2 Grundbegriffe der Zahlentheorie und der Algebra

In diesem Abschnitt sollen Sie die Begriffe bzw. Aussagen

- Teiler bzw. größter gemeinsamer Teiler (ggT)
- Primzahl
- (abelsche) Gruppe, Untergruppe, Ordnung einer Gruppe/ Elements
- inverses Element, neutrales Element
- Satz von Euler bzw. „Kleiner Fermat“

kennen und üben,

- Beweise mit Hilfe der vollständigen Induktion durchzuführen;
- mit Hilfe des euklidischen Algorithmus den ggT zweier ganzer Zahlen zu berechnen;
- in Restklassen zu rechnen (Modulorechnung);
- nachzuprüfen, dass es sich bei einer Menge mit Verknüpfung um eine Gruppe handelt;
- Untergruppen, Ordnung einer Gruppe bzw. eines Elements zu bestimmen;
- inverse Elemente einer Gruppe auszurechnen.

Motivation

Wir beschäftigen uns mit einigen grundlegenden Themen der Zahlentheorie und der Algebra, um am Ende dieses Abschnitts in der Lage zu sein, Prinzipien der Verschlüsselung und einfache Anwendungen der Modulorechnung in der Informatik zu verstehen.
Ein wichtiges Grundprinzip der Verschlüsselung besteht darin, eine Botschaft mit Hilfe einer sogenannten Ein-Weg-Funktion zu verschlüsseln. Eine Ein-Weg-Funktion ist eine Funktion, die leicht zu berechnen ist; deren Umkehrfunktion aber ohne Zusatzinformationen sehr schwierig bzw. sehr zeitaufwendig zu bestimmen ist. Ein Beispiel für eine solche Ein-Weg-Funktion ist die Multiplikation von Primzahlen. Das Produkt von zwei Primzahlen ist sehr leicht zu berechnen. Die Zerlegung eines Produktes in ihre Primfaktoren ist aber sehr zeitaufwendig, vor allem natürlich, wenn die Primfaktoren sehr große Zahlen sind.
Die Modulorechnung spielt in der Informatik eine wichtige Rolle, da der Speicherplatz für eine Zahl zwangsläufig beschränkt ist, so dass man sich bei der Verarbeitung sehr großer Zahlen, die die zulässigen Stellen überschreiten, der Modulorechnung behilft.
Zunächst müssen wir uns mit einigen Eigenschaften der ganzen Zahlen beschäftigen,

insbesondere mit dem Teilen mit Rest, der Primfaktorzerlegung und dem größten gemeinsamen Teiler.

2.1 Teiler und Division mit Rest

Definition 2.1

Eine Zahl $d \in \mathbb{N}$ heißt **Teiler** einer Zahl $a \in \mathbb{Z}$, falls ein $k \in \mathbb{Z}$ existiert, so dass

$$a = k \cdot d.$$

Man schreibt:

$$d \mid a \quad \text{lies:“}d \text{ teilt } a\text{“}$$

und nennt a ein **Vielfaches** von d.

Definition 2.2

Sei $d \in \mathbb{N}$ ein Teiler von $a, b \in \mathbb{Z}$. Falls für jeden Teiler d' von $a, b \in \mathbb{Z}$ gilt, dass $d' \leq d$, dann nennt man d **größter gemeinsamer Teiler** von a, b und schreibt $ggT(a, b) = d$.
Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremd** (oder relativ prim), falls gilt:

$$ggT(a, b) = 1.$$

Definition 2.3

Eine Zahl $p \in \mathbb{N}$ heißt **Primzahl**, falls gilt:

$$\forall d \in \mathbb{N} : \; d \mid p \quad \Rightarrow \quad d = 1 \text{ oder } d = p.$$

Satz 2.4

Zu jeder Zahl $n \in \mathbb{N}, n \geq 2$ existieren Primzahlen $p_1 < p_2 < \cdots < p_k$ und $a_1, \ldots, a_k \in \mathbb{N}$, so dass

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_k^{a_k}.$$

Diese Faktorisierung einer natürlichen Zahl heißt **Primfaktorzerlegung**. Sie ist eindeutig.

Beispiel 2.5

$$42 = 2 \cdot 3 \cdot 7,\ 28 = 2 \cdot 2 \cdot 7,\ 32 = 2^5.$$

Definition 2.6

Seien $a, b \in \mathbb{Z}$. Dann existiert genau eine Darstellung

$$a = bq + r$$

mit $q \in \mathbb{Z}$ und $0 \leq r < |b|$. Die Zahl r heißt **Rest** und b der Divisor oder Teiler. Man schreibt kurz:

$$a = r \mod b.$$

Beispiel 2.7

Seien $15, 4$ gegeben. Es ist $4 \not| 15$, also $15 = 3 \cdot 4 + 3$ bzw. $15 = 3 \mod 4$.

2.2 Euklidischer Algorithmus

Für kleine Zahlen berechnet man den ggT meist mit Hilfe der Primfaktorzerlegung. Für große Zahlen ist es aber schwierig und zeitaufwendig, die Primfaktorzerlegung zu berechnen. Hier eignet sich der euklidische Algorithmus besser, um den größten gemeinsamen Teiler zu bestimmen:

2.2.1 Euklidischer Algorithmus

1: **Input:** $a, b \in \mathbb{Z}$,$a \geq b$
2: Berechne $r = a - bq$, $0 \leq r < |b|$.
3: **if** r=0 **then**
4: return $d = b$.
5: **while** $r \neq 0$ **do**
6: $a = b$;
7: $b = r$;
8: Berechne $r = a - bq$;
9: return $d = b$.

Beispiel 2.8

Wir berechnen den $ggT(127, 24)$:

$$\begin{aligned} 127 &= 5 \cdot 24 + 7 \\ 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Wenn der Rest der Divison Null ist, endet der Algorithmus. Es ist $ggT(127, 24) = 1$, die Zahlen sind teilerfremd.

Beweis. Um zu beweisen, dass der Algorithmus funktioniert, überlegen wir uns zunächst, dass er immer abbricht: Der Rest r, der in jedem Iterationsschritt berechnet wird, ist eine nichtnegative ganze Zahl – $r \geq 0$–, die in jedem Schritt kleiner wird. Deswegen muss irgendwann gelten $r = 0$ und der Algorithmus endet.
Um zu beweisen, dass der Algorithmus immer den ggT berechnet, zeigen wir zunächst, dass die berechnete Zahl d den Input a, b teilt. Dafür setzen wir $a = r_0$ und $b = r_1$ und schreiben den Algorithmus mit Hilfe von Indizes. Da wir bereits wissen, dass der Algorithmus endlich ist, existiert ein $j \in \mathbb{N}$, so dass:

$$\begin{aligned} r_0 &= k_1 r_1 + r_2 \\ r_1 &= k_2 r_2 + r_3 \\ &\vdots \\ r_{j-2} &= k_{j-1} r_{j-1} + r_j \\ r_{j-1} &= k_j r_j \end{aligned}$$

Aus der letzten Zeile folgt: $r_j \mid r_{j-1}$. In der vorletzten Zeile stehen die Summanden $k_{j-1}r_{j-1}$ und r_j. Beide werden natürlich von r_j geteilt:

$$r_j \mid r_j \text{ und } r_j \mid k_{j-1}r_{j-1} \quad \Rightarrow \quad r_j \mid r_{j-2}.$$

Dieses Argument läßt sich iterativ auf alle Zeilen anwenden, so dass wir

$$r_j \mid r_1 = b \text{ und } r_j \mid r_0 = a$$

erhalten. Der Output d ist also ein Teiler von a, b.
Wir zeigen jetzt, dass es sich auch um den größten Teiler handelt: Sei d' ein beliebiger gemeinsamer Teiler von a, b, dann folgt aus der ersten Zeile

$$r_0 = k_1 r_1 + r_2 \text{ und } d' \mid r_1 \text{ und } d' \mid r_0 \quad \Rightarrow \quad d' \mid r_2.$$

Dieses Argument läßt sich wieder iterativ auf jede Zeile anwenden, und es folgt, dass $d' \mid r_j$, also $d' \mid d$. Wenn aber d' die Zahl d teilt, dann ist $d' \leq d$ und damit ist $d = ggT(a, b)$. □

2.2.2 Erweiterter Euklidischer Algorithmus

1: **Input:** $a, b \in \mathbb{Z}$, $a \geq b$.
2: Setze $x_0 = 0$,$x_1 = 1$,$y_0 = 1$, $y_1 = 0$.
3: Berechne $r = a - k \cdot b$,$0 \leq r < |b|$.
4: **if** $r = 0$ **then**
5: Setze $ggT(a, b) = b$,$x = x_0$,$y = y_0$ und return.
6: **while** $r \neq 0$ **do**
7: Setze $x_2 = x_0 - kx_1$, $y_2 = y_0 - ky_1$, $a = b$,$b = r$.
8: Berechne $r = a - k \cdot b$, $0 \leq r < |b|$.
9: Setze $x_0 = x_1, x_1 = x_2$, $y_0 = y_1$,$y_1 = y_2$.
10: return $x = x_0$,$y = y_0$ und $ggT(a, b) = b$.

Beispiel 2.9

Wir berechnen mit Hilfe des erweiterten euklidischen Algorithmus den $d = ggT(104, 47)$und Zahlen $x, y \in \mathbb{Z}$, so dass $d = ax + by$. Die Tabelle können Sie auch ohne die ersten beiden Spalten führen. Die erste Spalte nummeriert nur die Zeilen bzw. Variablen. Wir setzen $r_0 = a$ und $r_1 = b$ und rechnen immer für $i \geq 1$:

$$r_{i+1} = r_{i-1} - k_i r_i, \quad x_{i+1} = x_{i-1} - k_i x_i, \quad y_{i+1} = y_{i-1} - k_i y_i, \; i = i + 1.$$

i	a	b	x	y	k
0	104	47	1	0	-
1	47	10	0	1	2
2	10	7	1	-2	4
3	7	3	-4	9	1
4	3	1	5	-11	2
5	1	0	-14	31	3

Tabelle 2.1 Erweiterter eukldischer Algorithmus

Sobald der Rest $b = 0$ ist, endet der Algorithmus. Wir lesen in der letzte Zeile ab, dass $1 = ggT(104, 47)$ und $1 = (-14) \cdot 104 + 31 \cdot 47$ ist.

Die folgende sehr wichtige Aussage läßt sich leicht mit Hilfe des erweiterten euklidischen Algorithmus zeigen:

Satz 2.10

Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd. $\Leftrightarrow \exists\, x, y \in \mathbb{Z} :\ 1 = ax + by$.

2.3 Restklassen $\mathbb{Z}_n$

Definition 2.11

Sei $n \in \mathbb{N}$ gegeben und die Äquivalenzrelation

$$a \equiv_n b \quad :\Leftrightarrow \quad a - b = 0 \mod n.$$

Wir bezeichnen die Äquivalenzklassen

$$[r] = \left\{ r + kn \;\middle|\; k \in \mathbb{Z} \right\}, \quad 0 \leq r < n$$

als **Restklassen**, da sie alle diejenigen Zahlen zusammenfassen, die bei Division mit n denselben Rest r besitzen.
Die Menge von Restklassen bezeichnen wir mit $\mathbb{Z}_n$:

$$\mathbb{Z}_n := \{[0], [1], [2], \ldots, [n-1]\}.$$

Bemerkung 2.1. *Wenn aus dem Zusammenhang klar ist, dass es sich um die Restklassen handelt, lässt man häufig die Klammern weg und schreibt kurz*

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

Satz 2.12

Sei $n \in \mathbb{N}$. Die Äquivalenzrelation $\equiv_n$ besitzt genau n Äquivalenzklassen, nämlich

$$\begin{aligned} [0] &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\}, \\ [1] &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}, \ldots \\ [n-1] &= \{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}. \end{aligned}$$

Es gilt also $|\mathbb{Z}_n| = n$.

Beispiel 2.13

Zu $n = 1$ gibt es nur eine Restklasse, da jede ganze Zahl durch 1 teilbar ist. Also ist $\mathbb{Z}_1 = \{[0]\}$.
Zu $n = 2$ gibt es genau zwei Restklassen, da jede gerade Zahl durch 2 teilbar ist, jede ungerade Zahl mit Rest 1 durch 2 teilbar ist. Also ist $\mathbb{Z}_2 = \{[0], [1]\}$.

Beispiel 2.14

Die Restklassen zu $4 \in \mathbb{N}$ lauten

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\} = \left\{4k \;\middle|\; k \in \mathbb{Z}\right\}$$
$$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\} = \left\{4k+1 \;\middle|\; k \in \mathbb{Z}\right\}$$
$$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\} = \left\{4k+2 \;\middle|\; k \in \mathbb{Z}\right\}$$
$$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\} = \left\{4k+3 \;\middle|\; k \in \mathbb{Z}\right\}$$

Man kann mit Restklassen wie mit ganzen Zahlen rechnen:

Satz 2.15

Sei $n \in \mathbb{N}$. Dann gilt für alle $a, b \in \mathbb{Z}$:

$$a \mod n + b \mod n = (a+b) \mod n,$$

$$(a \mod n) \cdot (b \mod n) = (a \cdot b) \mod n.$$

Beispiel 2.16

1. Es ist $(38 + 22) \mod 9 = 60 \mod 9 = 6 \mod 9$. Leichter lässt es sich unter Anwendung der obigen Rechenregeln rechnen als:

$$\begin{aligned} 38 \mod 9 + 22 \mod 9 &= 2 \mod 9 + 4 \mod 9 \\ &= 6 \mod 9 \end{aligned}$$

   Ebenso ist $(38 \cdot 22) \mod 9$ sehr viel besser als

$$\begin{aligned} (38 \mod 9) \cdot (22 \mod 9) &= (2 \mod 9) \cdot (4 \mod 9) \\ &= 8 \mod 9 \end{aligned}$$

   auszurechnen.

2.

$$\begin{aligned}(101 + 234) \mod 5 &= 101 \mod 5 + 234 \mod 5 \\ &= 1 \mod 5 + 4 \mod 5 \\ &= 5 \mod 5\end{aligned}$$

Ebenso rechnet man

$$\begin{aligned}(101 \cdot 234) \mod 5 &= (101 \mod 5)(234 \mod 5) \\ &= 4 \mod 5\end{aligned}$$

Besonders hilfreich sind die Rechenregeln zur Berechnung von großen Potenzen:

Beispiel 2.17

Es soll $7^{66} \mod 13$ berechnet werden. Wir zerlegen die Potenz in $66 = 2^6 + 2$ und berechnen zunächst $7^2 \mod 13$ und die entsprechenden Zweierpotenzen, indem wir das Ergebnis jeweils quadrieren und wieder $\mod 13$ rechnen.

$$\begin{aligned}7^2 &\mod 13 = 10 \mod 13 \\ 7^4 &\mod 13 = (7^2 \mod 13)^2 = 100 \mod 13 = 9 \mod 13 \\ 7^8 &\mod 13 = 81 \mod 13 = 3 \mod 13 \\ 7^{16} &\mod 13 = 9 \mod 13 \\ 7^{32} &\mod 13 = 81 \mod 13 = 3 \mod 13 \\ 7^{64} &\mod 13 = 9 \mod 13\end{aligned}$$

Also erhalten wir $7^{66} \mod 13 = (7^{64} \mod 13) \cdot (7^2 \mod 13) = (9 \mod 13)(10 \mod 13) = 12 \mod 13$.

2.4 Teilbarkeitsregeln

Mit Hilfe der Modulorechnung kann man relativ leicht Teilbarkeitsregeln beweisen.

Teilbarkeit durch 3

Beispiel 2.18

Ist 1782 durch 3 teilbar?

Die Teilbarkeit können wir schreiben als

$$3 \mid 1782 \quad \Leftrightarrow \quad 1782 = 0 \mod 3.$$

Wir können 1782 als Summe von Zehnerpotenzen schreiben und erhalten

$$1782 = 1 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 2.$$

Es ist $10^k \mod 3 = 1 \mod 3$ für jede Zehnerpotenz. Also bekommen wir

$$\begin{aligned} 1782 \mod 3 &= \left(1 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 2\right) \mod 3 \\ &= 1 \mod 3 + 7 \mod 3 + 8 \mod 3 + 2 \mod 3 \\ &= (1 + 7 + 8 + 2) \mod 3 \end{aligned}$$

Also ist eine Zahl genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Satz 2.19

Sei $a = \sum_{k=0}^{n} a_k 10^k$ eine natürliche Zahl. Dann gilt

$$a = 0 \mod 3 \quad \Leftrightarrow \quad \left(\sum_{k=0}^{n} a_k\right) \mod 3 = 0 \mod 3.$$

Teilbarkeit durch 11

Beispiel 2.20

Ist 1782 durch 11 teilbar?
Die Teilbarkeit können wir wieder formulieren als

$$11 \mid 1782 \quad \Leftrightarrow \quad 1782 = 0 \mod 11.$$

Da $10 \mod 11 = (-1) \mod 11$, ist $10^k \mod 11 = (-1)^k \mod 11$. Wenn wir 1782 wieder als Summe von Zehnerpotenzen schreiben, erhalten wir somit:

$$\begin{aligned} 1782 &= \left(1 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 2\right) \mod 11 \\ &= (-1)^3 \mod 11 + 7 \mod 11 + 8(-1) \mod 11 + 2 \mod 11 \\ &= (-1 + 7 - 8 + 2) \mod 11 \end{aligned}$$

Eine Zahl ist also durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

Satz 2.21

Sei $a = \sum_{k=0}^{n} a_k 10^k$ eine natürliche Zahl. Dann gilt

$$a = 0 \mod 11 \quad \Leftrightarrow \quad \left(\sum_{k=0}^{n} (-1)^k a_k\right) \mod 11 = 0 \mod 3.$$

2.5 Die Menge $\mathbb{Z}_n^*$

Durch den erweiterten euklidischen Algorithmus können wir zu teilerfremden Zahlen $a, n \in \mathbb{Z}$ Zahlen $x, y \in \mathbb{Z}$ berechnen, so dass

$$ax + ny = 1 \quad \Leftrightarrow \quad ggT(a, n) = 1.$$

Die Gleichung $ax + ny = 1$ bedeutet, dass n das Produkt ax gerade mit Rest 1 teilt, also $ax = 1 \mod n$. Wir können also sagen, dass x das **multiplikative Inverse** von a in $\mathbb{Z}_n$ ist. Wir können für $a \in \mathbb{Z}$, die teilerfremd zu n sind, die Gleichung $[ax] = [1]$ in $\mathbb{Z}_n$ lösen. Es liegt also nahe, diese Zahlen in einer Menge zusammenzufassen:

$$\mathbb{Z}_n^* := \left\{ a \in \mathbb{Z}_n \setminus \{0\} \;\middle|\; ggT(a, n) = 1 \right\}.$$

Definition 2.22

Wir definieren die folgende Funktion

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad \varphi(n) = \left|\mathbb{Z}_n^*\right|.$$

Sie wird **Eulersche φ-Funktion** genannt.

Beispiel 2.23

1. Es ist $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Wenn wir nur die zu 4 teilerfremden Zahlen „behalten“, bekommen wir $\mathbb{Z}_4^* = \{1, 3\}$. Also ist $\varphi(4) = 2$.
2. Es ist $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Wenn wir die zu 6 teilerfremden Zahlen dieser Menge zusammenfassen, bekommen wir $\mathbb{Z}_6^* = \{1, 5\}$. Also ist $\varphi(6) = 2$.
3. Da jede Primzahl p nur durch 1 und p teilbar ist, ist $\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*$ und

damit $\varphi(p) = p - 1$.

Satz 2.24

Es gilt:

$$\forall\, n, m \in \mathbb{N} \text{ mit } ggT(n,m) = 1 : \ \varphi(n \cdot m) = \varphi(n)\varphi(m).$$

Weiter gilt für jedes $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$:

$$\varphi(n) = \varphi(p_1^{a_1}) \cdot \dots \cdot \varphi(p_k^{a_k}) = p_1^{a_1-1}(p_1 - 1) \cdot \dots \cdot p_k^{a_k-1}(p_k - 1).$$

Beispiel 2.25

Es ist $8800 = 2^5 \cdot 5^2 \cdot 11$, also ist

$$\varphi(8800) = \varphi(2^5 \cdot 5^2 \cdot 11) = 2^4 \cdot (2-1) \cdot 5 \cdot (5-1) \cdot 10 = 3200.$$

2.6 Grundlegende Begriffe der Gruppentheorie

Definition 2.26

Sei G eine Menge und $\circ : G \times G \to G$ eine Verknüpfung auf G. Falls gilt

(G1) Die Verknüpfung ist **assoziativ**, d.h.

$$\forall g, h, i \in G : \ (g \circ h) \circ i = g \circ (h \circ i).$$

(G2) Es gibt ein **neutrales Element**, d.h.

$$\exists\, e \in G : \ \forall\, g \in G : \ g \circ e = g.$$

(G3) Es gibt **inverse Elemente**, d.h.

$$\forall\, g \in G : \ \exists\, g^{-1} \in G : \ g \circ g^{-1} = e.$$

dann heißt $(G, \circ)$ eine **Gruppe**.
Gilt zusätzlich

(G4) Die Verknüpfung ist **kommutativ**, d.h.

$$\forall g, h \in G : \ g \circ h = h \circ g$$

dann heißt die Gruppe **abelsch**.
Die Anzahl $|G|$ von Elementen in G wird bei Gruppen als **Ordnung** bezeichnet.

Beispiel 2.27

1. Die Menge $(\mathbb{Z}, +)$ ist eine Gruppe. Das neutrale Element ist 0 und zu jedem $n \in \mathbb{Z}$ ist das inverse Element $-n \in \mathbb{Z}$ in der Menge enthalten. Die Addition ist assoziativ (und auch kommutativ).
2. Die Menge $\mathbb{N}$ bezüglich der Addition ist keine Gruppe: $\mathbb{N}$ entählt nicht das neutrale Element 0. Zu $n \in \mathbb{N}$ gibt es auch keine inversen Elemente in $\mathbb{N}$ (denn $-n \notin \mathbb{N}$).
3. Die Menge $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe bezüglich der Multiplikation, da keine inversen Elemente in $\mathbb{Z}$ enthalten sind: Zu $n \in \mathbb{Z}, n \neq 1$ ist $\frac{1}{n} \notin \mathbb{Z}$.
4. Die Menge $(\mathbb{Z}_n, +)$ der Restklassen ist eine Gruppe für $n \in \mathbb{N}$: Das neutrale Element ist 0 und zu jedem Element $k \in \mathbb{Z}_n$ gibt es ein inverses Element $(n - k) \in \mathbb{Z}_n$, so dass $(k + (n - k)) \mod n = 0 \mod n$. Als Beispiel sei die Additionstabelle für $\mathbb{Z}_4$ gezeigt. Solche Verknüpfungstabellen eignen

sich für Gruppen mit wenigen Element sehr gut, um die Gruppengesetze zu überprüfen:

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

Tabelle 2.2 Additionstabelle der Gruppe $(\mathbb{Z}_4, +)$

5. Die Menge $S_3 := \left\{ g : \{1,2,3\} \to \{1,2,3\} \;\middle|\; g \text{ bijektive Abbildung} \right\}$ aller bijektiven Abbildungen einer 3-elementigen Menge bildet mit der Komposition $\circ$ von Abbildungen eine Gruppe. Diese Abbildungen nennt man auch **Permutationen** und die Gruppe **symmetrische Gruppe** bzw. Permutationsgruppe. Man schreibt die Abbildungen vereinfacht als $s_1 = (132)$, wenn s_1 die Abbildung ist, die $1 \mapsto 1$, $2 \mapsto 3$ und $3 \mapsto 2$ zuordnet. Die Menge S_3 besitzt $3! = 6$ Elemente: $\mathrm{id} = (123)$, $s_1 = (132)$, $s_2 = (213)$, $s_3 = (231)$, $s_4 = (312)$ und $s_5 = (321)$. Wir überprüfen, dass es sich um eine Gruppe handelt, indem wir die Gruppentafel aufstellen:

$\circ$	id	s_1	s_2	s_3	s_4	s_5
id	id	s_1	s_2	s_3	s_4	s_5
s_1	s_1	id	s_4	s_5	s_2	s_3
s_2	s_2	s_3	id	s_1	s_5	s_4
s_3	s_3	s_2	s_5	s_4	id	s_1
s_4	s_4	s_5	s_1	id	s_3	s_2
s_5	s_5	s_4	s_3	s_2	s_1	id

Tabelle 2.3 Verknüpfungstabelle der Gruppe $(S_3, \circ)$

Wir erkennen an der Tafel, dass $\mathrm{id} = (123)$ das neutrale Element ist, denn $\mathrm{id} \circ g = g \circ \mathrm{id} = g$ für alle $g \in S_3$. In jeder Zeile finden wir einmal id, so dass auch jedes Element ein inverses Element besitzt: $s_1 \circ s_1 = \mathrm{id}$, $s_2 \circ s_2 = \mathrm{id}$, $s_3 \circ s_4 = \mathrm{id}$, $s_4 \circ s_3 = \mathrm{id}$ und $s_5 \circ s_5 = \mathrm{id}$. Also handelt es sich um eine Gruppe. Wir sehen, dass die Verknüpfung nicht kommutativ ist, da die Tafel nicht symmetrisch ist: $s_2 \circ s_3 = s_1 \neq s_3 \circ s_2 = s_5$.
Man kann zu jedem $n \in \mathbb{N}$ eine symmetrische Gruppe S_n aller bijektiven Abbildungen $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ definieren. Sie besitzt die Ordnung $|S_n| = n!$.

Ist $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ eine Gruppe? Wir überprüfen dies am Beispiel $\mathbb{Z}_4$ anhand einer

Multiplikationstabelle:

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Tabelle 2.4 Multiplikationstabelle von $(\mathbb{Z}_4, \cdot)$

Wir erkennen, dass das Element 2 kein inverses Element in $\mathbb{Z}_4$ besitzt: Es gibt kein $x \in \mathbb{Z}_4$, so dass $2x = 1 \mod 4$. Wir erinnern uns an Satz 2.10, der gerade aussagte, dass zu einer Zahl $a \in \mathbb{Z}_n$ genau dann ein $x \in \mathbb{Z}_n$ existiert, so dass $ax = 1 \mod n$, falls $ggT(a, n) = 1$ gilt. Dieses x aus dem Satz ist das inverse multiplikative Element, das wir suchen. In unserem Beispiel ist $ggT(2, 4) = 2$ – beide Zahlen sind nicht teilerfremd. Deswegen kann 2 in $\mathbb{Z}_4$ kein inverses (multiplikatives) Element besitzen. Wenn wir entsprechend die Menge $\mathbb{Z}_n$ auf die Menge der zu n teilerfremden Zahlen beschränken, also auf die Menge $\mathbb{Z}_n^*$, erhalten wir entsprechend eine Gruppe:

Satz 2.28

Die Menge $\mathbb{Z}_n^* = \left\{ a \in \mathbb{Z}_n \setminus \{0\} \;\middle|\; ggT(a, n) = 1 \right\}$ ist bezüglich der Multiplikation eine Gruppe der Ordnung $\varphi(n)$.

Beispiel 2.29

Wir betrachten die Gruppe $\mathbb{Z}_8^*$. Sie enthält $\varphi(8) = 4$ Elemente, nämlich 1,3,5 und 7. Wir stellen die Multiplikationstabelle auf:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Tabelle 2.5 Multiplikationstabelle von $(\mathbb{Z}_8^*, \cdot)$

Wir erkennen an der Tabelle, dass 1 das neutrale Element ist und in jeder Zeile eine 1 auftaucht, also besitzt jedes Element ein inverses Element: genauer ist $3^2 = 1$, $5^2 = 1$ sowie $7^2 = 1$. Die Gruppe ist abelsch, denn die Tabelle ist symmetrisch.

Definition 2.30

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Sei $g \in G$. Die kleinste Zahl $n \in \mathbb{N}$, so dass

$$g^n = g \circ \cdots \circ g = e,$$

heißt **Ordnung des Elements** g und man schreibt $ord(g) = n$.

Bemerkung 2.2. *In jeder Gruppe hat das neutrale Element die Ordnung 1, denn es ist* $e^1 = e$.

Beispiel 2.31

1. In der Gruppe $(\mathbb{Z}_8^*, \cdot)$ hat jedes Element außer der Eins die Ordnung 2: $ord(3) = ord(5) = ord(7) = 2$. Das Element 1 hat die Ordnung 1.
2. In der Gruppe $(S_3, \circ)$ haben die Elemente s_1, s_2 und s_5 die Ordnung 2, denn es ist $s_1 \circ s_1 = \mathrm{id}$, $s_2 \circ s_2 = \mathrm{id}$ und $s_5 \circ s_5 = \mathrm{id}$. Die Elemente s_3 und s_4 haben Ordnung 3: $s_3^3 = s_3 \circ s_3 \circ s_3 = \mathrm{id}$ und $s_4^3 = s_4 \circ s_4 \circ s_4 = \mathrm{id}$.

Es scheint – zumindest in den obigen Beispielen – so zu sein, dass ein Element in einer Gruppe keine beliebige Ordnung besitzen kann. Tatsächlich gilt der folgende Satz:

Satz 2.32

Sei $(G, \circ)$ eine endliche Gruppe, d.h. $|G| < \infty$. Die Ordnung eines Elements ist immer ein Teiler der Ordnung der Gruppe:

$$ord(g) \mid |G|$$

für alle $g \in G$.

Betrachtet man die Menge $\{\mathrm{id}, s_1\} \subset S_3$, stellt man fest, dass sie ebenfalls eine Gruppe bildet, denn $s_3 \circ \mathrm{id} = \mathrm{id} \circ s_3 = s_3$ und $s_3^2 = \mathrm{id}$, d.h. die Menge ist abgeschlossen bezüglich der Komposition, außerdem gibt es ein neutrales Element und inverse Elemente. Teilmengen von Gruppen mit dieser Eigenschaft heißen **Untergruppen**.

Definition 2.33

Sei $(G, \circ)$ eine Gruppe und $U \subset G$ eine Teilmenge, so dass gilt:

- $g, h \in U \Rightarrow g \circ h \in U$
- $g \in U \Rightarrow g^{-1} \in U$

Dann heißt U **Untergruppe** von G. Man schreibt $U < G$.

Bemerkung 2.3. *Aus den Eigenschaften einer Untergruppe folgt direkt, dass das neutrale Element in U ist, denn $g, g^{-1} \in U$ für jedes $g \in U$, also ist $e \in U$.*

Es gilt ein ähnlicher Satz bezüglich der Ordnung einer Untergruppe wie bezüglich der Ordnung eines Elementes:

Satz 2.34

Sei $(G, \circ)$ eine endliche Gruppe, d.h. $|G| < \infty$. Die Ordnung jeder Untergruppe ist immer ein Teiler der Ordnung der Gruppe:

$$U \mid |G|$$

für alle $U < G$.

Beispiel 2.35

1. Wir betrachten die Gruppe $(\mathbb{Z}_{26}^*, \cdot)$. Es ist $|\mathbb{Z}_{26}^*| = \varphi(26) = 12$. Die Teiler von 12 lauten 1,2,3,4 und 6 (und 12). Wir untersuchen, ob es Untergruppen mit 2,3,4 bzw. 6 Elementen gibt. Die Untergruppe mit einem Element ist immer die Menge $\{1\}$, die trivialerweise eine Untergruppe ist.
   Es ist $\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. Wir versuchen, eine erste Untergruppe zu finden, und starten mit der Menge $\{1, 3\}$. Es ist $3^2 \mod 26 = 9 \mod 26$, also müssen wir 9 zu der Menge hinzunehmen: $\{1, 3, 9\}$. Es ist $3 \cdot 9 \mod 26 = 1 \mod 26$ und $9^2 \mod 26 = 3 \mod 26$. Da die Multiplikation kommutativ ist, bildet die Menge $U_1 = \{1, 3, 9\}$ eine Untergruppe. Die Ordnung von U_1 ist 3.
   Gibt es auch eine Untergruppe aus 2 Elementen? Dafür müssen wir ein Element a in $\mathbb{Z}_{26}^*$ finden, dass Ordnung 2 besitzt, also $a^2 \mod 26 = 1 \mod 26$. Wir schreiben diese Gleichung um als $(a^2 - 1) \mod 26 = 0 \mod 26$, also $(a-1)(a+1) \mod 26 = 0 \mod 26$. Anhand dieser Gleichung sehen wir, dass für $a = 25$ gilt $(25+1) \mod 26 = 0 \mod 26$, also auch $(25-1)(25+1) \mod 26 = 0 \mod 26$. Nachrechnen zeigt auch, dass $25^2 \mod 26 = 1 \mod 26$ ist. Es ist also $ord(25) = 2$ und die Menge

$U_2 = \{1, 25\}$ bildet eine Untergruppe der Ordnung 2 in $\mathbb{Z}_{26}^*$.

2. Die Gruppe S_3 besitzt Ordnung 6. Sie kann also nichttriviale Untergruppen der Ordnung 2 oder 3 haben. In S_3 können wir mit allen Elementen der Ordnung 2 Untergruppen der Ordnung 2 bilden, also $\{\mathrm{id}, s_1\}$, $\{\mathrm{id}, s_2\}$ und $\{\mathrm{id}, s_5\}$. Weiter finden wir eine Untergruppe der Ordnung 3, die die beiden Elemente der Ordnung 3 enthält: $\{\mathrm{id}, s_3, s_4\}$, denn es ist $s_3 \circ s_4 = s_4 \circ s_3 = \mathrm{id}$, $s_3 \circ s_3 = s_4$ und $s_4 \circ s_4 = s_3$.

Eine direkte Folgerung aus Satz 2.32 ist die folgende Aussage:

Corollary 2.4. *Sei $(G, \circ)$ eine endliche Gruppe mit neutralem Element e. Dann gilt für jedes Element $g \in G$:*

$$g^{|G|} = e.$$

Beweis. Wir wissen aus Satz 2.32, dass $ord(g) \mid |G|$. Also existiert $k \in \mathbb{N}$, so dass $ord(g) \cdot k = |G|$. Damit und der Definition von $ord(g)$ folgt direkt die Aussage des Satzes:

$$g^{|G|} = g^{k \cdot ord(g)} = \left(g^{ord(g)}\right)^k = e^k = e.$$

Ein sehr wichtiger Spezialfall dieses Satzes ist seine Anwendung auf die multiplikativen Gruppen $(\mathbb{Z}_n^*, \cdot)$, der deswegen einen eigenen Namen trägt:

Corollary 2.5 (Satz von Euler). *Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$ mit $ggT(a, n) = 1$. Dann gilt*

$$a^{\varphi(n)} = 1 \mod n.$$

Bemerkung 2.6. *Im Fall, dass n eine Primzahl ist, wird aus der Aussage:*

$$a^{n-1} = 1 \mod n$$

für jedes $a \in \mathbb{Z}$, das kein Vielfaches von n ist. Dieser Spezialfall wird als ***„Kleiner Fermat“*** *bezeichnet.*

Beweis. Der Satz ergibt sich direkt aus dem Korollar 2.4, wenn wir ihn auf die Gruppe $(\mathbb{Z}_n^*, \cdot)$ anwenden, denn die Ordnung von $\mathbb{Z}_n^*$ ist $\varphi(n)$. Alle Elemente $a \in \mathbb{Z}_n^*$ sind per definitionem teilerfremd zu n. □

2.7 Zyklische Gruppen, Erzeuger und Homomorphismen

Definition 2.36

Eine Gruppe G heißt **zyklisch**, falls ein Element $g \in G$ existiert, so dass

$$G = \left\{ g^n \mid n \in \mathbb{Z} \right\}.$$

Das Element g wird **Erzeuger** der Gruppe G genannt.

Bemerkung 2.7. *Eine zyklische Gruppe kann mehrere Erzeuger besitzen. Er muss nicht eindeutig bestimmt sein.*

Beispiel 2.37

1. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch mit dem Erzeuger 1, denn jedes Element $n \in \mathbb{Z}$, kann als Summe bzw. Differenzen von Einsen geschrieben werden.
2. Jede Gruppe $(\mathbb{Z}_n, +)$ ist zyklisch mit dem Erzeuger 1.
3. Wir untersuchen, ob $(\mathbb{Z}_{12}^*, \cdot)$ zyklisch ist. Es ist $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$, und wir stellen die Multiplikationstabelle auf:

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Tabelle 2.6 Multiplikationstabelle von $\mathbb{Z}_{12}^*$.

   Wir sehen, dass jedes Element Ordnung 2 besitzt, also ist $\mathbb{Z}_{12}^*$ nicht zyklisch.

4. Wir untersuchen ob $(\mathbb{Z}_5^*, \cdot)$ zyklisch ist. Es ist $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, und wir stellen die Multiplikationstabelle auf:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabelle 2.7 Multiplikationstabelle von $\mathbb{Z}_5^*$.

   Wir erkennen, dass $2^2 \mod 5 = 4 \mod 5$, $2^3 \mod 5 = 3 \mod 4$ und $2^4 \mod 5 = 1 \mod 5$. Also ist $ord(2) = 4$ und 2 ist ein Erzeuger von $\mathbb{Z}_5^*$.

Weiter ist $3^2 \mod 5 = 4 \mod 5$, $3^3 \mod 5 = 2 \mod 5$, $3^4 \mod 5 = 1 \mod 5$. Also ist $ord(3) = 4$ und auch 3 ist ein Erzeuger von $\mathbb{Z}_5^*$. Das Element 4 hat Ordnung 2 und ist damit kein Erzeuger von $\mathbb{Z}_5^*$.

Definition 2.38

Seien $(G, \cdot)$, $(H, *)$ zwei Gruppen mit neutralen Elementen e_G bzw. e_H. Eine Abbildung $f : G \to H$ heißt **(Gruppen-)Homomorphismus**, falls für alle $g, h \in G$ gilt:

$$f(g \circ h) = f(g) * f(h).$$

Wir bezeichnen $f(G)$ wie gewohnt als **Bild** und $\ker(f) = \left\{ g \in G \;\middle|\; f(g) = e_H \right\}$ als **Kern**.
Ist die Abbildung f bijektiv, dann nennt man f einen **(Gruppen-)Isomorphismus** und die Gruppen G und H heißen **isomorph**. Man schreibt kurz $G \cong H$.

Beispiel 2.39

Die Abbildung $f_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f_n(a) = a \mod n$ ist ein Gruppenhomomorphismus für jedes $n \in \mathbb{N}$, denn

$$f_n(a + b) = (a + b) \mod n = a \mod n + b \mod n = f_n(a) + f_n(b).$$

Satz 2.40

Sei $f : G \to H$ ein Homomorphismus. Dann sind das Bild $f(G) < H$ und der Kern $\ker(f) < G$ jeweils eine Gruppe.

Beispiel 2.41

Wir betrachten noch einmal die Abbildung $f_n(a) = a \mod n$. Das Bild von f_n ist

$$f_n(\mathbb{Z}) = \{0, 1, \ldots, n - 1\}$$

und der Kern

$$\ker(f_n) = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}.$$

Aus Satz 2.40 wissen wir, dass $f_n(\mathbb{Z}) = \mathbb{Z}_n$ mit der Addition eine Gruppe ist. Ebenso ist die Menge $n\mathbb{Z}$ mit der Addition eine Gruppe.

Bemerkung 2.8. *Wir können für jeden Homomorphismus $f : G \to H$ eine Äquivalenzrelation wie folgt definieren:*

$$g \sim h \quad :\Leftrightarrow \quad f(g) = f(h).$$

Die Äquivalenzklassen bestehen aus all jenen Elementen $g \in G$, die dasselbe Bild in H besitzen:

$$[g]_f = \left\{ h \in G \;\middle|\; f(g) = f(h) \right\}.$$

Da wir die Bedingung $f(g) = f(h)$ auch umschreiben können als $f(g) - f(h) \in \ker(f)$ (falls die Gruppen additiv sind), schreibt man die Menge der Äquivalenzklassen als

$$G/\ker(f) = \left\{ [g]_f \;\middle|\; g \in G \right\}.$$

Die Verknüpfung $\circ$ in G wird in die Menge der Äquivalenzklassen „vererbt“, da f ein Homomorphismus ist: $[g]_f + [h]_f = [g+h]_f$. Dadurch wird $G/\ker(f)$ zu einer Gruppe.

Der folgende Satz liefert die wichtige Aussage, dass diese Gruppe der Äquivalenzklassen isomorph zum Bild von f ist:

Satz 2.42

Sei $f : G \to H$ ein Gruppenhomomorphismus, dann gilt:

$$G/\ker(f) \cong f(G).$$

Es folgt direkt, dass

$$\frac{|G|}{|\ker(f)|} = |f(G)|.$$

Bemerkung 2.9. *Mit Hilfe dieses Satzes kann man direkt zeigen, dass $f : G \to H$ genau dann injektiv ist, wenn $\ker(f) = \{e_G\}$, d.h. $f(e_G) = e_H$. Mit Hilfe dieses Kriteriums ist es häufig sehr viel leichter zu zeigen, dass eine Abbildung ein Isomorphismus ist.*

Beispiel 2.43

1. Wir betrachten noch einmal die Abbildung $f_n(a) = a \mod n$. Das Bild von f_n ist

   $$f_n(\mathbb{Z}) = \{0, 1, \ldots, n-1\}$$

   und der Kern

   $$\ker(f_n) = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}.$$

   Aus dem Satz folgt

   $$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

. Daran sehen wir nun, dass die additive Gruppe der Restklassen $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ tatsächlich isomorph zur Gruppe $\{0, 1, \ldots, n-1\}$ mit der Addition ist und wir getrost die Klammern in der Bezeichnung weglassen können.

2. Wir betrachten $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ mit $f(a \mod 6) = a \mod 3$. Es ist

$$f(a+b) = (a+b) \mod 3 = a \mod 3 + b \mod 3 = f(a) + f(b),$$

also liegt ein Homomorphismus vor. Wir bestimmen den Kern:

$$\ker(f) = \left\{ a \in \mathbb{Z}_6 \;\middle|\; f(a) = 0 \mod 3 \right\} = \{0, 3\}.$$

Es ist also $|\ker(f)| = 2$ und $|f(\mathbb{Z}_6)| = 3$. Weiter ist

$$\mathbb{Z}_6/\ker(f) \cong \mathbb{Z}_3.$$

Definition 2.44

Seien $(G, \circ)$ und $(H, *)$ zwei Gruppen. Dann ist auch das **direkte Produkt** $G \times H$ mit der wie folgt definierten Verknüpfung

$$\forall (g,h), (\tilde{g}, \tilde{h}) \in G \times H : \; (g \circ \tilde{g}, h * \tilde{h})$$

eine Gruppe.

Bemerkung 2.10. *Diese Definition kann selbstverständlich auf das Produkt von n Gruppen $(G_i, *_i)$ verallgemeinert werden.*

Beispiel 2.45

1. Sei $(\mathbb{Z}_2, +)$ und $(\mathbb{Z}_3, +)$. Dann ist auch $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ eine Gruppe mit

$$(a \mod 2, b \mod 3) + (c \mod 2, d \mod 3) = (a+c \mod 2, b+d \mod 3).$$

2. Die Menge $(\mathbb{R}, +)$ ist eine Gruppe. Entsprechend ist $(\mathbb{R} \times \mathbb{R}, +)$ mit $(a, b) + (c, d) = (a + c, b + d)$ eine Gruppe.

Beispiel 2.46

1. Die Gruppe $(\mathbb{Z}_6, +)$ ist isomorph zur Gruppe $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$. Wir definieren

wie folgt einen Isomorphismus:

$$f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3, \quad f(a \mod 6) = (a \mod 2, a \mod 3).$$

Da $\mathbb{Z}_6$ nur 6 Elemente hat, können wir alle Bilder betrachten und daran zeigen, dass f bijektiv ist:

$$f(0) = (0,0),\ f(1) = (1,1),\ f(2) = (0,2),\ f(3) = (1,0),\ f(4) = (0,1),\ f(5) = (1,2).$$

Alle Bilder von f sind verschieben, somit ist die Abbildung injektiv. Außerdem wird jedes Element aus $(\mathbb{Z}_2 \times \mathbb{Z}_3)$ getroffen, damit ist f auch surjektiv.

2. Die Gruppe $(\mathbb{Z}_{12}^*, \cdot)$ ist isomorph zur Gruppe $(\mathbb{Z}_3^* \times \mathbb{Z}_4^*, \cdot)$. Wir definieren den Isomorphismus als

$$f(a \mod 12) = (a \mod 3, a \mod 4)$$

Es handelt sich aufgrund der Rechenregeln der Modulorechnung um einen Homomorphismus. Die Abbildung sieht wie folgt aus:

$$f(1) = (1,1),\ f(5) = (1,2),\ f(7) = (3,1),\ f(11) = (3,2).$$

Daran erkennt man wiederum direkt, dass f injektiv und surjektiv ist. Damit sind beide Gruppen tatsächlich isomorph.

2.8 Der Chinesische Restsatz

Das letzte Beispiel zeigt, dass wir Rechnungen in einer großen Modulogruppe in dem Produkt von „kleineren“ Modulogruppen durchführen können. Statt in $\mathbb{Z}_{12}$ zu rechnen, können wir in $\mathbb{Z}_3 \times \mathbb{Z}_4$ rechnen. In beiden Gruppen ist das Rechnen natürlich unproblematisch; zur Anwendung kommt dieser Isomorphismus allerdings bei der Multiplikation oder Addition von sehr großen Zahlen. Durch den Isomorphismus zu Produkten von Gruppen kann die Addition parallelisiert werden und beschleunigt. Wir führen an dem folgenden einfachen Beispiel vor, wie das Prinzip dieser schnellen Addition funktioniert.

Beispiel 2.47

Wir wollen $1878 + 1384$ rechnen. Beide Zahlen sind < 2000, also wird die Summe < 4000 sein. Wir rechnen also in $\mathbb{Z}_{4000}$. Es ist $4000 = 2^5 \cdot 5^3 = 32 \cdot 125$. Wir wissen, dass $\mathbb{Z}_{4000} = \mathbb{Z}_{32} \times \mathbb{Z}_{125}$. Wir definieren den Isomorphismus f wie

oben als $f(a) = (a \mod 32, a \mod 125)$. Wir erhalten $f(1878) = (22, 3)$ und $f(1384) = (8, 9)$. Diese Zahlen können wir leicht addieren und bekommen

$$(22, 3) + (8, 9) = (30, 12)$$

Nun möchten wir natürlich die Zahl in $\mathbb{Z}_{4000}$ erhalten, der dieses Ergebnis entspricht. Das heißt wir suchen x, so dass

$$x \mod 32 = 30 \mod 32, \quad x \mod 125 = 12 \mod 125$$

Wir können dieses Zahl mit Hilfe des erweiterten euklidischen Algorithmus ausrechnen:

a	b	x	y	k
125	32	1	0	-
32	29	0	1	3
29	3	1	-3	1
3	2	-1	4	9
2	1	10	-39	1
1	0	-11	43	2

Wir wissen, dass $(-11 \cdot 125) + 43 \cdot 32 = 1$. Daraus folgt, dass $(-11) \cdot 125 = 1 \mod 32$. Also ist $(-11) \cdot 125 \cdot 30 = 30 \mod 32$. Weiter wissen wir, dass $(43 \cdot 32) = 1 \mod 125$, also ist $(43 \cdot 32 \cdot 12) = 12 \mod 125$. Damit erhalten wir aus der Summe eine Lösung für die Kongruenzgleichungen:

$$x = (-11) \cdot 125 \cdot 30 + 43 \cdot 32 \cdot 12 = -24738.$$

Diese Lösung müssen wir noch modulo 4000 rechnen und erhalten: $-24738 \mod 4000 = 3262$. Wie wir leicht nachrechnen können ist dies auch die richtige Lösung. In der Rechnung haben wir davon Gebrauch gemacht, dass 32 und 125 teilerfremd sind. Ansonsten hätten wir nicht mit Hilfe des erweiterten euklidischen Algorithmus die Lösung berechnen können! Die Existenz einer solchen Lösung ist die Aussage des **Chinesischen Restsatzes**, die wir nun vorstellen wollen:

Satz 2.48: Chinesischer Restsatz

Seien $n_i \in \mathbb{N}, i = 1, \ldots, k$ zueinander teilerfremde Zahlen, d.h. $ggT(n_i, n_j) = 1$ für $i \neq j$, $1 \leq i, j \leq k$ und $x_i \in \mathbb{Z}$, $i = 1, \ldots k$. Sei $n = n_1 \cdot \cdots \cdot n_k$. Dann besitzt das System der Gleichungen

$$x \mod n_i = x_i \mod n_i, \quad i = 1, \ldots, k$$

genau eine Lösung $x \in \mathbb{Z}_n$.

Beweis. Die Lösung wird wie folgt berechnet: Aufgrund der Voraussetzungen ist $ggT\left(n_i, \frac{n}{n_i}\right) = 1$ für jedes $i = 1, \ldots, k$. Also existieren wegen des erweiterten euklidischen Algorithmus Zahlen r_i, s_i, so dass

$$r_i \cdot n_i + s_i \cdot \frac{n}{n_i} = 1$$

Wir setzen $a_i = s_i \cdot \frac{n}{n_i}$. Dann ist $a_i = 1 \mod n_i$ und $a_i = 0 \mod n_j$ für $j \neq i$. Die Lösung erhalten wir somit als Summe

$$x = \sum_{i=1}^{k} x_i \cdot a_i \mod n.$$

Corollary 2.11. *Sei $n = n_1 \cdot \cdots \cdot n_k$ mit zueinander teilerfremden $n_i \in \mathbb{N}$, $i = 1, \ldots, k$. Dann ist*

$$(\mathbb{Z}_n, +) \cong (\mathbb{Z}_{n_1}, +) \times \cdots \times (\mathbb{Z}_{n_k}, +)$$

Beweis. Wir definieren $f : \mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ durch

$$f(a \mod n) = (a \mod n_1, \ldots, a \mod n_k).$$

Aufgrund des Chinesischen Restsatzes existiert zu jedem $(a_1, \ldots, a_k) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ genau ein a, so dass $f(a) = (a_1, \ldots, a_k)$. Da beide Mengen die gleiche Mächtigkeit besitzen, ist die Abbildung ein Isomorphismus und die Aussage bewiesen. □

Können wir diesen Trick auch für die Multiplikation ausnutzen? Wir betrachten ein etwas einfacheres Beispiel als oben:

Beispiel 2.49

Wir wollen $15 \cdot 15$ rechnen. Beide Zahlen sind ≤ 16, also wird das Produkt $\leq 16 \times 17$ sein. Wir rechnen also in $\mathbb{Z}^*_{16\times 17}$. . Wir versuchen also in $\mathbb{Z}^*_{16} \times \mathbb{Z}_{17}*$ zu rechnen. Wir definieren zunächst einen Homomorphismus

$$f : \mathbb{Z}_{16\times 17}* \to \mathbb{Z}^*_{16} \times \mathbb{Z}^*_{17}, \; f(a \mod (16 \times 17)) = (a \mod 16, a \mod 17).$$

Es ist

$$f(a \cdot b \mod (16 \times 17)) = (a \cdot b \mod 16, a \cdot b \mod 17) = (a \mod 16 \cdot b \mod 16, a \mod 17 \cdot b \mod$$

Der Homomorphismus ist injektiv: Sei $f(a) = (1 \mod 16, 1 \mod 17)$. Aufgrund des chinesischen Restsatzes gibt es aber nur ein $a \in \mathbb{Z}_{16\times 17}$ und das ist $a = 1$. Die Surjektivität folgt aus der Ordnung der Gruppen, denn $\varphi(16 \cdot 17) = \varphi(2^4)\varphi(17) = 2^3 \cdot 16$.
Es ist $f(15) = (15, 15) = (-1, -2)$, also ist $f(15 \cdot 15) = ((-1)^2, (-2)^2) = (1, 4)$. Wir suchen x, so dass $x = 1 \mod 16$ und $x = 4 \mod 17$. Dies erhalten wir wieder mit Hilfe des erweiterten euklidischen Algorithmus (oder durch scharfes Hinschauen): $1 = 1 \cdot 17 + (-1) \cdot 16$,also mit dem chinesischen Restsatz: $x = 17 \cdot 1 - 4 \cdot 16 = 17 - 72 = -47$. Nun rechnen wir noch $x \mod (16 \cdot 17) = -47 + (16 \cdot 17) = 225 = 15^2$.

Definition 2.50

Sei R eine Menge mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to$. Dann heißt $(R, +, \cdot)$ **Ring**, falls gilt

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) Die Multiplikation ist assoziativ:

$$\forall a, b, c \in R : \ (a \cdot b) \cdot c) = a \cdot (b \cdot c).$$

(R3) Es gilt das Distributivgesetz:

$$\forall a, b, c \in R : \ a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Beispiel 2.51

1. $(\mathbb{Z}, +, \cdot)$ ist ein Ring.
2. $(m\mathbb{Z}, +, \cdot)$ ist ein Ring.
3. $(\mathbb{Z}_n, +, \cdot)$ ist ein Ring.
4. Die Menge der Polynome mit Koeffizienten in einem Ring R bilden einen Ring.

Definition 2.52

Sei K eine Menge mit zwei Verknüpfungen $+$ und $\cdot$. Dann heißt $(K, +, \cdot)$ **Körper**, falls gilt:

(K1) $(K, +)$ ist eine abelsche Gruppe.

(K2) $(K \setminus \{0\}, \cdot)$ ist eine Gruppe.

(K3) Es gilt das Distributivgesetz:

$$\forall a, b, c \in R: \ a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Beispiel 2.53

1. Die Zahlenmengen $\mathbb{Q}$ und $\mathbb{R}$ bilden mit der üblichen Addition und Multiplikation Körper.
2. Der Zahlenring $\mathbb{Z}_5$ ist ein Körper, denn $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^*$ und damit eine Gruppe. Im Allgemeinen gilt:

Satz 2.54

Der Zahlenring $(\mathbb{Z}_n, +, \cdot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

2.9 Einfache Anwendungen in der Kryptographie

Jede Nachricht, also jede Zeichenkette, wird zwischen Rechnern als Zahl übermittelt. In der klassischen ASCII-Codierung stehen jedem Zeichen 7 Bit zur Verfügung, also können $2^7 = 128$ verschiedene Zeichen kodiert werden. Zum Beispiel entspricht dem Großbuchstaben M die Zahl 77. Der Zeichenkette MAUS die Zahl

$$N = 77065085083.$$

Die Verschlüsselung dieser Zahl N kann man als Anwendung einer Funktion f_K auffassen

$$f_K : N \to f_K(N),$$

wobei die Funktion häufig von einem Schlüssel K abhängt. Die Entschlüsselung entspricht dann der Anwendung der Umkehrfunktion f_K^{-1}. Gesucht sind zur Verschlüsselung Funktionen, deren Werte leicht zu berechnen sind, deren Umkehrfunktion aber unmöglich oder zumindest nur mit großem Zeitaufwand zu bestimmen ist. Eine solche Funktion ist die Multiplikation von zwei Primzahlen. Das Umkehrproblem

entspricht der Faktorisierung einer großen Zahl in ihre Primfaktoren. Auf diesem Prinzip beruht die RSA-Verschlüsselung, die wir im folgenden erklären möchten:

2.9.1 RSA-Verschlüsselung

1. Wir wählen zwei Primzahlen p, q und berechnen $n = p \cdot q$. Das Produkt n muss dabei größer als die zu verschlüsselnde Botschaft sein – in dem Beispiel der Nachricht MAUS größer als $N = 77.065.085.083 \approx 77 \cdot 10^9$. Beispielsweise sind $p = 999.979$ und $q = 999.983$ zwei Primzahlen und ihr Produkt ist größer als N.
2. Wir wählen ein Element $e \in \mathbb{Z}^*_{\varphi(n)}$. Zur Erinnerung: $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$.
3. Wir berechnen das multiplikative inverse Element zu e, also $d \in \mathbb{Z}^*_{\varphi(n)}$, so dass $ed = 1 \mod (p-1)(q-1)$. Ein solches Element existiert, da $ggT(e, (p-1)(q-1)) = 1$ ist.
4. Die öffentlichen Schlüssel sind n und e. Die privaten Schlüssel n, d.
5. **Verschlüsselung der Nachricht N:** Alice verschlüsselt die Nachricht für Bob mit dessen öffentlichen Schlüssel:
$$S = N^e \mod n.$$
6. **Entschlüsselung der Nachricht N:** Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel:
$$N = S^d \mod n.$$

Wir möchten kurz zeigen, dass die Entschlüsselung wirklich funktioniert. Sie beruht in erster Linie auf dem Satz von Euler und der Tatsache, dass d ein inverses Element zu e ist:

$$\begin{aligned} S^d \mod n &= N^{ed} \mod n, \quad \Big| \; ed = 1 \mod \varphi(n) \Rightarrow \exists k \in \mathbb{Z} : \; ed = 1 + k\varphi(n) \\ &= N^{1+k\varphi(n)} \mod n \\ &= (N \mod n)(N^{\varphi(n)} \mod n)^k, \quad \Big| \; \text{„Satz von Euler“: } N^{\varphi(n)} = 1 \mod n \\ &= N \mod n \end{aligned}$$

Wir versuchen die Verschlüsselung an einem kleinen Beispiel zu nachzuvollziehen:

Beispiel 2.55

Wir möchten die Botschaft $N = 12$ verschlüsseln und wählen entsprechend $p = 5$, $q = 3$ als Primzahlen, denn $n = p \cdot q = 15 > N$. Wir wählen ein beliebiges Element $e = 7 \in \mathbb{Z}^*_{\varphi(15)} = \mathbb{Z}^*_8$. Das inverse Element zu 7 ist 7, denn $7^2 \mod 8 = 1 \mod 8$. Dann ist

$$N^e \mod n = 12^7 \mod 15 = 3 \mod 15 = S \mod n.$$

Zur Entschlüsselung rechnen wir

$$S^d \mod n = 3^7 \mod 15 = 12 \mod 15 = N \mod n.$$

Wir erhalten die ursprüngliche Nachricht.

2.9.2 Diffie-Hellmann

Der Diffie-Hellmann-Algorithmus beruht auf der Funktion des Potenzieren. Wenn eine Potenz bekannt ist, ist die Bestimmung des diskreten Logarithmus dieser Potenz beliebig schwierig. Der Algorithmus wird auch dazu verwendet, um gemeinsame geheime Schlüssel für zwei Benutzer zu erzeugen:

1. Es wird eine Primzahl p bestimmt. Es werden zwei Zufallszahlen $q_A, q_B \in \mathbb{Z}_p$ gewählt.
2. Es wird ein erzeugendes Element a der Gruppe $\mathbb{Z}^*_p$ bestimmt.
3. Alice sendet an Bob: $r_A = a^{q_A} \mod p$ und Bob an Alice $r_B = a^{q_B} \mod p$.
4. Alice rechnet $r_B^{q_A} = a^{q_A \cdot q_B} \mod p = K$. Bob rechnet $r_A^{q_B} = a^{q_B \cdot q_A} \mod p = K$. Damit kann ein privater Schlüssel K erzeugt werden.
5. Alice verschlüsselt
$$S = K \cdot N \mod p.$$
6. Bob entschlüsselt
$$N = K^{-1} S \mod p$$
. Dafür muss er zunächst das multiplikative Inverse zu K in $\mathbb{Z}^*_p$ berechnen.

Beispiel 2.56

Alice möchte die Nachricht $N = 10$ an Bob senden. Wir wählen $p = 11$, denn $p > N$, und wählen zwei Zufallszahlen $q_A = 3$ und $q_B = 4$ in $\mathbb{Z}_{11}$. Als erzeugendes

Element von $\mathbb{Z}_{11}^*$ wählen wir 8.
Alice sendet also $r_A = 8^3 \mod 11 = 6$, Bob sendet $r_B = 8^4 \mod 11 = 4$.
Alice rechnet $4^3 \mod 11 = 9$ und Bob rechnet $6^4 \mod 11 = 9$. Also ist ihr gemeinsamer geheime Schlüssel $K = 9$. Alice verschlüsselt $N = 10$ als $S = 9 \cdot 10 \mod 11 = 2$.
Bob berechnet K^{-1} von K in $\mathbb{Z}_{11}^*$. Das machen wir mit Hilfe des erweiterten euklidischen Algorithmus. Wir benötigen nur das Inverse y, also lassen wir die Spalte x weg:

p	K	y	k
11	10	0	-
9	2	1	1
2	1	-1	4
1	0	5	2

Also ist $5 \cdot 9 = 1 \mod 11$, also ist $K^{-1} = 5$. Bob rechnet also:

$$K^{-1}S \mod 11 = 5 \cdot 2 \mod 11 = 10 \mod 11 = N \mod 11.$$

Abbildungsverzeichnis