_m$ vor: Wir sehen aus obiger Multiplikationstabelle, dass $2 \cdot 3 = 1 \pmod{5}$. Man kann also 3 als den *Kehrwert* von 2 in $\mathbb{Z}_5$ betrachten.

Definition 3.15 Wenn es zu $e \in \mathbb{Z}_m$ eine Zahl $d \in \mathbb{Z}_m$ gibt mit

$$e \cdot d = 1 \pmod{m},$$

so nennt man d den **Kehrwert** oder das **multiplikative Inverse** zu e modulo m. In Anlehnung an die gewohnte Schreibweise in $\mathbb{R}$ schreibt man das multiplikative Inverse zu e in $\mathbb{Z}_m$ kurz als e^{-1} oder als $\frac{1}{e}$.

Also ist in $\mathbb{Z}_5$ mit der Schreibweise $\frac{1}{2}$ die Zahl 3 gemeint. Achtung: Im Unterschied zum additiven Inversen gibt es nicht zu allen Zahlen aus $\mathbb{Z}_m$ ein multiplikatives Inverses. Wenig überraschend ist, dass es zu 0 kein multiplikatives Inverses in $\mathbb{Z}_m$ gibt.

Das ist klar: Denn für jedes $d \in \mathbb{Z}_m$ gilt ja, dass $0 \cdot d = 0$ ist, also kann das Ergebnis niemals 1 werden. Aus demselben Grund gibt es auch in $\mathbb{R}$ für die 0 keinen Kehrwert („Division durch 0 gibt es nicht“). Abgesehen von der 0 gibt es in $\mathbb{R}$ aber für jede Zahl einen Kehrwert.

Es kann aber abgesehen von 0 noch weitere Zahlen in $\mathbb{Z}_m$ geben, die keinen Kehrwert besitzen:

Satz 3.16 Sei $e \neq 0$ in $\mathbb{Z}_m$. Dann gilt: e besitzt ein multiplikatives Inverses genau dann, wenn e und m teilerfremd sind, wenn also $\text{ggT}(e, m) = 1$ ist.

Das kann man folgendermaßen sehen: Suchen wir zum Beispiel ein Inverses zu 2 modulo 6, also d mit $2d = 1 \pmod 6$. Das bedeutet, dass sich $2d$ und 1 um ein Vielfaches von 6 unterscheiden müssen, dass also $2d = 1+n6$ für ein $n \in \mathbb{Z}$ gelten muss; oder, umgeformt, $2d-6n = 1$. Weil 6 und 2 nun den gemeinsamen Teiler 2 haben, können wir diesen Teiler herausheben: $2d - 6n = 2(d - 3n) = 1$. Es gibt aber kein ganzzahliges d, sodass diese Gleichung, die ja die Form 2·ganze Zahl $= 1$ hat, erfüllt ist! Da 2 und 6 also einen gemeinsamen Teiler haben, gibt es kein multiplikatives Inverses für 2 modulo 6.

Wenn es einen Kehrwert gibt, dann kann er (zumindest für kleines m) durch systematische Suche gefunden werden:
• Weg 1: Wir berechnen für $d = 1, 2, 3, \ldots, m-1$ das Produkt $e \cdot d \bmod m$, bis wir als Ergebnis 1 erhalten. ($d = 0$ braucht man natürlich nicht zu probieren, denn damit wird man nie das Ergebnis 1 bekommen.)
• Weg 2: Wir verwenden $d = \frac{1+km}{e}$ und probieren $k = 1, 2, \ldots, e-1$, bis der Zähler durch e teilbar ist.

Warum reicht es bei Weg 2 aus, $k = 1, 2, \ldots, e-1$ zu probieren? Das kann man so sehen: Aus $d < m$ folgt $de < me$. Wenn wir $de = 1+km$ einsetzen, folgt $1+km < me$, also $km < me-1 < me$, somit $km < me$ und nach Kürzen durch m erhalten wir $k < e$.

Beispiel 3.17 (→CAS) Multiplikatives Inverses (Kehrwert) in $\mathbb{Z}_m$

a) Gibt es ein multiplikatives Inverses zu 4 in $\mathbb{Z}_9$? Geben Sie es gegebenenfalls an.
b) Für welche Zahlen aus $\mathbb{Z}_5$ gibt es ein multiplikatives Inverses? Geben Sie es gegebenenfalls an.
c) Für welche Zahlen aus $\mathbb{Z}_6$ gibt es ein multiplikatives Inverses? Geben Sie es gegebenenfalls an.

Lösung zu 3.17

a) Da 4 und 9 teilerfremd sind, gibt es zu 4 ein multiplikatives Inverses. Wir können es wie gewohnt als $\frac{1}{4}$ anschreiben, sind uns aber bewusst, dass damit eine Zahl aus $\mathbb{Z}_9$ gemeint ist. Wir finden $\frac{1}{4}$ durch systematisches Probieren einmal nach obigem Weg 1 und einmal zum Vergleich nach Weg 2:
• Weg 1: Wir suchen $d \in \mathbb{Z}_9$ mit

$$4 \cdot d = 1 \pmod 9.$$

$4 \cdot 1 = 4 \neq 1 \pmod 9$, $4 \cdot 2 = 8 \neq 1 \pmod 9$, $4 \cdot 3 = 12 = 3 \neq 1 \pmod 9$, $4 \cdot 4 = 16 = 7 \neq 1 \pmod 9$, $4 \cdot 5 = 20 = 2 \neq 1 \pmod 9$, $4 \cdot 6 = 24 = 6 \neq 1 \pmod 9$, $4 \cdot 7 = 28 = 1 \pmod 9$. Damit ist $\frac{1}{4} = 7$ in $\mathbb{Z}_9$.

• Weg 2: Wir suchen k mit $1 \leq k < 3$ (weil $e = 4$ und $k \leq e - 1$ sein wird) mit

$$\frac{1 + k \cdot 9}{4} \in \mathbb{N} :$$

$\frac{1+1\cdot 9}{4} \notin \mathbb{N}$, $\frac{1+2\cdot 9}{4} \notin \mathbb{N}$ aber $\frac{1+3\cdot 9}{4} = 7 \in \mathbb{N}$. Also ist $\frac{1}{4} = 7$ in $\mathbb{Z}_9$.

b) Für 0 gibt es niemals ein multiplikatives Inverses. Da $1, 2, 3, 4$ zum Modul 5 teilerfremd sind, gibt es für sie jeweils ein multiplikatives Inverses. Wir finden:

$$\frac{1}{1} = 1, \ \frac{1}{2} = \frac{1+5}{2} = 3, \ \frac{1}{3} = \frac{1+5}{3} = 2, \ \frac{1}{4} = \frac{1+3\cdot 5}{4} = 4.$$

c) Nur 1 und 5 haben einen Kehrwert, denn nur sie sind zum Modul teilerfremd:

$$\frac{1}{1} = 1, \ \frac{1}{5} = \frac{1+4\cdot 6}{5} = 5.$$

■

In der modularen Arithmetik muss bei Rechnungen darauf geachtet werden, dass es abgesehen von 0 je nach Modul noch weitere Zahlen geben kann, die keinen Kehrwert besitzen:

Beispiel 3.18 Multiplikatives Inverses (Kehrwert) in $\mathbb{Z}_m$
Ist die angegebene Aufgabenstellung sinnvoll? Wenn nein, begründen Sie! Wenn ja, berechnen Sie das Ergebnis in $\mathbb{Z}_{15}$:
a) $12 \cdot \frac{1}{6} \pmod{15}$ b) $12 \cdot \frac{1}{12} \pmod{15}$ c) $12 \cdot \frac{1}{7} \pmod{15}$ d) $12 \cdot \frac{1}{4} \pmod{15}$

Lösung zu 3.18 a) Da $\mathrm{ggT}(6, 15) \neq 1$, gibt es $\frac{1}{6}$ nicht in $\mathbb{Z}_{15}$, daher macht der Ausdruck $\frac{1}{6}$ keinen Sinn. (Es ist so, als ob wir beim Rechnen mit reellen Zahlen $\frac{1}{0}$ schreiben.)
b) Der Ausdruck $\frac{1}{12}$ macht keinen Sinn, weil $\mathrm{ggT}(12, 15) \neq 1$.
c) $12 \cdot \frac{1}{7} \pmod{15}$ macht Sinn, weil $\mathrm{ggT}(7, 15) = 1$, daher existiert $\frac{1}{7}$ in $\mathbb{Z}_{15}$. Wir berechnen $\frac{1}{7} = \frac{1+6\cdot 15}{7} = 13$, daher:

$$12 \cdot \frac{1}{7} = 12 \cdot 13 = 156 = 6 \pmod{15}.$$

d) $12 \cdot \frac{1}{4} \pmod{15}$ macht Sinn, weil $\mathrm{ggT}(4, 15) = 1$, daher existiert $\frac{1}{4}$ in $\mathbb{Z}_{15}$. Wir können $\frac{1}{4}$ (ohne es zu berechnen) mit dem Faktor 4 in 12 kürzen:

$$12 \cdot \frac{1}{4} = 3 \cdot 4 \cdot \frac{1}{4} = 3 \cdot 1 = 3 \pmod{15}.$$

Alternativ hätten wir auch zuerst $\frac{1}{4} = \frac{1+15}{4} = 4 \in \mathbb{Z}_{15}$ berechnen und dann $12 \cdot \frac{1}{4} = 12 \cdot 4 = 48 = 3 \pmod{15}$ rechnen können. ■

Wir haben das multiplikative Inverse von $e \in \mathbb{Z}_m$ (wenn es existiert) bisher nur durch Probieren gefunden und es ist leider nicht möglich, eine einfache Formel dafür anzugeben (wie für das additive Inverse in Satz 3.12). Wir werden zur effizienten Berechnung aber im nächsten Abschnitt den erweiterten Euklid'schen Algorithmus kennenlernen.

Zur Berechnung von Prüfziffern oder Entschlüsselungsvorschriften müssen Gleichungen gelöst werden.

Satz 3.19 (Lösung einer Gleichung) Seien a, b ganze Zahlen, m eine natürliche Zahl. Dann gilt:

a) $a + x = b \pmod m$ besitzt eine eindeutige Lösung x in $\mathbb{Z}_m$:

$$x = (-a) + b \pmod m.$$

Jede Zahl aus $\mathbb{Z}$, die sich von x um ein Vielfaches von m unterscheidet, ist ebenso eine Lösung.

b) Wenn a und m teilerfremd sind, dann besitzt $a \cdot x = b \pmod m$ eine eindeutige Lösung in $\mathbb{Z}_m$:

$$x = \frac{1}{a} \cdot b \pmod m.$$

Sind a und m jedoch nicht teilerfremd, so gilt:
- Ist $\mathrm{ggT}(a, m) = t > 1$ und t teilt b *nicht*, so gibt es keine Lösung.
- Ist $\mathrm{ggT}(a, m) = t > 1$ und t teilt b, so gibt es genau t Lösungen. Diese sind gegeben durch $x_j = x_0 + j\tilde{m}$, $0 \le j < t$, wobei x_0 die eindeutige Lösung ist von

$$\tilde{a} \cdot x = \tilde{b} \pmod{\tilde{m}} \qquad \text{mit} \qquad \tilde{a} = \frac{a}{t},\ \tilde{b} = \frac{b}{t},\ \tilde{m} = \frac{m}{t}.$$

Jede Zahl aus $\mathbb{Z}$, die sich von einer Lösung x um ein Vielfaches von m unterscheidet, ist ebenso eine Lösung.

Insbesondere darf man bei einer Gleichung der Form $c \cdot a \cdot x = c \cdot b \pmod m$ nur dann c auf beiden Seiten kürzen, wenn c teilerfremd zu m ist (und es daher den Kehrwert von c modulo m gibt). Ansonsten verliert man Lösungen (siehe Beispiel 3.20 e).

Satz 3.19 a) ist klar, denn wir subtrahieren auf beiden Seiten a (d.h. addieren das additive Inverse $-a$), wodurch nach x aufgelöst wird.
Satz 3.19 b) ist für den Fall, dass a und m teilerfremd sind, auch klar, denn dann gibt es $\frac{1}{a} \in \mathbb{Z}_m$ und man kann beide Seiten mit $\frac{1}{a}$ multiplizieren (d.h. durch a dividieren) und somit eindeutig nach x auflösen. Angenommen, es sind aber a und m nicht teilerfremd, also $t = \mathrm{ggT}(a, m) > 1$. Dann hängt es davon ab, ob t die rechte Seite b teilt. Denn ausgeschrieben lautet die Gleichung $a \cdot x = b + k \cdot m$. Gilt $a = t\tilde{a}$, $m = t\tilde{m}$, so folgt $t(\tilde{a} \cdot x - k \cdot \tilde{m}) = b$. Eine Lösung kann also nur existieren, falls $b = t\tilde{b}$. In diesem Fall können wir zunächst die eindeutige Lösung x_0 von

$\tilde{a} \cdot x = \tilde{b} \,(\mathrm{mod}\, \tilde{m})$ bestimmen. Die Lösungen unserer ursprünglichen Gleichung sind dann $x_0 + j\tilde{m}$, $0 \leq j < t$.

Beispiel 3.20 Gleichungen in $\mathbb{Z}_m$
Finden Sie alle $x \in \mathbb{Z}_m$, die die Gleichung lösen:
a) $4 + x = 3 \,(\mathrm{mod}\, 6)$ b) $5x = 2 \,(\mathrm{mod}\, 12)$ c) $3x = 6 \,(\mathrm{mod}\, 11)$
d) $2x = 3 \,(\mathrm{mod}\, 6)$ e) $18x = 24 \,(\mathrm{mod}\, 30)$

Lösung zu 3.20

a) Wir ziehen auf beiden Seiten 4 ab und wählen das Ergebnis so, dass es in $\mathbb{Z}_6$ liegt:
$$x = -4 + 3 = -1 = 5 \,(\mathrm{mod}\, 6).$$
Die eindeutige Lösung in $\mathbb{Z}_6$ ist also $x = 5$. (*Außerhalb* von $\mathbb{Z}_6$ ist jede zu $x = 5$ modulo 6 kongruente Zahl eine Lösung, zum Beispiel $11, 17, \ldots$ oder auch $-1, -7, \ldots$)

b) $a = 5$ und $m = 12$ sind teilerfremd, also gibt es $\frac{1}{5}$ in $\mathbb{Z}_{12}$. Wir multiplizieren beide Seiten der Gleichung damit und erhalten
$$x = \frac{1}{5} \cdot 2 = 5 \cdot 2 = 10 \,(\mathrm{mod}\, 12).$$
Hier haben wir $\frac{1}{5} = \frac{1+2\cdot 12}{5} = 5$ in $\mathbb{Z}_{12}$ verwendet.

c) $a = 3$ und $m = 11$ sind teilerfremd, daher existiert $\frac{1}{3}$ in Z_{11}:
$$x = 6 \cdot \frac{1}{3} = 2 \,(\mathrm{mod}\, 11).$$
Im letzten Schritt konnten wir, weil 6 Vielfaches von 3 ist, $6 \cdot \frac{1}{3} = 2 \cdot 3 \cdot \frac{1}{3} = 2$ rechnen, also durch 3 kürzen. (Alternativ hätte man natürlich auch $\frac{1}{3} = \frac{1+11}{3} = 4$ ermitteln und dann $x = 6 \cdot 4 = 24 = 2 \,(\mathrm{mod}\, 11)$ berechnen können.)

d) $a = 2$ und $m = 6$ sind nicht teilerfremd, ihr größter gemeinsamer Teiler ist $t = 2$. Da $t = 2$ kein Teiler von $b = 3$ ist gibt es nach Satz 3.19 keine Lösung.

e) Da nun $t = \mathrm{ggT}(18, 30) = 6$ die rechte Seite $b = 24$ teilt, gibt es nach Satz 3.19 insgesamt 6 Lösungen in $\mathbb{Z}_{30}$. Wir finden sie, indem wir zunächst $\tilde{a} \cdot x = \tilde{b} \,(\mathrm{mod}\, \tilde{m})$ lösen, also hier $3x = 4 \,(\mathrm{mod}\, 5)$. Damit ist die erste Lösung gleich $x_0 = \frac{1}{3} \cdot 4 = 2 \cdot 4 = 3$ und alle weiteren Lösungen erhalten wir durch Addition von Vielfachen von $\tilde{m}$ zu x_0: $x_1 = x_0 + 1 \cdot \tilde{m} = 3 + 5 = 8$; $x_2 = x_0 + 2 \cdot \tilde{m} = 3 + 2 \cdot 5 = 13$; weiters $x_3 = 18$, $x_4 = 23$ und $x_5 = 28$.

Bemerkung: Hätten wir hier zunächst beide Seiten der Gleichung durch 6 gekürzt (was nicht zulässig ist, da es den Kehrwert von 6 modulo 30 nicht gibt), so hätten wir $3 \cdot x = 4 \pmod{30}$ erhalten. Diese Gleichung hat aber keine Lösung.

■

Definition 3.21 Man bezeichnet die Menge der Zahlen aus $\mathbb{Z}_m$, für die es ein multiplikatives Inverses gibt, als

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \text{ggT}(a, m) = 1\}.$$

Die **Euler'sche Phi-Funktion** φ gibt die Anzahl der Elemente von $\mathbb{Z}_m^*$ an:

$$\varphi(m) = |\mathbb{Z}_m^*|.$$

Wenn insbesondere der Modul eine Primzahl p ist, dann hat jede Zahl aus $\mathbb{Z}_p$ außer 0 ein Inverses bezüglich der Multiplikation. Dann ist also

$$\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\} \qquad \text{und} \qquad \varphi(p) = p - 1.$$

Beispiel 3.22 $\mathbb{Z}_m$ **und** $\mathbb{Z}_m^*$
Geben Sie an: a) $\mathbb{Z}_4$ und $\mathbb{Z}_4^*$ b) $\mathbb{Z}_3$ und $\mathbb{Z}_3^*$

Lösung zu 3.22

a) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ sind alle möglichen Reste bei Division durch 4. Davon sind 1 und 3 teilerfremd zu 4. Also ist $\mathbb{Z}_4^* = \{1, 3\}$ und $\varphi(4) = 2$.

b) Es ist $\mathbb{Z}_3 = \{0, 1, 2\}$. Da 3 eine Primzahl ist, sind alle Zahlen in $\mathbb{Z}_3$ außer 0 teilerfremd zu 3, also $\mathbb{Z}_3^* = \{1, 2\}$ und $\varphi(3) = 2$.

■

Zur Berechnung von $\varphi(m)$ gibt es folgende Formel:

Satz 3.23 Sei $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ mit p_i prim, $k_i \in \mathbb{N}$ die Primfaktorzerlegung von $m \in \mathbb{N}$. Dann ist

$$\varphi(m) = \prod_{i=1}^{n} \left(p_i^{k_i} - p_i^{k_i - 1}\right).$$

Um diese Formel zu verstehen benötigt man, dass φ multiplikativ ist, d.h., es gilt $\varphi(m \cdot n) = \varphi(m)\varphi(n)$, falls m und n teilerfremd sind (warum das so ist, erfahren Sie am Ende von Abschnitt 3.4). Ist $m = p^k$ eine Primzahlpotenz, so sind alle Zahlen außer den Vielfachen von p, also $0, p, 2p, \ldots, p^{k-1}$, teilerfremd. Da das genau p^{k-1} Ausnahmen sind, folgt $\varphi(p^k) = p^k - p^{k-1}$. Anwendung auf die Primfaktorzerlegung liefert die besagte Formel.

Beispiel 3.24 Euler'sche Phi-Funktion
Berechnen Sie $\varphi(m)$ für
a) $m = 8$ b) $m = 1400$ c) $m = 37$

Lösung zu 3.24 a) $m = 8 = 2^3$, daher $\varphi(8) = 2^3 - 2^2 = 8 - 4 = 4$.
b) $m = 1400 = 2^3 \cdot 5^2 \cdot 7$; $\varphi(1400) = (2^3 - 2^2)(5^2 - 5^1)(7^1 - 7^0) = 4 \cdot 20 \cdot 6 = 480$.
c) $m = 37$ ist prim, daher $\varphi(37) = 37 - 1 = 36$. ■

Satz 3.25 (Satz von Euler) Für jede ganze Zahl a und jede dazu teilerfremde ganze Zahl m gilt

$$a^{\varphi(m)} = 1 \bmod m.$$

Der Beweis ist etwas trickreich, aber auch nicht schwer: Sei b das multiplikative Inverse von $a \in \mathbb{Z}_m^*$. Betrachten wir die Abbildung $f : \mathbb{Z}_m^* \to \mathbb{Z}_m^*$, die gegeben ist durch $f(x) = a \cdot x \pmod m$. Diese Abbildung ist umkehrbar, denn durch Multiplikation mit b erhält man wieder x zurück: $y = a \cdot x \pmod m \Leftrightarrow x = b \cdot y \pmod m$. Außerdem ist das Bild in $\mathbb{Z}_m^*$, da ja $(a \cdot x)^{-1} = bx^{-1}$ gilt. Jedes $x \in \mathbb{Z}_m^*$ wird durch f also auf genau ein $y \in \mathbb{Z}_m^*$ abgebildet. Bezeichnen wir mit $x_1, \ldots, x_{\varphi(m)}$ die Elemente von $\mathbb{Z}_m^*$, so sind die Elemente $y_1 = ax_1, \ldots, y_{\varphi(m)} = ax_{\varphi(m)}$ nur eine Umordnung. Wenn wir alle Zahlen in $\mathbb{Z}_m^*$ multiplizieren, so kommt es dabei auf die Reihenfolge nicht an, daher gilt

$$(ax_1) \cdot (ax_2) \cdot \ldots \cdot (ax_{\varphi(m)}) = x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} \pmod m.$$

Die linke Seite umgeformt liefert

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} = x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} \pmod m.$$

Multiplizieren wir nun der Reihe nach mit den multiplikativen Inversen von x_1, x_2, …, $x_{\varphi(m)}$, so bleibt am Ende $a^{\varphi(m)} = 1 \pmod m$ übrig.

Die Euler'sche Phi-Funktion liefert nicht die kleinste Zahl, für die Satz 3.25 gilt. Die kleinste Zahl ist Funktionswert der **Carmichael-Funktion** $\lambda(m)$ (nach dem US-amerikanischen Mathematiker Robert Carmichael, 1879–1967). In obigem Satz kann also $\varphi(m)$ durch $\lambda(m)$ ersetzt werden. Die Carmichael-Funktion ist etwas aufwendiger zu berechnen als die Euler'sche Phi-Funktion, es gilt aber immer $\lambda(m) \leq \varphi(m)$ und $\varphi(m)$ ist ein Vielfaches von $\lambda(m)$. Für teilerfremde Zahlen m und n gilt $\lambda(m \cdot n) = \text{kgV}(\lambda(m), \lambda(n))$. Insbesondere gilt für eine Primzahl p, dass $\lambda(p) = \varphi(p) = p - 1$ und für zwei verschiedene Primzahlen p, q, dass $\lambda(p \cdot q) = \text{kgV}(p - 1, q - 1)$.

Beispiel 3.26 Satz von Euler
Zeigen Sie die Aussage des Satzes von Euler für a) $n = 5$ b) $n = 6$.

Lösung zu 3.26

a) $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Damit ist $\varphi(5) = 4$.

a	$a^4 \pmod 5$
1	$1^4 = 1 (\mathrm{mod}\, 5)$
2	$2^4 = 16 = 1 (\mathrm{mod}\, 5)$
3	$3^4 = 9 \cdot 9 = 1 (\mathrm{mod}\, 5)$
4	$4^4 = 16 \cdot 16 = 1 (\mathrm{mod}\, 5)$

b) $\mathbb{Z}_6^* = \{1, 5\}$, also $\varphi(6) = 2$.

a	$a^2 \pmod 6$
1	$1^2 = 1 (\mathrm{mod}\, 6)$
5	$5^2 = 25 = 1 (\mathrm{mod}\, 6)$

■

Im Fall, dass $m = p$ eine Primzahl ist, folgt daraus

Satz 3.27 (Kleiner Satz von Fermat) Sei p eine Primzahl. Für jede Zahl $a \in \mathbb{Z}$, die teilerfremd zu p ist, gilt

$$a^{p-1} = 1 \pmod p.$$

Der kleine Satz von Fermat kann verwendet werden, um Potenzen mit großen Exponenten schneller zu berechnen:

Beispiel 3.28 Kleiner Satz von Fermat
Berechnen Sie:
a) $28^{40} \bmod 41$ b) $4^{1873} \bmod 11$

Lösung zu 3.28

a) $p = 41$ Primzahl, $\mathrm{ggT}(28, 41) = 1$, daher $28^{p-1} = 28^{40} = 1 \bmod 41$.

b) $p = 11$ Primzahl, $\mathrm{ggT}(4, 11) = 1$, daher $4^{p-1} = 4^{10} = 1 \bmod 11$. Somit:

$$4^{1873} = 4^{1870+3} = 4^{1870} 4^3 = 4^{187 \cdot 10} 4^3 = (4^{10})^{187} 4^3 = 1 \cdot 4^3 = 9 \bmod 11.$$

■

Wir haben gesehen, dass man in $\mathbb{Z}_m$ so wie in $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$ eine Addition und eine Multiplikation definieren kann. Es gibt aber auch Unterschiede: In $\mathbb{Z}_p$ mit p prim, $\mathbb{Q}$ oder $\mathbb{R}$ hat *jede* Zahl außer 0 ein multiplikatives Inverses, nicht aber in $\mathbb{Z}$ oder $\mathbb{Z}_m$ (wenn m keine Primzahl). Allgemein unterscheidet man verschiedene **algebraische Strukturen**, von denen wir vier erwähnen möchten:

Definition 3.29 Sei G eine Menge mit einer Verknüpfung, die je zwei Elementen $a, b \in G$ ein Element $a \circ b \in G$ zuordnet. Dann wird $(G, \circ)$ eine **Gruppe** genannt, wenn folgendes gilt:

a) Es gilt $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (**Assoziativgesetz**).
b) Es gibt ein **neutrales Element** $n \in G$, das $n \circ a = a \circ n = a$ für alle $a \in G$ erfüllt.
c) Zu jedem $a \in G$ gibt es ein **inverses Element** $i(a) \in G$, das $a \circ i(a) = i(a) \circ a = n$ erfüllt.

Gilt zusätzlich

d) $a \circ b = b \circ a$ für alle $a, b \in G$ (**Kommutativgesetz**),

so spricht man von einer **kommutativen** oder **abelschen Gruppe** (benannt nach dem norwegischen Mathematiker Niels Abel, 1802–1829).

Die Anzahl der Elemente in G wird **Ordnung** der Gruppe genannt und mit $|G|$ bezeichnet. Ist die Anzahl endlich, so spricht man von einer **endlichen Gruppe,** ansonsten von einer unendlichen Gruppe.

Man schreibt meistens nur kurz G (anstelle von $(G, \circ)$), wenn klar ist, welche Verknüpfung gemeint ist. Das neutrale Element und das inverse Element sind immer eindeutig bestimmt.

Warum? Sei n' ein weiteres neutrales Element, dann ist $n' = n \circ n' = n$. Sind b und c inverse Elemente zu a, so gilt $b = b \circ n = b \circ (a \circ c) = (b \circ a) \circ c = n \circ c = c$.

Außerdem folgt aus der Definition des Inversen sofort $i(i(a)) = a$, d.h. das Inverse des Inversen von a ist wieder a. Weiters gilt $i(a \circ b) = i(b) \circ i(a)$ (umgekehrte Reihenfolge!).

Eine Teilmenge $H \subseteq G$ heißt **Untergruppe** von G, wenn $(H, \circ)$ wieder eine Gruppe ist.

Satz 3.30 Um zu prüfen, ob $H \subseteq G$ eine Untergruppe ist, reicht es nachzuweisen, dass

- $n \in H$ ist und
- für alle $a, b \in H$ auch $a \circ b \in H$ (d.h., H **abgeschlossen bezüglich der Verknüpfung** $\circ$) ist und
- $i(a) \in H$ für alle $a \in H$ gilt.

Man braucht also das Assoziativgesetz (oder das Kommutativgesetz) nicht mehr zu prüfen, denn diese gelten automatisch in $H \subseteq G$, wenn sie in G gelten. Man sagt, sie werden von G **vererbt**.

Beispiel 3.31 **Additive Gruppen**

a) $(\mathbb{Z}, +)$, also die ganzen Zahlen $\mathbb{Z}$ mit der Addition, bilden eine kommutative Gruppe, denn:
• Das Assoziativgesetz gilt: $a + (b + c) = (a + b) + c$ für alle $a, b, c \in \mathbb{Z}$.
• Das neutrale Element bezüglich der Addition ist 0: $a + 0 = 0 + a = a$ für alle $a \in \mathbb{Z}$.
• Zu jedem $a \in \mathbb{Z}$ gibt es ein Inverses $-a$ bezüglich der Addition (additives Inverses): $a + (-a) = (-a) + a = 0$.
• Das Kommutativgesetz gilt: $a + b = b + a$ für alle $a, b \in \mathbb{Z}$.

b) Ebenso sind $(\mathbb{Z}_m, +)$ für beliebiges m, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ kommutative Gruppen. Die Gruppe $(\mathbb{Z}_m, +)$ ist endlich, mit $|\mathbb{Z}_m| = m$, die restlichen Gruppen sind unendlich.

c) $(\mathbb{N}_0, +)$ ist keine Gruppe: Assoziativgesetz wird von $\mathbb{Z}$ vererbt, neutrales Element 0 ist enhalten, aber es gibt nicht für jedes $a \in \mathbb{N}$ ein additives Inverses. Zum Beispiel gibt es keine *natürliche* Zahl a, sodass $3 + a = 0$.

d) Die geraden Zahlen $H = \{2n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ bilden eine Untergruppe $(H, +)$ von $(\mathbb{Z}, +)$.

Als Verknüpfung kann man auch die Multiplikation wählen:

Beispiel 3.32 **Multiplikative Gruppen**

a) $(\mathbb{Q}\backslash\{0\}, \cdot)$, bildet eine kommutative Gruppe, denn:
• Das Assoziativgesetz gilt: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle rationalen Zahlen $a, b, c \neq 0$.
• Das neutrale Element bezüglich der Multiplikation ist 1: $a \cdot 1 = 1 \cdot a = a$ für alle rationalen Zahlen $a \neq 0$.
• Zu jeder rationalen Zahl $a \neq 0$ gibt es ein Inverses bezüglich der Multiplikation (multiplikatives Inverses) $\frac{1}{a}$: $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$.
• Das Kommutativgesetz gilt: $a \cdot b = b \cdot a$ für alle rationalen Zahlen $a, b \neq 0$.

b) Ebenso sind $(\mathbb{Z}_m^*, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}\backslash\{0\}, \cdot)$ kommutative Gruppen. Die Gruppe $(\mathbb{Z}_m^*, \cdot)$ ist endlich, mit $|\mathbb{Z}_m^*| = \varphi(m)$, die restlichen Gruppen sind unendlich.

c) $(\mathbb{N}, \cdot)$ und auch $(\mathbb{Z}\backslash\{0\}, \cdot)$ sind keine Gruppen: Zwar wird das Assoziativgesetz von $\mathbb{Z}$ geerbt und das neutrale Element 1 ist enthalten, aber in $\mathbb{Z}\backslash\{0\}$ gibt es nicht für jedes a ein multiplikatives Inverses. Zum Beispiel gibt es keine *ganze Zahl* a, sodass $3 \cdot a = 1$.

Aus diesen letzten Beispielen sehen wir, dass $\mathbb{R}$ bezüglich der Addition sowie $\mathbb{R}\backslash\{0\}$ bezüglich der Multiplikation eine kommutative Gruppe bildet. Dasselbe gilt für $\mathbb{Q}$, $\mathbb{C}$ oder $\mathbb{Z}_p$. Daher haben $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ und $\mathbb{Z}_p$ dieselbe Struktur bzgl. Addition und Multiplikation, es gelten dafür dieselben Rechenregeln. Man nennt diese Struktur einen Körper:

Definition 3.33 Eine Menge $\mathbb{K}$ mit zwei Verknüpfungen $+$ und $\cdot$, geschrieben $(\mathbb{K}, +, \cdot)$, heißt **Körper** (engl. *field*), wenn folgendes gilt:

a) $(\mathbb{K}, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
b) $(\mathbb{K}\backslash\{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
c) Für alle $a, b, c \in \mathbb{K}$ gilt: $a \cdot b + a \cdot c = a \cdot (b + c)$ (**Distributivgesetz**).

(Das Distributivgesetz regelt, wie die beiden Verknüpfungen sich miteinander „vertragen“.)

Wieder schreibt man nur kurz $\mathbb{K}$ (anstelle von $(\mathbb{K}, +, \cdot)$), wenn klar ist, welche Verknüpfungen gemeint sind.

Beispiel 3.34 Körper

a) Für eine Primzahl p ist $\mathbb{Z}_p$ ein Körper. Ebenso sind $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ Körper.
b) Jedoch ist $\mathbb{Z}$ kein Körper, denn $(\mathbb{Z}\backslash\{0\}, \cdot)$ ist, wie wir in Beispiel 3.32 c) überlegt haben, keine Gruppe.

Hat nicht jedes Element ein multiplikatives Inverses, so wie z. B. in $\mathbb{Z}_m$, so spricht man von einem Ring:

Definition 3.35 Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, geschrieben $(R, +, \cdot)$, heißt **Ring**, wenn folgendes gilt:

a) $(R, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
b) Für alle $a, b, c \in R$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**Assoziativgesetz**).
c) Für alle $a, b, c \in R$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ (**Distributivgesetze**).

Gilt zusätzlich

d) das **Kommutativgesetz** $a \cdot b = b \cdot a$ für alle $a, b \in R$, so spricht man von einem kommutativen Ring, und wenn darüber hinaus
e) ein **neutrales Element** 1 **für die Multiplikation** existiert, also $a \cdot 1 = 1 \cdot a = a$ für alle $a \in R$,

so spricht man von einem **kommutativen Ring mit Eins**.

Wieder schreibt man kurz R (anstelle $(R, +, \cdot)$), wenn kein Zweifel besteht, welche Verknüpfungen gemeint sind. Wenn jedes Element (außer der 0) eines kommutativen Ringes mit Eins ein multiplikatives Inverses besitzt, dann ist der Ring ein Körper.

In einem Ring R mit Eins können wir nach der Existenz der multiplikativ inversen Elemente fragen. Man bezeichnet mit R^* die Menge aller Elemente aus R, die ein multiplikativ Inverses besitzen. Es ist mit Satz 3.30 einfach zu sehen, dass $(R^*, \cdot) \subseteq R$ eine Untergruppe von R bildet (neutrales Element 1 ist vorhanden und die inversen Elemente nach Definition von R auch; Abgeschlossenheit ist erfüllt, weil auch das Produkt von multitplikativ invertierbaren Zahlen wieder invertierbar ist: $(ab)^{-1} = b^{-1}a^{-1}$). Ein Element $a \in R$ heißt **Nullteiler**, wenn es ein $b \in R$ gibt mit $b \neq 0$, sodass $a \cdot b = 0$. Ist $a \in R^*$, so folgt aus $a \cdot b = 0$ sofort $b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$ und somit können Nullteiler kein multiplikatives Inverses besitzen.

In einem nullteilerfreien Ring gilt beim Lösen von Gleichungen die **Kürzungsregel**: Aus $a \cdot b = a \cdot c$ und $a \neq 0$ folgt $b = c$ (auch wenn a kein multiplikatives Inverses besitzt, mit dem wir beide Seiten multiplizieren können). In der Tat folgt aus $a \cdot b = a \cdot c$ sofort $a \cdot (b - c) = 0$ und da wir $a \neq 0$ vorausgesetzt haben, bleibt nur noch die Möglichkeit $b - c = 0$.

Beispiel 3.36 Ringe

a) Die ganzen Zahlen $\mathbb{Z}$ sind ein kommutativer Ring mit Eins; kein Körper, da es nicht zu jeder ganzen Zahl ein Inverses bezüglich der Multiplikation gibt (der Kehrwert ist ja im Allgemeinen keine ganze Zahl).

b) $\mathbb{Z}_m$ ist ein kommutativer Ring mit Eins; er ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist. So sind also z. B. $\mathbb{Z}_4$ oder $\mathbb{Z}_{256}$ nur Ringe, $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ hingegen Körper. Der einzige Nullteiler in $\mathbb{Z}_4$ ist 2, weil $2 \cdot 2 = 4 = 0$ in $\mathbb{Z}_4$. Die Nullteiler von $\mathbb{Z}_6$ sind 2 und 3, weil $2 \cdot 3 = 6 = 0$. Allgemein sind die Nullteiler in $\mathbb{Z}_m$ genau alle $a \in \mathbb{Z}_m$ mit $\mathrm{ggT}(a, m) \neq 1$.

c) Die Menge der Polynome $\mathbb{R}[x] = \{p(x) = p_n x^n + \cdots + p_1 x + p_0 \,|\, p_k \in \mathbb{R}\}$ ist ein kommutativer Ring mit Eins, aber kein Körper.

Denn: Die Addition und Multiplikation von Polynomen $p(x)+q(x)$ bzw. $p(x)\cdot q(x)$ erben das Kommutativ-, Assoziativ- und Distributivgesetz von den reellen Zahlen; neutrales Element bezüglich der Addition von Polynomen ist das Nullpolynom $p(x) = 0$; neutrales Element bezüglich der Multiplikation ist das konstante Polynom $p(x) = 1$; es gibt für jedes Polynom $p(x)$ ein Inverses bezüglich der Addition, nämlich $-p(x)$; es gibt aber nicht zu jedem Polynom ein Inverses bezüglich der Multiplikation: Zum Beispiel gibt es zu $p(x) = x^2$ keines, denn für kein Polynom $q(x)$ ist $x^2 \cdot q(x) = 1$ (das wäre $q(x) = \frac{1}{x^2}$, das ist aber kein Polynom). $\mathbb{R}[x]$ ist daher kein Körper.

d) Allgemein ist die Menge der Polynome $\mathbb{K}[x] = \{p(x) = p_n x^n + \cdots + p_1 x + p_0 \,|\, p_k \in \mathbb{K}\}$ mit Koeffizienten aus einem Körper $\mathbb{K}$ ein kommutativer Ring mit Eins, aber kein Körper. Zum Beispiel sind $\mathbb{C}[x]$ oder $\mathbb{Z}_2[x]$ Ringe, aber keine Körper. Die Menge $\mathbb{K}[x]$ wird als der **Polynomring** über $\mathbb{K}$ bezeichnet. In $\mathbb{K}[x]$ gibt es keine Nullteiler und man sagt auch $\mathbb{K}[x]$ ist nullteilerfrei.

Etwas allgemeiner kann man zu jedem Ring R den zugehörigen Polynomring $R[x]$ betrachten. $R[x]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist. Denn für zwei Polynome $p(x) = p_0 + \ldots + p_n x^n$ und $q(x) = q_0 + \ldots + q_m x^m$ mit $p_n, q_m \neq 0$ gilt $p(x)q(x) = p_0 q_0 + \ldots + p_n q_m x^{n+m}$.

Die Menge aller geraden Zahlen hat eine besondere Eigenschaft: Die Summe zweier gerader Zahlen ist gerade und die Multiplikation einer beliebigen Zahl mit einer geraden Zahl ist ebenfalls gerade. Teilmengen eines Rings mit dieser Eigenschaft haben einen eigenen Namen:

Definition 3.37 Eine Teilmenge I eines Rings R heißt **Ideal**, wenn gilt:

a) Es ist $0 \in I$ und für alle $a, b \in I$ sind $a + b \in I$ und $-a \in I$.

b) Für alle $a \in I$ und $b \in R$ sind $a \cdot b \in I$ und $b \cdot a \in I$.

Ein Ideal $I \subseteq R$ ist also nach Satz 3.30 eine Untergruppe bezüglich der Addition und jedes Vielfache eines Elementes aus I liegt wieder in I.

Beispiel 3.38 Ideale

a) Alle geraden Zahlen bilden ein Ideal in $\mathbb{Z}$.

b) Alle Polynome $p(x)$, für die $p(0) = 0$ ist, bilden ein Ideal in $\mathbb{R}[x]$.

Diese Überlegungen und Definitionen erscheinen Ihnen vielleicht auf den ersten Blick als abstrakt und nutzlos. Es trifft aber das Gegenteil zu! Sie bilden die Basis für viele Anwendungen in der Kryptographie und der Codierungstheorie und sind damit von fundamentaler Bedeutung für die Informatik.

Zum Schluss erwähnen wir noch den Begriff der **Isomorphie**: Zwei mathematische Strukturen nennt man isomorph, wenn sie sich nur durch die Benennung ihrer Elemente unterscheiden. Konkret bedeutet das, dass zwei Gruppen $(G_1, \circ_1)$ und $(G_2, \circ_2)$ isomorph sind, wenn es eine umkehrbar eindeutige Abbildung $\psi : G_1 \to G_2$ (also jedem Element aus G_1 wird genau ein Element aus G_2 zugeordnet und umgekehrt) gibt, die mit den Gruppenverknüpfungen **verträglich** ist, d.h. $\psi(a \circ_1 b) = \psi(a) \circ_2 \psi(b)$ für alle $a, b \in G_1$. Es folgt dann automatisch $\psi(n_1) = n_2$ für die neutralen Elemente $n_1 \in G_1$, $n_2 \in G_2$ und $\psi(i_1(a)) = i_2(\psi(a))$ für das Inverse von a in G_1 bzw. von $\psi(a)$ in G_2. Analoges gilt für Ringe und Körper, nur dass in diesem Fall sowohl die Addition als auch die Multiplikation erhalten werden muss.

Die Abbildung ψ wird als **Isomorphismus** bezeichnet und speziell im Fall $G_1 = G_2$ auch als **Automorphismus**. Ist die Abbildung ψ nicht umkehrbar, so spricht man von einem **Homomorphismus**.

Beispiel 3.39 Isomorphe Gruppen

Gegeben sind die beiden Gruppen $(G_1, \circ_1)$ und $(G_2, \circ_2)$ mit $G_1 = \{0, 1, 2\}$ und $G_2 = \{a, b, c\}$ und den Verknüpfungstabellen:

$\circ_1$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\circ_2$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Die Gruppen sind isomorph, wie aus den Tabellen ersichtlich. Denn wenn man die linke Tabelle anhand von $\psi(0) = b$, $\psi(1) = a$, $\psi(2) = c$ umbenennt, dann erhält man genau die rechte.

Nach diesem kurzen Ausflug in die **Zahlentheorie**, die sich mit den Eigenschaften der ganzen Zahlen beschäftigt, möchten wir noch einen kleinen Überblick über einige wichtige Teilgebiete der Mathematik geben: Die **Algebra** untersucht Gruppen, Ringe und Körper, im Gegensatz zur **Analysis**, die sich mit Differential- und Integralrechnung beschäftigt. Die **lineare Algebra** untersucht Vektorräume (z. B. $\mathbb{R}^n$) und verschmilzt im unendlichdimensionalen Fall von Funktionenräumen mit der Analysis zur **Funktionalanalysis**. Die **algebraische Geometrie** verwendet kommutative Ringe, um geometrische Objekte (also Kurven, Flächen, etc.) mit algebraischen Methoden zu untersuchen.

Die Menge aller Funktionen (mit bestimmten Eigenschaften), die auf einem geometrischen Objekt definiert sind, bilden nämlich auch einen Ring, der wichtige Informationen über die Geometrie enthält.

Untersucht man geometrische Objekte mit den Methoden der Analysis, so ist man in der **Differentialgeometrie**. Die **diskrete Mathematik**, einer unserer Schwerpunkte, befasst sich mit mathematischen Strukturen, die endlich oder abzählbar unendlich sind. Sie ist ein junges Gebiet mit vielen Bezügen zur Informatik, da Computer von Natur aus diskret arbeiten.

3.2.1 Anwendung: Welche Fehler erkennen Prüfziffern?

Im letzten Abschnitt haben wir gesehen, wie modulare Arithmetik für Prüfziffern verwendet werden kann. Eine gute Prüfziffer sollte die häufigsten Fehler erkennen, und das sind:

- Eingabe einer falschen Ziffer („Einzelfehler“)
- Vertauschung zweier Ziffern („Vertauschungsfehler“)

Wir wollen nun eine gute Prüfziffer konstruieren: Angenommen, die mit einer Prüfziffer zu versehende Ziffernfolge hat n Stellen, $x_1 \ldots x_n$. Ein allgemeiner Ansatz für die Prüfziffer wäre

$$P(x_1 \ldots x_n) = \sum_{j=1}^{n} g_j x_j \bmod q = g_1 x_1 + \ldots + g_n x_n \bmod q.$$

Dabei sind die Zahlen $g_j \in \mathbb{Z}_q$ beliebige Gewichte, die noch geeignet zu bestimmen sind. Welchen Wert soll der Modul q haben? Die Größe von q legt unseren Vorrat an Ziffern fest: $x_j \in \{0, 1, \ldots, q-1\} = \mathbb{Z}_q$.

Ist zum Beispiel $q = 9$, so könnten wir nur die Ziffern $\{0, 1, \ldots, 8\}$ verwenden. Denn würden wir bei $q = 9$ zum Beispiel auch die Ziffer 9 zulassen, so könnte zwischen den Ziffern 0 und 9

nicht unterschieden werden, da $9 = 0 \pmod 9$. Eine falsche Eingabe von 9 statt 0 würde von der Prüfziffer also nicht erkannt werden.

Wenn wir also jedenfalls die Ziffern $0, 1, \ldots, 9$ verwenden möchten, so muss q zumindest gleich 10 sein.

Überlegen wir als Nächstes, welche Eigenschaften die Prüfziffer haben muss, damit sie Einzel- bzw. Vertauschungsfehler immer erkennt. Beginnen wir mit dem Einzelfehler. Nehmen wir an, es wird anstelle von $x_1 \ldots x_n$ die Ziffernfolge $y_1 \ldots y_n$ eingegeben, wobei ein Fehler in der k-ten Stelle aufgetreten ist. Das heißt, es gilt $x_j = y_j$ für alle $j \neq k$ und $x_k \neq y_k$. Dann ist die Differenz der Prüfziffern

$$P(x_1 \ldots x_n) - P(y_1 \ldots y_n) = g_k(x_k - y_k) \bmod q.$$

Der Fehler wird erkannt, wenn die Differenz der Prüfziffern ungleich 0 ist. Damit ein Einzelfehler also immer erkannt wird, darf diese Differenz nur dann gleich 0 (modulo q) sein, wenn $x_k = y_k$. Die Gleichung $g_k(x_k - y_k) = 0 \pmod q$ muss also eine eindeutige Lösung, nämlich $x_k - y_k = 0 \pmod q$ haben. Nach Satz 3.19 b) ist das genau dann der Fall, wenn $g_k \in \mathbb{Z}_q^*$ (d.h., wenn g_k ein multiplikatives Inverses besitzt).

Kommen wir nun zur Erkennung von Vertauschungsfehlern: Nehmen wir an, es wird anstelle von $x_1 \ldots x_n$ die Ziffernfolge $y_1 \ldots y_n$ eingegeben, wobei die j-te und die k-te Stelle vertauscht wurden. Dann ist die Differenz der Prüfziffern

$$P(x_1 \ldots x_n) - P(y_1 \ldots y_n) = g_j x_j + g_k x_k - g_j x_k - g_k x_j = (g_j - g_k)(x_j - x_k) \bmod q.$$

Analog wie zuvor muss $g_j - g_k \in \mathbb{Z}_q^*$ gelten, damit der Fehler immer erkannt wird.

Satz 3.40 (Erkennung von Einzel- und Vertauschungsfehlern) Sei

$$P(x_1 \ldots x_n) = \sum_{j=1}^{n} g_j x_j \bmod q$$

eine Prüfziffer für eine Ziffernfolge $x_1 \ldots x_n$ mit Ziffern $x_j \in \mathbb{Z}_q$. Dann erkennt P genau dann alle Einzelfehler an der Stelle k, wenn $g_k \in \mathbb{Z}_q^*$, und genau dann alle Vertauschungsfehler an den Stellen j und k, wenn $(g_j - g_k) \in \mathbb{Z}_q^*$.

Eine besonders gute Wahl für q ist also eine Primzahl, denn dann ist $\mathbb{Z}_q^*$ besonders groß!

Leider ergibt sich nun ein kleines Dilemma: Wählen wir $q = 10$, so stehen für die Gewichte die Zahlen in $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ zur Verfügung, wenn alle Einzelfehler erkannt werden sollen. Da die Differenz zweier ungerader Zahlen aber gerade ist, können dann nicht mehr *alle* Vertauschungsfehler erkannt werden. Wählen wir $q = 11$ (Primzahl), so lassen sich die Bedingungen für die Erkennung aller Vertauschungs- und Einzelfehler erfüllen, aber dafür kann die Prüfziffer auch den Wert 10 haben, ist also nicht immer eine einstellige Dezimalziffer.

Zum Abschluss eine kleine Auswahl an Prüfzifferverfahren:

- Auf vielen Artikeln findet sich ein Strichcode bzw. die zugehörige 13-stellige oder 8-stellige Ziffernfolge, die **Europäische Artikelnummer (EAN)**. Mithilfe von Scannern wird der Strichcode an Computerkassen eingelesen. Bei der 13-stelligen Nummer *abcd efgh ikmn p* geben die beiden ersten Ziffern das Herkunftsland an, die folgenden 5 Ziffern stehen für den Hersteller, und die nächsten 5 Ziffern für das Produkt. Die letzte Ziffer p ist eine Prüfziffer, die

$$a + 3b + c + 3d + e + 3f + g + 3h + i + 3k + m + 3n + p = 0 \bmod 10.$$

  erfüllt. Es werden alle Einzelfehler erkannt (da die Gewichte 1 bzw. 3 aus $\mathbb{Z}_{10}^*$ sind), aber nicht alle Vertauschungsfehler. Auch die **internationale Buchnummer ISBN-13** ist auf diese Weise definiert und somit kompatibel mit der EAN (siehe auch Beispiel 3.7)

- Bei Banken wird das **Einheitliche Kontonummernsystem (EKONS)** verwendet. Die Kontonummern sind maximal zehnstellig: Die ersten (maximal 4) Ziffern stehen für die Klassifikation der Konten und die restlichen 6 Ziffern bilden die eigentliche Kontonummer, wobei die letzte Ziffer eine Prüfziffer ist. Es sind bei verschiedenen Banken verschiedene Prüfzifferverfahren üblich. Die Prüfziffer p der Kontonummer *abcd efghi p* berechnet sich zum Beispiel nach der Vorschrift

$$2i + h + 2g + f + 2e + d + 2c + b + 2a + p = 0 \bmod 10.$$

  Es werden nicht alle Einzelfehler erkannt (da das Gewicht 2 nicht in $\mathbb{Z}_{10}^*$ liegt), aber alle Vertauschungsfehler benachbarter Ziffern, da die Differenz der zugehörigen Gewichte, 1, in $\mathbb{Z}_{10}^*$ liegt.

- Die inzwischen durch die dreizehnstellige ISBN-13 abgelöste zehnstellige **Internationale Standard-Buchnummer (ISBN-10)** hat die Form *a bcd efghi p*. Dabei ist a das Herkunftsland, *bcd* kennzeichnet den Verlag und p ist die Prüfziffer, die

$$10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i + p = 0 \bmod 11$$

  erfüllt. Anstelle von 10 wird das Symbol X verwendet. Da alle Gewichte und auch die Differenzen von je zwei Gewichten in $\mathbb{Z}_{11}^*$ liegen, werden alle Einzelfehler und alle Vertauschungsfehler erkannt.

- Die **Internationale Bankkontonummer (IBAN)** setzt sich aus einer zweistelligen Länderkennung (z.B. AT, CH, DE), einer zweistelligen Prüfziffer und einer maximal 30-stelligen Kontoidentifikation (Bankleitzahl und Kontonummer) zusammen. Zur Validierung verwendet man die Umordung

„Kontoidentifikation, Länderkennung, Prüfziffer“ und wandelt alle Buchstaben in Ziffern um ('A'=10, 'B'=11, ..., 'Z'=35). Der Rest dieser Zahl modulo 97 muss 1 sein.

Die Gewichte sind in diesem Fall $g_j = 10^j$ (Dezimaldarstellung) und da 97 eine Primzahl ist, die weder g_j noch $g_j - g_k$ teilt (zumindest für $0 \leq j < k \leq 95$), werden alle Einzel- und alle Vertauschungsfehler von Ziffern erkannt. Um Fehler bei Buchstaben zu erkennen, müssen wir je zwei Ziffern zusammenfassen, sodass die *Ziffern* nun zweistellige Zahlen und die Gewichte $g_j = 100^j$ sind. Dann können wir immer noch alle Einzelfehler und alle Vertauschungsfehler erkennen (zumindest für $0 \leq j < k \leq 47$), solange die Differenz der Ziffern kein Vielfaches von 97 ist, was bei Buchstaben auf jeden Fall erfüllt ist.

Beispiel 3.41 Prüfziffer

a) Anstelle der EAN 72*cd efgh ikmn p* wird die EAN 27*cd efgh ikmn p* eingegeben, es wurden also die ersten beiden Ziffern vertauscht. Erkennt die Prüfziffer diesen Fehler?

b) Anstelle der EAN 26*cd efgh ikmn p* wird nun die EAN 62*cd efgh ikmn p* eingegeben, es wurden also wieder die ersten beiden Ziffern vertauscht. Erkennt die Prüfziffer diesen Fehler?

Lösung zu 3.41

a) Um uns auf das Wesentliche konzentrieren zu können, betrachten wir nur den Beitrag der ersten beiden Stellen zur Prüfziffer (die weiteren Stellen sind in beiden EANs gleich und geben daher den gleichen Beitrag zur Prüfziffer). In der ersten EAN erhalten wir aus den ersten beiden Stellen

$$1 \cdot 7 + 3 \cdot 2 = 13 = 3 \bmod 10,$$

und bei der zweiten EAN ergibt sich ebenfalls

$$1 \cdot 2 + 3 \cdot 7 = 23 = 3 \bmod 10.$$

Dieser Vertauschungsfehler wird also nicht erkannt.

b) In der ersten EAN erhalten wir nun aus den ersten beiden Stellen

$$2 + 3 \cdot 6 = 20 = 0 \bmod 10,$$

die zweite EAN liefert

$$6 + 3 \cdot 2 = 12 = 2 \bmod 10.$$

Dieser Vertauschungsfehler wird also erkannt. ■

3.3 Der Euklid'sche Algorithmus

Das multiplikative Inverse in $\mathbb{Z}_m$ kann für kleines m leicht durch Probieren gefunden werden. In praktischen Anwendungen, z. B. in der Kryptographie, hat man es aber oft mit großen Zahlen zu tun und benötigt daher ein besseres Verfahren. Wir beginnen mit einem effektiven Verfahren für die Bestimmung des größten gemeinsamen Teilers und werden sehen, dass wir damit gleichzeitig auch den gewünschten Algorithmus für das multiplikative Inverse erhalten.

Die einfachste Möglichkeit, um zum Beispiel den $\mathrm{ggT}(217, 63)$ zu finden, ist alle Zahlen von 1 bis 63 durchzuprobieren. Das ist allerdings ein sehr mühsames Verfahren und bereits der griechische Mathematiker Euklid (ca. 300 v. Chr.) hatte eine bessere Idee:

Dividieren wir zunächst 217, die größere der beiden Zahlen, durch 63, die kleinere der beiden:

$$217 = 3 \cdot 63 + 28.$$

Jeder gemeinsame Teiler von 217 und 63 muss auch $28 = 217 - 3 \cdot 63$ teilen.

Denn wenn t ein gemeinsamer Teiler von 217 und 63 ist, also $217 = kt$ und $63 = nt$, so folgt: $28 = 217 - 3 \cdot 63 = kt - 3 \cdot nt = t(k - 3n)$, also ist t auch ein Teiler von 28.

Analog muss jeder gemeinsame Teiler von 63 und 28 auch ein Teiler von $217 = 3 \cdot 63 + 28$ sein. Daher ist insbesondere der größte gemeinsame Teiler von 217 und 63 gleich dem größten gemeinsamen Teiler von 63 und 28. Das Problem, den $\mathrm{ggT}(217, 63)$ zu finden, reduziert sich also auf das Problem, den $\mathrm{ggT}(63, 28)$ zu finden! Als nächstes dividieren wir daher 63 durch 28,

$$63 = 2 \cdot 28 + 7.$$

Mit derselben Überlegung wie oben folgt, dass $\mathrm{ggT}(63, 28) = \mathrm{ggT}(28, 7)$. Wir dividieren nun nochmal:

$$28 = 4 \cdot 7 + 0.$$

Da 7 ein Teiler von 28 ist, ist $\mathrm{ggT}(28, 7) = 7$, und damit ist $7 = \mathrm{ggT}(28, 7) = \mathrm{ggT}(63, 28) = \mathrm{ggT}(217, 63)$ und das Problem ist gelöst!

Euklid hat den Algorithmus in seinem Werk, den *Elementen* beschrieben. Die *Elemente* bestehen aus 13 Bänden, ein Teil davon sind Euklids eigene Arbeiten, der Rest ist eine Sammlung des mathematischen Wissens der damaligen Zeit. Die *Elemente* sind eines der erfolgreichsten Lehrwerke aller Zeiten und waren bis ins 19. Jahrhundert das meistverkaufte Werk nach der Bibel.

Satz 3.42 (Euklid'scher Algorithmus) Die natürlichen Zahlen a, b seien gegeben. Setzt man $r_0 = a$, $r_1 = b$ und definiert man für $k \geq 2$ rekursiv r_k als Rest der Division von r_{k-2} durch r_{k-1},

$$r_k = r_{k-2} \bmod r_{k-1} \qquad (\text{also } r_{k-2} = q_k r_{k-1} + r_k \text{ mit } q_k \in \mathbb{Z}),$$

so bricht diese Rekursion irgendwann ab, d.h. $r_{n+1} = 0$, und es gilt $r_n = \text{ggT}(a, b)$. Also

$$\begin{aligned} r_0 &= q_2 r_1 + r_2, \qquad 0 < r_2 < r_1, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n, \end{aligned}$$

mit $r_n = \text{ggT}(a, b)$. Der letzte nichtverschwindende Rest ist also der größte gemeinsame Teiler.

Da $r_1 = b$ ist und r_k in jedem Schritt abnimmt, bricht der Algorithmus nach spätestens b Schritten ab.

Es ist übrigens sinnvoll (aber nicht notwendig), $a > b$ zu wählen. Tut man das nicht, so tauschen im ersten Schritt des Algorithmus a und b Platz, man muss also einen Schritt mehr im Vergleich zum Fall $a > b$ ausführen.

Beispiel 3.43 (→CAS) Euklid'scher Algorithmus
Bestimmen Sie den $\text{ggT}(a, b)$ für
a) $a = 39, b = 17$ b) $a = 204, b = 140$ c) $a = 75, b = 38$

Lösung zu 3.43 a) Wir setzen $r_0 = 39$ (die größere der beiden Zahlen) und $r_1 = 17$ und führen Division mit Rest $r_{k-2} = q_k r_{k-1} + r_k$ für $k \geq 2$ so lange durch, bis sich Rest 0 ergibt:

$$\begin{aligned} 39 &= 2 \cdot 17 + 5 \\ 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Der letzte Rest ungleich 0 ist $r_4 = 1 = \text{ggT}(39, 17)$. Die beiden Zahlen sind also teilerfremd.
b) Wir setzen $r_0 = 204$ und $r_1 = 140$ und führen wieder Division mit Rest durch, bis sich Rest 0 ergibt:

$$\begin{aligned} 204 &= 1 \cdot 140 + 64 \\ 140 &= 2 \cdot 64 + 12 \\ 64 &= 5 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

Der letzte Rest ungleich 0 ist $4 = \text{ggT}(204, 140)$.
c)

$$\begin{aligned} 75 &= 1 \cdot 38 + 37 \\ 38 &= 1 \cdot 37 + 1 \\ 37 &= 37 \cdot 1 + 0 \end{aligned}$$

Der letzte Rest ungleich 0 ist $1 = \text{ggT}(75, 38)$.

■

Wenn man den Euklid'schen Algorithmus etwas erweitert, so kann er auch verwendet werden um das multiplikative Inverse zu berechnen:

Beispiel 3.44 (→CAS) Berechnung des multiplikativen Inversen
Berechnen Sie das multiplikative Inverse von 17 modulo 39 mithilfe des erweiterten Euklid'schen Algorithmus.

Lösung zu 3.44 Wir haben den Euklid'schen Algorithmus zur Bestimmung des $\text{ggT}(39, 17)$ schon im Beispiel 3.43 ausgeführt. Unser Ziel ist nun, den $\text{ggT}(39, 17)$, also 1, in der Form $1 = 39 \cdot x + 17 \cdot y$ mit ganzen Zahlen x, y auszudrücken. Dann ist y das gesuchte multiplikative Inverse (warum das so ist, sehen wir gleich).

Wir schreiben uns nun die einzelnen Zeilen aus Beispiel 3.43 nochmals auf, diesmal aber nach den Resten aufgelöst (die letzte, triviale Zeile benötigen wir nicht):

$$\begin{aligned} 5 &= 39 - 2 \cdot 17 \\ 2 &= 17 - 3 \cdot 5 \\ 1 &= 5 - 2 \cdot 2 \end{aligned}$$

Die erste Zeile hat die Form 5 = „Vielfaches von 39 plus Vielfaches von 17“ und wird nicht mehr verändert. Nun verwenden wir die erste Zeile, um auch die zweite in die Form „Vielfaches von 39 plus Vielfaches von 17“ zu bringen:

$$2 = 17 - 3 \cdot \boxed{5} = 17 - 3 \cdot (\boxed{39 - 2 \cdot 17}) = 17 - 3 \cdot 39 + 6 \cdot 17 = \boxed{-3 \cdot 39 + 7 \cdot 17}.$$

Nun ist auch die zweite Zeile fertig. Jetzt setzen wir in der dritten Zeile für 5 bzw. 2 aus der ersten bzw. zweiten Zeile ein, um auch die dritte Zeile in die Form „Vielfaches von 39 plus Vielfaches von 17“ zu bringen:

$$1 = \boxed{5} - 2 \cdot \boxed{2} = \boxed{39 - 2 \cdot 17} - 2 \cdot (\boxed{17 - 3 \cdot 5}) = 7 \cdot 39 - 16 \cdot 17.$$

Nun bedeutet aber $1 = 7 \cdot 39 - 16 \cdot 17$, dass sich 1 und $(-16) \cdot 17$ um ein Vielfaches von 39 unterscheiden, mit anderen Worten,

$$(-16) \cdot 17 = 1 \,(\text{mod}\, 39).$$

Wir ersetzen -16 noch durch den Rest modulo 39 und erhalten

$$23 \cdot 17 = 1 \,(\mathrm{mod}\, 39).$$

Somit ist 23 das gesuchte multiplikative Inverse zu 17 in $\mathbb{Z}_{39}$, d.h. $\frac{1}{17} = 23$ in $\mathbb{Z}_{39}$. Probe: $17 \cdot 23 = 391 = 1 \,(\mathrm{mod}\, 39)$. ■

Das im letzten Beispiel beschriebene Vorgehen kann als Algorithmus formuliert werden, der das etwas allgemeinere Problem löst, zwei ganze Zahlen x und y zu finden, die $ax + by = \mathrm{ggT}(a, b)$ erfüllen.

Wenn wir die Gleichung $a = q_2 b + r_2$ nach r_2 auflösen, so erhalten wir eine Darstellung $r_2 = ax_2 + by_2$ mit $x_2 = 1$ und $y_2 = -q_2$. Analog können wir auch alle folgenden Gleichungen $r_{k-2} = q_k r_{k-1} + r_k$ nach r_k auflösen und erhalten durch Einsetzen der entsprechenden Darstellungen der vorhergehenden Reste $r_k = r_{k-2} - q_k r_{k-1} = (x_{k-2}a + y_{k-2}b) - q_k(x_{k-1}a + y_{k-1}b) = x_k a + y_k b$ mit $x_k = x_{k-2} - q_k x_{k-1}$ und $y_k = y_{k-2} - q_k y_{k-1}$. Wir können also rekursiv Zahlenpaare x_k, y_k berechnen und bricht der Algorithmus bei $r_n = \mathrm{ggT}(a, b)$ ab, so haben wir eine Lösung $ax_n + by_n = \mathrm{ggT}(a, b)$ gefunden.

Satz 3.45 (Erweiterter Euklid'scher Algorithmus) Gegeben ist die Gleichung

$$ax + by = \mathrm{ggT}(a, b)$$

mit beliebigen natürlichen Zahlen a und b. Eine ganzzahlige Lösung x, y kann mithilfe des erweiterten Euklid'schen Algorithmus rekursiv berechnet werden. Dazu wird der Euklid'sche Algorithmus wie in Satz 3.42 beschrieben durchgeführt, zusätzlich werden noch in jedem Schritt Zahlen x_k und y_k berechnet, mit den Anfangswerten $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$:

$$\begin{aligned} r_k &= r_{k-2} \bmod r_{k-1}, \quad & q_k &= r_{k-2} \operatorname{div} r_{k-1}, \qquad & (\text{also } r_{k-2} = q_k r_{k-1} + r_k) \\ x_k &= x_{k-2} - q_k x_{k-1}, \quad & y_k &= y_{k-2} - q_k y_{k-1}. \end{aligned}$$

Die Abbruchbedingung ist wieder $r_{n+1} = 0$. Für $r_n = \mathrm{ggT}(a, b)$ und das zugehörige x_n bzw. y_n gilt dann: $x_n a + y_n b = \mathrm{ggT}(a, b)$. Daher haben wir mit $x = x_n$ und $y = y_n$ eine Lösung der gegebenen Gleichung gefunden.

Wir halten also fest, dass der erweiterte Euklid'sche Algorithmus verwendet werden kann, um das multiplikative Inverse einer Zahl e modulo m zu berechnen:

Satz 3.46 (Berechnung des multiplikativen Inversen) Seien e und m teilerfremde natürliche Zahlen. Dann ist die Lösung $y \in \mathbb{Z}_m$ der Gleichung

$$m\, x + e\, y = 1$$

(die zum Beispiel mit dem erweiterten Euklid'schen Algorithmus berechnet wird), das multiplikative Inverse $\frac{1}{e}$ in $\mathbb{Z}_m$.

Falls der erweiterte Euklid'sche Algorithmus ein y liefert, das nicht in $\mathbb{Z}_m$ liegt, so muss noch der Rest von y modulo m aufgesucht werden. Der zweite Teil der Lösung (x), die der erweiterte Euklid'sche Algorithmus liefert, wird für die Berechnung des multiplikativen Inversen nicht gebraucht.

Warum ist x das gesuchte multiplikative Inverse? Nun, y erfüllt ja $m\,x + e\,y = 1$, oder etwas umgeformt: $e\,y = 1 - m\,x$. Das bedeutet aber, dass sich $e\,y$ und 1 nur um ein Vielfaches von m unterscheiden, und das bedeutet nichts anderes als $e\,y = 1 \pmod m$.

Beispiel 3.47 (→CAS) Berechnung des multiplikativen Inversen mithilfe des erweiterten Euklid'schen Algorithmus (Formeln)
Berechnen Sie das multiplikative Inverse von 17 modulo 39 mithilfe des erweiterten Euklid'schen Algorithmus, indem Sie die Formeln aus Satz 3.45 anwenden.

Lösung zu 3.47 Wir setzen die bereits bekannten Werte für q_k aus Beispiel 3.43 a) und die Startwerte $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$ ein:

$$\begin{aligned} x_2 &= x_0 - q_2 \cdot x_1 = 1 - 2 \cdot 0 = 1 \\ x_3 &= x_1 - q_3 \cdot x_2 = 0 - 3 \cdot 1 = -3 \\ x_4 &= x_2 - q_4 \cdot x_3 = 1 - 2 \cdot (-3) = 7 \end{aligned}$$

bzw.

k	q_k	$x_k = x_{k-2} - q_k x_{k-1}$	$y_k = y_{k-2} - q_k y_{k-1}$
0	-	1	0
1	-	0	1
2	2	1	-2
3	3	-3	7
4	2	7	-16

■

Diophantische Gleichungen

Der erweiterte Eukild'sche Algorithmus zeigt uns, wie eine ganzzahlige Lösung einer Gleichung der Form $ax+by = \mathrm{ggT}(a,b)$ gefunden werden kann. Eine Gleichung, bei der nur *ganzzahlige* Lösungen gesucht werden, bezeichnet man als **diophantische Gleichung**, benannt nach dem griechischen Mathematiker Diophant von Alexandrien (ca. 250 v. Chr.). Ursprünglich wurde der Algorithmus übrigens verwendet um diophantische Gleichungen aus der Astronomie zu lösen und genaue Kalender zu erstellen.

Die wohl bekannteste diophantische Gleichung ist $x^n + y^n = z^n$. Der Fall $n = 2$ entspricht dem Satz von Pythagoras und eine Lösung ist zum Beispiel $x = 3$, $y = 4$ und $z = 5$: $3^2 + 4^2 = 5^2$. Der französische Mathematiker Pierre de Fermat (1607–1665) hat die Behauptung aufgestellt, dass diese Gleichung für natürliches $n > 2$ keine Lösungen mit ganzzahligen x, y und z besitzt; dass es also z. B. keine ganzen Zahlen x, y, z gibt, die $x^3 + y^3 = z^3$ erfüllen. Fermat ist auf diese Vermutung beim Studium eines Bandes von Diophants Lehrwerk, der *Arithmetica* gekommen, und hat am Rand einer Seite vermerkt: „Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist dieser Rand hier zu schmal, um ihn zu fassen." Diese Notiz hat Generationen von Mathematiker:innen und Mathematik-Begeisterten den Schlaf geraubt, und für den Beweis von Fermats Behauptung wurden viele Preise ausgesetzt. Er wurde erst 1995 erbracht und umfasst Hunderte von Seiten ... Mehr zur spannenden Geschichte von „Fermats letzter Satz" finden Sie im gleichnamigen Buch von S. Singh.

Wo treten Situationen auf, wo nur ganzzahlige Lösungen gebraucht werden? Ein Beispiel: Eine Firma erzeugt zwei Produkte A und B, für die 75 bzw. 38 kg eines bestimmten Rohstoffes benötigt werden. Wie viele Stücke von A bzw. B sollen erzeugt werden, wenn 10 000 kg Rohstoff vorhanden sind und der gesamte Rohstoff verbraucht werden soll? Wenn x die Stückzahl von Produkt A und y die Stückzahl von Produkt B bedeutet, dann suchen wir hier also nichtnegative ganze Zahlen x und y, mit

$$75x + 38y = 10\,000.$$

Der entscheidende Schritt zur Lösung dieses Problems ist die Lösung der Gleichung $ax + by = \mathrm{ggT}(a, b)$. Denn haben wir eine Lösung gefunden, so löst nx, ny die Gleichung $a(nx) + b(ny) = n \cdot \mathrm{ggT}(a, b)$. Mehr noch, die Gleichung $ax + by = c$ hat *genau dann* ganzzahlige Lösungen, wenn $c = n \cdot \mathrm{ggT}(a, b)$, also wenn „die rechte Seite" c ein Vielfaches des $\mathrm{ggT}(a, b)$ ist.

Denn: Existiert eine ganzzahlige Lösung, so ist $\mathrm{ggT}(a, b)$ ein Teiler der linken Seite $ax + by$, muss also auch ein Teiler der rechten Seite c sein.

Beispiel 3.48 (→CAS) Erweiterter Euklid'scher Algorithmus
a) Finden Sie eine ganzzahlige Lösung x, y von

$$75x + 38y = 1.$$

b) Finden Sie eine ganzzahlige Lösung von

$$75x + 38y = 10000.$$

c) Besitzt die Gleichung $217x + 63y = 10$ eine ganzzahlige Lösung?

Lösung zu 3.48

a) Wir führen den Euklid'schen Algorithmus wie in Beispiel 3.43 durch und berechnen zusätzlich in jedem Schritt die x_k und y_k, wie im Satz 3.45 be-

schrieben (Startwerte $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$):

$$\begin{aligned} 75 &= 1 \cdot 38 + 37, & x_2 &= 1 - 1 \cdot 0 = 1, & y_2 &= 0 - 1 \cdot 1 = -1 \\ 38 &= 1 \cdot 37 + 1, & x_3 &= 0 - 1 \cdot 1 = -1, & y_3 &= 1 - 1 \cdot (-1) = 2 \\ 37 &= 37 \cdot 1 \end{aligned}$$

Der letzte Rest ungleich 0 ist $r_3 = 1 = \mathrm{ggT}(75, 38)$. Damit ist $x = x_3 = -1$ und $y = y_3 = 2$ eine Lösung der Gleichung. Probe: $75 \cdot (-1) + 38 \cdot 2 = 1$.

b) Da $x = -1$ und $y = 2$ eine Lösung von $75x + 38y = 1$, ist $x = -10000$ und $y = 20000$ eine Lösung von $75x + 38y = 10000$.

c) Wir wissen aus Beispiel 3.43, dass $\mathrm{ggT}(217, 63) = 7$ ist. Da nun 10 kein Vielfaches von 7 ist, gibt es keine ganzzahlige Lösung.

■

Nun haben wir mit $x = -10000$ und $y = 20000$ zwar eine Lösung von $75x + 38y = 10000$, aber ein Problem, wenn wir x und y als Stückzahlen interpretieren möchten! Dafür können wir nämlich nur nichtnegative Werte für x und y brauchen. Gibt es noch weitere Lösungen von $75x + 38y = 10000$? Ja! Hier alles zusammengefasst:

Satz 3.49 (Lösung einer diophantischen Gleichung) Die diophantische Gleichung

$$ax + by = c$$

hat genau dann eine ganzzahlige Lösung, wenn c ein Vielfaches des größten gemeinsamen Teilers von a und b ist, also $c = n \cdot \mathrm{ggT}(a, b)$ mit $n \in \mathbb{Z}$.

Ist x_0, y_0 eine ganzzahlige Lösung von $ax_0 + by_0 = \mathrm{ggT}(a, b)$ (gefunden zum Beispiel mithilfe von Satz 3.45), so ist $x = nx_0$, $y = ny_0$ eine ganzzahlige Lösung von $ax + by = n \cdot \mathrm{ggT}(a, b)$. Alle weiteren ganzzahligen Lösungen von $ax + by = n \cdot \mathrm{ggT}(a, b)$ sind gegeben durch

$$\tilde{x} = x + \frac{kb}{\mathrm{ggT}(a, b)}, \qquad \tilde{y} = y - \frac{ka}{\mathrm{ggT}(a, b)}$$

mit einer beliebigen ganzen Zahl k.

Man kann sich durch Einsetzen leicht davon überzeugen, dass mit x, y auch $\tilde{x} = x + k\frac{b}{\mathrm{ggT}(a,b)}$, $\tilde{y} = y - k\frac{a}{\mathrm{ggT}(a,b)}$ eine Lösung ist. Umgekehrt muss jede Lösung auch so aussehen. Denn ist $\tilde{x}$, $\tilde{y}$ irgendeine weitere Lösung, also $\tilde{x}a + \tilde{y}b = n \cdot \mathrm{ggT}(a, b)$, so erhält man durch Subtraktion der beiden Gleichungen $(\tilde{x} - x)a = (y - \tilde{y})b$. Kürzt man durch $\mathrm{ggT}(a, b)$, so erhält man $(\tilde{x} - x)\tilde{a} = (y - \tilde{y})\tilde{b}$ mit $\tilde{a} = \frac{a}{\mathrm{ggT}(a,b)}$ und $\tilde{b} = \frac{b}{\mathrm{ggT}(a,b)}$. Da keiner der Primfaktoren von $\tilde{a}$ in $\tilde{b}$ steckt, müssen alle in $(y - \tilde{y})$ stecken, also ist $y - \tilde{y}$ ein Vielfaches von $\tilde{a}$. Analog ist $\tilde{x} - x$ ein Vielfaches von $\tilde{b}$.

Nun haben wir alle Zutaten, um unser Rohstoffproblem endgültig zu lösen:

Beispiel 3.50 Diophantische Gleichung
Finden Sie nichtnegative ganze Zahlen x und y mit

$$75x + 38y = 10000.$$

Lösung zu 3.50 Wir kennen aus Beispiel 3.48 bereits eine Lösung $x = -10000$ und $y = 20000$. Mithilfe von Satz 3.49 erhalten wir nun weitere ganzzahlige Lösungen $\tilde{x} = -10000 + k \cdot 38$ und $\tilde{y} = 20000 - k \cdot 75$ für beliebiges $k \in \mathbb{Z}$.

Nun suchen wir ein k so, dass $\tilde{x}$ und $\tilde{y}$ nichtnegativ sind: Aus der Bedingung $\tilde{x} \geq 0$ folgt, dass dieses $k \geq \frac{10000}{38} = 263.158$ sein muss, und aus $\tilde{y} \geq 0$ folgt $k \leq \frac{20000}{75} = 266.\overline{6}$. Dies trifft für $k = 264, 265$ oder 266 zu. Mit jedem dieser k's erhalten wir also wie gewünscht nichtnegative Lösungen. Zum Beispiel ergeben sich für $k = 264$ die Stückzahlen $\tilde{x} = 32$ und $\tilde{y} = 200$. Probe: $75 \cdot 32 + 200 \cdot 38 = 10000$. ■

3.4 Der Chinesische Restsatz

Im 1. Jahrhundert v. Chr. stellte der chinesische Mathematiker Sun-Tsu folgendes Rätsel: „Ich kenne eine Zahl. Wenn man sie durch 3 dividiert, bleibt der Rest 2; wenn man sie durch 5 dividiert, bleibt der Rest 3; wenn man sie durch 7 dividiert, bleibt der Rest 2. Wie lautet die Zahl?“ In unserer Schreibweise ist eine Zahl x gesucht, die die Kongruenzen $x = 2 \pmod 3$, $x = 3 \pmod 5$, $x = 2 \pmod 7$ *gleichzeitig* löst.

Viele Anwendungen führen auf mehrere Kongruenzen, die gleichzeitig gelöst werden sollen. Man spricht von einem **System von Kongruenzen**. Wann ein solches System lösbar ist, sagt uns das folgende Kriterium:

Satz 3.51 (Chinesischer Restsatz) Sind $m_1, \ldots, m_n$ paarweise teilerfremde ganze Zahlen, dann hat das System von Kongruenzen

$$\begin{aligned} x &= a_1 \pmod{m_1} \\ &\vdots \\ x &= a_n \pmod{m_n} \end{aligned}$$

eine eindeutige Lösung $x \in \mathbb{Z}_m$, wobei $m = m_1 \cdot \ldots \cdot m_n$ das Produkt der einzelnen Module ist.

Die Lösung lässt sich auch leicht explizit konstruieren:

a) Wir berechnen die Zahlen $M_k = \frac{m}{m_k}$, das ist also jeweils das Produkt aller Module außer m_k.
b) Nun berechnen wir für jedes M_k das multiplikative Inverse $N_k \in \mathbb{Z}_{m_k}$.

c) Dann ist

$$x = \sum_{k=1}^{n} a_k M_k N_k = a_1 \cdot M_1 \cdot N_1 + \ldots + a_n \cdot M_n \cdot N_n \pmod{m}$$

die in $\mathbb{Z}_m$ eindeutige Lösung des Systems von Kongruenzen. Jede Zahl kongruent zu x modulo m ist wieder eine Lösung.

Beweis, dass wir hiermit eine Lösung haben: Es gilt $\text{ggT}(M_k, m_k) = 1$, da ja $\text{ggT}(m_i, m_k) = 1$ für alle $i \neq k$ ist nach Voraussetzung. Deshalb existiert für jedes M_k ein multiplikatives Inverses $N_k \in \mathbb{Z}_{m_k}$. Nun ist die Lösung durch

$$x = \sum_{k=1}^{n} a_k M_k N_k$$

gegeben, wie man leicht durch Einsetzen überprüft: Rechnet man $x \pmod{m_i}$, so ist m_i ein Faktor von M_k für alle $k \neq i$ und alle zugehörigen Summanden verschwinden; für $k = i$ gilt aber nach Konstruktion $M_i N_i = 1 \pmod{m_i}$. Daher bleibt $x \pmod{m_i} = a_i$.

Warum ist die Lösung eindeutig in $\mathbb{Z}_m$? Gäbe es eine weitere Lösung y, so muss $x - y = 0 \pmod{m_j}$ gelten. Somit enthält $x - y$ alle m_j als Faktoren, also auch m und ist damit ein Vielfaches von m.

Achtung: Der Chinesische Restsatz ist nur anwendbar, wenn die Module teilerfremd sind.

Beispiel: $x = 1 \pmod 2$ und $x = 2 \pmod 4$ hat keine Lösung. Das kann man so überlegen: Wenn $x \in \mathbb{Z}$ eine Lösung von $x = 1 \pmod 2$ und $x = 2 \pmod 4$ wäre, so müsste $x = 1 + 2m$ und $x = 2 + 4n$ für irgendwelche ganzen Zahlen $m, n \in \mathbb{Z}$ gelten. Setzen wir beide Darstellungen von x gleich, so erhalten wir $1 = 2(m - 2n)$. Das ist aber unmöglich, da 1 nicht gleich einer geraden ganzen Zahl sein kann. Wir haben also einen Widerspruch erhalten, somit kann es keine Lösung x geben.

Nun können wir das Rätsel von Sun-Tsu lösen:

Beispiel 3.52 (→CAS) Chinesischer Restsatz
Lösen Sie das System von Kongruenzen

$$\begin{aligned} x &= 2 \pmod 3 \\ x &= 3 \pmod 5 \\ x &= 2 \pmod 7. \end{aligned}$$

Lösung zu 3.52 Da die Module 3, 5, 7 Primzahlen sind, sind sie insbesondere paarweise teilerfremd. Das Produkt der Module ist $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$. Es gibt also eine eindeutige Lösung x mit $0 \leq x < 105$, und jede weitere Zahl aus der Restklasse von x modulo 105 löst das System. Konstruktion der Lösung:
a) Wir berechnen $M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35$, $M_2 = m_1 \cdot m_3 = 3 \cdot 7 = 21$, $M_3 =$

$m_1 \cdot m_2 = 3 \cdot 5 = 15$.
b) Berechnung der multiplikativen Inversen von M_1, M_2, M_3 modulo m_1, m_2 bzw. m_3: Das multiplikative Inverse N_1 von M_1 in $\mathbb{Z}_{m_1}$ erfüllt $35 \cdot N_1 = 1 \pmod 3$ oder, wenn wir anstelle 35 einen kleineren Vertreter von 35 aus derselben Restklasse modulo 3 nehmen (damit wir das multiplikative Inverse besser finden können), $2 \cdot N_1 = 1 (\mathrm{mod}\, 3)$. Nun können wir leicht ablesen, dass $N_1 = 2$ ist. Analog berechnen wir das multiplikative Inverse $N_2 = 1$ zu $M_2 = 21$ in $\mathbb{Z}_5$ und das multiplikative Inverse $N_3 = 1$ zu $M_3 = 15$ in $\mathbb{Z}_7$.
c) Damit berechnen wir $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 = 23 \pmod{105}$. Die gesuchte Lösung in $\mathbb{Z}_{105}$ ist also 23. ■

Eine „praktische“ Anwendung des Chinesischen Restsatzes sind Kartentricks: Sie denken an irgendeine Karte (insgesamt 20 Karten). Ich lege die Karten der Reihe nach (sichtbar) auf 5 Stapel (nach dem letzten beginne ich wieder beim ersten). Sie sagen mir, in welchem Stapel die Karte liegt. Wir wiederholen das mit 4 Stapeln, und ich sage Ihnen dann, an welche Karte Sie gedacht haben.

Mathematisch kann man den Chinesischen Restsatz auch so interpretieren, dass die Gruppen $\mathbb{Z}_m$ und $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ isomorph sind, wobei die Gruppenoperationen im letzten Fall komponentenweise zu verstehen sind. Der Isomorphismus ist $\psi(a) = (a_1, a_2, \ldots, a_n)$ mit $a_j = a \pmod{m_j}$. Dass ψ umkehrbar eindeutig ist, sagt genau der Chinesischen Restsatz; dass Addition und Multiplikation erhalten bleiben, folgt, da Gleichungen gültig bleiben, wenn wir sie addieren oder multiplizieren. Diese Beobachtung wird beim Rechnen mit großen Zahlen verwendet.

Eine andere nützliche Konsequenz ist die Tatsache, dass mit $\mathbb{Z}_m$ und $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ auch $\mathbb{Z}_m^*$ und $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$ isomorph sind. Also gilt für die Euler'sche Phi-Funktion $\varphi(m_1 m_2) = |\mathbb{Z}_m^*| = |\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*| = \varphi(m_1)\varphi(m_2)$, falls m_1 und m_2 teilerfremd sind.

3.4.1 Anwendung: Rechnen mit großen Zahlen

Zum Abschluss sehen wir uns noch an, wie man den Chinesischen Restsatz verwenden kann, um **mit großen Zahlen zu rechnen**. Dies kommt zum Beispiel in der Kryptographie (RSA-Algorithmus) zur Anwendung, wo mit großen Zahlen (mehr als 200 Stellen) gerechnet wird. Dabei ermöglicht die Verwendung des Chinesischen Restsatzes eine Beschleunigung um das mehr als 3-fache:

Bekanntlich können Computer ja nur natürliche Zahlen mit einer maximalen Größe verarbeiten, zum Beispiel $2^{32} - 1$, wenn 32-Bit zur Verfügung stehen. Wie rechnet man nun aber mit Zahlen, die größer sind?

Eine einfache Lösung zu diesem Problem wäre, eine Zahl in diesem Fall in zwei 16-Bit Blöcke zu zerlegen, und mit den einzelnen Blöcken zu rechnen. Wir betrachten einfachheitshalber nur zwei Blöcke, das Verfahren kann aber leicht auf beliebig viele Blöcke erweitert werden.

Warum 16-Bit, und nicht 32-Bit-Blöcke? Weil ansonsten das Produkt zweier Blöcke nicht in die 32-Bit passen würde, die zur Verfügung stehen.

Bei der Addition zweier Zahlen $x = 2^{16}x_1 + x_0$ und $y = 2^{16}y_1 + y_0$ müssen nur die Blöcke addiert werden: $x + y = 2^{16}p_1 + p_0$, wobei $p_0 = (x_0 + y_0) \bmod 2^{16}$ und $p_1 = (x_1 + y_1 + o_0) \bmod 2^{16}$ (wobei o_0 der eventuelle Überlauf aus der Addition von x_0 und y_0 ist).

Im Dezimalsystem überlegt: Angenommen, es stehen 6 Stellen zur Verfügung, und wir zerlegen eine Zahl in zwei dreistellige Blöcke, z. B. die Zahl $513\,489 = 513 \cdot 10^3 + 489 = x_1 \cdot 10^3 + x_0$ in die zwei Blöcke 513 und 489. Der erste Block $x_1 = 513$ gehört also hier zur Potenz 10^3, der zweite $x_0 = 489$ zur Potenz $10^0 = 1$. Haben wir eine zweite Zahl, z. B. $120\,721 = 120 \cdot 10^3 + 721 = y_1 \cdot 10^3 + y_0$, so ist die Summe der beiden Zahlen gleich $634 \cdot 10^3 + 210$. Hier ist 210 der Rest $(x_0 + y_0) \bmod 10^3 = (489 + 721) \bmod 10^3$, es bleibt der Überlauf 1 und $634 = x_1 + y_1 + o_0 = 513 + 120 + 1$.

Die Multiplikation ist schon aufwendiger: Es gilt $xy = 2^{48}q_3 + 2^{32}q_2 + 2^{16}q_1 + q_0$ mit $q_0 = (x_0y_0) \bmod 2^{16}$ und $q_1 = (x_1y_0 + x_0y_1 + o_0) \bmod 2^{16}$ wobei $o_0 = x_0y_0/2^{16}$ (ganzzahlige Division ohne Rest) ein eventueller Überlauf ist. Weiters ist $q_2 = (x_1y_1 + o_1) \bmod 2^{16}$ und $q_3 = x_1y_1/2^{16} + o_2$, wobei o_j der eventuelle Überlauf aus der Berechnung des j-ten Blocks ist. Die beiden letzten Blöcke q_2 und q_3 sollten allerdings gleich null sein, wenn zur Speicherung des Ergebnisses nur zwei Blöcke zur Verfügung stehen.

Das ist schon recht umständlich und wird natürlich bei noch mehr Blöcken noch umständlicher. Außerdem kann man sich überlegen, dass die Anzahl der notwendigen Multiplikationen quadratisch mit der Anzahl der Blöcke steigt.

Und so kann man nun das Rechnen mit großen Zahlen mithilfe des Chinesischen Restsatzes vereinfachen: Seien $m_1, m_2, \ldots, m_n$ paarweise teilerfremd und $m = m_1 \cdots m_n$, Dann kann jede Zahl x mit $0 \leq x < m$ eindeutig durch ihre Reste x_k modulo der m_k, $k = 1, \ldots, n$ repräsentiert werden:

$$x = (x_1, \ldots, x_n).$$

Beispiel: $m_1 = 9$, $m_2 = 8$. Dann ist etwa $39 = (3, 7)$, denn $39 = 3 \pmod 9$ und $39 = 7 \pmod 8$. Umgekehrt kann zu jedem Tupel sofort mithilfe des Chinesischen Restsatzes wieder die Zahl rekonstruiert werden. So erhält man $x = 39$ als eindeutige Lösung von

$$\begin{aligned} x &= 3 \pmod 9 \\ x &= 7 \pmod 8. \end{aligned}$$

Mit dieser Darstellung werden Addition und Multiplikation einfach (Satz 3.4): Sind $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$ zwei Zahlen, so ist ihre Summe

$$x + y = ((x_1 + y_1) \bmod m_1, \ldots, (x_n + y_n) \bmod m_n)$$

und ihr Produkt

$$x \cdot y = ((x_1y_1) \bmod m_1, \ldots, (x_ny_n) \bmod m_n)$$

(siehe Übungsaufgabe 24). Wir erhalten also die Reste der Summe durch Addition der Reste in $\mathbb{Z}_{m_k}$ und die Reste des Produktes durch Multiplikation der Reste in $\mathbb{Z}_{m_k}$. Insbesondere ist nun beim Produkt die Anzahl der notwendigen Multiplikationen gleich der Anzahl der Blöcke (und nicht quadratisch in der Anzahl der Blöcke wie zuvor). Außerdem können die einzelnen Reste getrennt berechnet werden, dieses Verfahren lässt sich somit gut auf Parallelrechnern umsetzen.

In der Praxis verwendet man für die Module m_k Zahlen der Form $2^\ell - 1$, da sich die modulare Arithmetik für diese Zahlen binär leicht implementieren lässt.

3.4.2 Anwendung: Verteilte Geheimnisse

Mit dem Chinesischen Restsatz lässt sich ein Geheimnis (z. B. ein Zugangscode oder Schlüssel) auf mehrere Personen verteilen. Auf diese Weise kennt jede der beteiligten Personen (aus Sicherheitsgründen) nur einen Teil des Geheimnisses.

Angenommen, Sie möchten ein Geheimnis, das als eine natürliche Zahl x gegeben ist, auf n Personen verteilen. Dann können Sie einfach n paarweise teilerfremde natürliche Zahlen $m_1, \ldots, m_n$ (mit $m_1 \cdots m_n > x$) wählen und jeder Person den Rest der Division von x durch ein m_k, also $a_k = x \bmod m_k$ $(k = 1, \ldots, n)$, mitteilen. Alle n Personen zusammen können dann x mithilfe des Chinesischen Restsatzes bestimmen und somit das Geheimnis rekonstruieren.

Was ist nun, wenn nur ein Teil der Personen verfügbar ist? Können wir ein Geheimnis auch so verteilen, dass r Personen ausreichen um das Geheimnis zu rekonstruieren (mit einem zuvor festgelegten $r \leq n$), nicht aber weniger Personen? Auch das ist möglich: Nach dem Chinesischen Restsatz reicht ja bereits ein Teil der Reste a_k aus um x eindeutig zu rekonstruieren, wenn nur das Produkt der zugehörigen Module größer als x ist. Damit *jedes* Produkt aus r Modulen (ausgewählt aus den n Modulen) größer als x ist, muss das Produkt der *kleinsten* r Module diese Bedingung erfüllen. Wenn die Module geordnet sind, $m_1 < m_2 < \cdots < m_n$, so muss also $x < m_1 \cdots m_r$ gelten, damit beliebige r Personen (unter den n Besitzern der Teilgeheimnisse) das Geheimnis rekonstruieren können. Damit auf der anderen Seite aber *weniger* als r Personen das Geheimnis nicht rekonstruieren können, muss x grösser oder gleich als das Produkt von $r-1$ oder weniger Modulen sein (ausgewählt aus den n Modulen). Diese Bedingung ist erfüllt, wenn $x \geq m_{n-r+2} \cdots m_n$ gilt (das ist das Produkt der größten $r-1$ Module).

In der Praxis ist das Geheimnis s als eine Zahl mit einer maximalen Größe m gegeben (z. B. der geheime Schlüssel eines Verschlüsselungsalgorithmus), also $s \in \mathbb{Z}_m$. Da s beliebig klein sein kann, ersetzen wir s durch $x = m_{n-r+2} \cdots m_n + s$, damit obige Bedingungen erfüllt werden können. Dann ist klar, dass $m_{n-r+2} \cdots m_n \leq x$ gilt. Damit auch $x < m_1 \cdots m_r$ erfüllt ist muss $m_1 \cdots m_r - m_{n-r+2} \cdots m_n \geq m$ sein. In diesem Fall können wir $a_k = x \bmod m_k$ verteilen. Aus r Geheimnissen kann dann x mithilfe des Chinesischen Restsatzes berechnet werden und das Geheimnis folgt aus $s = x - m_{n-r+2} \cdots m_n$.

Beispiel 3.53 **Verteilte Geheimnisse**
Das Geheimnis $s = 9 \in \mathbb{Z}_{16}$ soll unter 5 Vorstandsmitgliedern aufgeteilt werden. Für die Rekonstruktion des Geheimnisses sollen zumindest 3 der Vorstandsmitglieder notwendig sein.

Lösung zu 3.53 Wir versuchen es mit den Modulen $3, 5, 7, 8, 11$ und prüfen, ob die obigen beiden Bedingungen erfüllt sind: Es gilt $m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$ und $m_4 \cdot m_5 = 8 \cdot 11 = 88$. Wegen $105 - 88 = 17 \geq 16$ geht unsere Wahl in Ordnung. Wir berechnen $x = 88 + 9 = 97$ und verteilen die Teilgeheimnisse $a_1 = 97 \bmod 3 = 1$, $a_2 = 97 \bmod 5 = 2$, $a_3 = 97 \bmod 7 = 6$, $a_4 = 97 \bmod 8 = 1$, $a_5 = 97 \bmod 11 = 9$.

Nun reichen drei der Teilgeheimnisse a_1, a_2, a_3, a_4, a_5 aus, um mithilfe des Chinesischen Restsatzes x und damit $s = x - 88$ zu rekonstruieren. ■

Unser Verfahren hat einen praktischen Schönheitsfehler. Es ist in Beispiel 3.53 kein Zufall, dass das fünfte Teilgeheimnis a_5 gleich dem Geheimnis $s = 9$ ist! Das liegt daran, dass $a_5 = x \bmod 11 = (8 \cdot 11 + 9) \bmod 11 = 9 = s$ ist, da $s = 9 < 11 = m_5$ gilt. Um das zu verhindern müsste s größer als der größte Modul, also $s > m_n$ sein.

Auf der anderen Seite sollte aber $s < m_1$ sein, denn sonst könnten bekannte Teilgeheimnisse einen Angriff zumindest erleichtern: Wären im letzten Beispiel etwa a_2 und a_4 bekannt, so bräuchte man nur noch die $m_1 = 3$ Möglichkeiten für die zugehörigen Reste a_1 durchzuprobieren. Deshalb muss m_1 groß sein und insbesondere größer als s, damit das Durchprobieren aller möglichen a_1 zumindest genauso lange dauert wie das Durchprobieren aller möglichen s. Beide Forderungen, $s < m_1$ und $s > m_n$ lassen sich aber nur schwer unter einen Hut bringen.

Aus diesem Grund verwendet man folgendes modifizierte Verfahren (**Asmuth–Bloom Schema**), das hier nur kurz erwähnt sein soll: Um ein Geheimnis $s \in \mathbb{Z}_m$ zu verteilen, wählt man paarweise teilerfremde Zahlen $m < m_1 < m_2 < \cdots < m_n$ mit $m \cdot m_{n-r+2} \cdots m_n < m_1 \cdots m_r$. Nun wird zu s irgendein zufälliges Vielfaches $t \cdot m$ addiert (wobei t geheim bleibt — da es zur Rekonstruktion nicht benötigt wird, kann es nach dem Verteilen vernichtet werden), sodass $x = s + t \cdot m < m_1 \cdots m_r$ erfüllt ist und $a_k = x \bmod m_k$ wird verteilt. Aus r Geheimnissen kann dann x mithilfe des Chinesischen Restsatzes berechnet werden und das Geheimnis folgt aus $s = x \bmod m$.

Ist das verwendete t bekannt, so reicht ein Teilgeheimnis aus, um $s = a_k - t \cdot m \bmod m_k$ zu berechnen. Daher muss t geheim gehalten werden.

Die Bedingung $m \cdot m_{n-r+2} \cdots m_n < m_1 \cdots m_r$ bedeutet, dass das Verhältnis aus dem Produkt der kleinsten r Module und dem Produkt der größten $r-1$ Module größer als m ist. Damit kann man zeigen, dass auch bei Kenntnis beliebiger $r-1$ Teilgeheimnisse keinerlei Möglichkeiten für s ausgeschlossen werden können. Das Asmuth–Bloom Schema wird deshalb als **perfekt** bezeichnet.

3.5 Kontrollfragen

Fragen zu Abschnitt 3.1: Das kleine Einmaleins auf endlichen Mengen

Erklären Sie: Rest, kongruent modulo m, Restklasse.

1. Geben Sie den Rest modulo 3 der Zahlen $1, 2, 3, \ldots, 10$ an.

   (Lösung zu Kontrollfrage 1)

2. Geben Sie den Rest modulo 3 von $-1, -2, -3, \ldots, -10$ an.

   (Lösung zu Kontrollfrage 2)

3. Was trifft zu:
   a) $a = b \pmod 3$ bedeutet, dass $a - b$ ein Vielfaches von 3 ist.
   b) $a = 4 \pmod 3$ bedeutet, dass es ein $k \in \mathbb{Z}$ gibt, sodass $a = k \cdot 3 + 4$.

   (Lösung zu Kontrollfrage 3)

4. Richtig oder falsch?
   a) $3 = 0 \pmod 3$ b) $7 = 2 \pmod 3$ c) $-2 = 1 \pmod 3$
   d) $12 = 27 \pmod 5$ e) $17 = 9 \pmod 5$ f) $28 = 10 \pmod 9$

   (Lösung zu Kontrollfrage 4)

5. Geben Sie die Restklassen modulo 3 an.

   (Lösung zu Kontrollfrage 5)

Fragen zu Abschnitt 3.2: Gruppen, Ringe und Körper

Erklären Sie: additives Inverses, multiplikatives Inverses, $\mathbb{Z}_m$, $\mathbb{Z}_m^*$, Euler'sche Phi-Funktion, Gruppe, Satz von Euler, Kleiner Satz von Fermat, Körper, Ring, Ideal.

1. Geben Sie folgende Mengen an: a) $\mathbb{Z}_3$ b) $\mathbb{Z}_5$

   (Lösung zu Kontrollfrage 1)

2. Richtig oder falsch:
   a) In $\mathbb{Z}_m$ besitzt jede Zahl ein additives Inverses.
   b) In $\mathbb{Z}_m$ besitzt jede Zahl ein multiplikatives Inverses.

   (Lösung zu Kontrollfrage 2)

3. Finden Sie das additive Inverse von: a) 1 in $\mathbb{Z}_8$ b) 3 in $\mathbb{Z}_9$ c) 3 in $\mathbb{Z}_{11}$ d) 0 in $\mathbb{Z}_4$

   (Lösung zu Kontrollfrage 3)

4. Welche Zahlen besitzen modulo m ein multiplikatives Inverses (d.h. einen Kehrwert)? Geben Sie es gegebenenfalls an: a) 3 in $\mathbb{Z}_7$ b) 6 in $\mathbb{Z}_8$ c) 0 in $\mathbb{Z}_9$ d) 8 in $\mathbb{Z}_{11}$

   (Lösung zu Kontrollfrage 4)

5. Wo steckt der Fehler: $2 = 8 \pmod 6$, d.h. $1 \cdot 2 = 4 \cdot 2 \pmod 6$. Kürzen von 2 auf beiden Seiten ergibt $1 = 4 \pmod 6$!?

   (Lösung zu Kontrollfrage 5)

6. Was gibt die Euler-Funktion $\varphi(n)$ an?

   (Lösung zu Kontrollfrage 6)

7. Geben Sie an: a) $\mathbb{Z}_5^*$, $\varphi(5)$ b) $\mathbb{Z}_6^*$, $\varphi(6)$

   (Lösung zu Kontrollfrage 7)

8. Wenden Sie den Satz von Euler für $m = 8$ an.

   (Lösung zu Kontrollfrage 8)

9. Wenden Sie den kleinen Satz von Fermat für $p = 7$ an.

   (Lösung zu Kontrollfrage 9)

10. Richtig oder falsch?
    a) Die Lösung von $4x = 8 \pmod{27}$ ist $x = 8 \cdot \frac{1}{4} = 2$ in $\mathbb{Z}_{27}$.
    b) Die Lösung von $6x = 18 \pmod{42}$ ist $x = 18 \cdot \frac{1}{6} = 3$ in $\mathbb{Z}_{42}$.

    (Lösung zu Kontrollfrage 10)

11. Handelt es sich um eine Gruppe? Begründen Sie!
    a) $(\mathbb{Z}_8, +)$ b) $(\mathbb{Z}, \cdot)$ c) $(\mathbb{Z}_7, \cdot)$ d) $(\mathbb{Z}_7 \backslash \{0\}, \cdot)$

    (Lösung zu Kontrollfrage 11)

12. Handelt es sich um einen Körper (Addition und Multiplikation in diesen Mengen wie gewohnt)? Begründen Sie!
    a) $\mathbb{Z}_2$ b) $\mathbb{Z}_8$ c) $\mathbb{Z}$ d) $\mathbb{Q}$ e) $\mathbb{R}$

    (Lösung zu Kontrollfrage 12)

13. Wie viele Verknüpfungen gibt es in einem Ring?

    (Lösung zu Kontrollfrage 13)

14. Geben Sie ein Beispiel für einen Ring, der kein Körper ist.

    (Lösung zu Kontrollfrage 14)

15. Richtig oder falsch?
    In einem Körper hat jedes Element ein mulitplikatives Inverses.

    (Lösung zu Kontrollfrage 15)

Fragen zu Abschnitt 3.3: Der Euklid'sche Algorithmus

Erklären Sie: größter gemeinsamer Teiler, Euklid'scher Algorithmus, erweiterter Euklid'scher Algorithmus.

1. Was ist der Zusammenhang zwischen dem erweiterten Euklid'schen Algorithmus und dem multiplikativen Inversen?

   (Lösung zu Kontrollfrage 1)

2. Diophantische Gleichungen: Besitzen folgenden Gleichungen ganzzahlige Lösungen (sie brauchen nicht angegeben zu werden)?
   a) $36x + 15y = 3$ b) $36x + 15y = 12$ c) $36x + 15y = 5$
   d) $22x + 15y = 27$

   (Lösung zu Kontrollfrage 2)

Fragen zu Abschnitt 3.4: Der Chinesische Restsatz

Erklären Sie: System von Kongruenzen, Chinesischer Restsatz.

1. Hat das System von Kongruenzen $x = a_1 (\mathrm{mod}\, m_1)$, $x = a_2 (\mathrm{mod}\, m_2)$ immer eine Lösung in $\mathbb{Z}_{m_1 m_2}$?

   (Lösung zu Kontrollfrage 1)

2. Was sagt der Chinesische Restsatz über folgendes System von Kongruenzen aus?
   $x = 1 \,(\mathrm{mod}\, 4)$, $x = 3 \,(\mathrm{mod}\, 6)$.

   (Lösung zu Kontrollfrage 2)

3. Richtig oder falsch?
   $x = 25$ ist die einzige Lösung von $x = 7 \,(\mathrm{mod}\, 9)$ und $x = 1 \,(\mathrm{mod}\, 4)$ in $\mathbb{Z}_{36}$.

   (Lösung zu Kontrollfrage 3)

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 3.1

1.

a	1	2	3	4	5	6	7	8	9	10
$r = a \bmod 3$	1	2	0	1	2	0	1	2	0	1

2.

a	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10
$r = a \bmod 3$	2	1	0	2	1	0	2	1	0	2

3. a) richtig b) richtig

4. a) richtig b) Falsch, denn $7 - 2 = 5$ ist nicht durch 3 teilbar. c) richtig
   d) richtig e) Falsch, denn $17 - 9 = 8$ ist nicht durch 5 teilbar. f) richtig

5. $R_0 = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$, $R_1 = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$,
   $R_2 = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$

Lösungen zu Abschnitt 3.2

1. a) $\mathbb{Z}_3 = \{0, 1, 2\}$ b) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

2. a) richtig b) Falsch; nur wenn die Zahl teilerfremd zu m ist, besitzt sie ein multiplikatives Inverses.

3. a) $d = m - e = 8 - 1 = 7$ b) $9 - 3 = 6$ c) $11 - 3 = 8$ d) 0 (per Definition)

4. a) 3 und 7 sind teilerfremd, daher gibt es $\frac{1}{3} = \frac{1+2\cdot 7}{3} = 5$ in $\mathbb{Z}_7$.
   b) 6 und 8 sind nicht teilerfremd, daher gibt es keinen Kehrwert von 6 in $\mathbb{Z}_8$, d.h., die Schreibweise $\frac{1}{6}$ macht in $\mathbb{Z}_8$ keinen Sinn.
   c) Zu 0 gibt es nie einen Kehrwert.
   d) 8 und 11 sind teilerfremd, daher gibt es $\frac{1}{8} = \frac{1+5\cdot 11}{8} = 7$ in $\mathbb{Z}_{11}$.

5. $\mathrm{ggT}(6, 2) = 2 \neq 1$, also hat 2 kein multiplikatives Inverses in $\mathbb{Z}_6$ und man kann daher nicht beide Seiten der Gleichung damit multiplizieren (d.h. kürzen).

6. Die Anzahl der Elemente in $\mathbb{Z}_n^*$ (= alle Zahlen aus $\mathbb{Z}_n$, die teilerfremd zu n sind = alle Zahlen aus $\mathbb{Z}_n$, die ein multiplikatives Inverses besitzen).

7. a) $\mathbb{Z}_5^* = \mathbb{Z}_5 \backslash \{0\} = \{1, 2, 3, 4\}$, $\varphi(5) = 4$ b) $\mathbb{Z}_6^* = \{1, 5\}$, $\varphi(6) = 2$

8. Für alle Zahlen a aus $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ gilt: $a^{\varphi(8)} = a^4 = 1 \pmod 8$. Also $1^4 = 3^4 = 5^4 = 7^4 = 1 \pmod 8$.

9. $1^6 = 2^6 = 3^6 = \ldots 6^6 = 1 \,(\mathrm{mod}\, 7)$.

10. a) Richtig; $\frac{1}{4}$ existiert in $\mathbb{Z}_{27}$, daher kann eindeutig nach x aufgelöst werden: $x = 8 \cdot \frac{1}{4} = 2 \cdot 4 \cdot \frac{1}{4} = 2 \,(\mathrm{mod}\, 27)$.
    b) Falsch, denn $\frac{1}{6}$ existiert nicht in $\mathbb{Z}_{42}$, daher kann es nicht verwendet werden und somit nicht *eindeutig* nach x aufgelöst werden. (Es gibt 6 Lösungen, $x = 3$ ist eine davon.)

11. a) ja b) nein (denn dazu müssten alle $a \in \mathbb{Z}$ ein mult. Inverses haben)
    c) nein, denn die 0 hat keinen Kehrwert d) ja

12. a) ja b) nein (denn dazu müssten alle $a \in \mathbb{Z}_8 \backslash \{0\}$ ein mult. Inverses haben)
    c) nein, (denn dazu müssten alle $a \in \mathbb{Z} \backslash \{0\}$ ein mult. Inverses haben) d) ja e) ja

13. zwei

14. Zum Beispiel $\mathbb{Z}$, $\mathbb{Z}_4$ oder allgemein $\mathbb{Z}_m$ (wenn m keine Primzahl ist).

15. falsch: die 0 hat kein multiplikatives Inverses (aber alle anderen Elemente schon)

Lösungen zu Abschnitt 3.3

1. Der erweiterte Euklid'sche Algorithmus kann zur effektiven Berechnung des multiplikativen Inversen verwendet werden.

2. Die Gleichung $ax + by = c$ hat genau dann ganzzahlige Lösungen, wenn $c = n \cdot \mathrm{ggT}(a, b)$ (Satz 3.49):
a) ja, da $3 = 1 \cdot \mathrm{ggT}(36, 15)$ b) ja, da $12 = 4 \cdot \mathrm{ggT}(36, 15)$ c) nein, da $\mathrm{ggT}(36, 15) = 3$ kein Teiler von 5 ist d) ja, denn $27 = 27 \cdot \mathrm{ggT}(22, 15)$

Lösungen zu Abschnitt 3.4

1. Nicht notwendigerweise. Es kann keine oder mehrere Lösungen geben. Wenn aber die Module m_1 und m_2 teilerfremd sind, so garantiert der Chinesische Restsatz genau eine Lösung zwischen 0 und $m_1 \cdot m_2$ (und unendlich viele dazu kongruente Lösungen modulo $m_1 \cdot m_2$). Sind die Module nicht teilerfremd, so gibt der Chinesische Restsatz keine Information.

2. Nichts, da die Module 4 und 6 nicht teilerfremd sind. Wir wissen also von vornherein nichts über das Lösungsverhalten dieses Systems.

3. richtig

3.6 Übungen

Aufwärmübungen

1. Berechnen Sie effizient:
a) $(23 \cdot 19 - 2 \cdot 8 + 10 \cdot 37) \bmod 5$
b) $(14 \cdot 39 + 55 \cdot 349 + 28 \cdot 79) \bmod 11$

2. a) Berechnen Sie den Rest modulo 4 der Zahlen 10, -5, -3, 12, 7.
b) Geben Sie die Restklassen modulo 4 an.

3. Geben Sie $\mathbb{Z}_6$ und die Verknüpfungstabellen für die Addition und die Multiplikation in $\mathbb{Z}_6$ an.

4. Geben Sie das additive Inverse und (wenn vorhanden) das multiplikative Inverse an von: a) 3 in $\mathbb{Z}_7$ b) 1 in $\mathbb{Z}_9$ c) 4 in $\mathbb{Z}_6$ d) 8 in $\mathbb{Z}_{12}$

5. Finden Sie das additive Inverse und (wenn vorhanden) das multiplikative Inverse von 7 in: a) $\mathbb{Z}_{10}$ b) $\mathbb{Z}_{11}$ c) $\mathbb{Z}_{12}$ d) $\mathbb{Z}_{14}$

6. Bestimmen Sie $\varphi(8) = 4$.

7. Berechnen Sie alle Lösungen $x \in \mathbb{Z}_m$, wobei m der jeweilige Modul ist, an: a) $6 + x = 2 \pmod 7$ b) $4 + x = 0 \pmod 9$ c) $9 + x = 8 \pmod{13}$

8. Berechnen Sie alle $x \in \mathbb{Z}_m$ mit: a) $3x = 4 \pmod 7$ b) $4x = 5 \pmod 6$ c) $4x = 6 \pmod{10}$

9. Berechnen Sie $\mathrm{ggT}(14, 51)$ mit dem Euklid'schen Algorithmus:

10. Berechnen Sie mit dem Euklid'schen Algorithmus: a) $\mathrm{ggT}(261, 123)$ b) $\mathrm{ggT}(49, 255)$

11. Berechnen Sie $\frac{1}{14}$ in $\mathbb{Z}_{51}$ mithilfe des erweiterten Euklid'schen Algorithmus.

12. Berechnen Sie mithilfe des erweiterten Euklid'schen Algorithmus: a) $\frac{1}{7}$ in $\mathbb{Z}_{13}$ b) $\frac{1}{6}$ in $\mathbb{Z}_{19}$ c) $\frac{1}{28}$ in $\mathbb{Z}_{37}$

13. Lösen Sie das folgende System von Kongruenzen mithilfe des Chinesischen Restsatzes:
$x = 1 \pmod 2$, $x = 3 \pmod 5$, $x = 3 \pmod 7$.

Aufgaben

1. Berechnen Sie effizient: $25 \cdot 64 + 73 \cdot 81 + 29 \cdot 53 \bmod 11$.

2. Ist 978-3-662-49296-3 eine gültige ISBN-13?

3. Finden Sie das additive Inverse und (wenn vorhanden) das multiplikative Inverse von 8 in: a) $\mathbb{Z}_{10}$ b) $\mathbb{Z}_{11}$ c) $\mathbb{Z}_{12}$ d) $\mathbb{Z}_{13}$ e) $\mathbb{Z}_{91}$

4. Was versteht man unter einer **Gruppe**? Begründen Sie, ob es sich im Folgenden um eine Gruppe handelt:
a) $(\mathbb{Z}_{10}, +)$ b) $(\mathbb{Z}_{10}^*, +)$ c) $(\mathbb{Z}_{10}, \cdot)$ d) $(\mathbb{Z}_{10}^*, \cdot)$ e) $(\mathbb{Z}_7, \cdot)$ f) $(\mathbb{Z}_7 \backslash \{0\}, \cdot)$
Was versteht man unter einem **Körper**? Begründen Sie, ob es sich im Folgenden um einen Körper handelt:
g) $(\mathbb{Z}_{10}, +, \cdot)$ h) $(\mathbb{Z}_{10}^*, +, \cdot)$ i) $(\mathbb{Z}_7, +, \cdot)$

5. Begründen Sie, ob es sich im Folgenden um eine Gruppe handelt:
   a) $(\mathbb{Z}_5, +)$ b) $(\mathbb{Z}_5^*, +)$ c) $(\mathbb{Z}_8, +)$ d) $(\mathbb{Z}_8^*, +)$ e) $(\mathbb{Z}_2, +)$ f) $(\mathbb{Z}_8, \cdot)$
   g) $(\mathbb{Z}_8^*, \cdot)$ h) $(\mathbb{Z}_{11}, \cdot)$ i) $(\mathbb{Z}_{11}^*, \cdot)$
   Begründen Sie, ob es sich im Folgenden um einen Körper handelt:
   j) $(\mathbb{Z}_5, +, \cdot)$ k) $(\mathbb{Z}_8, +, \cdot)$ l) $(\mathbb{Z}_8^*, +, \cdot)$ m) $(\mathbb{Z}_2, +, \cdot)$ n) $(\mathbb{Z}_{11}, +, \cdot)$

6. Es sei S_n die Ziffernsumme der natürlichen Zahl n. Zeigen Sie, dass $n = S_n \pmod 3$.
   Tipp: Schreiben Sie n als Summe von Zehnerpotenzen und verwenden Sie $10 = 1 \pmod 3$.

   Wenn Sie das bewiesen haben, so haben Sie insbesondere die bekannte Teilbarkeitsregel bewiesen, dass eine Zahl durch 3 teilbar (Rest 0) ist genau dann, wenn ihre Ziffernsumme durch 3 teilbar ist.

7. Beweisen Sie, dass jedes Jahr einen Freitag den 13. hat. (Hinweis: Sei x der Wochentag (als Zahl beginnend bei 0=Montag) des 13. Jänner. Um wie viele Tage verschiebt sich der Wochentag, wenn man um ein Monat weiterwandert?)

8. Geben Sie $\mathbb{Z}_8$, $\mathbb{Z}_8^*$ und die Verknüpfungstabellen für die Addition und die Multiplikation in $\mathbb{Z}_8$ an.

9. Bildet $\{a, b, c\}$ mit der im Folgenden definierten Verknüpfung „$\circ$“ eine Gruppe?

$\circ$	a	b	c
a	c	b	a
b	a	c	b
c	a	b	c

10. Sei $\varphi(m) = |\mathbb{Z}_m^*|$ die Euler'sche Phi-Funktion von $m \in \mathbb{N}$. Geben Sie an:
    a) $\varphi(4)$ b) $\varphi(5)$ c) $\varphi(9)$ d) $\varphi(26)$ e) $\varphi(29)$ f) $\varphi(600)$
    Begründen Sie, warum $\varphi(m)$ besonders einfach gefunden werden kann, wenn m eine Primzahl ist.

11. Berechnen Sie mithilfe des kleinen Satzes von Fermat:
    a) $9^{20} \bmod 11$ b) $5^{74} \bmod 11$ c) $8^{37} \bmod 11$ d) $46^{372} \bmod 11$

12. Berechnen Sie, wenn möglich, mithilfe des kleinen Satzes von Fermat:
    a) $3^{24} \bmod 5$ b) $33^{48} \bmod 11$ c) $12^{36} \bmod 17$ d) $8^{72} \bmod 10$

13. Geben Sie alle Lösungen $x \in \mathbb{Z}_m$ an, wobei m der jeweilige Modul ist, an:
    a) $18x = 24 \pmod{30}$ b) $6x = 4 \pmod 9$ c) $9x = 1 \pmod{13}$
    d) $9x + 3 = 1 \pmod 7$ e) $8x + 1 = 4 \pmod{12}$

14. Geben Sie alle Lösungen $x \in \mathbb{Z}_m$ an, wobei m der jeweilige Modul ist:
a) $21x = 14 \pmod{28}$ b) $18x = 6 \pmod{27}$ c) $13x = 28 \pmod{50}$

15. Lösen Sie das folgende Gleichungssystem in $\mathbb{Z}_{27}$.

$$\begin{aligned} 5x + 17y &= 12 \\ 14x + 12y &= 11 \end{aligned}$$

16. Lösen Sie das folgende Gleichungssystem in $\mathbb{Z}_{10}$ und machen Sie die Probe:

$$\begin{aligned} 4x + 2y &= 8 \\ 3x + y &= 1 \end{aligned}$$

Hinweis: Es gibt mehr als eine Lösung.

17. Beweisen Sie, dass in jedem Ring $0 \cdot a = a \cdot 0 = 0$ für alle $a \in R$ gilt.

18. Berechnen Sie mithilfe des Euklid'schen Algorithmus den größten gemeinsamen Teiler von a) 329 und 117 b) 135 und 126.

19. Berechnen Sie mithilfe des Euklid'schen Algorithmus den größten gemeinsamen Teiler von a) 198 und 243 b) 2159 und 1054 c) 19 und 999

20. Berechnen Sie das multiplikative Inverse von 9 in $\mathbb{Z}_{13}$ mithilfe des erweiterten Euklid'schen Algorithmus.

21. Berechnen Sie mithilfe des erweiterten Euklid'schen Algorithmus das multiplikative Inverse von a in $\mathbb{Z}_m$:
a) $a = 7$ und $m = 26$ b) $a = 19$ und $m = 999$

22. Lösen Sie mithilfe des Chinesischen Restsatzes und machen Sie die Probe:

$$\begin{aligned} x &= 2 \pmod{9} \\ x &= 1 \pmod{8} \end{aligned}$$

23. Lösen Sie mithilfe des Chinesischen Restsatzes und machen Sie die Probe:

$$\begin{aligned} x &= 3 \pmod{7} \\ x &= 4 \pmod{9} \\ x &= 5 \pmod{11} \end{aligned}$$

24. **Beschleunigung mithilfe des Chinesischen Restsatzes:** Angenommen, ein Computer kann nur zweistellige ganze Zahlen *effizient* verarbeiten. Sie möchten aber auch dreistellige Zahlen effizient darstellen, addieren und multiplizieren. Verwenden Sie dazu die drei (paarweise teilerfremden) Module $m_1 = 97$, $m_2 = 98$ und $m_3 = 99$ und den Chinesischen Restsatz. Gesucht ist zum Beispiel Summe und Produkt von 203 und 125.
a) Stellen Sie 203 und 125 durch ihre Reste bezüglich der Module dar („Transformation“).
b) Berechnen Sie in dieser Darstellung die Summe und das Produkt von 203 und 125 (effiziente Berechnung).
c) Stellen Sie Summe bzw. Produkt mithilfe des Chinesischen Restsatzes wieder in Dezimaldarstellung dar („Rücktransformation“).

25. Zeigen Sie: Wenn p eine Primzahl ist, so hat die Gleichung $x^2 = 1 \pmod p$ nur die Lösungen $x = 1 \pmod p$ und $x = -1 \pmod p$ (Tipp: $x^2 - 1 = (x-1)(x+1)$).

    Das bedeutet, dass in $\mathbb{Z}_p$ nur 1 und $p-1$ gleich ihrem multiplikativen Inversen sind.

26. Zeigen Sie den Satz von Wilson: Wenn p eine Primzahl ist, so gilt $(p-1)! = -1 \pmod p$ (Tipp: Fassen Sie die Terme in $(p-1)!$ zu Paaren von zueinander multiplikativ inversen Zahlen zusammen und verwenden Sie Übungsaufgabe 25).

27. Finden Sie alle Lösungen des Systems $x = 1 \,(\mathrm{mod}\, 2)$, $x = 3 \,(\mathrm{mod}\, 4)$ in $\mathbb{Z}_8$. (Achtung: Der Chinesische Restsatz ist nicht anwendbar, da die Module nicht teilerfremd sind.)

Lösungen zu den Aufwärmübungen

1. a) Zur einfachen Berechnung wird jede vorkommende Zahl sofort durch ihren Rest modulo 5 ersetzt: $3 \cdot 4 - 2 \cdot 3 + 0 \cdot 2 = 12 - 6 + 0 = 2 - 1 = 1 \,(\mathrm{mod}\, 5)$.
   b) Nun ersetzen wir jede vorkommende Zahl durch ihren Rest modulo 11. Das ergibt: $14 \cdot 39 + 55 \cdot 349 + 28 \cdot 79 = 3 \cdot 6 + 0 \cdot 8 + 6 \cdot 2 = 8 \,(\mathrm{mod}\, 11)$

2. a) 2, 3, 1, 0, 3
   b) $R_0 = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = \{4k \mid k \in \mathbb{Z}\}$, $R_1 = \{\ldots, -7, -3, 1, 5, 9, \ldots\} = \{4k+1 \mid k \in \mathbb{Z}\}$, $R_2 = \{4k+2 \mid k \in \mathbb{Z}\}$, $R_3 = \{4k+3 \mid k \in \mathbb{Z}\}$

3. Verknüpfungstabellen für $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. additives Inverses: a) $7 - 3 = 4$ b) 8 c) 2 d) 4
mult. Inverses: a) existiert, da $\mathrm{ggT}(3, 7) = 1$; Berechnung: $\frac{1}{3} = \frac{1+7}{3} = \frac{1+2\cdot 7}{3} = 5$ b) 1 c) gibt es nicht, da 4 und 6 nicht teilerfremd d.h. $\mathrm{ggT}(4, 6) = 2 \neq 1$ d) gibt es nicht, da $\mathrm{ggT}(8, 12) \neq 1$

5. additives Inverses: a) 3 b) 4 c) 5 d) 7
mult. Inverses: a) 3 b) 8 c) 7 d) gibt es nicht

6. $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, daher $\varphi(8) = 4$.

7. a) $x = 2 - 6 = -4 = 3 \bmod 7$ b) $x = 5$ c) $x = 12$

8. a) Da $\mathrm{ggT}(3, 7) = 1$, existiert $\frac{1}{3}$ und daher können beide Seiten der Gleichung damit multipliziert werden; somit eindeutige Lösung $x = 4 \cdot \frac{1}{3} = 4 \cdot 5 = 20 = 6 \bmod 7$.
b) Keine Lösung, da 4 kein multiplikatives Inverses in $\mathbb{Z}_6$ hat (dann wäre die Lösung eindeutig) und da $\mathrm{ggT}(4, 6) = 2$ kein Teiler von 5 ist.
c) Zwei Lösungen in $\mathbb{Z}_{10}$, da $\mathrm{ggT}(4, 10) = 2$ ist und dieser auch 6 teilt. Die beiden Lösungen $x = 4$, $x = 9$ finden wir, indem wir alle Möglichkeiten aus $\mathbb{Z}_{10}$ durchprobieren oder sie mithilfe von Satz 3.19 berechnen.

9.

$$\begin{aligned} 51 &= 3 \cdot 14 + 9 \\ 14 &= 1 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Der letzte nichtverschwindende Rest, hier 1, ist der gesuchte ggT. Mit anderen Worten: 14 und 51 sind teilerfremd.

10. a) $\mathrm{ggT}(261, 123) = 3$
b) $\mathrm{ggT}(49, 255) = 1$, die beiden Zahlen sind also teilerfremd.

11. Wir verwenden die Schritte des EA, die wir zuvor in Aufgabe 9 bereits ausgeführt haben. Jede Zeile, beginnend mit der ersten, wird nach dem Rest aufgelöst. Dieser wird (mithilfe von rekursivem Einsetzen) in die Form $\ldots \cdot 14 + \ldots \cdot 51$ gebracht:

$$\begin{aligned} 9 &= 51 - 3 \cdot 14 \\ 5 &= 14 - 9 = \\ &= 14 - (51 - 3 \cdot 14) = \\ &= 4 \cdot 14 - 51 \\ 4 &= 9 - 5 = \\ &= (51 - 3 \cdot 14) - (4 \cdot 14 - 51) = \\ &= 2 \cdot 51 - 7 \cdot 14 \\ 1 &= 5 - 4 = \\ &= (4 \cdot 14 - 51) - (2 \cdot 51 - 7 \cdot 14) = \\ &= 11 \cdot 14 - 3 \cdot 51 \end{aligned}$$

Der Faktor von 14 in der letzten Zeile (also 11) ist nun der gesuchte Kehrwert: $\frac{1}{14} = 11 \bmod 51$.
Probe: $14 \cdot 11 = 1$ modulo 51 (denn $14 \cdot 11 - 1$ ist durch 51 teilbar).

12. a) EA (angeschrieben, bis sich der Rest 1 ergibt):

$$\begin{aligned} 13 &= 1 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \end{aligned}$$

Erweiterung (= rekursiv von oben nach unten nach den Resten auflösen):

$$\begin{aligned} 6 &= 13 - 7 \\ 1 &= 7 - 6 \\ &= 7 - (13 - 7) \\ &= 2 \cdot 7 - 13 \end{aligned}$$

Daran können wir ablesen: $\frac{1}{7} = 2 \pmod{13}$
b) EA:

$$19 = 3 \cdot 6 + 1$$

Erweiterung (= nach dem Rest 1 auflösen):

$$1 = 19 - 3 \cdot 6$$

Daran können wir ablesen: $\frac{1}{6} = -3 = 16 \pmod{19}$
c) EA:

$$\begin{aligned} 37 &= 1 \cdot 28 + 9 \\ 28 &= 3 \cdot 9 + 1 \end{aligned}$$

Erweiterung:

$$\begin{aligned} 9 &= 37 - 28 \\ 1 &= 28 - 3 \cdot 9 \\ &= 28 - 3 \cdot (37 - 28) \\ &= 4 \cdot 28 - 3 \cdot 37 \end{aligned}$$

Daher $\frac{1}{28} = 4 \pmod{37}$.

13. Da $m_1 = 2$, $m_2 = 5$ und $m_3 = 7$ teilerfremd sind, gibt es eine Lösung x mit $0 \leq x < 70$ (und jede dazu modulo 70 kongruente Zahl ist ebenfalls Lösung). Konstruktion:
a) $M_1 = m_2 \cdot m_3 = 5 \cdot 7 = 35$; $M_2 = m_1 \cdot m_3 = 2 \cdot 7 = 14$; $M_3 = m_1 \cdot m_2 = 2 \cdot 5 = 10$.
b) Multiplikative Inverse von M_1, M_2, M_3 modulo m_1, m_2, m_3: Gesucht sind N_1, N_2, N_3 mit $35 \cdot N_1 = 1 \cdot N_1 = 1 \,(\mathrm{mod}\, 2)$, $14 \cdot N_2 = 4 \cdot N_2 = 1 \,(\mathrm{mod}\, 5)$ und $10 \cdot N_3 = 3 \cdot N_3 = 1 \,(\mathrm{mod}\, 7)$. Es folgt, dass $N_1 = 1$, $N_2 = 4$ und $N_3 = 5$.
c) $x = a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2 + a_3 \cdot M_3 \cdot N_3 = 1 \cdot 35 \cdot 1 + 3 \cdot 14 \cdot 4 + 3 \cdot 10 \cdot 5 = 353 = 3 \,(\mathrm{mod}\, 70)$.

Lösungen zu ausgewählten Aufgaben

1. 8

2. Ja.

3. additives Inverses: a) 2 b) 3 c) 4 d) 5 e) 83
mult. Inverses: a) – b) 7 c) – d) 5 e) 57 ($= \frac{1+5 \cdot 91}{8}$ bzw. mit dem EEA ist $3 \cdot 91 - 34 \cdot 8 = 1$ die letzte Zeile des Algorithmus)

4. a) ja, weil:
• $\mathbb{Z}_{10}$ abgeschlossen bzgl. Addition modulo 10
• $+$ ist assoziativ (und kommutativ), weil dies bereits in $\mathbb{Z}$ gilt (muss nicht extra überprüft werden)
• $0 \in \mathbb{Z}_{10}$ ist neutrales Element
• zu jedem a aus $\mathbb{Z}_{10}$ liegt auch $10 - a$ als inverses Element in $\mathbb{Z}_{10}$
b) nein (0 fehlt) c) nein (nicht alle Elemente haben Kehrwert)
d) ja e) nein (0 hat keinen Kehrwert) f) ja, denn $\mathbb{Z}_7^* = \mathbb{Z}_7 \backslash \{0\}$
g) nein (nicht alle Elemente außer 0 haben Kehrwert) h) nein (0 fehlt)
i) ja, weil
• $(\mathbb{Z}_7, +)$ kommutative Gruppe
• $(\mathbb{Z}_7 \backslash \{0\}, \cdot)$ kommutative Gruppe
• Distributivgesetz gilt, weil es bereits in $\mathbb{Z}$ gilt (muss nicht extra überprüft werden)

5. a) ja b) nein c) ja d) nein e) ja f) nein g) ja h) nein i) ja j) ja k) nein l) nein m) ja n) ja

6. –

7. –

8. –

9. Nein, denn das Assoziativgesetz gilt nicht.

10. –

11. a) 1 b) 9 c) 2 d) 4

12. a) 1 b) Kl. S. v. F. nicht anwendbar; $33^{48} = 0^{48} = 0 \bmod 11$
    c) 13
    d) Kl. S. v. F. nicht anwendbar

13. a) sechs Lösungen b) keine Lösung c) 3 d) 6 e) keine Lösung

14. a) 7 Lösungen: $2, 6, 10, 14, 18, 22, 26$
    b) keine Lösung
    c) genau eine Lösung: 6

15. $x = 1, y = 2$
    Bemerkung: Zur Lösung eines Gleichungssystems modulo m können beliebige Äquivalenzumformungen (z.B. Gauß-Algorithmus) durchgeführt werden. Dabei darf eine Gleichung insbesondere nur mit Zahlen aus $\mathbb{Z}_m^*$ multipliziert (bzw. durch diese dividiert) werden.

16. $x_1 = 2, y_1 = 5$ und $x_2 = 7, y_2 = 0$

17. –

18. a) 1 b) 9

19. a) 9 b) 17 c) 1

20. 3

21. a) $\frac{1}{7} = 15$ in $\mathbb{Z}_{26}$ (letzte Zeile des EEA ist: $-11 \cdot 7 + 3 \cdot 26 = 1$)
    b) $\frac{1}{19} = 631$ in $\mathbb{Z}_{999}$ (letzte Zeile des EEA: $7 \cdot 999 - 368 \cdot 19 = 1$)

22. $x = 65 \,(\mathrm{mod}\, 72)$

23. $x = 346 \,(\mathrm{mod}\, 693)$

24. a) $203 = (9, 7, 5), 125 = (28, 27, 26)$ b) $s = (37, 34, 31)$ und $p = (58, 91, 31)$; c) Rücktransformation mithilfe des CRT mit m =941094; $M_1 = 9702$, $M_2 = 9603$, $M_3 = 9506$; $N_1 = 49$, $N_2 = 97$, $N_3 = 50$ ergibt $s = 328$ bzw. $p = 25375$

25. –

26. –

27. Durch Probieren: $x = 3$ und $x = 7$.