Lektion 2

Die Suche nach Sicherheit und modulares Rechnen

Menschen streben ständig nach mehr Sicherheit. Alle Anwendungen sollen so sicher wie nur möglich werden. Bei Kryptosystemen ist es nicht anders. Aber was verstehen wir unter Sicherheit im Zusammenhang mit Kryptosystemen? Sowohl der Sender als auch der Empfänger müssen damit rechnen, dass der verschickte Kryptotext einem Gegner in die Hände fallen kann (siehe Abbildung 2.1). Dieser Gegner wird **Kryptoanalyst** oder **Kryptoanalytiker** genannt. Wir verwenden diesen neutralen wissenschaftlichen Begriff, statt über Gegner oder Feinde zu sprechen, um den Kryptoanalytiker nicht in die Rolle des Bösewichts zu versetzen. In einem Krieg zum Beispiel haben beide Seiten ihre Sender, Empfänger und Kryptoanalytiker. Es ist also eine Frage der Sichtweise, wem man die positive und wem die negative Rolle zuordnet.

Auszug aus der Geschichte Im Zweiten Weltkrieg war der Engländer Alan Turing (1912–1954) ein Kryptoanalytiker im Dienst der Alliierten. Er war einer der Gründer der Informatik, denn er legte unter anderem den Begriff des Algorithmus exakt mathematisch fest. Mit seiner Definition von Algorithmen im Jahr 1936 datieren wir die Entstehung der Informatik als eigenständige Wissenschaftsdisziplin. Alan Turing knackte das Kryptosystem ENIGMA der deutschen Wehrmacht und ihm verdanken wir, dass das Ende des Zweiten Weltkriegs nicht noch später eingetreten ist.

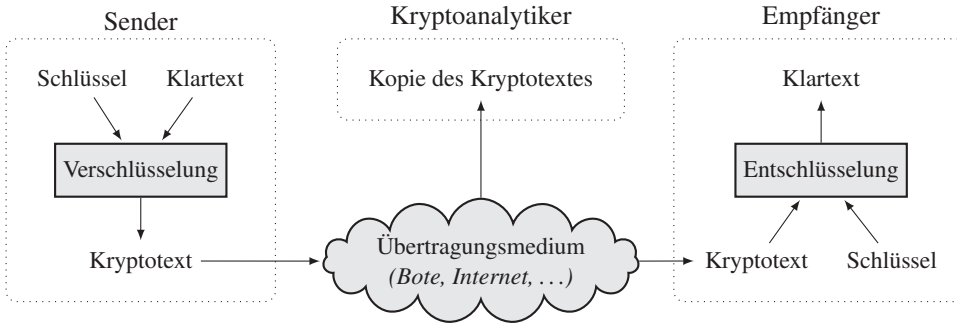

Abbildung 2.1 Dieses Kommunikationsschema zeigt die Übertragung einer verschlüsselten Nachricht (dem Kryptotext). Bei der Übertragung kann eine Kopie des Kryptotextes in die Hände einer unbefugten dritten Person – genannt Kryptoanalytiker – gelangen.

K. Freiermuth et al., *Einführung in die Kryptologie,* DOI 10.1007/978-3-8348-2269-7_2,

2.1 Kryptoanalyse und der Begriff der Sicherheit

Die Lehre der Geheimschriften nennt man **Kryptologie** (vom griechischen *kryptós*, „verborgen“, und *logos*, „Lehre“, „Kunde“). Die Aktivitäten der Kommunizierenden und Kryptoanalytiker teilen die Kryptologie in zwei Gebiete ein. Die **Kryptographie** (auch: Kryptografie; vom griechischen *kryptós*, „verborgen“, und *gráphein*, „schreiben“) ist die Wissenschaft der Entwicklung von Kryptosystemen, und die **Kryptoanalyse** ist die Lehre der Analyse von Geheimtexten und Kryptosystemen, die zum „Knacken“ der analysierten Kryptoysteme führen soll.

Damit ist die ganze Kryptologie ein intellektuelles Spiel zwischen Kryptosystemdesignern und Kryptoanalytikern. Die Designer versuchen clevere Kryptosysteme zu bauen, und die Kryptoanalytiker versuchen eines nach dem anderen zu knacken.

Für den Bau eines Kryptosystems ist der Begriff der **Sicherheit** von zentraler Bedeutung. Es ist aber schwierig, von der absoluten Sicherheit im Sinne der Unknackbarkeit eines Kryptosystems zu sprechen, wenn man gegen einen Kryptoanalytiker spielt, der geniale Ideen entwickeln kann. Deshalb hat sich auch das Verständnis für den Begriff der Sicherheit im Laufe der Zeit geändert, was die Entwicklung der Kryptographie wesentlich beeinflusst hat.

Intuitiv verstehen wir unter einem sicheren Kryptosystem ein System, bei dem die Geheimtexte ohne Kenntnis des Geheimnisses zwischen Sender und Empfänger nicht entschlüsselt werden können. Aber absolute Sicherheit gibt es im realen Leben nicht. Deswegen ist für uns Sicherheit nicht unbedingt die absolute Unmöglichkeit, Kryptosysteme zu knacken, sondern ein in vernünftiger Zeit unrealisierbarer Aufwand, der nötig ist, die Geheimtexte ohne Kenntnis des Geheimnisses zu entschlüsseln. Also ist man bestrebt, die Kryptosysteme so zu bauen, dass die Entschlüsselung für die Kryptoanalytiker so schwer ist wie die Suche nach einer Nadel in einem Heuhaufen.

Wir sehen, dass die Sicherheit mit der Geheimhaltung einer bestimmten Kenntnis verknüpft ist. Bei den Geheimschriften ist die Art der Chiffrierung (und damit auch der Dechiffrierung) das Geheimnis, bei den Kryptosystemen kam noch die Geheimhaltung des Schlüssels hinzu. Wenn die Sicherheit eines Kryptosystems auf der Geheimhaltung des Verschlüsselungsverfahrens basiert, dann sprechen wir von „security by obscurity“. Die Geheimhaltung des Verfahrens ist jedoch kein vernünftiges Kriterium für die Garantie der Sicherheit eines Kryptosystems. Der Grund dafür ist die Erfahrung, dass es nur eine Frage der Zeit ist, bis die Art der Verschlüsselung eines neuen Kryptosystems unbefugten Personen in die Hände fällt.

Deswegen formulierte schon im 19. Jahrhundert Auguste Kerkhoffs die folgende Sicherheitsanforderung, die als **Kerkhoffs-Prinzip der Sicherheit** bekannt ist:

> *Ein Kryptosystem ist sicher, wenn sich, trotz öffentlich bekanntem Verschlüsselungsverfahren, die ursprünglichen Klartexte nicht ohne die Kenntnis des Schlüssels aus den Kryptotexten ableiten lassen.*

Nach dieser Definition sind alle Geheimschriften, die wir als Kryptosysteme mit *nur einem* Schlüssel auffassen können, als unsicher zu betrachten. Das Kryptosystem CAESAR ist ebenfalls nicht sicher, denn es können alle möglichen 26 Schlüssel ohne großen Aufwand durchprobiert werden.

Damit erkennen wir, dass ein Kryptosystem nach dem Kerkhoffs-Prinzip nur dann als sicher betrachtet werden kann, wenn die Anzahl der Schlüssel so groß ist, dass es einen unrealisierbar großen Aufwand bedeuten würde alle auszuprobieren.

Aufgabe 2.1 Welche von den bisher vorgestellten Kryptosystemen kannst du nach dem Kerkhoffs-Prinzip als unsicher bezeichnen? Begründe deine Antwort.

Aufgabe 2.2 Die Spartaner wollen eine geheime Botschaft von Sparta nach Athen schicken. In dieser Nachricht ist die Strategie für die bevorstehende Schlacht mit mehreren tausend Zeichen ausführlich beschrieben. Die geplante Schlacht soll in drei Tagen beginnen. Um sicher zu gehen, dass die Botschaft in Athen ankommt, schicken die Spartaner mehrere Kopien der Botschaft nach Athen. Die Spartaner müssen aber damit rechnen, dass eine der Kopien in die Hände des Gegners kommt.

Das Ziel der Spartaner besteht nun darin, die Nachricht so zu verschlüsseln, dass der Gegner mehr als drei Tage benötigt um die abgefangene Nachricht zu entschlüsseln. Danach spielt es keine Rolle mehr, da mit dem Beginn der Schlacht der Plan sowieso öffentlich ist. Die Spartaner haben festgestellt, dass die Gegner nur einen einzigen Kryptoanalytiker haben: Lszqupt. Lszqupt ist sehr clever und arbeitet effizient. Für einen Versuch, den Kryptotext zu entschlüsseln, braucht er nur gerade eineinhalb Minuten. Ein Versuch entspricht dem Testen eines Schlüssels. Der unermüdliche Kryptoanalytiker kann drei Tage und drei Nächte am Stück arbeiten. Die Spartaner müssen auch damit rechnen, dass der clevere Lszqupt erahnen kann, welches Verschlüsselungsverfahren angewandt worden ist.

Die Spartaner entscheiden sich für das folgende Kryptosystem:

Kryptosystem 3TAGE

Klartextalphabet:	Lat
Geheimtextalphabet:	Lat
Schlüsselmenge:	(i, k, j), wobei $i, j \in \{0, 1, \ldots, 25\}$ und $k \in \{1, 2, \ldots, 100\}$
Verschlüsselung:	Die Verschlüsselung läuft in drei Schritten ab: 1. Verschlüssle den Klartext mit CAESAR und dem Schlüssel i zu $Text_1$. 2. Verschlüssle $Text_1$ mit SKYTALE und dem Schlüssel k zu $Text_2$. 3. Verschlüssle $Text_2$ mit CAESAR und dem Schlüssel j, um den endgültigen Kryptotext zu erhalten.

Beschreibe die Entschlüsselung, die vom mit 3TAGE verschlüsselten Kryptotext zum ursprünglichen Klartext führt. Weshalb bekommt man den richtigen Klartext? Haben die Spartaner eine gute Wahl getroffen?

Aufgabe 2.3 Die Wahrscheinlichkeit, dass Lszqupt mit seiner Kryptoanalyse erfolgreich ist, entspricht der Anzahl Versuche, die Lszqupt innerhalb von drei Tagen durchführt, um den Schlüssel

zu erraten, dividiert durch die Anzahl aller möglichen Schlüssel. Das Ziel ist nun, diese Wahrscheinlichkeit so klein wie möglich zu halten, damit die Chance auf einen Erfolg für Lszqupt möglichst gering ist. Was würdest du als Spartaner unternehmen, um die Erfolgswahrscheinlichkeit auf weniger als $\frac{1}{100}$ zu senken?

2.2 Modulare Addition

Wir haben erkannt, dass CAESAR auch für einen Kryptoanalytiker ohne Rechner leicht zu knacken ist. Wir werden CAESAR so verbessern, dass es für einen Unbefugten ohne Rechnerunterstützung aufwändiger wird, ohne Kenntnis des Schlüssel den Klartext herzuleiten. Dabei lernen wir auch erste Ideen des **modularen Rechnens** kennen, mit dessen Hilfe wir später pfiffigere Kryptosysteme verstehen können.

Wenn mit natürlichen oder ganzen Zahlen gearbeitet wird, verwendet man oft die sogenannte **ganzzahlige Division**. Zum Beispiel

$$72 : 5 = 14 \quad \text{Rest } 2.$$

Diese Gleichung bedeutet, dass sich 72 auch durch die folgende Formel ausdrücken lässt:

$$72 = 14 \cdot 5 + 2,$$

weil die 5 genau 14-mal in 72 vorkommt und 2 der Rest der Division $72 : 5$ ist. Das Resultat 14 der Division $72 : 5$ drücken wir durch

$$72 \text{ div } 5$$

aus und den Rest 2 bezeichnen wir mit

$$72 \bmod 5.$$

Es gilt also

$$72 = (72 \text{ div } 5) \cdot 5 + 72 \bmod 5\,.$$

Ganz allgemein bezeichnen wir für zwei beliebige natürliche Zahlen b und a (mit $a \neq 0$) das Resultat der ganzzahligen Division von b durch a mit

$$b \,\mathbf{div}\, a$$

und den Rest der ganzzahligen Division von b durch a mit

$$b \,\mathbf{mod}\, a.$$

Weil $b \bmod a$ der Rest der ganzzahligen Division durch a ist, muss $b \bmod a$ immer kleiner als a sein. Mit dieser Bezeichnung gilt

$$b = (b \text{ div } a) \cdot a + b \bmod a.$$

für alle natürlichen Zahlen b und a, wobei $a \neq 0$.

Aufgabe 2.4 Bestimme $b \operatorname{div} a$ und $b \bmod a$ für die folgenden natürlichen Zahlen b, a (mit $a \neq 0$).

(a) $b = 72$, $a = 9$

(b) $b = 225$, $a = 3$

(c) $b = 257$, $a = 8$

(d) $b = 13$, $a = 25$

Eine natürliche Zahl a ($a \neq 0$) **teilt** eine natürliche Zahl b, wenn es eine natürliche Zahl k gibt, so dass

$$b = k \cdot a.$$

In anderen Worten, a teilt b, wenn

$$b \bmod a = 0.$$

Man sagt, dass a ein **Teiler** von b ist und schreibt $a \mid b$.

So wie wir die üblichen arithmetischen Operatoren $+$, $-$, $\cdot$, und $/$ verwenden, können solche Operatoren mit ähnlicher Bedeutung auch für das modulare Rechnen eingeführt werden. Die Operation

$$\oplus_a$$

wird für jede natürliche Zahl a unterschiedlich von 0 und zwei natürliche Zahlen x und y durch

$$\boxed{x \oplus_a y = (x + y) \bmod a}$$

definiert. Somit ist $\oplus_a$ eine Operation auf natürlichen Zahlen, deren Resultat immer kleiner als a ist. Zum Beispiel rechnen wir

$$15 \oplus_{26} 17 = (15 + 17) \bmod 26 = 32 \bmod 26 = 6\,.$$

Später werden wir diesen Operator auf negative ganze Zahlen erweitern. Dazu brauchen wir aber noch mehr Hintergrundwissen. Vorerst betrachten wir die modulare Addition nur für natürliche Zahlen.

Aufgabe 2.5 Bestimme die Resultate der folgenden Rechnungen:

(a) $25 \oplus_{26} 25$

(b) $0 \oplus_{26} 19$

(c) $231 \oplus_3 222$

(d) $1378 \oplus_{10} 24\,795$

(e) $13\,874 \oplus_2 123$

Aufgabe 2.6 Beantworte die folgenden Fragen:

(a) Es ist 9 Uhr. Wie spät ist es nach 100 Stunden?

(b) Heute sei Mittwoch. Welchen Wochentag haben wir in 53 Tagen?

(c) Es sei September. In welchem Monat sind wir in 47 Monaten?

Aufgabe 2.7 Peter und Hans führen eine kleine Kneipe in Engelberg. Normalerweise läuft alles ziemlich ruhig, heute aber bekommen die beiden Besuch vom Turnverein Bümpliz. Die zwei Wirte haben während drei Stunden alle Hände voll zu tun und stellen deshalb die leeren Flaschen einfach in die Küche. So herrscht am Abend natürlich das große Chaos. Als sich die Gäste auf den Heimweg gemacht haben, müssen die zahlreichen leeren Flaschen in die Harasse versorgt werden, welche am nächsten Morgen vom Getränkehändler abgeholt werden. Peter und Hans machen sich an die Arbeit, sie arbeiten beide gleich schnell. In jedem Harass haben genau 12 Flaschen Platz, und der Händler nimmt nur volle Harasse an. In der Küche liegen 124 Flaschen herum.

(a) Wie viele Harasse füllen die beiden Wirte je, wenn sie die Arbeit gemeinsam in Angriff nehmen? Wie viele Flaschen bleiben übrig?

(b) Wie viele Harasse würde Peter füllen, wenn er alleine arbeiten würde? Bleiben gleich viele Flaschen übrig?

(c) Hans findet im Keller noch 39 Flaschen vom Vortag. Wie viele Harasse kann er mit diesen Flaschen füllen? Wie viele Flaschen bleiben übrig?

(d) Kann er mit den aus der Küche und dem Keller übriggebliebenen Flaschen noch einen Harass füllen?

(e) Am darauffolgenden Tag hat Hans starke Rückenschmerzen vom Flaschen Einfüllen. Deshalb bleibt er zu Hause. Peter ist alleine in der Kneipe, möchte aber am Abend nicht alle Harasse abfüllen. An diesem Tag stehen 51 Flaschen herum. Er rechnet nun aus, wie viele Flaschen er in die Harasse einfüllen muss, damit Peter am nächsten Tag genau die gleiche Anzahl von Flaschen in die Harasse füllen muss. Wie viele Harasse muss jeder füllen?

Die Operation $\oplus_a$ nennen wir **Addition modulo *a***. Wozu kann so etwas nützlich sein? CAESAR arbeitet mit der Addition modulo 26 auf der Ordnung der Symbole des Alphabets Lat. Die Ordnung der Symbole aus Lat haben wir wie folgt festgelegt:

$$\mathrm{Ord}(\mathrm{A}) = 0,\ \mathrm{Ord}(\mathrm{B}) = 1,\ \mathrm{Ord}(\mathrm{C}) = 2,\ \ldots,\ \mathrm{Ord}(\mathrm{Y}) = 24,\ \mathrm{Ord}(\mathrm{Z}) = 25\,.$$

Somit kann für jedes Symbol $\square \in \mathrm{Lat}$ und für jeden Schlüssel $s \in \{0, 1, 2, \ldots, 25\}$ die Verschlüsselung mittels CAESAR wie folgt beschrieben werden:

$$\mathrm{Ver}(\square, s) = \triangle, \qquad \text{wobei } \mathrm{Ord}(\triangle) = \mathrm{Ord}(\square) \oplus_{26} s.$$

In Worten: Wir verschlüsseln jedes Symbol $\square$ des lateinischen Alphabets mit dem Schlüssel s durch das Symbol $\triangle$ mit der Ordnung $(\mathrm{Ord}(\square) + s) \bmod 26$. Diese Addition modulo 26 entspricht genau der Verschiebung der Scheibe um den Wert k des Schlüssels. Somit gilt zum Beispiel

$$\mathrm{Ver}(\mathrm{C}, 24) = \mathrm{A},$$

weil

$$\begin{aligned}\mathrm{Ord(C)} \oplus_{26} 24 &= \big(\mathrm{Ord(C)} + 24\big) \bmod 26\\ &= (2 + 24) \bmod 26\\ &= 26 \bmod 26\\ &= 0\,.\end{aligned}$$

Für zwei beliebige natürliche Zahlen x und y und eine natürliche Zahl $a \neq 0$ haben wir den Operator $\oplus_a$ wie folgt definiert:

$$x \oplus_a y = (x + y) \bmod a\,.$$

Zuerst soll also $x + y$ berechnet und anschliessend soll die Summe durch a dividiert werden. Der Rest dieser Division ist dann das Resultat. In einer Gleichung mit mehr als einem Operator $\oplus_a$, wie zum Beispiel in

$$x \oplus_a y \oplus_a z = (x + y + z) \bmod a,$$

kann diese Vorgehensweise jedoch sehr aufwändig werden. Vor allem erschweren große Zahlen x und y das Rechnen, da durch manche arithmetische Operationen noch größere Zahlen erzeugt werden und danach ein relativ kleiner Rest (der Rest ist immer kleiner als a) berechnet wird. Um das Auftreten von unnötig großen Zahlen zu vermeiden, können vor jeder arithmetischen Operation die Operanden x und y kleiner als der Wert a gemacht werden, und zwar durch modulares Rechnen mit modulo a. Anstatt die Summe von x und y modulo a zu berechnen, kann nämlich genauso gut vor der Berechnung der Summe jeder Summand einzeln modulo a gerechnet werden. Es gilt im Allgemeinen das folgende Gesetz (der Beweis wird weiter unten folgen):

$$(x + y) \bmod a = \big((x \bmod a) + (y \bmod a)\big) \bmod a.$$

Das heißt, die Summe von zwei Zahlen (x und y) modulo a ist gleich der Summe von (x modulo a) und (y modulo a) modulo a. Nicht zu vergessen ist, dass das Resultat von $(x \bmod a) + (y \bmod a)$ auch noch modulo a gerechnet werden muss. Mithilfe dieses Gesetzes kann vor allem bei großen Zahlen x und y und wiederholter Anwendung der Operation modulo a der Rechenaufwand um einiges verringert werden, da die Zwischenresultate nie größer als a werden.

Zum Beispiel kann der Ausdruck

$$2287 \oplus_3 1322$$

wie folgt nach der Definition von $\oplus_3$ berechnet werden:

$$\begin{aligned}2287 \oplus_3 1322 &= (2287 + 1322) \bmod 3\\ &= 3609 \bmod 3\\ &= 0.\end{aligned}$$

Mit Hilfe des oben eingeführten Gesetzes kann die Berechnung vereinfacht werden:

$$\begin{aligned} 2287 \oplus_3 1322 &= \big((2287 \bmod 3) + (1322 \bmod 3)\big) \bmod 3 \\ &= (1 + 2) \bmod 3 \\ &= 3 \bmod 3 \\ &= 0. \end{aligned}$$

Aufgabe 2.8 Vergleiche jeweils die Resultate der beiden Ausdrücke:

(a) $(13\,257 + 178\,791) \bmod 77$ und $\big((13\,257 \bmod 77) + (178\,791) \bmod 77)\big) \bmod 77$

(b) $(2\,087\,644 + 137\,822) \bmod 4$ und $\big((2\,087\,644 \bmod 4) + (137\,822 \bmod 4)\big) \bmod 4$

(c) $(37\,872\,949 + 13\,287) \bmod 10$ und $\big((37\,872\,949 \bmod 10) + (13\,287 \bmod 10)\big) \bmod 10$

Die Lösungen der Terme in den Teilaufgaben von Aufgabe 2.8 führen immer zum gleichen Resultat. Jetzt werden wir zeigen, dass dies tatsächlich allgemein gilt. Dafür brauchen wir aber noch ein weiteres Gesetz, welches wir zuerst zeigen werden.

Der Operator $\oplus_a$ ist für jede positive ganze Zahl a definiert, und im Folgenden sind x, y und z natürliche Zahlen. Grundsätzlich gilt, dass sich ein Wert z mod a nicht ändert, wenn zu z ein Vielfaches von a, also $m \cdot a$, für eine beliebige natürliche Zahl m addiert wird. Dass der Ausdruck $(z + m \cdot a)$ mod a immer gleich z mod a ist, kann wie folgt begründet werden: Der Term $(z + m \cdot a)$ mod a beschreibt den Rest nach der Division von $z + m \cdot a$ durch a. Den Summanden z kann man als ein Vielfaches von a mit einem Rest r ausdrücken, wenn z mod $a = r$ ist. Der Rest r ist nicht durch a teilbar. Es gilt also

$$z = n \cdot a + r.$$

Damit können wir das z in $(z + m \cdot a)$ mod a ersetzen:

$$\begin{aligned} (z + m \cdot a) \bmod a &= (n \cdot a + r + m \cdot a) \bmod a \\ &= \big(a \cdot (m + n) + r\big) \bmod a \qquad \{a \text{ ausgeklammert}\} \end{aligned}$$

Der erste Summand $a \cdot (m + n)$ ist durch a teilbar, also ist der Rest bei der Teilung von $z + m \cdot a$ durch a genau der Rest r. Das heißt, es gilt

$$(z + m \cdot a) \bmod a = r$$

und somit

$$(z + m \cdot a) \bmod a = r = z \bmod a.$$

Dies ist bereits das erste Gesetz (M1) des modularen Rechnens. Für alle natürlichen Zahlen z und m und jede positive ganze Zahl a gilt

$$\boxed{z \bmod a = (z + m \cdot a) \bmod a.} \qquad \text{(M1)}$$

Mit Hilfe dieses Gesetzes können wir das zweite Gesetz

$$\boxed{(x+y) \bmod a = (x \bmod a + y \bmod a) \bmod a} \tag{M2}$$

wie folgt herleiten:

$$\begin{aligned}
(x+y) \bmod a &= (a \cdot x \operatorname{div} a + x \bmod a + a \cdot y \operatorname{div} a + y \bmod a) \bmod a \\
&\quad \{\text{weil } x = a \cdot x \operatorname{div} a + x \bmod a \text{ und } y = a \cdot y \operatorname{div} a + y \bmod a\} \\
&= \big(a \cdot (x \operatorname{div} a + y \operatorname{div} a) + x \bmod a + y \bmod a\big) \bmod a \\
&\quad \{\text{nach Kommutativ- und Distributivgesetz}\} \\
&= (x \bmod a + y \bmod a) \bmod a \\
&\quad \left\{\begin{array}{l}\text{nach Gesetz (M1),} \\ \text{weil } a \cdot (x \operatorname{div} a + y \operatorname{div} a) \text{ ein Vielfaches von } a \text{ ist.}\end{array}\right\}
\end{aligned}$$

Das Gesetz (M2) besagt auch ganz allgemein, dass eine modulare Summe von beliebig vielen Zahlen auf zwei unterschiedliche Arten berechnet werden kann: Eine Möglichkeit ist, zuerst alle Summanden zu addieren und für die Summe anschließend modulo a den Rest zu bestimmen. Die andere Möglichkeit ist, zuerst für alle Summanden modulo a den Rest zu bestimmen und die erhaltenen Reste anschließend zu addieren. Sobald man aber beim Addieren eine Teilsumme erhält, die größer als a ist, muss für diese Teilsumme wiederum der Rest modulo a berechnet werden, um die Summanden klein zu halten.

Aufgabe 2.9 Das Gesetz (M2) sieht für die Berechnung der Summe von drei Zahlen x, y und z wie folgt aus:

$$(x+y+z) \bmod a = \big((x \bmod a + y \bmod a) \bmod a + z \bmod a\big) \bmod a.$$

Wie kann das Gesetz für die Berechnung der Summe von vier Zahlen w, x, y und z formuliert werden?

Aufgabe 2.10 Analog zum Gesetz (M2) für die Addition gibt es ein Gesetz für die Subtraktion: Für zwei natürliche Zahlen x und y mit $x \geq y$ gilt:

$$(x-y) \bmod a = (a + x \bmod a - y \bmod a) \bmod a.$$

(a) Prüfe das Gesetz der Subtraktion für die Zahlen $a = 11$, $x = 60$ und $y = 40$.

(b) Wie kann das Gesetz der Subtraktion hergeleitet werden? (Vergleiche dazu die Herleitung des Gesetzes (M2).)

Hinweis für die Lehrperson Der Rest dieser Lektion kann auch später behandelt werden, weil die darin vermittelten Kenntnisse erst in Lektion 7 gebraucht werden. Der Grund, weshalb wir es hier behandeln, liegt darin, dass die für das Verständnis des Buches notwendigen mathematischen Grundlagen über alle Lektionen so verteilt werden, dass lange rein mathematische Lektionen vermieden werden.

2.3 Algebraische Strukturen

Es ist möglich, mit dem Operator $\oplus_{26}$ die CAESAR-Verschlüsselung von Buchstaben mathematisch zu beschreiben. Wenn das Symbol $\square$ des Klartextalphabets durch das Symbol $\triangle$ des Kryptotextalphabets ersetzt wird, dann gilt

$$\text{Ord}(\triangle) = \text{Ord}(\square) \oplus_{26} s,$$

wobei s der Schlüssel ist. Hilft uns dieser Operator aber auch für die Beschreibung der Entschlüsselung von einem mit CAESAR verschlüsselten Kryptotext? Auf den ersten Blick mag es nicht so aussehen.

Schauen wir uns ein konkretes Beispiel an. Angenommen, das Symbol D mit der Ordnung $\text{Ord}(\text{D}) = 3$ im Kryptotextalphabet wurde mit dem Schlüssel $s = 24$ verschlüsselt. Das heißt, ein uns noch unbekannter Buchstabe wurde durch den um 24 Stellen weiter hinten liegenden Buchstaben D ersetzt. Um diese Verschlüsselung rückgängig zu machen, rechnen wir intuitiv

$$\text{Ord}(\text{D}) - s = 4 - 24 = -20.$$

Das Prinzip der Verschiebung besagt, dass der resultierende Buchstabe der zwanzigste Buchstabe vom Ende des Alphabets her gesehen ist. Zum Entschlüsseln haben wir keine Addition, sondern die Subtraktion verwendet, und deshalb erhalten wir eine negative Zahl. Alle Resultate bei der Anwendung von $\oplus_{26}$ sind aber natürliche Zahlen von 0 bis 25, also nicht negative Zahlen. Dies scheint uns auf den ersten Blick zum Verhängnis zu werden. Wir werden jedoch gleich sehen, wie mit dem Operator $\oplus_{26}$ trotzdem entschlüsselt werden kann. Um genau zu verstehen, wie das funktioniert, müssen wir zuerst ein paar wenige mathematische Grundlagen aus dem Bereich der Algebra einführen.

Wir bezeichnen die Menge der ganzen Zahlen mit $\mathbb{Z}$, die Menge aller rationalen Zahlen mit $\mathbb{Q}$, und die Menge aller reellen Zahlen mit $\mathbb{R}$. Wie schon früher erwähnt, sind $\mathbb{Z}^+$, $\mathbb{Q}^+$ und $\mathbb{R}^+$ die Menge der positiven ganzen Zahlen, die Menge der positiven rationalen Zahlen und die Menge der positiven reellen Zahlen. In der Mathematik arbeitet man mit unterschiedlichen Zahlensystemen. Wenn eine Menge S von Zahlen zusammen mit einer oder mehreren Operationen vorliegt und alle Resultate der Operationen auf den Zahlen aus S wieder in der Zahlenmenge S liegen, dann (und nur dann) sprechen wir von einer **algebraischen Struktur**. Im Folgenden betrachten wir **binäre Operationen**, die nur zwei Operanden haben. Als Beispiel von binären Operationen kennt ihr die **arithmetischen Operationen** mit den Operatoren $+$, $-$, $\cdot$ und $/$. Den Begriff der **algebraischen Struktur** kann man formal wie folgt ausdrücken:

> *Sei S eine beliebige Zahlenmenge[1] und seien σ_1, σ_2, σ_3, …, σ_k beliebige binäre Operationen, die über alle $a, b \in S$ definiert sind (das heißt, der Wert $a\,\sigma_i\,b$ ist für alle $i \in \{1, 2, 3, \ldots, k\}$ eindeutig definiert).*

[1] In der Mathematik wird die algebraische Struktur mit einer beliebigen Menge definiert. Man könnte beispielsweise auch Mengen von Strecken oder noch ausgefallenere Mengen betrachten. Wir möchten uns aber in diesem Buch auf Zahlenmengen beschränken.

http://www.springer.com/978-3-8348-1855-3

Einführung in die Kryptologie
Lehrbuch für Unterricht und Selbststudium
Freiermuth, K.; Hromkovič, J.; Keller, L.; Steffen, B.
2014, IX, 399 S. 86 Abb., Softcover
ISBN: 978-3-8348-1855-3